Dezember 2023

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

IT-Verkabelung im Serverraum gestalten mit „Rangierorten“

von Hartmut Kell
Vor ca. 1 Jahr hat der Autor einen Artikel zur IT-Verkabelung veröffentlicht, bei dem es um die Anwendung der Norm EN 50600 ging und in dem an Beispielen gezeigt wurde, welche Idee der Norm zugrunde liegt, welche Vorgaben die Norm macht und wo es Interpretations-spielräume gibt.

Seite 9

Die wichtigsten Netztrends 2024

von Dr. Behrooz Moayeri
In den letzten Jahren gab es vor Jahresende an dieser Stelle einen Blick auf die wichtigsten Trends in der Entwicklung von IT-Infrastrukturen. Wir haben anhand der jeweils aktuellen Projektanfragen der ComConsult-Kunden die Prognose darüber gewagt, welche Themen die IT-Verantwortlichen im bevorstehenden Jahr hauptsächlich beschäftigen werden.

Seite 2

Zukunftssichere WLAN-Zellplanung für Wi-Fi 6 und Wi-Fi 6E – Teil 1

von Felix Gillessen und Michael Schneiders
Die Einführung von Wi-Fi 6 (802.11ax) und 6E liegt bereits einige Zeit zurück. Mittlerweile sind längst entsprechende Access Points und Endgeräte verfügbar und finden mehr und mehr Verbreitung.

Seite 22

Webinar der Woche

Die wichtigsten Netztrends 2024

Seite 36

Intelligentes Netzwerkmanagement beeinflusst die Produktentscheidung

von Dr. Joachim Wetzlar
Am Wochenende habe ich mich seit längerer Zeit mal wieder mit der Konfiguration meiner TETRA-Handfunkgeräte beschäftigt.

Seite 34

Die wichtigsten Netztrends 2024

von Dr. Behrooz Moayeri

In den letzten Jahren gab es vor Jahresende an dieser Stelle einen Blick auf die wichtigsten Trends in der Entwicklung von IT-Infrastrukturen. Wir haben anhand der jeweils aktuellen Projektanfragen der ComConsult-Kunden die Prognose darüber gewagt, welche Themen die IT-Verantwortlichen im bevorstehenden Jahr hauptsächlich beschäftigen werden. Dieser Tradition wollen wir auch dieses Jahr treu bleiben. Dabei konzentrieren wir uns auf die Trends im Netzbereich.

2022 habe ich in den Insider-Ausgaben für Oktober, November und Dezember auf folgende Netztrends hingewiesen:

- VLANs als einfachste Segmentierungsmethode auf Ebene der Schicht 2
- VRFs als einfachste Virtualisierungsmethode auf Ebene der Schicht 3
- Weiterentwicklung von MPLS und EVPN für skalierbare mandantenfähige Netze
- Technische Vorkehrungen für gute Mobilfunkversorgung in Gebäuden
- Vorausschauende WiFi-Planung
- Glasfasern als Hauptmedium für den leistungsfähigen Internetanschluss
- Netzautomatisierung

Im Folgenden gehe ich auf meine Beobachtungen in 2022 bezüglich der oben genannten Aspekte ein und aktualisiere sie.

Trends im Campusnetz

Auch wenn man nicht selbst Netze betreibt oder anderweitig direkt mit Netztechnologie zu tun hat, assoziiert man mit dem Stichwort „Datennetz“ den Bedarf an einer immer leistungsfähigeren und ausfallsichereren Infrastruktur.

Ausfallsicherheit wird fast immer mit redundanter Hardware in Verbindung gebracht. Es gibt jedoch Ausfallszenarien, zu denen es trotz einer durchgängigen Hardware-Redundanz kommt. Den Fehlerfall Endlosschleife (Loop) gibt es sogar nur in einem redundanten Netz. Es darf auch nicht in Vergessenheit geraten, dass die Funktionalität des Netzes auf Hardware und Software angewiesen ist. Software auf Netzkomponenten kann zum Single Point of Failure werden, wenn alle Geräte mit derselben fehlerhaften Software arbeiten.

Deshalb gilt es, neben Hardware-Redundanz auf einige weitere Maßnahmen zur Maximierung der Verfügbarkeit eines Netzes zu setzen. Dazu zählt zum Beispiel die Verkleinerung von Fehlerdomänen. Das sehr robuste Internet lebt davon, dass es ein echtes INTER-net ist, d.h. ein relativ lose zusammenhängendes Gebilde aus verschiedenen administrativen Domänen (Autonomen Systemen, AS). Das bewährte Border Gateway Protocol (BGP) sorgt für den erforderlichen Austausch von Erreichbarkeitsinformationen zwischen den AS. Ich kann mich nicht an ein flächiges, AS-übergreifendes Problem erinnern, das auf Fehler in der Software oder Konfiguration von BGP zurückzuführen war.

Die Verkleinerung von Fehlerdomänen kann ebenso die Verfügbarkeit eines Campusnetzes erhöhen. Die Segmentierung des Netzes sorgt damit nicht nur für mehr Sicherheit, sondern auch für weniger flächige Fehler.

Zur Hardware-Redundanz und Segmentierung kommt als dritter Erfolgsfaktor die Einfachheit des Netzdesigns. Planer und Betreiber von Netzen müssen sich auf ihre Kernaufgaben konzentrieren und jeglicher Versuchung widerstehen, den Netzen über diesen Kern hinaus immer neue Funktionen und damit immer mehr Komplexität aufzubürden, die alle Versuche konterkariert, die Ausfallsicherheit und Beherrschbarkeit der Netze zu erhalten und ständig zu verbessern.

Verkleinert man die Fehlerdomänen, braucht man auch keine komplexen Verfahren, die erst in großen Netzen erforderlich werden. Technologien wie MPLS, EVPN und SDN sind komplex. Mandantentrennung via EVPN und VXLAN ist komplexer als

IT-Verkabelung im Serverraum gestalten mit „Rangierorten“

von Hartmut Kell

Vor ca. 1 Jahr hat der Autor einen Artikel zur IT-Verkabelung veröffentlicht, bei dem es um die Anwendung der Norm EN 50600 ging und in dem an Beispielen gezeigt wurde, welche Idee der Norm zugrunde liegt, welche Vorgaben die Norm macht und wo es Interpretationsspielräume gibt. In einem Teil wurde kurz ein relativ unbekanntes Element zum Aufbau einer Verkabelung vorgestellt, die Norm nennt es den „Zwischenverteiler“. Diesen Zwischenverteiler sieht die Norm als optionales Element in einer hierarchischen Verkabelung vor. Er kann auf unterschiedliche Arten aufgebaut werden, eine davon ist die Bildung eines „zentralen Rangierortes“. Der nachfolgende Artikel erklärt, in welcher Form die aktuellen Normen dieses Teilelement vorsehen, wie es aufgebaut werden könnte, welche technische Varianten es gibt, und wann es auch bei Ihrer Planung sinnvoll sein könnte, dieses Element zu realisieren.

Standardverkabelung im Serverraum

Was ist eine Standardverkabelung im Sinne von „so machen es die meisten“? Hier können nur die subjektiven Erfahrungen des Autors im Rahmen der Beratungen, Fachplanungen und Seminartätigkeiten wiedergegeben werden, dies muss natürlich nicht repräsentativ sein. Doch vielleicht findet sich der ein oder andere Leser wieder. Vor allem ältere Standardverkabelungen

- berücksichtigen nicht die Begrifflichkeiten der Normen, denn nicht allen IT-Verantwortlichen sind Begriffe wie z. B. Hauptverteiler bekannt,
- haben häufig keinen hierarchischen Aufbau in Form von Sterntopologien,
- trennen eher nach Netzwerk- und Serverracks – sowohl begrifflich als auch in der Planung –,
- wurden nicht nach einer vorausgehenden Anforderungsanalyse entworfen, d.h. mit Festlegung der benötigten Übertragungsverfahren, Medien und anschließender Ableitung der Kabeltypen,
- sehen eine Verkabelung vor, die bei und zu jedem Rack anders ist, eine Einheitlichkeit wurde nie angestrebt,
- lösen häufig nicht die Problematik der hohen Mengen an Anschlussschnüren und unterschiedlichen Längen derselben,
- wurden nicht wirklich in Anlehnung an die Normen geplant.

Es gibt demzufolge Racks, in denen vorwiegend Netzwerk-Komponenten positioniert werden und Racks, in denen vorwiegend Server positioniert werden. Das sind dann klassische zentrale Lösungen oder abgestuft mit Komponenten in den Positionen Middle-of-Row (MoR) bzw. End-of-Row (EoR). Wurden die Server-Access-Switches zusammen mit den Servern in Racks montiert, spricht man von Top-of-Rack (ToR). Diese 3 Arten werden in der ursprünglichen Norm EN 51073-5 überhaupt nicht erwähnt, in der EN 50600 werden sie im Anhang ausführlich erläutert (siehe Abbildung 1).

Bei den eher zentralen Lösungen ist es üblich, dass eine Datenverkabelung von den Serverracks aus zu den zentral im Raum positionierten Netzwerk-Schränken vorgesehen wird. Je nach Größe des Serverraums bzw. Anzahl der Server-Racks werden dazu lange Anschlussschnüre verwendet – besser ist eine strukturierte Verkabelung, d.h. Kabel schließen mit Buchsen ab. Zwischen den Netzwerk-Schränken wurde noch eine Datenverkabelung zum Aufbau des Backbones vorgesehen, und „fertig ist die Verkabelung“.

ToR ist noch etwas einfacher: Die Anbindung der Server an die ToR-Switches erfolgt innerhalb des Racks mit kurzen Anschluss-

Zukunftssichere WLAN-Zellplanung für Wi-Fi 6 und Wi-Fi 6E – Teil 1

von Felix Gillessen und Michael Schneiders

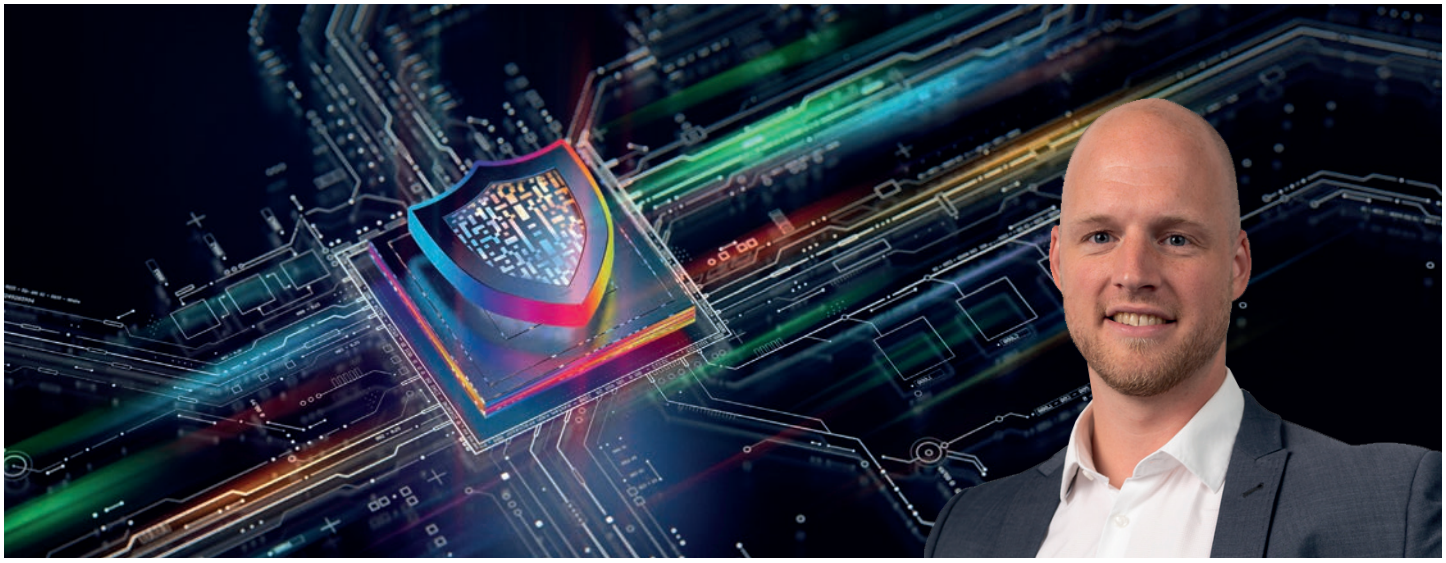
Die Einführung von Wi-Fi 6 (802.11ax) und 6E liegt bereits einige Zeit zurück. Mittlerweile sind längst entsprechende Access Points und Endgeräte verfügbar und finden mehr und mehr Verbreitung. Nahezu jedes neu erworbene WLAN-fähige Endgerät, ob privat oder im Enterprise-Umfeld, unterstützt mindestens Wi-Fi 6, immer mehr Geräte auch 6E. Dennoch gibt es eine sehr große Basis an Endgeräten, die Wi-Fi 6 noch nicht unterstützen. Doch was bedeutet das für die WLAN-Infrastruktur im Unternehmen? Sind mit neuem Standard und neuem Frequenzband auch Anpassungen der bestehenden WLAN-Zellplanung erforderlich? Wie unterscheidet sich das Vorgehen von der bisherigen Planung? Und wie können Planungen neuer Gebäude aussehen? Diese und weitere Fragen wollen wir im vorliegenden Artikel klären, damit auch Sie den neuen Standard effektiv nutzen können. In Teil 1 dieses Artikels gehen wir auf die Besonderheiten hinsichtlich Wi-Fi 6 und speziell Wi-Fi 6E, also WLAN gemäß IEEE 802.11ax im 6-GHz-Band, ein. Im zweiten Teil des Artikels beschreiben wir die generelle Vorgehensweise bei der Planung von WLANs.

Warum ist eine WLAN-Zellplanung erforderlich?

Eine der wichtigsten Aufgaben beim Aufbau einer WLAN-Infrastruktur ist die Platzierung der WLAN-Access-Points. Die optimalen Positionen für die Access Points werden bei der Zellplanung durch Messung oder Simulation bestimmt. Grundlage ist hier die von einem WLAN-Access-Point ausgestrahlte Funkzelle je relevantem Frequenzband. Abhängig von den festgelegten Anforderungen sind hier unterschiedliche Parameter wie Mindestsignalstärke oder Kapazität relevant. Die Positionen der Access Points müssen den geforderten Anforderungen entsprechen und für zu versorgende Bereiche ein flächendeckendes WLAN ermöglichen. Die gewählten Positionen in den Flächen sind nach Installation und Inbetriebnahme oftmals nur mit größerem Aufwand veränderbar (z. B. wenn Kabel unter Putz verlegt sind), weswegen der Planung der Positionierung eine entscheidende Bedeutung zukommt. Eine strukturierte Planung bildet den Grundstein für einen stabilen WLAN-Betrieb. Nur auf diese Weise können die Nutzer-Anforderungen an das WLAN, wie Datenrate, Kapazität, Verfügbarkeit, Flächendeckung und optimales Roaming sichergestellt werden.

Technischer Hintergrund Wi-Fi 6 und Wi-Fi 6E

Über das WLAN-Zugriffsverfahren IEEE 802.11ax sowie über die zugehörige Zertifizierung der Wi-Fi-Allianz, genannt Wi-Fi 6, berichteten wir bereits ausführlich im Insider 10/2021 [1]. Die im Februar 2021 vom IEEE verabschiedete Standard-Erweiterung brachte neben der – offensichtlich obligatorischen – Erhöhung der maximal möglichen Bruttodatenrate auf ca. 9,7 GBit/s zahlreiche Mechanismen zur Erhöhung der Effizienz des Shared-Me-



Beratung und Unterstützung zum Thema Netzwerkzugangskontrolle (NAC) bei einer Stadtverwaltung

Mit Daniel Prinzen sprach Christiane Zweipfennig

Mit dem Anstieg von BYOD (Bring Your Own Device) und IoT-Geräten wächst die Anzahl von Endgeräten in Unternehmensnetzwerken exponentiell. Dies eröffnet eine breitere Angriffsfläche für Cyberbedrohungen. Ein kontrollierter Zugang dieser Geräte ist die erste Verteidigungslinie vor unberechtigten Netzwerkzugriffen. Network Access Control (NAC) beschreibt das Gewähren oder Ablehnen von Netzwerkzugriffsversuchen auf der Grundlage von Identifikationsmerkmalen. Ein Hauptziel ist, nur autorisierte und vertrauenswürdige Clients, die im Besitz und unter Verwaltung eines Unternehmens sind, den Zugang zum Netzwerk zu gewähren und unbekannte Clients fernzuhalten.

Daniel Prinzen startete bei ComConsult als studentische Hilfskraft und wurde nach seinem Abschluss zum Diplom-Informatiker im Jahr 2010 als fest angestellter Berater in das Competence Center IT-Sicherheit übernommen.

Daniel, Dein Spezialgebiet bei ComConsult ist die Netzwerkzugangskontrolle. Was beinhaltet das genau?

Die Netzwerkzugangskontrolle oder Network Access Control (kurz NAC) ist eigentlich eine ganz simple Idee und meint, dass wir einen „Türsteher“ für das On-Premises-Access-Netzwerk aufbauen, der unberechtigte Zugriffsversuche auf das Netzwerk verhindert. Wir kümmern uns vor allem um die Welt der Endgeräte, die an das Netzwerk angeschlossen werden. In der WLAN-Welt ist das ziemlich einfach und es gibt wenig Beratungsbedarf. Warum? In der Kabelwelt sieht das anders aus. Der Kunde braucht von uns Unterstützung für seine IT-Infrastruktur. NAC impliziert hier auch den intensiven Austausch mit den Kollegen von den Endgeräten. Wir stimmen zum Beispiel die Prozesse für die erste Installation von Komponenten ab, denn nur über Prozesse kann man Henne-Ei-Probleme lösen. Es ist beispielsweise wichtig, von Anfang an den Einkaufsprozess zu optimieren und zu klären, ob neue Assets in einem Register als Wirtschaftsgut registriert werden. Zwar haben viele Unternehmen wegen Leasingrückläufern und Ähnlichem Wirtschaftsdaten, doch liegen detaillierte technische Daten oft nicht vor. Wird ein neues Gerät im Karton angeliefert, sollte es nicht nur einfach eingescannt, sondern auch die MAC-Adresse mit aufgenommen werden, denn darüber kann das Endgerät zumindest rudimentär identifiziert werden.

> Der Türsteher für das On-Premises-Access-Netzwerk und die daran angeschlossenen Endgeräte

Intelligentes Netzwerkmanagement beeinflusst die Produktentscheidung

von Dr. Joachim Wetzlar

Am Wochenende habe ich mich seit längerer Zeit mal wieder mit der Konfiguration meiner TETRA-Handfunkgeräte beschäftigt. TETRA – Sie erinnern sich – steht für „Terrestrial Trunked Radio“ und wird in Deutschland vor allen bei den Behörden und Organisationen mit Sicherheitsaufgaben (BOS) genutzt, doch auch in verschiedenen anderen Organisationen. Funkamateure beschäftigen sich ebenfalls mit dieser Technik; ich gehöre dazu. TETRA wurde in den 90ern spezifiziert. Es ist erkennbar an den 2G-Mobilfunk angelehnt, der bekanntlich auch aus dieser Zeit stammt.

Mobilfunk-typisch handelt es sich um ein komplexes Verfahren. Alleine die Konfiguration eines einfachen Handfunkgeräts ist ohne Spezialwissen nicht zu bewerkstelligen. Die Customer Programming Software (CPS) enthält hunderte Parameter, die sich modifizieren lassen. Dank einer illustrierten Anleitung aus Amateurfunkkreisen konnte ich die ca. 20 Parameter finden, die tatsächlich anzupassen waren. Hätte ich an der falschen Stelle etwas geändert, wäre das Funkgerät vielleicht zu einem Stein geworden; neudeutsch: ich hätte es „gebrickt“.

Warum erzähle ich Ihnen das? Zum einen sollten Sie sich eine einfachere Funktechnik aussuchen, wenn Sie je digitalen Betriebsfunk einführen wollen. Schauen Sie sich z. B. Digital Mobile Radio (DMR) an, das ist einfacher zu verstehen, und überdies in einiger Hinsicht besser. Zum anderen könnten Sie in dasselbe Problem laufen, wenn Sie jemals ihr eigenes 5G-Mobilfunknetz aufbauen und betreiben wollen.

Wie bereits gesagt steckt hinter dem Mobilfunk eine komplexe Technik. Bisher war dies die Domäne der großen Provider. Diese Unternehmen haben jahrzehntelang Personal mit Erfahrung aufgebaut, wie man Mobilfunknetze plant, aufbaut und betreibt. Entsprechende Management Tools waren auf die Bedürfnisse der Spezialisten angepasst, die sie bedienten.

Mit privaten 5G-Mobilfunknetzen öffnet sich die Technik nun einem Massenmarkt. Zugegeben, dieser Begriff scheint in diesem Zusammenhang ein wenig übertrieben zu sein. Dennoch sehen wir bei unseren Kunden die Herausforderungen des Massenmarkts: Auch weniger erfahrenes Personal ist in die Lage zu versetzen, eine komplexe Technik zu beherrschen. Damit kommt den Management Tools eine zusätzliche Aufgabe zu. Sie müssen zwischen komplexer Technik und menschlichen Anwendern vermitteln.

Beim Massenmarkt WLAN kennen wir das schon lange. Sogar Ihr Chef schafft es, seinen heimischen WLAN-Router innerhalb von Minuten zum Laufen zu bringen – der „Einrichtungs-Assistent“ weiß, wie´s geht. Ihre großen WLAN-Managementsysteme unterstützen Sie in ähnlicher Weise. Verschiedenste Templates geben sinnvolle Werte vor. Sie brauchen sich in der Regel nicht um Details des Radio Resource Management zu kümmern; Access Points fassen Sie in Gruppen zusammen und wenden darauf eine