ComConsult Research

Der Netzwerk Insider

August 2012

Systematische Weiterbildung für Netzwerk- und IT-Professionals

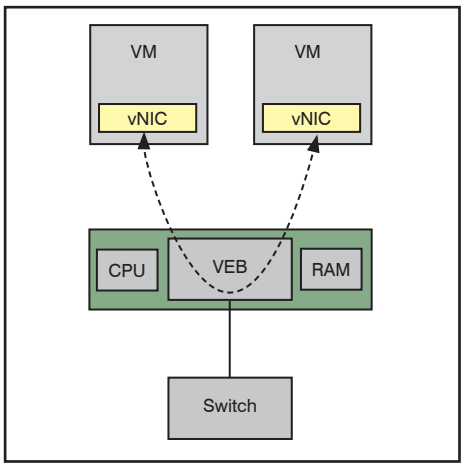
Schwerpunktthema

Virtuelle Netze - Zurück zum Soft-Switch?

von Dipl.-Inform. Damian Lukowski

Die Servervirtualisierung hat sich mittlerweile in vielen Rechenzentren als eine erprobte Technologie etabliert, mit deren Hilfe mehrere virtuelle Maschinen sich die Systemressourcen eines einzelnen physischen Hosts teilen. Werden bestimmte Ressourcen (z.B. CPU-Leistung) von einer virtuellen Maschine zu einem gewissen Zeitpunkt nicht benötigt, können diese Ressourcen von anderen Maschinen genutzt werden, ohne dass es zu Engpässen kommt.

Die Tatsache, dass mehrere virtuelle Systeme auf einem physischen Host betrieben werden, implizierte eine Ausweitung des Netzwerks in den Host hinein, und



damit ein erstes Umdenken im Netzdesign. Da die Anzahl virtueller Maschinen auf einem Host die Anzahl der verfügbaren physischen Schnittstellen mit Leichtigkeit übersteigt, teilen sich im Allgemeinen mehrere VMs einige wenige Host-Schnittstellen zur Kommunikation mit der Außenwelt. Innerhalb des Hosts werden die virtuellen Schnittstellen (vNICs) mehrerer VMs sowohl miteinander als auch mit dem Uplink-Port verschaltet; der Hypervisor implementiert eine virtuelle Ethernet Bridge in Software. VMware hat dem Konstrukt einen schöneren Namen gegeben (virtueller Switch, vSwitch), Citrix und Microsoft nennen es in ihren Produkten ein „virtuelles Netzwerk“ (≠ VLAN).

weiter auf Seite 12

Zweitthema

IPv6 und Sicherheit - technische Ansätze, der Weg zum Sicherheitskonzept

von Dipl.-Inform. Oliver Flüs

IPv6 steht vor der Tür – und die Fragestellung eines sicheren Umgangs damit hat den Fuß mindestens schon in der Tür. Wie in einem früheren Insider-Artikel mit Blick auf IPv6 und Sicherheit dargelegt wurde, gibt es nicht nur die Aufforderung der IETF an Hersteller von IT-Produkten, IPv6 nicht länger als „Option“ zu betrachten, sondern erste Hersteller, die IPv6-fähige Lösungen auch schon anbieten.

Insbesondere Microsoft zwingt mit seinen neuesten Betriebssystemversionen dazu, sich mit der Thematik auseinanderzusetzen, da es einen vor die Wahl stellt, IPv6 eingeschaltet zu lassen und damit eine neue Angriffsfläche für böse Buben zu bieten oder aber IPv6 konsequent zu deaktivieren, dies jedoch auf eigene Gefahr, nämlich unter Inkaufnahme von Seiteneffekten, vor denen auch mehr oder weniger deutlich gewarnt wird.

weiter auf Seite 23

Geleit

Scheitert UC an mobilen Endgeräten?

ab Seite 2

Aktuelle Kongresse

ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012

ComConsult TK-, UC- und Videokonferenzforum 2012

ab Seite 4

Standpunkt

Neue WLAN auf dem Vormarsch!

auf Seite 22

Neuerscheinung

Moderne Wireless-Technologien

auf Seite 21

Zum Geleit

Scheitert Unified Communications an mobilen Endgeräten?

In der traditionellen TK-Welt hat ein Benutzer einen Desktop-PC und ein Telefon. Beide Systeme haben etwas gemein: der normale Benutzer kann den Funktionsumfang nur sehr beschränkt benutzen, da die Bedienoberflächen mehr eine intellektuelle Herausforderung als eine Hilfe waren.

Dann kam Unified Communications UC mit zwei wesentlichen Zielen. Zum einen sollten noch mehr Funktionen in bereits unbedienbare Systeme integriert werden und zum anderen sollten zwei Benutzerfeindliche Welten vereint werden. Und die Überraschung war groß, als die Benutzer aus kaum nachvollziehbaren Gründen die Nutzung der neuen Funktionen verweigerten. Inkonsistente Clients, verschiedene Clients auf verschiedenen Endgeräten, Aufteilung von Funktionen auf mehrere Clients, Funktionen wild in Untermenüs versteckt, die Liste der Hürden für den Benutzer könnte nicht länger sein.

Dann kam der Tag, der die Industrie veränderte. Apple führte das iPhone ein und zeigte einer Jahrzehnte alten Industrie, dass ihre Produkte aus Sicht der Benutzer in den Mülleimer gehören. Wo sie dann auch konsequenter Weise seitdem landen. In der Mobilfunk-Welt ist seitdem nichts mehr wie es vorher war. Apple, Samsung und HTC dominieren die Welt. Weitere Android-Anbieter wie Huawei werden ggf. in den nächsten Jahren folgen. Nokia sucht seine Rettung bei Microsoft, das sagt alles.

Und was passiert in der UC-Welt? Obwohl mittlerweile 5 Jahre vergangen sind seitdem Steve Jobs das iPhone vorstellte passierte lange Zeit nichts. Dann kam Microsoft mit Lync und für alle überraschend einem Produkt, das den Client und das Benutzererlebnis in den Mittelpunkt stellt. Zwar bisher nicht perfekt, aber doch deutlich besser als bei den meisten Mitbewerbern. Und endlich begannen die Hardware-zentrischen TK-Anbieter inklusive Cisco zu reagieren. Und so können wir jetzt in den nächsten 18 Monaten endlich eine Welle neuer Clients mit einem Benutzer-zentrischen Design erwarten.

Reicht das? Die Antwort ist nein. Es ist schön, dass die TK-Hersteller jetzt auf eine Entwicklung reagieren, die vor 5 Jahren begonnen hat. Aber dummerweise ist die Technologie mobiler Endgeräte in der Zwischenzeit nicht stehen geblieben.

Und speziell für UC war die Einführung des iPads ein ganz gravierender Meilenstein. Ein iPhone oder auch ein Samsung Galaxy sind zu klein, um alle UC-Funktionsbereiche sauber abzudecken. Speziell für die Webkonferenz und das Lesen von Folien und Texten reicht ein Smartphone nicht aus, überhaupt der gesamte Dokumenten- und Videobereich machte auf dem Smartphone nur Sinn, solange es kein iPad gab. Wer schon lange auf das universelle mobile Kommunikationsgerät gewartet hat, der weiß nun wie es in Zukunft eventuell aussehen wird. Es fehlen vernünftige HD-Kameras und die Integration der Telefonie, aber das ist eine Frage der Zeit.

Aha, dann brauchen wir jetzt also nur noch den passenden Client für Smartphone und iPads und UC ist gerettet? Leider nein, wir haben ein neues Problem. Mit iOS und Android kam ein neues Konzept von intuitiver Bedienbarkeit. UC war entstanden, um die Komplexität verschiedener aufwendiger Funktionsbereiche mit einem leicht bedienbaren Client zu beseitigen. Wie wir inzwischen wissen, ist das gescheitert, weil die Entwickler wohl dieses Ziel nicht gekannt haben. Aber für iOS und Android hat dieses Ziel an Bedeutung verloren. Die meisten Apps sind intuitiv bedienbar, es gibt keinen messbaren Mehrwert in der Integration dieser Apps in einer zentralen App.

Ist UC damit am Ende? Das hängt davon ab, wie wichtig der Kommunikations-Übergang zwischen Apps ist. Besteht das Ziel aus einer Sprach-App lückenlos in eine Video-Kommunikation zu wechseln, dann braucht man ein System, das beide zusammen führt. Sollen Erreichbarkeits-Stati über verschiedene Apps integriert werden, braucht man ein entsprechendes System. Sollen Apps mit einem Hardware-Telefon und einem Desktop-PC integriert werden, braucht man auch dafür eine Lösung, die den Funktionsrahmen der Einzel-App eventuell sprengt. Aber auch hier ist Vorsicht geboten. Immerhin haben wir Standards wie SIP, denen auch die Apps folgen können, um dieses Ziel zu erreichen.

Zumindest haben die TK-Hersteller den Zahn der Zeit erkannt. Hinter den Kulissen herrscht aufgeregte Hektik, alle arbeiten an neuen Endgerätetypen und Clients. Cisco Cius und Avaya Flare sind Beispiele dafür.

Also doch Hoffnung? Eine Frage bleibt weiterhin im Raum stehen: wissen die TK-Hersteller eigentlich, dass Unternehmen ihr Geld mit Kunden verdienen? Die Effizienz und Qualität der Kommunikation mit Kunden ist der entscheidende Punkt. Dem gegenüber ist es schon peinlich, wenn die Anbieter die Sekunden-Bruchteile ausrechnen, die Unternehmen intern sparen können, wenn es eine bessere interne Erreichbarkeit gibt. Was könnte das Versagen einer ganzen Industrie besser zum Ausdruck bringen! Dabei gab es Lösungsansätze. Wir haben immer noch das Video eines UC-Forums, auf dem Cisco eine Lösung zur Kommunikation über Unternehmensgrenzen vorgestellt hat. Die sah auch ziemlich gut aus. Sie verschwand so schnell wieder vom Markt, dass man nur spekulieren kann, warum das so war. Aber wer wird schön Übles dabei denken, wenn die Provider mit die größten Kunden von Cisco sind. Und so wird vermutlich die alles entscheidende Technologie der Einbeziehung der Kunden vom Diktat einiger weniger weltweit dominanter Anbieter blockiert.

Macht UC dann überhaupt noch Sinn? Keine Sorge, wir haben ja noch Microsoft. Microsoft muss sich dem Diktat nicht unterwerfen. Und die Übernahme von Skype deutet an, wo es hingeht. Eine Federation zwischen Lync und Skype könnte den gesamten Markt umdrehen. Zum Ende des Jahres kommt die neue Lync-Version und Microsoft wird seine Ansätze auf dem ComConsult TK-, UC- und Videokonferenz-Forum vorstellen.

Die spannende Frage lautet nun: muss

Scheitert Unified Communications an mobilen Endgeräten?

sich nun das Kartell der Verweigerer bewegen? Werden endlich die Interessen der Kunden in den Vordergrund gestellt? Dazu gehört auch die Nutzung verfügbarer und bisher konsequent verweigerter Video-Standards. Wir brauchen dringend eine HD-Konferenz auf der Basis von 512 kBit/s, um Home-Offices anbinden zu können und internationale Standorte mit geringerer Broadband-Qualität. Die Technik ist seit Jahren verfügbar, es fehlen Kleinigkeiten im Standard, aber wenn man wirklich gewollt hätte, hätte man diese Probleme lösen können. Aber wer sein Geld mit MCUs verdient, der unterstützt eine neue Technologie, die MCUs überflüssig macht, natürlich nicht gerne. Aber auch hier wird Microsoft hoffentlich die Blockade brechen. Gleichzeitig hat LifeSize eine virtualisierte MCU angekündigt, immerhin eine Alternative für kleinere Unternehmen und gut geeignet, um die typischen mobilen Teilnehmer zu integrieren.

Fassen wir es zusammen:

- Es gibt klar benennbare Gründe, warum UC bisher nicht so erfolgreich ist wie es eigentlich sein sollte.
- Aber der Markt ändert sich. Benutzerzentrische Clients und neue Bedienkonzepte überwinden bestehende Hürden.
- Das wird aber nicht ausreichen. Der eigentliche Mehrwert entsteht in der Kommunikation mit dem Kunden. Aber auch hier ist Bewegung in einen blockierten Markt gekommen.

Die Schlussfolgerung ist klar: wir werden in den nächsten 12 bis 24 Monaten endlich an den Punkt kommen, den wir seit über 10 Jahren anpeilen. Das ist zwar alles andere als schmeichelhaft, aber immerhin ist Licht am Ende des Tunnels. Trotzdem hat sich der Markt inzwischen geändert. Die Rahmenbedingungen machen die weitere Entwicklung sehr spannend.

Genau an diesem Punkt setzen wir mit unserem diesjährigen ComConsult TK-, UC- und Videokonferenzforum 2012 an. Es erwartet uns eine spannende Veranstaltung.

Ihr
Dr. Jürgen Suppan

Aktueller Kongress

ComConsult TK-, UC- und Videokonferenzforum 2012

19.11. - 22.11.12 in Düsseldorf

Frühbucherphase bis zum 30.09.12

Die ComConsult Akademie veranstaltet vom 19.11. bis 22.11.12 ihr "ComConsult TK-, UC- und Videokonferenzforum 2012" in Düsseldorf.

Dieses hochaktuelle Forum analysiert Trends, neue Technologien, sowie Produkt- und Hersteller-Strategien im Bereich TK, UC und Videokonferenztechnik. In diesem Jahr stehen fünf Themen im Mittelpunkt des Forums:

Wie viel UC braucht TK?
Telefonieren muss Jeder, aber wie viel Unified Communication wird wirklich benötigt und welche Alternativen der Umsetzung gibt es? Wir analysieren:

- Wo stehen integrierte Lösungen, die TK und UC aus einem Guss liefern?
- Wie sinnvoll sind Ergänzungs-Lösungen, die mehr TK-orientierte Installationen durch eine externe UC-Lösung ergänzen?
- Was bieten die Hersteller?
- Welche Lösungen werden bevorzugt umgesetzt?
- Welche Anforderungen stellt der Mittelstand an die Kommunikationsinfrastruktur?

Zukunftsweisende Client-Strategien – Welche Bedeutung haben mobile Endgeräte in Zukunft und wie werden sie integriert?
Für viele Benutzer ist der zeitgleiche Umgang mit mehreren Endgeräten inzwischen die Normalität. Der traditionelle Ansatz mit Desktop PC und Telefon wird der aktuellen Lage nicht mehr gerecht. Nach Apple und Google wird nun auch Microsoft den Markt der mobilen Endgeräte attackieren – und bietet erstmals eine einheitliche Plattform für alle Endgeräte. Parallel bieten die mobilen Endgeräte ein völlig neues Bedienverständnis, das speziell UC unter erheblichen Druck setzt. Wir analysieren:

- Welche Rolle spielen mobile Endgeräte in Zukunft?
- Lassen mobile Endgeräte die Bedienbarrieren zwischen verschiedenen Apps verschwinden? Brauchen wir dann UC überhaupt noch?
- Wie sieht UC im Umfeld mobiler Endgeräte aus? Wie spielen die verschiedenen Geräte zusammen?
- Wohin entwickelt sich die Client-Technik auf mobilen Geräten?
- Was passiert mit privaten iPads und iPhones, die dienstlich genutzt werden sollen?

User Centric Communications UCC
Nach der Infrastrukturkonvergenz rückt der Anwender von UC-Lösungen wieder in den Mittelpunkt. UC kann nur funktionieren, wenn der Client alle Funktionen intuitiv nutzbar umsetzt. Hieran scheitern bisher fast alle Lösungen. Anders im Bereich der mobilen Kommunikation: Apple hat mit dem iPhone den Markt verändert und den Benutzer in die Mitte der Architektur gestellt. Traditionelle Anbieter wie Nokia sind mit ihren Bedienkonzepten in der Versenkung verschwunden. iOS und Android prägen heute das Verständnis der Benutzer in der Handhabung auch komplexer Kommunikations-Funktionen. Unter den inzwischen weit verbreiteten Apps auf den mobilen Geräten befinden sich viele Apps, die Funktionalität aus dem Bereich UC anbieten. An diesen Lösungen aus dem Konsumenten-Markt muss sich UC messen lassen. UC wird nur überleben, wenn Benutzer-zentrische Lösungen von den Herstellern auch tatsächlich umgesetzt werden. Wir analysieren:

- Von UC zu UCC: was bedeutet das?
- Die Rolle von Social Media im Unternehmensumfeld
- Neue Messaging Dienste und ihre Nutzung
- UCC aus der Cloud: eine wirkliche Alternative?
- Wie sollte der ideale Client aussehen?
- Sollte es einen einheitlichen Client über alle Plattformen geben?

Der Kunde, das unbekannte UC-Wesen?
Unternehmen verdienen ihr Geld mit Kunden. Aber genau an dieser Stelle hören UC-Lösungen typischerweise auf. Dabei liegt genau hier der größte potenzielle Mehrwert. Das Contact Center ist dabei einer der Angelpunkte der Unternehmenskommunikation. Hier entfalten moderne Kommunikationsplattformen und Social Media ihr volles Potenzial. Wir analysieren:

- Welche Alternativen der Einbindung externer Kommunikationspartner gibt es?
- Wann kommt die wirklich offene UC-Lösung?
- Ist Skype die Lösung und welche Rolle spielt die Skype-Integration in Microsoft Lync?
- Das Contact Center – Zwischen Vermittlungsplatz 2.0 und Social Media Hub.

Videokonferenz in der Sackgasse?
Die Anbieter von Videokonferenz-Lösungen treten seit Jahren auf der Stelle. Genau die im Marketing immer wieder beschworene Integration aller Mitarbeiter und Kunden in eine Gesamtlösung, also der Übergang von einer teuren Lösung für wenige Teilnehmer hin zu einer bezahlbaren Lösung für viele erfolgt im Rahmen von UC bisher nicht. Dabei fordert die Explosion mobiler Endgeräte mit Diensten wie Fuze und WebEX aber genau diesen Übergang. Wir analysieren:

- Wie sieht die Video-Konferenz-Lösung der Zukunft aus?
- Wird die Webkonferenz die Videokonferenz verdrängen?
- Welche neuen Standards sind wann verfügbar und verändern sie die Welt?

In einem weiteren Schwerpunkt widmen wir uns dem aktuellen Portfolio der Hersteller. Mit Cisco Jabber erzielt erstmals ein Konkurrent eine vergleichbar tiefe Integration in die Client-Welt wie Microsoft Lync. Aber auch die Konkurrenz schläft nicht und feilt eifrig an intuitiven Bedienkonzepten. Microsoft legt mit Lync 2013 nach. Wie die Hersteller die Anforderungen der Kunden lösen wollen und wie sie sich strategisch positionieren erfahren Sie im Rahmen des Intensivtages:

- Wie setzt Microsoft den Markt mit dem neuen Release unter Druck?
- Welche Konzepte verfolgen die anderen Hersteller?
- Wie setzen die Hersteller die Kundenanforderungen um?
- Was kommt in den nächsten Jahren?

Das ComConsult TK-, UC- und Videokonferenzforum 2012 bietet Top-aktuelle Information und Analysen mit ausgewählten Experten. Eine ausgewogene Mischung aus Analysen, Hintergrundwissen und Projekterfahrungen in Kombination mit Produktbewertungen und Diskussionen liefert das ideale Umfeld für alle Planer, Betreiber und Verantwortliche solcher Lösungen. Zögern Sie nicht, sich rechtzeitig einen Platz in dieser herausragenden Veranstaltung zu sichern.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
ComConsult TK-, UC- und Videokonferenzforum 2012

☐ 3 Tage	☐ 4 Tage	☐ 1 Tag
Kongress vom 19. - 21.11.12 in Düsseldorf zum Preis von € 1.890,-- netto*	**Kongress mit Intensiv-Tag** vom 19. - 22.11.12 in Düsseldorf zum Preis von € 2.290,-- netto*	**Intensiv-Tag** am 22.11.12 in Düsseldorf zum Preis von € 790,-- netto*

*Preise gültig bis zum 30.09.12. Die Buchung eines Kongresses innerhalb der Frühbucherphase kann nicht storniert werden. Gerne akzeptieren wir aber einen Ersatzteilnehmer.

☐ **Bitte reservieren Sie für mich ein Hotelzimmer**

vom _____ bis zum _____12
im Van der Valk Airporthotel Düsseldorf.

Selbstzahler-Sonderpreis von € 139,-- pro Übernachtung inklusive Frühstück

Zusätzlich bestelle ich folgenden Technologie-Report

☐ Session Initiation Protocol - zum Sonderpreis von 338,- € netto

☐ Unified Communications: Cisco versus Microsoft - zum Sonderpreis von 338,- € netto

☐ Sicherheitsmechanismen für Voice over IP - zum Sonderpreis von 338,- € netto

☐ VoIP-Kollektion - alle drei Reports zum Sonderpreis von 890,- € netto

_____
Vorname

_____
Nachname

_____
Firma

_____
Straße

_____
PLZ, Ort

_____
Telefon, Fax

_____
E-Mail

Ich habe die Kongressbedingungen zur Kenntnis genommen.

_____
Unterschrift

ComConsult Akademie
Pascalstraße 25 - 52076 Aachen
Telefon +49 (2408) 955-300
info@comconsult-akademie.de
www.comconsult-akademie.de

Aktueller Kongress

ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012

05.11. - 08.11.12 in Köln

Die ComConsult Akademie veranstaltet vom 05.11. bis 08.11.12 ihr "ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012" in Köln.

Unsere Rechenzentren befinden sich in einer der größten Redesign-Phasen der letzten 20 Jahre. Nahezu alle Gestaltungs-Bausteine von den Servern, Speicher-Technologien, Netzwerken bis hin zu den Applikations-Architekturen sind im Umbruch. Gleichzeitig entstehen durch eine Explosion mobiler Teilnehmer auf der einen und durch Cloud-Technologien auf der anderen Seite völlig neue Rahmenbedingungen.

RZ-Architekturen und Infrastrukturen: wohin geht der Weg?
Neue Server, Zweifel an Virtualisierung, immer mehr Leistung auf der Speicher-Seite, neue Anwendungs-Architekturen, Integration in die Cloud und neue Anforderungen durch Endgeräte: hier ist eine klare Linie gefordert, damit die Bausteine sinnvoll zusammen spielen und die Gesamtleistung des RZ nicht gefährdet ist. Wir analysieren die Fragen:

- Was passiert auf der Serverseite?
- Ist Virtualisierung in der bekannten Form am Ende?
- Immer mehr Leistung auf der Speicherseite: was bedeutet das?
- Netzwerk-Infrastrukturen: völlig neue Konzepte gefordert?
- Was bedeutet die Explosion mobiler Endgeräte für die RZ-Infrastrukturen?
- Private oder Public Cloud: was ist zu tun?

Sicherheit in einer immer komplexeren RZ-Umgebung
Die Komplexität der Architektur nimmt immer weiter zu. Eine zunehmende Abhängigkeit der verschiedenen Technologiebereiche voneinander, neue Formen schlecht kontrollierbarer Endgeräte, eine zunehmende Öffnung der Architekturen durch Mehr-Standort-Konzepte , eine Cloud-Integration und Webdienste für Kunden und Zulieferer erfordern weitreichende Sicherheits-Konzepte. Wir analysieren die Fragen:

- Wie Praxis-tauglich sind Mandanten-fähige Lösungen?
- An welcher Stelle soll Sicherheit erbracht werden?
- Was leisten Zonen- und Firewall-Architekturen?
- Möglichkeiten und Grenzen typischer Lösungsansätze
- Wie sieht eine sinnvolle Trennung geschäftlicher und privater Daten und Applikationen aus?
- Was leisten Sandboxing, Server-based Computing und Virtualisierung?
- Wie erfolgreich können Zonenkonzepte eingesetzt werden?

Web-Architekturen im RZ
Immer mehr mobile Teilnehmer auf der Kunden- und Zulieferer-Seite erfordern neue Lösungen im Rechenzentrum. Die Möglichkeiten einer besseren und effizienteren Ansprache und Einbindung von Kunden, Partnern und Zulieferern müssen genutzt werden. Web-Applikationen sind das Mittel der Wahl. Aber was bedeutet das? Wir analysieren für Sie:

- Was macht moderne Webanwendungen aus?
- Wie kann Skalierbarkeit als Architekturmerkmal umgesetzt werden?
- Wie erhalten Kunden, Partner und eigene Mitarbeiter den Zugang?
- Sind Apps für Windows, Android und iOS eine Option?
- Welche Konsequenzen hat das für die Sicherheit des RZ?

Netzwerk-Infrastrukturen: die Achillesferse unter Druck
Immer mehr Leistung wird in immer weniger Knoten konzentriert. Das gilt für Server aber auch für Speicher-Systeme. Auf der einen Seite explodiert der Bandbreitenbedarf, auf der anderen Seite stellt sich die Frage, ob traditionelle Netzwerk-Ansätze nicht bald überholt sind. Wir analysieren für sie:

- Performance Optimized Data Centre POD: liegt hier unsere Zukunft?
- Was bedeuten neue Technologien für das Netzwerk der Zukunft?
- Neue Chips für 10 und 100 Gigabit: kommt die Revolution?
- Software Defined Networking: die Lösung für immer komplexere Netzwerke und Mandantenfähigkeit?
- TCP/IP: erzwingt immer mehr Leistung neue Formen der Implementierung?
- Das RZ im Schrank: liegt hier unsere Zukunft?

Mobile Endgeräte und BYOD
Die Zeiten, in denen Mitarbeiter genau ein Endgerät hatten, sind vorbei. Mobile Endgeräte explodieren und Smartphones und Tablets verändern die IT. Wir werden in Zukunft mehr mobile als stationäre Endgeräte haben und Apps werden das traditionelle Applikations- und Sicherheitsverständnis auflösen. Wir analysieren für Sie:

- Wie wichtig wird Bring Your Own Device BYOD?
- Was bedeutet das für die Datenhaltung?
- Welche Rückwirkungen hat das für Unternehmens-eigene Endgeräte?

Virtualisierung
Nahezu alle Unternehmen haben Virtualisierung in der Grundform umgesetzt. Jetzt entstehen neue Herausforderungen. Zum einen entstehen neue Formen von Virtualisierung, zum anderen wird die Notwendigkeit von Virtualisierung in Frage gestellt. Was bedeutet das? Wir analysieren für Sie:

- Wie positionieren sich Hersteller strategisch?
- Was passiert bei VMware, Cirtix und Microsoft in nächster Zeit?
- Welche Relevanz hat das für das RZ?
- Welche Auswirkungen haben verteilte RZ-Architekturen auf die erforderlichen Infrastrukturen?
- Anbindung virtueller Server: gibt es die optimale Lösung?

Speicher-Technologien
Der Bedarf an Speicher wächst ohne erkennbare Grenze. Speziell unstrukturierte Daten explodieren. Kombiniert man das mit der notwendigen Zentralisierung von Speicher, entstehen massive Anforderungen an Leistung und Funktionalität. Aber speziell Funktionalität hat ihren Preis. Welche der High-End-Funktionen werden wirklich gebraucht und wie erreicht man eine wirtschaftlich und technisch optimale Lösung? Wir analysieren für Sie:

- Was sind die aktuellen Technologien, was sind die Trends für die Zukunft?
- Wo steht der Markt?
- Welche Optionen der Einbindung existieren?
- Wie sinnvoll ist Hierarchisches Speicher-Management?
- Ist Auto-Tiering der Schlüssel zum Erfolg?

Das ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012 greift die herausragenden Fragen der Umsetzung zukunftsorientierter und wirtschaftlicher Rechenzentren auf. Mit nahezu allen betroffenen Technologien im Umbruch ist dies das richtige Forum zum richtigen Zeitpunkt. Zögern Sie nicht, sich hier rechtzeitig einen Platz zu sichern.

Programmübersicht - ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012

Montag, den 05.11.2012

9:30 bis 10:45 Uhr
Neue IT-Technologien und die Auswirkungen auf RZ-Infrastrukturen
- Cloud-Technologien im Unternehmen: was bedeutet das?
- Neue Endgeräte-Technologien und Auswirkungen auf Architekturen
- Infrastrukturen für mobile Endgeräte • Gibt es den Server der Zukunft?
- Wie wichtig wird OpenStack? • Virtualisierung: am Anfang oder am Ende?

Dr. Jürgen Suppan, ComConsult Research Ltd.

10:45 - 11:15 Uhr Kaffeepause

11:15 bis 12:30 Uhr
Analyse: Data-Center-Architekturen:
- Architekturmodell für die Unterstützung kooperierender Web-Anwendungen • Aktuelle Entwicklungen der Schaltkreistechnologie und Auswirkungen auf zukunftssichere Investitionen
- Traditionelle Netzwerke am Ende? SDN und Open Flow ändern unser Verständnis von Netzwerken
- Leistungsfähige Alternativen der VM-Anbindung

Dr. Franz-Joachim Kauffels, freier Unternehmensberater

12:30 bis 14:00 Uhr Mittagspause

14:00 bis 14:45 Uhr
Analyse: Server-based Computing, Virtualisierung und Cloud Computing
- Kapselung von Daten und Anwendungen im RZ mit Server-based Computing und Desktop Virtualisierung
- Gefährdungen durch Zentralisierung von Clients
- Malware-Schutz: Umdenken ist erforderlich
- Data Center Firewalls: Neue Konzepte und deren Tücken
- Kerndisziplin: Data Loss Prevention (DLP)
- Sicherheitsarchitekturen für Private Clouds
- Rolle von Public Clouds für die Enterprise IT
- Anforderungen an sichere Public Clouds

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

14:45 bis 15:30 Uhr
Mandantenfähigkeit und Zonenkonzepte im RZ
- Mandantenfähige RZ-Netze: Techniken und deren Praxistauglichkeit
- Brauchen wir angesichts Server-based Computing und Cloud Computing noch Sicherheitsmaßnahmen im Netz?
- Zonen- und Firewall-Architekturen im RZ
- Zwiebelschalen-Modelle im Widerspruch zu Mehrmandantennetzen

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

15:30 bis 16:00 Uhr Kaffeepause

16:00 bis 16:45 Uhr
Sicherer Betrieb von Zonenarchitekturen
- Terminal Server als Jump Host: Möglichkeiten und Grenzen
- Virtualisierungstechniken zur sicheren Entkopplung administrativer Zugriffe
- Zonen für die Administration und Überwachung: Firewall-Infation droht
- SIEM: Sondermülldeponie oder sinnvolles Instrument des Security Incident Management? • Kurzschluss in SAN und NAS vermeiden

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

16:45 bis 17:30 Uhr
Web-Anwendungen im Rechenzentrum
- Webanwendungen: mehr als nur Webseiten
- Architektur und Skalierbarkeit
- Integration von Kunden, Partnern und Mitarbeitern
- Windows, Mac, iOS, Android: eine App für alle?
- Sicherheitsrelevante Aspekte • Was bringt die Zukunft?
- Empfehlungen

Markus Schaub, ComConsult Research Ltd.

17:30 bis 18:00 Uhr
Service-basierte Netzwerke: das Ende des normalen Netzwerk-Designs
- Mandentenfähigkeit und Trennung von Datenströmen über L2/L3-Grenzen gefordert
- MPLS hat im Enterprise ausgedient
- L2/L3-Abgrenzungen sind Diskussionen von Gestern
- VXLAN ohne die Komplexität von PIM /PIM-SM/PIM-SSM etc.
- L2/L3-übergreifende Multicast-Dienste sind erforderlich
- Vision: Anwendungs-orientierte Netzwerk-Services

Heinz Behrens, Avaya GmbH & Co KG

Ab 18:00 Uhr Get Together

Dienstag, den 06.11.2012

9:00 bis 10:00 Uhr
Performance Optimized Data Center POD
- Bedarf für modulare Data Center Lösungen
- Was ist ein POD (Performance Optimized Data Center, Point of Delivery, Point of Deployment)?
- POD Architektur-Elemente (Container, Server-Block, Storage-Block, Netzwerk-Block) • Referenz-Architekturen
- POD-Beispiele (Cisco VMDC, Dell vStart, HP EcoPOD, IBM PMDC, SGI CloudRack)

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN Unternehmensberatung

10:00 bis 11:00 Uhr
Auf dem Weg zum RZ und den Infrastrukturen der Zukunft
- Migration DC zum Fabric enabled DC
- POD Design und Cloud Ready
- Überblick SW Router CSR1000v: liegt hier die Zukunft für virtuelle Umgebungen? • Erster Blick auf „onePK“
- Ciscos Sicht zu SDN/OF

Gerd Pflueger, Matthias Wessendorf, Cisco Systems GmbH

11:00 bis 11:30 Uhr Kaffeepause

11:30 bis 12:15 Uhr
Optimierte Switche für den RZ-Bedarf
- Erfüllen Standard-Chip-Architekturen den Bedarf?
- Vorteile einer offenen Linux-Lösung
- Software Defined Networking
- Low Latency
- Wieviel Stromverbrauch darf es ein?
- Wie wichtig wird VxLAN?

Manfred Felsberg, Frank Laforsch, ARISTA Networks, Inc.

12:15 bis 12:45 Uhr
Technologie-Statements

12:45 bis 14:00 Uhr Mittagspause

14:00 bis 14:45 Uhr
Positionierung der TCP/IP-Intelligenz
- Welche Alternativen gibt es? • Ist Offload wirklich die beste Lösung?
- Vor- und Nachteile, Empfehlung

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

14:45 bis 15:30 Uhr
RZ-Netze: Evolution oder Revolution?
- Mängelbereiche bisheriger Konstruktionen
- Entwicklung von Switching-Substraten mit speicherbasierenden ASICs
- SDN: neuer Provider-Hype oder nutzbar für alle?
- Das RZ im Schrank • Migrationsempfehlungen

Dr. Franz-Joachim Kauffels, freier Unternehmensberater

15:30 bis 16:00 Uhr Kaffeepause

16:00 bis 16:45 Uhr
BYOD, DLP und mobile Virtualisierungs-Technologien
- Welche Anforderungen stellt BYOD an die Datenhaltung?
- Sind diese Anforderungen auch für Company-owned-Devices relevant?
- Welche Technologien eignen sich zur Trennung privater und geschäftlicher Daten?
- Was ist mobile DLP und eignet es sich zur Umsetzung von BYOD/COD?
- Sandboxing, Server-based Computing und Virtualisierung - ein Überblick

Dominik Zöller, ComConsult Beratung und Planung GmbH

16:45 bis 17:30 Uhr
Smartphones, Tablets und der Gast-Zugang
- Einsatzszenarien für mobile Endgeräte im Unternehmen
- Mobile und nomadische Nutzung von Smartphones & Tablets
- Netzanbindung via 3G/4G und WLAN
- BYOD, Zonenkonzepte und Gastzugänge

Dominik Zöller, ComConsult Beratung und Planung GmbH

Programmübersicht - ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012

Mittwoch, den 07.11.2012

9:00 bis 09:45 Uhr
Aktuelle Trends und Entwicklungen am Hypervisor-Markt
- Welche entscheidenden Neuerungen brachte die VMworld 2012 für den VMware ESX?
- Was wurde auf der Synergy 2012 in puncto Citrix XenServer vorgestellt?
- Wie hat Microsoft im Windows Server 2012 seine Virtualisierungsplattform Hyper-V verbessert?
- Welche Relevanz haben diese Entwicklungen auf aktuelle Data Center Designs?
- Wie haben sich die Hersteller damit strategisch positioniert?

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

9:45 bis 10:30 Uhr
Automatic Storage Tiering: Wunderwaffe oder technischer Overkill?
- Herausforderung exponentiellen Speicherwachstums
- Hierarchisches Speicher-Management (HSM), Information Lifecycle Management (ILM) und ihre Grenzen
- Voraussetzung: Definition unterschiedlicher Speicherklassen (Storage Tiers)
- Wie funktioniert Automatic Storage Tiering?
- Welche Unterschiede gibt es bei den marktführenden Storage-Systemen?
- An welche Grenzen stößt dieser technische Ansatz?
- Wie positionieren sich die Hersteller?
- Welche Strategie sollte im modernen Data Center verfolgt werden?

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

10:30 bis 11:00 Uhr Kaffeepause

11:00 bis 11:45 Uhr
Zukunftsorientierte Speicherlösungen und -methoden
- Herausforderungen an Speicherlösungen
- Senkung der Investitionskosten
- Eindämmung der Betriebskosten
- Enterprise Funktionalitäten zu einem auch für kleine Unternehmen bezahlbaren Preis

Dr. Georgios Rimikis, Hitachi Data Systems GmbH

11:45 bis 12:30 Uhr
Service-orientierte Infrastruktur: Konvergierte HP-Lösungen für das RZ
Florian Bettges, Hewlett-Packard GmbH

12:30 bis 14:00 Uhr Mittagspause

14:00 bis 14:45 Uhr
Aktuelles zu IBM XIV Storage
- Neue Ankündigungen
- Ausblick
- Kundenbeispiel
- Live-Demo

Dirk Vogelsang, IBM Deutschland GmbH

14:45 bis 15:30 Uhr
Projektbericht Datensicherung
- Herausforderung: Einheitliche Backup-Landschaft für eine komplexe Systemumgebung
- Backup2Disk- versus Backup2Tape-Lösungen
- Chancen durch den Einsatz moderner VTLs
- Backup- & Redundanzkonzepte für Datenbanken

Dipl.-Ing. Peter Koch, inforsacom Informationssysteme GmbH

15:30 bis 16:15 Uhr
Virtualisierte Serveranbindung: Kampf der Konzepte
- Software-basierte vSwitches
- Direct I/O
- Probleme bei der vMotion+FT
- Hybrides Treiber-Design, SR-IOV
- Unterstützung der offenen Standards
- VMware vCloud
- VXLAN
- STT
- NVGRE

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

16:15 Uhr Ende der 3-tägigen Veranstaltung
Kaffeepause für Teilnehmer der 4-tägigen Veranstaltung

Donnerstag, den 08.11.2012 - Cloud Computing und die Auswirkungen auf das Rechenzentrum der Zukunft

9:00 bis 09:45 Uhr
Analyse: Was leistet Cloud-Computing: was leistet es und wo sind die Grenzen?
- Ziele, Vorteile und Versprechen
- Cloud Service- und Liefermodelle im Vergleich
- Analyse der verschiedenen Lager: wer will was erreichen?
- Vor- und Nachteile von Public Cloud Diensten
- Private Cloud: die Lösung?
- Bewertung: werden die Ziele eingehalten?
- Empfehlungen für eine Cloud-Strategie

Dr. Jürgen Suppan, ComConsult Research Ltd.

9:45 bis 10:30 Uhr
Wie ist eine Private Cloud aufzubauen?
- Betriebliche und technische Anforderungen
- Auswahl des Hypervisors
- Dimensionierung der Virtualisierungsumgebung
- Cluster-Design
- DMZ-Design
- Storage-Design
- Migration und Provisioning
- Monitoring und Reporting

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

10:30 bis 10:50 Uhr Kaffeepause

10:50 bis 12:05 Uhr
Virtualisiertes RZ als Basis für die Private Cloud
- Was bedeuten HA, FT, und Disaster Recovery Mechanismen für unsere Ressourcen?
- Globale und regionale RZ-Virtualisierung
- Anforderungen an Storage und Netz

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

12:05 bis 13:00 Uhr
Public-Cloud-Marktübersicht
- Dienste aus der Public Cloud: Übersicht
- Public Cloud Produkte und Anbieter
  - IaaS
  - PaaS
  - SaaS
  - UCaaS

Dominik Zöller, ComConsult Beratung und Planung GmbH

13:00 bis 14:00 Uhr Mittagspause

14:00 bis 14:45 Uhr
Worauf ist bei der Ausschreibung von Cloud-Diensten zu achten?
- Daten- und Rechtssicherheit
- Integration in das Service-Portfolio
- Service-Vereinbarungen
- Anbietersicherheit und Rückmigration

Claus Elfering, ComConsult Beratung und Planung GmbH

14:45 bis 15:45 Uhr
Rechtliche Aspekte bei Public Clouds
- Was ist erlaubt, was nicht?
- Helfen individuelle Verträge?
- Wie wichtig ist die Unternehmens-seitige Verschlüsselung?

Ulrich Emmert, esb Rechtsanwälte

15:45 Uhr Ende der 4-tägigen Veranstaltung

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012

☐ 3 Tage	☐ 4 Tage	☐ 1 Tag
Kongress vom 05.11. - 07.11.12 in Köln zum Preis von € 1.890,-- netto*	**Kongress mit Intensiv-Tag** vom 05.11. - 08.11.12 in Köln zum Preis von € 2.290,-- netto*	**Intensiv-Tag** am 08.11.12 in Köln zum Preis von € 790,-- netto*

*Preise gültig bis zum 31.08.12. Die Buchung eines Kongresses innerhalb der Frühbucherphase kann nicht storniert werden. Gerne akzeptieren wir aber einen Ersatzteilnehmer.

☐ **Bitte reservieren Sie für mich ein Hotelzimmer**

vom _____ bis zum _____12
im Radisson Blu Hotel Köln

Selbstzahler-Sonderpreis von € 140,-- pro Übernachtung inklusive Frühstück

Zusätzlich bestelle ich folgenden Technologie-Report

☐ RZ Netzwerk-Infrastruktur Redesign
zum Sonderpreis von 338,- € netto

☐ Moderne WAN-Technologien -
zum Sonderpreis von 338,- € netto

☐ TRILL kontra SPB (802.1aq)
zum Sonderpreis von 310,- € netto

☐ RZ-Kollektion - alle drei Reports
zum Sonderpreis von 870,- € netto

Vorname _____

Nachname _____

Firma _____

Straße _____

PLZ, Ort _____

Telefon, Fax _____

E-Mail _____

Ich habe die Kongressbedingungen zur Kenntnis genommen.

Unterschrift _____

ComConsult Akademie
Pascalstraße 25 - 52076 Aachen
Telefon +49 (2408) 955-300
info@comconsult-akademie.de
www.comconsult-akademie.de

ComConsult-Study.tv

WAN-Spezial im September bei ComConsult-Study.tv

Über 6,5 Stunden geballtes Wissen rund um das Thema WAN von Dr. Franz-Joachim Kauffels! Sparen Sie über 30% gegenüber den Normalpreisen.

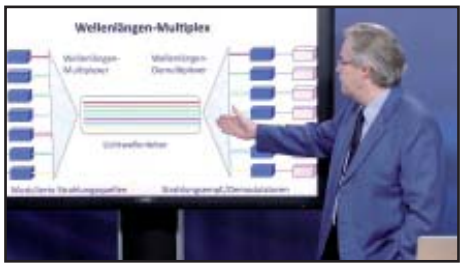
100G

Referent: **Dr. Franz-Joachim Kauffels**
Zeit: 01:29:32 gesamt
Einzelpreis: 59,00 € netto
Im Abo: kostenlos

Der Sprung auf 100 Gigabit hat für die meisten Anwender erhebliche Konsequenzen. Der Übergang von 40 auf 100 ist genau die Grenze, die viele ältere Switch-Produkte nicht überschreiten können. In diesem 3-teiligen Seminar lernen Sie, warum Sie in den nächsten 3 Jahren mit 100G rechnen müssen und wie es funktioniert.

Optische Netze

Referent: **Dr. Franz-Joachim Kauffels**
Zeit: 03:10:06 gesamt
Einzelpreis: 59,00 € netto
Im Abo: kostenlos



Optische Netze sind die Zukunft der Datenübertragung. Immer kleinere und preiswertere Komponenten mit Datenraten bis in den Terabit-Bereich legen die Basis für viele zukünftige Nutzungsformen. Dieses 10-teilige Seminar zeigt die wesentlichen Elemente, Technologien und Strukturen.

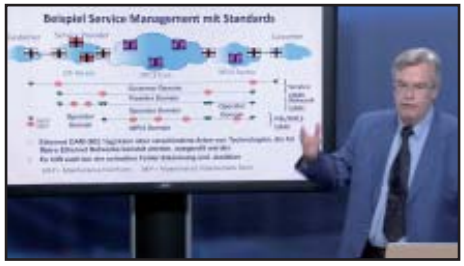
Integration optischer Komponenten: die Zukunft der Unternehmens-Netzwerke

Referent: **Dr. Franz-Joachim Kauffels**
Zeit: 0:32:12
Einzelpreis: 39,00 € netto
Im Abo: kostenlos

Optische Technik ist im Wandel. Übertragungsraten nehmen weiter zu, Komponenten werden kleiner und preiswerter. Neue Technologien ermöglichen die weitere Nutzung "alter" Fasern. Gleichzeitig gehen neue Netzwerk-Technologien wie 40/100 Gigabit-Ethernet neue Wege. Die Zukunft liegt in skalierbaren Netzwerken.

Carrier Ethernet

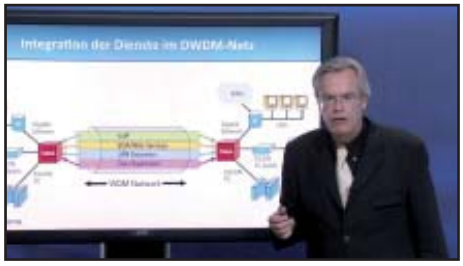
Referent: **Dr. Franz-Joachim Kauffels**
Zeit: 01:14:51 gesamt
Einzelpreis: 59,00 € netto
Im Abo: kostenlos



3-teilige Übersicht über die Konzepte und Ideen von Carrier Ethernet. Diskussion über den möglichen Einsatz innerhalb von Unternehmen.

G.709 im Unternehmens-Netzwerk

Referent: **Dr. Franz-Joachim Kauffels**
Zeit: 00:12:28
Einzelpreis: 39,00 € netto
Im Abo: kostenlos



G.709 ist das Protokoll, das in heterogenen Provider-Netzwerken für Interoperabilität sorgt. Dr. Kauffels stellt die Grundidee dieses Protokolls vor und diskutiert den Nutzen für Unternehmensnetzwerke. Dabei geht er speziell auf die Kopplung von Rechenzentren und die damit verbundene Konvergenz von Übertragungstechnologien ein.

Bundle-Erweiterung mit neuem Report Moderne WAN-Technologien

Autor: **Dr. Franz-Joachim Kauffels**
Einzelpreis: 398,-- € netto

Die Schwerpunkt-Themen dieses neuen Reports sind: Nutzungsbereiche und Individualschnittstellen von DSL zu EFM, Optische Netze, neue Modulationsverfahren und WAN-Ethernet-Standards, Strukturstandards SONET, Carrier Ethernet und G.709, Nutzungsbeispiele RZ-Kopplung und moderne VPN-Strukturen.

Das Bundle dieser fünf Videos kostet nur € 169,--* netto. Sie sparen über 30%.
*Statt regulärer Preis € 255,-- netto. Diese Angebote gelten nur im September 2012.

Video-Bundle + Report nur € 507,--* netto.
*Statt regulärer Preis € 653,-- netto.

Weitere Details und die Bestellung finden Sie auf unserer Homepage unter www.comconsult-study.tv

Das Wissensportal

Das Wissensportal

"Das Wissensportal“ ist das neu gestaltete Web-Portal von ComConsult Research. Hier finden Sie eine bunte Mischung aus aktuellen Informationen, persönlichen Meinungen und ausführlichen Grundlagen-Artikeln über die gesamte Themenpalette der IT- und Netzwerkwelt. Die Artikel des ComConsult Wissensportals geben Ihnen die Möglichkeit der Stellungnahme, des Kommentars oder der Diskussion mit anderen Lesern. Nutzen Sie diese Gelegenheit, die Sichtweise anderer Spezialisten zu erfahren. Unser Newsletter informiert Sie hierbei regelmäßig über Neuerscheinungen.

Neue Technologien für Converged Network Adapter

30. Juli 2012 von Dr. Franz-Joachim Kauffels

In verschiedenen Publikationen wurden Entwicklung und Bedeutung speicherbasierender Switch-ASICs vorgestellt. Sie werden zu völlig neuen Produktgenerationen führen, die neben erheblich erhöhter Leistung und gesenkter Latenz auch noch wesentlich weniger Strom verbrauchen als ihre Vorgänger. Zu diesen neuen Switches gehören aber auch neue Netzwerk-Adapter, damit ihre Fähigkeiten vollständig ausgenutzt werden können. Der aktuelle Stand sind 10 GbE Dual-Port CNAs. Das ändert sich aber bald, denn die Quad-Port CNAs stehen bereits vor der Tür und bieten neben mehr Funktionen vor allem eine viel glattere Migration zu 40 GbE, falls diese nötig werden sollte...

Kompletten Artikel lesen unter www.comconsult-research.de

Infiniband: die Welle rollt!

23. Juli 2012 von Dr. Franz-Joachim Kauffels

Mellanox, der weltweit nach Umsatz führende Infiniband-Hersteller, hat seinen Gewinn im letzten Quartal erheblich gesteigert. Der Gewinn stieg um das 15-fache (!) gegenüber dem 2Q2011. Primärer Umsatzträger sind die SwitchX-ASICs und die dazu passenden ConnectX Adapter. Die Markteinführung des FDR-IB (FDR = Fourteen Data Rate 56 Gbit/s.) kann nur als grandios bezeichnet werden. Die Aussichten für die nächsten Quartale sind sogar noch besser. Spannend ist aber auch, dass der Besitzer konvergenter Ethernets von den IB-Qualitäten profitieren kann.

Mellanox hat ganz klar dadurch Boden gut gemacht, dass zwar viel über 40 und 100 GbE geredet wird, die Lösungen dann aber oft für die Betreiber, die das wirklich benötigen, zu spät kommen. IB ist schon seit vielen Jahren fest im HPC-Umfeld verankert, aber die Anwendungsbereiche sind dabei, sich deutlich auszudehnen.

Besitzer von DB-Clustern, Clustered Storage und Cloud Provider wissen...

Kompletten Artikel lesen unter www.comconsult-research.de

Der Komplexitäts-CODE

10. Juli 2012 von Lars Sudmann

Komplexität im Geschäftsalltag klar und einfach präsentieren
Kennen Sie die folgende Situation: eine nicht enden wollende Präsentation, voller komplexer Grafiken, Zahlen und natürlich viel Text. Sie wollen am liebsten rausgehen. Haben Sie schon einmal an so einer Präsentation teilgenommen? Haben Sie vielleicht schon selbst einmal so eine Präsentation gehalten?

Komplexität - ein Phänomen unseres Alltags
Das Leben ist komplex geworden. Und wir wissen oft nicht genau, wie wir diese Komplexität darstellen sollen. Zum einen wissen wir natürlich viel über unser Projekt, unsere Analyse etc. Und die Dinge sind auch nicht immer einfach. Wir wollen alles richtig und vollständig darstellen, ohne wichtige Punkte zu vergessen. Leider führt das dann häufig dazu, dass wir alles und jedes in die Präsentation einbringen möchten. Die Brüder Chip und Dan Heath sprechen in ihrem exzellenten Buch ‚Made to Stick’ in dem Zusammenhang vom „Fluch des Wissens“. Dieser kann dann dazu führen, dass eine Grafik in der Präsentation so wir hier aussieht.

Kompletten Artikel lesen unter www.comconsult-research.de

Jetzt kommt LTE!

04. Juli 2012 von Dr. Franz-Joachim Kauffels

Die Deutsche Telekom macht beim Ausbau ihres Mobilfunknetzes Dampf. Ab sofort ist LTE als nächste Evolutionsstufe in 50 Städten verfügbar, zu denen Berlin, Bremen, Bochum und Stuttgart gehören, wie der Konzern am 3.7.2012 mitteilte. Bis zum Ende des Jahres sollen 50 weitere Städte hinzukommen. Das setzt Diskussionen über die Nutzung der neuen Mobilfunkgeneration in den Unternehmen frei.

In vielen Publikationen wurde LTE noch mit Datenraten zwischen 20 und 50 Mbit/s. für den Benutzer diskutiert. Die Telekom verwendet aber die neueste definierte Variante, LTE 10, mit bis zu 100 Mbit/s. Möglich wird dies vor allem durch den konsequenten Ausbau des Backbones. Dieser ist nach Angaben des Unternehmens grundsätzlich darauf ausgelegt, ca. 10 Millionen Benutzer in Deutschland mit jeweils mindestens 50 Mbit/s zu versorgen. Das ist die Datenrate, die ein Privathaushalt heute schon mit VDSL bekommen und z.B. für mehrere parallele HDTV-Datenströme im Rahmen von Entertain nutzen kann. Durch die Einführung von LTE ist es im Grunde genommen jetzt gleichgültig, ob der Kunde einen festen oder mobilen Anschluss benutzt. Gleichermaßen kann in Gegenden, in denen...

Kompletten Artikel lesen unter www.comconsult-research.de

Schwerpunkthema

Virtuelle Netze - Zurück zum Soft-Switch?

Fortsetzung von Seite 1

Dipl.-Inform. Damian Lukowski ist seit 2010 Mitarbeiter bei der ComConsult Beratung und Planung GmbH. Zu seinen Schwerpunkten zählen dort die Planung von Virtualisierungsumgebungen und Speicherlandschaften sowie die Bewertung relevanter Technologien im Bereich Data Center.

Werden alle virtuellen Maschinen an die gleiche Ethernet Bridge angeschlossen, sind sie Teil einer gemeinsamen Layer-2 Domäne, und das ist natürlich nicht immer gewünscht. In der Regel werden daher mehrere Ethernet Bridges verwaltet, die eine Teilmenge gehosteter VMs anbinden. Um die Netzsegmentierung auch in das physische LAN zu exportieren, werden entweder unterschiedliche Uplinks genutzt oder die Netze mittels VLAN-Tagging unterschieden.

Nach einiger Zeit hatte man Optimierungspotenzial erkannt, was die Konfiguration der vSwitches und ihrer (VLAN-) Segmentierung betraf. Dies war in erster Linie der Live-Migration und der High-Availability-Funktionalität für virtuelle Maschinen geschuldet. Diese Funktionen setzen voraus, dass eine VM auf einem beliebigen Host eines Clusters lauffähig ist. Für den Betreiber des Clusters bedeutet dies, dass die Netzanbindung aller Hosts einheitlich zu konfigurieren ist – die gleichen Konfigurationsschritte sind für jeden Host und jeden Access-Port (Freischalten der VLANs) durchzuführen.

Unter VMware vSphere stellte der „vNetwork Distributed Switch“ die erste Möglichkeit dar, alle Hosts eines Virtualisierungsclusters homogen zu konfigurieren, ohne die Konfigurationsaufgaben für jeden Host wiederholen zu müssen. Basierend auf der API für den vDS hat Cisco zudem den Nexus 1000v vermarktet, der einen Teil der netzwerkspezifischen Konfigurationsaufgaben wieder in die Verantwortung der Netzwerkadministratoren geben sollte. Über die NX-OS Konsole werden virtuelle Ports (vEth) oder Port-Profile erstellt und bezüglich VLANs, ACLs, QoS, etc. konfiguriert. Der vSphere-Administrator ist lediglich dafür zuständig, eine virtuelle Maschine dem passenden Port-Profil zuzuordnen.

Die bis hierhin beschriebenen vSwitch-Varianten sind reine Software-Konstrukte und mittlerweile nichts Neues. Mit zunehmender Konsolidierung immer mehr virtueller Maschinen auf einzelnen Hosts und der steigenden Verbreitung von 10Gigabit (zukünftig 40G) Ethernet-Adaptern steigt die Wahrscheinlichkeit, dass die theoretisch verfügbare Netzwerkperformance auch real abgerufen werden soll. Das bedeutet insbesondere, dass softwarebasierte Switches eine höhere CPU-Belastung des physischen Hosts nach sich ziehen. (siehe Abbildung 1)

In diesem Zusammenhang existieren einige neue Technologien, die zumindest teilweise damit motiviert sind, den Hypervisor von der Switching-Last zu befreien. Um zu verstehen, welche Verbesserungen diese Neuentwicklungen mit sich bringen, wollen wir uns kurz die Architektur gängiger Soft-Switch-Implementierungen anschauen.

Hypervisor- und Soft-Switch-Architektur

Abbildung 1 stellt eine abstrakte Sicht eines Virtualisierungshosts dar. Virtuelle Maschinen nutzen virtuelle NICs über einen „Front-End“ Treiber. Bei der vNIC kann es sich um die emulierte Version eines echten Ethernet-Adapters handeln (z.B. Intel 82545EM), der über den vom Hersteller angebotenen Treiber genutzt wird oder es handelt sich um einen paravirtualisierten Treiber, der speziell zur Nutzung in virtuellen Umgebungen angeboten wird.

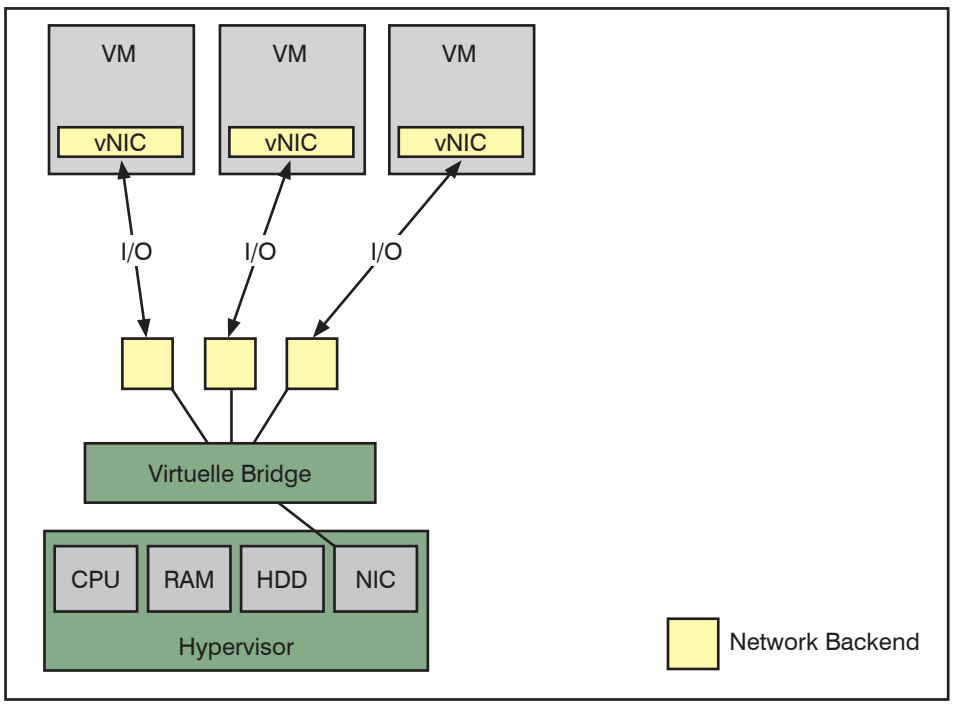


Abbildung 1: Abstraktes I/O Modell bei der Servervirtualisierung

Zu jeder vNIC gehört ein Gegenspieler im „Back-End“, bildlich die andere Seite des virtuellen Kabels zwischen VM und der virtuellen Bridge. Die heutigen Virtualisierungslösungen unterscheiden sich in ihrer Implementierungsform, insbesondere in der Hinsicht, an welcher Stelle die Elemente innerhalb des punktierten Bereichs (Back-End-Ports und virtuelle Bridge) betrieben werden. Unter Xen und Hyper-V sind die Back-End-Ports, die Bridge und die Treiber der physischen NIC Teil einer privilegierten VM („Domain-0“ bzw. „Parent-Partition“). ESX(i) nutzt eine direktere Architektur und verwaltet Treiber, Back-End und Bridging innerhalb des Hypervisors. KVM folgt einer dritten Variante und verleiht dem Linux-Kernel selbst Hypervisor-Funktionalität, sorgt durch diese Architektur aber immer wieder für hitzige Debatten, ob es sich dabei eigentlich noch um einen Bare-Metal-Hypervisor handelt.

Wie auch immer die konkrete Architektur aussieht, wird die Host-CPU durch das Bridging belastet. Im Falle eines extern einkommenden Datenpakets ist der Host auf einer Low-Level-Ebene mit folgendem Ablauf konfrontiert:

1. Der physische Ethernet-Adapter des Hosts empfängt ein Paket vom angeschlossenen physischen Switch, das für den virtuellen Adapter einer VM bestimmt ist.

2. Der Adapter schreibt das empfangene Ethernet-Paket mittels DMA (Direct Memory Access) in einen vom Hypervisor vorgesehenen Speicherbereich.

3. Der Adapter erzeugt einen Hardware-Interrupt.

4. Ein Host-CPU-Kern unterbricht seine aktuelle Aufgabe und wechselt in den Hypervisor-Kontext („VMX root“ Modus auf VT-x fähigen Hosts), genauer in den entsprechenden Interrupt-Handler. Dieser Handler ist Teil des Hardware-Treibers für den Ethernet-Adapter, bzw. bereitet den Hypervisor darauf vor, die Treiber-Logik zeitnah auszuführen.

5. Das Paket durchläuft den Netzwerk-Stack, die Bridging-Logik und letztendlich den korrekten Back-End-Port. Es findet mindestens einmal ein Kopiervorgang des Pakets in eine Speicherregion statt, auf die die virtuelle Maschine Zugriff hat.

6. Der Hypervisor generiert einen virtuellen Interrupt, um den NIC-Treiber innerhalb der virtuellen Maschine zu aktivieren.

7. Der Host-CPU-Kern kann den Hypervisor-Kontext verlassen, und steht für die Gast-VMs wieder zur Verfügung.

Schritte 1 bis 3 sind Aufgaben, die vom Adapter ohne Zuhilfenahme der CPU übernommen werden können. Der Hardware-Treiber des Ethernet-Adapters programmiert im Vorhinein zukünftige DMA-Transfers mit der „Host Physical Address“, welche dem Paketpuffer des Treibers im Host-Speicher entspricht.

In den Schritten 4 bis 6, insbesondere in Schritt 5, ist ein CPU-Kern mit relativ komplexen Aufgaben betreut, wenn man bedenkt, dass heutige 10G Ethernet-Adapter 250.000+ IOPS, und dementsprechend viele Interrupts pro Sekunde erzeugen können. Diese Komplexität gilt es aufzulösen.

Device Passthrough / Direct-IO

Über sogenanntes Device Passthrough bzw. Direct-I/O ist es möglich, PCI/PCIe Funktionen an eine virtuelle Maschine durchzureichen, so dass die Funktion exklusiv durch die besagte Maschine genutzt werden wird. Was eine Funktion ist, werden wir später noch genauer spezifizieren.

Abbildung 2 illustriert den Datenpfad zwischen Host-Hardware und virtueller Maschine bei der Nutzung von Direct-I/O, falls es sich bei dem durchgereichten Device um einen Ethernet-Adapter handelt. Es ist anzumerken, dass Device Passthrough nicht auf Netzwerk-Adapter beschränkt ist. Eine essenzielle Voraussetzung für Passthrough ist die Nutzung einer IOMMU (Input/Output Memory Management Unit, z.B. bei Intel VT-d), welche virtuelle Adressen in Host-Adressen umrechnen kann. Wird nämlich der Ethernet-Adapter vom Front-End Treiber innerhalb der VM betrieben, werden DMA-Adressen initialisiert, die das virtuelle Betriebssystem für die tatsächliche physische Adresse hält. Man spricht hier von der „Guest Physical Address“, im Gegensatz zur Host Physical Address, die vom physischen Ethernet-Adapter eigentlich angesteuert werden müsste. Die Zustellung eines Ethernet-Pakets mittels Direct-I/O und VT-d sieht dann wie folgt aus:

1. Der physische Ethernet-Adapter des Hosts empfängt ein Paket vom physischen Switch.

2. Der Adapter initiiert einen DMA-Transfer unter Nutzung der Guest Physical Address, die vom Treiber der Gast-VM programmiert wurde.

3. Die IOMMU übersetzt die Guest Physical Address in eine Host Physical Address; das Ethernet-Paket wird vom Adapter an die Stelle im Host-Speicher geschrieben, die dem Paket-Puffer des virtuellen Treibers innerhalb der virtuellen Maschine entspricht.

4. Der Host-Ethernet-Adapter erzeugt einen Hardware-Interrupt.

5. Ein Host-CPU-Kern unterbricht seine aktuelle Aufgabe und wechselt in den Hypervisor-Kontext.

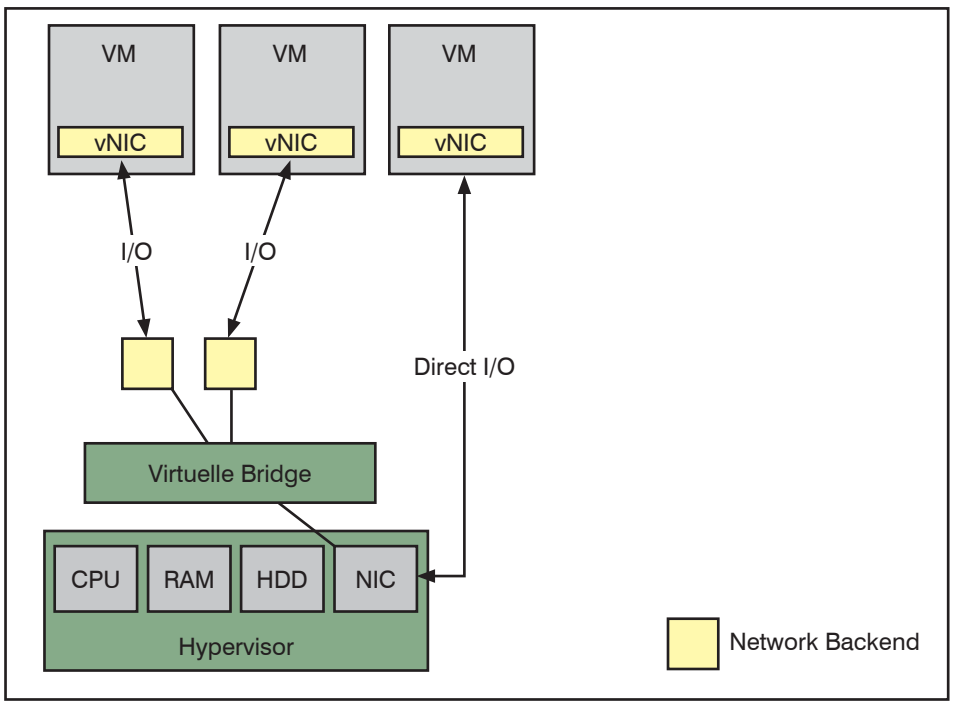


Abbildung 2: vSwitch-I/O im Vergleich zu Direct I/O

6. Der Hypervisor prüft, welcher VM der Host-Adapter zugeordnet ist, und generiert einen virtuellen Interrupt, um den NIC-Treiber innerhalb der VM zu aktivieren.

7. Der Host-CPU-Kern kann den Hypervisor-Kontext verlassen, und steht für die Gast-VMs wieder zur Verfügung.

Im Vergleich zum vSwitch-Szenario ist die Aufgabe, die der Hypervisor im Passthrough-Fall erledigen muss, trivial. Andererseits ist es in den wenigsten Fällen sinnvoll, ein Gerät, in diesem Fall den Ethernet-Adapter, exklusiv einer virtuellen Maschine zuzuordnen. Es gibt jedoch Möglichkeiten die Situation zu entschärfen.

Wir hatten vorhin kurz erwähnt, dass PCI bzw. PCI-e Funktionen exklusiv an virtuelle Maschinen durchgereicht werden können, hatten eine Funktion dann aber mit dem physischen Gerät gleichgesetzt. Die Situation sieht jedoch so aus, dass PCI-Express Geräte bis zu 8 sogenannter Physical Functions (PFs) anbieten können, die sich dem Betriebssystem als eigenständige Geräte präsentieren. Über Physical Functions werden z.B. Multi-Port Karten realisiert, bei dem ein ASIC eine Physical Function pro Ethernet-Port anbietet.

Es spricht in diesem Umfeld aber nichts dagegen, mehr PFs zu nutzen als Adapter-Ports vorhanden sind. Converged Ethernet Adapter (CNAs) bieten eine Ethernet-PF und eine Fibre-Channel-PF auf dem gleichen Ethernet-Port an. Produkte wie HP VirtualConnect oder IBM Virtual Fabric bieten 4 virtuelle NICs pro Port auf einem 10G Dual-Port Adapter an, die ein Virtualisierungshost mittels Passthrough einzelnen virtuellen Maschinen zuordnen könnte. Der Begriff der virtuellen NIC ist in diesem Zusammenhang nicht mit vNICs bei VMware zu verwechseln – bei so vielen Abstraktionsschichten gehen einem nun mal leicht die Begriffe aus. (siehe Abbildung 3)

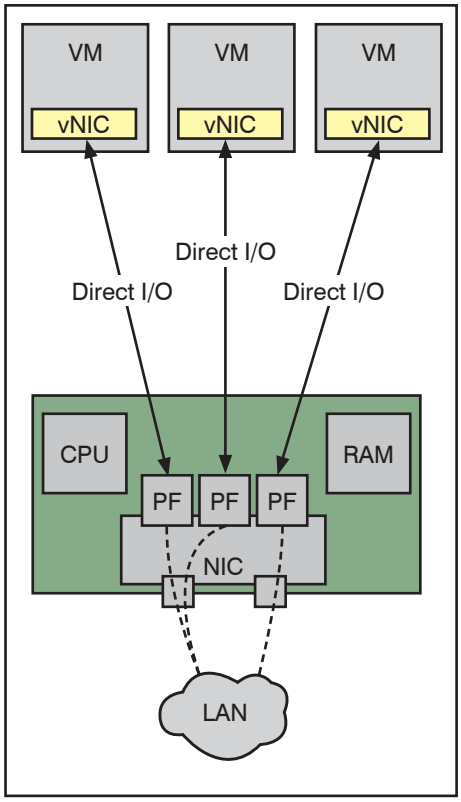


Abbildung 3: NIC-Virtualisierung über Physical Functions

SR-IOV

Die Lösungsansätze von IBM und HP sind auf 8 virtuelle NICs pro PCI-e Adapter beschränkt, zudem sind sie proprietär und mit Zusatzfunktionen ausgestattet, die der Kunde vielleicht nicht unbedingt haben und bezahlen will. Die PCI-SIG hat in dem Zusammenhang einen neuen offenen Standard verabschiedet, welcher die angesprochene Limitierung aufhebt. Der als **Single-Root-I/O-Virtualization** bezeichnete Standard definiert neue, sogenannte **Virtual Functions (VFs),** die eine leichtgewichtige Variante der Physical Functions darstellen. Ihre einzige Aufgabe ist im Grunde der I/O-Transport, weitergehende Konfigurationsfunktionen und Signalisierung werden weiterhin über Physical Functions realisiert, was impliziert, dass eine Gruppe von VFs immer einer PF untergeordnet ist. Der Standard erlaubt mehrere Hundert VFs pro PCI-e Gerät, die jeweils über Device Passthrough an individuelle virtuelle Maschinen angebunden werden können. Ein Hypervisor muss jedoch explizite SR-IOV-Unterstützung mitbringen, um VFs zu erzeugen und konfigurieren zu können. XenServer 6, Hyper-V (im neuen Windows Server 8) und KVM sind mittlerweile SR-IOV-fähig. VMware vSphere folgt nicht dem offiziellen SR-IOV Standard, ermöglicht in Kooperation mit Cisco aber ähnliche Resultate.

Intra-Host Kommunikation

Die direkte Anbindung von PCI-e Funktionen an virtuelle Maschinen hat Auswirkungen auf die VM-zu-VM Kommunikation innerhalb eines Hosts. Die EVB-Standards (Edge Virtual Bridging) beschäftigen sich mit möglichen Realisierungsformen einer solchen VM-VM-Kommunikation.

- Die Bridging-Funktionalität kann innerhalb des Adapters realisiert sein; man spricht hier von einer hardware-basierten Virtual Ethernet Bridge **(VEB)**.

- Der **VEPA-**Standard (Virtual Ethernet Port Aggregator), ebenfalls Teil von **IEEE 802.1Qbg**, verlagert das Bridging gänzlich in die Access-Switches der physischen Netzinfrastruktur, Ethernet-Pakete werden also generell immer Richtung Außenwelt kommuniziert. Es ist die Aufgabe VEPA-fähiger Switches, einen sogenannten Hairpin-Turn durchzuführen, falls das Ziel eine VM des Quell-Hosts ist. (siehe Abbildung 4)

Ein weiterer (Prä-)Standard, die **Bridge Port Extension** nach **IEEE 802.1BR**, definiert ein Verfahren, wie man die virtuellen Ports einzelner VMs im physischen

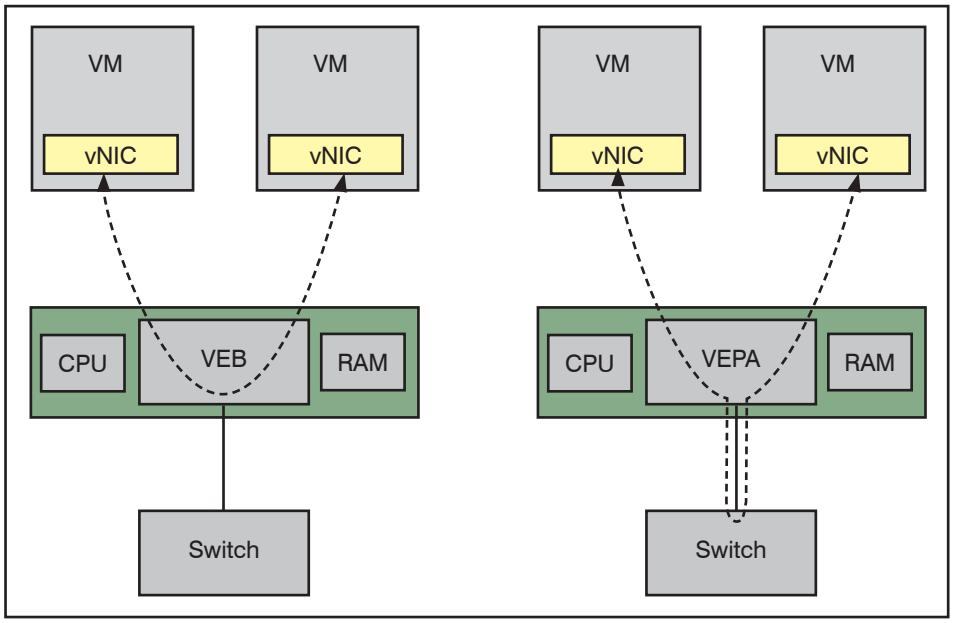


Abbildung 4: VEB und VEPA

Netzwerk zwecks individueller Konfiguration und Monitoring greifbar machen kann. Es läuft also darauf hinaus, dass man die externe Konfigurationsmöglichkeit einzelner Ports, wie sie z.B. beim Nexus 1000v gegeben sind, mit Direct I/O kombinieren können möchte.

Als Beispiel sei die Cisco **Unified Computing Platform** genannt, ein System bestehend aus Serverhardware und Netzkomponenten, welches beide Aspekte bereits heute erfolgreich kombiniert. Virtuelle Maschinen auf KVM oder vSphere-Basis können hardwarebasierte vNICs über Direct-I/O einbinden, die ihrerseits individuell aus dem physischen Netzwerk heraus einsehbar sind. Es sei angemerkt, dass die hardwarebasierten vNICs nicht mittels SR-IOV, sondern über ein proprietäres Verfahren bereitgestellt werden. Ebenso folgt Cisco mit seiner **VM-FEX** genannten Bridge-Port-Extension Implementierung nicht dem 802.1BR Draft, sondern dem Vorläufer-Draft IEEE 802.1Qbh. Cisco verfolgt aber das Ziel, zukünftig beide Frame-Formate zu unterstützen.

Und nun zurück zum Soft-Switch?

Die beschriebenen Bemühungen der IEEE und diverser Hersteller deuten also auf eine Ablösung der Soft-Switches hin. Doch es gibt derzeit auch gegenläufige Entwicklungen. VMware, Red Hat, Citrix, Cisco, Broadcom und Arista arbeiten derzeit an einem Layer-2 Overlay-Protokoll namens **VXLAN**. Das Hauptziel des Overlay-Netzes ist die Nutzung Host-übergreifender, voneinander isolierter Netze, wie sie heute über gewöhnliche VLANs realisiert werden. Als Motivation werden zwei Aspekte angeführt. Dies sind zum Einen das protokollbedingte Limit von 4094 VLANs, zum Anderen die Schwierigkeit, standortübergreifende VLAN-Domänen, z.B. zwecks Live Migration virtueller Maschinen, einzurichten.

Der VXLAN-Draft schlägt vor, Ethernet-Pakete virtueller Maschinen in UDP zu verpacken und mittels IP zum Host der Ziel-VM zu routen, eine Aufgabe, die von einem **VXLAN Tunnel End Point** (VTEP) innerhalb des Hosts übernommen wird.

Ein VXLAN-Header markiert mittels eines 24-bittigen VXLAN Network Identifiers (VNI) das zugehörige logische Netz, die Zuordnung virtueller Maschinen bzw. ihrer vNICs wird vom Administrator der Virtualisierungsplattform durchgeführt. Um Broadcast-Frames virtueller Maschinen effizient übertragen zu können, wird für jedes VXLAN eine eigene Multicast-Gruppe eingerichtet, der die VTEPs der Virtualisierungshosts beitreten, falls mindestens eine VM dem entsprechenden VXLAN zugeordnet ist. Analog zu gewöhnlichen Layer-2 Switches unterhalten VTEPs eine Zuordnungstabelle von VM-MAC-Adressen und zugehöriger VTEP-Adresse entfernter Hosts. (siehe Abbildungen 5 und 6)

Man kann sich nun fragen, was das Ganze soll. Es wird nicht nur die Switching-Logik wieder in den Host verlagert, sondern auch um eine Einkapselungsschicht erweitert. Zudem wird die Multicast-Fähigkeit des Transportnetzes vorausgesetzt. Für wen ist VXLAN also gedacht? Die Antwort ergibt sich aus der bereits

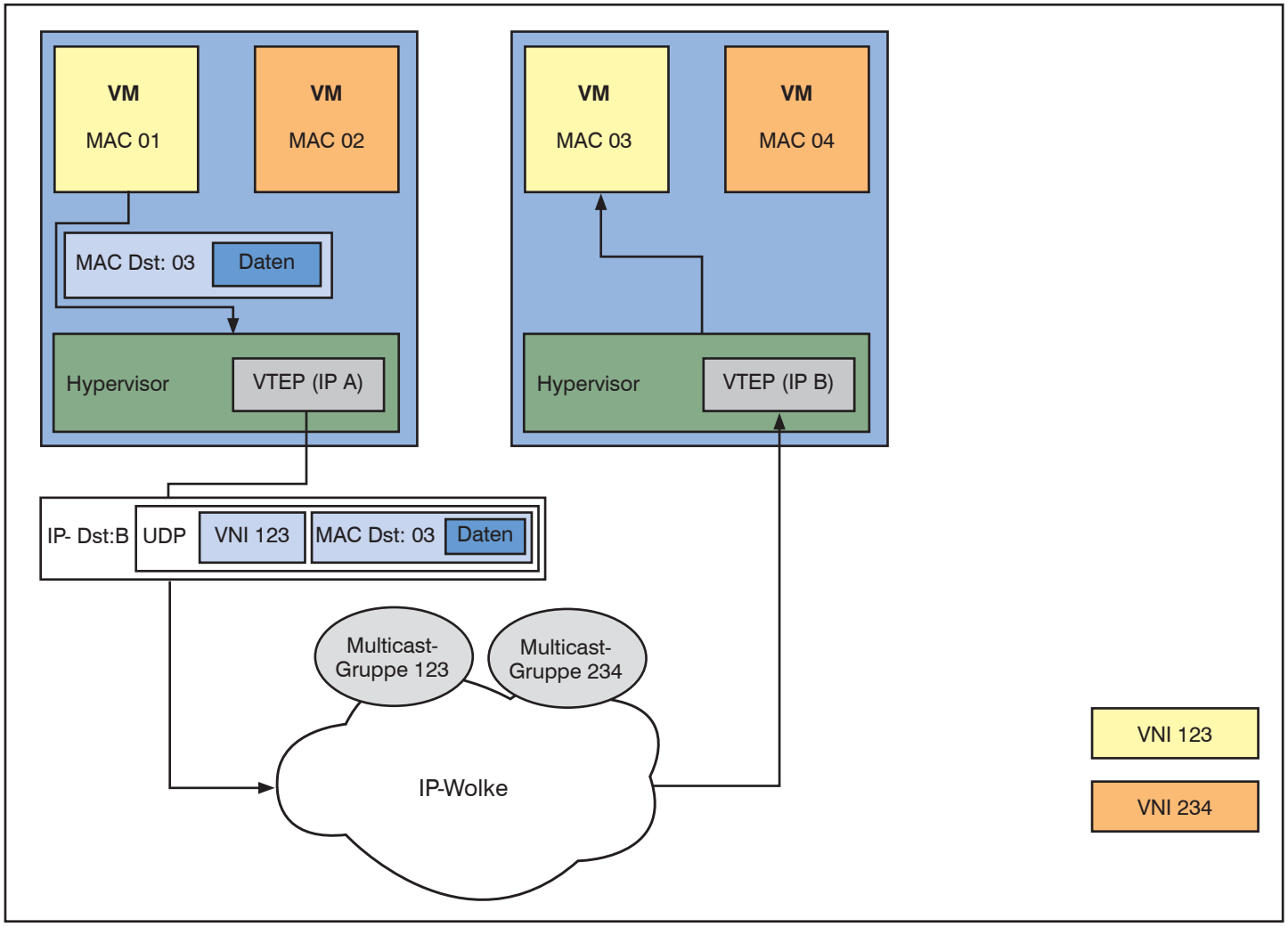


Abbildung 5: Einkapselung und Unicast-Transport von VM-Unicast-Daten

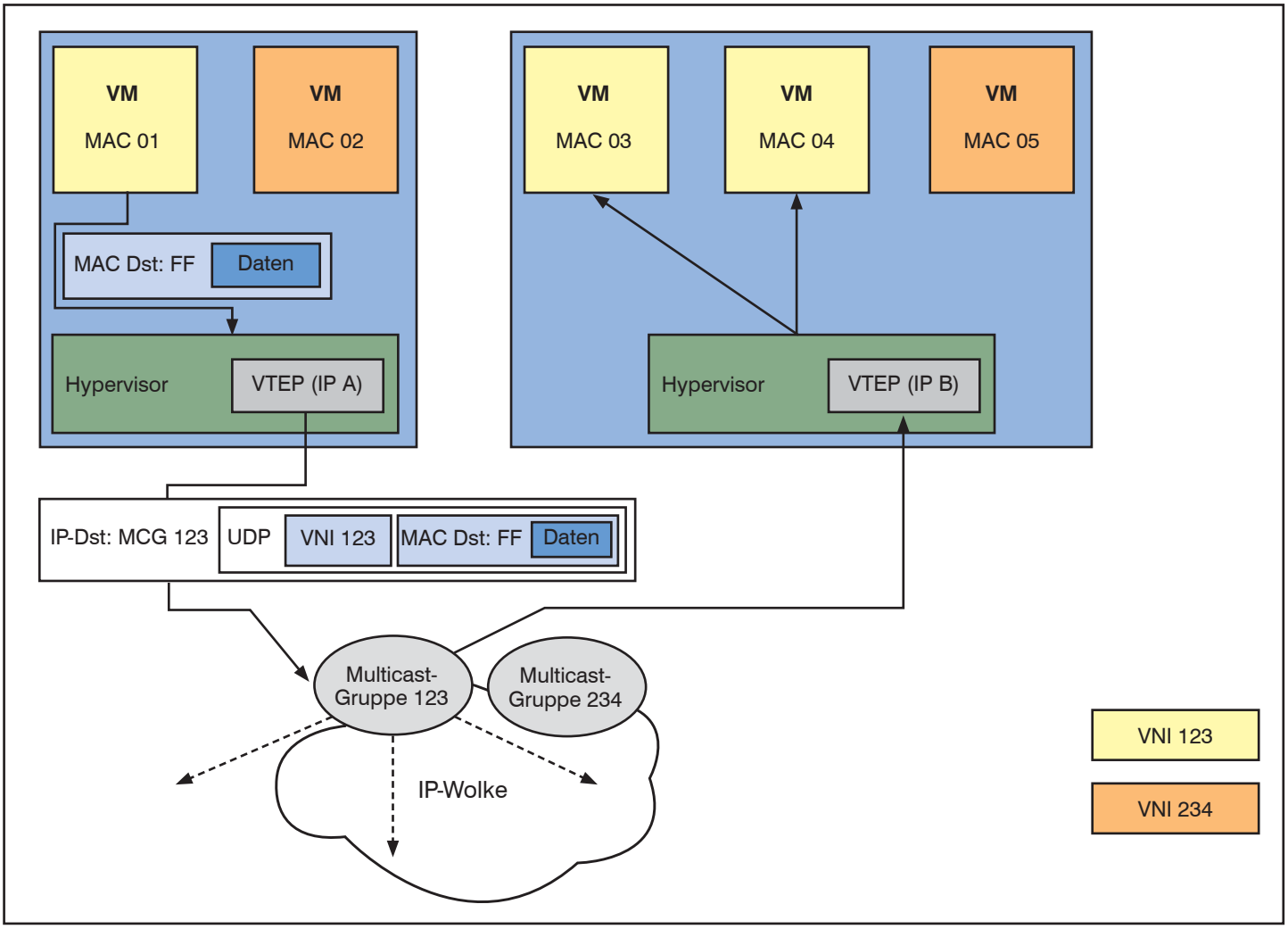


Abbildung 6: Einkapselung und Multicast-Transport von VM-Broadcast-Daten

beschriebenen Motivation und dem Produkt, welches bereits heute VXLAN einsetzt: der VMware vCloud Director. Der vCloud Director ist eine IaaS-Lösung, mit deren Hilfe mandantenfähige virtuelle Netzstrukturen erzeugt werden können. Mandanten können in einem gewissen Rahmen selbst virtuelle Netze definieren und mittels virtueller Router miteinander verschalten. Auf globaler Ebene, also im physischen Netz des Cloud-Providers, müssen all diese logischen Netze real und isoliert transportiert werden können.

Abbildung 7 illustriert typische logische Netze eines vCloud Director Mandanten. Man muss bedenken, dass selbst Daten der internen und isolierten Netze über das physische Netz des Cloud-Providers transportiert werden müssen, falls sich die virtuellen Maschinen dieser logischen Netze auf unterschiedlichen Virtualisierungshosts befinden. Hieraus wird klarer, warum VLANs als Isolationsverfahren in großen Provider-Netzen an ihre Grenze stoßen können. Neben der Erhöhung

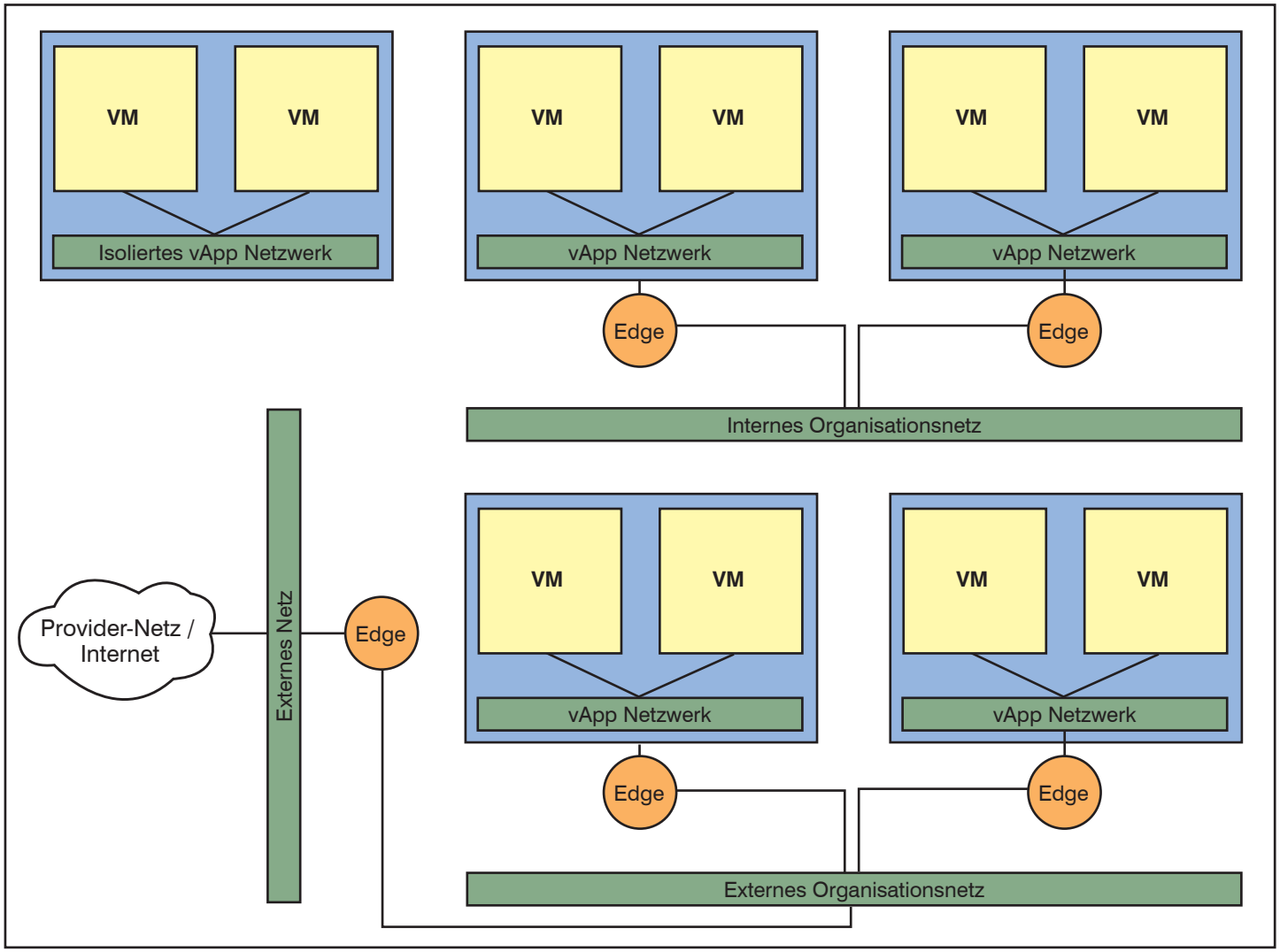


Abbildung 7: vCloud Director Netze eines Mandanten

verfügbarer Netze haben VXLAN-basierte logische Layer-2-Netze den Vorteil, dass sie prinzipiell global-geographisch aufgespannt werden können. In der Realität wird man sich allerdings um Latenzen und Durchsatz Gedanken machen müssen, zudem stellt sich die Frage, wie sich die obligatorische Multicast-Infrastruktur über das Internet realisieren lässt (z.B. über zusätzliche Multicast-Tunnel zwischen Standorten).

Der vCloud Director ist kein Einzelfall. Werden dort VXLANs als „Mittel zum Zweck“ genutzt, bietet der Software-Hersteller Nicira mit seiner Network Virtualization Platform ein generisches Netzvirtualisierungsprodukt an. Die NV-Plattform implementiert einerseits eine Overlay-Logik (Einkapselung, Control-Plane), andererseits bietet sie eine dokumentierte API zur Einrichtung logischer Netzkomponenten (Router, Firewalls, Load-Balancer) und ihres Monitorings. Wer will, implementiert darauf seine eigene Cloud-Lösung, Drittanbieter-Produkte werden sicher bald folgen.

Zur Einkapselung nutzt Nicira übrigens ein eigenes Tunnel-Protokoll, das **Stateless Transport Tunneling Protocol (STT)**, welches bei der IETF als Draft vorliegt. Es ist insofern erwähnenswert, als dass die Autoren erkannt haben, dass ein „Rückschritt“ in Richtung des Soft-Switches nicht optimal ist. Das STT-Einkapselungsformat ist speziell darauf abgestimmt, die TSO- bzw. LRO-Funktion **(TCP Segmentation Offload** bzw. Large Receive Offload) verbauter Ethernet-Adapter auszunutzen. Mit Hilfe der 64-bittigen **Context-ID** innerhalb des **STT Frame Headers** können logische Netze unterschieden werden. Die Context-ID ist jedoch nicht unbedingt als Zahl zu verstehen, sondern kann mehrere Informationen kodieren und eine Struktur besitzen – die Details bleiben der jeweiligen Implementierung überlassen.

Bei der Kommunikation über Ethernet werden Daten in Ethernet-Frames aufgespalten, deren Größe üblicherweise bei ca. 1500 Bytes liegt. Weiter innen liegende Protokoll-Header wie die von IP und TCP führen Informationen mit sich, die vom Netzwerk-Stack der Kommunikationsendpunkte interpretiert werden können. Bei TCP stellen insbesondere die Berechnung der Prüfsumme sowie die Buchführung über die Sequenz- und Acknowledgement-Nummern einen Aufwand für die Kommunikationspartner dar. Ein TSO-fähiger Netzwerk-Adapter entlastet den Netzwerk-Stack des Betriebssystems, indem er anbietet, bis zu 64kb TCP-Nutzdaten selbst zu segmentieren und zu übertragen.

Das Ziel des STT-Protokolls ist allerdings nicht der Aufbau eines TCP-Stroms, sondern die Übertragung von Ethernet-Frames. Um die TSO-Fähigkeit des Hardware-Adapters nutzen zu können, müssen Daten als TCP-Paket maskiert

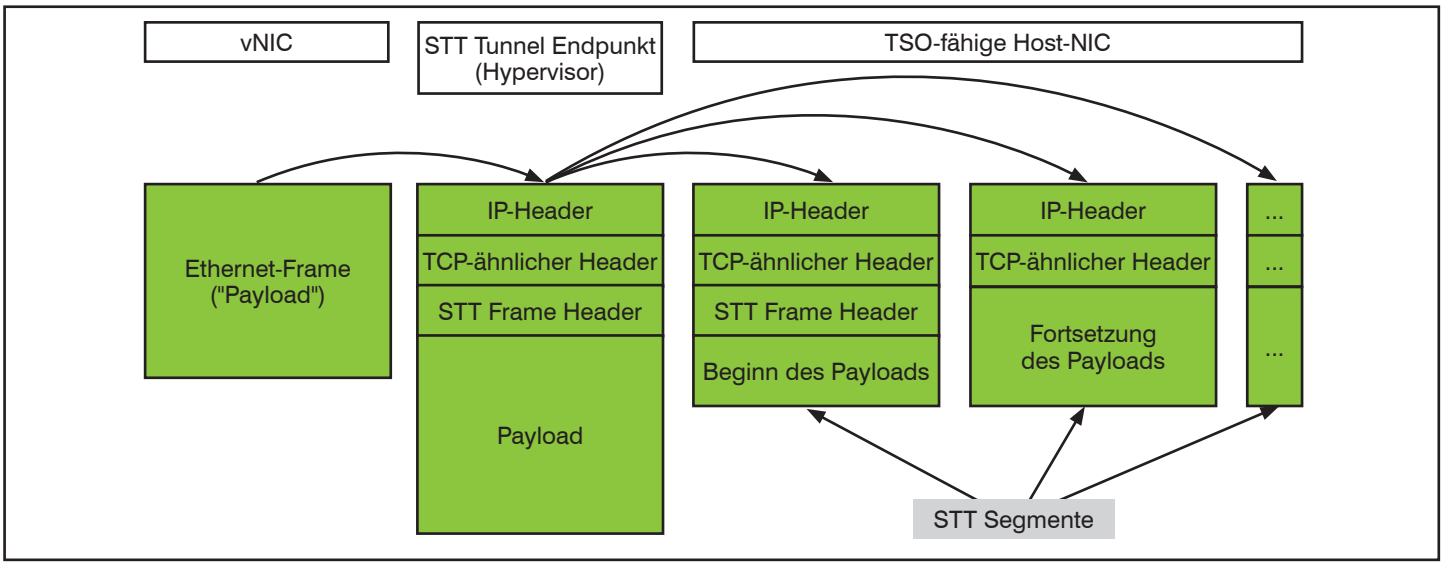


Abbildung 8: TCP Segmentation Offload beim Stateless Transport Tunneling Protocol

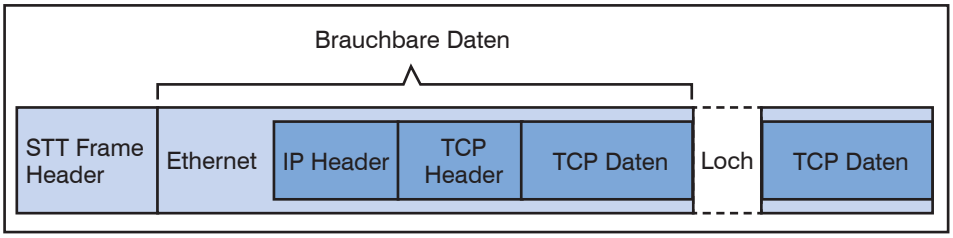


Abbildung 9: Prinzipiell nutzbare Payload-Daten im Falle von Paketverlust

werden, um den syntaktischen Anforderungen der TSO-Logik des Hardware-Adapters zu genügen. Abbildung 8 illustriert die Verfahrensweise.

Der Draft erwähnt nicht per se, dass die virtuelle NIC innerhalb der virtuellen Maschine die TSO-Funktionalität signalisieren soll. Es scheint jedoch die einzige Möglichkeit zu sein, das VM-Betriebssystem dazu zu bringen, übergroße Ethernet-Frames für TCP-Daten versenden zu wollen. Bei der Nutzung paravirtualisierter vNIC-Treiber ist zwar eine 64kb große MTU auf VM-Seite denkbar, jedoch gäbe es dann Probleme beim Versenden von Non-TCP-Datenpaketen.

Im Allgemeinen müssen einige Seiteneffekte beachtet werden, die einer Design-Entscheidung des STT-Protokolls geschuldet sind. Syntaktisch gesehen entsprechen STT-Segmente gewöhnlichen TCP-Paketen, der Datenstrom folgt in seiner Gesamtheit aber nicht der TCP-Semantik: Es gibt keinen TCP-Handshake, keine Flusskontrolle und keine Sendewiederholungen bei Paketverlust. Sollte zwischen zwei STT-Endpunkten eine Stateful Firewall in Betrieb sein, würden STT-Segmente als Anomalie erkannt, und wahrscheinlich verworfen werden. (siehe Abbildung 9)

Aufgrund der fehlenden Sendewiederholung ist STT sensibel gegenüber Paketverlusten. Sollte das erste STT-Segment, welches den STT Frame Header beinhaltet, im Transportnetz verloren gehen, können die restlichen STT-Segmente des jeweiligen STT-Frames keinem Kontext zugeordnet werden. Darüber hinaus gilt im Allgemeinen, dass der Verlust irgendeines STT-Segments das gesamte STT Frame und damit den Payload korrumpiert. Der Payload, der den inneren Ethernet-Frame darstellt, besitzt also ein „Loch“ und müsste verworfen werden. Eine Ausnahme ergibt sich, wenn der Payload selbst ein Protokoll kapselt, das eine Sendewiederholung implementiert (TCP, SCTP). In diesem Fall können alle STT-Segmente bis zum ersten Paketverlust

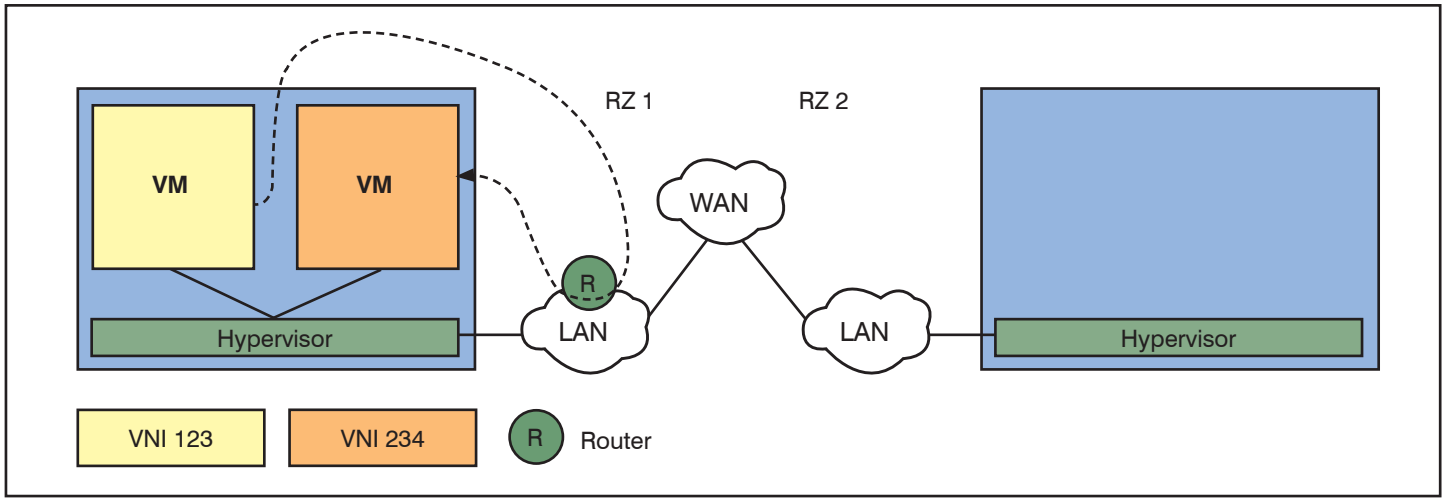


Abbildung 10: VM-Gateway-VM-Kommunikation in der Ausgangssituation

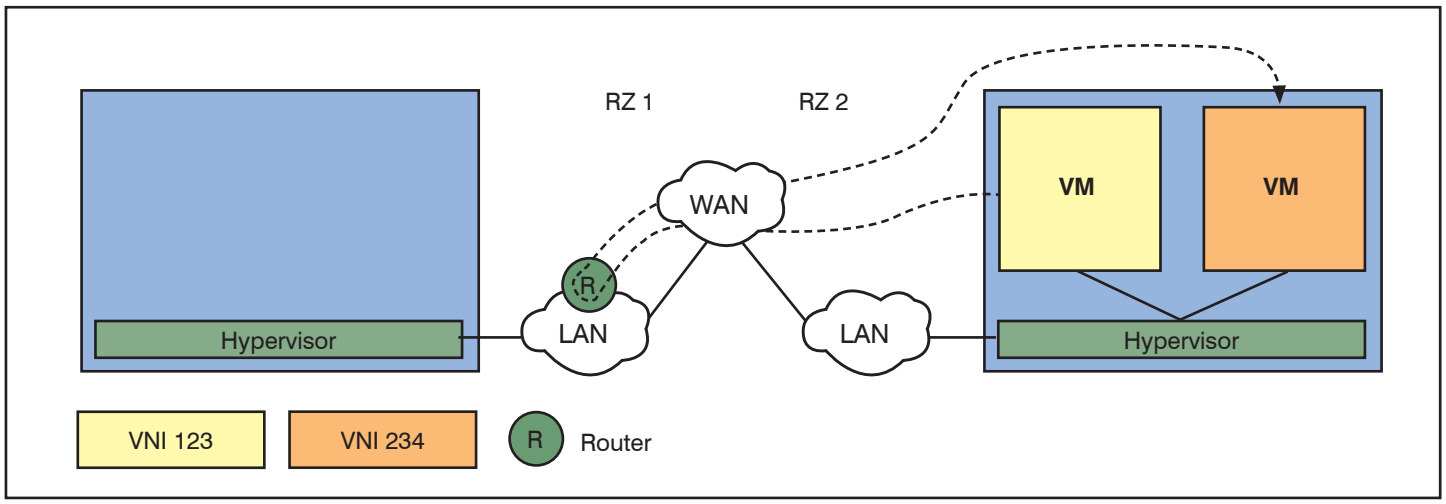


Abbildung 11: Ungünstige VM-Gateway-VM-Kommunikation nach einer VM-Migration

zusammengesetzt, und an die Ziel-MAC-Adresse weitergeleitet werden. Der STT-Endpunkt versendet also nicht das ursprünglich eingekapselte Ethernet-Frame, sondern ein Anfangsstück desselben. Zuvor müssen jedoch die innenliegenden Protokoll-Header angepasst werden – die Total Length und die Prüfsumme des IP-Headers, sowie die Prüfsumme des TCP/SCTP-Headers. Man darf angesichts dieser Komplexität gespannt sein, ob es Implementierungen außerhalb der NV-Plattform von Nicira geben wird.

Wie sind diese gegenläufigen Entwicklungen nun zu bewerten? Auf der einen Seite haben wir neue Standards wie etwa SR-IOV und VEB/VEPA, auf der anderen Seite nutzen heutige Implementierungsformen von VXLAN und STT eine Einkapselung auf Software-Basis. Doch das kann, und ist im Begriff, sich zu ändern.

Der Switch-Hersteller Arista, ein Co-Autor des VXLAN-Drafts, hat bereits Switches mit VXLAN-Support angekündigt. Genauer gesagt werden die neuen Modelle eine VXLAN-Gateway-Funktion mitbringen, und den Übergang zwischen der VXLAN-Welt und der VLAN-Welt in Hardware implementieren. Stand heute sind nur Software-basierte Gateways möglich, indem eine VM sowohl an ein VXLAN-basiertes als auch an ein VLAN-basiertes Netz angebunden wird. Die offiziellen Lösungen lauten hier bisher VMware *vShield Edge und Cisco ASA 1000v*.

Das darf jedoch nicht das Ende der Reise sein. Um den Host zu entlasten, muss die Einkapselungslogik aus dem Hypervisor wieder herausgenommen werden. Mit Broadcom als einem der Co-Autoren von VXLAN ist eine Implementierung dieser Logik innerhalb einer NIC-VEB denkbar.

Es bietet sich ebenfalls an, Bridge Port Extensions mit einer Switch-basierten Einkapselung zu kombinieren. Cisco, ebenfalls VXLAN-Co-Autor, könnte Datenpakete per VM-FEX angebundener Maschinen zukünftig innerhalb seiner UCS Fabric Interconnects in UDP kapseln und in Richtung des Ziel-VTEPs versenden. Analog könnten zukünftige, IEEE 802.1BR konforme Switches ihren virtuellen Bridge-Ports ein VXLAN zuordnen und bei Bedarf in UDP einkapseln, während virtuelle NICs/Functions auf Host-Seite mittels SR-IOV und Passthrough direkt an die VMs angekoppelt werden. Bei Arista steht IEEE 802.1BR derzeit nicht auf dem Plan, allerdings wird es voraussichtlich möglich sein, ein VLAN→VNI-Mapping zu nutzen und individuelle VMs, oder sogar physische (nicht-virtuelle) Server anhand des VLAN-Tags einem VXLAN zuzuordnen. Die UDP-Einkapselungslogik hätte man damit aus dem Hypervisor wieder herausgeholt, und durch VLAN-Tagging ersetzt – bei Nutzung von SR-IOV und Direct-I/O kann letzteres allerdings in Hardware geschehen.

Der Hersteller wird ein Managementwerkzeug liefern müssen, um ein VLAN→VNI-Mapping sinnvoll zu verwalten. Da es über 16 Millionen VNIs im Gegensatz zu 4000

VLANs geben kann, läuft ein fabric-weites Mapping dem Sinn von VXLANs zuwider. VLANs werden als Mittel zum Zweck lediglich Switch-lokale Gültigkeit, oder sogar nur Port-lokale Gültigkeit besitzen, um virtuelle Maschinen eines Hosts (und letztendlich eines gemeinsamen Switch-Ports) unterschiedlichen VNIs zuordnen zu können. Auf der anderen Seite bedeutet es, dass VLAN-IDs nichts darüber aussagen, ob zwei VMs auf unterschiedlichen Virtualisierungshosts miteinander kommunizieren können. Diese Information wird über ein zusätzliches Werkzeug aufbereitet werden müssen, das die Vielzahl lokaler Zuordnungen in einer globalen Übersicht vereint.

Wagen wir einen mutigen Blick in Zukunft und gehen von der Annahme aus, dass sich die hier vorgestellten Technologien und Overlay-Protokolle sinnvoll und effizient miteinander kombinieren lassen werden. Müssen wir uns dann weiterhin um das Layer-2-Design des Transportnetzes Gedanken machen? Der Blogger Brad Hedlund sagt „Nein“, und vergleicht dabei das physische Transportnetz mit einem einzelnen Switch. So wie wir uns heute keine Gedanken darüber machen, wie Ethernet-Frames von einem Switch-Port zum anderen geleitet werden, sollten wir uns in Zukunft keine Gedanken darüber machen, welche Wege ein Datenpaket in einem virtuellen Overlay-Netzwerk real zurücklegt.

Ich persönlich würde mir jedoch eine Lösung wünschen, die die reale Topologie zu einem gewissen Grad berücksichtigen kann. Im Zusammenhang mit Overlay-Netzen stellt sich häufig die Frage, wie ein Endpunkt mit seinem IP-Gateway kommuniziert. In Abbildung 10 sind zwei Rechenzentren dargestellt, die die RZ-überspannenden VXLANs 123 und 234 betreiben. Da keine direkte Kommunikation der beiden VMs im Rechenzentrum 1 möglich ist, wird eine Routing-Instanz, ebenfalls ansässig im RZ 1, als Gateway genutzt. Die spannende Frage ist, wie der reale Kommunikationspfad aussieht, wenn beide Maschinen in das gegenüberliegende Rechenzentrum migriert werden (Abbildung 11). Im Idealfall sollte die Routing-Instanz mitwandern, so dass folgender Datenverkehr auf das Rechenzentrum 2 beschränkt bleibt. Der VXLAN Draft sieht aber keine Mechanismen vor, die eine solche Lokalisierung etablieren lassen würden. Beim OTV-Protokoll (Overlay Transport Virtualization) von Cisco sieht das anders aus: ARP-Anfragen bezüglich der Gateway-MAC-Adresse werden vom RZ-lokalen Switch beantwortet, so dass die Routing-Instanz im übertragenden Sinne mit den virtuellen Maschinen mitwandert. Eine ähnliche Logik könnte Arista in seinen Switches als ergänzendes Feature für VXLAN implementieren, auch wenn diese Möglichkeit im Draft (noch) nicht erwähnt wird.

Fazit

Die beschriebenen Entwicklungen widersprechen sich nicht prinzipiell, sondern lediglich in ihrer heutigen Ausprägung. Da sie zudem unterschiedlich motiviert sind, ist die heutige Unvereinbarkeit nur dann relevant, wenn das Potenzial beider Lösungen ausgeschöpft werden soll.

Ansonsten ist die Entscheidung klar: Wer seinen Mandanten heute flexibel logische Netze bereitstellen will, wird die verfügbaren software-basierten Produkte nutzen und den Hypervisor-Overhead berücksichtigen müssen. Letzterer kann sich für den RZ-Betreiber durchaus als vernachlässigbar herausstellen, falls dessen Mandanten genügsam mit den Netzwerkressourcen umgehen.

VEB/VEPA und SR-IOV hingegen sind in Rechenzentren interessant, die nachweislich mit hohen Daten- und Paketraten am Server Edge konfrontiert sind. Betreiber, die ein relativ statisches Netzwerk unterhalten und ihre Dienste sowie Datenströme kennen, sehen in der Netzvirtualisierung möglicherweise keinen höheren Mehrwert, so dass die Entscheidung auch hier eindeutig ausfällt.

Betreiber aus der Schnittmenge müssen sich derweil mit einer nicht-optimalen Lösung zufrieden geben. Doch was ist überhaupt optimal? Letztendlich sind die Kosten doch einer der wichtigsten Faktoren. Wenn ein Betreiber vor der Wahl steht, leistungsfähigere (Standard-)Server einzusetzen oder in neue Netztechnologien zu investieren, die der Hersteller ebenfalls entlohnt haben möchte, werden die schnelleren Server solange die günstigere Wahl sein, bis sich die Alternative als Alltagstechnologie durchgesetzt hat. Erst danach wird die Verheiratung beider Welten – Hypervisor-externes Switching und hardwaregestützte Netzvirtualisierung – auf breiter Basis Anwendung finden.

Report Neuerscheinung

Moderne Wireless-Technologien

ComConsult Research hat im August den Report „Moderne Wireless-Technologien“ veröffentlicht.

Die Entwicklung der Endgeräte wie Smartphones und Tablets scheint in immer schnellerem Takt zu erfolgen. Dass diese Geräte am Nabel der Cloud hängen, zieht sofort höhere Anforderungen an die Leistung der Infrastruktur nach sich.

In den letzten 2-3 Jahren haben Provider eine einzigartige Aufrüstungswelle vorgenommen und die 3G-Mobilfunknetze auf 4G umgestellt, in Europa meist mit LTE. Die Kernfrage ist jetzt, ob und wie die Wireless-Infrastrukturen in Unternehmen und Organisationen sinnvoll aufgerüstet werden können. Dafür gibt es aktuell zwei Kandidaten:

- IEEE 802.11ac als unmittelbare Weiterentwicklung von 11n im 5 GHz-Band
- IEEE 802.11ad als neuer Standard für die Kommunikation im 50 GHz-Band

Beide versprechen in der Werbung bis zu 7 Mbit/s. pro Zelle, bei 11ac wird die Leistung in der Praxis erheblich geringer sein. 11ad ist konstruktiv deutlich besser und könnte tatsächlich eine Leistung in der Größenordnung einiger Gigabit/s. pro Zelle erreichen. Consumer-Markt-Komponenten nach IEEE 802.11ac werden ab Mitte 2012 ausgeliefert. Die Frage ist, ob es für ein Unternehmen überhaupt sinnvoll ist, WLANs nach 11n durch WLANs nach 11ac abzulösen. Der Unterschied zwischen der höchsten Leistungsstufe von 11n (nominal 540 Mbps/Zelle) und der Leistungsstufe der

ersten Produktgenerationen von 11ac (real 700 -1200 Mbps/Zelle) ist in realen Szenarien nämlich gar nicht so groß.

Denkt man etwas weiter, liegen die Kosten für eine Erweiterung nämlich bei den neuen Access Points, sondern vielmehr in der Infrastruktur. Spätere Generationen von 11ac und schon die erste Generation von 11ad haben eine Datenrate von deutlich mehr als 1 Gbps/Zelle. Daher muss die gesamte Infrastruktur, die die APs versorgt, auf 10 GbE umgestellt werden!!! Mit 11ad verschärft sich diese Situation noch weiter, denn die Eigenschaften der Wellenausbreitung im Millimeterwellenbereich führt zu Zellen, deren Größe selbst unter optimistischen Annahmen 50 bis 70 qm kaum überschreiten wird.

Um die Markteinführung von 11ac nicht zu behindern, ist trotz vorhandener Muster für alle Komponenten die Weiterentwicklung von 11ad für etwa zwei Jahre auf Eis gelegt worden. Diesen Zeitraum können Unternehmen und Organisationen dazu nutzen, zu entscheiden, welche Technik sie denn in Zukunft einsetzen möchten. In der Zwischenzeit wird sich aber noch eine weitere Diskussion entwickeln, nämlich die Frage, ob man überhaupt die eigene WLAN-Infrastruktur noch weiterentwickelt oder sie lieber durch LTE ergänzt oder ganz ersetzt. Denn LTE ist verfügbar und letztlich ist es nur ein Rechenexempel.

In einer solch verfahrenen Situation hilft nur umfassendes Grundlagenwissen. Genau dazu dient dieser Report. Abgesehen von einer grundsätzlichen Einführung in die Möglichkeiten der Implementierung von Multi-Gigabit-WLANs in den bekannten Frequenzbereichen und Bändern werden die Technologien von 11n, 11ac und 11ad vorgestellt und untereinander verglichen. Zusätzlich werden wesentliche Grundeigenschaften von LTE erläutert und die Möglichkeit der Schaffung hybrider Umgebungen erläutert.

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

Vergünstigter Technologie-Report
Wir bieten Ihnen diesen Report bei der Buchung des Seminars " Wireless LAN professionell" zu einem Sonderpreis an.
Statt regulär € 349,-- netto zahlen Sie nur € 310,-- netto

Fax-Antwort an ComConsult 02408/955-399

Bestellung

Moderne Wireless-Technologien

☐ Ich bestelle den Report
Moderne Wireless-Technologien
zum Preis von € 349,-- netto

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Bestellen Sie über auch über
www.comconsult-research.de

Standpunkt Troubleshooting

Neue WLAN auf dem Vormarsch!

Der Standpunkt Troubleshooting 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.

Bisher war es ja recht still um die neuen WLAN-Techniken. Es schien, als ob die Entwicklung ins Stocken geraten wäre. „11n“ mit 300 Mbit/s ist überall verfügbar und auch 450 Mbit/s (jeweils brutto) wird jetzt von den Herstellern im so genannten Enterprise-Bereich mehr und mehr angeboten. 600 Mbit/s, das gibt der Standard eigentlich her – Fehlanzeige! Und dabei ist der Standard IEEE 802.11n bereits seit 3 Jahren in Kraft.

Doch seit Anfang des Jahres tut sich wieder etwas. Allerdings nicht bei 600 Mbit/s – MIMO mit mehr als 3 Spatial Streams bewahren sich die Hersteller für spätere Zeit auf. Stattdessen kommt die Entwicklung des Gigabit-WLAN in Fahrt. Da ist zum einen die Erweiterung „11ac“, die die Techniken von 11n an einigen Stellen entscheidend „aufbohrt“ und damit 7 Gbit/s schaffen möchte. Und da ist zum anderen die Erweiterung „11ad“, die mit 5 Millimetern Wellenlänge, d.h. mit Frequenzen bei 60 GHz (demgegenüber funken die herkömmlichen WLAN sozusagen mit Gleichstrom) ebenfalls 7 Gbit/s erzielen möchte. Von den technischen Details der genannten Verfahren haben Sie wahrscheinlich noch einiges aus meinem Artikel im Netzwerk Insider vom Mai dieses Jahres behalten. Was hat sich seither getan?

Bei 11ac gibt es seit Juni eine neue Vorabversion („Draft“) mit der Nummer 3.0. Und grundsätzlich scheint die Spezifikation jetzt so stabil zu sein, dass sich die Hersteller mit Macht an die Entwicklung von Geräten geben. Inzwischen sind mir 4 Hersteller bekannt, die Produkte gezeigt haben und diese ab dem vierten Quartal 2012 auf den Markt bringen möchten. Alle Produkte sind für den Consumer-Markt bestimmt. In ersten unabhängigen Tests (nein, nicht durch ComConsult) wurden Nutzdaten mit mehr als 500 Mbit/s übertragen. Und dennoch, mit der Verabschiedung des Standards sollten Sie vor Ende 2013 nicht rechnen.

Bei 11ad hat es in der Zwischenzeit vier (!) neue Drafts gegeben. Man ist also bei der Version 9.0 angelangt. Und die wird wahrscheinlich bis Jahresende als Standard freigegeben werden. Der Chip-Hersteller Marvell hat im Juli eine Allianz mit dem Hersteller Wilocity bekanntgegeben. Dabei geht es um die Entwicklung von WLAN-Schaltkreisen, die auf allen 3 Bändern funken. Marvell hat allerlei Produkte für die herkömmlichen Bänder 2,4 und 5 GHz im Programm – unter anderem einen 11ac-Chipsatz. Wilocity ist stark in der Wireless Gigabit (WiGig) Alliance engagiert und entwickelt Chips für 60 GHz.

Und welche WLAN-Technik werden Sie in Zukunft einsetzen? O.k. – zunächst bleibt abzuwarten, wann auch die Enterprise-Hersteller Produkte für Gigabit-WLAN herausbringen und welche. Und dann sind noch weitere Punkte zu beachten. Zunächst einmal werden Sie das große Bitraten-Angebot der neuen Techniken natürlich nur dann ausnutzen können, wenn Sie Ihre Access Points mit entsprechender Bandbreite in das LAN einbinden. Gigabit Ethernet ist also Pflicht und wird langfristig nicht ausreichen. Die Zellplanung wird – anders als beim Schritt von 11a/b/g zu 11n – neu zu erstellen sein und dabei viel mehr und kleinere Zellen ergeben.

Nicht zuletzt benötigen Sie für Planung und Betrieb der Gigabit-WLAN Werkzeuge. So müssen Tools zur Zellplanung und für das Site Survey die Übertragungs-Eigenschaften der neuen Techniken und z.B. auch die Ausbreitungseigenschaften im 60-GHz-Band kennen, um aussagekräftige Ergebnisse liefern zu können. Diesbezüglich ist heute noch gar nichts in Sicht. Bei der Protokollanalyse besteht die letzte Neuerung in der Unterstützung von 11n mit 3 Spatial Streams. Messtechnik für Signal- Protokoll- und Spektralanalyse der neuen WLAN-Techniken gibt es derzeit nur als Labor-Ausstattung, die unter anderem den Herstellern dazu dient, ihre Komponenten zu prüfen. Doch schon alleine aus Kostengründen eignet sich diese Messtechnik nicht zur Unterstützung von WLAN- Planung und Betrieb.

Lehnen Sie sich also getrost zurück und beobachten Sie die weitere Entwicklung. Machen Sie die Verfügbarkeit von Messtechnik und Planungswerkzeugen zu einem K.-o.-Kriterium für den Einsatz der neuen WLAN-Techniken! Dann ist es für deren Einsatz früh genug.

Zweitthema

IPv6 und Sicherheit - technische Ansätze, der Weg zum Sicherheits-konzept

Fortsetzung von Seite 1

Dipl.-Inform. Oliver Flüs verfügt über langjährige Kenntnisse im Betrieb von IT-Infrastrukturen. Als Leiter des Competence Center IT-Service der ComConsult Beratung und Planung GmbH bearbeitet er seit Jahren Projekte in den Bereichen Services im IT-Bereich. Zu diesen Themengebieten ist er regelmäßig als Referent bei der ComConsult Akademie tätig, unter anderem als Schwerpunktreferent zu TCP/IP-Aspekten, in der Trouble Shooter-Seminarreihe sowie im Rahmen der Sicherheitsseminare.

Da auch die Verfügbarkeit und damit das störungsfreie Funktionieren von Lösungen mittlerweile als „Sicherheitsgrundwert“ behandelt wird, haben Sicherheitsbeflissene somit keine Zeit mehr, dem Thema IPv6 und Sicherheit noch länger auszuweichen und eine Situation mit günstigeren Rahmenbedingungen abzuwarten. Dabei ist Microsoft nicht etwa besonders „kundenunfreundlich“ mit seiner Strategie, IPv6 als verbindlichen Lösungsbestandteil zu behandeln, sondern (wie so häufig mit Blick auf Umsetzung von RFC-Spezifikationen) nur Vorreiter – weitere Hersteller werden folgen.

Andererseits wurde in dem früheren Artikel an einigen wichtigen Beispielen erläutert, dass es für die Aufgabenstellung „sicherer Umgang mit IPv6“ (noch) keine einfachen Standardantworten gibt. Dies ist teilweise auf die produkteseitige Umbruchsituation zurückzuführen, zum Teil auch darauf, dass manche aus Sicherheitsgründen verlockend erscheinende Ansätze betriebstechnisch nicht unbedingt für jede Umgebung ideal sind (z.B. ein Rückgriff auf „private“ IPv6-Adressen für interne Adressierung).

Insgesamt sind eine Reihe von Aspekten unter Berücksichtigung von Umgebungsbedingungen und IPv6-Fähigkeit präferierter Produktlinien zu beleuchten und zu entscheiden (siehe Abbildung 1).

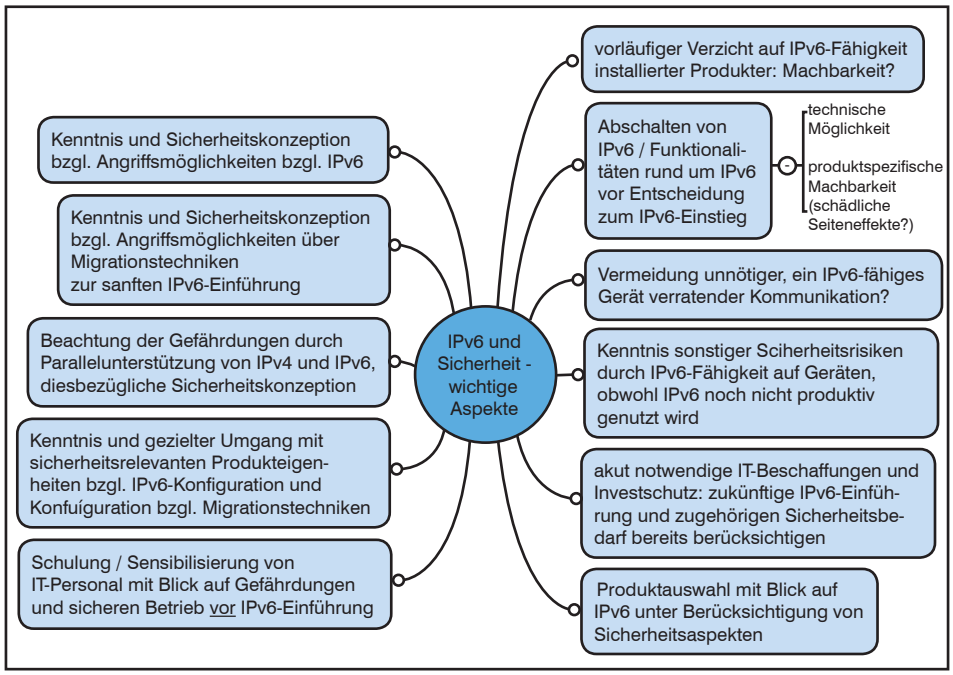


Abbildung 1: Übersicht: wichtige Elemente einer IPv6-Einführung unter Sicherheitsgesichtspunkten

Mit der Aktivierung von IPv6, vorerst typisch parallel zu IPv4 („dual stack-Betrieb“) kommen zu den bekannten Sicherheitsrisiken neue hinzu, teils durch IPv6 an sich, teils durch die parallele Verfügbarkeit von IPv4 und IPv6 – ein Angreifer kann über beide Protokollwelten ein Gerät schlimmstenfalls „in die Zange“ nehmen. Abschalten hat aber auch seine Gefahren (Seiteneffekte bzgl. Verfügbarkeit), und die Hersteller von Produkten mit Sicherheitsfunktionalitäten können auch noch nicht am Ende der Entwicklung notwendiger Gegenmaßnahmen sein: Dazu fehlt noch die ausreichend lange Praxisphase mit IPv6, während der so langsam alle grundlegenden „Schweinereien“ bzw. Implementierungsschwächen ausprobiert, entdeckt und durch Gegenmaßnahmen entschärft werden konnten.

Also: Man kann nur verlieren und ist hilflos?

Ganz so ist es nicht, auch wenn der Weg zu einem „umfassenden“ IPv6-Sicherheitskonzept und dessen erfolgreicher Umsetzung mühselig und sein Ende noch nicht absehbar ist. Entsprechend wäre die Ankündigung, mit dem vorliegenden Artikel ein „best practice“-Sicherheitskonzept zu IPv6 anzubieten, natürlich Schwindelei. Eindrücke, Beispiele und über diese auch erste konkrete Informationen für die IPv6-Sicherheitspraxis können und sollen aber gegeben werden.

Die Aufgabe wird sein, schrittweise unter Berücksichtigung jeweils neuester Erkenntnisse zu Angriffsformen, deren Ansätzen, Ideen zur Erkennung oder gar

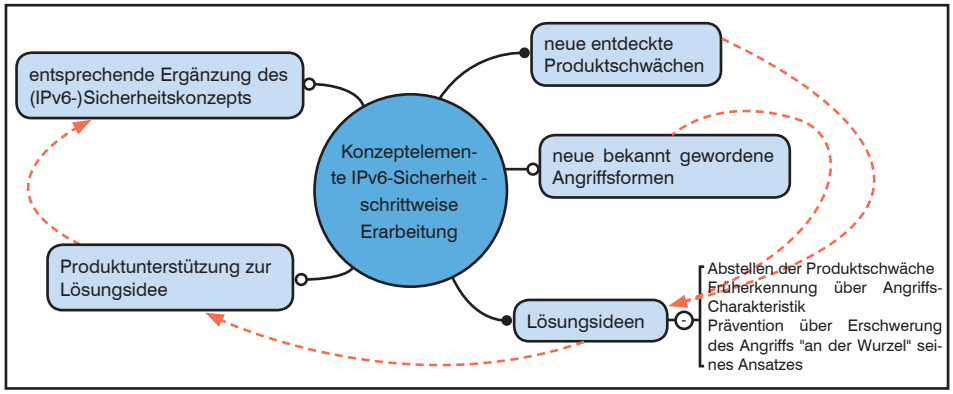


Abbildung 2: Typische Abfolge von Teilschritten auf dem Weg zu ausreichender IPv6-Sicherheit

Prävention und entsprechender Machbarkeit auf Produktebenen immer neue Puzzle-Steine zum Sicherheitskonzept zu legen, bis mittelfristig ein geeignet umfassender Schutz aufgebaut ist (siehe Abbildung 2).

Diese vorerst eher reaktive Erarbeitung eines IPv6-Sicherheitskonzepts wird im Zuge einer schrittweisen Einführung von IPv6 mehrfach anfallen. Dabei heißt es, aufmerksam zu bleiben und jeweils mit Ideen auf neue Herausforderungen zu reagieren.

Auch wenn dies mühselig ist und die Produktsituation jeweils zumindest anfangs aus Sicherheitsperspektive noch Wünsche übrig lassen wird, heißt dies nicht, dass man nichts tun kann.

Die nachfolgend diskutierten Beispiele sollen zeigen, dass man ohne große Genialität sowohl Ideen für Sicherheitsvorkehrungen mit Blick auf neue Angriffsformen bzw. Schwachstellen entwickeln als auch ganz konkrete Produktanforderungen daraus ableiten kann – bzw. zumindest mit gegebenen Produktmöglichkeiten Übergangslösungen finden kann, die das Risiko zumindest reduzieren.

Beispiel 1: IPv6 ist das Ende von „ping sweep“? Nicht ganz, aber …

Das erste Beispiel beginnt dabei scheinbar nicht mit einer Sicherheitsfrage, sondern einer Antwort auf eine altbekannte Frage: Wie verhindert man das Ausprobieren von Adressen als ersten Angriffsschritt? Häufig ist ein Auskundschaften einer Umgebung ein erster wichtiger Vorbereitungsschritt im Rahmen eines Sicherheitsangriffs; gelingt es, einem Angreifer bereits an so früher Stelle das Leben schwer zu machen, lässt er womöglich von dieser Umgebung ab, oder muss sich zumindest so auffällig verhalten, dass man große Chancen hat, ihn zu entdecken, ehe er mit den nächsten Angriffsschritten fortfahren kann.

weist. Wer einen solchen Vorrat der Reihe nach mittels Ping durchtesten will, verliert eine Menge Zeit und setzt sich dabei entsprechend lange der Gefahr aus, entdeckt zu werden.

Allerdings, wenn man sich genauer mit dem Thema beschäftigt, ist der Ping-Sweep-Versuch doch nicht so „sinnlos“ – statt einfach durchzuprobieren, kann man nämlich auch systematisch vorgehen. Die Systematik besteht darin, die praxisrelevanten Alternativen der Generierung von IPv6-Adressen durchzugehen und hierdurch die mit hoher Wahrscheinlichkeit in Frage kommenden Adressen von weniger

```
RFC 4291                IPv6 Addressing Architecture                February 2006

   For all unicast addresses, except those that start with the binary
   value 000, Interface IDs are required to be 64 bits long and to be
   constructed in Modified EUI-64 format.
```

Abbildung 3: Auszug aus RFC 4291 (Standards Track) bzgl. Interface ID-Länge

Eine unter IPv4 übliche Methode der Informationsgewinnung über ein Angriffsziel ist das systematischen Durchführen von Ping-Versuchen an aufeinanderfolgende Adressen („ping sweep“) mit dem Ziel, aktive IP-Adressen ausfindig zu machen und diese dann mit weiteren gezielten Testschritten bzgl. verwendeten Produkten und potenziellen Schwachstellen weiter einzugrenzen. Im Falle von IPv6 scheint dieser brute-force-Ansatz auf den ersten Blick wenig zielführend: Eine Möglichkeit der Adresserzeugung für ein Gerät unter IPv6 ist Autoconfiguration, bei der zu einem gegebenen „Netzwerk-Präfix“ die zur 128-Bit-Adresse fehlenden Bits des „Interface Identifiers“ von der IP-Software des Geräts selbst berechnet werden. Ein Ansatz dabei ist das Überführen der Layer 2-Adresse in den Interface Identifier, wobei Layer 2-Adressen von bis zu 64 Bit-Länge als Ausgangspunkt zu unterstützen sind (Stichwort: modified EUI64-Adressen). Um die gegebenenfalls 64 Bit der Layer-2-Adresse dabei vollständig verwerten zu können, ist etablierte Konvention (ursprünglich sogar: verbindliche Anforderung), dass ein Interface Identifier stets 64 Bit zu umfassen habe (siehe Abbildung 3).

Na und (mal abgesehen davon, dass diese Forderung nicht als „MUST“ formuliert und daher nicht in Stein gemeißelt ist)? Nun, setzt man diese RFC-Passage in die Praxis um, damit der Weg für Autoconfiguration mit modified EUI-Adressen in jedem Fall offen gehalten wird, so hat dies zur Konsequenz, dass jedes IP-Teilnetz die Größenordnung von 2^{64} Adressen aufwahrscheinlichen abzugrenzen. Beispiele:

- Geht man davon aus, dass auf Layer 2 Ethernet verwendet wird, sind die ersten 24 Bit der MAC-Adresse und damit die in Frage kommenden Bitmuster zu Beginn einer EUI64-Interface ID nicht mehr willkürlich, sondern durch die als „Herstellerkennungen“ im Ethernet-Bereich verwendeten Bitfolgen beschränkt.

- Diesen Ansatz über führende „Hersteller-Bits“ den vorderen Teil der Interface ID einzugrenzen, kann man als Angreifer noch gezielter ausnutzen, wenn man es auf bestimmte Gerätetypen abgesehen hat, bei denen man „autokonfigurierte Adressen“ erwartet, z.B. Notebooks oder Drucker.

- Werden Adressen aus einem Pool mittels DHCPv6 zugeteilt („stateful DHCPv6“), und die DHCP-Server-Software vergibt aus den freien Adressen „fortlaufend“, so genügt die Kenntnis einer ersten so verwalteten Adresse, um von dort aus systematisch auf- bzw. absteigend weiter zu probieren.

So oder ähnlich lässt sich zumindest für nach einer bekannten Systematik erzeugten bzw. festgelegten Adressen der Umfang der erfolgversprechenden Testkandidaten für Ping-Sweep durchaus signifikant eingrenzen und leider wieder mit erträglichem Aufwand ein Ping-Sweep als erster Schritt zur Informationsgewinnung über eine „Opfer-Umgebung“ durchführen – man versetzt sich in eine systematisch

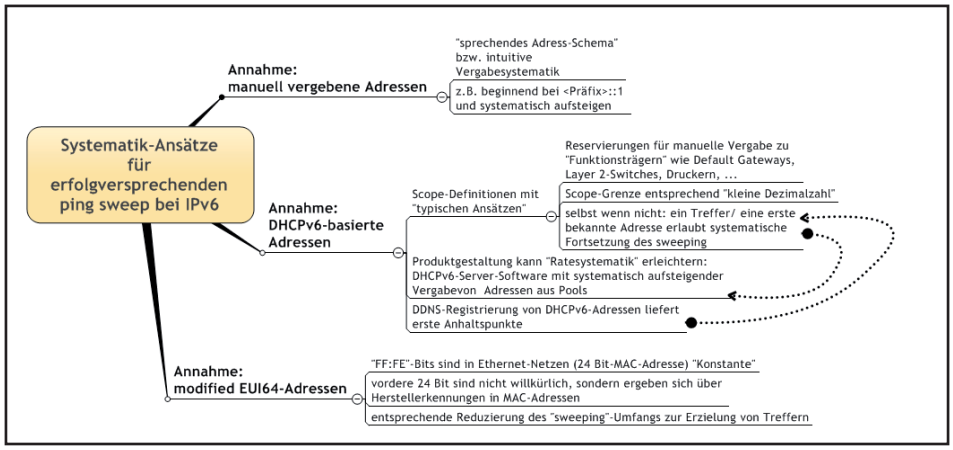


Abbildung 4: Systematik-Ansätze für erfolgversprechenden Ping-Sweep bei IPv6

arbeitende Software oder ein systematisches „manuelles Vergabekonzept“ hinein (siehe Abbildung 4).

Voraussetzung hierfür ist natürlich, dass ein Angreifer mit Ping überhaupt bis zum „Subnetz“ interessanter Angriffsziele durchkommt. Für Angriffe „von außen“ ist das Gegenmittel der Wahl wie unter IPv4 eine Firewall-artig arbeitende Komponente – die Idee ist weder IPv6-spezifisch noch ein neuer Gedanke.

Bleibt der Innentäter, der innerhalb einer Sicherheitszone, also ohne störende Firewall zwischen sich und möglichen Angriffszielen, tätig wird. Typische Maßnahmen, mit denen nur „kontrollierten“ Geräten ohne installierte Angriffstools Netzzugang gewährt oder dieser auf für Angreifer uninteressante Gastnetze beschränkt wird, wirken hier genauso wie zur „Abwehr“ von Angriffsversuchen mittels IPv4-basierter Tools!

Darüber hinaus kann man versuchen, dennoch auffällig häufiges Ping an wechselnde Adresse mittels Intrusion-Detection-Intelligenz zu erkennen und zu melden. Sofern man bei DHCPv6 nicht von vorneherein auf eine bestimmte Serverseitige Software-Lösung festgelegt ist, kann man zudem die Produktanforderung einer „pseudo-zufälligen“ Wahl der jeweils als nächstes angebotenen freien Pool-Adresse stellen und verfolgen.

Das sind doch gleich eine ganze Reihe von Ideen, mit dem Thema IPv6-Ping-Sweep umzugehen:

- Netzzugangskontrolle u.Ä. (auch für IPv4 wirksame!) Ansätze
- Einsatz von DHCP-Server-Software mit „unsystematischer Poolnutzung“
- IDS-Einsatz – massives Echo-Request-Aufkommen als Angriffsindiz (Vorsicht: die IDS-Lösung sollte mit „weißen Listen“ differenziert konfiguriert werden können – Autodiscovery-artige Funktionalitäten von Management-Tools nutzen aus „IPv4-Tradition“ ebenfalls gerne Ping-Sweep als Ansatz!)
- Sperrung von ICMP Echo auf Sicherheitsübergängen

Hilflosigkeit gegenüber einem Angriffsversuch sieht anders aus …

Beispiel 2: Denial of Service-Attacken auf IPv6-Mechanismen

Die Väter von IPv6 haben großen Wert auf die Möglichkeit gelegt, vernetzte Geräte aus ihrer Umgebung lernen zu lassen, so dass größere Unabhängigkeit von (herstellerspezifischen) Lösungen zur Geräte-lokalen Verwaltung von Konfigurationsparametern besteht. Allerdings: sicherheitstechnisch birgt jeder Input aus der Netzumgebung auch die Gefahr, mit vorsätzlich gefälschten Informationen angegriffen zu werden.

Rein destruktive Angriffe setzen Inhalte gefälschter Pakete dann so, dass der Empfänger bei korrekter Reaktion auf diese Inhalte teilweise oder gänzlich davon abgehalten wird, Nutzkommunikation aufzunehmen. Hierzu bieten sich gleich mehrere IPv6-Mechanismen und zugehörige Pakettypen an:

- Duplicate Address Detection DAD

  Gedacht ist dieser Ansatz zur Vermeidung doppelter Adressen, bei Verwendung gleich verschiedener Möglichkeiten automatischer Adressgenerierung (stateful DHCPv6, Autoconfiguration mit mehreren Varianten) wichtiger denn je. Die vom Windows-DHCP-Client unter IPv4 schon lange verwendete Methode des „ARP-Requests auf die eigene IP-Adresse“ wird hier mit den Mitteln der IPv6-Neighbor-Discovery zum Standard-Test gemacht.

  Wenn jedoch ein Angreifer die „ausnahmsweise“ Negativmeldung „Adresse wird benutzt!“ zur Regel werden lässt … Natürlich kann man auf die Idee kommen, DAD als Gegenmaßnahme „abzuschalten“. Dies ist für die Praxis jedoch gut zu überlegen – zu wertvoll ist die durch DAD angebotene „automatische“ Verhinderung von Störungen durch doppelte Adressen und ähnliche nützliche Auswirkungen von DAD auf den Betriebsaufwand.

- Autoconfiguration basiert auf speziellen Router-Advertisements, welche zu solchen Präfixes, für die eine Autoconfiguration erfolgen soll, den notwendigen Input und per Flag die „Erlaubnis“ zur Verwendung des Präfix für Autoconfiguration geben.

  Ein Denial-of-Service-Angriff kann darin bestehen, dass gefälschte Router-Advertisements „Negativ-Informationen“ liefern, so dass kein sinnvoller Autoconfiguration-Vorgang mehr stattfindet.

- Router-Discovery

  Über spezielle „Router-Advertisements“ können Subnetz-Router unter anderem ihre Fähigkeit, als Subnetz-Router den „first hop“ zum restlichen Netzwerk zu bilden, an die Teilnehmer im Subnetz kundtun.

  Wird ein (zu einem Paar redundanter Subnetz-Router) gehörender Layer 3-Switch geplant abgeschaltet, z.B. zwecks Wartung, so ist das Senden eines Router-Advertisements zur „Abkündigung“ der Bereitschaft als Subnetz-Router „guter Stil“ des Produkts, um unnötige Störungen zu vermeiden.

  Schickt jedoch ein Angreifer solche Abkündigungen häufig genug, kann aus Sicht der Subnetz-Teilnehmer der Ausgang zum Restnetz vollständig verloren gehen.

  Dabei muss man als Angreifer noch nicht einmal unbedingt die schädlichen Pakete „konstruieren“. Mit genügend Zeit und Geduld kann man ein anzugreifendes Subnetz zunächst passiv „abhören“ (Vorarbeiten wie für Belauschen von IPv4-Traffic, also nichts Neues), bis Subnetz-Gateways zu Wartungszwecken o.Ä. planvoll „heruntergefahren“ werden. Die mitgeschnittenen Pakete werden dann als „Replay-Attacke“ wiederholt vom Angreifer gesendet …

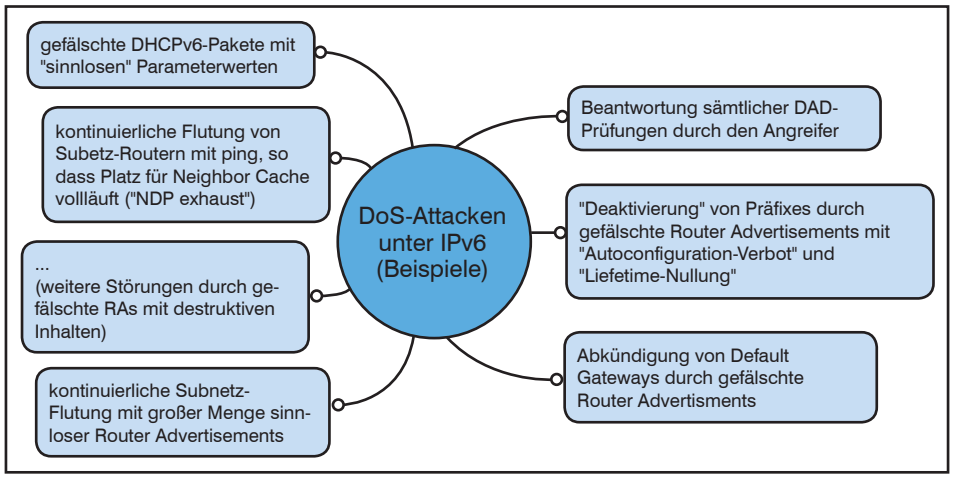


Abbildung 5: Übersicht DoS-Ansatzbeispiele

Dies sind nur einige Beispiele, die zeigen, dass gerade die Subnetz-lokalen („first hop"-Bereich) Lern- und Informationsmechanismen leicht für Denial-of-Service-Ansätze missbraucht werden können; es gibt deutlich mehr. Hinzu kommt die Anwendung von bereits unter IPv4 sinngemäß gegebenen Ansätzen wie gefälschte, destruktive DHCP-Paketinhalte oder Lastattacken auf wichtige Objekte wie eben die Subnetz-Router.

So mächtig Router-Advertisements als Hilfsmittel für den Betrieb von Teilnehmer-Subnetzen sind, so vielfältig sind leider auch die Möglichkeiten, die verschiedenen Parameter und Optionen zu missbrauchen. Unter dem Deckmantel einer Nutzung solcher sinnvollen Hilfsmechanismen können sich „weitere Störungen durch gefälschte RAs mit destruktiven Inhalten" verbergen:

- „Autoconfiguration-Verbot" (Parameter SLAAC) für alle Präfixe und Setzen des „M-Flags", mit dem ein Anfordern einer Adresse mittels DHCPv6 vorgegeben wird, in einer Umgebung, in der gemäß der echten Router Advertisements gar kein stateful DHCPv6 vorgesehen, also vermutlich auch kein Pool eingerichtet ist

  Das besonders heimtückische an so aufgebauten Paketen besteht darin, dass sie nicht unmittelbar als „destruktive Flag-Kombination" eingestuft werden und somit nicht durch eine IDS-Lösung gemeldet werden können. In einem Subnetz, das genau mittels stateful DHCPv6 aus einem Adress-Pool betrieben werden soll, wäre ein solcher Paketaufbau ja gewollt, d.h. solche Paketinhalte sind nicht per se „bösartig"!

- Router-Advertisements mit Propagieren einer unnötig kleinen MTU-Size
  Reagiert ein IP-Stack hierauf, so werden auch bei umfangreichen Datenübertragungen unnötig kleine Pakete gebildet – fatal, weil eine durchaus spürbare Beeinträchtigung der Übertragungsperformance die Folge ist und die durchlaufenen Netzkomponenten völlig unnötig mit einem Vielfachen an Transportentscheidungen „gestresst" werden. Absolut destruktiv, aber wegen des „unnatürlichen" Parameterwerts auch treffsicherer durch IDS-Intelligenz zu entlarven, sind derartige Fake-RAs mit so kleinem MTU-Parameterwert, dass bei Befolgen dieses „Vorschlags" die minimale Paketgröße des verwendeten Layer 2- Protokolls unterschritten würde – hier kommt gar keine Kommunikation zustande. Da wünscht man sich ja fast IP-Stacks, die zu simpel programmiert sind, um auf solche Parameter zu reagieren …

  Wenn wir schon bei „sinnlosen", aber dabei schädlichen Inhalten sind: Lastattacken funktionieren nicht nur mittels ICMP-Echo (gegen das man Geräte ohne Behinderung der Nutzkommunikation „taub" stellen kann), sondern auch mit Router-Advertisements: So kann man z.B. in sehr kurzen Abständen Router-Advertisments mit inkorrekter Prüfsumme verschicken.

  Unangenehm dabei: Hat ein etwa verwendetes IDS-System bislang nur die Intelligenz, auffällige Parametersetzung zu prüfen, nicht aber auch zur Prüfung und Meldung falscher Prüfsummen, so schlüpfen solche Fake-Pakete durch die Maschen der Überwachung und beschäftigen sinnlos die im betroffenen Subnetz angeschlossenen Teilnehmer mit Lesen – Prüfen – Wegwerfen, ohne unmittelbar entdeckt zu werden.

Leider sind Angriffszenarien der beschriebenen Art längst keine theoretische Gedankenspielerei mehr, es gibt Proof-of-Concept-Tools im Internet, die natürlich auch ein Angreifer als „Werkzeug" missbrauchen kann.

Beispiel 3: Erschleichung von Man-in-the-Middle-Position unter IPv6

Damit noch nicht genug – „natürlich" kann man nicht nur rein destruktiv Missbrauch von IPv6-Lernmechanismen betreiben. Statt Kommunikation lahm zu legen, kann ein Angreifer versuchen, über gefälschte Inhalte von Informationspaketen zu IPv6-Mechanismen sich selbst „widerrechtlich" als Träger einer Rolle auszugeben, die dazu führt, dass Netzwerkkommunikation ab jetzt konsequent zum Angreiferrechner gelangt – das Ziel ist dabei typisch, in eine Man-in-the-Middle-Position zu kommen, vor allem in die Rolle eine scheinbaren Subnetz-Routers, indem

- der Angreifer-Rechner sich selbst auf die Default-Gateway-Kandidaten-Liste „schmuggelt"
- sich selbst dabei mit entsprechender Priorität an die Spitze dieser Liste manövriert oder/ und
- die eigentlichen Subnetz-Router „abkündigt", so dass diese Konkurrenz um die Rolle des „first hop" aus dem Weg geräumt wird.

Die unter IPv4 schon bekannte Idee, sich anstelle des eigentlichen Subnetz-Gateways in den ARP-Tabellen einzunisten, kann ebenfalls unter IPv6 angewandt werden – was unter IPv4 als ARP-Mechanismus angegriffen wurde (ARP-Poisoning), kann gleichartig unter IPv6 als „Neighbor Discovery" wiedererkannt und attackiert werden.

Das Ziel des Man-in-the-Middle (als Vorbereitung des eigentlichen Angriffs, etwa auf die Vertraulichkeit der so mitgehörten Kommunikationsinhalte) ist nicht neu, die Idee des gefälschten Inputs als Methode auch nicht, aber mit IPv6 bieten sich neue Ansatzmöglichkeiten zur Umsetzung – bzw. schlichtweg eine Übergangssituation, während der ein unter IPv4 bekannter und mit verfügbaren Produkt-Eigenschaften abwehrbarer Angriffsversuch in neuem Gewand noch ohne produktverfügbare Gegenwehr bleibt. Tools zum Praktikabilitätsnachweis solcher Angriffsmethoden gibt es dagegen schon längst. „Der neueste Schrei" scheint dabei die schädliche Verwendung von unter IPv6 neu verfügbaren, optionalen „Extension-Headern" zu sein, offenbar in der nicht unberechtigten Hoffnung, dass Firewalls und IDS-Systeme, die auf „Standard-An-

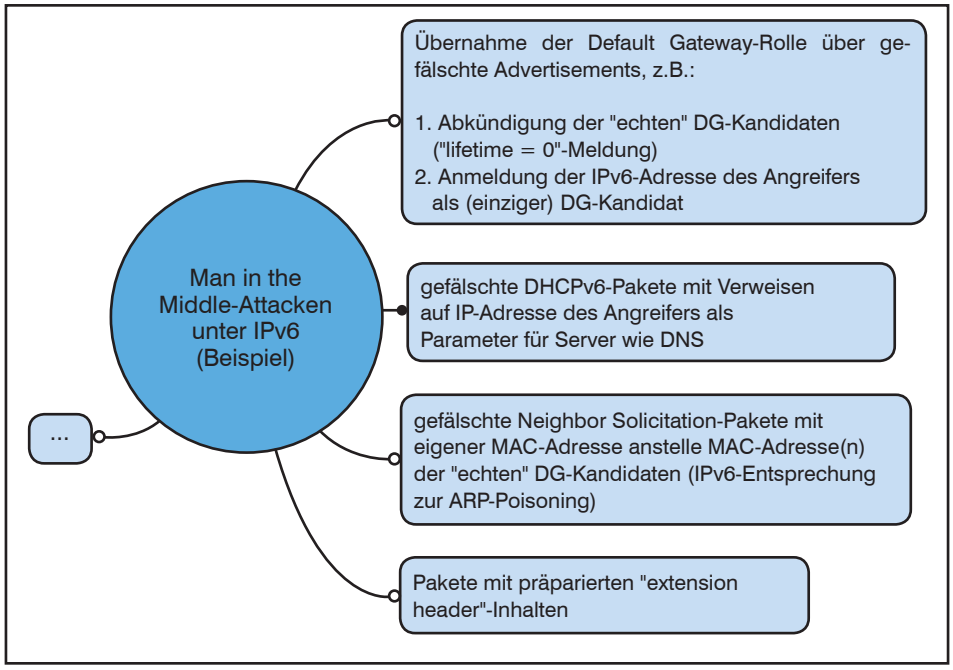


Abbildung 6: Beispiele für Ansätze zu Man-in-the-Middle-Anbahnung unter IPv6

griffe“ über IPv6-Standard-Header-Felder mittlerweile intelligent reagieren können, für Extension-Header vorerst noch keine solche Intelligenz aufweisen (siehe Abbildung 6).

Bei näherem Hinsehen entpuppen sich die „beiden“ Beispiele 2 und 3 also gar nicht als „nur“ zwei Angriffsformen, sondern gleich als ein ganzer Sack voll, mit zum Teil von IPv4 bekannten Ideen erweitert durch gezielte „Fehlinterpretation“ unter IPv6 neuer Detailmechanismen.

Allerdings fehlten bislang anders als beim ersten Beispiel die Antwortversuche in Form von Ansätzen für Gegenmaßnahmen. Der Grund: Die Methoden unter Beispiel 2 und Beispiel 3 haben grundlegende Gemeinsamkeiten, so dass man auch auf die (berechtigte) Idee kommen kann, sie gemeinsam mit gezielten Gegenmaßnahmen zu bekämpfen.

Die grundlegende Gemeinsamkeit ist zunächst eine Einmischung in Lernmechanismen, die vor allem Subnetz-lokal Aussicht auf Erfolg hat. Dies bedeutet, der Angreifer muss unmittelbar eine Innentäter-Position einnehmen, oder per Schadsoftware einen berechtigten Teilnehmer infiltriert und mit Angriffswerkzeugen verseucht haben, die er „fernsteuern“ kann. Zur Vermeidung der Fernsteuerung per platzierter Schadsoftware kann IPv6-spezifische Abwehr wenig Neues beitragen, hier greifen die üblichen, hoffentlich bereits mit Blick auf IPv4 als „Abwehr-Infrastruktur gegen Schadsoftware“ realisierten Vorkehrungen gegen Schadsoftware-Befall. So oder so – es gilt, den Innentäter als Position zu vermeiden (auch hier ist Netzzugangskontrolle ein richtiges Stichwort), bzw. zumindest, ihn auf Grund seines besonderen Verhaltens zu entlarven und hierauf zu reagieren

- durch Verweigerung der Reaktion auf seinen Input (dies wäre durch die an das Netz angeschlossenen „Teilnehmer“ zu leisten) bzw.

- durch Entzug des Netzzugangs bei auffälligem Verhalten (eher eine Aufgabe für die Netzkomponenten).

Außerdem wäre da natürlich noch der Brachialansatz – Mechanismen, über die ein Angreifer ansetzen kann, schlichtweg zu deaktivieren. Dies würde allerdings in vielen Fällen mindestens so stark schaden wie nutzen, da dann das „Betriebskonzept“ auf statische Einträge in zur Kommunikation notwendigen gerätelokalen Tabellen hinausliefe sowie manuelle Grundkonfiguration aller Teilnehmer – das macht unter IPv4 aus guten Gründen niemand „in der Fläche“, und das wäre auch unter IPv6 wenig praktikabel als „Grundkonzeption der IPv6-Sicherheit“. Als besonders harte Vorsichtsmaßnahme für besonders hohen Sicherheitsbedarf kann man sich diese Idee einmal merken, für den Durchschnittsfall im „Massenbetrieb“ großer Netze muss etwas mit geringerem Aufwand Handhabbares her, das Raum für zeitgemäße Betriebskonzepte lässt.

Wer seinen Bestand an Netzkomponenten sichtet und recherchiert, was diese – ggf. nach Durchführung eines Firmware-Updates – an Sicherheitsbeiträgen zu den dargelegten Angriffsszenarien anbieten, kann zum jetzigen Zeitpunkt zu einem unbefriedigenden Ergebnis gelangen. Da Einsatzpraxis mit IPv6 noch am Anfang steht, ist es auch nicht verwunderlich, wenn seitens der Hersteller insbesondere das Sicherheitsthema noch „Baustelle“ ist – zuerst ist aus verständlichen Gründen die Unterstützung der IPv6-Mechanismen implementierungstechnisch an der Reihe, dann folgen womöglich erst Aspekte wie Sicherheitsbeiträge und IPv6-basiertes Management. Dennoch oder auch gerade dann ist eine Beschäftigung zum heutigen Zeitpunkt mit möglichen Sicherheitsbeiträgen durch die Netztechnik sinnvoll:

- erst auf Basis von Überlegungen bzw. ersten Informationen bzgl. möglichen Sicherheitsfunktionalitäten kann gezielt für die in der eigenen Umgebung präferierten Produktlinien recherchiert werden

- auf Grundlage von konkreten Entwürfen für präferierte und realistische Sicherheitskonzepte zum Umgang mit IPv6-Sicherheitsfragen kann man den bzw. die eigenen Lieferanten mit entsprechenden Anforderungen konfrontieren – und so das Signal für einen „business case“ aus Sicht der Hersteller aussenden, so dass diese das Sicherheitsthema mit erhöhter Priorität im Produktmanagement berücksichtigen.

Also: Was können Netzkomponenten zur IPv6-Sicherheit (potenziell) beitragen?

Mögliche Beiträge zur IPv6-Sicherheit durch Netzkomponenten

Im Zusammenhang mit Sicherheitsbeiträgen durch die Netzinfrastruktur fallen einem vermutlich reflexartig sofort Paketfilter-Funktion und vergleichbares ein, also etwa Access-Control-Listen (ACLs) auf Layer 3-Switches oder gleich dedizierte Firewall-Komponenten und Ähnliches. Das ist natürlich richtig und hier kann man mit Blick auf IPv6 mehrfach aktiv werden:

- Schutz von Netzbereichen durch vollständige Sperrung von IPv6-Kommunikation

  Ein derart drastischer Eingriff ist natürlich nur sinnvoll für Netzbereiche, in denen jetzt oder in naher Zukunft schon IPv6-fähige Geräte angeschlossen werden, auf denen dabei ein Abschalten von IPv6-Unterstützung problematisch ist, aber IPv6 noch gar nicht genutzt werden soll. Diese kann man per vorgelagertem „Firewall-Schutz“ pauschal vor Angriffsversuchen via IPv6 von au-

ßerhalb des so abgeschotteten Netzbereichs schützen, ohne gewollte Nutzkommunikation zu behindern.

Will man zu dieser Methode greifen, muss man dabei darauf achten, auch IPv6-über-IPv4-Tunnel zu verhindern, d.h. auch IPv4-Pakete mit Anzeichen auf solches Tunneling (z.B. „protocol"-Feld im IPv4-Header mit Wert 41 besetzt oder Verwendung der für Teredo typischen UDP-Ports) sind in der Pauschalsperrung mit zu erfassen.

- Schutz vor Angriffen über IPv6 mit nicht vorgesehenen Kommunikationsformen

  Dies ist die unter IPv4 jahrelang bereits „geübte" Standard-Rolle von Firewalls und Switches mit ACLs. Neu unter IPv6 ist hier das zusätzlich zu erlernende Detailwissen, welche Sperrungen nützlich und welche mit Blick auf gewollte Nutzkommunikation schädlich sind – hier muss IPv6-Detailwissen mit Kenntnis über in einer Zielumgebung produktiv eingesetzte Anwendungen und Dienste und zugehörige Kommunikation kombiniert werden. Ansonsten gibt es hierzu nichts grundsätzlich Neues zu sagen (bis auf die Tatsache natürlich, dass die eingesetzten Firewalls etc. erst einmal eine Software-Version aufweisen müssen, die solche IPv6-spezifischen Regeln unterstützt – auch hier wartet Arbeit in Form von Produktrecherchen, Lieferanten- und Herstelleranfragen und Migration).

Abschotten alleine genügt für ein zeitgemäßes Sicherheitskonzept aber nicht, auch für die gewollte produktive Nutzung zunächst grundsätzlich zuzulassenden Paketen müssen auf unnötige Restrisiken untersucht und nach Möglichkeit entsprechend unterschieden werden. Außerdem: Für etliche der oben diskutierten Angriffsformen mit Blick auf „first hop-Security", vor allem auf Neighbor-Discovery-Mechanismen, ist durch Abschottung von Netzbereichen keine entscheidende Gegenwehr möglich. Solche Angriffe mischen sich in Subnetz-lokale Abläufe ein, d.h. ein Firewall- oder Layer 3-Switch-Übergang ist gar nicht beteiligt.

Hier müssen weitere Ansätze gefunden werden, welche die Bildung von „Netzzonen" durch Firewall-Schutz gezielt ergänzen.

Denkbar sind eine Reihe von Prüfungen und Reaktionen durch Netzkomponenten auf mögliche Sicherheitsangriffe. Eine Grundidee für solche Mechanismen kann verallgemeinert so beschrieben werden:

1. (Die Netzkomponente prüft, ob Paketinhalte korrekt aufgebaut sind.)
2. Die Netzkomponente prüft, ob derartige Pakete Eigenschaften aufweisen, die verdächtig sind bzw. auf die eine Transportverbotsregel zutrifft.
3. Werden „verdächtige Unregelmäßigkeiten" entdeckt, so unterbleibt der Weitertransport.

Auf den ersten Blick liest sich das wie eine sehr unsaubere Beschreibung einer Firewall-Intelligenz. Tatsächlich ist einem größeren Teil von Angriffen der oben beschriebenen Art („first hop security") jedoch mit einer ab Layer 3 arbeiteten Prüfintelligenz nicht beizukommen, denn: First hop security bezeichnet Aspekte, die Subnetz-lokale Mechanismen betreffen, eben im unmittelbaren Umfeld des Senders eines Pakets. Dieser Sender soll betrogen oder kommunikationsunfähig gemacht werden, indem ihm Fehlinformationen über seine unmittelbare Umgebung (Nachbarschaft – „Neighbor-Discovery"-Mechanismen sind betroffen) gegeben werden oder er mit zu Neighbor-Discovery-Funktionalitäten gehörenden Paketen in schädlicher Menge gestresst wird. Ein Routing-Hop kommt also gar nicht erst ins Spiel – der Layer 2-Switch ist gefragt! Dieser muss erkennen, dass mit den Angreiferpaketen etwas faul ist, und diese „kassieren", d.h. verwerfen, statt sie zu verteilen. Nun soll ein Layer 2-Switch aber vor allem mit hoher Performance Pakete transportieren, allzu aufwändige Prüfmechanismen siedelt man lieber auf Layer 3-intelligenten Komponenten (Switches oder spezielle Sicherheitskomponenten) an. Also wird eine einfache Prüffrage benötigt, die mit geringem Zeitaufwand beantwortet werden und das Transportverhalten des Layer 2-Switches unter Sicherheitsgesichtspunkten beeinflusst. Eine Frage, die dieser Anforderung genügt, ist:

„Ist der Eingang eines solchen Pakets auf diesem Port zu erwarten?" Oder anders formuliert: „Kann von dem an diesem Port angeschlossenen Gerät ein solches Paket kommen, wenn alles mit rechten Dingen zugeht?"

Das soll eine einfache Fragestellung sein? Im Fall der oben vorgeführten Fälle von Paketfälschungen ja: Router-Advertisements kommen „rechtmäßig" nur von Subnetz-Routern, die der Netzbetreiber entsprechend konfiguriert hat, und dasselbe gilt typisch für DHCP-„Antworten" auf Anfragen (Request- oder Solicit-Pakete) durch DHCPv6-Clients – der direkte Anschluss eines DHCP-Servers an Teilnehmernetze ist doch eher die Ausnahme, und als Relay Agent wird zumeist der Subnetzrouter verwendet.

Verweigert also ein Layer 2-Switch den Weitertransport von Router-Advertisements und informativen DHCP-Nachrichtentypen, sofern sie nicht von einem Port stammen, den er als „Router-Anschlussport" erkennt, so muss ein Angreifer schon den Subnetzrouter selbst übernehmen, um noch über solche Pakete Unfrieden zu stiften. Hat man ein solches Switch-Produkt zur Verfügung, muss dieses also nur noch „lernen", welches die rechtmäßigen „Router-Ports" sind, und eine Menge Angriffe sind deutlich erschwert. Hier darf man natürlich nicht leichtsinnig die in Neighbor Advertisements enthaltene Information „bin ein Router" ungeprüft als Basis hernehmen – dies wäre mit einem selbstgebastelten „amtlichen" Ausweis zu vergleichen, den ein Betrüger vorzeigt, um an der Tür Vertrauen zu erwecken und in die Wohnung gelassen zu werden (siehe Abbildung 7).

Auch die verwendete Senderadresse eines solchen Pakets ist natürlich kein Beweis für die Authentizität dieser Information, selbst dann nicht, wenn diese Information „Solicited", d.h. als Antwort auf eine konkrete Anfrage, eintrifft. Entweder, man kann die Vertrauenswürdigkeit der Quelle eines solchen Advertisements kontrollieren, oder aber die Einstufung eines Ports als „Router-Anschluss" muss „von Hand", also per Konfiguration durch den Netzbetreiber erfolgen können.

Beachtet man diese Details, ist die Idee aber nicht besonders kompliziert, so dass damit gerechnet werden kann, dass derartige Ansätze in absehbarer Zeit von di-

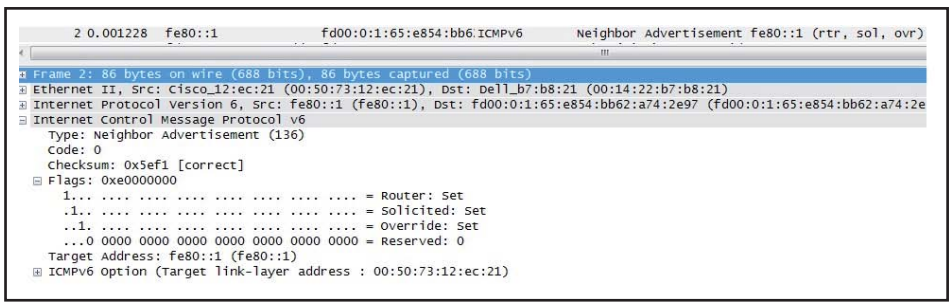


Abbildung 7: Neighbor-Advertisment mit gesetztem „Router"-Flag

versen Switch-Herstellern angeboten werden können. Für IPv4 gibt es Vergleichbares schon lange, und nicht nur über Sicherheitsthemen ist unter IPv4 erfolgreich vorgeführt worden, dass das Prüfen und Unterdrücken einer Verteilung von Paketen auf alle Ports eines Layer 2-Switches ohne negativen Einfluss auf die sonstige Performance des Switches realisiert werden kann, siehe etwa Snooping für Multicasts. Auch wenn notwendiger Konfigurationsinput zunächst lästig ist, diesen Preis der Sicherheit zahlt doch unter IPv4 heute schon jeder bereitwillig, der mit ACLs auf Layer 3-Switches oder mit IDS-Komponenten als Elementen seines IPv4-Sicherheitskonzepts arbeitet.

Also: Ja, über Netzwerkkomponenten können Beiträge zur Erschwerung von Angriffen auf IPv6-Grundmechanismen geleistet werden, und es lohnt sich, die Entwicklung des Produktangebots in diesem Sinne zu beobachten bzw. im Rahmen des Möglichen durch gezielte Interessenbekundung an solchen Features zu beeinflussen. Auch mögliche Berichte über Schwächen erster derartiger Implementierungen bzw. verbleibende Möglichkeiten, diese mit erhöhtem Aufwand doch auszutricksen, sollten nicht davon abhalten, das IPv6-Sicherheitskonzept bei Verfügbarkeit um solche Lösungselemente zu ergänzen. Man verzichtet doch auch nicht auf das Anlegen des Sicherheitsgurts beim Autofahren, weil dieser keine hundertprozentige Sicherheit gewährleistet?!

Im Übrigen haben sich die Väter von IPv6 auch schon frühzeitig ihre Gedanken gemacht, dass und wie man IPv6-Basismechanismen, insbesondere Mechanismen rund um Neighbor Discovery (Neighbor Solicitation, Router Solicitation, Autoconfiguration, Duplicate Address Detection usw.) missbrauchen könnte, und einen RFC mit Ansätzen zur Unterbindung solcher Angriffsideen herausgegeben. Unter der Überschrift Secure Neighbor Discovery („SEND“, RFC 3971) ist ein Standard-Track RFC schon seit langem verfügbar, der eine Reihe typischer Sicherheitsansätze als Optionen kombiniert beschreibt, um diverse Ansätze zum Angriff auf Neighbor-Discovery-Mechanismen zu vereiteln und die Wirkung von Neighbor-Discovery-Paketen auf vertrauenswürdige Quellen zu beschränken (siehe Abbildung 8).

- Durch Signieren von Informationspaketen kann deren Verfälschung verhindert werden.
- Durch Verwendung kryptographisch generierter Adressinformationen, die nur der „echte“ Sender bilden und der Empfänger auf Grund gemeinsamen Wissens auf Echtheit prüfen kann, kann die Vertrauenswürdigkeit des Erzeugers eines Pakets kontrolliert werden.
- Mit Zeitstempeln und Einweg-Pseudozufallszahlen („Nonce“) als Begleitinformation kann das Mitschneiden und Wiederverwenden signierter und mit kryptographisch generierter Adresse gesicherter Pakete durch einen Angreifer deutlich erschwert werden.

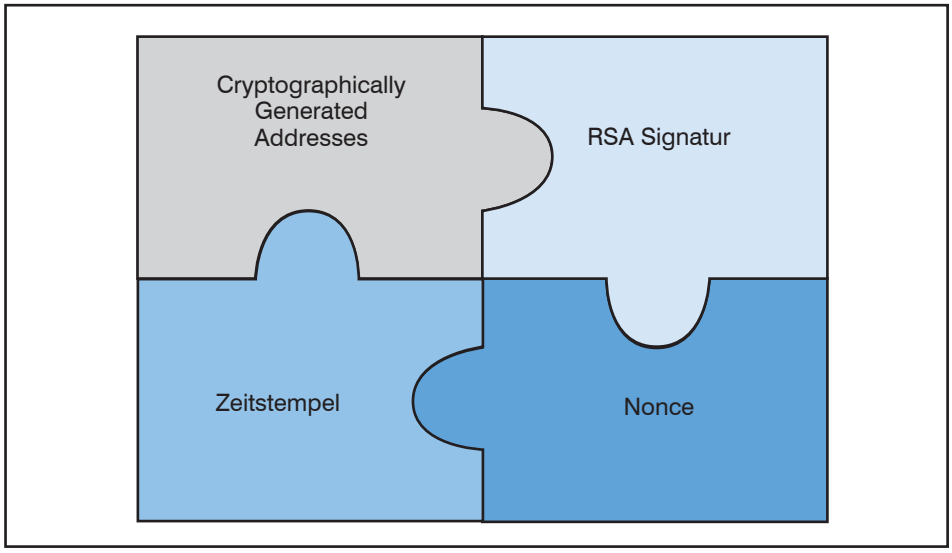


Abbildung 8: Bausteine von SEND

Wer sich bereits länger mit Sicherheitslösungen beschäftigt, erlebt hier keine bahnbrechenden Überraschungen, es werden „typische“ Sicherheitselemente miteinander kombiniert, nur jetzt eben mit Blick auf Angriffe auf IPv6-Mechanismen (siehe Abbildung 9).

Warum also die zuvor dargelegte Idee des „IPv6-Sicherheits-intelligenten Layer 2-Switches“, wenn man doch Plan A schon als RFC in der Tasche hat? Die Antwort: Praktikabilität! Secure Neighbor Discovery ist kein Selbstläufer, sondern erfordert signifikanten Betriebsaufwand, nicht zuletzt durch die Verwaltung der notwendigen Schlüssel/ Zertifikate („Trust Anchor“, der aufgebaut und auf den vernetzten Teilnehmern eingetragen werden muss). Der hiermit verbundene Aufwand ist nicht in jeder Netzumgebung und –größe sinnvoll realisierbar, das „Impfen“ von Layer 2-Switches kann dann die verhältnismäßigere Variante sein. Außerdem: SEND kann nur erfolgreich eingesetzt werden, wenn Netzkomponenten und vernetzte Teilnehmer es durchgängig unterstützen. Auf Seiten der Komponentenhersteller gibt es erste Beispiele von Produktverfügbarkeit, bei der Vielzahl von Produkten im „IP-Host“-Bereich ist SEND noch nicht in einer Form angekommen, dass man es sinnvoll in die Fläche bringen könnte. Hier muss man die

Angriffsbeispiel	Absicht z.B.	Entschärfung mittels SeND
Spoofing (Fälschung) von Neighbor Solicitation	Provozieren von Advertisements zum Ausspähen der Umgebung	Forderung nach RSA Signature und Verwendung von CGA Options in Solicitations
Spoofing (Fälschung) von Neighbor Advertisment	Übermittlung gefälschter Basisinformationen für "next hop-Bestimmung" zur Herbeiführung einer Man in the Middle-Position	Forderung nach RSA Signature und Verwendung von CGA Options in Solicitations; Verwendung von Nonce in Solicitation
DoS-Angriff mittels gefälschter Advertisements als Antwort auf DAD-Neighbor Solicitations	"Denial of Servie": angegriffener Rechner kann keine ihm zugeteilte / automatisch generierte Adresse verwenden	Forderung nach RSA Signature in Neighbor Advertisment als Antwort auf DAD-Solicitations, Prüfung der Echtheit vor Akzeptieren
Router Solicitaion / Advertisement-Attacken	Ausspähen der Umgebung / Vorbereitung einer Man in the Middle-Position	Forderung nach RSA Signature in Neighbor Advertisment als Antwort auf DAD-Solicitations, Prüfung der Echtheit vor Akzeptieren
Replay Attacken	z.B. Denial of Service durch fortwährende Beschäftigugn der Empfänger mit Aktualisierung ihrer Caches	Nutzung / Prüfung von Nonce und / oder Timestamp

Abbildung 9: Beispiele für gezielte Abwehr von Angriffsformen mittels SEND-Ansätzen

Marktentwicklung abwarten – vielleicht wird SEND mittelfristig ein selbstverständliches Sicherheitskonzeptelement, vielleicht wird es auch dauerhaft ein Ansatz für Netzbereiche mit besonders hohem Sicherheitsbedarf bleiben, angesichts dessen man eine eingeschränkte Produktauswahl zu akzeptieren bereit ist …

Mögliche Beiträge zur IPv6-Sicherheit durch vernetzte Teilnehmer (Clients, Server)

Die Unterstützung von Secure Neighbor Discovery ist also ein erster wünschenswerter Beitrag, den vernetzte Teilnehmer (Clients, Server, Peripheriegeräte wie Drucker, also insgesamt „Hosts" in der RFC-Sprache) zur IPv6-Sicherheit leisten können.

Gibt es noch mehr, das man auf Sinnfälligkeit für den eigenen Geräteeinsatz prüfen und ggf. mit Blick auf Produktunterstützung fordern sowie wenn vorhanden auch gezielt nutzen kann?

Möglichkeiten zur Feinkonfiguration des IP-Stacks, z.B. zur Verhinderung zu großer Empfänglichkeit für Angriffsformen, bei denen Tabellen wie Neighbor Cache (Nachfolger der ARP-Tabelle) und Destination Cache (für First-Hop-Entscheidung) zugemüllt und so Einträge für Nutzkommunikation unmöglich gemacht werden sollen, werden mit der Zeit ähnlich wie unter IPv4 hoffentlich entstehen. Dies erfordert aber zunächst noch einige Einsatzpraxis mit IPv6 als Lernphase, damit Default-Einstellungen gefunden werden können, die nicht am Ende eher Gewolltes behindern als Angreifern das Leben schwermachen (mal wieder ein Thema auf Wiedervorlage, d.h. für kontinuierliche Beobachtung der Produktentwicklung bei Herstellern, deren Lösungen man einsetzt).

Die Karte „Firewall-Funktionalität" ist mit den hierzu bislang angestellten Betrachtungen aber noch nicht ausgereizt: Auch die Geräte-lokale Firewall (so vorhanden) lohnt einen genaueren Blick. Diese kann man bei erkanntem und entsprechend hohem (Rest-)Risiko bzgl. IPv6-basierter Angriffsversuche in mehrerlei Hinsicht als Konzeptelement prüfen:

- Schutz von (mobilen) Geräten, die in unsicheren Netzen verwendet werden sollen

  „Haken dran" – das ist der unter IPv4 etablierte Konzeptansatz, den man natürlich auch für IPv6 weiter verfolgen wird. Ehe man auf solchen Geräten IPv6 zur Nutzung einrichtet, wird man hoffentlich auch an diese Standard-Hausaufgabe denken.

- Schutz von Geräten vor Restrisiken durch Angriffe über ungewollte Mechanismen
  Lässt sich IPv6 für ein Gerät / ein eingesetztes Produkt nicht länger durch Härtungsmaßnahmen pauschal deaktivieren (z.B. wegen drohender Seiteneffekte und zu großen Aufwands entsprechender vorbereitender Tests), kann man versuchen, den Schutz vor unerwünschten Paketen, der oben zunächst bzgl. vorgelagerter Netzkomponenten betrachtet wurde, durch Einsatz der lokalen Firewall zu ergänzen.

  Einfaches Beispiel: Pauschal kann in einem Netzbereich stateful DHCPv6, also Adresszuteilung mittels DHCPv6, nicht ausgeschlossen, also auch nicht auf den Netzkomponenten unterdrückt bzw. durch vorgelagerte Firewalls pauschal abgeblockt werden. Ein solcher Netzbereich ist dann natürlich anfällig für Angriffe, die darauf basieren, dass einem Gerät zunächst vom Angreifer eine Adresse zugewiesen wird, die dieser dann kennt und somit sofort für die eigentlichen schädlichen Angriffsschritte verwenden kann. Soll ein konkret betrachtetes Gerät jedoch seine IPv6-Adresse(n) auf anderem Weg erhalten, so kann man mittels lokaler Firewall bei entsprechender Intelligenz die zu Stateful DHCPv6 gehörenden Nachrichtentypen gezielt sperren (hier ist hilfreich, dass bei stateful und stateless DHCPv6 unterschiedliche Nachrichtentypen verwendet werden).

  Ein pauschales Deaktivieren des DHCP-Clients für IPv6 lässt sich dagegen längst nicht für genauso viele Geräte als Maßnahme einsetzen – oft wird DHCPv6 zumindest in der stateless-Variante gebraucht werden, um andere Parameter als die IPv6-Adresse von zentraler Stelle zuzuteilen.

  Die Abbildung 10 zeigt, dass eine Verfügbarkeit lokaler IPv6-Firewallintelligenz kein reines Wunschdenken ist: die Windows-Firewall unter aktuellen Windows-Versionen kann da schon einiges, und dies bei Unterscheidung von ausgehenden und ankommenden Paketen. Die dargestellten Regeln sind dabei bereits vorbereitet – was man nicht braucht, kann auf dieser Basis bequem gesperrt werden (das Definieren weiterer Regeln auf ähnlichem Detaillierungsgrad als „benutzerdefinierte Regeln" ist auch möglich.

  Kennt man bei einem konkreten vernetzten Gerät (auch oder gerade: Server!) die zulässigen / gewollten Kommunikationspartner und ähnliche Einzelheiten, so kann man bei entsprechendem Schutzbedarf dieses Gerätes die lokale Firewall natürlich auch dazu verwenden, das Restrisiko durch Limitierung der Kommunikationsmöglichkeiten für dieses Gerät weiter zu senken. Werden IPv6-fähige lokale Firewalls zukünftig so pfiffig, dass gar verschiedene RA-Typen unterschieden werden können, bestünde hier eine weitere Option im Kampf gegen Innentäter, die es auf Neighbor-Discovery-Mechanismen als Angriffsvektor abgesehen haben.

  Wirklich revolutionär ist der Gedanke an die Geräte-lokale Firewall natürlich auch nicht. Unter IPv6 kann und sollte man sie aber neu bewerten, z.B. in Phasen, in denen etwa Möglichkeiten zum Schutz von Netzbereichen durch Firewalls, IDS/ IPS oder Switch-Funktionalitäten wie zuvor diskutierte vorübergehend noch zu wünschen übrig lassen. Man möchte ja mit dem realisierten Schutz nicht unter das bei IPv4 Erreichte zurückfallen, kann aber voraussichtlich selten konsequent abwarten, bis die Produktsituation bzgl. IPv6-Sicherheitsmaßnahmen zu IPv4 gleichwertig ist.

Fazit

Man sieht: Eine Einführung von IPv6 bringt sicherheitstechnisch eine Men-

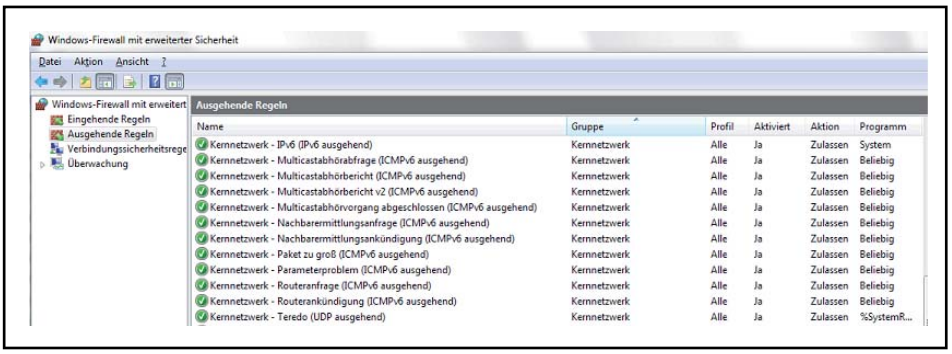


Abbildung 10: IPv6-Regeln der Windows 7-Firewall

ge Arbeit mit sich. Die Produktunterstützung bzgl. wünschenswerter Optionen für ein IPv6-Sicherheitskonzept lässt dabei vorübergehend noch zu wünschen übrig, man kann nicht mit einem pauschalen „best practice"-Ansatz forsch planen und dann erwarten, dass die in der eigenen Umgebung unter IPv4 bewährten Produktlinien das Nötige an Unterstützung selbstverständlich mitbringen. Vielmehr ist ein Lernprozess in mehreren Schritten notwendig – bei Herstellern und Sicherheitsspezialisten gleichermaßen. Wissen, Markt und damit auch das eigene IPv6-Sicherheitskonzept müssen in eine „best practice"-Situation erst noch hineinwachsen.

Eine Vogel-Strauß-Strategie hilft da allerdings nicht – so lange wird kaum jemand auf IPv6-Aktivierung völlig verzichten können und dies womöglich auch gar nicht wollen, um nicht auf neue, von Herstellern präferiert auf IPv6-Basis realisierte und betreute Lösungsangebote verzichten zu müssen.

Also:
Beobachten, Nachfragen/ Interesse bekunden und nötigenfalls im IPv6-Sicherheitskonzept neue Wege gehen, die unter IPv4-Security für einen betrachteten Fall nicht nötig gewesen wären. Möglichkeiten, über deren Sinn für die eigenen Zwecke man schon heute nachdenken und dann zugehörige Produktanforderungen als Basis einer kontinuierlichen Marktbeobachtung und Konzeptverbesserung daraus ableiten kann, hat der Artikel schon eine Reihe vorgeführt.

Der Weg zum „Sicherheitskonzept der Zukunft":

1. Frühzeitig Konzeptideen entwickeln und Produktanforderungen ableiten.
2. Markt beobachten / Lieferanten gezielt anfragen, Bedarf signalisieren und konkretisieren.
3. Bis zur Verfügbarkeit optimaler Präventionsmöglichkeiten gegen bekannte IPv6-Angriffe verstärkt auf „Detection" setzen und/ oder besonders kritische / gefährdete Geräte durch Beschränkung der IPv6-Kommunikationsbereitschaft schützen.

Die Rahmenbedingungen sind mühseliger als unter IPv4, aber eines sollte der Artikel auch gezeigt haben: wer sich bereits unter IPv4 mit Sicherheit beschäftigt hat, muss nicht völlig neu denken lernen – er muss Bekanntes auf die neue Technik übertragen und auch bereit sein, auf bekannte Fragen anders zu antworten als bisher. Ganz oben auf der Liste der Aktivitäten sind natürlich Sicherheitsmaßnahmen empfehlenswert, die sich sowohl gegen Angriffe auf IPv4 als auch auf IPv6 richten, indem einem Angreifer massive Steine in den Weg gelegt werden für den Versuch, eine Innentäterposition als Ausgangspunkt für den Einsatz von Angriffssoftware zu erlangen. Entsprechende Lösungen gibt es heute schon, eben mit Blick auf Absicherung von IPv4-Netzen, und man kann sofort starten bzw. sollte die Umsetzung entsprechender Planungen mit Blick auf IPv6 eher forcieren.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

IPv6: Planung, Migration und Betrieb, 10.09. - 12.09.12 in Berlin

Der Wechsel von IPv4 auf IPv6 wird für die meisten Unternehmen und Behörden in den nächsten Jahren unvermeidbar kommen. Dabei liefert IPv6 nicht nur ein neues Adress-Konzept sondern auch ein völlig verändertes Betriebs-Szenario. DHCP und auch DNS müssen neu durchdacht werden. Naturgemäß sind auch Firewall-Installationen und NAT von einer IPv6-Umstellung betroffen. Mit Windows 7 und Windows Server 2008 (R2) steht laut Microsoft umfassende IPv6-Unterstützung für die „Windows-Netzwerke“ zur Verfügung. Entsprechend überlegen viele, bei der Migration zu diesen Betriebssystem-Versionen gleich die Migration auf IPv6 mit zu vollziehen. Das kann ja nicht so schwer sein, einfach die IPv4- gegen IPv6-Adressen auszutauschen, und alles läuft!? Falsch! IPv6 ist ein Gesamtpaket, das sich deutlich von IPv4 unterscheidet. Dieses Paket muss verstanden werden. In diesem Seminar erfahren Sie, wo sich mit einer IPv6-Einführung etwas ändert, und wie Migrationsphase und Betriebsalltag aussehen.

Preis: € 1.890,-- netto

Intensiv-Tag VLAN-Planung: was ist das Optimum?, 17.09.12 in Bonn

Auf dieser eintägigen Veranstaltung wird Petra Borowka-Gatzweiler in die Thematik „VLANs: Alptraum oder unverzichtbares Betriebsinstrument?“ einführen und Standpunkt beziehen. Es wird im Anschluss ein Unternehmens-Szenario vorgestellt und vier bis fünf ausgewählte und eingeladene Hersteller stellen sich der Diskussion mit ihren Lösungsansätzen für das Szenario. Ziel ist, dabei auch die unterschiedlichen Sichtweisen der Hersteller zu diesem Thema transparent zu machen. Der Tag wird beendet mit einer offenen Diskussion des Themas.

Preis: € 990,-- netto

TCP/IP intensiv und kompakt, 17.09. - 21.09.12 in Düsseldorf

LAN-, WLAN- und WAN-Netzwerke sind heutzutage IP-Netze, und ein Verzicht auf Nutzung des IP-basierten Internet undenkbar. Auch für früher nur mit herstellerspezifischen Protokollen in Verbindung gebrachte Anwendungsgebiete wie Telefonie oder Produktionsumgebungen gibt es mittlerweile geeignete IP-basierte Lösungen. Hersteller und Dienstanbieter versuchen den Eindruck zu vermitteln, die Nutzung sei kinderleicht, fast schon plug and play - man trägt ein paar Adressen ein (wenn überhaupt), und es kann losgehen. Falsch!

Preis: € 2.490,-- netto

Netzzugangskontrolle: Technik, Planung und Betrieb, 17.09. - 19.09.12 in Düsseldorf

Dieses 3-tägige Seminar vermittelt den aktuellen Stand der Technik der Netzzugangskontrolle (Network Access Control, NAC) und zeigt die Möglichkeiten aber auch die Grenzen für den Aufbau einer professionellen NAC-Lösung auf. Schwerpunkt bildet die detaillierte Betrachtung der Standards IEEE 802.1X, EAP und RADIUS. Dabei wird mit IEEE 802.1X in der Fassung von 2010 und mit IEEE 802.1AE (MACsec) auch auf neueste Entwicklungen eingegangen.

Preis: € 1.890,-- netto

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 24.09. - 26.09.12 in Bonn

Dieses Seminar behandelt die Projektschritte, Einsatz- und Migrations-Szenarien, einsetzbare Basis-Technologien, Komponenten und erweiterte TK-Anwendungen, Bewertungskriterien für eine TK-Lösung und gibt eine Übersicht über den bestehenden TK-Markt etablierter Hersteller wie Alcatel-Lucent, Avaya, Cisco, Nortel und Siemens aber auch des Newcomers Microsoft.

Preis: € 1.890,-- netto

Virtualisierungstechnologien in der Analyse, 26.09. - 28.09.12 in Bonn

Dieses Seminar liefert einen umfassenden und zugleich detaillierten Einblick in die aktuellen Virtualisierungstechnologien der marktführenden Anbieter. Vom Server über das Netzwerk bis zum Speicher und schließlich auch zum Client werden die Möglichkeiten und Grenzen der Virtualisierungslösungen analysiert. Dabei bleiben auch Sicherheitsaspekte nicht unberücksichtigt. Basis hierfür bilden neben den technischen Grundlagen und Hintergründe die Erfahrungen aus dem Projektalltag sowie die Diskussion mit den Teilnehmern.

Preis: € 1.890,-- netto

Verkabelungssysteme für Lokale Netze, alles standardisiert, alles klar?, 01.10.12 in Düsseldorf

Dieses Seminar erklärt die Zusammenhänge der wichtigsten Standards und Normen, vergleicht diese mit dem aktuellen Stand der Technik und bewertet insbesondere die Praxistauglichkeit der im Normenumfeld getroffenen Empfehlungen. Neben einer Betrachtung des aktuellen Normungsstands aus der Sicht eines Normennutzers, der Bewertung von ausgewählten herstellerspezifischen Lösungen wird auch auf Planungs- und installationsbegleitende Maßnahmen eingegangen, die im Rahmen einer anstehenden Verkabelung zu beachten sind.

Preis: € 990,-- netto

RZ-RZ-Kopplung - alles nur eine Frage der Bandbreite?, 01.10.12 in Düsseldorf

Immer mehr Unternehmen sehen sich derzeit damit konfrontiert, ihre Rechenzentrumsdienstleistungen über entfernte Standorte redundant anzubieten. Neben den entsprechenden Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) für Desaster Recovery Konzepte fordert auch die Kundenseite entsprechende Service Level Agreements zur Hochverfügbarkeit ihrer Dienste und Daten ein. In diesem Seminar werden die aktuellen Techniken vorgestellt, technisch erläutert und für die richtige strategische Entscheidung zu einem Gesamtkonzept zusammengeführt.

Preis: € 990,-- netto

Anwendungs-Virtualisierung für Android, iPad & Co, 01.10.12 in Düsseldorf

Der Einsatz mobiler Endgeräte explodiert. Speziell Tablet-Computer und Smartphones werden innerhalb von Unternehmen immer stärker eingesetzt. Dabei geht es nicht nur um die Ablösung oder Ergänzung von Laptops, sondern auch um neue Anwendungsbereiche.

Preis: € 990,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
12.11. - 16.11.12 in Aachen
21.01. - 25.01.13 in Aachen
22.04. - 26.04.13 in Aachen
09.09. - 13.09.13 in Aachen
25.11. - 29.11.13 in Aachen

TCP/IP intensiv und kompakt
17.09. - 21.09.12 in Düsseldorf
18.02. - 22.02.13 in Stuttgart
13.05. - 17.05.13 in Bonn
07.10. - 11.10.13 in Stuttgart

Internetworking
22.10. - 26.10.12 in Aachen
11.03. - 15.03.13 in Aachen
17.06. - 21.06.13 in Aachen
14.10. - 18.10.13 in Aachen

Paketpreis für alle drei Seminare € 6.720,-- netto (Einzelpreise: je € 2.490,-- netto)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
23.10. - 26.10.12 in Aachen
05.02. - 08.02.13 in Aachen
11.06. - 14.06.13 in Aachen
24.09. - 27.09.13 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
04.12. - 07.12.12 in Aachen
12.03. - 15.03.13 in Aachen
09.07. - 12.07.13 in Aachen
05.11. - 08.11.13 in Aachen

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

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
24.09. - 26.09.12 in Bonn
26.11. - 28.11.12 in Bonn
25.02. - 27.02.13 in Köln
03.06. - 05.06.13 in Bonn
16.09. - 18.09.13 in Berlin
02.12. - 04.12.13 in Bonn

Session Initiation Protocol Basis-Technologie der IP-Telefonie
29.10. - 31.10.12 in Bonn
18.03. - 20.03.13 in Berlin
24.06. - 26.06.13 in Köln
07.10. - 09.10.13 in Stuttgart

Umfassende Absicherung von Voice over IP und Unified Communications
01.10. - 02.10.12 in Düsseldorf
11.04. - 12.04.13 in Bonn
18.07. - 19.07.13 in Bonn
04.11. - 05.11.13 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
29.10. - 30.10.12 in Bonn
18.02. - 19.02.13 in Stuttgart
13.05. - 14.05.13 in Bonn
30.09. - 01.10.13 in Düsseldorf

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 4.840,-- netto statt € 5.370,-- netto
Optionales Einsteigerseminar: Aufpreis € 1.190,-- netto statt € 1.590,-- netto

ComConsult Certified Service Catalogue Manager

Servicialisierung - Leitkonzept für verlässliche Service-Erbringung
01.10. - 02.10.12 in Düsseldorf

Service-Identifizierung - Von Service-Begriff bis Service-Konsumentennutzen
29.10. - 30.10.12 in Bonn

Service-Offerierung - Von Service-Spezifizierung bis Service-Katalogisierung
12.11. - 13.11.12 in Bonn

Paketpreis für alle drei Seminare € 4.290,-- netto (Einzelpreise: je € 1.590,-- netto)

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: insider@comconsult-akademie.de
http://www.comconsult-research.de

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

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