ComConsult Research

Der Netzwerk Insider

April 15

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Schluss mit dem Rangierchaos: Das intelligente Rangierfeld macht alles einfacher

von Dipl.-Ing. Harmut Kell

Wer kennt es nicht, die Verkabelung wurde fachgerecht installiert, alles perfekt dokumentiert und die Inbetriebnahme der einzelnen Teilstrecken stehen an.

Am Anfang ist noch alles sehr übersichtlich, ein Aufschalten der Strecken geht leicht von der Hand, Erfolgserlebnisse sind schnell zu bekommen. Da verzichtet man, insbesondere aufgrund des Zeitdrucks, der bei einer Inbetriebnahme herrscht, gerne auf die Dokumentation der Rangierungen, wohlwissend, dass man ohnehin niemals wieder Zeit dafür finden wird. Doch dann kommt der Tag X: Im laufenden Betrieb müssen Änderungen an den Rangierungen durchgeführt werden, da größere Umzüge von Abteilungen oder Projektteams anstehen. Oder es ist die Suche nach einem Fehler notwendig, die ein Nutzer eines Endgerätes – oder noch schlimmer – eines Servers meldet. Spätestens in diesem Moment wird sich herausstellen, ob der Verzicht auf eine Rangierdokumentation nicht bereut wird. Im vorliegenden Artikel wird dargestellt, worauf es bei einer Dokumentation der Rangierung ankommt und wie aktuelle Techniken durch automatische Erfassung von Rangierungen das Leben einfacher machen können.

weiter auf Seite 7

Zweitthema

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle – Zusammenhänge, Perspektiven, Marktrelevanz - Teil 2

von Dipl.-Inform. Petra Borowka-Gatzweiler

1.4 OpenDaylight Projekt

Nicht zuletzt aus Unzufriedenheit mit der ONF hinsichtlich der dauerhaft verschleppten Spezifikation des Northbound Interface, aber auch mit der Motivation, eine vollständige Architektur zu spezifizieren und pragmatisch als OpenSource zu implementieren, wurde im April 2013 das OpenDaylight Consortium gegründet. Im September 2014 hatten sich 41 Mitglieder dem Consortium angeschlossen, im Februar 2014 wurde mit "Hydrogen" das erste Release, im Oktober 2014 das zweite Release "Helium" verabschiedet. (siehe Abbildungen 1.8 und 1.9)

Während sich ONF nicht wirklich entscheiden konnte, hat OpenDaylight sich für ein marktfreundliches REST API als Northbound Schnittstelle entschieden. Die Southbound Schnittstelle ist ziemlich agnostisch, hier sind verschiedenste Protokolle zugelassen, in Helium nochmals mehr als in Hydrogen. Funktionserweiterungen von Helium enthalten unter anderem Service Chaining (wird im Kapitel NFV behandelt), Föderation von SDN Controllern (East-Westbound Interface), zusätzliche Netzwerk-Virtualisierungs-Optionen und mehr Layer-4 bis Layer-7 Funktionalität.

weiter auf Seite 21

Geleit

Individuelle maßgeschneiderte Infrastrukturen für Unternehmen: der Planungs-Alptraum, aber können wir ihn verhindern?

auf Seite 2

Aktueller Kongress

ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

ab Seite 4

Standpunkt

Nachhaltige Informationssicherheit: Ohne Druck geht es nicht

auf Seite 18

Neue Sonderveranstaltungen

Das PSTN stirbt: Die neue Kommunikation mit SIP/IP Das neue IT-Sicherheitsgesetz

ab Seite 19

Zum Geleit

Individuelle maßgeschneiderte Infrastrukturen für Unternehmen: der Planungs-Alptraum, aber können wir ihn verhindern?

Wir erleben seit einigen Monaten einen weitgehenden Wandel in den IT-Architekturen mit erheblichen Auswirkungen auf unsere IT-Infrastrukturen. Und wir müssen feststellen, dass alte Design-Ansätze und Regeln auf einmal nicht mehr gültig sind.

Wie können wir damit umgehen und welche Ansätze gibt es, diesem Wandel sowohl in der Planung von Infrastrukturen als auch im Betrieb gerecht zu werden? Wie individuell müssen Planungen wirklich sein und welche Auswirkungen hat das auf den Betrieb?

Lassen Sie mich zuerst einige Beispiele geben, die den Wandel unterstreichen:

- bis vor Kurzem war die Welt der Server und Speicher-Architekturen zumindest zu 90% einfach in Worte zu fassen. Anwendungen mit hoher CPU- und I/O-Last und einem gleichzeitig hohen Grad an parallelen Benutzern werden am besten mit integrierten Lösungen mit Speicher und Server in einem Schrank bedient. Typische Lösungen kommen u.a. von Oracle und IBM. Alle anderen Anwendungen werden auf virtualisierten Servern mit Ost-West Architekturen zum Zugriff auf einen zentralen Speicher umgesetzt. Zentrale Speichersysteme mit 10 Gigabit Ethernet Anschluss in Kombination mit Low-Latency-Netzwerken führten dazu, dass ein Performance-Unterschied zu einer direkt im Server installierten Festplatte (Direct Attached Storage DAS) kaum feststellbar war. Nun haben PCIe-basierte SSDs zu einer deutlichen Verschiebung geführt. Mit Durchsatzwerten von 10 bis 15 Gigabit/s erreichen sie Leistungen, die über den Ost-West-Verkehr zu einem zentralen Speichersystem nicht mehr ohne erheblichen finanziellen und technischen Aufwand umgesetzt werden können. Also erleben wir eine Wiederbelebung von DAS für einen bestimmten Typ von Anwendungen. Das hat sofortige Auswirkungen auf Virtualisierung und das Wandern von Applikationen zwischen Servern sowohl in der Wahl der überhaupt in Frage kommenden Server als auch im Umfang der zu bewegenden Daten. Gleichzeitig erleben wir eine deutliche Verschiebung im Bereich

von In-Memory Computing. Bisher waren derartige Lösungen mehr in integrierten Schränken anzufinden und typischerweise große Lösungen. Einer der wesentlichen Gründe dafür war das spezielle Datenmodell, das erforderlich war und das erhebliche Anpassungsarbeiten erforderte, um eine bestehende “alte” Anwendung auf In-Memory umzustellen. Dementsprechend hat man diesen Aufwand auch nur für wenige und strategische Anwendungen ins Auge gefasst. Die neue Version von Oracle, die seit dem dritten Quartal 2014 auf dem Markt ist, hat den Umfang der Anpassungsarbeiten in sich zusammen fallen lassen. Damit ist die Tür auf für die Nutzung von In-Memory auch in kleineren und weniger strategischen Anwendungen, die in der Regel den preislichen Mehraufwand einer integrierten Schrank-Lösung nicht rechtfertigen. Hier könnten weitere Beispiele stehen, die aber alle in der gleichen Erkenntnis enden: die Zeiten der wenigen und klar angreifbaren Server-Architekturen ist vorbei. Kombiniert man das mit Anforderungen wie der schnellen Bereitstellung von Anwendungen, dann ist man schnell bei sehr individuellen Lösungen.

- wie viel Gigabit Ethernet sollen es denn nun sein? Die Auswahl der bald verfügbaren Datenraten erweitert sich fast täglich. Und natürlich gibt es irgendwie einen guten Grund für fast jede dieser Datenraten und die Nutzung von Twisted Pair ist eng damit verbunden. Aber für wen ist welche Datenrate die beste? Lässt sich das überhaupt noch sagen? Und wir können nicht pauschal auf modularer Switch-Systeme als Lösung zurück fallen, die Mehrkosten sind einfach zu hoch.

- WLANs können Gigabit. Wirklich? In der Praxis ist das verbunden mit sehr kleinen Zellen, wir sprechen von Mikrozellen-Design. Große Zellen enden da wo sie herkommen, eben nicht bei Gigabit. So weit so gut. Aber viele kleine Zel-

Individuelle maßgeschneiderte Infrastrukturen für Unternehmen

len sind zum Beispiel für ein Hotel, ein Krankenhaus oder allgemein eine Umgebung mit vielen sich bewegenden mobilen Endgeräten eine Herausforderung. Endgeräte neigen dazu, so lange wie möglich an ihrem Access Point zu kleben. Damit sind sie fast immer am "falschen" Access Point. Das Mega-Desaster für den Planer und den Betreiber.

- die Cloud mag ja für viele Unternehmen in Deutschland weiterhin ein rotes Tuch sein. Aber es gibt auch Unternehmen, die die Vorteile der Cloud nutzen wollen. Dabei sind wiederum die Zeiten der isolierten Lösungen in der Cloud vorbei, wenn es sie denn jemals gab. Cloud-Lösungen müssen in vorhandene Prozesse und Infrastrukturen integriert werden. Das kann eine einfache lokale Python- oder zentrale Javascript-Anwendung mit Zugriff auf die APIs des Cloud Dienstes sein, es kann aber auch der Aufbau einer in sich mobilen Anwendungsarchitektur mit Network Function Virtualisation und der intensiven Nutzung von Software-Netzwerk- und Sicherheits-Komponenten sein. Gerade dieser Typ von Anwendungen ist extrem individuell und Lösungen lassen sich kaum verallgemeinern.

Was zeigen diese Beispiele ohne sie weiter vertiefen oder ausweiten zu wollen? In meinen Augen müssen wir uns mit zwei wesentlichen Entwicklungen auseinander setzen:

1. Die "one size fits all" Planung für IT-Infrastrukturen ist nun endgültig vorbei. Ein Hotel ist nun mal kein isolierter 50 qm Besprechungsraum in einem Unternehmen. Eine über Parallelität skalierende Webanwendung ist kein Email-Server. Unternehmen haben immer mehr individuelle Anforderungen, die in maßgeschneiderten Lösungen umgesetzt werden müssen. Dazu müssen die verfügbaren Bausteine bekannt sein und sie müssen geeignet kombiniert werden.

2. Wir sprechen ja schon lange davon, aber die Beispiele machen deutlich, dass die Zeit des Silo-Denkens nun endlich ein Ende haben muss. Ohne ein intensives Verständnis der Gesamtsituation lassen sich diese sehr individuellen Anforderungen nicht umsetzen. Wir brauchen einen Typ von Planer und Betreiber, der über Technologie-Grenzen hinaus arbeiten kann und die jeweils beste Lösungs-Architektur für ein Unternehmen entwickeln kann.

Was können wir tun, um Ihnen zu helfen? Ich möchte auf zwei herausragende Veranstaltungen hinweisen, die sich dieser Entwicklung widmen:

- Das ComConsult Netzwerk- und IT-Infrastrukturforum 2015 im April widmet sich der Frage der verfügbaren Infrastruktur-Bausteine auf der Netzwerkseite. Von der Basistechnik bis hin zur Sicherheit.

- Die ComConsult Technologie-Tage 2015 im November widmen sich der Planung und dem Betrieb von IT-Architekturen über Technologie-Grenzen hinweg. Hier geht es um das "Big Picture" speziell auch für Entscheider, um genau das Zusammenspiel der einzelnen Technologie-Bausteine im Rahmen der aktuellen Entwicklungen zu vermitteln.

Es wird eben nie langweilig in unserem Job.

In diesem Sinne und in der Hoffnung Sie als Teilnehmer lebhafter Diskussionen auf einem der beiden Kongresse persönlich begrüßen zu können

Ihr
Dr. Jürgen Suppan

Kongress

ComConsult Netzwerk- und IT-Infrastruktur Forum 2015
20.04. - 22.04.15 in Königswinter

Das ComConsult Netzwerk-Forum 2015 stellt die drei momentan dominantesten Netzwerk-Themen in den Mittelpunkt der Veranstaltung:

- Netzwerke im Rechenzentrum
- Netzwerk-Design
- Betriebsoptimierung

Der Netzwerk-Markt ist in Bewegung wie diese Beispiele zeigen. Das ComConsult Netzwerk- und IT-Infrastruktur-Forum 2015 ist das richtige Forum zur richtigen Zeit. Wir analysieren exklusiv für Sie:

- was passiert im Rechenzentrum und wie können Sie Ihr Netzwerk darauf optimal vorbereiten
- wie verändert sich Netzwerk-Design und wie können Sie die Vorteile zu Ihren Gunsten nutzen ohne das gesamte Netzwerk ablösen zu müssen
- wie können Sie die Komplexität des Netzwerkes im Betrieb reduzieren und dabei gleichzeitig besser werden

Wie in jedem Jahr hat auch dieses Forum einen Vertiefungstag, an dem wir ein ausgewähltes Thema ausgiebig analysieren und mit Ihnen diskutieren. Dieser Tag ist optional buchbar, aber wir empfehlen ihn allen Teilnehmern.

Unser Vertiefungstag in diesem Jahr dreht sich komplett um IPv6 und die aktuellen Projekterfahrungen in diesem Bereich.

Moderation: Dr. Jürgen Suppan
Preis: € 2.390,-- netto

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

Aktueller Kongress

ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

20.04. - 22.04.15 in Königswinter

Das ComConsult Netzwerk-Forum 2015 stellt die drei momentan dominantesten Netzwerk-Themen in den Mittelpunkt der Veranstaltung:

Netzwerke im Rechenzentrum
- mehr Flexibilität für ein immer größeres Spektrum an IT-Architekturen
- mehr Service-Orientierung (selbstlernend und automatisch konfigurierend?)
- neue Produkte und Technologien

Netzwerk-Design
- kommt eine neue Form von Netzwerk?
- neue Bandbreiten
- dynamisch und über Standort-Grenzen hinweg skalierende Netzwerk-Architekturen
- IPv6

Betriebsoptimierung
- mehr Kontrolle
- weniger Komplexität
- schnellere Reaktion

Dabei beobachten wir in allen drei Bereichen momentan herausragende Entwicklungen, die sowohl die Leistung als auch die Wirtschaftlichkeit von Netzwerken in den nächsten Jahren stark beeinflussen werden. Drei Beispiele aus dem Programm des Forums sollen das verdeutlichen.

Im Rechenzentrum führen die Anforderungen von Virtualisierung, dem Aufbau von Private Clouds und der performanten Integration von Speicher-Systemen dazu, dass wir unsere bisherigen Architekturen mehr und mehr in Frage stellen. Stattdessen drängen neue Themen in die Diskussion:

- die Rolle von Software-Switches in den Architekturen und als Teil von Lösungen wie VMware NSX
- die Rolle von virtuellen Appliances, um ganze Anwendungsbereiche über mehrere Server hinweg mobil zu gestalten und zwischen Standorten verlagern zu können (wesentlicher Teil für Notfall-Szenarien, das ging so bisher nicht)
- SDN gewinnt in diesem Umfeld rapide an Bedeutung, zwar nicht wie ursprünglich als Technologie vorgestellt, sondern mehr als Speziallösung zur Steuerung von Software-Switches und virtuellen Appliances, aber dafür hat es in diesem Bereich den Status einer unreifen Technologie längst verlassen

Im Bereich Netzwerk Design dominiert die Kombination aus einer besseren Anpassung von Netzwerken an den Bedarf und nach flexibleren Lösungen. So sehen wir:

- neue Ethernet-Bandbreiten, die auf den ersten Blick überraschen, aber bei näherer Analyse sehr viel Sinn machen
- neue Design-Konzepte zur Verbesserung von Skalierung und Provisionierung, zum Beispiel als Edge/Core-Design
- die erste große Welle der IPv6-Projekte

Im Bereich Betrieb geht es sehr viel um die Optimierung bekannter Technologien und die dynamische Anpassung an einen sich permanent verändernden Bedarf:

- im Bereich WLAN haben wir zwar mit 802.11ac eine neue Technologie und müssen Planung und Design daran anpassen. Aber die eigentlichen Anforderungen liegen in vielen Projekten mehr und mehr im Betrieb. Und Bandbreiten-Management in Kombination mit Sicherheits-Aspekten und einer Integration in ein sehr leistungsfähiges Monitoring sind hier die Schlüssel-Funktionen
- wir haben im Betrieb ein zunehmendes Problem mit der Komplexität des Netzwerk-Aufbaus und der daraus resultierenden Destabilisierung des Netzwerks an sich. Eine der wesentlichen Ursachen für die Destabilisierung liegt in der Explosion der Anzahl von MiddleBoxes im Netzwerk (Firewalls, IDS, Load Balancer, …). Wir beobachten eine zunehmende Zahl von Netzwerken, die im Core mehr MiddleBox-Systeme als Switches haben
- das Thema Sicherheit nimmt noch weiter an Bedeutung zu. In den Projekten ist es in vielen Fällen inzwischen das Thema Nummer 1 für die Gestaltung des Betriebs. Das Problem liegt hier nicht in der Auswahl einer Lösung, sondern in der Gestaltung der Lösung in einer Form, dass sie mit überschaubarem Aufwand betrieben werden kann.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

Ich buche den Kongress
ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

☐ vom 20.04. - 22.04.15 in Königswinter zum Preis € 2.390,-- netto

☐ vom 20.04. - 21.04.15 in Königswinter zum Preis € 1.990,-- netto

☐ am 22.04.15 in Königswinter zum Preis € 990,-- netto

Zum Kongressportal
www.comconsult-research.de

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Programmübersicht ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

Montag, 20.04.2015

9:30 - 10:15 Uhr
Keynote: Netzwerk- und IT-Infrastruktur-Trends 2015: wohin geht der Weg?
- Bedarfsanalyse
- Die Top 5 Zukunfts-Technologien in der Bewertung von ComConsult Research
- Investitions-Alternativen im Vergleich

Dr. Jürgen Suppan, ComConsult Research Ltd.

Netzwerke und Infrastrukturen im Rechenzentrum

10:15 - 11:00 Uhr
Das tatsächliche Potential von SDN
- Wo steht SDN heute?
- SDN ist nicht gleich SDN - eine Klarstellung
- Was macht SDN denn so attraktiv?
- Anwendungsbeispiele mit SDN, die traditionell nicht oder nur mit hohem Aufwand umsetzbar sind
- Empfehlungen

Dipl.-Ing. Markus Nispel, Extreme Networks GmbH

11:00 - 11:30 Uhr Kaffeepause in der Ausstellung

11:30 - 12:15 Uhr
Neue Lösungsansätze für RZ-Netze
- Unterschiede zu klassischen Netzwerktechnologien
- Was ist der Kern von SDN?
- OpenFlow-SDN vs. Netzwerkvirtualisierung
- NV und SDN als Bausteine für das Software-Defined Datacenter von VMware (NSX)
- Wo bleiben die Anwendungen: Cisco ACI und QoS im Rechenzentrum

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

12:15 - 13:00 Uhr
Private Clouds und die Auswirkung auf IT-Infrastrukturen
- Was eine Private Cloud als solche qualifiziert
- Software-Defined Data Center: Voraussetzung für die Cloud
- Virtualisierte Server als Kernbestandteil
- Elemente einer modernen Speicherstrategie
- Das passende RZ-Zonenkonzept zur Cloud
- Organisatorische Herausforderungen

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

13:00 - 14:15 Uhr Mittagspause

14:15 - 15:00 Uhr
Application Centric Infrastructure: Die Basis für eine Policy-Definierte RZ, LAN und WAN-Infrastruktur
- ACI als Basis für die Policy-Definierte RZ-Infrastruktur (Bausteine der ACI-Architektur, Grundlage für Automation im RZ, Policy-Modell: wie Anwendungen abgesichert werden können)
- Wie APIC-EM den LAN- und WAN-Betriebsprozess optimiert (Vorteile der Controller gemanagten Infrastruktur, Abstraktion als Basis für Automatisierung, QoS, ACL, Richtlinien auf der Basis abstrahierter Topologie, die Rolle des Controllers)

Dipl.-Inform. Matthias Wessendorf, Markus Harbeck, Cisco Systems GmbH

Netzwerk-Planung und Design

15:00 - 15:45 Uhr
Neue Datenraten für Ethernet
- 2,5GbE und 5GbE zur Unterstützung flächendeckender WLAN-Inrastrukturen
- 25GbE und 50GbE als skalierbare Alternative zum unseligen 40GbE
- Die neue Generation der 25/50/100G Switch ASICS wie Broadcom Tomahawk
- 40G am Scheideweg: kommt 40 GBASE-T oder doch nicht?

Dr. Franz-Joachim Kauffels, unabhängiger Unternehmensberater

15:45 - 16:15 Uhr Kaffeepause in der Ausstellung

16:15 - 17:00 Uhr
IPv6: Wo wir stehen, was wir noch brauchen
- Aktueller Stand bei Unternehmen, Providern und Herstellern
- Mit welchen Schwierigkeiten müssen Unternehmen rechnen?
- Welche ungeklärten Problemfelder müssen noch angegangen werden?

Markus Schaub, ComConsult-Study.tv

17:00 - 17:45 Uhr
The New IP – welche Rolle wird NFV in heutigen Netzen spielen?
- Warum Software und wie sehen typische Lösungen aus?
- Vergleich mit Hardware-Lösungen: Vor- und Nachteile
- Kosten-Vergleich: wie viel Geld lässt sich sparen
- Einsatz-Szenerien und Empfehlungen

Christopher Feussner, Brocade Communications GmbH

ab 18:00 Uhr Happy Hour

Dienstag, 21.04.2015

9:00 - 9:45 Uhr
Neue Designkonzepte im Vergleich: Verbesserung von Skalierung und Provisionierung
- Trennung in Edge und Core / Backbone
- Erhöhte Skalierbarkeit
- Verbesserte Provisionierung (Virtualisierung, Quality of Service, Zugangskontrolle/NAC, Mobilität)
- Anforderungen für den Edge: RZ, Access
- Anforderungen für den Core: RZ, Campus
- Technologien: Tunnelverfahren und Markierung
- Migrations-Aufwand
- Multivendor-Unterstützung
- Einheitlichkeit für Campus, RZ und Access

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

Betrieb, Verfügbarkeit und Wirtschaftlichkeit von Netzwerken

9:45 - 10:30 Uhr
WLAN-Netzwerke mit 802.11ac: Methoden zur Bandbreiten-Optimierung und zuverlässigen Versorgung mobiler Teilnehmer
- Analyse: wie viel Bandbreite hat 11ac wirklich und wo liegen Probleme
- Warum Bandbreiten-Management erforderlich ist
- Einfache Prioritäten-Schemata versagen, wie kann eine intelligente und adaptive Lösung genau auf den Bedarf zugeschnitten werden
- Wahl eines optimierten 802.11 ac Channel Design
- Intelligente Steuerung der Clients um optimale Bandbreite für die gesamte WLAN Infrastruktur zu gewährleisten.

Reinhard Lichte, Aruba Networks GmbH

10:30 - 11:00 Uhr Kaffeepause in der Ausstellung

Programmübersicht ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

Dienstag, 21.04.2015

11:00 - 11:45 Uhr
Quality of Service im WLAN: Grenzen und Möglichkeiten der Technologie
- QoS auf der Luftschnittstelle: IEEE 802.11e und WiFi Multimedia (WMM)
- Übertragungs-Kapazität, der Schlüssel für hohe Dienstegüte: Wie plant man leistungsfähige WLAN?
- Multi-User MIMO wird verfügbar, nützt es der QoS?
- QoS zum „Nulltarif", wie funktionieren Anwendungs-sensitive WLANs?
- Software Defined Networking (SDN), ein alternativer Ansatz zur Umsetzung von QoS

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:45 - 12:30 Uhr
Problematik und Zukunft von Middleboxes
- Firewalls, IPS, Proxies, Load Balancer, WAN-Optimierer & Co.: warum sie immer mehr Aufwand verursachen
- Ist SDN die Zukunft für Middleboxes?
- Bestehende vielversprechende Ansätze

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

12:30 - 14:00 Uhr Mittagspause

14:00 - 14:45 Uhr
Neue Herausforderungen für die Netzwerksicherheit
- Abwehr von Lauschangriffen und Advanced Persistent Threats: Anforderungen an die Netzwerk-sicherheit und resultierende Sicherheitsarchitekturen
- Netzzugangskontrolle, Verschlüsselung auf Ebene des Netzwerks, Zonenkonzepte: Aufwand vs. Sicherheitsgewinn
- Virtualisierung und Vertikal integrierte Systeme: Evolution zu Plattform-integrierten Sicherheitskomponenten
- SDN, ACI und Co.: Notwendigkeit Anwendungs-zentrierter Sicherheitskonzepte im modernen RZ

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

14:45 - 15:30 Uhr
Vom klassischen Infrastruktur Monitoring zum Ende zu Ende Business Applikations Monitoring
- Proaktive Überwachung und Root-Cause Analyse von Applikationsproblemen
- Überwachung der Business Transaktionen auf dem Weg durch die IT Infrastruktur
- Business Impact Analyse
- End Benutzer Monitoring
- Applikations und Datenbank Decodierung (L2-L7 Decodierung)
- Automatische Erkennung von Anomalien

Peter Rehle, ICS GmbH

15:30 - 16:15 Uhr
Technologien, die die nächsten Jahre beeinflussen werden und unsere Netzwerke und Infrastrukturen verändern werden
- Die Top-Technologien der nächsten Jahre
- Auswirkung auf Infrastrukturen
- Empfehlungen für die Vorbereitung, Planung und Investition sowie die zukünftige Nutzung

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

16:15 Uhr Abschließende Kaffeepause

Mittwoch, 22.04.2015

IPv6 Migration: Projekterfahrungen und -empfehlungen
- Organisation eines IPv6 Rollouts (Planung des Vorgehens, was muss wann entschieden werden, welche Abteilungen sind in welcher Projektphase gefordert, wo existiert Schulungsbedarf)
- Adresskonzept (Welche Alternativen stehen zur Verfügung, was sind die Vor- und Nachteile)
- Zuweisung von IPv6 Adressen (Welche Verfahren stehen zur Verfügung, wie integriert man Komponenten, die kein DHCPv6 unterstützen)
- Anforderungen an Netzwerk- und Infrastrukturkomponenten (Erstellung von Anforderungsprofilen für einzelne Komponenten, Testdurchführung, ausgewählte Testergebnisse)
- LAN-Archtitektur (Redundanzverfahren: VRRP, HSRP, Routing von IPv6, Umgang mit QoS bei IPv6)
- Migration der Internetpräsenz
- Migration von Anwendungen und Appliances
- Erstellung eines Anforderungskataloges für die Anschaffung von Hard- und Software
- Externe Anbindungen (WAN, Internet, Internet-VPN, Externe Partnerunternehmen)
- Security (Ergebnisse von Proxy-Tests, Firewalls & IDS, First-Hop-Security)

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH
Markus Schaub, ComConsult Study.tv

10:30 - 11:00 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 Uhr Ende der Veranstaltung

Folgende Aussteller nehmen an der Veranstaltung teil

AixpertSoft, Alcatel·Lucent, aruba networks, AVAYA The Power of We, BROCADE, CISCO, ComConsult Beratung + Planung, ComConsult Research, ComConsult Study.tv, controlware communicationssysteme, Extreme networks, FLUKE networks, hp, ics, MICROSENS, NETWORK INSTRUMENTS, psiber, semonit service monitoring IT, TELONIC, WÜRTHPHOENIX

Schwerpunktthema

Schluss mit dem Rangierchaos: Das intelligente Rangierfeld macht alles einfacher

Fortsetzung von Seite 1

Dipl.-Ing. Hartmut Kell kann bis heute auf eine mehr als 20-jährige Berufserfahrung in dem Bereich der Datenkommunikation bei lokalen Netzen verweisen. Als Leiter des Competence Center IT-Infrastrukturen der ComConsult Beratung und Planung GmbH hat er umfangreiche Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken gesammelt und vermittelt sein Fachwissen in Form von Publikationen und Seminaren.

Ausgangsbasis

Wie dargestellt, stellt die Ausgangsbasis ein durch das Installationsunternehmen fachgerecht installierter und dokumentierter physikalischer passiver Link im Sinne eines sogenannten Permanent Link dar, also eine Strecke zunächst ohne Anschluss- oder Rangierschnüre. In diesem Falle darf man erwarten, dass beide Enden des Links dokumentiert und vor allem beschriftet sind. Ein Ende stellt in der Regel immer ein Rangierfeld dar und das andere Ende entweder wieder ein Rangierfeld oder eine Anschlussdose. Den im industriellen Umfeld durchaus nicht ungewöhnlichen Fall eines Permanten Links ohne Abschluss in einem Rangierfeld oder einer Dose betrachten wir hier nicht. Die Beschriftung bzw. der dazugehörende Code am Rangierfeld oder Dose wird in der Regel bei den deutlich meisten Dokumentationen – falls sie gemacht wird - in irgendeiner Art in die Rangierdokumentation einfließen. Die Aufgabe der Rangierdokumentation ist es, einen Bezug zwischen dem Port des Rangierfeldes (bzw. der Dose) und dem aktiven Gerät, also z.B. dem Switch (bzw. dem PC oder auch Server) herzustellen. Dazu gibt es mehrere Möglichkeiten, auf die nachfolgend eingegangen werden soll.

Sinn und der Zweck einer Rangierdokumentation

Es darf nicht überraschen, dass es in einer nicht geringen Anzahl von Netzwerkumgebungen gar keine Rangierdokumentation gibt, dies gilt gerade für den Bereich der Endgeräteverkabelung (typischerweise Etagenverteiler mit Twisted Pair als Horizontalkabel). Auch in dem einen oder anderen Rechenzentrum wird gerne darauf verzichtet. Dagegen werden Backbone-Verbindungen - in der Regel Glasfaserstrecken - meistens dokumentiert, denn ein Ausfall einer solchen Strecke bei fehlender Dokumentation benötigt weitere zusätzliche Zeit bis zur eigentlichen Fehlerbehebung und verlängert damit die Mean Time to Repair und bei Backbone-Verbindungen betrifft das häufig größere Teile des Netzwerkes. Es geht tatsächlich in vielen Fällen auch ohne durchgängige Dokumentation, wie gut auch immer.

Mit der Dokumentation sollen insbesondere folgende Dinge vereinfacht werden:

- Bei einer Änderung der Aufschaltungen soll verhindert werden, dass irrtümlich eine falsche Aufschaltung zu einer Unterbrechung eines aktiven Links führt oder die Aufschaltung nicht zum Ziel führte und es zu Verzögerungen kommt, bis der Link aktiv wird.

- Bei einem gemeldeten Fehler auf einem aktiven Link soll nachvollzogen werden können, welche physikalischen Teile des Links, insbesondere welche Verkabelungselemente dazu gehören und weiter zu analysieren sind.

- Zusätzlich gehört natürlich im Rahmen von Change Management-Prozessen auch die Dokumentation der Anweisung an einen Techniker, wie er eine Änderung der Rangierung durchzuführen hat.

Ideal wäre es, eine End-to-End-Dokumentation vorzunehmen, die beide am aktiven Link „beteiligten“ aktiven Geräte berücksichtigt. Da der Verteiler in der Regel der Ausgangspunkt der Änderungen oder auch der Fehlersuche ist, steht dieser in den meisten Fällen im Vordergrund. Für die oben aufgeführten Fälle müssen mindestens bekannt sein:

- Name der aktiven Komponente (häufig auch als Objekt-ID bezeichnet)

- Ebenfalls Name und Einbauort des Rangierfeldes (ebenfalls Objekt-ID)

- Slot- und Port-Nummer auf beiden Komponenten

Diskutiert werden kann, ob folgende Infos ebenfalls zur Input-Dokumentation gehören müssen/sollen:

- Objekt-ID der Rangier- oder Anschlussschnur (siehe Textblock auf Seite 25)

- Übertragungstechnische Qualität der Strecke (sogenannte Channel Link Performance)

- Angaben zum „anderen“ Ende der Strecke; bei der Tertiärverkabelung wäre das z.B. der Raum der Dose oder ein Koordinatenpunkt in einem Grundriss (z.B. bei einer Dose für einen WLAN-Anschluss)

Aus der Dokumentation müssen im Idealfall über jedes bekannte Detail alle Elemente des aktiven (oder auch passiven) Links ermittelt werden können. Vereinfachend folgende Beispiele:

Beispiel Tertiärbereich: Meldet ein Nutzer mit einem kabelgebundenen Anschluss eine völlige Unterbrechung seiner

Schluss mit dem Rangierchaos: Das intelligente Rangierfeld macht alles einfacher

Netzwerk-Verbindung muss im einfachsten Falle über die Dosen/Portnummer des Anschlusses ermittelt werden können, auf welchem Switch-Port das Endgerät angeschlossen worden ist. Bei den meisten Beschriftungsrichtlinien weist die Dosen/Port-Nummer aus, in welchem Technikraum, welchem Schrank und auf welchem Rangierfeldport das Endgerät angeschlossen ist. Bis hier ist eine Rangierdokumentation noch nicht zwingend notwendig, sie vereinfacht aber die Suche bereits. Spätestens bei der Frage, auf welchen Switch-Port denn der Anschluss aufgeschaltet ist, braucht man entweder eine Dokumentation oder man muss sehr mühsam mit Hilfe von „Kabelabtasten“ die Zuordnung ermitteln.

Abbildung 1: Beschriftung mit direkter Ablesbarkeit des Ziels

Beispiel Rechenzentrum: Ein Server in einem Server-Schrank in der Mitte einer Schrankreihe wurde mit Hilfe einer Glasfaserverbindung über das Rangierfeld im Server-Schrank und dann wieder über den Kopfschrank der Reihe zu einem weiteren Netzwerk-Schrank irgendwo im Raum durchgeschaltet (siehe Abbildung 2); der Server soll in Zukunft nicht mehr benutzt werden. Diese Verbindung ist aufgrund des bereits vollständig belegten Rangierfeldes vollständig aufzulösen. Ohne eine Dokumentation der Rangierungen kann es zu einem sehr gewagten Unternehmen werden, die Rangierungen einfach zu entfernen. Selbst ein Abtasten der Rangierkabel ist mit Risiko verbunden, da Fehler auch hier nicht ausgeschlossen werden können.

Traditionelle Rangierdokumentation

Bei einer „traditionellen“ Methode erfolgt die Erfassung des rangierten Links auf Basis von einfachen Tabellen, oder bei einer „eleganteren“ Lösung auf Basis eines speziellen Dokumentations- oder Datenbanksystems. In beiden Fällen erfolgen die Erfassung der Informationen und

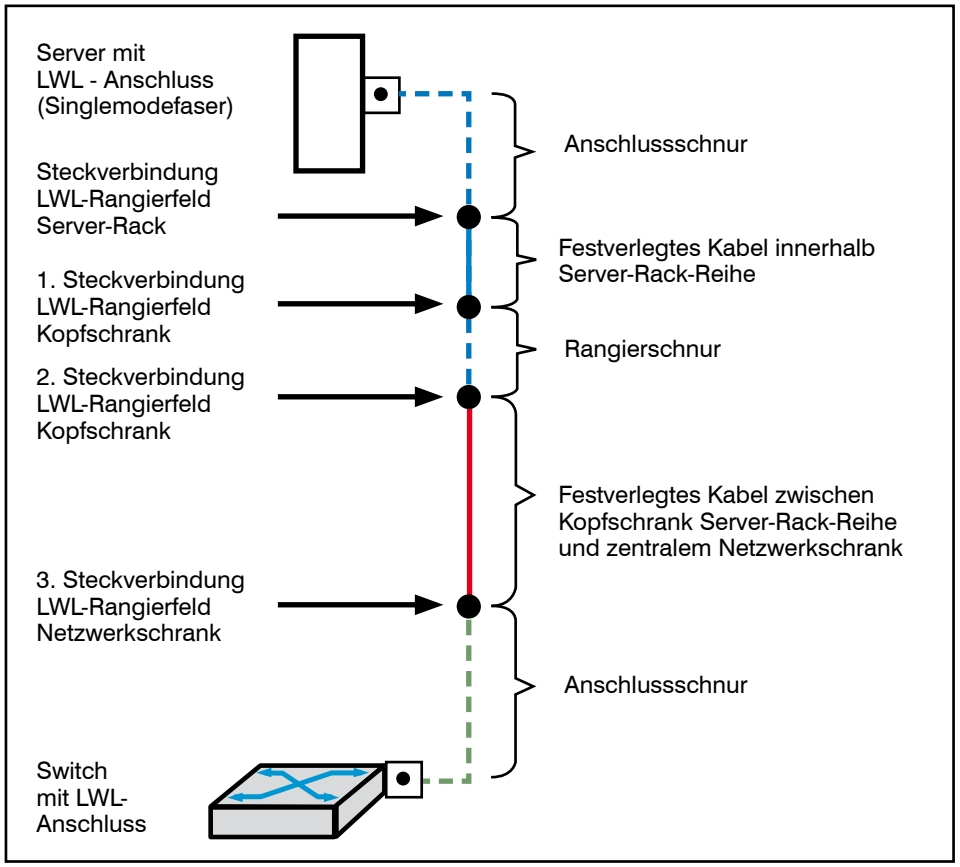

Abbildung 2: LWL-Rangierungen im Rechenzentrum

auch die Änderungen des Zustands manuell, sie muss von Personen durch eine visuelle Erfassung vor Ort aufgenommen und in den Listen / Datenbanksätzen nachgetragen werden.

ComConsult BERATUNG • PLANUNG	Rangierliste			Erfasser:_____			Datum:_____
	Gebäude:			Etage:			Verteilernr.:
Rangierkabel	von ·····			····· nach			Bemerkungen:
Typ/Nr.	Schrank	Rangierfeld Nr.	Port	Schrank	Switch	Slot	Port

Abbildung 3: Grundaufbau Rangierliste

Schluss mit dem Rangierchaos: Das intelligente Rangierfeld macht alles einfacher

Das Grundelement der Erfassung stellt eine Liste der rangierten Verbindung im Verteiler dar.

Diese einfache Liste stellt jedoch nur einen Teil der gesamten beschalteten Strecke dar, im Prinzip gibt sie nur EIN Ende der Strecke wieder, weiter erfasst werden müssen:

- Informationen, die zum anderen Ende der Strecke gehören (Rangierfeld oder Dose inklusive aktives Gerät dort).
- Optionale weitere Rangierpunkte, insbesondere bei Glasfaserstrecken mit mehrfachen Durchrangierungen.

Beide lassen sich prinzipiell mit demselben, leicht modifizierten Sheet in weiteren separaten Listen erfassen bzw. dokumentieren, was dann trotzdem fehlt ist eine anschauliche durchgehende Ende-zu-Ende-Darstellung. In vielen Projekten werden dazu EXCEL-Tabellen erstellt, die mit Hilfe von sehr vielen Spalten den kompletten beschalteten Weg beschreiben. In Abbildung 4 und Abbildung 5 wird in Form einer Grafik ein derartiger Schaltweg mit den wichtigsten Informationen dargestellt.

Trotz der Trivialität der Bilder bzw. der damit verbundenen Informationen wird jeder, der für die Erstellung von solchen Tabellen in einem Rechenzentrum einmal verantwortlich gewesen ist, wissen, wie komplex dieses sein kann (insbesondere bei sehr häufigen Durchrangierungen in einem Link) und wie wichtig es ist, diese zu haben (oder eine entsprechende Darstellung/Erfassung in einem Dokumentationssystem). Wenn eine Zuordnung eines gesteckten Ports zu einem Rangierkabel oder zum anderen Ende des Rangierkabels nicht möglich ist, kann ein hochverfügbarer und dynamisch anpassbarer RZ-Betrieb eines Netzwerkes aus Sicht des Autors kaum möglich gemacht werden. Im Tertiärbereich mag darauf noch verzichtet werden können, gerade im Umfeld von geringen Umzügen, aber im RZ kaum.

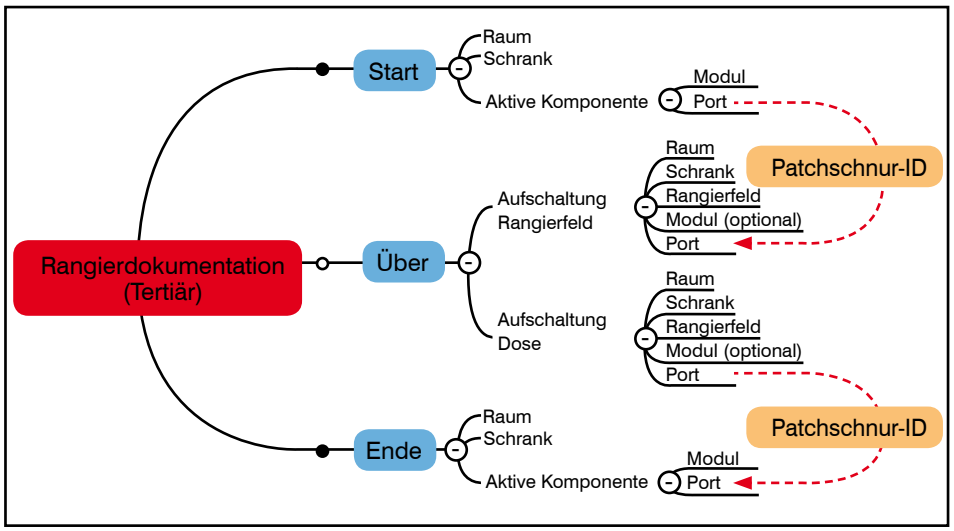

Abbildung 4: Typische Elemente einer Rangierdokumentation Tertiärbereich

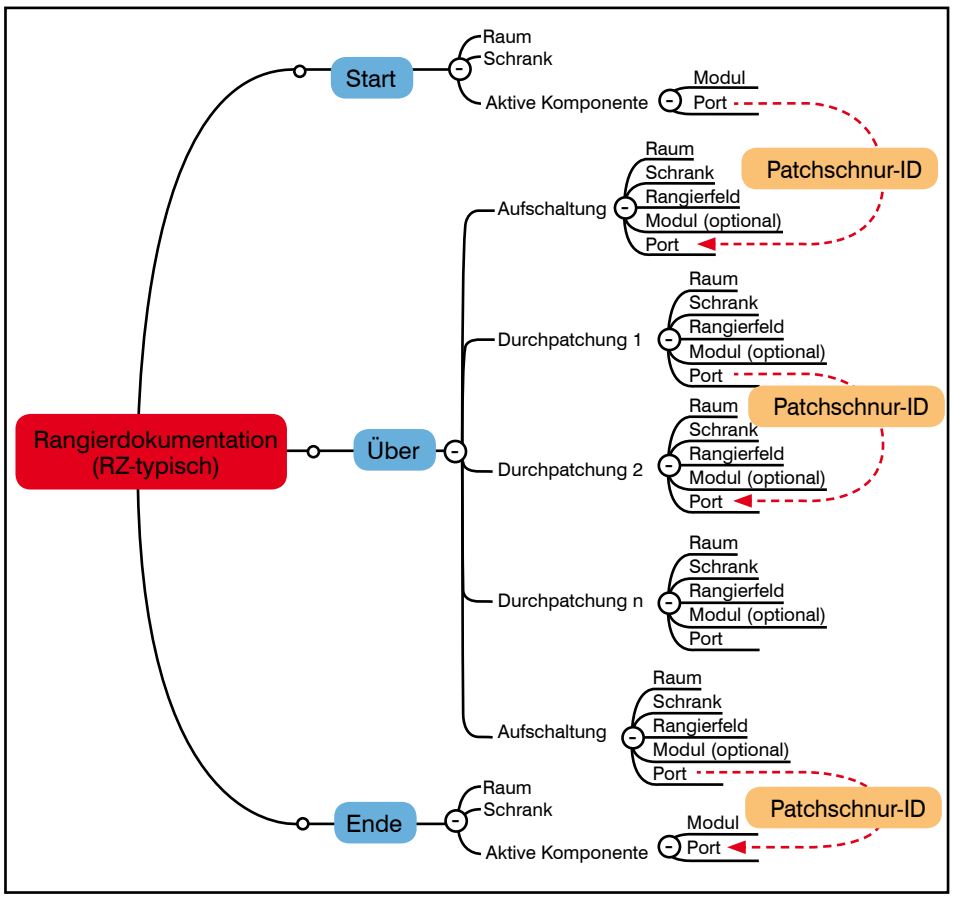

Abbildung 5: Typische Elemente einer Rangierdokumentation bei Glasfaser im RZ

Defizite von tabellarischen Dokumentationen

In der Praxis läuft ein einfaches Change Management darauf heraus, dass die Patchbeauftragten einen Ausdruck der Rangierliste mit in den Verteiler nehmen, Änderungen durchführen und diese handschriftlich nachtragen, um sie später dann wieder digital zu übernehmen (entweder als EXCEL-Tabelle auf einem Server oder in einem Dokumentationssystem), diese Verfahrensweise wird häufig auch als „reaktive“ Dokumentation bezeichnet. Das erste Problem liegt in dem zeitlichen Verzug und der damit verbundenen Gefahr, dass die Übernahme zu spät (oder gar nicht) erfolgt. Eine – wenn auch eher selten angetroffene - optimierte Version sieht vor, dass bereits vor Ort mit Hilfe eines Notebooks (oder Tablets) direkt die Aktualisierung übernommen wird.

Leistungsfähige Dokumentationssysteme (Produkte wären z.B. AixBoms oder Command) bieten eine „proaktive“ Dokumentation, dabei wird bereits die Änderungsanweisung im System so erzeugt, dass nach der durchgeführten Patchung nur noch eine Bestätigung durch den Patchbeauftragten erfolgen muss und damit eine höhere Aktualität gewährleistet wer-

den kann.
Ein zweites Problem ist gegeben, wenn kein Dokumentationssystem genutzt wird: Wie lassen sich die getätigten Einträge gerade in einem größeren Umfeld durch Suchmechanismen finden. Beispiel: Am Switch-Port xyz wird eine permanente Fehlerrate angezeigt und es ist schnell herauszufinden, mit welchem Endgerät dieser Port verbunden ist. Der Switch-Port stellt also den Suchparameter dar und in möglicherweise sehr vielen Listen muss dann über diesen Parameter gesucht werden. In Projekten mit durchaus sehr hoher Anzahl von erfassten Patchungen, auch mit einer sehr großen Anzahl von EXCEL-Tabellen konnte man mit den einfachen Windows-Suchmechanismen erstaunlicherweise sehr gut und sehr schnell auch konkrete Zeichenketten in diesen Tabellen suchen lassen.

Ein Vorteil der sehr einfachen Dokumentation mit EXCEL-Listen besteht darin,

- dass die dazu notwendigen Voraussetzungen im Prinzip bei jedem vorhanden sind,
- dass sich die zu jeder Rangierung gewünschten zusätzlichen Attribute beliebig und einfach erweitern lassen (z.B. Materialeigenschaften des Permanent Links, Zuordnung von Switch-typischen Eigenschaften wie z.B. VLAN-Zugehörigkeiten etc.),
- dass jeder damit ohne großartige vorausgehende Schulung umgehen kann,
- dass die Möglichkeiten zur Sicherung der Informationen wie bei jedem Dateibasierenden System sehr einfach sind.

Viel mehr als die oben beschriebene Erfassung des Ende-zu-Ende-Links ist aber auch nicht möglich, da bieten Infrastruktur-Management-Systeme deutlich mehr.

Sonderfall DCIM

In Zusammenhang mit der Betrachtung der Infrastruktur in Rechenzentren ist derzeit ein Begriff „in aller Munde“, Data Center Infrastructure Management (DCIM). Wie steht dieser Begriff im Zusammenhang mit dem Thema des Artikels? Damit die Kernaufgabe eines Rechenzentrums wie z.B. das Speichern von Daten oder der Zugriff auf zentrale organisierte datenbasierende Prozesse möglich ist, muss ein Rechenzentrum mit unterschiedlichen Infrastrukturen ausgestattet sind. Dies sind grob unterteilt gebäude- und raumbezogene Infrastrukturen (Stromversorgung, Zutrittsschutz, Klimatisierung etc.) und Kommunikationsinfrastrukturen wie die Verkabelung oder auch das Netzwerk. In allen Fällen erfolgt nach der Erstinstallation und Abnahme in der Regel die Übergabe einer Dokumentation, im Baugeschäft auch häufig Revisionsdokumentation genannt. Viele dieser Infrastrukturen stellen komplexe technische Anlagen dar, die sich im Laufe des Betriebs mit Hilfe von eigenen Regelungstechniken den im RZ stattfindenden Änderungen anpassen (automatisch oder manuell). Die dazu notwendigen Eingangsparameter und von der Anlage neu eingestellten Ausgangsparameter lassen sich mit anlagenspezifischen softwarebasierenden Management-Oberflächen überwachen.

Im Rahmen von DCIM wird das Ziel verfolgt, diese unterschiedlichen Oberflächen (und auch Prozesse) zu vereinheitlichen. Umfangreiche DCIM-Management-Lösungen zeichnen sich dadurch aus, dass sie möglichst viele Infrastrukturelemente eines Rechenzentrums möglichst komfortabel und effektiv integrieren können. Bei den „klassischen“ Techniken (Z.B. Kühlung) darf man davon ausgehen, dass die vom Anlagenhersteller angebotenen Möglichkeiten erstens grundsätzlich verfügbar sind und zweitens sehr ausgereift sind. Dies ist bei dem Infrastrukturelement Verkabelung für die allermeisten Verkabelungssysteme so nicht gegeben, es gibt keine Regelungstechniken oder Sensoriken, die eine erfolgte Änderung eines Zustands (z.B. von Patchungen) oder gar eine per Software gesteuerte Änderungsanweisung möglich macht. Hier kommt meistens die klassische Lösung zum Einsatz: Änderungen werden über eine einfache Dokumentation („händisch“) erfasst und das Change Management erfolgt ebenfalls manuell über eine Änderung der bis dahin existierenden Dokumentation; entweder als Anweisung oder wieder als Revision einer existierenden Dokumentation. Genau an dieser Stelle sehen die Anbieter von automatisierten Rangierdokumentationen ihren Anteil an DCIM, sinngemäß „weg von der händischen Dokumentation“.

Automatisierte Rangierdokumentation

Das Grundprinzip bei automatisierten Rangierdokumentationen liegt darin, dass ein manuelles Nachführen von durchgeführten Patchaufträgen bzw. den damit verbundenen Erfassungen der Ende-zu-Ende-Verbindung nicht notwendig ist, diese Erfassung erfolgt automatisch im Rahmen der durchgeführten Rangierung. Bereits der Auftrag selber wird dem durchführenden Techniker vor Ort nicht über eine einfache Liste, ausgedruckten Schaltauftrag o.ä. übergeben, sondern sie kann visuell mit Leuchtelementen vor Ort (in der Regel über eine LED am Rangierfeld) vermittelt werden.

Dies setzt in der Regel folgende Elemente voraus:

- Spezielle Rangierfelder oder Zusatzeinheiten, die eine Sensorik haben zur Erfassung der Patchungen („intelligente Rangierfelder“) plus einer LED-Signalisierung zur Anzeige von Porteigenschaften.

Schluss mit dem Rangierchaos: Das intelligente Rangierfeld macht alles einfacher

- Patchschnüre mit zusätzlichen Elementen an den Steckern zur Kennzeichnung dieser Kabelenden mit Zusatzinformationen (z.B. RFID oder Chips).

- 19“-Steuerungseinheiten, auf welche die Rangierfeld-Sensorik aufgeschaltet wird und welche dann über das Netzwerk gemanaged wird (in der Regel mit einem RJ45-LAN-Anschluss).

- Eine Hardware inklusive Datenbank-Bausteine und herstellerspezifischer Software zur Überwachung der Steuerungseinheiten.

Diese Elemente ermöglichen dann

- eine automatische Dokumentation und Überwachung des Netzes auf Layer 1 (nicht vollständig, da z.B. Ethernet-spezifische Informationen des Layer 1 nicht erfasst werden),

- eine automatisierte Anzeige bei Änderungen und Einleitung von Reaktionen,

- eine Steuerung/Optimierung des Arbeitsflusses.

Je nach Hersteller-Lösung können zu dem dokumentierten Link auch verkabelungsspezifische Informationen hinterlegt werden wie z.B. Leitungslänge, übertragungsspezifische Eigenschaften des Permanent- und Channel-Links, welche dem Nutzer des Links eine Beurteilung der Qualität z.B. im Rahmen einer geplanten 10-Gigabit-Nutzung möglich macht.

Alle Systeme setzen voraus, dass genau nur die vom Hersteller hierfür vorgesehenen Rangierfelder und Patchschnüre eingesetzt werden, andere Hersteller können möglicherweise nicht mehr zum Einsatz kommen. Damit werden alle sonst bei einem Verkabelungssystem wichtigen Eigenschaften wie Übertragungsqualitäten, Montagefreundlichkeit, Robustheit o.ä. völlig der automatischen Dokumentation untergeordnet. Wohlgemerkt, es bedeutet nicht, dass die nachfolgend beschriebenen Systeme in diesen Punkten nicht ebenfalls hochqualitativ sind.

Keines der Systeme präsentiert eine Lösung zur Erfassung von Aufschaltungen in einer Dose oder in einem weit vom Verteiler entfernt stehenden Endgerät. Damit wird der Einsatzschwerpunkt deutlich: das Rechenzentrum. Im Übrigen fokussieren sich die Internet-Informationen der Firmen auch sehr deutlich auf diesen Bereich, insbesondere die Bedeutung dieser Technik für ein vollständiges Data Center Infrastructure Management (DCIM) wird verstärkt betont.

Bedingt durch die Nutzung von SNMP als Übertragungsprotokoll für die aus dem Rangierfeld bzw. Controller ausgelesenen Informationen lassen sich diese auch sehr einfach in AIM-Systeme (Automated Infrastructure Management) wie z.B. den bereits erwähnten System AixBoms oder Command übernehmen und verarbeiten.

Die Auswahl an Systemen zur automatisierten Rangierdokumentation ist nicht besonders groß, eine Markpräsenz im deutschen Raum haben zwei Systeme, das FuturePatch-System von TKM und Quareo von TE. Auf einen Vergleich der unterschiedlichen Möglichkeiten zur Auswertung der Informationen durch die verschiedenen Management-Platformen der Hersteller selber wird im Artikel nicht eingegangen. Eine sehr ausführliche Beschreibung der Systeme ist der Tabelle im Artikel zu entnehmen. (siehe Tabelle am Ende des Artikels)

FuturePatch

Bei FuturePatch gibt es immer eine eigenständige 19“-Controller-Einheit Rack Control Unit (RCU) und je nach Kabeltechnik unterschiedliche 19“-Panel Control Units (PCU), sprich Rangierfelder, die auf die RCU aufgeschaltet werden müssen (bis zu 40 Stück pro RCU). Diese dienen sowohl der Erkennung von gepatchten Anschlüssen wie auch der visuellen Anzeige von Informationen (z.B. wohin zu patchen ist). Folgende Typen können derzeit angeboten werden:

- RJ45 Panel 24 - mit Cat6 und Cat6A - 1HE

- FO LCdx 24 - Fasertyp nach Wunsch - 1HE

- FO SCdx 24 - Fasertyp nach Wunsch - 1HE

Die „Patchkabel-Erkennung“ erfolgt mit Hilfe eines RFID, der es möglich macht dem Patchkabel neben der eindeutigen ID auch Zusatzinformationen zuzuweisen. Dieser RFID ist als sehr kleines Zusatzelement sichtbar (siehe Abbildungen 6 und 7) und soll nach Herstellerangaben auch an Patchkabel von Drittherstellern angebracht werden können. Dem Foto mit einem RFID an einem LC-Duplex ist zu entnehmen, dass der Duplex-Clip den RFID beinhaltet, damit kann vermutlich auch eine Drehung von Tr/Rc ohne Probleme durchgeführt werden (siehe Unterschied zum Lösungsansatz von TE). Ein Angebot von MPO mit RFID-Tags ist in den allgemeinen Publikationen des Herstellers nicht erkennbar.

Quareo

TE Connecitivity bietet zwei Systeme an,

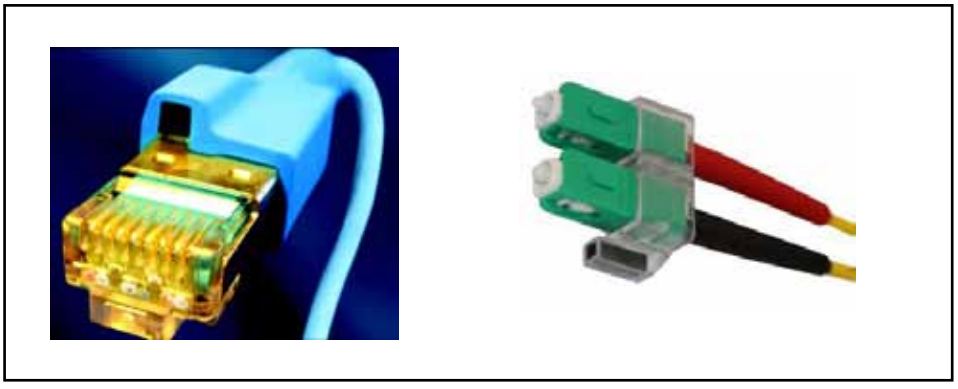

Abbildung 6: RFID-basierende Sensor-Elemente System Future Patch

Abbildung 7: RCU bei Future Patch

Schluss mit dem Rangierchaos: Das intelligente Rangierfeld macht alles einfacher

das ältere Quareo AMPTRAC und das neuere Quareo CPID. Das ältere System arbeitet mit speziellen Sensorstreifen, die entweder bereits an Rangierfeldern des Herstellers TE angebracht sind oder nachträglich - je nach vorhandenem Platz - auch auf Rangierfelder von Drittherstellern (oder aktiven Systemen) angebracht werden können. Diese Sensorelemente werden mit einem zentralen AMPTRAC Analyzer verbunden, welcher wiederum über ein Netzwerk überwacht werden kann. Spezielle Patchkabel haben einen zusätzlichen Leiter im Kabelmantel (!) und an jedem Ende einen Sensorstift, der bei eingestecktem Zustand eine zusätzliche ohmsche Verbindung zu den Sensorfeldern bewirkt. Damit kann erfasst werden, welcher Port belegt ist und wo das andere Ende aufgeschaltet ist.

Das neuere System Quareo CPID besitzt im Prinzip drei unterschiedliche (intelligente) Rangierfeldeinheiten, eins für RJ45 mit der Bezeichnung Q2000 (in zwei Größen) und zwei für Glasfaser, jeweils der Typ Q4000 und QHDEP. QHDEP ist ein High-Density-Feld, beide sind modular aufgebaute Rangierfelder. Die RJ45-Qualität beim Q2000 erlaubt eine Übertragung von 10 Gigabit über UTP/STP nach TIA-Standard, im Glasfaserbereich gibt es sowohl LC-Rangierfelder (bzw. Module) als auch MPO-Module, damit wird eine Übertragungsrate bis inklusive 100 Gbit/s sichergestellt. LC/MPO-Hydra-Kabel ergänzen das Portfolio, so dass die im MPO-Bereich notwendigen Adaptierungen möglich sind. Module mit anderen Steckertypen wie z.B. SC oder E2000 sind als Standard-Produkt auch hier nicht erkennbar.

Im Unterschied zum FuturePatch oder AMPTRAC gibt es keinen separaten zentralen Controller, sondern jeder Rangierfeldtyp erhält einen eigenen aufsteckbaren Controller, eine Kompatibilität der Controller zwischen den Rangierfeldtypen ist aber nicht gegeben (also gibt es bei drei Rangierfeldtypen drei unterschiedliche Controller). Der Controller und damit auch das Rangierfeld wird über einen PoE-LAN-Port mit Strom (IEEE 802.3af) und Daten (10/100 Mbit/s) versorgt, bei fehlendem PoE können separate Netzteile für den QHDEP eingesetzt werden. Bei Verwendung dieser Technik im Rechenzentrum ist also auch Switch-Technologie mit PoE notwendig (was nicht selbstverständlich sein muss). Der Controller wird von hinten auf das Rangierfeld aufgesteckt, was eine rückseitige Zugänglichkeit voraussetzt aber den Vorteil mit sich bringt, keine zusätzlichen HE im Schrank zu belegen.

Abbildung 8: AMPTRAC-Controller und Sensorelemente am Rangierfeld

Abbildung 9: Quareo-Rangierfeld (Front/Rückseite) mit aufsteckbarem Controller

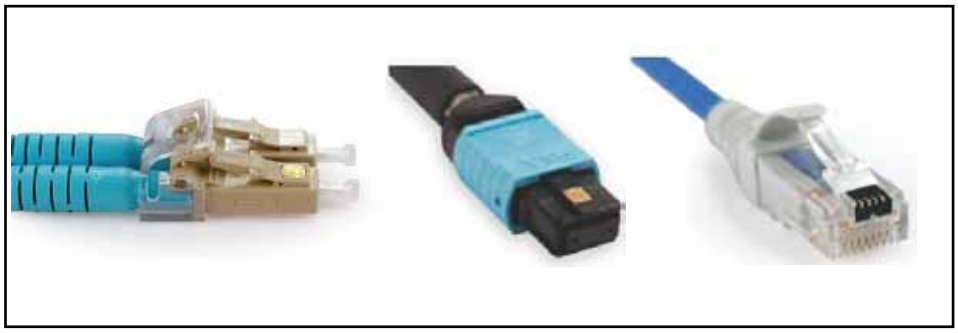

Abbildung 10: Chip-basierende Sensor-Elemente System Quareo

An den Rangierfeldern befinden sich ebenfalls LEDs zur Kennzeichnung von verschiedenen Stati.

Die Patchkabel sind bei der neueren Lösung mit Hilfe von speziellen Mini-Chips „Connection Point Identification“ (CPID) gekennzeichnet, diese fallen in der Größe etwas kleiner aus als RFIDs (siehe Abbildungen 9 und 10). Auffallend in der Abbildung für den LC-Duplex ist, dass nur einer der beiden Stecker mit diesem CPID ausgestattet ist. Da möglicherweise dies bei einem manuellen Drehen des Anschlusses zu Schwierigkeiten bei der Erkennung geführt hat, sind im TE-Portfolio Patchschnüre mit unterschiedlicher Polarität zu finden. Dies erschwert aus Sicht des Autors etwas die Handhabung. Es gibt keinerlei Hinweis bei TE, dass Patchschnüre von Drittanbietern mit dieser Technik nachträglich gekennzeichnet werden können.

Fazit

Die größte zu überwindende Hürde zum Einsatz von automatischer Rangierdokumentation ist die Bereitschaft nach einer herstellerabhängigen Verkabelung, deren mittel- und langfristige mechanische und übertragungstechnischen Qualitäten von den Herstellern noch unter Beweis zu stellen sind. Herstellerneutrale Zertifizierungen wie z.B. im Rahmen des PVP-Programms sind noch eher selten zu finden und es bleibt die Unsicherheit, ob diese speziellen Verkabelungssysteme tatsächlich in der gleichen Qualität zur Verfügung stehen wie die High-Tec-Systeme der sel-

Schluss mit dem Rangierchaos: Das intelligente Rangierfeld macht alles einfacher

ben Hersteller. Auch bleibt die Sensorik an den aktiven Komponenten eine aus Sicht des Autors „unklare“ Lösung, mit welchem Hersteller von aktiven Komponenten lässt sich mit welchen „Klimmzügen“ ein gesteckter Port erfassen (Klebestreifen, Zwischenrangierfelder oder ….). Ein Mix-and-Match zwischen verschiedenen Herstellern - selbst zwischen verschiedenen Systemen des selben Herstellers - kann fast völlig ausgeschlossen werden. Damit entzieht man sich der Möglichkeit, auf sich verändernde Anforderungen an die Verkabelung durch sukzessive Implementierung von neuen Lösungen zu reagieren. Ein gutes Beispiel dafür wäre ein erzwungener Technologiewechsel bei 40- und 100 Gbit/s über Ethernet oder die sich abzeichnende Einführung von 40 Gbit/s über Kupfer, wie werden solche Systeme damit umgehen (oder sind damit umgegangen).

Eine Nutzbarkeit der Lösungen für eine vollständige Erfassung eines rangierten Links im Tertiärbereich ist nicht erkennbar, der Einsatzschwerpunkt bleibt auf den Verteilerschrank beschränkt.

Falls eine Bereitschaft zum Einsatz dieser proprietären Verkabelungstechnologien im Rechenzentrum gegeben ist, muss im nächsten Schritt festgelegt werden, ob die auszuwählende Dokumentationslösung, z.B. im Rahmen von DCIM, ein weiterer Bestandteil einer übergeordneten AIM-Lösung werden soll. Die möglichen Schnittstellen bzw. Integrationsmöglichkeiten sind zu analysieren (Aussage eines Anbieters von AIM: dank SNMP sollte die Integration technisch kein Problem sein). Einfacher wird es, wenn die Hersteller-Lösung eine autarke Lösung bleibt und die vom Hersteller geschaffenen Möglichkeiten der Management-Plattform ausreichend sind.

Eine Abschätzung des Mehrwertes von Rangierfeldern mit automatischer Erfassung der Rangierungen im Vergleich zur erwartenden Herstellerabhängigkeit sollte sorgfältig gemacht werden, denn die Bindung an einen Verkabelungs-Hersteller bzw. an eine spezielle Lösung kann insbesondere im Rechenzentrum auch in eine Sackgasse führen.

Nummerierung von Rangier- oder Anschlussschnüren

Die Berücksichtigung der Anschlussschnüre in einem Numerierungsschema wird sehr unterschiedlich gehandhabt. Eine Schnur erfüllt eine ganz wesentliche Rahmenbedingung nicht, sie befindet sich nicht permanent an ein und demselben Ort. In vielen Netzen geht man damit auf zwei Arten um:

- Die Schnüre werden überhaupt nicht beschriftet bzw. nummeriert.
- Die Schnüre werden mit einer Nummerierung versehen, die passend zur aktuellen Patchung ist.

Die erste Methode hat den Nachteil, dass man im Betrieb entweder diszipliniert geführte und korrekte Rangierlisten führt (was den meisten Betreibern viel zu aufwendig ist) oder man durch Tasten/Fädeln herauszufinden versucht, welcher Port womit verbunden ist. Für den Fall, dass man sich beim Fädeln „vergreift“, würden daraus ganz falsche Folgehandlungen resultieren. Je länger die Schnur ist, z.B. im Falle einer Rangierung über mehrere Schränke oder durch Doppelböden hinweg, desto größer wird die Gefahr, dass man Fehler macht. Eine Kennzeichnung der Schnüre an beiden Enden kann hier Fehler vermeiden helfen.

Die zweite Methode hat zur Folge, dass man bei jeder Änderung der Rangierung bzw. Aufschaltung die Kennzeichnung an einem oder beiden Enden ändern muss. Auch das erfordert ein zeitnahes Handeln und große Disziplin. Diese Methode ist ungeeignet für Rangiertechniken im TP-Bereich bei Netzen mit häufigen Umzugsraten. Dagegen kann sie sehr wohl im relativ statischen Backbone-Bereich, also insbesondere bei LWL-Verkabelungen, benutzt werden. Eine sehr einfache Beschriftungsmethode sieht einen wesentlich einfacheren Weg vor: Schnüre jeder Art werden an beiden Enden mit einfachen durchlaufenden Nummern beschriftet (mindestens 4-stellig), die unbedingt innerhalb des Technikraumes eindeutig sein sollten. Daher ist beim Kauf der Schnüre darauf zu achten, dass der Lieferant die Schnüre beidseitig mit einem vorgegebenen Nummernbereich versieht.

Fragen	Herstellerangaben TKM Future-Patch	Herstellerangaben TE (System Quareo AMPTRAC und Quareo CPID)
Allgemein		
Wie erfolgt die automatische Erfassung von Patchungen?	Patchkabel sind mit RFID Transpondern ausgestattet, darüber erhält das Kabel eine eindeutige Kabel ID, wie eine Seriennummer. Die permanent überwachenden RFID Scanner an den Verteilerfeldern detektieren dieses Kabel, sobald es sich im Einrastzustand in der Buchse befindet. Die erkannte Kabel ID wird an die übergeordnete Instanz kommuniziert.	Bei Quareo AMPTRAC durch 9. Pin/ Draht an beiden Steckern des Patchkabels. Bei Quareo CPID durch einen Chip auf dem Stecker des Patchkabels
Liegen Referenzen zur Integration in DCIM-Systeme bzw. Dokumentationssysteme vor (z.B. AIXBoms oder Command)? Mit welchem System?	Ja, es liegen Referenzen vor: DCIM Tool A) Patch Manager - ww.patchmanager.com Diverse Installationen über Middleware Schnittstelle* und vollständige Kompatibilität zur RFID Hardware DCIM Tool B) VM.7 von AT+C Systeme - www.atc-systeme.de Z.B. Endkundenseitig bei DB-Systel in Berlin, 3 Rechenzentrumssäle mit ca. 25.000 überwachten Ports. Vollständige Integration über Middleware Schnittstelle* und vollständige Kompatibilität zur RFID Hardware DCIM Tool C) Command von FNT - http://www.fntsoftware.com/ ** openCONNECTOR - ein Produkt von KTS-Systeme (TKM Gruppe)*	Durch die Programmierung einer Middleware und durch die offene Quareo PLM-Software, ist im Prinzip die An- und Einbindung in jedes Management System möglich. Fertige Middleware gibt es für FNT Command.

Schluss mit dem Rangierchaos: Das intelligente Rangierfeld macht alles einfacher

Fragen	Herstellerangaben TKM Future-Patch	Herstellerangaben TE (System Quareo AMPTRAC und Quareo CPID)
Wie erfolgt Darstellung der Patch-Anweisung (z.B. über LEDs)?	Über Hardwareseite: Grundsätzlich eindeutige Anzeige über LED, zusätzlich per Klartext auf dem Display der Rack Control Unit Über Softwareseite: In der Schrankansicht mit Real-Time Anzeige, optional auf Patchlisten, über Mobilgeräte wie Smartphone oder Tablett PC auch vor Ort am Schrank selbst	Bei Quareo AMPTRAC durch ein Display am Analyzer der im entsprechenden Schrank eingebaut ist, per Email an den Techniker oder per App auf ein Smartphone oder Tablet. Bei Quareo CPID durch LED am Panel, per Email an den Techniker oder per App auf ein Smartphone oder Tablet.
Wie erfolgt Patch-Erfassung an aktiven Komponenten (Switches, Server), was ist dazu notwendig, welche Einschränkungen gibt es (insbesondere bei aktiven Komponenten mit hoher Portdichte)?	Serverports: Serverports werden mit einem Transponder markiert. Dies im Idealfall schon bei der Anlieferung, unabhängig ob der Server in Betrieb geht oder noch für eine Zeit eingelagert wird. Dies kann so gleichzeitig mit einem RFID Asset- oder Inventarisierungssystem verknüpft werden. Diese Markierung erfolgt über eine kurze Stecker-Buchse Komponente, die den Transponder trägt. Diese ist nach einmaligem Einsetzen in den Serverport nicht mehr per Hand lösbar. Das Auslesen dieser Transponder am Server erfolgt nun über Sensorkabel. Das Sensorkabel sitzt typischerweise zwischen einem Verteilerfeld und dem Server. Der RFID Scanner am Verteilerfeld, welcher nur eine kurze Distanz in Luft vor den Ports scannen kann, nutzt die Eigenschaft des Sensorkabels, übertrag das RFID Signal über eine zusätzlich Doppelader im Kabel und kann so bis zu 20m entfernte Transponder an den Serverports detektieren. Diese Lösung existiert sowohl für Glasfaser als auch für Kupferverbindungen. Switchports: Methode A) Switchports können mit einem individuell für den Switchtyp designten RFID Scanner überwacht werden. Diese wird von vorne am Switch befestigt. Einschränkung / Nachteil: Sinnvoll erst bei größeren Stückzahlen von Switchgeräten, da unter Umständen Einmalkosten der Scanneranpassung umgelegt werden müssen. Methode B) Um die Anpassungsnotwendigkeit zu minimieren, werden die Switchports über o.g. Stecker-Buchse Komponente um eine „Ebene“ nach vorne verlegt. Dies hat den Vorteil, dass dann alle z.B. 48 Switchports eine einheitliche Geometrie aufweisen. Die Stecker-Buchse Komponenten sind so gestaltet, dass nun in der Mittelreihe ein RFID Scanner angebracht werden kann. Allgemein: Für sehr hohe Packungsdichten, z.B. an HD LWL Panel muss eine Scannerelektronik individuell designed werden. Dazu eignet sich die RFID Technik sehr gut.	Bei Quareo AMPTRAC besteht die Möglichkeit einen Sensorstreifen am Switch anzubringen. Einschränkungen in der Funktion der Switche gibt es nicht, es hängt lediglich von den Platzverhältnissen ab, ob ein Sensorstreifen hergestellt werden kann oder nicht. Bei Quareo CPID über eine Cross Connect Lösung (Anmerkungen Autor: Üblicherweise wird dazu ein weiteres Zwischenrangierfeld benötigt). Server werden, wie Endgeräte über die Erkennung von IP- und MAC-Adressen dokumentiert, es sind dazu keine mechanischen Vorkehrungen nötig. Desweiteren besteht die Möglichkeit QR-Codes (Anmerkung Autor: QR-Code = Quick Response Code; Code zur Markierung von Baugruppen und Komponenten) für alle Komponenten zu erstellen. Damit können alle Daten über eine QR-App vor Ort abgefragt werden.
Welche Hersteller von aktiven Komponenten wurden bereits im System integriert? Gibt es dazu eine Übersichtsmatrix?	Es gibt RFID Scanner, die direkt auf Switchgeräten verwendet werden können, mechanisch kompatibel sind und auf die Front aufgebracht werden. Dazu zählen: • Nexus 2248TP • Cisco Catalyst WS X4148/6148 • Alcatel Lucent OmniSwitch 6850-P24 Diese Scanner sind für den Einsatz von RFID Transponderkabeln designed. Ein direkter Einsatz von Sensorkabeln, die Serverports direkt mit den Switchports verbinden ist nicht bei allen o.g. Typen möglich. Dies hat bauartbedingte Gründe.	Cisco, Extreme, Nortel, Alcatel, HP
Können kabelspezifische Attribute (z.B. Qualität des Patchkabels) hinterlegt werden, welche? Können auch Attribute der Installationsstrecke hinterlegt werden?	Ja! Die RFID Transponder haben einen Speicherbereich. So wird beispielsweise direkt bei der Kabelkonfektion kabelspezifische Daten (Länge, Kabeltyp (SM / MM), Fasertyp oder Kategorie (OM3, OM4, Cat. 6A), Steckertyp usw.) hinterlegt. Diese sind fest mit dem Kabel verbunden und können über die Scanner ausgelesen und von der DCIM Software verwendet werden. Funktionalbeispiele: • Hinweis, wenn SM Kabel in MM Strecke gebaut wird • Hinweis, wenn zu langes Patchkabel verwendet wird (Längenristriktion 100m) Zusätzliche werden aber noch Messwerte, z.B. Einfügedämpfung usw. hinterlegt, welche auch z.B. nach einer Planung über zu Verfügung stehendes Dämpfungsbudget ausgelesen werden können, und so eine Analyse zwischen Planung und Realisierung möglich ist. Steckzykluszähler: Im Transponderspeicher kann ebenso ein Steckzykluszähler realisiert werden. Dieser zählt die Anzahl der z.B. bei LWL Kabeln gesteckten Zyklen und gibt bei einer zu definierenden Anzahl eine Warnmeldung über das DCIM System ab.	Bei Quareo AMPTRAC können sowohl kabelspezifische Attribute als auch Attribute der Installationsstrecke in der Datenbank der Quareo PLM Software hinterlegt werden. Bei Quareo CPID können kabelspezifische Attribute auf dem Chip am Patchkabel gespeichert werden und Attribute des Patchkabels und der Installationsstrecke in der Datenbank der Quareo PLM Software hinterlegt werden.

Schluss mit dem Rangierchaos: Das intelligente Rangierfeld macht alles einfacher

Fragen	Herstellerangaben TKM Future-Patch	Herstellerangaben TE (System Quareo AMPTRAC und Quareo CPID)
Welche Export-Möglichkeiten der erfassten Rangierdaten gibt es, falls kein Dokumentationssystem verwendet wird (csv-Format o.ä.)?	Bislang existieren keine Exportmöglichkeiten sofern keine Dokumentationsoftware verwendet wird. Perspektivisch wird es diese geben: XML und csv.	CSV-Format
Ist MPO-Technologie verfügbar?	Nein, ist aber angekündigt.	Ja.
Patchkabel		
Faktor Preisunterschied Spezial-Kabel zu gleichwertigen Standard-Patchkabel (innerhalb der eigenen Produktfamilien)?	Der Faktor variiert über die Kabellänge, da RFID-Zusatz nur Einmalkosten darstellen. Beispielsweise: • F=1,6 bei Cat 6A 5m • F=1,4 bei OM4 LCdx 4m	Faktor Zwei
Welche Übertragungsqualitäten sind bei Cu/LWL erhältlich?	Alle Übertragungsqualitäten, die es sonst auch gibt, da RFID Transponder nur an beiden Kabelenden zusätzlich angebracht werden. So bspw. Cat.6, Cat. 6A, OS2, OM2 bis OM4	LWL: OS2, OM3, OM4 Cu: Kat. 5E, Kat. 6, Kat. 6A, Kat. 7A
Wie können Patch-Kabel von anderen Herstellern bei der automatischen Erfassung integriert werden?	Die Position des Transponders zur Steckerstirnseite wird offen gelegt, so dass Kabelhersteller bei Bedarf sich einen eigenen Clip designen können. Besonderheiten TKM-Lösung: Wenn bewusst nicht gewünscht ist (aus welchem Grund auch immer), dass Kabel fremder Hersteller verwendet werden, so hat der Anwender die Möglichkeit eine „RFID Staubschutzkappe“ zur elektronischen Versiegelung des Ports zu verwenden. Bei unbefugtem Entfernen wird eine Nachricht ausgelöst.	Standard-Patchkabel ohne Managementfunktion können als normale Patchkabel jederzeit benutzt werden. Bei Quareo CPID werden Standard-Patchkabel ebenfalls als gesteckt und nicht gesteckt erkannt.
Rangierfelder		
Wie erfolgt Integration von Rangierfeldern Drittherstellern, gibt es funktionale Einschränkungen?	TKM bietet Integrationsunterstützung an, so dass sich Fremdanbieter ein eigenes „Leerverteilerfeld“ designen können, welches mechanisch kompatibel ist und somit den Scanner aufnehmen kann! Bei Vorliegen geeigneter Rahmenbedingungen kann eine individuelle Anpassung der Elektronik gegen Beauftragung erfolgen!	Bei Quareo AMPTRAC besteht grundsätzlich die Möglichkeit auch für Dritthersteller Sensorstreifen zu fertigen und anzubringen.
Welche Drittheresteller wurden bereits im System integriert?	Aus rechtlichen Gründen ist eine Auflistung leider nicht möglich!	Keine Angaben.
Brauchen die „intelligenten“ Rangierfelder einen Stromanschluss, welchen?	Kein zusätzlicher Stromanschluss notwendig. Die intelligenten Rangierfelder benötigen für die Kommunikation einen Anschluss an den Systembus. Über diesen erfolgt auch die Stromversorgung.	Quareo AMPTRAC: nein Quareo CPID: PoE oder Steckernetzteil
Wie erfolgt für den Patch-Beauftragten und den Administrator die Anzeige der Abweichung bei falschem Patchen?	<u>Patch-Beauftragten:</u> Nicht vollständig korrekt ausgeführte Patchungen werden durch Blinken der Port-LED angezeigt. Zusätzlich zeigt das Textdisplay per Klarschrift den falschen Port an und weist erneut auf den richtigen Port hin. Beim Entfernen der Falschsteckung wird automatisch der richtige Port erneut blinkend angezeigt. <u>Administrator:</u> Durch Push-Nachrichten wie bspw. dem Zusenden einer eMail mit den Daten der Patchung. Weiterhin sind in diversen tabellarischen Listen über ungeplante Änderungen sowie Real-Time Ansicht des Schrankzustandes vorhanden.	Akustische und optische Signale direkt im Verteilerschrank, sofortige Email-Benachrichtigung
Müssen die Rangierfelder programmiert/konfiguriert werden?	Die Rangierfelder selber nicht. Nach der Installation eines Rangierfeldes wird dies über dessen Seriennummer automatisch erkannt und in dem DCIM Tool als „neues“ Rangierfeld angezeigt. Dies kann dann z.B. per Drag&Drop in dem Schrank an die richtige Position gezogen werden.	Nein.

Schluss mit dem Rangierchaos: Das intelligente Rangierfeld macht alles einfacher

Fragen	Herstellerangaben TKM Future-Patch	Herstellerangaben TE (System Quareo AMPTRAC und Quareo CPID)
Kann eine Ende-zu-Ende-Erfassung für ein angeschlossenes Endgerät oder einen Sever erfolgen oder kann nur eine Patchung im Verteilerbereich dokumentiert/erfasst werden? Wie? Welche Voraussetzung müssen dazu auf der Endgeräte/ Server-Seite getroffen werden?	*Die Frage wurde wie folgt verstanden: „Kann eine Ende-zu-Ende-Erfassung" automatisch und in Echtzeit überwacht werden:* Eine automatische Ende-zu-Ende Erfassung ist nicht möglich. Eine Darstellung des gesamten Ende-zu-Endes Kabels schon, allerdings beinhaltet dieser dann auch nicht automatisch überwachte, manuelle Abschnitte. Je nach Ort des Endgeräts kann dies mit der o.g. Stecker-Buchse Komponente ausgerüstet werden, welche einen Transponder trägt. Dann ist eine Ende-zu-Ende Verbindung möglich. Rahmenbedingung dazu: maximale Entfernung 20m und typischerweise über eine Rangierschnur angebunden.	Die Quareo PLM Software erfasst alle SNMP fähigen Endgeräte, völlig unabhängig welcher Art. Über eine Verknüpfung der logischen Informationen IP- und MAC-Adresse und der in der Datenbank hinterlegten physischen Information des Netzwerks, weiß die PLM-Software wo im Netz und wo geografisch sich das betreffende Endgerät befindet.
Controlpanel (= Einheit zur Überwachung der intelligenten Rangierfelder)		
Wie erfolgt Integration von Rangierfeldern Drittherstellern, gibt es funktionale Einschränkungen?	Siehe bitte oben, Punkt: „Rangierfelder" - erste Antwort	Bei Quareo AMPTRAC sitzt die „Intelligenz" nicht im Rangierfeld. Es gibt einen externen im Verteilerschrank eingebauten 19"-Analyzer, der die Patchfelder überwacht. Somit sind auch Rangierfelder von Drittanbietern grundsätzlich einbindbar, Voraussetzung ist, es gibt einen passenden Sensorstreifen, siehe oben. Bei Quareo CPID hat jedes Rangierpanel einen Panel-Controller, eine Einbindung von Drittanbietern ist nicht möglich.
Wie erfolgt die Stromversorgung der Controlpanel? Gehen die Konfigurationen bei Stromausfall verloren?	Stromversorgung über die Busverbindung. Konfigurationsdaten gehen nicht verloren bei Stromausfall.	Quareo AMPTRAC: Der Analyzer hat einen 230 Volt Anschluss Quareo CPID: PoE oder Steckernetzteil Konfigurationsdaten gehen bei Stromausfall nicht verloren.
Wie erfolgt der Anschluss der Rangierfelder an das Controlpanel? Wie viele Rangierfelder können an ein Controlpanel angeschlossen werden?	Das Controlpanel und die Rangierfelder sind mit einem Bussystem verbunden. Die Busstecker sind einfach einzustecken, die Rangierfelder sind hot-swapable, können also im laufenden Betrieb hinzugefügt oder entfernt werden. Eine Controlpanel versorgt bis zu 42 Rangierfelder mit Strom. Dies ist die einzige Limitierung, die für das Controlpanel zu „managenden" Ports der Rangierfelder limitieren nicht die Anzahl.	Quareo AMPTRAC: Mittels Scanning-Modul, Scanning-Modul-Kabel und Standard-Patchkabel. Die AMPTRAC Analyzer gibt es in 3 Versionen: 384 Ports = 16x 24 Port Patchfeld, 768 Ports = 32x 24 Port Patchfeld und 1152 Ports = 48x 24 Port Patchfeld Quareo CPID: Jedes Rangierfeld hat seinen eigenen Panel-Controller
Womit kann auf die intelligenten Rangierfelder zugegriffen werden, nur mit einer übergeordneten speziellen MGM-Software oder z.B. auch mit einem Browser?	Möglichkeit A) Stand-Alone Variante: man kann die intelligenten Rangierfelder und die Controlpanel auch vollständig ohne Software verwenden. Dann besteht die Möglichkeit per IP Adresse und Web-Browser direkt auf die Controlpanel zu gehen und sich dort die Portzustände ansehen bzw. Änderungen direkt anzuwählen. Möglichkeit B) Verwendung einer MGM Software: da das TKM System über die Middleware Schnittstelle mit mehreren Softwarepartnern zusammenarbeitet, ist der Funktionsumfang des Gesamtsystems sehr unterschiedlich je nach Einsatz des Softwareprodukts. Allerdings besteht hier auch bei mindestens einem Softwareprodukt die Möglichkeit per Browser zuzugrifen.	Die Quareo PLM Software ist Browserfähig für Remote-Zugriff und es gibt eine Mobile App für Smartphones und Tablets. Desweiteren besteht die Möglichkeit QR-Codes für alle Komponenten zu erstellen. Damit können alle Daten über eine QR-App vor Ort abgefragt werden.
Können Fehlermeldungen automatisch erzeugt und gezielt versendet werden? Welche (entfernte Patchung, falsche Patchung)? Was ist dazu notwendig?	Ja, Fehlermeldungen werden z.B. per eMail an zuvor definierte Adressen gesendet. Welche Typen von Fehlermeldungen gesendet werden sollen ist frei wählbar, z.B. nicht autorisierte Verbindungen, Informationen über die Kabeleigenschaften, Warnmeldungen bei Rangierverbindungen falschen Typs (Stichwort SM Kabel in MM Strecke).	Ja, grundsätzlich zu jeder Änderung im automatisiert überwachten Patchbereich, aber auch bei Änderungen an Endgeräten, z.B. PC wird abgesteckt und an einer anderen Dose wieder angeschlossen. Konfiguration der Alarme erfolgt über die Quareo-PLM-Software.

Schluss mit dem Rangierchaos: Das intelligente Rangierfeld macht alles einfacher

Fragen	Herstellerangaben TKM Future-Patch	Herstellerangaben TE (System Quareo AMPTRAC und Quareo CPID)
Was lässt sich über die reine Rangierdokumentation hinaus mit dem System erfassen/ dokumentieren (Stromversorgung, Temperatur, Türkontakte o.ä.)?	Jeder Scanner an den Verteilerfeldern hat Sensorik für Temperatur und Feuchtigkeit, somit sind komplette Messdatenprofile über die gesamte Schrankhöhe möglich. Für eine weitere automatische Überwachung an den physikalischen PDU Verbindungen liegt ein Konzept und Funktionsmuster vor. Dabei handelt es sich um ein RFID-Monitoring der Spannungsversorgungskabel von der PDU Dose zum jeweiligen Device (z.B. Switch, Server usw.). Diese Überwachung ist eine physikalische Überwachung der Stromversorgung, sodass automatisch bestätigt werden kann, dass z.B. die Server tatsächlich redundant an zwei unabhängigen Phasen angeschlossen sind. Die reine manuelle Dokumentation umfasst je nach eingesetztem Softwaretool z.B. auch PDU Dokumentation, Asset Management usw.	Alle SNMP-fähigen Komponenten im Netzwerk.

Standpunkt

Nachhaltige Informationssicherheit: Ohne Druck geht es nicht

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

Seit letztem Jahr wird die Arbeit am neuen IT-Sicherheitsgesetz [1], das Betreiber kritischer Infrastrukturen betreffen wird, in der IT mit besonderer Spannung verfolgt. Im aktuellen Gesetzentwurf heißt es beispielsweise in § 8a unter anderem:

- „(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei ist der Stand der Technik zu berücksichtigen."

- „(3) Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Bei Sicherheitsmängeln kann das Bundesamt die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen."

Dies ist nichts anderes als die Forderung innerhalb eines gewissen Zeitraums ein sogenanntes Information Security Management System (ISMS) zu implementieren und dessen nachhaltige Umsetzung in regelmäßigen Abständen nachzuweisen.

Wesentliche Standards sind in diesem Zusammenhang neben den BSI-Standards

(inklusive der BSI IT-Grundschutz-Kataloge) insbesondere ISO 27001 aber auch COBIT.

Die Umsetzung von Sicherheitskonzepten nach solchen Standards ist zunächst ein aufwendiges Vorhaben, das bis zu einem akzeptablem Umsetzungsgrad durchaus mehrere Jahre in Anspruch nehmen kann. Besonders wichtig ist dabei, dass Sicherheitskonzepte im Rahmen eines geregelten Prozesses erstellt, umgesetzt und gepflegt werden, um mit dem Entwicklungstempo in der IT Schritt halten zu können. Kernelemente hierzu sind unter anderem:

- Schnittstellen zu anderen (IT-)Prozessen, z.B. Beschaffung, Change Management, Configuration Management, Incident Management, Compliance Management und Risikomanagement

- IT-Sicherheitsrisiko-Management für den Umgang mit nicht oder nur teilweise umgesetzten Maßnahmen

- Kennzahlen für die Informationssicherheit zur Erfolgsmessung und entsprechendes Reporting an das Management

- Nachhaltigkeit durch regelmäßige Prüfungen bzw. Audits erzwingen

Gerade der letzte Punkt ist von besonderer Bedeutung, denn ohne Druck wird früher oder später an entscheidenden Punkten in der Informationssicherheit gespart. Innerhalb von kürzester Zeit klaffen so Lücken in den Sicherheitskonzepten und Risikobewertungen, die letztendlich die gesamte bis dahin geleistete Anstrengung fragwürdig machen und zu einem entsprechend großen Schaden für die jeweilige Institution führen können.

Die notwendige regelmäßige Prüfung der Informationssicherheit kann zunächst z.B. von der IT-Revision wahrgenommen werden. Wenn das ISMS auf Basis von ISO 27001 oder der BSI-Standards aufgebaut wird, ist jedoch auch eine Zertifizierung möglich. Für die Aufrechterhaltung solcher Zertifikate sind regelmäßige Audits (z.B. in einem jährlichen Raster) und Re-Zertifizierungen (z.B. alle drei Jahre) erforderlich. Auf diese Weise entsteht ein natürlicher Druck zur Aktualisierung und Vervollständigung von Sicherheitskonzepten und von Risikobetrachtungen für die Bereiche, in denen Maßnahmen nicht angemessen umgesetzt werden konnten.

Es ist von daher eigentlich nicht überraschend, dass eine Zertifizierung im eben angesprochenen IT-Sicherheitsgesetz als Element eines Nachweises der Nachhaltigkeit deutlich genannt wird. Sie wird auch immer häufiger bei der Ausschreibung von Outsourcing-Vorhaben (inklusive Cloud Computing) gefordert. Letztendlich wird in der Zukunft ein anerkannter Nachweis der Qualität der Informationssicherheit ein Normalfall für das IT Business werden. Das IT-Sicherheitsgesetz ist hierzu als treibende Kraft ausgesprochen zu begrüßen!

[1] Siehe **https://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/12/bundeskabinett-beschlie%C3%9Ft-it-sicherheitsgesetz.html**

Sonderveranstaltung

Das neue IT-Sicherheitsgesetz - Was Unternehmen jetzt wissen müssen

22.06.15 in Bonn

Die ComConsult Akademie veranstaltet am 22.06.15 ihr neues Seminar "Das neue IT-Sicherheitsgesetz" in Bonn.

Die digitale Gesellschaft ist seit geraumer Zeit in jeglichen Bereichen eng mit IT-Systemen verknüpft. In Zeiten einer steigenden Bedrohungslage aus dem Cyberraum wird diese Verknüpfung allerdings zunehmend bedenklich. Ein Ausfall von IT-Systemen an neuralgischen Stellen kann gravierende Folgen für das öffentliche Leben haben. Die Bundesregierung hat den damit einhergehenden Handlungsbedarf erkannt und am 17. Dezember 2014 mit dem Beschluss eines sog. IT-Sicherheitsgesetzes reagiert. Mit einer Verabschiedung durch den Bundestag ist noch im Sommer 2015 zu rechnen. Ziel des Gesetzes ist es, deutsche IT-Systeme in neuralgischen Bereichen besonders abzusichern. Hierzu sollen Betreiber von sog. „kritischen Infrastrukturen“ künftig einem besonders strengen Pflichtenkatalog unterliegen. Das Seminar soll in Betracht kommende Unternehmen auf die künftige Rechtslage vorbereiten:

- Stand des Gesetzgebungsverfahrens
- Verhältnis zu europäischen Rechtsakten (NIS-Richtlinie)
- Adressatenkreise des Gesetzes

- Wegweisendes Merkmal der „kritische Infrastrukturen“
- Mindestanforderungen an kritische IT-Systeme
- Branchenstandards
- Nachweispflichten gegenüber der Aufsichtsbehörde (IT-Audits)
- Einrichtung von Alarmierungskontakten
- Meldepflichten von IT-Sicherheitsvorfällen
- Weitergehende Pflichten für besondere Unternehmen (z.B. Telekommunikation und Telemedien)
- Möglichkeiten der Aufsichtsbehörden und Rechtsfolgen/Sanktionen bei Verstößen

Die Veranstaltung soll kompakte und praktische Grundkenntnisse zu den Eckpunkten des von der Bundesregierung kürzlich verabschiedeten IT-Sicherheitsgesetzes vermitteln. Die Adressaten des neuen Gesetzes müssen mit erheblichen Neuerungen in ihrem IT-Betrieb rechnen. Betroffen sind Unternehmen mit IT-Systemen, deren Ausfall gravierende Folgen für das gesellschaftliche Leben haben kann und die daher als „Betreiber kritischer Infrastrukturen“ im Sinne des Gesetzesentwurfes einzuordnen sind.

Druch die Veranstaltung führen Sie Rechtsanwalt Dr. Jan Byok und Benjamin Wübbelt.

Der Fokus von Dr. Byok liegt in den Gebieten des öffentlichen Vergabe-, Vertrags- und Preisrechts, des ITK-Rechts, des Wettbewerbs- und Kartellrechts und in der juristischen Projektsteuerung.

Der Beratungsschwerpunkt von Herrn Wübbelt ist das Vergaberecht mit besonderem Bezug zum Informationstechnologie- und Datenschutzrecht.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Ich buche das Seminar
Das neue IT-Sicherheitsgesetz

☐ am 22.06.15 in Bonn
zum Preis von € 1.090,-- netto

☐ Bitte buchen Sie mir ein Hotelzimmer

vom_____ bis_____15

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Sonderveranstaltung

Sonderveranstaltung Das PSTN stirbt: Die neue Kommunikation mit SIP/IP 22.06.15 in Bonn

Die ComConsult Akademie veranstaltet am 22.06.15 ihre Sonderveranstaltung "Das PSTN stirbt: Die neue Kommunikation mit SIP/IP" in Bonn.

Die Deutsche Telekom hat angekündigt, bis 2018 das klassische PSTN-Netz, respektive analoge und ISDN-Anschlüsse abzuschalten. Dies betrifft alle Unternehmen, die weltweit kommunizieren wollen und müssen.

Abgesehen von den rein technischen Unterschieden: Leitungsvermittlung vs. Paketvermittlung, E.164 Telefonnummer vs. URI gibt es erhebliche funktionale Unterschiede, denn das Dienstspektrum bei All-IP wird erheblich umfangreicher sein als es im PSTN jemals der Fall war.

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

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

werden sollte und wie sich der SBC-Markt präsentiert.

Im Rahmen der Veranstaltung analysieren wir, wie der Wechsel von PSTN auf All-IP im Unternehmen verläuft. Wir zeigen auf, welche Funktionalität heute erreicht werden kann und mit welchem Aufwand für Anpassung und Fehlersuche zu rechnen ist. Wie gut ist die Unterstützung durch den Enterprise-Hersteller und Provider? Wie ändert sich Betriebs- und Kostenaufwand?

Nicht nur klassische PSTN-Provider werden diesen Markt unter sich aufteilen, sondern auch Kabelnetzbetreiber, Mobilfunkanbieter und ISPs werden ihr Dienstspektrum auf den All-IP Kommunikationsmarkt ausdehnen. Wir analysieren, wie das aktuelle Angebotsspektrum aussieht und welche Roadmap erkennbar ist.

Für die Provider ist All-IP kein Neuland, aber dennoch ein Technologiewechsel mit großen Herausforderungen. Wir diskutieren, welche Anforderungen ein Provider an den Enterprise-Kunden stellt, wie SLAs gestaltet werden können, wie ein typischer Projektablauf aussieht und mit welchen Problemen zu rechnen ist.

Der Ersatz von E.164 durch All-IP muss zu einer neuen globalen Kommunikations-Architektur führen. Stand heute gibt es kein einheitliches, standardisiertes SIP-Interconnect zum Provider-Peering oder als Meta-Ebene. Wir zeigen die aktuellen Standardisierungs-Vorschläge, Möglichkeiten und Trends auf, über die die Provider diskutieren.

Die Sonderveranstaltung zum Thema PSTN-Migration hin zu All-IP bietet topaktuelle Informationen 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.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Ich buche das Seminar
Das PSTN stirbt:
Die neue Kommunikation mit SIP/IP

☐ am 22.06.15 in Bonn
zum Preis von € 990,-- netto

☐ Bitte buchen Sie mir ein Hotelzimmer

vom_____ bis_____15

Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

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

Zweitthema

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle – Zusammenhänge, Perspektiven, Marktrelevanz (Teil 2)

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

Fortsetzung von Seite 1

Als Strategie ist klar erkennbar, ein einheitliches Northbound Interface festzulegen und vielfältige Southbound Interfaces zu unterstützen. Hier bewegt sich OpenDaylight diametral entgegengesetzt zur ONF (NBI = offen, SBI = eindeutig OpenFlow).

Somit lässt sich sagen, dass OpenDaylight klar einen breiteren Horizont als ONF SDN hat und sich hier die Grenzen zwischen SDN und NFV (Network Function Virtualisation) teilweise verwischen.

Stimmen aus dem Markt sagen: “OpenDaylight is quickly evolving into something formidable with good potential for mainstream relevancy” (Andrew Lerner, Gartner). Oder. “OpenDaylight is making steady progress cultivating a growing community of developers and users interested in adopting an open, common SDN controller platform” (Brad Casemore, IDC Research Director for Datacenter Networks).

Insgesamt hat OpenDaylight das Potenzial, sich an ONF vorbei zum de facto Standard entwickeln.

2. NFV - Network Function Virtualisation

Salopp gesagt steckt dahinter NFV die Vision, Netzwerke aus einer Ansammlung proprietärer Boxen zu einer Ansammlung von Software-Komponenten zu überführen, die auf Industriestandard-Hardware (COTS) laufen. Solche Netzkomponenten sind beispielsweise Router, Deep Packet Inspection (DPI) Komponenten, CDN Appliances, Firewalls, Load Balancer, NAT-Boxen, SBCs, WAN-Beschleuniger, Controller für Mobilnetz-Basisstationen, Mobilnetz Packet Gateways, Test- und Monitoring Komponenten usw. Bei den aufgeführten Komponenten drängt sich der Gedanke auf, dass NFV sich mit Layer-4 bis Layer-7 Diensten befasst. Dies ist aktuell tatsächlich der Fokus, grundsätzlich könnte NFV aber auch niedrigere Netzwerk-Schichten implementieren (natürlich nicht das Physical Layer …).

NFV will konventionelle Netzwerke weg von proprietären Boxen und hin zu Software-Komponenten überführen, die auf Industriestandard-Hardware (COTS) laufen.

Für NFV gilt das Motto: Cores haben wir reichlich, und Alles ist darauf lauffähig; warum also nicht auch Netzwerk-Funktionen? So weit so gut – oder auch nicht. Warum kam nicht schon früher Jemand auf die Idee NFV? Weil es erst mit den neuesten Entwicklungen Standardhardware mit ausreichend Rechenleistung, ausreichend viel und ausreichend schnellem Cache Speicher gibt. Damit hat sich die Bandbreite, die die Peripherie-Chips einer CPU unterstützen, drastisch erhöht.

Grundsätzlich gilt für Netzwerke: die Con-

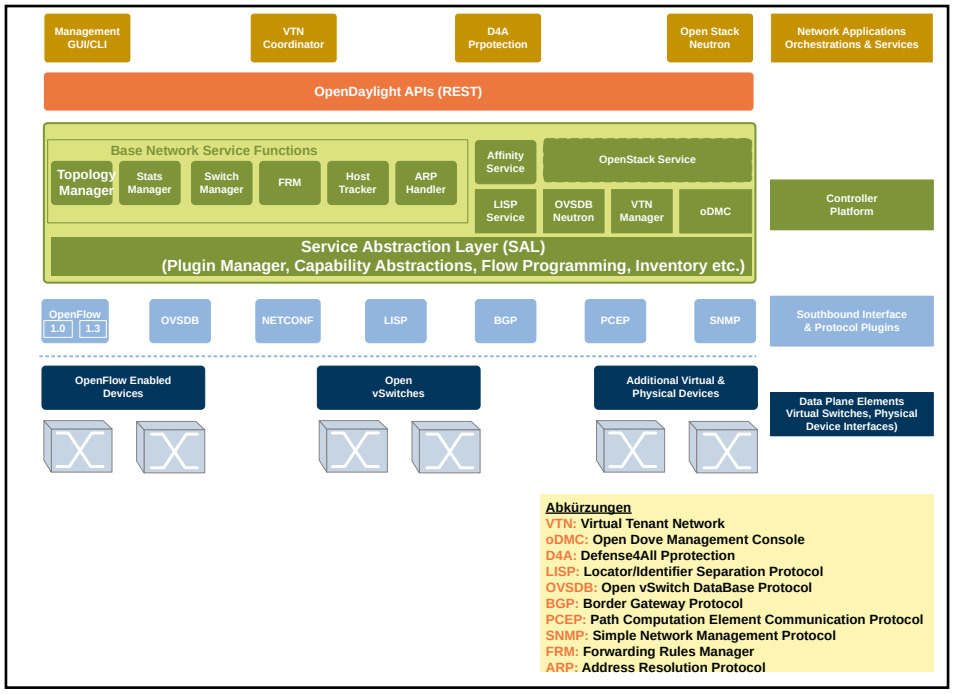

Abbildung 1.8: OpenDaylight Hydrogen Architektur

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle – Zusammenhänge, Perspektiven, Marktrelevanz - Teil 2

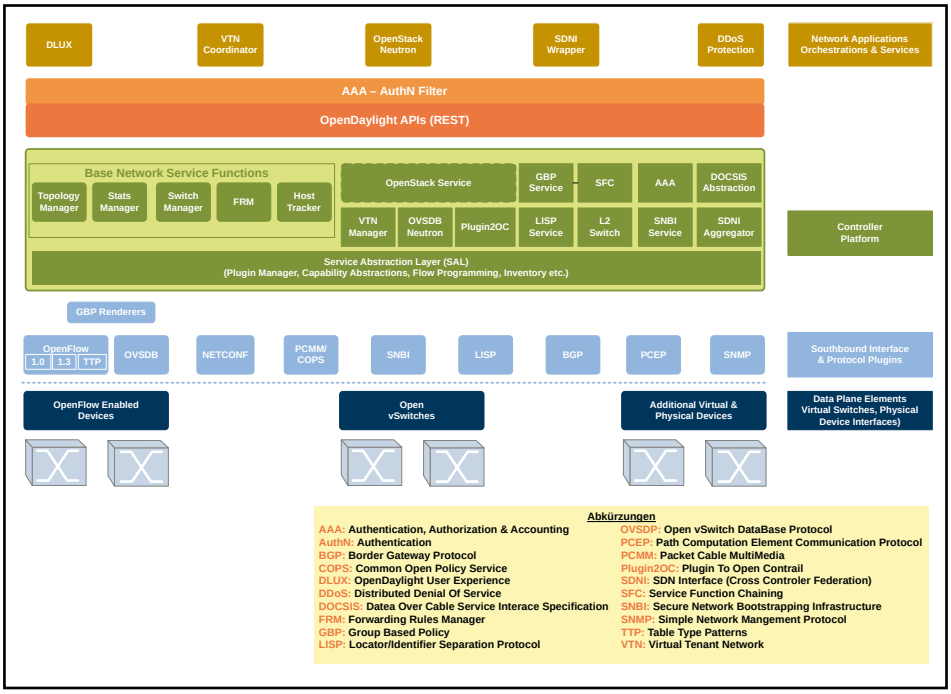

Abbildung 1.9: OpenDaylight Helium Architektur

trol Plane beschäftigt sich mit Routing- oder Signalisierungs-Protokollen, Einrichtung oder Herunterfahren von Sessions, Authentisierung und ähnlichem. Sie ist CPU-intensiv, benötigt aber wenig Bandbreite. Die Data Plane beschäftigt sich mit der Weiterleitung der realen Verkehrslast, diese ist bandbreitenintensiv, benötigt aber wenig CPU-Leistung. Ein Beispiel: Das Aufsetzen eines Telefonats in einem IMS Netzwerk benötigt typischerweise 10 bis 15 SIP Signalisierungs-Pakete aufseiten der Control Plane, während 3 Minuten Telefongespräch (Media Stream) den Austausch von 36.000 RTP Paketen erfordern. Control Planes arbeiten heute schon mit General Purpose CPUs, die Data Plane wird bislang dagegen vielfach aus Leistungsgründen mit proprietärer Hardware bestückt.

Im Bereich Network Function Virtualisation gibt es mehrere Aktivitäten. Das zur Zeit aktivste Standardisierungs-Gremium ist die ETSI mit ihrer Industry Specification Group NFV, die sich im Januar 2013 konstituiert hat. Hier wurden unter Mitarbeit von weltweit ca. 230+ Unternehmen eine Reihe Technische Spezifikationen verabschiedet, die Einsatz-Szenarien, Architektur und verschiedene Unterbereiche beschreiben. Mit Phase 1 der Arbeitsgruppe wurde die Basis-Arbeit abgeschlossen, in der jetzigen Phase 2 sollen Spezifikationen zur Implementierung erarbeitet werden.

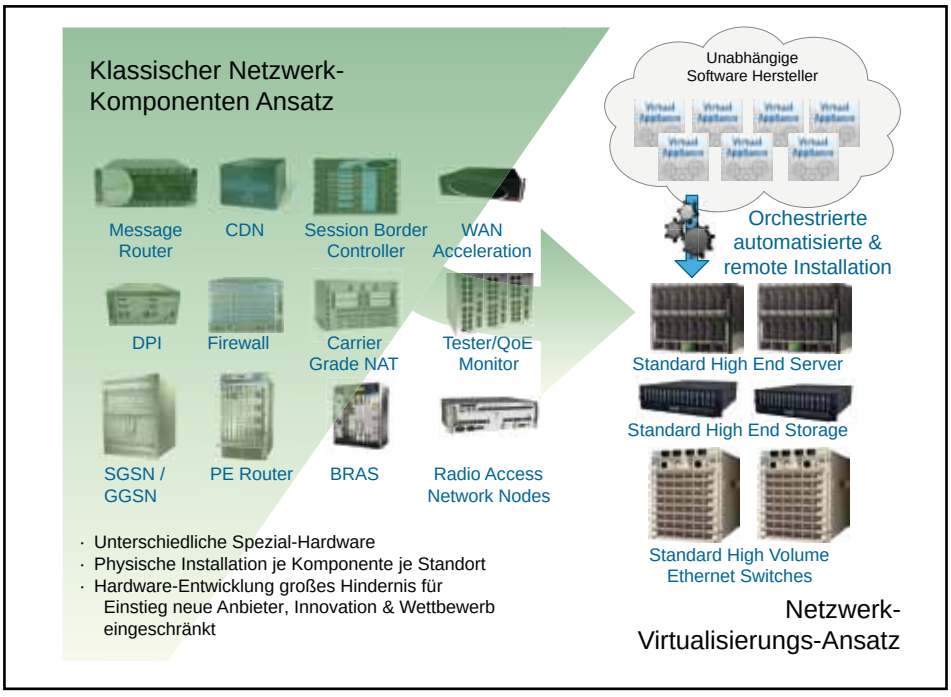

Abbildung 2.1: Vision von Network Functions Virtualisation

Im September 2014 hat die Linux Foundation ein Projekt "Open Platform for NFV" aufgelegt (OPNFV), das auf der Basis der ETSI-Spezifikationen eine NFV Referenz-Plattform entwickeln will.

Bei der IETF gibt es eine Arbeitsgruppe SFC zum Thema Service Function Chaining, die eine ähnliche Richtung wie die VNF-Forwarding Graphen der ETSI NFV Arbeitsgruppe hat.

In diesem Beitrag wird NFV in Anlehnung an die ETSI Spezifikationen betrachtet.

NFV hat das Ziel, Netzwerk-Architekturen und Netzwerk-Betrieb so zu transformieren, dass das bislang sehr vielfältige Netzwerk-Equipment durch Standard IT Virtualisierungs-Technologien auf den Einsatz von Industriestandard Hochleistungs-Servern, Industriestandard Switches und Industriestandard Speicher konsolidiert wird, wie Abbildung 2.1 zeigt.

Im Zuge der Netzwerkarchitektur-Transformation werden Netzwerkfunktionen in Software implementiert, die auf Industriestandard Serverhardware lauffähig ist, der Netzwerkbetrieb wird dahingehend transformiert, dass diese Software je nach aktuellem Bedarf dynamisch an verschiedene Lokationen migrieren oder in verschiedenen Lokationen instanziiert werden kann, ohne dass Irgendjemand hierfür physisch neue Komponenten / neues Equipment installieren und in Betrieb nehmen muss. Somit ist NFV insbesondere auf Cloud Umgebungen fokussiert. Ziel ist über die Architektur hinaus die Nutzung von IT Standardprozessen für das gesamte Netzwerk-Lifecycle Management, insbesondere auch durch den Einsatz entsprechend an NFV angepasste OSS/BSS Tools.

In der Praxis besteht eine NFV Lösung in der Regel aus drei Kernelementen: COTS Hardware, einem Hypervisor wie KVM oder ESXi, einer Cloud Management Lösung wie OpenStack oder VMware vSphere.

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle – Zusammenhänge, Perspektiven, Marktrelevanz - Teil 2

Vorteile von und Anforderungen an NFV
Durch die Standardisierung von NFV, den Einsatz von Standard-Hardware und Software mit standardisierten Schnittstellen verspricht sich die NFV-Gemeinde folgende Vorteile:

- Bessere Kosteneffizienz (soll heißen: niedrigere Kosten)
- Mehr Flexibilität, Netzfunktionen den vorhandenen Hardware-Ressourcen zuzuweisen
- Bessere Skalierungs-Möglichkeiten hinsichtlich Scale In/Out, Scale Up/Down
- Dynamische Bereitstellung durch bedarfsgerechte bzw. an die Verkehrslast angepasste Instanziierung von Netzwerk-Diensten / -Funktionen
- Schnelle Entwicklung neuer Dienste, kleine Neuerungs-Zyklen
- Bessere und leichtere Testmöglichkeiten durch die Implementierung von Sandbox-Umgebungen
- Verbesserte operative Effizienz (soll heißen: Einsparung von Head Counts)
- Niedrigerer Energieverbrauch (schon mal neben einem Cisco NX7800 gestanden ??)
- Standardisierte und offene Schnittstellen zwischen virtualisierten Netzwerk-Funktionen und der Infrastruktur sowie dem assoziierten Management; so soll ein breites Multivendor Ecosystem entstehen

Hierbei werden nach ETSI folgende Anforderungen an eine NFV-Lösung gestellt (Dokument NV 004: "Network Functions Virtualisation (NFV); Virtualisation Requirements):

- Portierbarkeit, das bedeutet Laden, Ausführen und Migrieren von Software Funktionen über verschiedene, aber standardisierte Data Center hinweg
- Performance, das bedeutet die Spezifikation von Funktionen, mit deren Hilfe sich die Infrastruktur-Anforderungen für spezifische Leistungsziele und Software Funktionen beschreiben lassen
- Management und Orchestrierung, um Infrastruktur Ressourcen während des gesamten Lifecycle managen zu können
- Elastizität: Funktionen, die je nach Verkehrsaufkommen ein einfaches Scale In/Out oder Scale Up/Down von Hardware Ressourcen ermöglichen
- Sicherheit: Analyse der Virtualisierungs-Umgebung hinsichtlich spezifischer Angriffsmöglichkeiten, die sich aus der Virtualisierung neu ergeben
- Robustheit und Stabilität: Anforderungen, um weitestgehende Unterbrechungsfreiheit erreichen zu können, wobei insbesondere keine der Netzwerk-Funktionen ein Single Point of Failure sein soll
- Service-Kontinuität: Anforderungen für eine kontinuierliche Diensterbringung, die zu den vereinbarten SLAs konform ist
- Berieb: Anforderungen an Automatisierung und operative Betriebsaspekte wie Kapazitäts-anpassungen, Software Upgrades oder Fehlerbehebung / Wiederanlauf
- Energie-Effizienz: technische Anforderungen zur Minimierung des Energiebedarfs
- Migration und Koexistenz: Anforderungen an eine Migration heutiger Architekturen in eine NFV Umgebung und Koexistenz von non-NFV und NFV Umgebungen

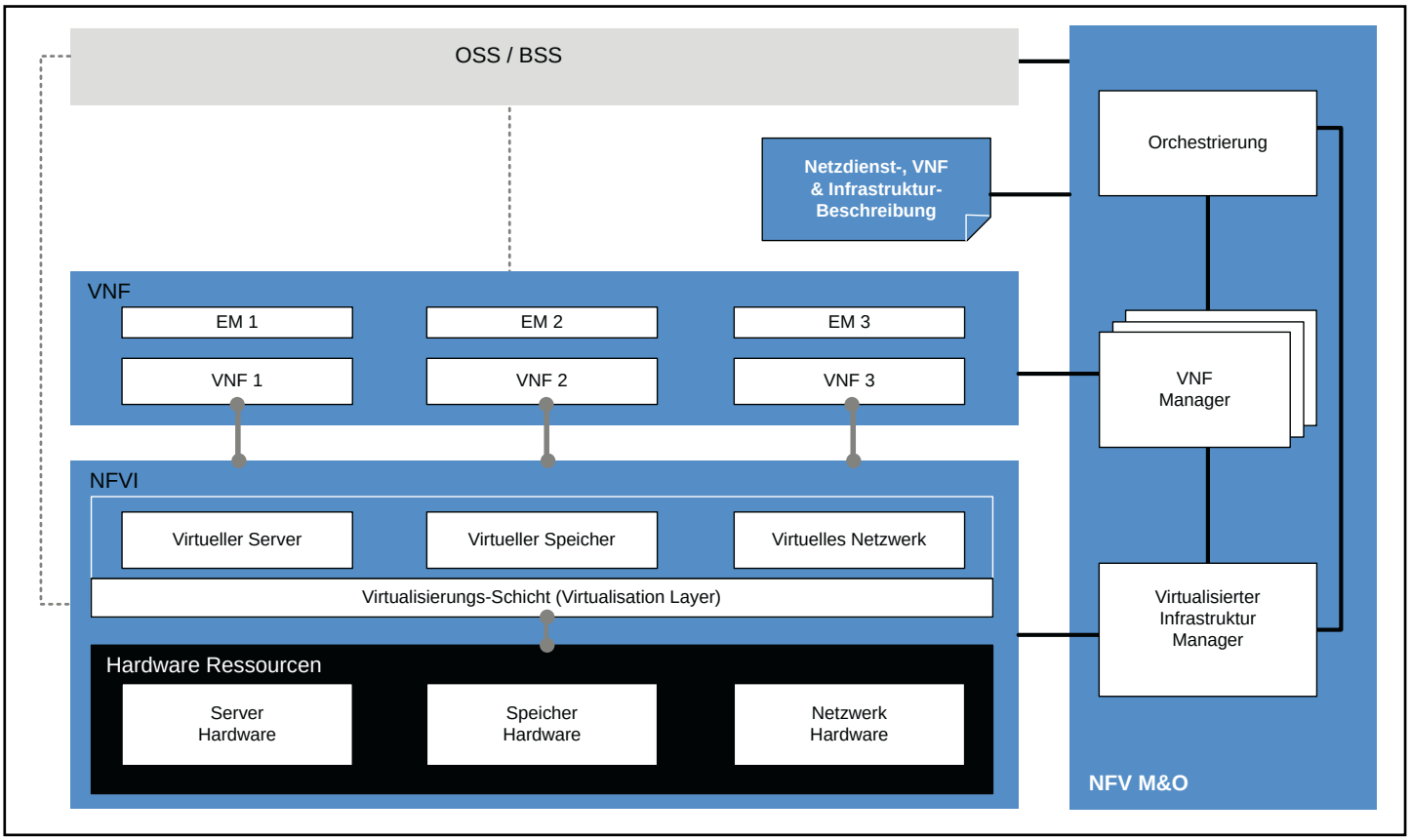

Abbildung 2.2: NFV Architektur-Übersicht (NFV Architectural Framework)

2.1 NFV Architektur

In nicht-virtualisierten Netzen sind Netzwerk-Funktionen (NFs) als Kombination herstellerspezifischer Hard- und Software implementiert. Diese werden vielfach Netzknoten (NN Network Node) oder Netzwerk-Element (NE) genannt. Insbesondere im Providerumfeld will man im Vergleich zu heutigen Hardware-Netzen folgende Verbesserungen erreichen:

- Entkopplung der Hardware von der Software, so dass beide unabhängig voneinander weiterentwickelt werden können
- Flexibles Deployment: Entkopplung der Software von der Hardware ermöglicht Neuzuweisung von Ressourcen und Ressourcen-Sharing bei Ressourcen-Pools. Die aktuelle Instanziierung einer Software kann zudem besser automatisiert werden
- Dynamischer Betrieb: Da eine VNF-Software bei Bedarf instanziierbar ist, ergeben sich bessere und granularere Skalierungs-Möglichkeiten, abhängig von der jeweiligen Verkehrslast

Network Function Virtualisation soll diese Verbesserungen bewirken. Die NFV-Architekturübersicht in Abbildung 2.2 zeigt die verschiedenen Funktionsblöcke von NFV auf.

Die Architektur besteht aus zwei funktionalen Blöcken: den virtualisierten Netzwerk-Funktionen (NFVs) und der NFV Infrastruktur (NFVI). Nebengeordnet wird ein Mangement- und Orchestrierungs-Block definiert.

NFVI Block

Der Block NFV Infrastruktur (Network Functions Virtualisation Infrastructure) deckt die Gesamtheit der Hardware- und Software-Komponenten ab, aus denen eine VNF Umgebung aufgebaut ist, in der VNFs ausgerollt, ausgeführt und verwaltet werden. Er stellt die virtuellen Ressourcen bereit, die zur Ausführung der Virtualised Network Functions erforderlich sind. Er besteht grundsätzlich aus drei Sub-Schichten: Virtuelle Komponenten, Virtualisierungs-Schicht und Hardware Ressourcen.

Naturgemäß ist die Virtualisierungs-Schicht das Kernstück des NFVI Blocks. Sie ist insbesondere für drei Funktionsbereiche verantwortlich:

- Abstraktion und logische Partitionierung der physischen Ressourcen
- Software, die eine NFV implementiert, dazu befähigen, die unterliegende NFVI zu nutzen
- Bereitstellung von virtualisierten Ressourcen für die VNF, die die VNF zur Ausführung benötigt

Das NFV Architektur Framework gibt keine bestimmte Virtualisierungs-Layer Lösung vor. Stattdessen wird erwartet, dass eine vorhandene Lösung Standard-Features und Referenzpunkte (Execution Reference Points) in Richtung VNFs und Hardware nutzt. Nur im Ausnahmefall sollten VMs aus Leistungsgründen direkten Hardwarezugriff erhalten.

Die Hardware Ressourcen beinhalten COTS Hardware für Server (Compute), Speicher (NAS und DAS Storage) und Netzwerk und soweit erforderlich Hardware-Beschleuniger. Das Virtualisation Layer ist eine zwischengeschaltete Software-Ebene, die die Virtualisierung leistet und von der unterliegenden Hardware abstrahiert und so die Instanziierung virtueller Rechen, Speicher- und Netzelemente ermöglicht.

Die NFVI kann sich über mehrere Lokationen (NFVI-PoPs) erstrecken. In diesem Fall wird die Netzwerk-Infrastruktur, die diese Lokationen verbindet, als Teil der NFVI betrachtet.

Soweit es sich um die Virtualisierung von Netzressourcen handelt, wird die Hardware durch die Virtualisierungs-Schicht (Virtualisation Layer) abstrahiert, um virtuelle Netzverbindungen (Wege) zu realisieren, die die Konnektivität zwischen einer VM und einer VNF oder zwischen VNF Instanzen herstellen. Hierfür werden typischerweise Netzwerk-Overlay Verfahren eingesetzt, die die Logik von der Physik isolieren. Bekannte und weniger bekannte Vertreter sind hier VLAN, SPBM, VPLS, VXLAN, NVGRE sowie zukünftig VXLAN GPE, GENEVE und NSH.

VNF Block

Der VNF (Virtualised Network Function) Block ist die Software-Implementierung von Netzwerk-Funktionen, die NFVI unterstützen, d.h. auf NFVI aufsetzen können. Eine VNF kann aus mehreren internen Komponenten zusammengesetzt sein (Composition) und so über mehrere VMs verteilt implementiert werden. Eine oder mehrere VNFs können zusammen mit einem Element Manger (EM) implementiert sein, soweit dies für spezielle Besonderheiten dieser VNF(s) erforderlich ist. Die VNF hat Dienst-Attribute wie Zuverlässigkeit, Verfügbarkeit, Manageabarkeit, Sicherheit und Leistung; bei einer Composite VNF ergeben sich diese Attribute aus der Summer der Attribute der einzelnen Unter-VNFs.

Eine Server- oder Speicher-Ressource für eine VNF wird typischerweise als VM oder verteilt auf mehrere VMs implementiert, zur Virtualisierung wird dann der entsprechende Hypervisor genutzt.

Die VNFs entsprechen den heutigen Netzknoten, sind dann aber eine reine Software-Implementierung. Beispiele für VNFs sind Netzwerk Elemente des 3GPP Evolved Packet Core (EPC) wie Mobility Mangement Entity (MME), Serving Gateway (SGW), Packet Data Network Gateway (PGW), Residental Gateway (RGW), DHCP Server, Firewall e.a.

Aus Sicht einer VNF stellen sich Virtualisierungs-Layer und Hardware-Ressourcen wie eine Einheit dar, die der VNF die gewünschten Ressourcen zur Verfügung stellt.

Insgesamt wird unterstellt, dass das funktionale Verhalten und die externen operationalen Schnittstellen einer physischen Netzwerkfunktion (PNF) und einer VNF identisch sind.

MANO Block
Das NFV Management & Orchestrierung (M&O, MANO) ist ein vertikal VNF- und NFVI-übergreifender flankierender Architekturblock. Er deckt die Orchestrierung und das Lifecycle Management der VNFs sowie der physischen und Software Ressourcen ab, die die Infrastruktur-Virtualisierung unterstützen. MANO fokussiert sich dabei auf die virtualisierungs-spezifischen Management-Aufgaben des NFV Frameworks. Darüber hinaus interagiert es mit den OSS/BSS Tools zur Integration in die allgemeine Mangement-Landschaft. Der M&O Block ist analog zu den Funktionsblöcken hierarchisch unterteilt in eine Orchestrierung, darunter einen oder mehrere VNF Manager für die Handhabung der VNFs sowie darunter einen Virtualisierten Infrastruktur Manager für die Handhabung virtualisierter Ressourcen.

Das NFV Framework ermöglicht die dynamische Erstellung und das Management von VNF Instanzen und legt die Beziehungen zwischen VNF Instanzen hinsichtlich Daten, Kontrolle, Management, Abhängigkeiten und anderer Attribute fest. Hierbei werden drei Perspektiven berücksichtigt:

- die Deployment / Onboard Perspektive, wobei der Kontext üblicherweise eine VM ist
- die Softwarepaket-Perspektive (wobei das Software-Paket von einem Hersteller entwickelt wurde), bei der der Kontext verschiedene miteinander verbundene VMs sind; hierfür gibt es ein Deployment Template, das ihre Attribute beschreibt
- die Operator Perspektive, bei der der Kontext Betrieb und Management einer VNF sind, die in Form eines Software-Pakets vom Hersteller erworben wurde.

In allen genannten Kontexten gibt es jedoch mindestens folgende Relationen zwischen VNFs:

- Der VNF Forwarding Graph (VNF-FG) behandelt den Fall, in dem Netzwerk-Konnektivität zwischen VNFs spezifiziert wird, zum Beispiel eine VNF-Kette auf dem Weg zur Webserver-Ebene – wie Firewall, NAT, Load Balancer – und wird typischerweise als Dienstkette (Service Chain) beschrieben

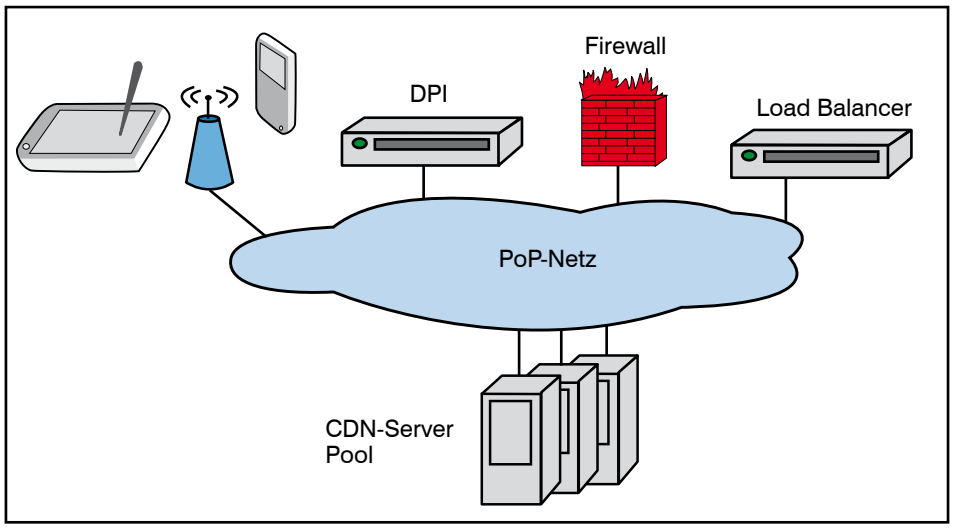

Abbildung 2.3: Ende-zu-Ende Netzwerk Dienst für eine Smartphone

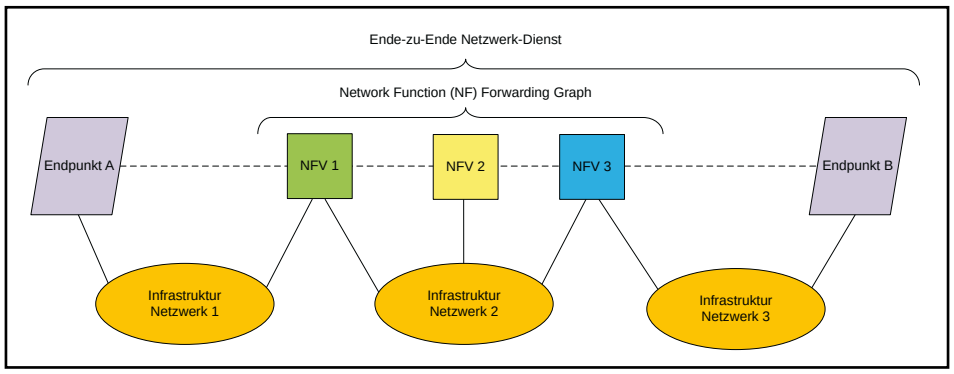

Abbildung 2.4: Graph-Darstellung eines Ende-zu-Ende Netzwerk Dienstes

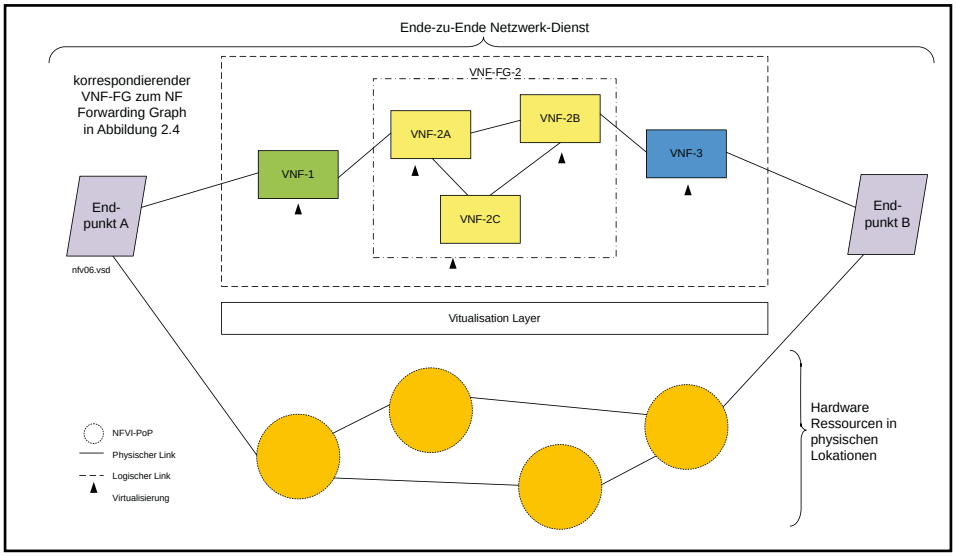

Abbildung 2.5: Graph-Darstellung eines Ende-zu-Ende Netzwerk Dienstes mit NFV

- Das VNF Set behandelt den Fall, bei dem zwischen verschiedenen VNFs keine Netzwerk-Konnektivität spezifiziert ist, z.B. ein Web Server Pool oder voneinander unabhängige Gateways im Home Network Bereich

In einem VNF-FG werden die VNF-Sequenzen, die von einem Verkehrsfluss durchlaufen werden müssen, entweder von vorneherein (per Design) festgelegt oder werden bei der Ausführung (runtime) festgelegt (z.B. nach Erhalt von

Routing Nachrichten von mehreren Call Servern).

Netzwerk-Dienste in NFV

Ein Netzwerk-Dienst kann architekturmäßig als ein Weiterleitungs-Graph (FG) von Netzwerk-Funktionen (NFs) betrachtet werden, die durch die unterliegende Netzwerk-Infrastruktur miteinander verbunden sind. Jede einzelne NF trägt zur Gesamtfunktion des Netzwerk-Dienstes bei. Somit ist der Ende-zu-Ende Dienst eine Kombination der einzelnen funktionalen Blöcke, die Einzel-NFs, zusammengesetzte NFs und NF-Gruppen sein können. Ein NF-Forwarding Graph kann Netzknoten beinhalten, die durch logische, unidirektionale, bidirektionale oder Broadcast Links angebunden sind. In jedem Fall enthält er an beiden Enden die Endsysteme, zwischen denen der Dienst geleistet wird (End Node). Eine einfache Ausprägung ist eine Kette von Netzwerk-Funktionen (Service Chain), wie zum Beispiel bei einem Ende-zu-Ende Dienst zwischen einem Smartphone und einem CDN-Server Pool, der über ein Wireless Netz, eine DPI-Komponente, einen Firewall und einen Load Balancer verläuft (siehe Abbildung 2.3). In Abbildung 2.4 entspricht End Point A dem Smartphone, NF1 dem DPI, NF2 dem Firewall, NF3 dem Load Balancer und End Point B dem CDN-Server Pool.

Mit NFV stellt sich nun der Ende-zu-Ende Dienst und sein zugehöriger Forwarding Graph dar, wie in Abbildung 2.5 gezeigt: Ressourcen für Server, Speicher und Netzwerk sind in den NFVI-PoPs enthalten. Die virtualisierten Netzwerk-Funktionen laufen oberhalb des Virtualisation-Layer ab, das zur VNFI gehört, was durch den Pfeil "Virtualisierung" verdeutlicht wird. Der zu Abbildung 2.4 passende VNF-FG stellt sich nun dar wie in Abbildung 2.5. VNF-1 entspricht dem DPI, VNF-2 ist eine aus VNF-2A, VNF-2B und VNF-2C zusammengesetzte VNF und entspricht dem Firewall, VNF-3 entspricht dem Load Balancer. Im Unterschied zu den NFs aus Abbildung 2.4 laufen die VNFs und ihre Infrastruktur jedoch auf offenen Standards (Norm, Industrie- oder de facto Standard).

Ein wichtiger Punkt an dieser Stelle: für die Ende-zu-Ende Perspektive ist die exakte physische Lokation einer VNF-Instanz nicht mehr sichtbar. Dadurch wird es möglich, eine VNF auf verschiedenen physischen Ressourcen zu implementieren, die auch geografisch getrennt liegen können. Alles ist möglich, solange die Leistung und Policy-Einschränkungen des Ende-zu-Ende Dienstes eingehalten werden.

Eine Ausnahme bilden spezifische Policy-Garantien wie zum Beispiel die Lokations-Bindung (location awareness) eines CDN-Knotens, hier kann natürlich keine geografische Unabhängigkeit gegeben sein.

NFV Schnittstellen und Referenzpunkte

Die Schnittstellen zwischen den einzelnen Funktionsblöcken der NFV Referenzarchitektur sind in drei Kategorien unterteilt, fokussieren sich jedoch auf das Management:

- Ausführungs-Referenzpunkte: Vn-Nf, Vi-Ha
- Haupt-Referenzpunkte zwischen Funktionsblöcken und Management so-

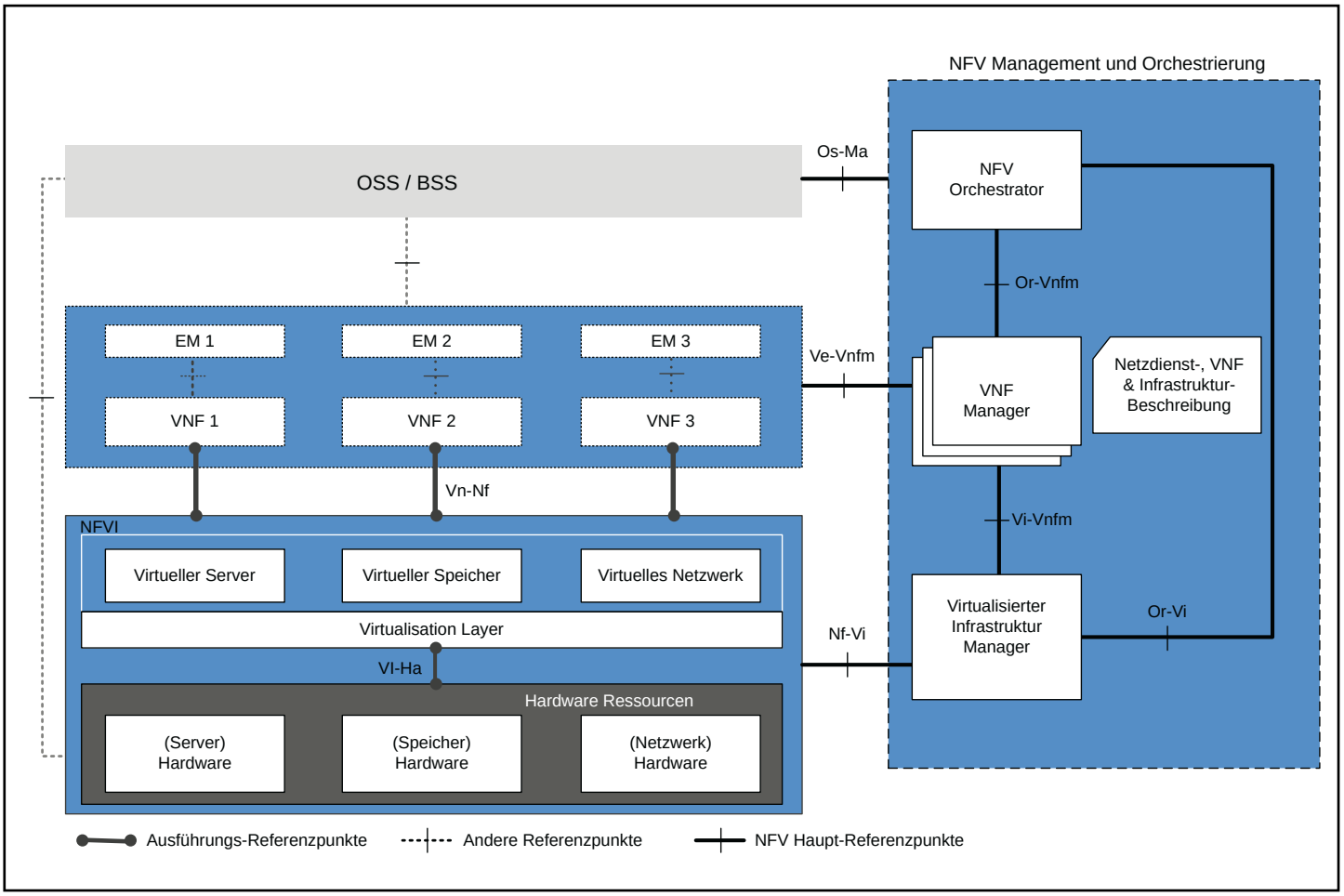

Abbildung 2.6: Schnittstellen zwischen den Architektur-Blöcken von NFV

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle – Zusammenhänge, Perspektiven, Marktrelevanz - Teil 2

wie zwischen den Management-Subblöcken: Os-Ma, Or-Vi, Ve-Vnfm, Nf-Vi, Or-Vnfm, Vi-Vnfm

- weitere Referenzpunkte (zukünftige Erweiterungen)

Sie werden nachfolgend in der Reihenfolge der Kategorien beschrieben.

Der Ausführungs-Referenzpunkt **Vn-Nf** repräsentiert die Ausführungsumgebung, die einer VNF von der NFV Infrastruktur zur Verfügung gestellt wird. Er setzt kein spezifisches Kontrollprotokoll voraus und stellt für die NFV einen hardware-unabhängigen Lifecycle, Leistungs- und Portierungs-Anforderungen sicher.

Der Ausführungs-Referenzpunkt **Vl-Ha** ist die Schnittstelle zwischen Virtualisierungs-Schicht und Hardware-Ressourcen. Er realisiert die (konkret hardwarebezogene) Ausführungsumgebung für VNFs und sammelt relevante Status-Informationen der Hardware Ressourcen, um so VNFs managen zu können, ohne von einer bestimmten Hardware Plattform abhängig zu sein.

Der Referenzpunkt **Os-Ma** ist die Schnittstelle zwischen den allgemeinen OSS/BSS Tools und der NFV Orchestrierung. Er wird für Anforderungen des Lifecycle Mangement für Netzwerk-Dienste und VNFs genutzt; zur Weiterleitung von NFV Statusinformationen; Informationsaustausch im Policy Management und der Datenanalyse, Weiterleitung entsprechender NFV-bezogener Accounting und Nutzungs-Werte sowie zum Austausch von Kapazitäts- und Inventar-Management-Informationen.

Der Referenzpunkt **Or-Vnfm** ist die Schnittstelle zwischen NFV Orchestrierung und dem oder den VNF Manager(n). Die Orchestrierung stellt ressourcen-spezifische Requests wie Autorisierung, Validierung, Reservierung und Bereitstellung, die der VNF Manager bedient. Der Orchestrator sendet Konfigurationsinformationen an den VNF Manager, so dass dieser die VNFs so konfigurieren kann, dass sie dem VNF Forwarding Graph entsprechen. Der VNF Manager sammelt Statusinformationen der VNFs, die für das Lifecycle Management erforderlich sind, und sendet sie an die Orchestrierung.

Der Referenzpunkt **Vi-Vnfm** ist die Schnittstelle zwischen dem oder den VNF Manager(n) und dem Virtualisierten Infrastruktur-Manager. Hier stellt der VNF Manager Requests für die Ressourcen-Bereitstellung, die der Virtualisierte Infrastruktur-Manager bedient. Zudem erfolgt der Austausch von Konfigurations- und Status-Informationen der virtualisierten Hardware.

Der Referenzpunkt **Or-Vi** ist die Schnittstelle zwischen NFV Orchestrierung und dem Virtualisierten Infrastruktur-Manager. Über diesen Referenzpunkt fordert die NFV Orchestrierung direkt, ohne Beteiligung eines VNF-Managers, Ressourcen-Reservierung oder Ressourcen-Bereitstellung vom Virtualisierten Infrastruktur-Manager an und tauscht Konfigurations- und Statusinformationen über virtualisierte Hardware Ressourcen aus.

Der Referenzpunkt **Ve-Vnfm** ist die Schnittstelle zwischen dem oder den VNF Manager(n) und VNF oder Element Manager (EM). Hierüber werden Lifecycle Management Anforderungen, Konfigurations-Informationen und Status-Informationen übermittelt.

Der Referenzpunkt **Nf-Vi** ist die Schnittstelle zwischen NFVI und dem Virtualisierten Infrastruktur-Manager. Über diesen Referenzpunkt erfolgt die spezifische Ressourcenzuweisung als Folge der (von oben durchgereichten) Bereitstellungs-Requests. Zudem werden Konfigurations-Informationen zur Hardware und Status-Informationen zur Hardware und zu virtualisierten Ressourcen übermittelt.

Im nächsten Teil lesen Sie:
- NFV und SDN
- NFV Einsatzszenarien
- Marktrelevanz von SDN und NFV und Fazit
- Overlay Protokolle für SDN und NFV

Abkürzungen

AR	Access Router
CDN	Content Delivery Network
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
CSP	Cloud Service Provider
DPI	Deep Packet Inspection
EANTC	European Advanced Networking Test Center
E-CPE	Enterprise Customer Premises Equipment
ETSI	European Telecommunications Standards Institute
FW	Firewall
IaaS	Infrastructure as a Service
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
IT	Informations-Technologie
ITU-T	International Telecommunications Union for Telecommunication Standards
LAN	Local Area Network
LB	Load Balancer
LISP	Locator / ID Separation Protocol
M&O	Management and Orchestration
MAC	Media Access Control
MAN	Metropolitan Area Network
NFV	Network Function Virtualisation
NFVI	NFV Infrastructure
NG-FW	NextGen Firewall
NIST	National Institute of Standards and Technology
PE	Provider Edge
PoP	Point of Presence
SDN	Software-Defined Networking
SLA	Service Level Agreement
SPoF	Single Point of Failure
vCDN	virtuelles CDN
VNF	Virtual Network Function
VNFaaS	VNF as a Service
VNP	Virtual Network Platform
VNPaaS	VNP as a Service
WOC	WAN optimization Controller

Links

www.etsi.org/technologies-clusters/technologies/nfv
www.opendaylight.org/project/technical-overview
www.opennetworking.org

Literatur

- ETSI: Network Functions Virtualisation (NFV) White Paper 3, 10/2014
- ETSI: Network Functions Virtualisation (NFV) White Paper 2, 10/2013
- ETSI: GS NFV 001 (10/2013) Network Functions Virtualisation (NFV); Use Cases
- ETSI: GS NFV 002 (12/2014) Network Functions Virtualisation (NFV); Architectural Framework
- ETSI: GS NFV-INF 001 (01/2015) Network Functions Virtualisation (NFV); Infrastructure Overwiew
- ETSI: GS NFV-INF 005 (12/2014) Network Functions Virtualisation (NFV); Infrastructure; Network Domain
- ONF: OpenFlow Switch Specification 1.5.0, Dezember 2014
- ONF: OpenFlow Switch Specification 1.3.0, April 2012
- ONF: North Bound Interface Working Group (NBI-WG) Charter (06/2013)
- ONF: OF-CONFIG 1.1 OpenFlow Management and Configuration Protocol
- OpenDayligt: Hydrogen Diagramm
- OpenDayligt: Helium Diagramm
- SDxCentral: What ist NFV – Network Functions Virtualization?

Lesen Sie auch den Artikel aus dem Netzwerk Insider Oktober 2012 "Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?" von Petra Borowka-Gatzweiler.

ComConsult Veranstaltungskalender

TCP/IP-Netze erfolgreich betreiben, 13.04. - 15.04.15 in Düsseldorf

Garantietermin

IP ist die Grundlage jeden Netzes. Die Protokolle TCP und UDP bilden die Basis jeder Anwendungskommunikation. Es werden zudem Kenntnisse über Routingprotokolle, DHCP, DNS benötigt. Dieses Seminar vermittelt praxisnah das notwenige Wissen.

Preis: € 1.890,-- netto

SIP - Basis-Technologie der IP-Telefonie, 13.04. - 15.04.15 in Düsseldorf

Garantietermin

Ziel der Schulung ist die Erläuterung von SIP als den Schlüssel für eine offene, leistungsfähige und Kosten-optimale Kommunikations-Lösung. Es umfasst nahezu alle Dienste, die wir heute für UC benötigen: Sprache, Video, Daten und Präsenz. Lernen Sie was SIP leistet, worin sich wesentliche Hersteller-Lösungen unterscheiden und wie sie das Beste aus beiden Welten zukunftsorientiert nach Ihrem Bedarf optimieren.

Preis: € 1.890,-- netto

IT-Projektmanagement Kompaktseminar, 20.04. - 22.04.15 in Königswinter

Garantietermin

Seminar über Projektmanagement in der IT. Es wird speziell auf die Anforderungen und Herausforderungen von IT-Projekten eingegangen. Lernen Sie wie Sie Projekte sauber aufsetzen und überwachen und mit welchen Methoden und Hilfsmitteln Sie die Termineinhaltung sicherstellen können.

Preis: € 1.890,-- netto

IP-Wissen für TK-Mitarbeiter, 27.04. - 28.04.15 in Nürnberg

Garantietermin

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

Preis: € 1.590,-- netto

Virtualisierungstechnologien in der Analyse, 27.04. - 28.04.15 in Nürnberg

Garantietermin

Im Zuge stetig zunehmender Konsolidierung ist Virtualisierung längst zum Standard in jedem Rechenzentrum geworden. Doch der Blick hinter die Kulissen offenbart einen rapide wachsenden Komplexitätsgrad, dessen Beherrschung ein tieferes Verständnis dieser Technologie erfordert. In diesem Seminar werden die Zusammenhänge zwischen Server, Netzwerk und Storage im Umfeld der Virtualisierung analysiert.

Preis: € 1.590,-- netto

Verkabelungssysteme für Lokale Netze, alles standardisiert, alles klar?, 04.05.15 in Bonn

Garantietermin

Dieses Seminar erklärt praxisnah und herstellerneutral wie Sie hohe Qualität, Verfügbarkeit und lange Nutzbarkeit bei der Planung und im Betrieb einer Verkabelungs-Lösung erreichen. Die Bausteine einer Verkabelung werden vorgestellt und zu einem handhabbaren Gesamtsystem kombiniert. Lernen Sie wo sich gute von schlechten Lösungen unterscheiden. Dabei werden die Normen diskutiert und die praktische Handhabung der Normungsvorgaben erklärt. Produktbewertungen wechseln sich mit bewährten Tipps aus der Praxis zu Installation und Betrieb ab.

Preis: € 990,-- netto

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 04.05. - 06.05.15 in Bonn

Dieses Seminar vermittelt alle notwendigen Projektschritte zu einer erfolgreichen Umsetzung von VoIP Projekten. Diese erstrecken sich über die Einsatz- und Migrations-Szenarien, die einsetzbaren Basis-Technologien und Komponenten und die erweiterten TK-Anwendungen wie IVR, UM oder UC. Es werden Bewertungskriterien für eine TK-Lösung und eine Übersicht über den bestehenden TK-Markt mit allen etablierten Hersteller vorgestellt.

Preis: € 1.890,-- netto

Recht und Datenschutz bei Einführung von Voice over IP, 04.05. - 05.05.15 in Bonn

Ziel der Schulung ist es, den Teilnehmern einen Überblick über die aktuelle Situation im Bereich des Datenschutzes im Kommunikationsumfeld zu verschaffen. Datenschutz und Datensicherheit werden zunehmend wichtiger im Umgang mit Kunden und Mitarbeitern. Gerade mit der Einführung von IP basierten Lösungen in den Bereichen Telefonie oder Contact Center, stellen sich neue Herausforderungen in Bezug auf personenbezogene Informationen. Um Ihnen eine Überblick über den rechtlichen Rahmen zu geben beschäftigt sich dieses Seminar u.a. mit Fragen zur Abhörsicherheit, Vorratsdatenspeicherung, Datenverlust und den dazugehörigen Aspekten. Weitere Schwerpunkte bilden die etwaigen Vorgaben seitens der Bundesnetzagentur oder auch von Betriebsvereinbarungen, die es zu beachten gilt.

Preis: € 1.590,-- netto

Öffentliche Ausschreibungen im Informationsbereich, 04.05. - 05.05.15 in Bonn

Dieses 2-tägige Seminar bietet einen praxisnahen Leitfaden für öffentliche Auftraggeber, die in ihren ITK-Vergabeverfahren unter Einhaltung aller gesetzlichen Auflagen das optimale Ausschreibungsergebnis erreichen wollen.

Preis: € 1.590,-- netto

Trouble Shooting in vernetzten Infrastrukturen, 05.05. - 08.05.15 in Aachen

Garantietermin

Dieses 2-tägige Seminar bietet einen praxisnahen Leitfaden für öffentliche Auftraggeber, die in ihren ITK-Vergabeverfahren unter Einhaltung aller gesetzlichen Auflagen das optimale Ausschreibungsergebnis erreichen wollen.

Preis: € 2.290,-- netto

Sicherheitsstandards in der Praxis, 18.05.15 in Köln

Die Sonderveranstaltung zu Sicherheitsstandards in der Praxis beschreibt praxisorientiert Wege zur nachhaltigen Umsetzung eines Information Security Management System auf Basis von anerkannten Standards wie ISO 27001 und BSI IT-Grundschutz. Dabei werden auch Werkzeuge und die notwendigen Prozesse der Informationssicherheit sowie die Verzahnung mit der IT-Prozesslandschafft analysiert.

Preis: € 990,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
18.05. - 22.05.15 in Aachen
28.09. - 02.10.15 in Aachen

TCP/IP-Netze erfolgreich betreiben
13.04. - 15.04.15 in Düsseldorf
15.06. - 17.06.15 in Nürnberg
11.11. - 13.11.15 in Bonn

Internetworking
08.06. - 12.06.15 in Aachen
19.10. - 23.10.15 in Aachen

Paketpreis für zwei 5-tägige und ein 3-tägiges Intensiv-Seminar € 6.180,-- netto (Einzelpreise: € 2.490,-- netto bzw. 1.890,-- netto)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
05.05. - 08.05.15 in Aachen
27.10. - 30.10.15 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
09.06. - 12.06.15 in Aachen
17.11. - 20.11.15 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
04.05. - 06.05.15 in Bonn
28.09. - 30.09.15 in Köln

Session Initiation Protocol Basis-Technologie der IP-Telefonie
13.04. - 15.04.15 in Düsseldorf
15.06. - 17.06.15 in Nürnberg
11.11. - 13.11.15 in Bonn

Umfassende Absicherung von Voice over IP und Unified Communications
08.06. - 10.06.15 in Stuttgart
19.10. - 21.10.15 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
27.04. - 28.04.15 in Nürnberg
14.09. - 15.09.15 in Bonn

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

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