



Access Switching

– hier geht's um mehr als nur den Preis

Ist Access Switching wirklich so einfach?

Die Planung eines Access Netzwerkes erscheint vielen als recht banale Angelegenheit. Art und Anzahl der Ports je Unterverteiler ermitteln, Interfacetyp der Uplinks unter Beachtung der passiven Infrastrukturen festlegen, Preisvergleich der gewünschten Hersteller – fertig! Oder vielleicht doch nicht?

Die Forderung nach möglichst vielen Ports auf möglichst wenig Raum und gleichzeitig geringer Energieaufnahme führt dazu, dass die Geräte der verschiedenen Hersteller optisch recht ähnlich erscheinen und oberflächlich betrachtet kaum funktionale Unterschiede aufzuweisen scheinen. Neue Anforderungen durch die Entwicklung hoch-performerer WLAN-Access-Points, Geräte mit 2,5 bzw. 5 Mbps-Schnittstellen, zeigen erste Unterschiede auf.

Bei der Geräusch-Emission und beim Stromverbrauch gibt es dann bereits deutliche Unterschiede. Bei der Ermittlung des PoE-Budgets beginnt es knifflig zu werden: 802.11at und af, proprietäre Ansätze wie z. B. Universal PoE, teilweise modulare Netzteile unterschiedlicher Leistung und bewusst unterdimensionierte Designs können dazu führen, dass die PoE-Unterstützung nicht für alle Endgeräte zeitgleich möglich ist.



Bezüglich der unterstützten Layer-2 und Layer-3 Switching-Features hilft ein Blick ins Datenblatt und nur mit guter Kenntnis der Netzwerkanforderungen kann entschieden werden, welche Leistungsmerkmale in Summe erforderlich sind und welche nicht.

Wer sich hier keine Gedanken macht stellt oftmals sehr schnell fest, dass er den falschen Switch gekauft hat und ein kostenpflichtiger Softwareupgrade, oder noch gravierender, eine andere Switchhardware erforderlich ist.

Zur Verdeutlichung hier ein kleiner, unvollständiger Auszug solcher Features:

Converged Wired, Wireless Access	zur Integration von WLAN-Controllerfunktionen in den Access Switch
Hochverfügbarkeit	z. B. mittels Bidirectional Forwarding Detection (BFD), Link-Redundanz, Multiple Spanning Tree (MSTP), Per-VLAN Rapid Spanning Tree (PVRST+) oder redundanter Stromversorgung
LISP	zur Entkopplung von Endgeräte-ID und Lokation, so dass IP-Adressen auch bei Lokationswechseln beibehalten werden können
NetFlow	zur Auswertung und Optimierung von Applikationsverhalten
QoS	zur Sicherstellung der applikations-spezifisch notwendigen Qualitätsparameter der Netzwerkverbindung
Software-Defined Networking	ist mittlerweile auch für Access-Umgebungen relevant und für die Abbildung einer Vielzahl von Business-Prozessen essentiell erforderlich
NFV	Mit Network Function Virtualization werden Access Switches zu hybriden Devices, durch die die Bereitstellung von unterschiedlichen Applikationen bereits auf dem Network-Layer ermöglicht werden

Unterschiede zeigen sich auch beim Vergleich von Paketdurchsatz und Latenz – besonders Betreiber zeitkritischer Infrastrukturen, z. B. im Finanzwesen, wissen um den Vorteil, eine Transaktion ein paar Milli- oder Nanosekunden schneller durchführen zu können als der Wettbewerb.



Beachten Sie auch die Auswirkungen des Betriebes von IPv6 auf die Netzwerkperformance. Spätestens hier wird deutlich, dass die Auswahl der richtigen Komponenten direkten Einfluss auf die Wertschöpfungskette des Unternehmens haben kann.

Effizientes Management

Die Managementsysteme und -konzepte moderner Netzwerke entwickeln sich stetig weiter, was den Konfigurationsaufwand der Netzelemente immer weiter reduzieren kann. So zeigen sich auch viele Anwender zur Vermeidung von Herstellerabhängigkeiten offen gegenüber einer Dual-Vendor-Strategie – doch wie setzt man diese sinnvoll um, ohne sich Kopfzerbrechen über Kompatibilitätsprobleme und überbordenden Administrationsaufwand machen zu müssen? Mit der Auswahl von zueinander passenden Herstellern und der richtigen Managementplattform kann dem begegnet werden.

Durch das breite Herstellerportfolio, das Controlware betreut, sind wir in der Lage, Sie herstellerneutral bei der Auswahl der für Ihre Anforderungen passenden Systeme zu beraten.

Und die Sicherheit?

Begründet durch eine immer diffuser werdende Bedrohungslage besteht ein Trend, möglichst viele potenzielle Bedrohungen bereits am Perimeter – dem Rand des Netzwerkes – zu eliminieren und zentrale Sicherheitsressourcen zu entlasten.

NAC (Network Access Control, Netzwerk-Zugangskontrolle) gewinnt damit neben Wireless- auch für Wired Umgebungen einen deutlich höheren Stellenwert. Mit NAC wird die Kontrolle darüber erlangt, wer wann mit welchem Endgerät und in welcher Qualität Zugang zu welchen Netzressourcen erhält. Dank identitätsbezogener Netzwerk-, Cloud- und Anwendungssicherheit sind kritische und sensible Daten geschützt. Der BYOD-Zugriff oder ein Gast-Zugang ist ohne Sicherheitsrisiko möglich und es werden umfassende Funktionen für die Verwaltung, Sichtbarkeit und Überwachung des Netzwerkzugriffs bereitgestellt.

Software Defined Networking: Digitalisierung als Treiber für den Geschäftserfolg

Die Anforderungen nach dem Einsatz von „Software-Defined“-Konzepten zur Umsetzung von Digitalisierungsstrategien beeinflussen in immer stärkerem Maße die Auswahl der erforderlichen Netzkomponenten. Die Einbindung der Access-Switching Infrastrukturen in sog. Fabric-Strukturen, die Controllergestützt die Dienstebereitstellung ermöglichen und das Management vereinfachen, gewinnen immer mehr an Bedeutung. Besonders relevant ist dies bei der Umsetzung von Digitalisierungsstrategien der Unternehmen.

Hier ist die Systemauswahl oftmals entscheidend für den Erfolg bei der Umsetzung der Strategie und den Geschäftserfolg.

Ohne fundierte Planung geht es nicht

Sicher lässt sich die Planung einer Access-Switching Infrastruktur darauf beschränken, die Anzahl der Ports zu zählen, den Interfacetyp festzulegen und das billigste Angebot oder den bekanntesten Hersteller zu wählen. Ob mit dieser Vorgehensweise eine zukunftssichere, agile und flexible Infrastruktur erstellt wird, die zudem stabil läuft, wirtschaftlich betreibbar ist und zu den speziellen Anforderungen des Unternehmens passt, ist indes fraglich. Wenn Sie z. B. sicherstellen wollen, dass unternehmenskritische Applikationen bedarfsgerecht funktionieren, die Stromversorgung von PoE-Endgeräten gewährleistet ist, eine einfache Administration ermöglicht wird, sowie CAPEX und OPEX in einem ausgewogenen Verhältnis zueinander stehen, dann erfordert dies eine professionelle Planung.

Controlware verfügt über eine langjährige Expertise auch in komplexen Umgebungen und unterstützt Sie gerne.

Hilfe auch im Störfall

Controlware unterstützt Sie nicht nur im normalen Betrieb des Netzwerkes, sondern auch bei einem Störfall. Gerade hier helfen wir Ihnen gerne direkt vor Ort bei der Entwicklung der genau passenden Services.

Controlware als Ihr Partner

Wir haben in der Praxis bereits die komplexesten Probleme gelöst. Unsere Kunden schätzen die Leistung der Controlware als Trusted Advisor für Network Solutions.

Ihr Vorteil - Mit Network Solutions von Controlware profitieren Sie von ...

- mehr als 35 Jahren Erfahrung im Bereich IT-Networking,
- umfangreicher Expertise in verschiedensten Branchen, z. B. öffentliche Verwaltung, Banken und Versicherungen, Energieversorger, Produktion, Logistik, Gesundheitswesen, Medien, Gastgewerbe und Bildungswesen,
- einem hervorragenden Marktüberblick – nicht nur theoretischer Natur, sondern auch in der Praxis
- flächendeckender Präsenz und Kundennähe mit 15 Standorten in der DACH-Region,
- nachgewiesener Servicequalität mit unserem ISO 27001-zertifiziertem Customer Service Center und mehr als 250 System-Ingenieuren und Consultants.

Zentrale

Controlware GmbH

Waldstraße 92
63128 Dietzenbach

Tel. +49 6074 858-00
Fax +49 6074 858-108

info@controlware.de
www.controlware.de