Netzwerkvirtualisierung: Kosten senken im LAN & WAN

Pamela Krosta-Hartl, Roland Burlaga

LANCOM Systems GmbH
Adenauerstraße 20/B2
52146 Würselen
pamela.krosta-hartl@lancom.de
roland.burlaga@lancom.de

Abstract: Der vorliegende Beitrag führt in das Thema Netzwerkvirtualisierung ein, beleuchtet die unterschiedlichen Methoden in LAN, WLAN und WAN und zeigt anhand konkreter Praxisbeispiele, inwieweit die konsequente Virtualisierung von Netzen – wir sprechen von „Total Network Virtualization" – Unternehmen helfen kann, sowohl bei den Investitionen als auch bei Betriebskosten massiv Kosten zu reduzieren.

1 Netzwerkvirtualisierung und Einsparpotentiale

Grundsätzlich bezeichnet der Begriff Virtualisierung die Trennung einer IT-Anwendung von der verwendeten Hardware. Bei der Netzwerkvirtualisierung werden die Netzwerkdienste von der Netzwerkinfrastruktur abgelöst. Eine solche Virtualisierung kann im LAN über entsprechend intelligente Managed Switches realisiert werden, auf denen so genannte VLANs – Virtual Local Area Networks – konfiguriert werden. Ebenso stehen im Wireless LAN Virtualisierungsmöglichkeiten zur Verfügung, bekannt unter den Begriffen Multi-Service-WLANs oder Multi-SSIDs. Wird der Gedanke der Netzwerkvirtualisierung konsequent fortgesetzt, kann bei Einsatz geeigneter Hardware eine Virtualisierung bis ins WAN erfolgen – also auch des Routers und der dazugehörigen Internet-Anbindung. Das von LANCOM vor einigen Jahren eingeführte Advanced Routing & Forwarding (ARF) ermöglicht eine solche Router-Virtualisierung. Damit werden aus einem Router bis zu 64 logische – virtuelle – „Maschinen".

Die Gründe für den Griff zur Virtualisierung sind vielfältig. Während bei den Servern die zentrale Wartung eine große Rolle spielt, eröffnen virtualisierte Netzwerke völlig neue Anwendungen, die „normale" Netzwerke nicht bieten können. Beiden Bereichen ist jedoch eines gemein: durch die Virtualisierung sparen Unternehmen teure Ressourcen, was sich sowohl auf Investitionen als auch auf die laufenden Kosten nachhaltig positiv auswirkt.

Doch wodurch werden diese Einsparungen möglich? Der wirtschaftliche Hauptnutzen der Netzwerkvirtualisierung liegt in der Möglichkeit der Mehrfachnutzung der Netzwerkinfrastruktur. Konkret heißt das, dass auf Basis eines physikalischen Netzes mehrere logische Netze geschaffen werden, die zwar dieselbe Geräteinfrastruktur nutzen, abgesehen davon aber vollständig und sicher voneinander getrennt und füreinander unsichtbar sind. Diese Mehrfachnutzung kann sich einerseits auf Dienste beziehen – ein häufig zitiertes Beispiel ist der WLAN-Gastzugang, den Unternehmen ihren Besuchern gerne gewähren –, andererseits aber auch auf die Nutzung ein und desselben Netzwerks durch mehrere Firmen, zum Beispiel in einem Gründerzentrum.

Dank Virtualisierung reicht also ein physikalisches Netz aus Switches, Kabeln, Access Points und Routern aus, um mehrere logische Netze zu betreiben. Das Einsparpotential hinsichtlich der benötigten Geräte ist enorm, ebenso die Senkung der laufenden Kosten beispielsweise beim Energiebedarf.

2 Methoden der Virtualisierung

Technisch gesehen kommen bei der Netzwerkvirtualisierung zwei unterschiedliche Methoden zum Einsatz.

2.1 Statische Virtualisierung auf Layer 2

Bei VLANs und Multi-SSIDs bezieht sich die Virtualisierung auf das Übertragungsmedium, das zu einem Shared Medium umfunktioniert wird. Ein Access Point mit mehreren SSIDs spannt beispielsweise einfach mehrere voneinander getrennte Funkzellen „nebeneinander“ auf. VLANs und Multi-SSIDs werden also auf der physikalischen Netzwerkebene, dem Layer 2 des OSI-Modells, realisiert. Diese Art der Virtualisierung ist auf das verkabelte oder drahtlose Unternehmensnetz, das LAN, begrenzt.

Fakt ist jedoch, dass die IP-basierte Zusammenarbeit zunehmend über die Grenzen einer Organisation und damit des LAN hinausgeht, sie verlagert sich immer mehr ins WAN. Zudem orientiert sie sich immer stärker an den Aufgaben der Mitarbeiter oder Kommunikationsteilnehmern. Das einfachste Beispiel für das Überschreiten der Grenzen des LAN ist der Netzwerkzugang für Gäste in den eigenen Räumen, in komplexen Szenarien erhalten externe Dienstleister über das Internet Zugriff auf bestimmte Anwendungen im lokalen Netzwerk. Eine rein statische Virtualisierung wie sie bei VLANs und Multi-SSIDs auf Layer 2 geschieht, reicht hier nicht mehr aus.

2.2 Dynamische Virtualisierung auf Layer 3

Der nächste Schritt in der Virtualisierung von Netzwerken ist daher die dynamische Virtualisierung auf Layer 3, also die Trennung der Anwendung selbst von den physikalischen Übertragungsmedien: die IP-Netzwerke und das Routing der Datenpakete zwischen diesen IP-Netzwerken. Ähnlich wie bei der Virtualisierung von Servern wird dabei eine Hardware – ein Router – genutzt, um mehrere virtuelle Router einzurichten. Jeder dieser virtuellen Router kann speziell für sein Netzwerk konfiguriert werden.

Mit einer solchen höheren Ebene der Virtualisierung können auf vorhandenen Infrastrukturen parallel völlig unterschiedliche Anwendungen mit dedizierten Einstellungen für das Routing und die Zugriffsberechtigungen realisiert werden. Ein Mechanismus, mit dessen Hilfe solch komplexe Virtualisierungsszenarien realisiert werden können, ist das eingangs erwähnte Advanced Routing & Forwarding.

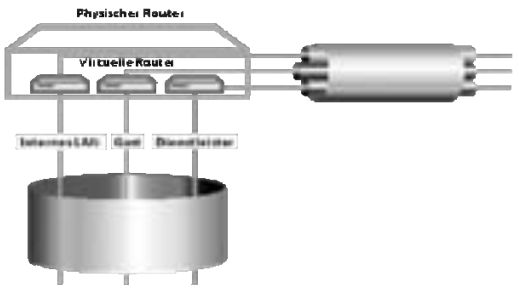

Abbildung 1: Router-Virtualisierung mit ARF

Der Kernpunkt dieser Technologie ist die Möglichkeit, für jede Anwendung ein eigenes IP-Netzwerk auf dem zentralen physikalischen Router einzurichten. Für jedes dieser Netzwerke können grundlegende Funktionen wie die Firewall oder der DHCP-Server separat konfiguriert werden. Besonders wichtig ist jedoch die Möglichkeit, über ein spezielles Tag die Einträge in der Routing-Tabelle einem IP-Netzwerk zuzuordnen: so entstehen in einem physikalischen Router mehrere virtuelle Router, deren Verhalten speziell auf das jeweilige IP-Netzwerk abgestimmt wird. Dabei werden die Tags zur Unterscheidung der Datenpakete anhand verschiedener Kriterien zugewiesen.

Bei der Einrichtung eines WLAN-Zugangs für die Besucher eines Unternehmens können die Gäste nach der Authentifizierung automatisch mit beschränkten Rechten, z. B. nur mit Internetzugang und Zugriff auf einen Netzwerkdrucker ausgestattet werden. Neben den internen Teilnehmern können aber auch externe Unternehmen in die virtuelle Netzwerkstruktur aufgenommen werden. Wird z. B. einem Dienstleister ein VPN-Zugang zur Überwachung der Heizungsanlage eingerichtet, kann dieser Zugang gezielt einem anderen IP-Netz zugeordnet werden.

Um diese Form der Virtualisierung zu erreichen, müssen die verwendeten Router ARF beherrschen und die Zuordnung der IP-Netzwerke zu einer LAN-oder WLAN-Schnittstelle unterstützen, gegebenenfalls genauer spezifiziert über eine VLAN-ID. Um die Tags zur Unterscheidung der IP-Netzwerke richtig zu behandeln, müssen alle Switches und Access Points im LAN VLAN- beziehungsweise Multi-SSID-fähig sein.

Sollen überlappende IP-Netze dann getrennt über eine WAN-Verbindung weiter übertragen werden, kommt ein zusätzliches Tunnel-Protokoll zum Einsatz: das PPTP (Point-to-Point Tunneling Protocol). Dadurch bleibt die LAN-seitige Trennung durch VLAN oder Multi-SSID auch bei der Übertragung über das Internet komplett erhalten. Für maximale Sicherheit sorgt dabei die verschlüsselte Übertragung durch einen IPSec-VPN-Tunnel.

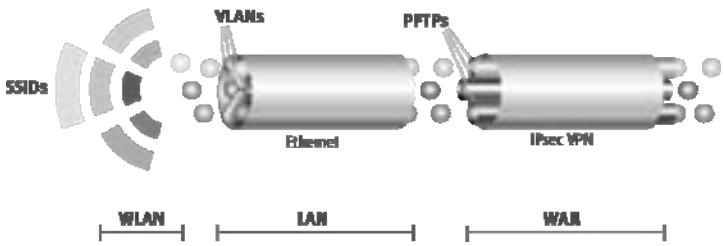

Abbildung 2: Multi-VPN: Tunnel im Tunnel

3 Praxisbeispiele

3.1 Bürogemeinschaft

Virtualisierte Netzwerkstrukturen bieten schon für kleine Unternehmen deutliche Vorteile. Auch Arztpraxen, Steuerkanzleien oder Ingenieur-Büros können heute nicht mehr auf die Vernetzung mit Geschäftspartnern verzichten. In vielen Gebäuden reicht die vorhandene Verkabelung aber nicht aus, um für jeden Mieter ein komplett eigenes Netzwerk einzurichten.

In diesem Fall kann für z. B. für die Arztpraxis und das Ingenieurbüro auf Basis desselben physikalischen Netzwerks jeweils ein separates virtuelles IP-Netzwerk eingerichtet werden. Beide Netzwerke sind intern völlig voneinander getrennt, so dass kein unbefugter Zugriff auf Patientendaten oder Konstruktionspläne möglich ist. Das Ingenieur-Büro kann zusätzlich noch einen WLAN-Zugang für Gäste einrichten, die nur Zugriff auf das Internet haben.

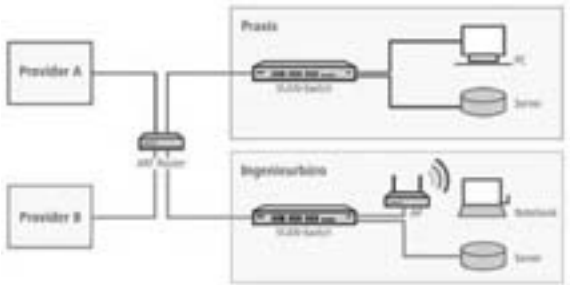

Abbildung 3: Gemeinschaftliche Nutzung durch mehrere Teilnehmer

Durch die gemeinschaftliche Nutzung sparen unsere Arztpraxis und das Ingenieurbüro gleich mehrfach: 30 - 40 % der Investition in Hardware (Access Points, Switches und Router – je nach Räumlichkeiten); 50 % bei der Internet-Anbindung (Leitungskosten); 30 - 50 % beim Energiebedarf; Einsparungen bei Verkabelung und Verlegung je nach Räumlichkeiten.

3.2 Supermarkt

In dem ersten Beispiel geht es vor allem um die Trennung von internen Datenströmen. Ein entscheidender Vorteil von Netzwerkvirtualisierung ist jedoch, auch Anwendungen mit externen Teilnehmern sauber in das eigene Netzwerk zu integrieren – ohne in zusätzliche, separate Infrastruktur investieren zu müssen.

Der Blick hinter die Kulissen einer modernen Supermarktfiliale zeigt, welche umfangreichen Sparpotentiale „Total Network Virtualization“ mittels VLAN, ARF und PPTP eröffnet.

Die Supermarktfiliale ist mit der Zentrale der Handelskette per VPN vernetzt, die PCs in der Filiale sind direkt in das ERP-System der Handelskette eingebunden, um den Warenfluss optimal zu steuern. Eine weitere VPN-Verbindung zwischen der Filiale und einem Geldinstitut sichert den elektronischen Zahlungsverkehr ab, wenn Kunden sicher und bequem per EC-Karte und PIN bezahlen möchten. Innerhalb des Supermarkts wird die gesamte Inventur mittels WLAN-fähiger Handscanner durchgeführt, die die Ergebnisse automatisch und in Echtzeit in das ERP System übermitteln und Nachbestellungen auslösen.

Zusätzlich zu diesen unternehmensinternen Verbindungen müssen zahlreiche externe Dienstleister in das Netzwerk des Supermarkts gelangen, denn viele Filialisten haben bedeutende Teile der Arbeiten in ihren Filialen bereits ausgelagert: so werden beispielsweise Kassensysteme, Kühltruhen und Getränkerückgabeautomaten schon heute vielerorts per IP-Verbindung durch externe Dienstleister in Echtzeit überwacht und gewartet. Die Inhalte auf den digitalen Werbedisplays werden von einer externen Werbeagentur direkt über eine Internet-Verbindung eingespeist, die Heizungssteuerung bezieht die Klima-Prognose von einem Wetter-Server, die VoIP-Telefone nutzen eine externe SIP-Telefon-Anlage.

Während es beim ersten Beispiel um die reine Trennung von Datenströmen ging, ist die Gemengelage im Supermarkt ungleich komplexer. Neben der Trennung unterschiedlicher Datenströme muss sichergestellt sein, dass die zahlreichen externen Dienstleister jeweils nur auf die Anwendung und Ressource zugreifen können, für die sie verantwortlich sind.

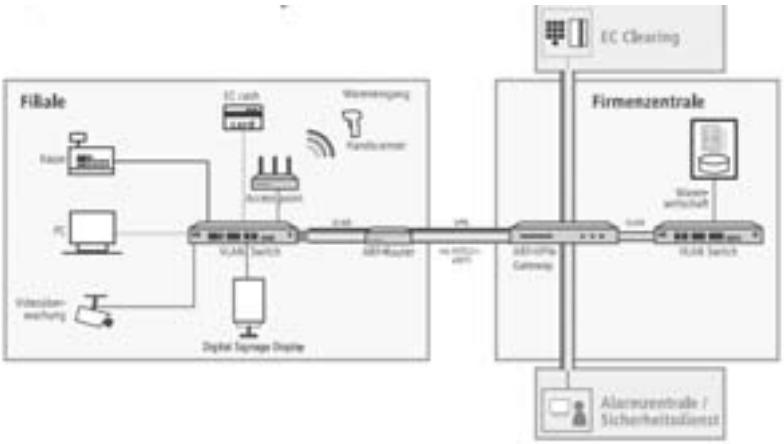

Abbildung 4: Virtualisierung im Supermarkt

Nur über die konsequente, dynamische Virtualisierung des gesamten Netzes inklusive der WAN-Verbindungen der Filiale kann dies wirtschaftlich realisiert werden. Andernfalls müsste aus Sicherheitsgründen eine Vielzahl von Netzen aufgebaut und eine Vielzahl an Internet-Anbindungen betrieben werden. Die Kosten für Geräte, Wartung, Energieverbrauch und Leitungen wären auf Dauer nicht tragbar.

Im Rahmen der Virtualisierung des Supermarkt-Netzes wird für jede Anwendung bzw. jeden Dienstleister ein eigenes virtuelles IP-Netzwerk eingerichtet, für das ein spezieller IP-Adresskreis und separate Routing-Einstellungen definiert werden. Der Netzabschnitt für die Kassenabrechnung kann so z. B. an die IP-Adressen angepasst werden, die der Betreiber in seiner VPN-Struktur verwendet. Im hausinternen LAN werden die IP-Netze zusätzlich über entsprechende VLAN-Tags markiert, die über einen VLAN-fähigen Switch getrennt werden. Alle anderen Teilnehmer können nicht auf dieses Netzwerk zugreifen.

Die Einsparpotentiale sind enorm, lassen sich jedoch aufgrund der sehr unterschiedlichen Szenarien nur für Einzelfälle genauer beziffern: Auslagerung arbeitsintensiver Dienstleistungen an günstige, externe Anbieter; Minimierung der Hardware-Ausstattung (Access Points, Switches und Router); Wegfall von Leitungskosten durch Mehrfachnutzung der Internet-Verbindung z. B. für EC-Zahlung, Warenflusslogistik und die Anbindung externer Dienstleister; Minimierung des Verkabelungsaufwands durch konsequente Kommunikation über IP-Netze (ein Netz für alles); massive Einsparungen beim Energiebedarf.

4 Fazit

Die hier skizzierten Beispiele lassen sich auf viele andere Bereiche übertragen. Unternehmen und Institutionen profitieren massiv von den Möglichkeiten der konsequenten Netzwerkvirtualisierung. Einerseits durch massive Einsparungen bei Hardware, Installation, Betrieb und Nebenkosten, andererseits aber auch durch ganz neue Interaktionsmöglichkeiten z. B. mit externen Partnern wie Kunden und Lieferanten und durch ein deutlich höheres Maß an Sicherheit, das sich durch die sehr flexible Lenkung von Datenströmen und Zugriffsberechtigungen erzielen lässt.

Voraussetzungen hierfür ist der konsequente Einsatz weithin bekannter Virtualisierungskonzepte wie VPN, VLAN und Multi-SSID in Kombination mit der Virtualisierung der IP-Netze und Router mittels ARF und der Weiterführung der getrennten Übertragung übers WAN mittels PPTP.

Moderne Kommunikationskomponenten integrieren diese Funktionalitäten standardmäßig, so dass für eine kostensparende Virtualisierung keine zusätzliche Software-Lösung erforderlich ist.