

Schwerpunktthema

SIP Trunking

Vom Ende der klassischen TK

von Dr. Michael Wallbaum

Laut einer Umfrage haben 16% der deutschen Unternehmen den Schritt zu VoIP bereits hinter sich. Die überwiegende Mehrheit telefoniert zwar noch konventionell, aber dennoch ist der Zug Richtung VoIP schon lange abgefahren. Hierzu muss man sich eigentlich nur die Produktpalette bzw. -pflege der großen Hersteller anschauen. Von Alcatel-Lucent bis Siemens gehen die Entwicklungskapazitäten fast ausschließlich in den Aufbau reiner VoIP-Lösungen. Quereinsteiger und Exoten wie Microsoft und SER kümmern sich gar nicht erst um klassische Telefonie.



Bis der Umbruch in allen Unternehmen vollzogen ist werden allerdings noch einige Jahre ins Land gehen. Die Carrier sind hier bereits weiter, denn sie stellen ihre Netze Zug um Zug auf die so genannte Next Generation Network (NGN) Architektur um. Im Kern arbeiten die Carriernetze dann paketvermittelt auf Basis von IP und den hierauf aufbauenden Protokollen wie z.B. SIP. Folgt man den Ankündigungen von T-Systems, KPN, BT und Co., so sind die konventionellen Telefonnetze in drei bis vier Jahren Geschichte.

weiter auf Seite 18

Zweitthema

Netzdesign 2008:

Was gehört auf die Agenda der Netzplanung?

von Dr.-Ing. Behrooz Moayeri

Der Investitionsstau, der von der Wirtschaftskrise ab 2001 verursacht wurde, ist mittlerweile in fast allen Unternehmen aufgelöst. Man gibt wieder Geld aus, auch für IT-Infrastruktur. Der Netzplaner ist wieder eine gefragte Person. Er müsste sich klonen lassen, um alle Projektaufträge bewältigen zu können, die auf ihn zukommen. An einer Orientierung anhand von Prioritäten führt kein Weg vorbei. Was gehört auf die

2008er Agenda der Netzplanung?

Wenn es nach manchem Hersteller ginge, sollten die Unternehmen am besten die gesamte IT-Infrastruktur austauschen, um ihre in die Jahre gekommenen Netze auf die neuen Herausforderungen vorzubereiten: Voice, Video, RZ-Vernetzung mit Höchstleistung, Authentifizierung, um nur ein paar Stichworte zu nennen. Aber selbst wenn das Unternehmen

bereit wäre, die Investition in eine komplett erneuerte Netzlandschaft zu tätigen, würde eine solche Herkulesaufgabe über die Möglichkeiten der für die Planung und Umsetzung zuständigen Personen hinaus gehen. Im Folgenden wird daher der Frage nachgegangen, wie viel Erneuerung wirklich erforderlich und was eher verzichtbar ist.

weiter auf Seite 6

Intensiv-Seminar

**Winterschule
2007: Intensiv-
Update auf den
letzten Stand der
Netzwerktechnik**

ab Seite 3

Geleit

**Unified
Communication:
Realitätsnähe
gefragt**

ab Seite 2

Spezial-Seminare

**Elektro-
magnetische
Verträglichkeit**

ab Seite 17

Zweitthema

Netzdesign 2008:

Was gehört auf die Agenda der Netzplanung?

Fortsetzung von Seite 1

Voice Readiness

Auch an der Schwelle zu 2008 bleibt „Voice Readiness“ das Schlüsselwort für die meisten Netzredesign-Projekte. Unter Voice Readiness wird eine breite Palette an Kriterien verstanden, mit denen die Eignung der Netze für die Einführung von Voice over IP (VoIP) geprüft werden soll. Mit diesen Kriterien wird das Netz in den folgenden Bereichen einem Review unterzogen:

- Verfügbarkeit
- Portdichte
- IP-Adresskonzept
- VLAN-Konzept
- Stromversorgung
- Quality of Service (QoS)
- Sicherheit
- Service Level Management

Die „Nichteignung“ gemäß einem dieser Kriterien zieht ein Netzredesign nach sich. Im Folgenden wird diskutiert, ob dies in jedem Fall so sein muss.

Verfügbarkeit

Das Hauptargument, mit dem begründet wird, dass die Einführung von VoIP eine wesentliche Erhöhung der Verfügbarkeit der Netze erfordere, ist in der Abbildung 1 schematisch dargestellt.

Bisher nutzen Datenanwendungen und Telefonie weitgehend entkoppelte, von einander unabhängige Infrastrukturen: Die Telefonanlage und die daran angebotenen Endgeräte sind weitgehend unabhängig von der IP-Infrastruktur, den PCs und den Servern. Der typische Satz eines Verfechters unabhängiger Infrastrukturen lautet: „Wenn mein PC nicht funktioniert, muss ich immer noch zum Telefon greifen und die Hotline anrufen können.“



Dr. Behrooz Moayeri ist Leiter des Competence Centers Netze bei ComConsult Beratung und Planung GmbH, Aachen. Zu seinen Arbeitsschwerpunkten gehören neben Netzdesign die Bereiche IT-Sicherheit, WAN, Telekommunikationsanlagen und Voice over IP.

Die Einführung von VoIP bedeutet, dass jetzt nicht nur die Datenanwendungen, sondern auch die Telefonie auf die IP-Infrastruktur angewiesen ist. Fällt diese aus, ist der Benutzer von jeglicher Kommunikation abgeschnitten - so zumindest das von den Skeptikern an die Wand gemalte Schreckgespenst.

Kein Zweifel: die Verfügbarkeit der IP-Infrastruktur ist mittlerweile für fast alle Unternehmen lebenswichtig. Kaum ein Unternehmen kann ohne IP-Infrastruktur weiter arbeiten. Und das nicht erst seit der Einführung von VoIP. In vielen Unternehmen gibt es noch wichtigere Anwendungen als Telefonie. Eine hochverfügbare IP-Infrastruktur ist unvermeidlich.

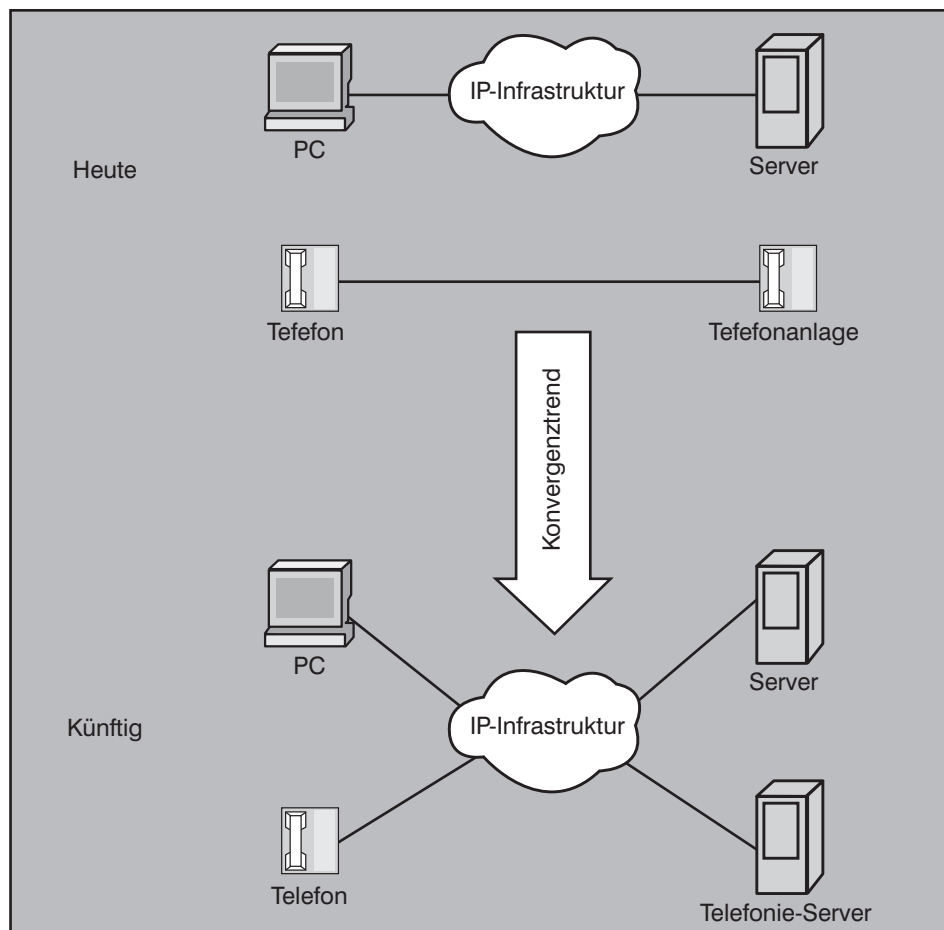


Abbildung 1: Auswirkung der Konvergenz auf die Verfügbarkeit

Netzdesign 2008: Was gehört auf die Agenda der Netzplanung?

Die IP-Infrastruktur ist jedoch ein komplexes Gebilde, das aus lokalen Netzen und Weitverkehrsnetzen besteht. Oft gibt es eine signifikante Diskrepanz zwischen der Verfügbarkeit des LAN und des WAN. Selbst für sehr viel Geld ist eine WAN-Anbindung mit einer Verfügbarkeit von über 99,98 % kaum zu realisieren, was einfach mit der Restwahrscheinlichkeit zusammenhängt, dass bei allen Vorkehrungen irgendwann doch ein Standort von der Außenwelt abgeschnitten ist. Eine durchschnittliche Ausfallzeit von zwei Stunden pro Jahr würde ungefähr der Verfügbarkeit von 99,98 % entsprechen. Sind selbst keine zwei Stunden Ausfall pro Jahr zu verkraften (man denke an eine Fabrik, ein Kraftwerk etc.), benötigt der Standort eben für alle Prozesse mit höheren Verfügbarkeitsanforderungen eigene Ressourcen. Diese können eigene Server sein, ein eigener Zugang zum öffentlichen Telefonnetz und - vor allem ein hochverfügbares LAN (siehe Abbildung 2).

Das hochverfügbare LAN selbst kann wiederum so aufgebaut sein, dass Teile davon nahezu 100% ausfallsicher sind, andere Teile aber aus wirtschaftlichen Gründen mit einer niedrigeren Verfügbarkeit auskommen.

LAN-Hochverfügbarkeit wird allzu häufig mit redundanter Hardware gleich gesetzt. Die Erfahrung hat jedoch gezeigt, dass die häufigste Ursache von LAN-Ausfällen nicht die Hardware ist. Netz-Hardware arbeitet mittlerweile sehr stabil und fällt sehr selten aus. Häufiger kommt es zu einem durch einen Software-Fehler der Netzkomponenten verursachten Ausfall. Dagegen hilft jedoch keine redundante Hardware. Im Gegenteil: manche Redundanzmechanismen schaffen erst die Anfälligkeit der Netze bei Software-Problemen.

Aber die unumstrittene Nummer 1 als Ursache von LAN-Ausfällen ist menschliches Versagen. Fast alle Ausfälle passieren nach Änderungen im Netz. Bei solchen Änderungen wird häufig nicht alles bedacht. Durch Unaufmerksamkeit kann es zu großen Netzausfällen kommen, so wie zum Beispiel durch falsche Rangierung oder durch fehlerhafte Routing-Konfiguration Netzschleifen entstehen.

Deshalb sind bei der Sicherstellung einer hohen Verfügbarkeit des Netzes Disziplin und ein geregelter, minutiös eingehaltener Change-Prozess wichtiger als Hardware-Redundanz. Ebenfalls wichtig ist ein möglichst einfaches Design, welches die Wahrscheinlichkeit der Auswirkung von Software-Bugs in den Netzkomponenten minimiert – einfach durch weniger Soft-

ware bzw. Beschränkung auf Nutzung jener Features der Netzkomponenten, die tausendfach erprobt sind und keine Überraschungen mehr bergen. Außerdem zu empfehlen ist eine Testumgebung, in der jede neue Konfiguration, jede neue Anwendung und jede weitere wesentliche Änderung im Netz zunächst erprobt wird. In einer Testumgebung werden manchmal Fehler entdeckt, die ohne solche Tests das produktive Netz lahm legen würden.

Portdichte

Mit der Einführung der IP-Telefonie verdoppelt sich ungefähr die Anzahl der an das IP-Netz angeschlossenen personengebundenen Endgeräte. Der Netzplaner steht vor der Aufgabe, beinahe 100% mehr Ports im Endgerätebereich zur Verfügung zu stellen. Die Mehrkosten für diese Erweiterung der lokalen Netze beschränken sich je nach Lösung für dieses Problem nicht nur auf die Kosten für die aktiven Komponenten, sondern beinhalten auch die wesentlich höheren Kosten für die passive Verkabelung. Insbesondere bei Neubauten stellt sich die Frage, welche Anschlussdichte bei der Verkabe-

lung vorgesehen werden muss. Die Tertiärverkabelung macht 20 bis 25 % der Gesamtkosten für ein LAN aus. Deshalb ist die Frage berechtigt, ob zwei getrennte Kupferkabelsegmente für den PC und das IP-Telefon wirklich sein müssen. Um die Mehrkosten für die erhöhte Portdichte einzusparen, entscheiden sich viele Unternehmen für die Nutzung der in viele IP-Telefone integrierten Mini-Switches. Diese Entscheidung ist angesichts der damit verbundenen Kosteneinsparung nachvollziehbar.

Gleichwohl muss man berücksichtigen, dass mit der Kaskadierung von Telefonen und PCs einige neue Netzfunktionen, die von wem auch immer auf die Agenda gesetzt worden sind, nicht mehr genutzt werden können. Bis heute ist die Kombination aus dem Anschluss der PCs an die Mini-Switches der Telefone und der dynamischen, von der Authentifizierung gesteuerten Zuordnung von PC und Telefon zu separaten VLANs ein ungelöstes Problem.

Die Kaskadierung von PC und Telefon würde auch den Betrieb des PCs mit einer Bitrate von 1 Gbit/s erschweren, denn

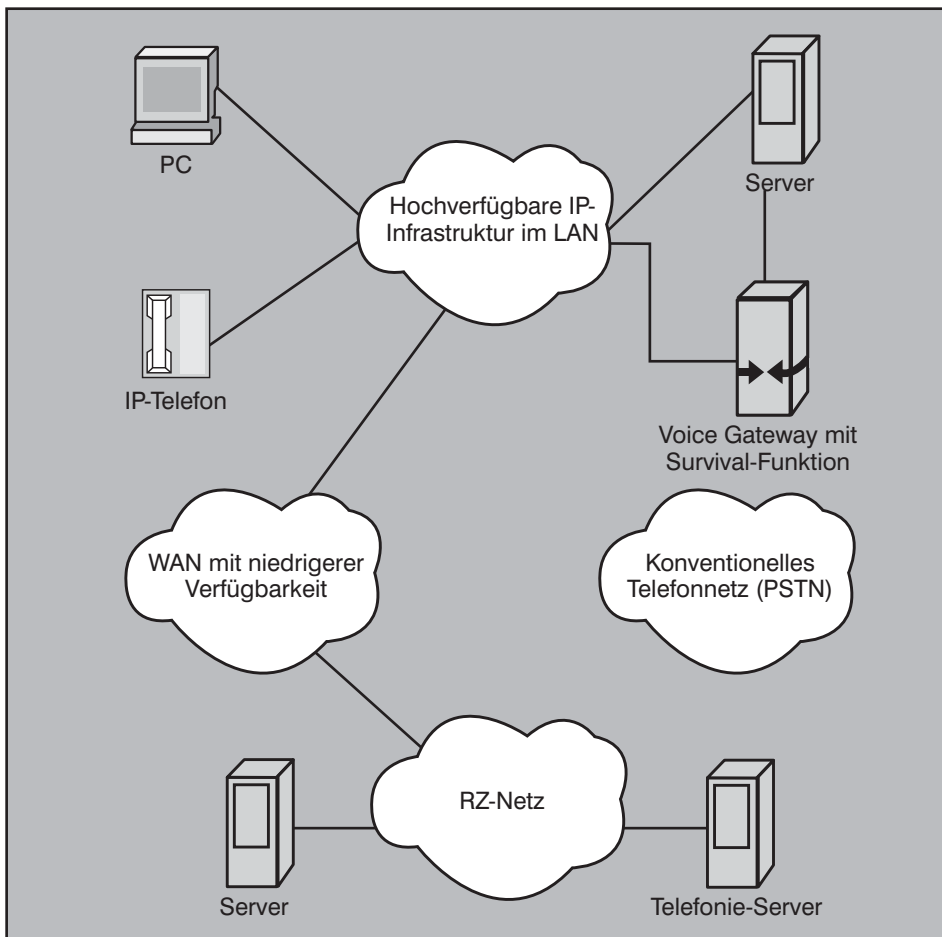


Abbildung 2: Hochverfügbare Umgebung

Netzdesign 2008: Was gehört auf die Agenda der Netzplanung?

Stand heute bieten nur wenige IP-Telefone Gigabit Ethernet Ports an. Will sich die Netzplanung den Freiheitsgrad vorenthalten, die PCs per Gigabit Ethernet anzubinden, dürfen nur bestimmte Telefone eingesetzt werden, d.h. es gibt dann Einschränkungen für die IP-Telefonie-Planung. Auch wenn die Zahl der Telefone mit Gigabit-Unterstützung zunimmt, haben diese Telefone die Gemeinsamkeit, dass sie wesentlich mehr Strom verbrauchen und in die Klasse 3 gemäß IEEE 802.3af, dem Standard für Power over Ethernet (PoE), fallen. Die Mehrkosten für diesen erhöhten Stromverbrauch beschränken sich nicht auf die vom Telefon selbst verbrauchte Energie, sondern beinhalten auch Mehrkosten für teurere Switches, mehr Klimatisierungsleistung und USV-Leistung in den Technikräumen etc.

Geht also die Kaskadierung mit der Lösung „Gigabit und PoE an allen Ports“ einher, bleibt von der mit der Kaskadierung beabsichtigten Kosteneinsparung nicht mehr viel übrig.

IP-Adresskonzept

Nicht nur mehr Ethernet-Ports, sondern auch mehr IP-Adressen werden benötigt. Unternehmen, die ihre IP-Adressen bisher ohne Berücksichtigung der IP-Telefonie vergeben haben, brauchen ein Redesign des IP-Adresskonzeptes. In großen Unternehmen kann allein die ungefähre Verdoppelung der benötigten IP-Adressen ein Problem sein, wenn der insgesamt einem LAN zugewiesene IP-Adressbereich ohnehin knapp bemessen ist. Das Ausmaß des Redesigns kann in solchen Fällen sogar das WAN einschließen, wenn der jedem Standort zugeordnete IP-Adressbereich nicht mehr ausreicht. Einige sehr große Unternehmen würden auch mit dem oft genutzten privaten IP-Adressbereich 10.x.x.x nicht mehr auskommen. Bei solchen Unternehmen wird allein die Findung des zusätzlich benötigten Adressraums ein Problem sein.

Sollte man also auf IPv6 setzen? Leider ist IPv6 nur als eine langfristige Lösung zu sehen. Die Geräte und Anwendungen sind noch nicht ganz „IPv6 ready“. Selbst wenn alle Geräte und Anwendungen volle IPv6-Unterstützung bieten würden, wäre der Aufwand für die Umstellung großer Netze auf das neue Protokoll immens.

So muss man sich auch in 2008 mit IPv4 und den damit verbundenen Adressengpässen herumschlagen. Unternehmen, die weder über genügend registrierte Adressen verfügen noch mit dem 10er Adressbereich auskommen (dabei handelt es sich aber um sehr wenige, sehr große, weltweit

agierende Firmen), bleibt wohl nichts anderes übrig, als zum Beispiel die bisher reservierten Bereiche 173.x.x.x bis 185.x.x.x zu nutzen, ohne Gewähr dafür, dass dieses Wildern im reserviertem Gefilde künftig ohne Konsequenzen für die externe Kommunikationsfähigkeit des Unternehmens bleibt.

Die meisten Unternehmen kommen zumindest mit dem insgesamt ca. 16 Millionen Adressen und ca. 65.000 Subnetze der Class-C-Größe bietenden 10er Bereich aus. Viele Unternehmen müssen aber mit den IP-Adressen besser haushalten und dürfen diese nicht mehr wie bisher verschwenden. Im engen Adressraum muss man eben etwas näher zusammerrücken.

Das IP-Redesign beschränkt sich aber nicht nur auf die Findung neuer Adressbereiche. Es geht auch darum zu entscheiden, ob für die IP-Telefone Subnetze vorgesehen werden, die von den Subnetzen anderer Endgeräte getrennt sind. Diese Frage hängt untrennbar mit dem VLAN-Redesign zusammen.

VLAN-Konzept

Die meisten IP-Telefonie-Hersteller empfehlen den Anschluss von IP-Telefonen an dedizierte Virtual Local Area Networks (VLANs). Viele Unternehmen folgen dieser Empfehlung. Einige Argumente dafür sind wie folgt:

- Für die Datenanwendungen und die Telefonie gelten manchmal verschiedene Sicherheitsrichtlinien (ob aus nachvollziehbaren oder vielleicht nicht mehr plausiblen Gründen), sodass gefordert wird, die Telefone von den Datenendgeräten zu trennen.
- Die Telefonie ist für manche Unternehmen wichtiger als jede Datenanwendung, so dass man die Telefonie vor denkbaren Beeinträchtigungen aus dem Datennetz schützen muss.
- Teilweise müssen nicht nur die zu den Datenanwendungen und zur Telefonie gehörenden Informationsströme, sondern auch die Zuständigkeiten für den Betrieb der beiden Netzbereiche separiert werden, etwa wenn ein Service Provider die Telefonie im Unternehmen als „Managed Service“ realisiert und daher die Mischung der Telefonie mit anderen Applikationen in gemeinsamen Broadcast-Domänen als problematisch angesehen wird.

Für viele Unternehmen bedeutet die Notwendigkeit der Einrichtung eigener VLANs für IP-Telefone ein vollständiges Redesign ihrer Netze. Der Teufel steckt dabei in den Details. Wenn eine VLAN-Trennung eine Art Sicherheitsmaßnahme darstellen soll, stellt sich die Frage, wie zu verhindern ist, dass die Benutzer durch das einfache Anschließen von PCs an die für Telefone vorgesehenen Dosen (absichtlich oder aus Versehen) diese Sicherheitsmaßnahme umgehen?

Seminar



Winterschule 2007 - Intensiv-Update auf den letzten Stand der Netzwerktechnik 03.12. - 07.12.07 in Aachen

Die Winterschule 2007 bringt Sie in 5 Intensiv-Tagen auf den neuesten Stand. Die ausgewählten Themen repräsentieren die wichtigsten Diskussionen und Entwicklungen der letzten Monate, zeigt neue Technologien in der Übersicht, analysiert die wichtigsten Entwicklungen und beleuchtet aktuelle Produktrends. Damit wendet sich die Winterschule speziell an erfahrene Teilnehmer/Innen, die den Betrieb ihrer bestehenden Netzwerke weiter optimieren und neue Entwicklungen und Technologien kennen lernen wollen.

Preis: € 2.290,- zzgl. MwSt.



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

Netzdesign 2008: Was gehört auf die Agenda der Netzplanung?

Die Netzplanung muss auf solche Fragen antworten, zum Beispiel so:

- Alle Ports für Telefone werden so konfiguriert, dass über diese Ports ankommende Pakete nur dann in die den Telefonen vorenthaltene VLANs übertragen werden, wenn sie einen bestimmten VLAN-Tag im Header gemäß IEEE 802.1Q führen. Es wird verboten oder technisch verhindert (durch Verweigern von Administrationsrechten für PCs), dass die Benutzer die Netzadapter ihrer PCs für die Nutzung der Telefonie-VLANs konfigurieren. Und es wird verboten, dass Fremdgeräte an das Netz angeschlossen werden.
- Für die Telefone und PCs werden separate Dosen vorgesehen. Die Telefone werden nach IEEE 802.1X authentifiziert, und der von jedem Telefon genutzte Port auf dem Access Switch wird automatisch dem jeweils genutzten Telefonie-VLAN zugeordnet. Die Mini-Switches in den Telefonen werden nicht genutzt und administrativ deaktiviert.

Aber die Verhinderung der Nutzung von Telefonie-VLANs durch andere Endgeräte ist nicht alles. Es ist auch zu klären, wie im Netz mit den Telefonie-VLANs umgegangen wird. Ist die VLAN-Trennung als Sicherheitsmaßnahme vorgesehen, ist es wohl nicht sehr sinnvoll, die Telefonie-VLANs in der erstbesten Layer-3-Instanz wieder mit anderen VLANs zusammenzubringen. Die VLAN-Trennung bleibt nur dann konsequent, wenn es auch auf der Ebene von Routing (Layer 3) eine Trennung zwischen der Telefonie und anderen Applikationen gibt. Und dies führt in den meisten Unternehmen automatisch zu einem Redesign des Routing-Konzeptes. Policy-based Routing, Virtual Routing and Forwarding (VRF) oder Multi-Protocol Label Switching (MPLS) können eingesetzt werden, um die Telefonie auch auf Layer-3-Ebene von anderen Anwendungen zu trennen. Als nicht gerade wirtschaftliche Alternative bietet sich auch die vollständige physikalische Trennung der Netze an.

Stromversorgung

Einige Unternehmen sehen vor, dass die IP-Telefone wie alle anderen Endgeräte auch am Ort ihres Einsatzes über Netzteile mit Strom versorgt werden. Dies ist eine Abkehr von der zentralen Stromversorgung von Telefonendgeräten über Telefonkabel, die in der konventionellen Telefonie für die meisten Endgeräte selbstverständlich ist.

Für andere Unternehmen ist eine solche Lösung aus verschiedenen Gründen nicht akzeptabel, unter anderem:

- Man will am Arbeitsplatz nicht noch einen zusätzlichen Verbraucher an das Stromnetz anschließen müssen, was häufig aufgrund der nicht ausreichenden Anzahl von Anschlüssen den Einsatz von Mehrfachsteckdosen nach sich zieht.
- Der Einsatz von Netzteilen und noch mehr Kabeln am Arbeitsplatz wird manchmal abgelehnt, sei es zum Beispiel aus Platzgründen oder aus Gründen des Brandschutzes.
- Während Telefonanlagen häufig batteriegepuffert arbeiten und zumindest bei kurzzeitigen Stromausfällen unterbrechungsfrei weiter arbeiten, gilt das für die meisten Steckdosen am Arbeitsplatz nicht.

Diese Unternehmen entscheiden sich für Power over Ethernet zur Versorgung von IP-Telefonen. Neben der Nutzung von konventionellen Netzteilen für die IP-Telefone, die in der Abbildung 3 als die oberste Lösung dargestellt ist, bieten sich die folgenden Varianten:

- Inline Power, d.h. Versorgung des Verbrauchers mittels einer der Signalspannung überlagerten Gleichspannung (s. zweite Lösung von oben in der Abbildung 3). Diese Variante wird gemäß dem bisherigen Standard IEEE 802.3af nur vom so genannten „Endpoint Power Sourcing Equipment (PSE)“ unterstützt, d.h. einer Stromquelle, die in die Access Switch integriert ist. Bei dieser Lösung müssen die Access Switches PoE mit der ausreichenden Leistung für die anzuschließenden Telefone unterstützen.

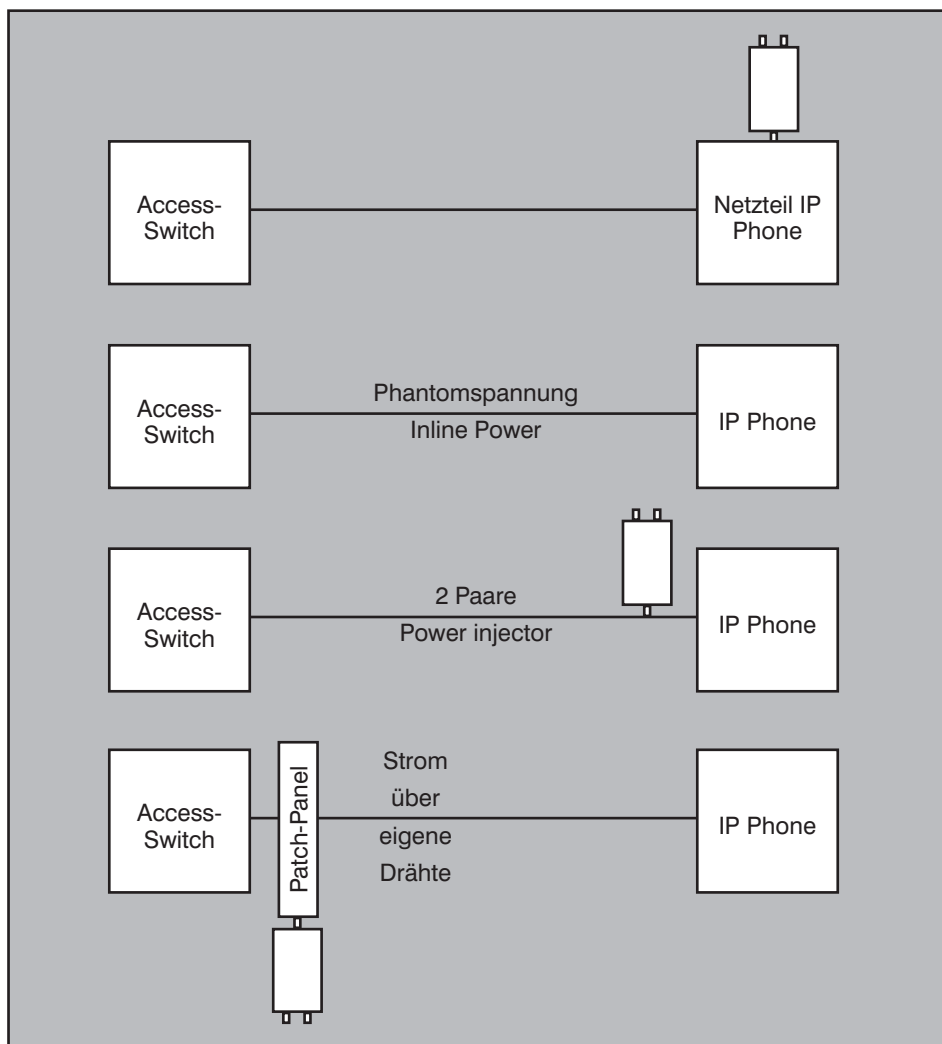


Abbildung 3: Varianten bei der Stromversorgung von IP-Telefonen

Netzdesign 2008: Was gehört auf die Agenda der Netzplanung?

- Einsatz von so genannten Midspan PSE, d.h. Geräten, die gemäß dem bisherigen Standard IEEE 802.3af das als Powered Device (PD) bezeichnete Endgerät über dedizierte, von Ethernet nicht genutzte Drähte mit Strom versorgen. Dabei kann das Midspan PSE entweder ein so genannter Power Injector am Arbeitsplatz sein (dritte Lösung von oben in der Abbildung 3), was allerdings die Vorteile der zentralen Stromversorgung nicht bietet, oder das in der letzten Lösung gemäß Abbildung 3 dargestellte im Bereich des Access Switches eingesetzte Midspan PSE, zum Beispiel in Form eines Power Patch Panels. Nach dem bisherigen Standard sind solche Geräte nicht mit 1000BaseT vereinbar, weil es bei 1000BaseT keine freien Adern gibt.

Die zentrale Stromversorgung von IP-Telefonen bietet zwar den Vorteil der Unabhängigkeit der Telefonie vom Stromnetz am Arbeitsplatz, aber diesen Vorteil muss man sich manchmal mit erheblichem Aufwand in den Technikräumen und bei den Switches erkaufen. Je leistungsfähiger und intelligenter die IP-Telefone, umso größer ist die Wahrscheinlichkeit, dass sie nicht mehr der PD-Klasse 1 oder 2 gemäß dem PoE-Standard, sondern der Klasse 3 entsprechen. Spätestens dann (wenn nicht sogar schon mit Klasse-2-Geräten) kommt man mit den bisher eingesetzten preiswerten Access Switches nicht mehr aus. Außerdem ist der Einsatz von PoE oft mit der Notwendigkeit verbunden, bisher nicht klimatisierte Schränke und Technikräume mit Klimageräten auszustatten. Hinzu kommen Kosten für die USV.

QoS

Genau jene Hersteller, die für ihre IP-Telefone dedizierte VLANs empfehlen, sprechen auch eine sehr starke Empfehlung für QoS im LAN aus. Diese „Empfehlung“ geht teilweise so weit, dass die Unterstützung für die eingesetzte Telefonielösung von deren Herstellern eingeschränkt wird, wenn sich der Kunde gegen QoS im LAN entscheidet. Der Autor musste immer wieder feststellen, dass bei Problemen mit der Sprachqualität oder Stabilität der IP-Telefonie die Hersteller zunächst versucht haben, das Netz für die Probleme verantwortlich zu machen. Um bei Problemen die uneingeschränkte Unterstützung des Telefonieherstellers nicht zu verlieren, geben viele Unternehmen der Forderung der Hersteller nach und führen QoS-Mechanismen ein, die manchmal ein komplettes Redesign der LANs bedeuten.

Dabei sind die meisten umgesetzten QoS-Konzepte nicht schlüssig und konsequent.

Hier sind einige der Schwachstellen, an denen viele QoS-Modelle kränkeln:

- In vielen QoS-Modellen wird die Sprachübertragung nur dann priorisiert, wenn Quelle oder Ziel der Audioströme Hardware-Telefone sind. Soft Phones werden dabei ignoriert. Aber Soft Phones spielen vor dem Hintergrund der Konvergenz der Anwendungen und der zunehmenden Anzahl von mobilen Benutzern, die auf ihren Notebooks Soft Phones nutzen, eine immer größere Rolle.
- Die normalerweise mit der obersten Priorität versehene Verkehrsklasse Voice ist teilweise nicht hinreichend vor absichtlichem oder unbeabsichtigtem Missbrauch geschützt.
- Der langfristig vielleicht interessanteste Bereich für den Einsatz von IP-Telefonie, nämlich das Internet, unterstützt überhaupt keine QoS.

Gerade die Erfolgsgeschichte der Internet-Telefonie zeigt, dass QoS für die Telefonie doch nicht die alles entscheidende Rolle spielt, die ihr von manchem Hersteller zugedacht wird.

Aber in den VoIP-Markt kommt spätestens seit dem Eintritt von Microsoft in denselben Bewegung, auch was QoS betrifft. Microsoft wirbt für PC-basierende Telefonie und rührt zugleich die Trommel gegen QoS. Der Hersteller hat mit seinem – leider proprietären – Codec RTAudio den Beweis erbracht, dass VoIP auch ohne QoS funktioniert. Dann stellt sich die Frage, ob vor diesem Hintergrund umfangreiche Redesign-Maßnahmen nur dadurch gerechtfertigt werden können, dass IP-Telefonie angeblich die flächendeckende Einführung von QoS erfordere.

Sicherheit

Die Netztrennung ist nicht der einzige Sicherheitsaspekt im Zusammenhang mit der Einführung von IP-Telefonie. Die konventionelle Telefonie hat ihre eigene, von anderen Netzen separierte Infrastruktur, in der bestimmte in IP-Netzen übliche oder denkbare Angriffsszenarien nicht relevant sind. Um solchen Szenarien zu begegnen, werden neben der Forderung nach getrennten VLANs auch andere Forderungen an das IP-Netz gestellt, zum Beispiel:

- Unter anderem um die IP-Telefonie zu schützen, wird der Ruf nach Port-basierender Authentifizierung gemäß IEEE 802.1X laut, s. den Abschnitt zum VLAN-Konzept in diesem Beitrag. Die

flächendeckende Einführung einer solchen Architektur gemäß IEEE 802.1X stellt ein gewaltiges Redesign der lokalen Netze dar, das oft mit immer noch ungelösten Problemen einher geht.

- Getrennte Netze für IP-Telefonie kommen angesichts der immer häufiger eingesetzten integrierten Anwendungen nie ohne Verbindungen zu den Netzen aus, über die Datenströme übertragen werden. Zu diesen Applikationen gehören Unified Messaging und Computer Telephony Integration (CTI). Die dafür erforderlichen Verbindungen zwischen Telefon- und Datennetzen sollten konsequenterweise eingeschränkt und mithilfe von Werkzeugen wie Firewalls kontrolliert werden - oder die Netztrennung ist nicht sinnvoll. Auf die Firewall-Verantwortlichen kommen vor diesem Hintergrund neue Herausforderungen im Bereich der Regeldefinition und des Firewallbetriebs zu.
- Noch komplizierter sind die Herausforderungen im Bereich Firewalling, wenn VoIP über Firewalls hinweg zu übertragen ist, zum Beispiel bei der externen Kommunikation oder zwischen Hard Phones und Soft Phones, wenn IP-Telefone und PCs an physikalisch oder logisch getrennte Netze angeschlossen werden. VoIP arbeitet mit dynamisch ausgehandelten UDP-Ports, die auf den Firewalls ebenso dynamisch und im Zuge des Auf- und Abbaus von Telefonie-Sessions geöffnet und - nicht zu vergessen - geschlossen werden müssen. Nicht jedes Firewall-System ist dazu in der Lage.
- Insbesondere wenn der bisherige Grad der Sicherheit der LANs für die Telefonie als nicht ausreichend empfunden wird, müssen auf Netzkomponenten neue Funktionen implementiert werden. Dazu gehört zum Beispiel die Verhinderung von Maskeradeangriffen oder die kontrolliertere Weiterleitung von DHCP-Paketen, mit denen Endgeräte konfiguriert werden.

Auch wenn der entscheidende Beitrag zur Sicherheit der IP-Telefonie nur auf Applikationsebene durch Verschlüsselung geleistet werden kann, kann die Netzplanung die Forderungen nach Sicherheitsmechanismen im Netz nicht ignorieren. Diese Forderungen sind nämlich für die Auswahl von Netzkomponenten - von LAN-Switches bis Firewalls - entscheidend.

Service Level Management

In der klassischen Telefonie ist das Ser-

Netzdesign 2008: Was gehört auf die Agenda der Netzplanung?

vice Level Management relativ einfach. Der Benutzer kann telefonieren, wenn die Telefonanlage und der dem Benutzer zugewiesene Port auf der Telefonanlage funktionieren. Die Telefonverkabelung und das Telefonendgerät fallen so gut wie nie aus. Die Situation bei der IP-Telefonie ist komplexer. Die monolithische Telefonanlage wird durch eine im IP-Netz verteilte Anordnung von Servern und Gateways abgelöst, und zwischen diesen zentralen Einrichtungen und den Endgeräten gibt es ein Gebilde namens IP-Netz, das aus mehr besteht als der reinen Verkabelung. Außerdem handelt es sich bei der IP-Telefonie immer noch um eine neue Technik mit mancher Kinderkrankheit wie schlechter Sprachqualität, die zwar meistens ihre Ursachen in den Telefoniekomponenten hat, aber allzu häufig auf das Netz geschoben wird.

So muss die Netzplanung an ein Service Level Management für das Netz denken, das mehr Parameter als bisher abdeckt. Damit der Netzbetreiber mit Fug und Recht behaupten und belegen kann, dass die von ihm verantwortete Infrastruktur alle Anforderungen der IP-Telefonie erfüllt, muss er nicht nur reaktiv messen können, wie groß Delay, Jitter und Packet Loss im Netz sind, sondern bei Bedarf auch in der Lage sein, rückwirkend nachzuweisen, dass diese Parameter zu einem Zeitpunkt oder über einen Zeitabschnitt in der Vergangenheit im grünen Bereich lagen. Der Netzbetreiber braucht neue Monitoring- und Reporting-Werkzeuge.

Anforderungen von Videoübertragung

Über die heißen Diskussionen zu Voice Readiness wird oft eine andere neue Anwendung im Netz übersehen, nämlich die Videoübertragung. Diverse Videostreams kommen auf die IP-Netze zu, darunter:

- IP-Videokonferenzen
- Videoüberwachung
- IPTV

Videokonferenzen können im WAN die Anforderungen an die Netzkapazität wesentlich erhöhen. In Zeiten von immer teurer werdenden Reisen und den damit verbundenen Risiken und Unannehmlichkeiten gehört die verstärkte Nutzung des Mediums Videokonferenz zu den vernünftigsten Maßnahmen, die Unternehmen vorsehen können. In vielen Fällen reicht die Leistung des WAN dafür nicht aus. Selbst bei ausreichender Leistung bleibt die Herausforderung, wie sich Videokonferenzen (samt der damit verbundenen Audioströme) und Telefonie im Netz vertragen. Bisher wird meistens vorgesehen, dass

Voice die höchste und Video die zweithöchste Priorität unter den differenzierten Verkehrsklassen belegen. Ist diese Zuordnung gerechtfertigt, wenn man bedenkt, dass eine Videokonferenz ohne Ton oder mit schlechtem Ton sinnlos ist und die Audio Streams einer Videokonferenz eigentlich genau so interaktiv und damit zeitkritisch sind wie die Telefonie?

Die Videoüberwachung wird in unserer immer unsicher werdenden Welt zunehmend beliebter. Das LAN muss plötzlich bis zu Bereichen ausgedehnt werden, die bisher unversorgt bleiben konnten: entlang der Zäune im Gelände, auf Parkplätzen, in Tiefgaragen etc. In diesen Bereichen herrschen teilweise raue Umgebungsbedingungen. Häufig fehlt dort ein Anschluss an das Stromnetz. Videokameras mit PoE-Unterstützung erfordern immer noch den Einsatz einer aktiven Netzkomponente im Umkreis von 100 Metern. Dazu müssen die Netzkomponenten manchmal an Stellen eingesetzt werden, die an alles andere als klimatisierte Technikräume erinnern. Hier entsteht der Bedarf nach mechanisch und thermisch robusten Switches, die uns von Industrial Ethernet her bekannt sind.

IPTV ist für die meisten Unternehmen noch kein Thema. Aber nicht nur die Aufgabe, Reden des Vorstandsvorsitzenden live in alle entlegenen Winkel des Unternehmens zu übertragen, zwingen einige Unternehmen dazu, IPTV über ihre Netze zu übertragen. Man denke zum Beispiel an Krankenhäuser. Immer mehr Kranken-

häuser lösen die Koax-Verkabelung für die Übertragung von Fernsehen in die Krankenzimmer durch IPTV ab. Ohne IP Multicasts würde die Übertragung von vielen Fernsehkanälen mit einer akzeptablen Qualität im IP-Netz nicht möglich sein. Aber IP Multicast ist nicht IP. Es handelt sich um ein anderes Protokoll mit eigenen Routing-Mechanismen und Adressstrukturen. Ein Multicast-Design ist nicht auf die leichte Schulter zu nehmen. Da gibt es viele Fragen, die von der Netzplanung beantwortet werden müssen, von der dynamischen Anforderung von Kanälen durch die Empfänger bis zur Auswahl und richtigen Konfiguration von IP Multicast Routing.

RZ-Vernetzung

Unternehmen konzentrieren ihre Server auf wenige Rechenzentren. Serverfarmen werden durch immer mehr Applikationen und Firmenfusionen immer komplexer. In Serverfarmen herrschen für die Vernetzung Gesetze, die sich fundamental von den Regeln der Client-Vernetzung unterscheiden.

Da ist zunächst die Frage der Anschlussdichte. Hunderte Ports müssen für immer kleiner werdende, immer zahlreichere Server in wenigen Schränken bereit gestellt werden. Das Medium Glasfaser kommt in RZs für die Versorgung der Server aus der Mode, da die Server meistens mit eingebauten 100BaseT-Ports geliefert werden und deren Nachrüstung mit LWL-Adaptoren

Seminar



Sicherheitsmechanismen für Voice over IP 26.11. - 27.11.07 in Neuss

In diesem Seminar wird vermittelt: was sich in Bezug auf Informationssicherheit mit der Umstellung auf VoIP ändert; welche Gefahrenpotenziale berücksichtigt werden müssen; welche Standards für VoIP-Sicherheit relevant sind; wie die Vertraulichkeit der Sprachkommunikation in IP-Netzen geschützt werden kann; worauf beim Design von VoIP-Umgebungen hinsichtlich Verfügbarkeit zu achten ist; wie die IP-Telefonie in vorhandene Sicherheitsstrukturen in Netzen einzubinden ist; welche Probleme bei VoIP über Vertrauensgrenzen hinweg entstehen und wie sie zu lösen sind; welche rechtlichen Aspekte bei VoIP-Sicherheit relevant sind.

Referent: Dr.-Ing. Behrooz Moayeri
Preis: € 1.390,- zzgl. MwSt.



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

Netzdesign 2008: Was gehört auf die Agenda der Netzplanung?

immer schwieriger wird. So wird schon die Planung der Kupferverkabelung in Serverräumen zu einer Herausforderung. Die „fliegende“ Verkabelung mittels Patchkabel führt bei solch hohen Anschlussdichten unweigerlich zum Chaos (s. Abbildung 4). So muss man auch in RZs eine fest installierte Tertiärverkabelung planen, aber mit welcher Struktur? Wie viele passive Verteiler sollte man vorsehen? Welches Maß an Konzentration von Kabeln ist noch handhabbar? Teilt man die RZ-Fläche in Parzellen auf, die jeweils ihre eigene Kupferverkabelung haben und über Lichtwellenleiter (LWL) mit zentralen Verteilern des RZs verbunden sind? Oder verkabelt man alles von einer zentralen Stelle aus? Ab einer bestimmten RZ-Größe führt an einer mindestens zweistufigen Netzstruktur mit Tertiärverkabelung in Kupfer und Sekundärverkabelung in LWL kein Weg vorbei. Die Sekundärverkabelung sollte sowohl Multimode- als auch Singlemode-Fasern beinhalten, Ersteres wegen der niedrigeren Preise für aktive Komponenten, Letz-

teres wegen der größeren Reichweite von Singlemode, die mit 10 Gbit/s, spätestens aber mit 100 Gbit/s auch in RZs relevant wird. Die Kupferverkabelung muss mindestens der neuen Kategorie 6 bzw. der neuen Klasse E entsprechen, denn mit der 2006 erfolgten Standardisierung von 10GBASE-T (IEEE 802.3an) und der Verfügbarkeit der ersten Serveradapter mit 10 Gbit/s ist damit zu rechnen, dass 10GBASE-T bald in die Rechenzentren Einzug findet.

Die Verkabelungsstruktur in Serverräumen ist nicht ohne Auswirkung auf die dortige logische Netzstruktur. Während man im Client-Bereich eine weitgehende Vermeidung von Switch-übergreifenden VLANs einhalten kann, ist dies im Serverumfeld oft deshalb nicht möglich, weil verschiedene Knoten eines Server-Clusters virtuelle IP-Adressen teilen müssen. Sind diese Knoten an verschiedene Switches angeschlossen, was aus Gründen der Ausfallsicherheit sinnvoll ist, muss oft ein und die

selbe IP-Adresse vom Switch zu Switch „wandern“ können. So müssen sich Layer-2-Broadcast-Domänen (VLANs) auf verschiedene Switches erstrecken. Dabei muss auch die Layer-2-Verbindung zwischen diesen Switches möglichst ausfallsicher sein. Denn bei einer Unterbrechung dieser Verbindung zerfällt die Broadcast-Domäne in zwei Teile; es kommt zum so genannten Split Subnet. Mit einem solchen nicht mehr zusammenhängenden Subnetz kann nicht mehr zuverlässig kommuniziert werden, weil die Pakete an dieses Subnetz mal in den einen und mal in den anderen Teil geroutet werden. Also braucht man einen Redundanzmechanismus auf der Ebene von Layer 2. Erstreckt sich das Server-VLAN auf nur zwei Switches, kann zwischen diesen eine redundante Layer-2-Verbindung mittels Link Aggregation realisiert werden. Dieses Verfahren ist das zuverlässigste und robusteste auf der Ebene von Layer 2. Zugleich können die redundanten Verbindungen parallel genutzt werden, d.h. Link Aggregation sorgt nicht nur für Ausfallsicherheit, sondern auch für Lastverteilung.

Oft wird jedoch gefordert, dass sich ein Server-VLAN auf mehr als zwei Switches erstreckt. In einigen Fällen soll ermöglicht werden, dass ein Server-VLAN in jeder Parzelle eines Rechenzentrums „abgreifbar“ ist, damit zum Beispiel die Knoten eines zugehörigen Server-Clusters beliebig im Rechenzentrum aufgestellt werden können. In solchen Fällen muss als Redundanzmechanismus auf Layer-2-Ebene Spanning Tree eingesetzt werden, denn unter den standardisierten Verfahren erlaubt nur Spanning Tree die Bildung einer sich auf mehrere Switches erstreckende, redundante Layer-2-Broadcast-Domäne, deren Verfügbarkeit von keinem „Single Point of Failure“ (einem einzelnen Switch oder einer einzelnen Verbindung) abhängig ist.

Die Kunden des Herstellers Nortel Networks haben das (leider proprietäre) Verfahren Split Multi-Link Trunking (SMLT oder Split MLT) schätzen gelernt (s. Abbildung 5).

Mit diesem Verfahren kommt man auch in großen RZs ohne Spanning Tree aus. Obwohl jede Broadcast-Domäne auf viele Switches verteilt und die Netzstruktur nicht schleifenfrei ist, kommt es auch ohne Spanning Tree und der damit verbundenen Blockierung von Links zu keiner Endlosübertragung von Paketen. Die beiden zentralen Layer-2-Switches bilden eine Art virtuellen Switch und leiten die Pakete schleifenfrei zum Ziel weiter. Die anderen Layer-2-Switches können auch von



Abbildung 4: Würden Sie hier gerne einen Fehler suchen?

Netzdesign 2008: Was gehört auf die Agenda der Netzplanung?

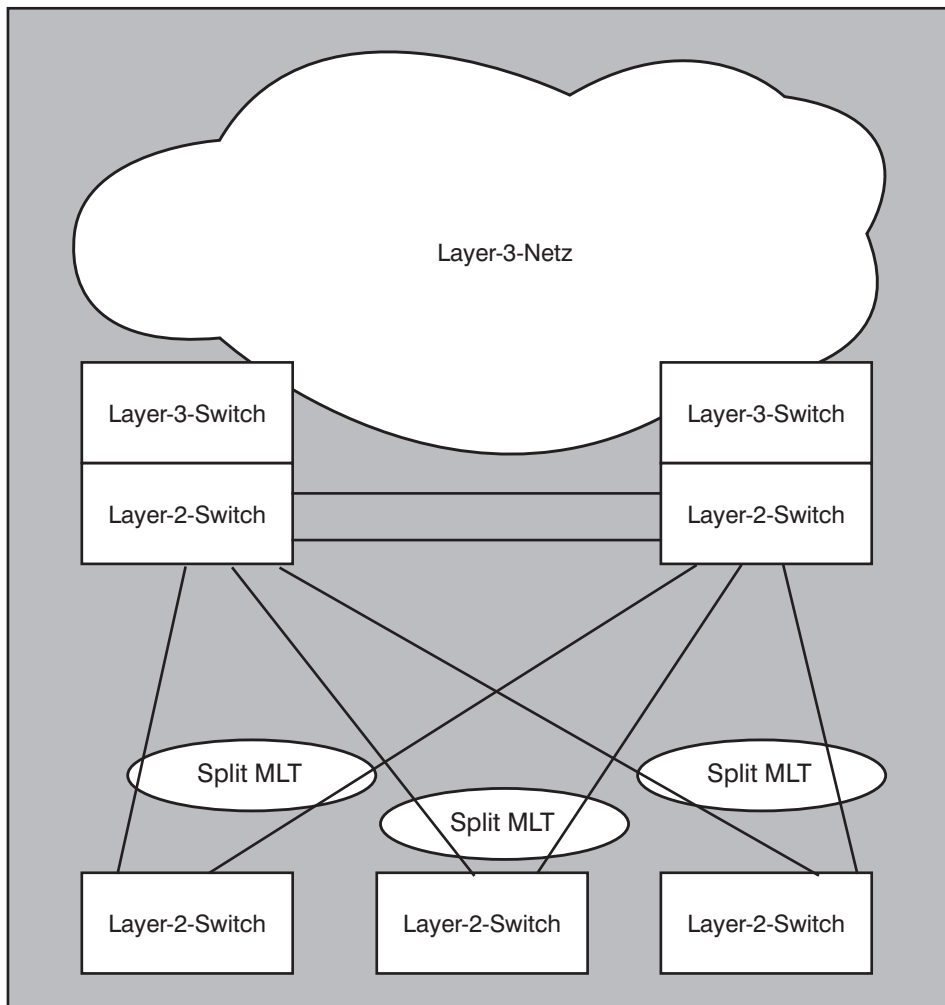


Abbildung 5: Split MLT von Nortel

anderen Herstellern sein, da sie keine andere Funktionalität als herkömmliche Link Aggregation benötigen.

Es wäre zu begrüßen, wenn das IEEE das bewährte SMLT-Verfahren auch standardisieren würde. Noch ist das Verfahren Nortel-spezifisch und erfordert den Einsatz von Komponenten dieses Herstellers als zentrale Layer-2-Switches.

10Gigabit Ethernet und jenseits davon

Der erste Bereich, in dem der Einsatz von 10Gigabit Ethernet sinnvoll ist oder sein wird, ist die Verbindung zwischen Switches im RZ-Bereich. Neue Server werden heute mindestens mit integrierten Gigabit Ethernet Ports ausgeliefert (siehe Abbildung 6).

Dies bedeutet, dass sich unter Umständen viele Server jeweils wenige Uplinks teilen müssen, was 10Gigabit Ethernet auf die Agenda der Netzplanung für RZs setzt. Insbesondere wenn Datensiche-

rungerungen über Ethernet durchgeführt werden müssen, kommt man häufig mit Gigabit Ethernet nicht aus. Die Einführung von 10Gigabit Ethernet geht allerdings langsamer voran als seinerzeit der Übergang zu Gigabit Ethernet. Der Standard IEEE 802.3z, der Gigabit Ethernet spezifiziert, wurde 1998 verabschiedet. Gemäß dem Diagramm in der Abbildung 6 wurden bereits fünf Jahre später, d.h. im Jahr 2003, alle Server bereits mit eingebauten Gigabit Ethernet Ports ausgeliefert. Der Standard IEEE 802.3ae für 10Gigabit Ethernet existiert seit 2002. Es hat jedoch fünf Jahre gedauert, bis in 2007 die ersten Intel-Server mit 10-Gbit-Interfaces zum Einsatz gekommen sind. Und es wird laut der Prognose in der Abbildung 6 noch weitere sechs Jahre dauern, bis 10Gigabit Ethernet im Serverbereich Gigabit Ethernet komplett verdrängt hat (bis 2013).

Das heißt: Die Erhöhung der Bitraten im LAN hat sich in den letzten Jahren verlangsamt. Die Mehrheit der Firmen setzt heute, fünf Jahre nach der Marktpremiere von 10Gigabit Ethernet, diese Technologie immer noch nicht ein. Ist in LANs eine Sättigung eingetreten?

Diese Frage ist nicht eindeutig zu beantworten. Vielleicht hat der Investitionsstau der letzten Jahre seinen Part dazu beigetragen, dass die Einführung von 10Gigabit Ethernet im Vergleich zu Gigabit Ethernet eher schleppend vor sich ging. Aber es ist nicht zu verkennen, dass es in den Unternehmensnetzen kaum Gigabit-Links gibt, die im hohen Lastbereich arbeiten. Wenn

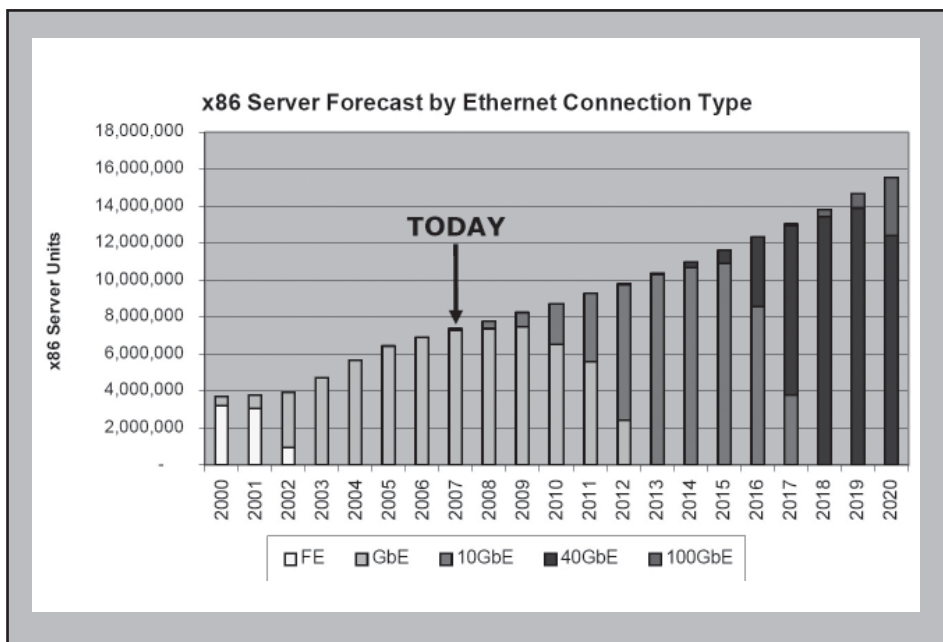


Abbildung 6: Ausstattung der verkauften Server mit Ethernet Ports verschiedener Bitrate (Quelle: http://iecc802.org/3/hssg/public/sept07/tutorial_01_0907.pdf)

Netzdesign 2008: Was gehört auf die Agenda der Netzplanung?

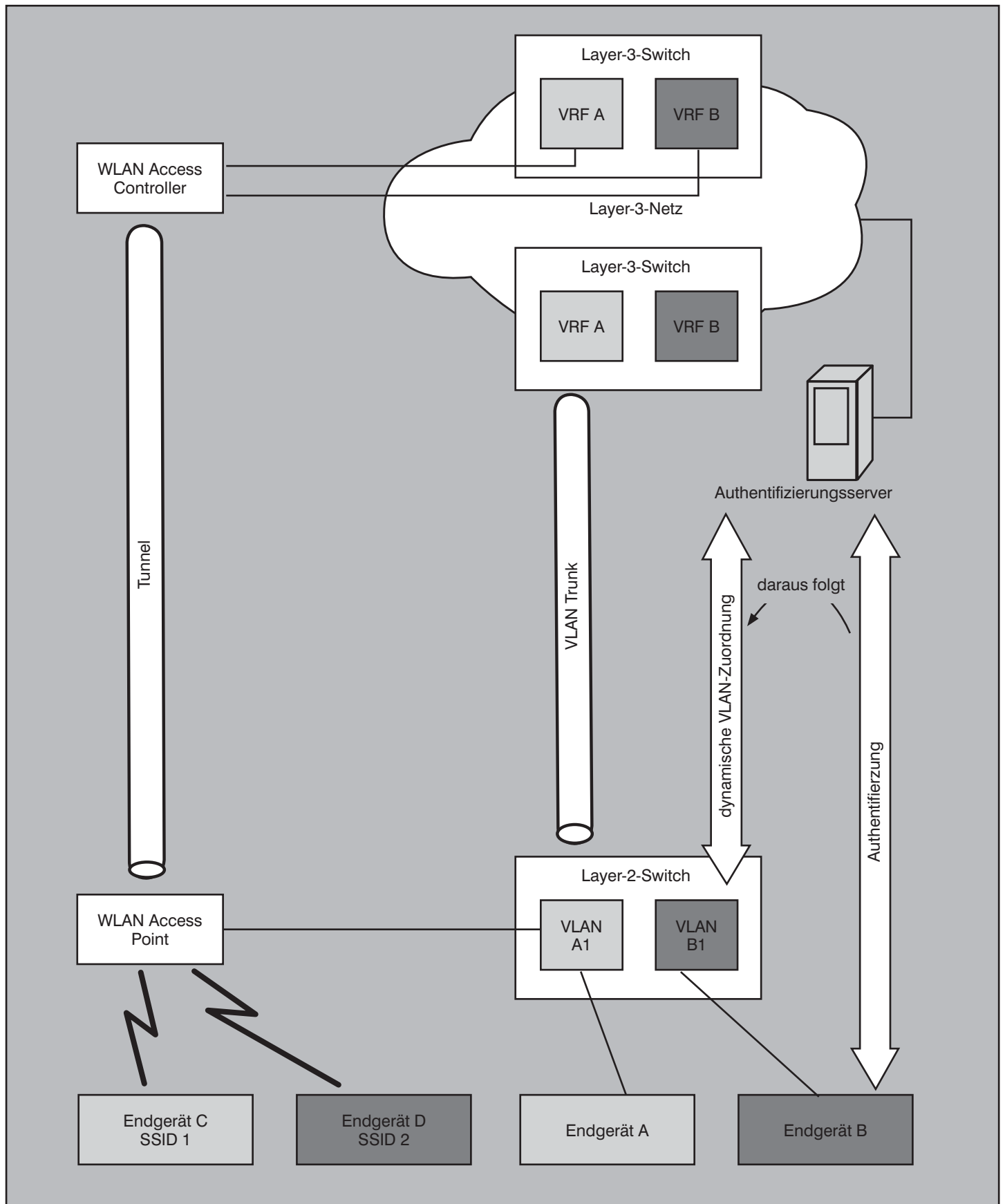


Abbildung 7: Mandantenfähiges LAN

 Netzdesign 2008: Was gehört auf die Agenda der Netzplanung?

die Gigabit Ethernet Links im Bereich von wenigen Prozent Last vor sich hindümpeln, muss man nicht unbedingt Tausende Euro pro Port für 10Gigabit Ethernet ausgeben.

Aber das IEEE scheint überzeugt zu sein, dass sich dies ändern wird. Sonst würde es keine High Speed Study Group (HSSG) geben, die sich das Ziel gesetzt hat, bis Mai 2010 den Standard mindestens für 100Gigabit Ethernet zu verabschieden (voraussichtlich zusammen mit der Spezifikation von 40Gigabit Ethernet).

Hier denkt man wohl zunächst eher an Service Provider Backbones als an Unternehmensnetze. Aber arbeiten die ersten Provider-Netze (und das Internet) in ihrem Kern mit 40 oder 100 Gigabit Ethernet, ist der Schritt zu bezahlbaren WANs mit 10Gigabit Ethernet für Unternehmen nicht mehr weit. Dann öffnen sich für die Unternehmen neue Möglichkeiten der RZ-Konsolidierung und der Virtualisierung ihrer Geschäftsprozesse, was wiederum zu mehr Kapazitätsbedarf in den RZ-Netzen führen wird.

Mandantenfähige Netze

In vielen Branchen ist der Bedarf entstanden, die Netze mandantenfähig in dem Sinne zu gestalten, dass ein und die selbe physikalische Infrastruktur von unabhängigen Firmen genutzt wird, die abgeschottete Virtuelle Private Netze (VPNs) brauchen. Beispiele für solche Umgebungen sind Industrieparks mit mehreren Firmen in einem Gelände. Vorbilder für derartige Netze sind die Plattformen der Service Provider, die bereits seit Jahren VPNs unterstützen. Bereits mit Technologien wie Frame Relay war es möglich, den teilnehmenden Unternehmen geschlossene Benutzergruppen zur Verfügung zu stellen, die von den Benutzergruppen anderer Unternehmen logisch getrennt waren, mit diesen aber die selbe physikalische Infrastruktur teilten. Später wurden ATM-Dienste nach dem selben Schema vermarktet. Und Stand der Technik für heutige VPNs sind solche auf der Basis von MPLS oder IPsec.

VPNs finden nun Einzug in die Domäne der LANs. Nicht nur dort, wo unabhängige Firmen in einem Gelände oder Gebäude angesiedelt sind, sondern auch innerhalb von einigen Unternehmen oder Verwaltungen müssen voneinander getrennte Vertrauensbereiche gebildet werden. Man denke zum Beispiel an die Netze der Polizei innerhalb von Netzen der Landesverwaltungen in Deutschland.

Können die Netzplaner noch mit Hinweis auf die immer weniger Sinn ergebende Trennung von Sprache und Daten die Einrichtung separater VLANs für IP-Telefonie erfolgreich verweigern, ist dieser Widerstand gegen logische Netztrennung in anderen Fällen weniger aussichtsreich. Die Forderung nach mandantenfähigen LANs wird mittlerweile in so vielen Umgebungen erhoben, dass die Planung solcher Strukturen zunehmend unvermeidbar wird.

Die WAN Service Provider können VPNs relativ einfach realisieren. Ein Gebäude wird normalerweise einem VPN zugeordnet, d.h. die Verbindung zu diesem Gebäude wird in der Regel statisch so konfiguriert, dass die über diese Verbindung empfangenen Pakete innerhalb des Provider-Backbones in ein bestimmtes VPN übertragen werden.

In LANs ist die Bildung von VPNs manchmal komplizierter. Man stelle sich ein Unternehmen vor, das neben eigenen Endgeräten auch Fremdgeräte netztechnisch versorgen, dabei aber diese an getrennte logische Netze anschließen will. Sind die eigenen und fremden Gerätepopulationen nicht physikalisch zu trennen, ist eine Port-basierende Authentifizierung die logische Konsequenz der Netztrennung zwischen eigenen und fremden Geräten, denn sonst könnte durch das Vertauschen der Ports ein Fremdgerät in das interne logische Netz gelangen. Um dies zu verhindern, müssen zumindest die eigenen Geräte sicher authentifiziert werden können, gemäß IEEE 802.1X und zum Beispiel mit Zertifikaten auf den Endgeräten. Wird ein Gerät als ein firmeneigenes Gerät sicher authentifiziert, kann daraus eine VLAN-Zuordnung abgeleitet werden. Der Authentifizierungsserver gibt dazu dem Access-Switch den Befehl, den vom Endgerät benutzten Port einem VLAN für firmeneigene Endgeräte zuzuordnen (s. Abbildung 7). Ein Fremdgerät, das nicht authentifiziert werden kann, wird mit einem anderen VLAN verbunden. Die verschiedenen VLANs auf Layer 2 sind verschiedenen logischen Routing-Instanzen auf Layer 3 (verschiedenen VRFs) zugeordnet.

Im Wireless LAN setzt sich die logische Netztrennung fort, indem für verschiedene Benutzergruppen verschiedene SSIDs (Service Set Identifiers) genutzt werden. Firmeneigene Geräte durchlaufen die selbe Authentifizierungsprozedur wie im verdrahteten LAN, und Fremdgeräte nutzen eine eigene SSID. In den Tunnels zwischen WLAN Access Points und WLAN Controllern werden die verschiedenen

Benutzergruppen ebenfalls auseinander gehalten, und der WLAN Controller verbindet diese Benutzergruppen mit unterschiedlichen VPNs.

Zusammenfassung

Neue Anforderungen setzen neue Themen auf die Agenda für die Netzplanung in 2008 und die Jahre danach. Zur Vorbereitung der Übertragung von Sprache über IP-Netze müssen vor allem mehr Ports und mehr IP-Adressen vorgesehen und Power over Ethernet eingeführt werden. Aber auch mehr Firewalls mit VoIP-Unterstützung, der bessere Schutz von LANs durch Mechanismen auf Switches und die Ausweitung von Monitoring und Reporting gehören auf die Tagesordnung.

IP-Videokonferenzen erfordern vor allem die Erhöhung der WAN-Kapazität, während Videoüberwachung die Ausdehnung von LANs auf bisher unversorgte Bereiche nach sich zieht. IPTV bedeutet in der Regel die Einführung von IP Multicasts.

Die RZ-Netze werden immer komplexer und müssen immer mehr Server aufnehmen. Die Verkabelungsplanung in Serverräumen wird damit zur Herausforderung. Im RZ-Bereich wird oft eine Layer-2-Virtualisierung gefordert, was mangels Alternativen oft zu Spanning-Tree-Strukturen in solchen Bereichen führt.

10Gigabit Ethernet kommt langsamer als damals Gigabit Ethernet, aber es kommt, und zwar zunächst im RZ-Bereich. Die nächsten Stufen der Weiterentwicklung von Ethernet sind auch in Sicht.

In vielen Bereichen ist der Bedarf entstanden, mandantenfähige Strukturen zu bilden, d.h. auf der Basis der selben physikalischen Infrastruktur eine logische Trennung zwischen Netzbereichen zu unterstützen, mit denen die Endgeräte von unabhängigen Firmen oder geschlossenen Benutzergruppen innerhalb von Unternehmen verbunden werden oder die Separierung von Fremdgeräten erlauben. Solche Strukturen sind am sinnvollsten mit einer Authentifizierung gemäß IEEE 802.1X und der daraus folgenden automatischen VLAN-Zuordnung zu kombinieren. Die VLAN-Trennung auf Layer 2 ist mit der logischen Trennung auf Layer 3 zu ergänzen, sonst bleibt sie inkonsequent.

Diese und andere Themen werden auf der diesjährigen Winterschule der ComConsult Akademie ausführlich behandelt. Die Veranstaltung findet vom 3. bis zum 7. Dezember 2007 in Aachen statt.