ComConsult Research

Der Netzwerk Insider

Februar 2012

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Bring your own Device - Vorbote eines Umbruchs in der IT

von Dr. Simon Hoff, Dominik Zöller

Mit Bring Your Own Device (BYOD) erleben wir im Moment einen Trend, von dem immer deutlichere Signale ausgehen, dass hier ein Umbruch der gesamten IT seinen Anfang genommen hat. Mit BYOD drängen mit Macht privat genutzte bzw. fremde Endgeräte, insbesondere Smartphones und Tablets, die ursprünglich primär für den Consumer-Markt geschaffen wurden, in die IT. Dieser Artikel beschreibt die Techniken, die für eine sichere Unterstützung von BYOD notwendig sind, und analysiert die Möglichkeiten und Grenzen der verfügbaren Produkte.

1. IT Consumerization und die Folgen

Die Antike der IT, in der innovative Technologien zuerst Unternehmen zur Verfügung standen, bevor sie anschließend den Privatsektor eroberten, ist Geschichte. Heute wird Innovation verstärkt durch Konsumentenmärkte getrieben. Die Anwender tragen ihre Erwartungshaltung an Leistungsfähigkeit und Bedienbarkeit von Applikationen und Endgeräten in das Unternehmen.

weiter auf Seite 11

Zweitthema

Funktionsreichtum kontra Vereinfachung

von Dr. Behrooz Moayeri

Aus unserem Kundenkreis bekommen wir bezüglich der Konzipierung von Local Area Networks zwei widersprüchliche Arten von Signalen: einerseits die Nachfrage nach immer mehr LAN-Funktionen in verschiedenen Bereichen (Security, QoS, Energiemanagement, ...) und andererseits die Botschaft, dass angesichts der zunehmenden Anforderungen an die LAN-Verfügbarkeit und vor dem Hintergrund knapper Personalressourcen ein robustes, möglichst einfach aufgebautes LAN gefragt sei.

Dieses Dilemma ist nicht neu. Seit mindestens 15 Jahren diskutieren wir mit unseren Kunden über die Frage, wie viel Funktionsreichtum ein LAN verkraftet, das jahrelang zuverlässig arbeiten und betrieben werden muss. Der Autor erinnert sich immer wieder an den Leitsatz eines unserer Kunden: „Komplex wird das LAN im Laufe der Jahre ohnehin; man braucht nicht auch noch komplex anfangen. “Dieser Spruch lässt sich durchaus wissenschaftlich mit dem Entropiegesetz fundieren.

weiter auf Seite 20

Aktuelle Kongresse

ComConsult Netzwerk-Redesign Forum 2012
ComConsult IPv6-Forum 2012

ab Seite 5

Geleit

Bring Your Own Device

auf Seite 2

Standpunkt

Sicherheitsrisiko Firewall

auf Seite 19

Neues Seminar

Anwendungs-Virtualisierung für Android, iPad & Co

auf Seite 18

Zum Geleit

Bring Your Own Device

Die Nutzung mobiler Endgeräte nimmt explosionsartig zu. Stärkere Prozessoren, mehr Speicher und eine gute Grafik gestatten die Nutzung auch komplexer Applikationen auf einem mobilen Endgerät, sei es ein Smartphone oder ein Tablet. Spätestens die letzten Verkaufszahlen von Apple zeigen, dass wir in sehr kurzer Zeit mit einer weiteren und schnellen Zunahme dieser Geräte in den Unternehmen rechnen müssen. Der weltweit diskutierte Mega-Trend ist dabei die Nutzung privater Geräte für Unternehmens-Anwendungen: Bring-Your-Own-Device BYOD. Was auf den ersten Blick wie eine geniale Möglichkeit wirkt, Interessen von Mitarbeitern und Unternehmen in einer typischen Win-Win-Situation gleichermaßen zu befriedigen, generiert bei näherer Betrachtung erhebliche betriebliche und auch wirtschaftliche Probleme.

Für viele Mitarbeiter ist BYOD interessant. Zwar übernehmen sie quasi Investitionen für das Unternehmen aus eigener Tasche. Häufig können sie jedoch auf diese Weise die zu engen Regeln für Unternehmens-eigene Geräte umgehen und moderne Geräte und Applikationen nutzen. Betrachtet man die Zahl der Unternehmen mit mehr als 5 Jahre alten PCs und Internet Explorer 6, dann ist jeder Weg, diesem Technologie-Museum zu entgehen für die Mitarbeiter ein Fortschritt.

Für die Unternehmen ergeben sich auf den ersten Blick erhebliche Einsparungen im Invest-Bereich, da die Mitarbeiter ja die Kosten der Anschaffung tragen. Tatsächlich motiviert gerade dieser Aspekt offenbar viele Führungskräfte BYOD als interessant zu sehen und zu puschen.

Bei näherer Betrachtung hat BYOD je nach Art und Umfang der Nutzung im Unternehmen eine ganze Reihe von Nachteilen:

- beginnen wir mit der Idee der Einsparung. Die ist natürlich grober Unfug. Für alle IT-Geräte spielt die Höhe der Betriebskosten eine erhebliche Rolle. Diese sinken nicht dadurch, dass mobile Geräte zum Einsatz kommen. Vielmehr ist zu befürchten, dass je nach genutzten Anwendungen die Betriebskosten im Sinne von Service-Leistungen steigen. Gerade bei scheinbar preiswerten Geräten ist das kritisch, da die Betriebskosten schnell die Anschaffungskosten übersteigen. Die einfache Regel ist: je preiswerter ein Endgerät ist, desto mehr sind die Betriebskosten entscheidend.

- dann kommen wir zur Frage der genutzten Applikationen. Email können wir als überschaubar ansehen, auch wenn je nach genutztem Gerät ein IMAP-Gateway erforderlich wird, das gegebenenfalls ansonsten nicht zum Einsatz käme. Aber schon bei der mobilen Bearbeitung von Texten beginnen die Probleme. Das reine Lesen ist ok, aber wenn es darum geht, Text zu ändern oder zu kommentieren, ist das nicht ganz trivial. Zwar werben diverse Apps mit der Kompatibilität zu Microsoft Office, aber hier liegen die Tücken im Detail. Auch wenn die Apps immer besser werden, unsere Tests zeigen je nach Dokument weiterhin Probleme. Und wer die Idee hat, diese Dokumente nach der Veränderung wieder ins Unternehmen zurück zu übertragen, der sollte besonders vorsichtig sein. PDF ist lösbar, allerdings ist darauf zu achten, dass bei der Rückübertragung ins Unternehmen Anmerkungen oder Markierungen erhalten bleiben. Schon an diesen Beispielen wird klar, dass wir hier auf ein Service-Minenfeld stoßen. Wer dies nicht sauber vorbereitet, wird schnell deutlich mehr Geld für Personal oder Beratung ausgeben, als er bei der Beschaffung der Geräte einsparen würde.

- auch die Frage, wie Daten eigentlich zu den Geräten und wieder zurück ins Unternehmen kommen, ist spannend. Der übliche Weg ist durch die Nutzung von Webdiensten wie Dropbox oder Sugar-

Abbildung 1: Vertriebsunterstützung auf dem iPad Quelle: Apple

Schwerpunktthema

Bring your own Device - Vorbote eines Umbruchs in der IT

Fortsetzung von Seite 1

Dr. Simon Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück.

Dominik Zöller ist seit 2006 Berater bei der ComConsult Beratung und Planung. Während seines Studiums konzentrierte er sich bereits auf moderne Kommunikationsnetze und Betriebssysteme. Zu seinen Spezialgebieten gehören jetzt u.a. die Konzeption und Ausschreibung professioneller Unified-Communications- und Kollaborations-Systeme sowie Microsoft-Lösungen.

Die „Consumerization“ stellt die IT dabei aber vor eine Vielzahl ungelöster Probleme. Standardisierung war und ist das grundlegende Credo der IT. Nur durch Standardisierung, so glaubte man, können die Kosten des IT-Betriebs gesenkt, sowie Sicherheit und Revisionsfähigkeit für Unternehmensdaten gewährleistet werden. Für weite Teile der IT-Landschaft ist dies auch nach wie vor gültig. Ohne Standardisierung sind Netz-Infrastrukturen und Rechenzentren schlicht nicht wirtschaftlich zu betreiben. Der Trend zu Consumerization ist somit auf die unmittelbare Nutzerschnittstelle, also Applikationen und Endgeräte beschränkt.

Im Bereich der Unternehmensanwendungen ist insbesondere ausschlaggebend, dass auf konsistenten Datenbeständen gearbeitet wird. Die Unternehmensdaten sollen eine einheitliche Basis des Geschäftsprozesses bilden. Wie das einzelne Nutzer-Frontend aussieht ist zweitrangig, solange es dem Anwender ein möglichst effizientes Arbeiten erlaubt. Effizientes Arbeiten ist aber genau dann möglich, wenn der Anwender die Bedienelemente versteht und zielgerichtet einzusetzen vermag. Und das möglichst intuitiv, ohne hohen Schulungsaufwand für die Unternehmen. Ob der Anwender seine Groupware mit einem Outlook-Client, einen Drittanbieter-Client oder über eine Weboberfläche abruft, ist für die Tätigkeit als solche irrelevant. Das Bedienkonzept von Applikationen ist aber – gerade im Bereich der mobilen Endgeräte – in höchstem Maße von der Endgeräte-Plattform abhängig. Hier gibt es bei der privaten Nutzung klare Präferenzen der Anwender, z.B. für Apple iOS oder Android-basierte Geräte. Geht man auf die Nutzerpräferenzen ein, so lassen sich Synergie-Effekte durch bessere Nutzerakzeptanz und Anwenderzufriedenheit, sowie geringeren Schulungs- und Betriebsaufwand nutzbar machen. Das ist der Kerngedanke von „Bring your own Device“ (BYOD).

2. Der Endgerätezoo

Consumerization führt dazu, dass die Mitarbeiter eine Vielzahl von Endgeräte-Plattformen in die Unternehmen tragen. Die Endgeräte-Hardware ist hochgradig individuell und wird von verschiedenen Herstellern wie Apple, HTC, Motorola, Nokia, RIM, Samsung oder Sony-Ericsson geliefert, um nur einige zu nennen. Die Betriebssysteme sind entweder herstellergebunden, wie Apple iOS und RIM Blackberry OS, oder für Hardware-Plattformen verschiedener Hersteller verfügbar, wie Android und Windows Phone 7. Während die Eigenschaften der Endgeräte-Hardware (Gewicht, Akkulaufzeit, Verarbeitungsqualität, Display, (Netz-) Schnittstellen, Bedienelemente) kaum Auswirkungen auf den Unternehmenseinsatz haben, ist das Betriebssystem sowohl in Hinblick auf Geschäftsapplikationen, Datensicherheit und Management der bestimmende Faktor.

Die heute relevanten Smartphone-Betriebssysteme sind Android, Apple iOS, und Blackberry OS. Während Apples abgeschottetes iOS mit dem starken Entwickler-Ökosystem und dem „Style-Factor“ den Boom der Smartphones befeuerte, setzte Google Android auf eine vergleichsweise offene Plattform und überrollte so den Consumer-Markt. Beide setzen damit RIM, dem ehemaligen Marktführer für geschäftstaugliche Smartphone-Lösungen, massiv unter Druck. Symbian hat seine Marktführerschaft aufgrund des verpassten Anschlusses an die Smartphone-Welt verloren.

Auch Windows Phone, der Nachfolger des im Geschäftsbereich erfolgreichen Windows Mobile, hat bislang keine nennenswerten Marktanteile gewinnen können. Es fristet momentan noch ein Nischendasein zusammen mit Betriebssystemen wie bada, dem von Samsung entwickelten, offenen Smartphone-Betriebssystem. Die Kooperation mit Nokia zeigt allerdings erste Erfolge. Die ersten Absatzzahlen der in Kooperation entwickelten Lumia-Endgeräte sind vielversprechend, und Marktforscher wie IDC und IHS isupply prophezeien eine Aufholjagd zu Android, Blackberry OS und iOS.

Die Aussagen der Experten, wie die Konkurrenten den Markt in den kommenden Jahren unter sich aufteilen werden, ge-

hen allerdings auseinander. Sicher ist nur, dass Android wohl die Marktführerschaft im Gesamtsegment ausbauen wird, man aber weiterhin mit mindestens vier verschiedenen Mobilplattformen rechnen muss. Hinzu kommt eine fast unüberschaubare Zahl von verschiedenen Releases, Versionsständen und herstellerspezifischen Adaptionen. All diese Plattformen bezüglich ihrer Sicherheitsaspekte im Blick zu behalten, ist eine Aufgabe, der kaum eine IT-Abteilung auf Dauer gewachsen sein dürfte.

Hinzu kommt, dass nicht nur Smartphones für eine BYOD-Strategie in Frage kommen. Der gesamte Client-Bereich dürfte in den kommenden Jahren zur Disposition stehen. Das Notebook hat den stationären PC in vielen Bereichen bereits verdrängt; niedriger Energiebedarf, geringe Geräuschentwicklung und vereinfachter Support bei gleichzeitig geringen Mehrkosten waren Haupttreiber für den Austausch stationärer Workstations durch mobile PCs. Auch die zunehmende Mobilität der Mitarbeiter hat diesen Trend befeuert. Doch der klassische, Windows-basierte Arbeitsplatz ist auf lange Sicht in Gefahr. Tablet-PCs bieten ein vollständig neues Bedienkonzept. Damit werden sie heute den Anforderungen einer vollwertigen Arbeitsplatzlösung noch nicht gerecht, sondern eigenen sich vor allem zum automatisierten Erfassen, Darstellen und Präsentieren von Informationen. Doch erste Geräte, wie z.B. das Transformer oder das Lapdock, erweitern Tablet bzw. Smartphone um eine Docking-Station mit integrierter Tastatur, womit die Leistungsfähigkeit der Nutzerschnittstelle nah an ein herkömmliches Notebook heranreicht. Andere Geräte, wie das voraussichtlich im Sommer verfügbare Padfone, kombinieren Smartphone und Tablet. Somit verschmelzen die Grenzen zwischen Smartphone, Tablet und Notebook. Spätestens mit Verfügbarkeit von standardisierter Business-Software, wie z.B. leistungsfähigen und kompatiblen Office-Anwendungen, wird die Grenze zwischen Office-PC und mobilem Endgerät fallen. Eine Integration in die Unternehmens-Infrastruktur zu realisieren und gleichzeitig die Vertraulichkeit der verarbeiteten Daten zu gewährleisten, ist schon bei einem standardisierten Client-Portfolio eine Herausforderung. Doch wie kann dies bei der Vielzahl von Endgeräten und Betriebssystemen in einem BYOD-Szenario erreicht werden?

3. Gefährdungen durch mobile Endgeräte und BYOD

BYOD ist zunächst mit dem grundsätzlichen Risiko des Verlusts von Vertraulichkeit und Integrität von Unternehmensdaten durch die Aufweichung der Abgrenzung von unternehmenseigener und fremder IT verbunden.

Als mobile Endgeräte sind dabei Smartphones und Tablets wie mobile PCs und mobile Datenträger einzustufen und entsprechenden Gefährdungen ausgesetzt. Hierzu zählen insbesondere die im Folgenden diskutierten Punkte:

Verlustrisiko (inklusive Diebstahl)

Mit dem Verlust eines Endgeräts besteht generell die Gefahr eines Verlusts von Unternehmensdaten (Dokumente, Kontakte, Passwörter, etc.) und des Zugriffs auf vertrauliche Informationen.

Transportwirt für Schadprogramme

Ein Smartphone oder Tablet ist in vielen Fällen ein Zwischenspeicher für per Internet, MMS oder SMS bezogene Daten, die manuell oder automatisch mit der Dateiablage in einem PC oder einer zentralen Dateiablage synchronisiert werden. Auf diese Weise lässt sich analog zu USB-Sticks Schadsoftware in das Unternehmensnetz einschleusen. Basis ist oft ein Web-Zugriff über den eine schadenstiftende Datei auf Smartphone oder Tablet heruntergeladen wurde.

Ziel für Schadprogramme

Smartphones und Tablets sind auch das direkte Ziel von schadenstiftender Software (Malware). Diese Gefahr darf nicht unterschätzt werden. Beispielsweise wird seit 2009 ein exponentielles Wachstum an Malware für Android festgestellt (siehe z.B. Malcious Mobile Threats, Report 2010/2011 von Juniper Networks). Die Konsequenzen eines Befalls mit Malware sind im Prinzip analog zu Windows-PCs. Beispiele sind:

- Zugriff auf vertrauliche Informationen, die auf dem Endgerät gespeichert sind (Dokumente, Passwörter, Kontakte, E-Mails, etc.)
- Gerät nicht länger nutzbar
- finanzieller Schaden durch missbräuchliche Nutzung von Mehrwertdiensten

Unberechtigter Zugriff auf Infrastruktur-Ressourcen

Über ein kompromittiertes mobiles Endgerät kann ein ggf. weitgehender Zugriff auf Unternehmensressourcen erfolgen, sofern der Zugang zur Infrastruktur nicht angemessen geschützt ist. Hier geht es nicht nur um Datendiebstahl. Als Szenario stelle man sich beispielsweise ein mit Malware verseuchtes Fremdgerät vor, das versucht alle erreichbaren Kommunikationsziele im Unternehmen zu infizieren.

Die Strategie zum Schutz vor den genannten Gefährdungen liegt auf der Hand:

- Härten der Systeme (sichere, zentrale Konfiguration, Virenschutz und Sandboxing)
- Absicherung des Zugriffs auf Infrastrukturressourcen

Welche Möglichkeiten und Grenzen hier für BYOD bestehen, wird in den folgenden Kapiteln erörtert.

4. Endgeräte-Management und User-owned Devices

Die Absicherung von unternehmenseigenen Endgeräteflotten wird in der Regel durch Mobile Device Management (MDM) Lösungen erzielt. Über diese Lösungen

Seminar

Bring Your Own Device - Sichere Integration von mobilen Privatgeräten in die IT-Infrastruktur, 17.04.12 in Bonn

Dieses Seminar analysiert die Gefährdungen und beschreibt die Wege zur sicheren Anbindung privater und fremder mobiler Endgeräte. Verfügbare technische Lösungen werden vorgestellt und Strategien für den Betrieb dieser Lösungen erarbeitet.

Referenten: Dr. Simon Hoff, Dominik Zöller
Preis: 990,-- netto

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

Zweitthema

Funktions-reichtum kontra Vereinfachung

Fortsetzung von Seite 1

Dr. Behrooz Moayeri ist bei der ComConsult Beratung und Planung GmbH als Mitglied der Geschäftsleitung tätig. Er hat in den letzten beiden Jahrzehnten viele Unternehmen zur IT-Infrastruktur beraten.

Auch das Netz unterliegt diesem Gesetz und weist im Laufe seines historischen Wachstums eine steigende Entropie, sprich eine steigende Komplexität auf. Wenn man auch noch vom Beginn an eine komplexe Netzstruktur plant, läuft man Gefahr, dass das Gebilde schon bald nach der Inbetriebnahme unbeherrschbar wird.

Aber die Nachfrage nach mehr Funktionen ist ja nicht unbegründet. Nehmen wir das Beispiel LAN Security. In den letzten Jahren haben wir im Auftrag unserer Kunden immer mehr Lokale Netze mit der Funktion Network Access Control (NAC) konzipiert, getestet und dem Betrieb übergeben. Den meisten NAC-Projekten sind die Ziele gemeinsam, erstens das LAN vor unbefugten Zugriffen zu schützen und zweitens bereits beim physikalischen Anschluss eines Gerätes an das LAN das Gerät automatisch einer von mehreren Benutzergruppen zuzuordnen, die sich hinsichtlich ihres Schutzbedarfs wesentlich unterscheiden. Dies erfolgt in Form einer dynamischen Zuordnung zu einem Virtual Local Area Network (VLAN).

Beide Ziele lassen sich vom realen Bedarf der Unternehmen ableiten. Vor dem Hintergrund der zunehmenden Sicherheitsvorfälle passt ein offenes, ungeschütztes LAN nicht mehr zur heutigen Zeit. Hinzu kommt, dass in Räumlichkeiten vieler Unternehmen immer mehr Geräte vernetzt werden müssen, die nicht einer einheitlichen administrativen Hoheit und damit einheitlichen Sicherheitsrichtlinien unterliegen. NAC ist die Voraussetzung für den Aufbau eines mandantenfähigen LAN, das logisch in separate Segmente für die Aufnahme von Geräten mit unterschiedlicher Security-Einstufung aufgeteilt wird.

Aber NAC erhöht die Komplexität des Netzbetriebs. Unsere NAC-Erfahrungen der letzten Jahre belegen die Warnung, dass die Komplexität von NAC nicht unterschätzt werden darf. Mit NAC tritt eine Wechselwirkung zwischen Endgeräten und ihren Betriebssystemen einerseits und den LAN-Komponenten andererseits in Kraft, die uns bis vor wenigen Jahren unbekannt war. Mit NAC bürden wir dem LAN-Betrieb neue Aufgaben auf. Die Fehlersuche wird komplexer, die Abhängigkeiten von Funktionen und Mechanismen außerhalb des Einflusses von LAN-Betreibern (zum Beispiel Verzeichnisdiensten, vgl. Abbildung 1) größer.

Ein anderes Beispiel ist die Quality of Service (QoS). Wir erleben nunmehr das zweite Jahrzehnt der Diskussion über das Für und Wider von QoS in Lokalen Netzen. Vor allem die Einführung von Voice over Internet Protocol (VoIP) hat diese Funktion beflügelt. VoIP-Hersteller zwangen viele LAN-Betreiber mit ultimativen Forderungen nach QoS zu Einstellungen auf LAN Switches, deren Sinnfälligkeit immer wieder bezweifelt wird. Die zunehmende Nutzung von Video, der verstärkte Einsatz von Unified Communications (UC) auf Geräten, die nicht nur der Audio- und Videoübertragung, sondern vielmehr als Basis diverser Anwendungen dienen, die vielen Probleme gerade durch die Einführung von QoS und die explosionsartige Vervielfachung der verfügbaren Übertragungskapazität in Lokalen Netzen haben immer wieder die Frage aufgeworfen, ob QoS-Konzepte, die vor über zehn Jahren für die damalige Generation von VoIP-Endgeräten erstellt wurden, noch zeitgemäß sind.

Auch so alt wie IP-Telefonie ist die Diskussion über die Energiefunktionen von LAN-Switches. Um den Kunden die Hemmschwelle bei der Einführung von VoIP zu nehmen, sollten IP-Telefone wie seit über

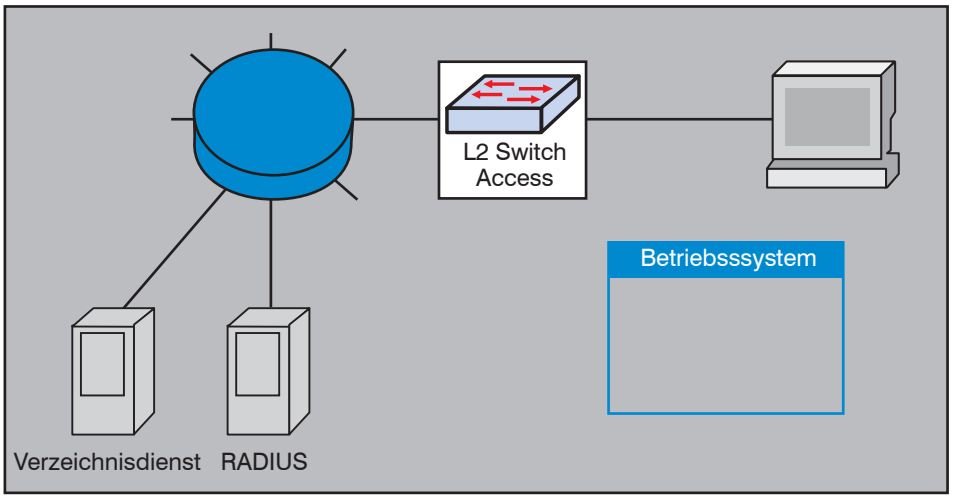

Abbildung 1: Einflussfaktoren bei NAC

hundert Jahren bei klassischen Telefonen der Fall „vom Netz gespeist“, d. h. von den Switches mit elektrischer Energie versorgt werden. Dass diese Forderung viele Detailprobleme verursacht, von der Erkennung des Leistungsbedarfs der Endgeräte durch den Switch bis zur Überlegung, auf welche Gesamtleistung von angeschlossenen Endgeräten ein Switch ausgelegt sein sollte, ist angesichts von über zehn Jahren Erfahrung mit Power over Ethernet (PoE) unbestritten. Qualvoller wurde die Wahl zwischen verschiedenen PoE-Optionen dadurch, dass mittlerweile nicht nur VoIP-Endgeräte, sondern auch Wireless Access Points mit PoE versorgt werden und weitere Gerätetypen wie Docking Stations als Kandidaten für PoE im Gespräch sind.

Einige Hersteller sind auf die Idee gekommen, LAN-Switches nicht nur für die Versorgung von Endgeräten mit Energie, sondern darüber hinaus auch für die Implementierung von Funktionen des Energiemanagements zu nutzen, die eine breite Palette von der reinen Überwachung und dem Reporting des Energieverbrauchs bis hin zur Steuerung von Endgeräten und deren Energieaufnahme reichen. Die immer wieder aufgegriffene Thematik der „Green IT“ leistet solchen Konzepten Vorschub.

Ganze Seiten voll kann man über Pro und Kontra VLANs schreiben. VLANs können zur Trennung von Benutzergruppen, für Netzmanagement, zur Isolierung bestimmter Gerätetypen wie Telefone, Gebäudemanagementeinrichtungen, Wireless Access Points etc. eingesetzt werden. Mit VLANs ist aus einem Layer-2-Switch schnell eine Reihe von logisch getrennten Switch-Instanzen gemacht (siehe Abbildung 2). Aber auch hier stellt sich die Frage: Ist ein VLAN-Flickenteppich noch beherrschbar? Wird durch die exzessive VLAN-Nutzung die Fehlersuche nicht komplexer, die Gefahr von Fehlfunktionen nicht größer und damit die Verfügbarkeit des Netzes nicht reduziert? Kommt die Netzdokumentation noch mit, wenn die VLAN-Konfiguration jedes Switches anders aussieht als die jedes anderen Switches?

Während über NAC, QoS, PoE und VLANs schon seit Jahren kontrovers gesprochen wird, hat der Wandel der Rechenzentrumsstrukturen in den letzten zwei bis drei Jahren neue Diskussionen darüber aufkommen lassen, was von neuen Funktionen für RZ-Netze zu halten ist, welche von den aktuellen Produkten angeboten werden: Link State Bridging, prioritätsgesteuerte Flusskontrolle (Priority-Based Flow Control, PFC), Enhanced Transmission Selection (ETS). Diese Funktionen werden oft mit der Forderung begründet, Speicherverkehr über Ethernet zu leiten. Speichersysteme kommunizieren aber teilweise seit Jahren über Ethernet, und zwar ohne dass es Data Center Bridging (DCB), also solche Funktionen wie PFC und ETS gibt. Warum müssen RZ-LANs neu erfunden werden, wenn es auch anders geht?

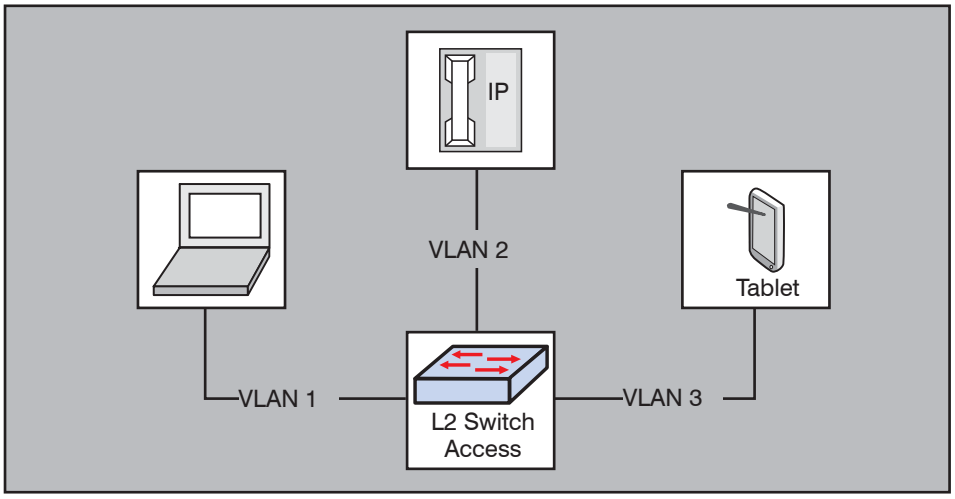

Abbildung 2: Einsatz von VLANs für logische Segmentierung

Mindestens seit drei Jahren wird im Markt sehr intensiv über künftige Layer-2-Verfahren gesprochen. Noch bevor sich die Branche auf einen Standort für Link State Bridging einigen konnte, haben mehr oder weniger alle Hersteller Mechanismen für Multi-Chassis Link Aggregation (MC-LAG) in ihren Produkten implementiert. Proprietäre Varianten von Link State Bridging sind mittlerweile auch verfügbar. Da die meisten Layer-2-Netze ohnehin auf Spanning Tree und Rapid Spanning Tree basieren und höhere Anforderungen an die Geschwindigkeit der Umschaltung zunehmend mit MC-LAG erfüllt werden, stellt sich die Frage, wer noch den künftigen Standard für Link State Bridging braucht. Wenn man ihn (so er sich tatsächlich etabliert) einsetzt, läuft man möglicherweise Gefahr, auf eine selten genutzte Technik zu setzen und mit den ganzen Fehlern und Geburtswehen der Technik ziemlich einsam da zu stehen.

Mehr Intelligenz in die LAN-Komponenten bringen auch Mechanismen, welche für Netzmanagement und Netzanalyse genutzt werden. Da es sich bei den LAN-Switches um Komponenten handelt, die an den zentralen Schaltstellen der IT-Infrastruktur platziert sind, über die der gesamte Datenverkehr geleitet werden muss, ist es naheliegend, diese Schalt-

Intensiv-Tag - Kongress

Intensiv-Tag "VLAN-Optimierung" 26.04.12 in Bad Neuenahr

Auch die größten Puristen kommen an der Nutzung von VLANs zur Konfiguration Lokaler Netzwerke nicht vorbei. Aber VLANs bieten einen erheblichen Gestaltungspielraum und wer diesen nutzt, der wird schnell über das unvermeidbar Notwendige hinaus viele weitere VLANs anlegen. Wir haben deshalb den Intensiv-Tag des ComConsult Netzwerk-Redesign Forums gewählt, um der Sache auf den Grund zu gehen. Ziel ist, dabei auch die unterschiedlichen Sichtweisen der Hersteller zu diesem Thema transparent zu machen. Der Tag wird beendet mit einer offenen Diskussion des Themas.

Moderation: Dipl.-Inform. Petra Borowka-Gatzweiler, Dr.-Ing. Behrooz Moayeri
Intensiv-Tag im Anschluss an das ComConsult Netzwerk-Redesign Forum 2012
am 26.04.12: 990,-- netto

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