

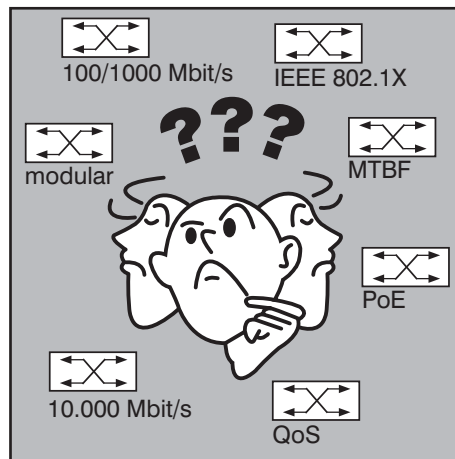
Schwerpunktthema

Auswahl von Access-Switches in modernen Datennetzen

von Dipl.-Ing. Hartmut Kell, Dipl.-Ing. Harald Krause

In den letzten Jahren stand bei den meisten Planungen die Auswahl der Komponenten für den Backbone-Bereich im Vordergrund; allen war klar, dass Fehler bei diesen sehr teuren Komponenten eine langjährige Last bedeuten müssen. Der Access-Bereich bot im Vergleich dazu - unter Vernachlässigung der unterschiedlichen Preise zwischen den verschiedenen Herstellern - kaum gravierende Unterschiede zwischen den angebotenen Systemen.

Die Auswahl beschränkte sich zumeist auf L2-Switches als modulare/nichtmodulare Systemen, mit 12, 24, 36 oder 48 10/100 Mbit/s-Lobe-Ports pro Gerät bzw. Modul, 2 Uplink-Ports bei den fest konfigurierten Systemen und den fast gleichen Redundanz-Lösungen. Die Situation hat sich ge-



Da fällt die Wahl schwer!

ändert: neben vollkommen unterschiedlichen Hardware-Ausstattungen werden unterschiedlichste, weitere Features angeboten, deren Nutzen zum Teil einer genauen Analyse bedarf. Dieser Artikel wendet sich an Netzwerk-Planer, die vor dem Problem stehen, welcher Switch-Typ im Access-Bereich am besten passt. Obwohl die Einsatzumgebungen sehr stark voneinander abweichen können zeigt die Planungserfahrung, gewonnen bei vielen Projekten, dass es einen Grundanteil an gleichen Kernanforderungen gibt, die stets zu beachten und zu bewerten sind. Ein Teil dieser Kernanforderungen soll im vorliegenden Artikel näher analysiert werden.

weiter auf Seite 23

Zweitthema

Quality of Service

von Dr. Frank Imhoff

Seit die Datenübertragung aus der modernen Kommunikationswelt nicht mehr wegzudenken sind, wird über die Notwendigkeit von Dienstgüte oder Quality of Service (QoS) diskutiert. Darunter werden in der Regel Obergrenzen für die Anzahl von Fehlern, Übertragungszeiten, Laufzeitschwankungen und ähnlichen Parametern bei der Übertragung von Daten verstanden.

Während es anfänglich bei der Übertragung von Sprache in Telekommunikati-

onsnetzen nicht sonderlich schlimm war, wenn es kleine Störungen, Verzerrungen oder kurze Unterbrechungen in der Leitung gab, mussten Daten „sicher“, d.h. ohne Verluste und ohne Veränderungen übertragen werden.

Daher wurden gleich zu Beginn der Entwicklung Kommunikationsprotokolle wie das Internet Protocol (IP) und später das Transmission Control Protocol (TCP) zur sicheren Übertragung von Daten entworfen und implementiert (die Absicht, mithil-

fe dieser Verfahren einen thermonuklearen Erstschock zu überleben, kam - wenn überhaupt - erst später hinzu, um Geld für die weitere Entwicklung beim amerikanischen Verteidigungsministerium locker zu machen).

weiter auf Seite 8

Top Veranstaltung

**Sommerschule
2006**

auf Seite 4

Zum Geleit

**Vom Einsatz
neuer Medien
bis zum Zwang,
präsent zu sein**

auf Seite 2

Report des Monats

**Planung für
Voice over IP**

auf Seite 19

Zum Geleit

Vom Einsatz neuer Medien bis zum Zwang, präsent zu sein

Als Netzwerker und IT-Personen haben wir uns an die Existenz des Internets gewöhnt. Stories über die hohen Potenziale dieser Infrastruktur belächeln wir souverän, kennen wir ja alles schon, machen wir doch seit Jahren, wir waren schließlich bei der Erfindung dabei.

Dabei stehen wir in dem Risiko, wichtige Änderungen in diesem Markt zu unterschätzen. Es zeigt sich aber, dass eine schnelle und korrekte Einschätzung von Technologie- und Nachfrage-Entwicklung die Wettbewerbsposition von Unternehmen deutlich verschieben kann. Speziell ist die Frage zu beantworten, ob der Umgang mit neuen Medien im Unternehmen einer klaren Regelung bedarf.

Die Kernfragen sind:

- was bieten uns neue Medien-Technologien?
- welche Informationen und Services werden angeboten?
- wie nutzen wir diese individuell und als Unternehmen?
- benötigen Unternehmen einen Rahmenstandard zum Einsatz neuer Medien?

Auf der Unternehmensseite werden seit Monaten im internationalen Markt vor allem vier Themen heiß diskutiert (Hintergrund ist auch der Erfolg mit neuen Medien durch die New York Times, Yahoo, Google und Apple).

Thema 1: Nutzung neuer Medien und Informations-Quellen

Wie verändert sich der Medienmarkt, welche Auswirkungen haben neue Technologien und ihre Nutzung auf die traditionellen Märkte, Zeitschriften, TV und Werbung? In welchem Umfang können Unternehmen diese neuen Ansätze für sich selber sinnvoll einsetzen?

Mittelpunkt der Diskussion ist hier zurzeit Korea. Hier hat Oh Yeon Ho mit der Online-Zeitschrift Ohmy News mit 700.000 Besuchern und 2 Millionen Seitenzugriffen pro Tag eine Revolution angestoßen. Die Grundidee: die Zeitschrift wird von den Lesern geschrieben, Mr. Oh redigiert die Artikel und sorgt für qualitative Kontinuität, aber es gibt keine Journalisten mehr. Die neueste Errungenschaft von Mr. Oh: die Leser geben Bewertungen ab, die Artikel werden dynamisch nach ihrem Ranking



sortiert. Parallel werden Leser aufgefordert, kleine Spenden für gute Artikel abzugeben. Zuletzt brachte es ein guter Artikel auf 30.000 USD in 5 Tagen.

Derartig neue Ansätze, dazu gehört auch MyYahoo mit dem personalisierten Portal, haben das Potenzial, die Medienlandschaft, aber auch die Mediennutzung in den Unternehmen zu ändern. Podcasts, Vodcasts, Blogs, Wikis verändern das Angebot an Information, aber sie verändern auch Märkte.

In welchem Umfang sollen Unternehmen diese neuen externen Informations-Quellen systematisch erschließen? Bleibt dies den Mitarbeitern offen überlassen oder wird es reguliert oder gar verboten? Wer klärt die Sicherheitsfrage, wer beantwortet die Frage nach dem Nutzen für die Unternehmen? Immerhin verbraucht der Umgang mit den Themen ja Zeit? Wer verantwortet die notwendigen Ressourcen in Form von Netzwerk- und Speicherkapazität? Die Reduzierung auf die Sichtweise, dass Unternehmen dies nicht brauchen, kann nur von Leuten kommen, die sich noch nie mit den neuen Diensten befasst haben. Was zum Beispiel im Umfeld einzelner Anwendungen wie Photoshop abläuft, bietet für das Unternehmen und den Endanwender einen so signifikanten Mehrwert, dass jeder Verzicht darauf ein Schaden für das Unternehmen ist.

Direkt damit verbunden ist die Frage, in welchem Umfang neue Arten von Medien für ein Unternehmen Sinn für eine interne Nutzung machen. Können zum Beispiel

Video-Podcasts (Vodcasts) für die interne Weiterbildung eingesetzt werden? Sollten Streaming-Server wichtige Informationen als MP4-Clips anbieten (Schulung, Produkt-Information, ...)? Können Blog-/Weblog-Server eine Whiteboard-Funktion übernehmen und unternehmensinterne oder projektinterne Diskussionsforen realisieren (siehe www.sixapart.com/movabletype für Fallstudien und weitere Informationen)?

Meine persönliche Sicht: Unternehmen brauchen einen Medien-Standard, der als Rahmenstandard die Nutzung dieser neuen Medien festlegt. In diesem Standard sollte auch geklärt werden, in welchem Umfang interne Ressourcen aufgebaut werden (zum Beispiel ein zentraler Streaming-Server, ein Weblog-Server usw.). Auch sollte die Frage nach einem Redaktionsteam für Video-Podcasts geklärt werden, das sinnvolle Vodcasts nach Themengruppen zusammenstellt und zentral bereitstellt.

Thema 2: Software-Markt im Wandel

Wie verändert sich der Software-Markt? Wird das Bereitstellen von Software als Service oder Abo-Dienst im Internet (Software as a Service, kurz SAAS) mit Nutzungsgebühren das Lizenz-Monopol der großen Anbieter Microsoft, Oracle und SAP aufbrechen? Oder bleibt es einem Nischenmarkt für Spezialanbieter wie Salesforce oder generell Spezialthemen wie CRM? Zitate: „Traditional software is dead“ von Jason Maynard Credit Suisse, „It is the end of software as we know it“ von Marc Benioff Salesforce.com. Noch macht Microsoft nur mit Windows und Office mehr als die Hälfte seines 40 Mrd. USD-Umsatzes und einen Großteil seiner Gewinne. Doch die Nutzungsdauer von Betriebssystem und Office-Anwendungen erhöht sich immer weiter. Für Unternehmen ist der Anreiz, in neue Versionen einzusteigen, häufig sehr niedrig, die Kosten für die Umstellung liegen sehr oft über den angestrebten Effizienzgewinnen. Microsoft arbeitet auch mit Macht daran, sein Software-Portfolio auszubauen. Doch die lange so erfolgreiche Bindung an das Betriebssystem, der für Microsoft so ertragreiche Fat-Client-Ansatz, kann sich jetzt in den neuen Anwendungsgebieten bitter rächen. Bei Server-basierten Anwendungen oder weiter gehend bei Anwendungen, die als Internet-Service angeboten werden, ist

Vom Einsatz neuer Medien bis zum Zwang, präsent zu sein

Microsoft noch in der Steinzeit. IBM hat hier deutlich früher die Zeichen der Zeit erkannt. Der Markt wird sich an dieser Frage voraussichtlich spalten. Für Großunternehmen kann der IBM-Ansatz deutlich interessanter sein, während kleinere Unternehmen eigentlich auf den externen Dienstleister zur Umsetzung solcher Leistungen angewiesen sind. Hier wird Microsoft voraussichtlich weiter punkten. Aber wo wird die Grenze verlaufen, wie werden sich Marktanteile verschieben?

Thema 3: Mobile Arbeitsplätze

Wie können wir Arbeitsplätze so gestalten, dass sie im vollen Funktionsumfang mobil genutzt werden können? Wie kann es erreicht werden, dass Mitarbeiter unabhängig vom Ort, der Zeitzone und vom Endgerät in alle wichtigen Unternehmensprozesse eingebunden werden können? Die Frage ist durchaus komplex, sobald sie über Email und Telefonie hinausgeht. Auch müssen Offline-Phasen sinnvoll abgedeckt werden. Das mag in der Dokumenten-Verarbeitung noch handhabbar sein, bei Datenbank-Änderungen ist es ein Problem.

Thema 4: Kollaboration

Wie können wir die neuen Möglichkeiten nutzen, um effizienter und produktiver zu sein? Was wird die Kombination aus neuen Geräten à la Ultra-Kompakt-PC, immer mehr Bandbreite im 3G und neuer Kollaborations-Funktionalität bringen? Auf welcher Basis akzeptiert der Markt diese neuen Möglichkeiten, als traditionelle Fat-Applikation oder als Internet-/Server-basierte Architektur? Wird sich IBM hier mit der besseren Server-zentrierten Software-Architektur Marktanteile von Microsoft zurückholen?

Generationenfrage

Es zeigt sich in der Diskussion, dass der Umgang mit diesen Themen auch eine Generationenfrage ist. Ein schönes Zitat dazu aus dem Economist von Terry Semel, Chef von Yahoo, über seine Töchter 24, 19 und 13 Jahre alt: "The first does a lot in the internet, the second does everything in the internet, and the third lives online". Ich kann diese Sichtweise bestätigen. Ich gebe als „Hobby“ IT-Kurse in der Schule meiner Kinder. Die Kenntnisse, die heute bereits 9 bis 14 jährige Kinder haben, sind erstaunlich. Aber wirklich schockierend ist ihre Lerngeschwindigkeit, man kann von PowerPoint und Excel-Lektionen im Minutentakt sprechen. Dies zeigt auch die aktuelle Generation, die aus den Schu-

len und Hochschulen in die Arbeit drängt. Fragt man junge Mitarbeiter, welche Ideen und Denkweisen sie zu Technologien haben, kommen völlig andere Antworten als man sie von älteren Mitarbeitern erhalten würde (wie schaffe ich es nur, ohne mein persönliches Grid zu leben?).

Mit diesen Trends wird auch die Welt kleiner und dynamischer. Dies betrifft nicht nur die Reisemöglichkeiten und den heiß ersehnten Airbus 380. Mit Podcasts/Vodcasts und vor allem Blogs entstehen Länder- und Kontinente-übergreifende Informationsnetzwerke. Man hat heute mobil oder stationär Zugriff auf eine solche Fülle von Informationen und Funktionen, dass der eigene Standort keine Rolle spielt. Der Stellenwert und Nutzen des mobilen Mitarbeiters muss dementsprechend neu definiert werden.

Kritik

Was ohne Zweifel in der Markteuphorie über diese Entwicklungen fehlt, ist eine kritische Sichtweise. Man kann schon von einem Zwang, einer Sucht, Online zu sein, sprechen. Wer nicht Online ist, ist out. Auch dies ist die Botschaft der modernen IP-Telefonie-Clients: ich zeige meine Präsenz, ich bin online, ich gehöre dazu. Das menschliche Streben „dazu-zu-gehören“ oder „ein Teil von etwas Wichtigem zu sein“ nimmt in der modernen Online-Manie schon fast perverse Züge an. Die Idee, dass ein Mensch auch Zeit für sich braucht, dass gute und effiziente Arbeit

auch Ruhe erfordert, scheint völlig abhandeln gekommen zu sein.

Ich würde deshalb gerne die Verheißungen der neuen Technologie anders definieren: die neuen Technologien und Möglichkeiten sind gut, solange sie es mir gestatten, effizienter an Information zu kommen und diese kreativer zu verarbeiten. Ziel dieser Effizienz kann aber nicht die permanente Erreichbarkeit und Verbrauchbarkeit sein. Informationen müssen auch verarbeitet und hinterfragt werden können. Dies erfordert Zeit und Ruhe, die wir uns ja auch gerade mit der gesteigerten Effizienz verschaffen. Wenn wir unsere Effizienz steigern und besser werden, dann sollten wir die daraus entstehenden Freiräume auch konsequent nutzen, um nicht immer online zu sein.

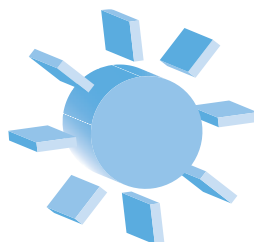
Ausblick Sommerschule

Für die Sommerschule haben wir uns aus diesem breiten Spektrum als einen der Schwerpunkte das Thema Mobilität ausgewählt. Parallel werden wir sicher auch in anderen Vorträgen auf Teilaspekte dieser Entwicklung eingehen. Immerhin stellt diese Entwicklung ja auch Anforderung an Infrastrukturen und Sicherheits-Systeme. Die Sommerschule bietet sicher den aktuellen Rahmen, um die modernsten Trends dieser Art zu diskutieren.

Ihr äußerst mobiler
aber nicht permanent online
Dr. Jürgen Suppan

Sommerschule 2006

**19.06. - 23.06.06
in Aachen**



Die Sommerschule 2006 greift die aktuellsten Entwicklungen der Netzwerk-Technologien auf, stellt die wichtigsten Trends zur Diskussion und gibt Empfehlungen zur Weiterentwicklung und Verbesserung bestehender Netzwerke. Mit diesem 5-Tages-Intensiv-Update auf den letzten Stand der Netzwerk-Technik haben wir für Sie die aktuellen Entwicklungen analysiert, Erfahrungen aus Labor und gerade abgeschlossenen Projekten eingearbeitet und daraus eine Auswahl aus den zur Zeit anliegenden Top-Themen getroffen.

Moderation: Markus Schaub
Preis: € 2.290,- zzgl. MwSt.



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

Top-Veranstaltung

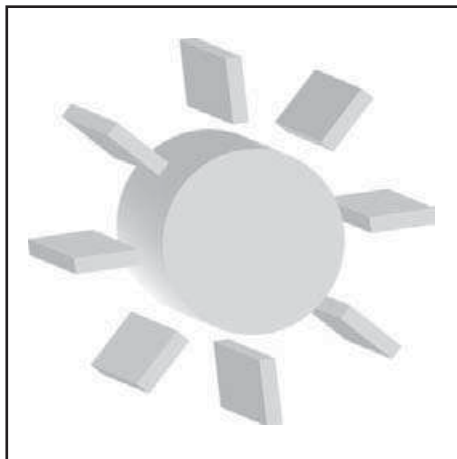
Sommerschule 2006

Die Comconsult Akademie veranstaltet vom 19. - 23. Juni die „Sommerschule 2006“ in Aachen.

Auch in diesem Jahr bietet die Sommerschule wieder den Intensiv-Update auf den neuesten Stand der Netzwerk-Technik, zeigt neue Nutzungs-Potenziale, diskutiert Änderungen im Design, analysiert aktuelle Produktrends. Damit wendet sich die Sommerschule speziell an erfahrene Teilnehmer/Innen, die den Betrieb ihrer bestehenden Netzwerke weiter optimieren und neue Entwicklungen und Technologien kennen lernen wollen.

Die Sommerschule 2006 bietet folgende Schwerpunkte:

- Der Cisco-Design-Guide in der Analyse
- Mobile Kommunikation
- Privacy und Sicherheit bei der mobilen Kommunikation
- Bluetooth-Sicherheit in der Praxis
- Netzwerk-Design 2006
- Das Session-Initiation Protokoll SIP in der Analyse
- Auswahl neuer Switch-Systeme für den Workgroup-Bereich
- Videoüberwachung über IP
- Einsatz von Netzwerk-basierten IPS
- Wireless-Networks



- Sicherheit in der IP-Telefonie
- Identity und Access-Management an einem Projektbeispiel
- Von 802.1X zur Anmeldung von Benutzern und Trennung von Benutzergruppen
- Quality of Service in Netzwerken professionell nutzen

Zur Sicherstellung der Diskussionsfähigkeit und einer interaktiven Kommunikation haben wir die Teilnehmerzahl begrenzt. Zögern Sie deshalb nicht, sich schnell ei-

nen Platz in dieser herausragenden Veranstaltung zu sichern.

Ab sofort bieten wir Ihnen die neuen Reports „Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X“ (März 2006) und „Quality of Service in modernen Infrastrukturen Standards und Architekturen“ (April 2006) bei der Buchung dieses Kongresses zu einem Sonderpreis an. Statt regulär € 398,- zahlen Sie je Exemplar nur € 338,-. Sie können auch beide Reports erwerben und sparen 20%. Statt regulär € 796,- zahlen Sie im Paket nur € 636,-. (alle Preise zzgl. MwSt.)

Moderieren wird diese Veranstaltung Markus Schaub. Er ist seit vielen Jahren für die ComConsult Technologie Information GmbH tätig. Seine Aufgabenbereiche umfassen die Evaluierung, Konfiguration und Inbetriebnahme neuester Hard- und Software aus dem Netzwerkumfeld. Insbesondere verfügt er über langjährige Betriebs- und Praxiserfahrung mit CISCO-Routern und CISCO-Switch-Systemen. Er ist ComConsult Certified Network Engineer und von Cisco CCNP™ zertifiziert. Darüber hinaus ist er für den Betrieb des CISCO-Router-Netzes der ComConsult Akademie verantwortlich.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Sommerschule 2006

Ich buche das Seminar **Sommerschule 2006** vom 19.06. - 23.06.06 in Aachen **zum Preis von nur € 2.290,- zzgl. MwSt.**

mit Report „Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X“ **zum Preis von € 338,- zzgl. MwSt.**

mit Report „Quality of Service in modernen Infrastrukturen Standards und Architekturen“ **zum Preis von € 338,- zzgl. MwSt.**

Bitte reservieren Sie für mich ein Hotelzimmer vom _____ bis _____ 06

Vorname _____ Nachname _____

Firma _____ Abteilung _____

Telefon _____ Fax _____

Straße _____ PLZ, Ort _____

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

eMail _____ Unterschrift _____

Programmübersicht Sommerschule 2006

Montag, der 19.06. 2006

09:30 - 12:30 Uhr

Der Cisco-Design-Guide in der Analyse

- Hierarchisches Netzdesign
- Komponenten-Redundanz
- Basis-Dienste:
 - Layer-3-Protokolle
 - Router-Redundanz
 - Layer-2-Redundanz
 - Layer-2-EtherChannel / Link Aggregation
 - Layer-2-VLAN Trunking / Tagging
- QoS und Überbuchung
- Best Practices
- Alternativen
- Kosten und Funktionalität in der Abwägung
- Bewertung: Vor- und Nachteile
- Empfehlungen zum optimalem Design

Dipl.-Inform. Petra Borowka,
UBN

13:45 - 14:45 Uhr

Mobile Kommunikation

- Einsatz von Konfigurations-Datenbanken zur zentralen Steuerung
 - Testverfahren für bestehende Netzwerke und Produkte
- Dr. Frank Imhoff,
ComConsult Beratung und Planung GmbH

14:45 - 15:45 Uhr

Privacy und Sicherheit bei der mobilen Kommunikation

- Bekannte und weniger bekannte Schwachstellen mobiler Geräte
- Strategien für mehr Privacy und mehr Sicherheit
- Herausforderung zentrales Management
- Aktuelle Trends und Empfehlungen

Dr. Frank Imhoff,
ComConsult Beratung und Planung GmbH

16:15 - 17:15 Uhr

Bluetooth-Sicherheit in der Praxis

- Wie abhörsicher ist „Frequency Hopping“?
- Verbindungsaufbau, Authentisierung und Verschlüsselung bei Bluetooth
- Bietet die neue Bluetooth-Variante 2.0 mehr Sicherheit?
- Bloover, Carwhisperer und Co., Angriffe auf Bluetooth und die Konsequenzen
- Empfehlungen zur Absicherung von Bluetooth-Devices

Dr.-Ing. Joachim Wetzlar,
ComConsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause
12:30 - 13:45 Uhr Mittagspause
15:45 - 16:15 Uhr Kaffeepause
ab 18:30 Uhr Happy Hour

Dienstag, der 20.06. 2006

09:00 - 12:30 Uhr

Netzwerk-Design 2006

- Zentrale Trends und Technologieentwicklungen
- LAN-Redesign: Alternativen und Bewertung
- Neue Funktionen bei Backbone-Switches
- 10 Gigabit-Ethernet, preiswerte Varianten, Nutzung und Trends
- Voice-Integration
- LLDP/LLDP-MED: Multivendor-Management und Management von Voice-Endgeräten auf Layer 2
- WLAN-Integration: Integrationsalternativen von Fat-Access-Points und Wireless-Controller-Architekturen
- Meshed WLANs: Einsatzszenarien, Auswirkungen von Meshed LANs als Sekundär-Technologie auf das zukünftige Netzwerk-Design
- Empfehlungen

Dipl.-Inform. Petra Borowka,
UBN

14:00 - 17:00 Uhr

Das Session-Initiation Protokoll SIP in der Analyse

- Motivation
- VoIP-notwendige Standards
 - RTP, Basisprotokoll für die Echtzeitübertragung
 - SIP, Signalisierung, was ist das überhaupt?
 - SDP, Aushandeln von Sitzungsparametern
 - Weitere Protokolle
- Welche Bedeutung hat SIP - Stand heute?
 - SIP nur für die Telefonie?
 - Existente Anwendungen im Multimedia-Bereich auf SIP-Basis
 - Welche Leistungsmerkmale sind in SIP integrierte? Welche können auf Basis des bestehenden Standards entwickelt werden?
 - Welche Leistungsmerkmale werden heute typischer Weise unterstützt?
- Welche Bedeutung wird SIP in Zukunft haben?

- Was ist mit „reiner“ Standardtechnik möglich?
- Welche Stärken und Schwächen besitzt SIP?
- An welchen Erweiterungen und Leistungsmerkmalen wird gearbeitet?
- Wird SIP proprietäre Protokolle verdrängen wie einst TCP/IP?
- Wie kann ein SIP basiertes Netz heute bereits aussehen?
 - Was ist mit reinen SIP Anlagen und Proxys heute bereits möglich?

Dipl.-Inform. Petra Borowka,
UBN
Markus Schaub,
ComConsult Research

10:30 - 11:00 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 - 16:00 Uhr Kaffeepause

Mittwoch, der 21.06. 2006

09:00 - 10:00 Uhr

Auswahl neuer Switch-Systeme für den Workgroup-Bereich

- 1000 oder 100? • Stacking
 - Power over Ethernet
 - Routing • Anbindung an den Core
- Dipl.-Ing. Hartmut Kell,
ComConsult Beratung und Planung GmbH

10:00 - 11:00 Uhr

Videoüberwachung über IP

- Bildkompression, Übertragungsraten, Varianten
 - Justage der ausreichenden Bildqualität
 - Analoge und digitale Architekturen im Vergleich
 - Typische Produkte
 - Netzwerk-Parametrierung
 - Empfehlungen
- Dipl.-Ing. Hartmut Kell,
ComConsult Beratung und Planung GmbH

11:30 - 12:30 Uhr

Einsatz von Netzwerk-basierten IPS

- IPS versus IDS und Abgrenzung von Firewalls
 - Zu beachtende Aspekte bei der Auswahl von IPS
 - Produktbeispiele
 - Praktische Erfahrungen und daraus abzuleitende Empfehlungen
- Dr. Simon Hoff,
ComConsult Beratung und Planung GmbH

- keit und Anwendungsbereiche
- ETSI und die 5 GHz Gedenkminute, was steckt dahinter, welche Konsequenzen hat es? (oder: Bürokraten und der Bezug zur Praxis)
- WiMAX: professionelle Wireless-Technologie, Nutzung und Trends
- IEEE 802.11n und die Auswirkung auf den Enterprise-Markt
- Projekterfahrungen und daraus abzuleitende Empfehlungen

Dr. Simon Hoff,
ComConsult Beratung und Planung GmbH

14:00 - 17:00 Uhr

Wireless-Networks

- Fat-AP mit zentralem Management kontra Controller-basierte Lösungen: funktions-technische Vorteile und Visionen
- Wireless-LANs in Fabrik und Logistik
- Meshed WLANs: Funktechnische Nutzbarkeit?
- 5GHz und Dual-Radio: Produkt-Verfügbarkeit

11:00 - 11:30 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 - 16:00 Uhr Kaffeepause

Programmübersicht Sommerschule 2006

Donnerstag, der 22.06. 2006

09:00 - 11:00 Uhr

Sicherheit in der IP-Telefonie

- Unterschiede zwischen konventioneller Telekommunikation und VoIP hinsichtlich Sicherheit
 - Unterschiede in der Signalisierung
 - Unterschiede beim Transport
 - Unterschiede in der Architektur
 - Folgen für die Informationssicherheit
- Standards für VoIP-Sicherheit
 - Secure Real-time Transport Protocol (SRTP)
 - Sicherheit beim Session Initiation Protocol (SIP)
 - Sicherheit bei H.323
 - Sicherheit bei anderen Signalisierungsprotokollen
 - Weitere relevante Standards
- VoIP über Vertrauensgrenzen hinweg
 - Probleme bei Firewalling
 - Proxy-Architekturen
 - Session Border Controller als Schlüsseltechnologie für VoIP-Sicherheit
- Projekterfahrungen und Empfehlungen

*Dr.-Ing. Behrooz Moayeri,
ComConsult Beratung und Planung GmbH*

11:30 - 12:30 Uhr

Identity und Access-Management an einem Projektbeispiel

- Ausgangslage: Netzwerk mit vielfältiger Nutzung
- Typische Sicherheitsrisiken bei unzureichendem

Identity und Access-Management

- Technische Herausforderung
- Organisatorische Dimension
- Lösungsansatz

*Dipl.-Ing. Harald Krause,
ComConsult Beratung und Planung GmbH*

14:00 - 17:00 Uhr

Von 802.1X zur Anmeldung von Benutzern und Trennung von Benutzergruppen

- Bedrohungsanalyse
- Bestehende Standards
 - RADIUS: die Basis einer zentralen Authentifizierungsinfrastruktur
 - IEEE 802.1X: Fortschritt oder Luftschloss?
 - EAP: Wie arbeitet das Verfahren und welche Versionen sind sinnvoll?
- Authentifizierung - Aber wie?
 - Sind Passwort Abfragen heute noch zeitgemäß, welche Varianten gibt es?
 - Token und Smart Cards: Analyse
 - Zertifikate:
 - Client oder User-Überprüfung?
 - Wie aufwendig ist der Betrieb?
 - Biometrie und seine aktuelle Nutzbarkeit
 - Welches Verfahren ist für welchen Anwendungsbereich geeignet?
- Trennung auf Benutzerebene
 - Vergabe von Zugriffsrechten auf Basis des Users/Clients
 - Zuweisung von Netzwerkparametern (QoS)
 - Eine Lösung für das IP-Phone-PC Problem?

- Lösungen der Hersteller: Cisco kontra Enterasys
- Ist das Ganze zu beherrschen oder eine Administrationsfalle?
- Prüfung der Endsysteme vor dem Netzwerkzugriff
 - Überprüfung des Patchlevels systemkritischer Software
 - Aktives Scannen des Systems auf Sicherheitslücken
 - Update eines Systems vor dem Netzwerkzugang
 - Wie sehen die aktuellen Herstellerlösungen aus?
- Problematische Bereiche und Einsatzszenarien beim Einsatz von 802.1X
 - VoIP:
 - Wie geht man mit Softclients um?
 - Welche Möglichkeiten gibt es für die Kaskardierung von Telefon und PC bei gleichzeitigem Einsatz von 802.1X?
 - WLAN: shared medium und trotzdem User-Authentifizierung?
 - Wie bringt man „alte“ Geräte ans Netz?
 - Wie lässt sich ein Gastanschluss/Hot-Spot realisieren?

*Markus Schaub,
ComConsult Research*

11:00 - 11:30 Uhr Kaffeepause

12:30 - 14:00 Uhr Mittagspause

15:30 - 16:00 Uhr Kaffeepause

Freitag, der 23.06. 2006

09:00 - 15:00 Uhr

Quality of Service in Netzwerken professionell nutzen

- QoS-Grundlagen
 - QoS-Ziele
 - QoS-Parameter
 - QoS-Mechanismen
- Bearbeitungsstrategie für Warteschlangen
 - Policing
 - Shaping

- Quality of Service im LAN
 - QoS in IEEE 802.1D
 - QoS in IEEE 802.1Q
 - Empfehlungen von IEEE
- Der Standard Differentiated Service (Diff-Serv) und sein Stellenwert
 - DiffServ-Architektur
 - DiffServ-Implementierungen in Produkten
- Quality of Service in WAN
 - QoS-Funktionen von Routern

- Strategien bei der Behandlung von Warteschlangen in Routern

*Dr.-Ing. Behrooz Moayeri,
ComConsult Beratung und Planung GmbH*

10:30 - 11:00 Uhr Kaffeepause

12:30 - 14:00 Uhr Mittagspause

15:00 Uhr Ende der Veranstaltung

Neuer Kongress

Trouble-Shooting Forum 2006

Die ComConsult Akademie veranstaltet vom 23. - 24. Oktober erstmalig ihren neuen Kongress „Trouble-Shooting Forum 2006“ in Neuss.

Leider laufen Netzwerke, Applikationen und Sicherheits-Infrastrukturen nicht immer so wie sie es im Idealfall sollen. Dabei gehören Totalausfälle noch zu den „angenehmen“ Störungen. Schlimmer sind Performance-Probleme und generell sporadisch auftretende und nur schwer reproduzierbare Störungen. Mit der immer weiter zunehmenden Abhängigkeit der Unternehmen von IT und Netzwerken ist deshalb das Thema Trouble-Shooting zu einem Top-Thema geworden.

Das ComConsult Trouble-Shooting-Forum 2006 ist unsere Top-Veranstaltung des Jahres zu diesem Thema. Seine Top-Themenbereiche sind:

Applikationen

- Bandbreite ist nur die halbe Miete: Die Laufzeit als begrenzender Faktor
- Neue Probleme im Umfeld von VPNs, Mobile und Co. (z.B. verringerte MTU, unkorrelierte Störungen von TCP bei Funk)
- Messung und Bewertung von Voice
- Wie wird man der großen Datenmengen Herr? Braucht man Spezial-Messtechnik im Anblick von Gigabit und 10 Gigabit?



Sicherheitsinfrastrukturen

- Problembereich Tunneling und Verschlüsselung: Messungen, Analyse, Überwachung und Fehlersuche
- Beispiel: Trouble Shooting von IPSec
- Beispiel: IEEE 802.1X
- Wenn Firewalls, Application Layer Gateways, Proxies und Intrusion Prevention Systeme nicht das filtern, was sie eigentlich sollten

„Management“ von Fehlern

- ITIL
- Prozesse zu Verhinderung von Fehlern (Configuration Management, Change Management), auch ein Fehler ist ein „Configuration Item“

- Wie kann schnell auf Fehler reagiert werden (Incident Management); effektive und effiziente Meldewege
- Sinnvoller Umfang externer Unterstützung beim Incident Management und beim (Business) Continuity Management.
- Dokumentation und Post Mortem Analyse

Last- und Stresstests

- Präventive Prüfung von Anwendungen und Netzelementen
- Vorgehensweise bei Last- und Stresstests
- Werkzeugüberblick

Funk

- Koexistenz verschiedener Funktechniken als Problem
- Aktuelle Messtechnik: Protokollanalyse, Spektrumanalyse, Überwachungstools
- Was leisten aktuelle Access Points für die Überwachung, was ist der Mehrwert spezieller Sensoren à la Airmagnet Sensor?
- Standortbestimmung mit WLAN? Wie arbeiten aktuelle Lösungen? Neue Ansätze.

Die Moderation der Veranstaltung erfolgt durch Dr.-Ing. Joachim Wetzlar, der seit über 10 Jahren zu den Top-Trouble-Shooting-Experten der Branche zählt.

Fax-Antwort an ComConsult 02408/955-399

Frühbucherphase
bis 30.07.06

Anmeldung Trouble-Shooting Forum 2006

Frühbucherphase
bis 30.07.06

- Ich buche den Kongress **Trouble-Shooting Forum 2006** vom 23. - 24.10.06 in Neuss zum Preis von € 1.390,-* zzgl. MwSt. *gültig bis 30.07.06 (dann regulär € 1.590,- zzgl. MwSt.)
- mit Report „Fehlersuche in konvergenten Netzen“ zum Preis von 338,- zzgl. MwSt.
- Bitte reservieren Sie für mich ein Hotelzimmer vom _____ bis _____ 06

Vorname

Nachname

Firma

Telefon/Fax

Straße

PLZ, Ort

eMail

Unterschrift



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

Zweitthema

Quality of Service

Fortsetzung von Seite 1



Dr. Frank Imhoff ist technischer Direktor und Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Erfahrung in Forschung, Entwicklung und Betrieb von lokalen Netzen, Voice-over-IP, Wireless Local Area Networks sowie anderen Mobilfunk- und Telekommunikationssystemen zurück. Zu diesen Themenbereichen sind von ihm bereits zahlreiche Veröffentlichungen erschienen und Seminare betreut worden.

Viele Jahre später bemühte sich dann die Welt der Telekommunikation, vorwiegend von staatlichen Postverwaltungen geprägt, ihre Netze auch für die Übertragung von Daten attraktiv zu machen. Der erste, halbwegs erfolgreiche Ansatz war die Einführung des Integrated Services Digital Network (ISDN) und die Entwicklung des Asynchronous Transfer Mode (ATM).

In den letzten Jahren zeichnet sich jedoch ab, dass die Telekommunikation den Kampf um die Vorherrschaft verloren hat, denn immer mehr werden bisherige Datenkommunikationsnetze auch für die Übertragung von zeitkritischen Daten wie Sprache oder Videokonferenzen genutzt. Gleichzeitig setzt sich damit IP als Kommunikationsprotokoll auch für solche Daten durch, obwohl es aufgrund seiner Paket orientierten Übertragungseigenschaften dafür eigentlich ungeeignet ist. Um diesen Nachteil im Hinblick auf zeitkritische Übertragungen zu kompensieren, ist bereits eine Reihe von Maßnahmen entwickelt worden. Gleichzeitig ist jedoch die Qualität der Netze und die damit verbundene Übertragungsqualität aufgrund der technologischen Entwicklungen und des rasanten Preisverfalls im Vergleich zu früheren Datenkommunikationsnetzen immens gestiegen. Beispiele dafür sind nahezu fehlerfrei übertragende Glasfasern oder vor Überlastungen weitgehend geschützte Netzkomponenten.

Nachdem nun der Konvergenz-Wettstreit zwischen Telekommunikation versus Datenkommunikation zugunsten der Datenkommunikation entschieden ist, hat sich der Expertenstreit zu der Frage verlagert, welche Maßnahmen in Kommunikationsnetzen zu ergreifen sind, um den hohen Qualitätsansprüchen bei der Übertragung von zeitkritischen Daten gerecht zu werden. Dieser Artikel befasst sich daher mit

der Dienstgüte heutiger Kommunikationsnetze.

Maßnahmen und Verfahren

Unter QoS versteht man in der Regel zweierlei: Zum einen alle Maßnahmen und Verfahren, die den Datenfluss in Kommunikationsnetzen so beeinflussen, dass eine Übertragung von beliebigen Daten mit einer festgelegten Qualität erfolgt. Zum anderen versteht man darunter die Qualität einer Übertragung selbst, also das Ergebnis aller eingesetzten Verfahren zur Herstellung oder Sicherung einer bestimmten Übertragungsqualität. Es handelt sich also letztendlich um die Charakterisierung eines Übertragungsdienstes, dessen Qualität der Nutzer messen kann. Technisch handelt es sich um eine Parametrisierung von Protokollen zur Bestimmung des Übertragungsverhaltens für bestimmte Dienste.

In den letzten Jahren haben sich aber dank immer größerer Übertragungskapazitäten und preiswerterer Hardware neue zeitkritische Übertragungsdienste in den Datenkommunikationsnetzen verbreitet. Neben Sprachübertragungen werden immer häufiger Videokonferenzen sowie Übertragungen von Filmen und Musik in Echtzeit (neben weniger zeitkritischen Downloads) über Datenkommunikationsnetze abgewickelt. Bei diesen Beispielen wird klar, dass schon Verzögerungen von weniger als einer Sekunde unangenehm sind. Kritisch wird es dann, wenn gleich mehrere der zu übertragenden Datenpakete hintereinander verloren gehen. In diesem Fall würde ein Stück des Films einfach fehlen oder bei der Videokonferenz der Beitrag eines Teilnehmers unter den Tisch fallen. Solche Paketverluste waren aber vor allem in den Anfängen der paketorientierten Übertragung sehr häufig, da

die verwendeten Kupferkabel nur unzureichend gegen induktive Störungen abgeschirmt waren oder sehr häufig Überlastungen einzelner Übertragungswege auftraten. Um den Anforderungen dieser zeitkritischen Daten gerecht zu werden, mussten Maßnahmen ergriffen werden, um die beeinflussenden Faktoren in definierten Grenzen zu halten.

Eine Liste der Ziele von QoS in Netzen kann jedoch nicht abschließend und vollständig sein, da es aufgrund neuer Anwendungen, neuer Hardware oder sich änderndem Nutzerverhalten ständig neue Anforderungen geben wird. Zunächst sind aus heutiger Sicht aber zwei Bereiche von Zielen zu unterscheiden, globale und spezielle Ziele.

Die eher globalen Ziele wie Sicherheit (Safety und Security), Verfügbarkeit (Redundanz, Fehlertoleranz), Ausbaubarkeit (Reserven, Skalierbarkeit) etc. beziehen sich zumeist auf die gesamte Infrastruktur oder die gesamten IT-Ressourcen eines Unternehmens. Hierzu bedarf es sehr weitgehender und individueller Betrachtungen. Z.B. werden Banken und Versicherungen andere Sicherheitsansprüche an ihre Netze stellen als z.B. ein Autohändler - schon allein aufgrund der Vorschriften von Gesetzgeber und Aufsichtsbehörden, aber auch, weil hier höchst sensible Daten transportiert und gespeichert werden. Umfangreiches Abhören oder ein weitreichender Verlust von Daten kommt einer Existenz bedrohenden Katastrophe sehr nah.

Die speziellen Ziele von QoS betrachten hingegen einzelne Abschnitte oder einzelne Betriebsmittel eines Netzes und beziehen sich auf Parameter, die für den Benutzer spürbar oder verständlich werden. Zu den wichtigsten dieser Parameter ge-

Quality of Service

hört die Mindestbitrate, die Fehlerfreiheit, die Verlustfreiheit, die maximale Paketlaufzeit, die maximale Varianz der Paketlaufzeit und die korrekte Reihenfolge der Pakete beim Empfänger.

Um die oben genannten QoS-Parameter erfüllen zu können, ist eine Reihe von QoS-Mechanismen erforderlich. Hier hat es in den letzten Jahren sehr viele, vor allem proprietäre Ansätze verschiedener Hersteller gegeben. Wichtigste Voraussetzung für die Anwendung komplexerer QoS-Mechanismen ist jedoch die Klassifizierung von Paketen, da ansonsten den Komponenten des Netzes die Bedeutung eines Pakets verborgen bleibt. Diese Klassifizierung wird üblicherweise mithilfe einer Markierung gemacht. Anhand dieser Markierung kann ein beliebiger Mechanismus zur Sicherstellung der QoS die Behandlung differenzieren, weshalb eine Übertragung unmarkierter Pakete dann beispielsweise nur noch nach dem Best-Effort-Prinzip erfolgt, also ohne Beachtung von QoS-Mechanismen.

Einer der einfachsten und gleichzeitig auch wirkungsvollsten QoS-Mechanismen ist die Priorisierung von Paketen. Die Übertragung von Paketen erfolgt bei diesem Verfahren in einem Router z. B. nicht nach dem Prinzip First-In-First-Out (FIFO) durch Abarbeiten einer einzigen Warteschlange, sondern durch die Bildung mehrerer Warteschlangen und die Zuordnung unterschiedlich markierter Pakete zu unterschiedlichen Warteschlangen. Zu bevorzugende Pakete werden von den Netzkomponenten priorisierten Warteschlangen zugeordnet.

In Fachkreisen besteht Einigkeit darüber, dass die Priorisierung von Paketen die Methode der Wahl für die Sicherstellung von QoS ist. Jedoch führt sie unter Umständen zu einer Reihe von Nachteilen. Beispielsweise können einige priorisierte Anwendungen zu einer monopolartigen Nutzung einzelner Komponenten des Netzes führen. Auch können mit relativ einfachen Mitteln manipulierte Pakete in den Genuss der Prioritäten kommen, obwohl es sich nur um unwichtige Daten handelt. Zudem müssen die Netzkomponenten entsprechend konfiguriert und gepflegt werden. Um diese Probleme zu vermeiden, ist eine Reihe von unterschiedlichen Verfahren entwickelt und z.T. implementiert worden. Unter diesen Verfahren leidet zum Teil aber wieder die Gesamt-Performance, da für die beteiligten Komponenten noch mehr Aufwand entsteht.

Um die monopolisierte Nutzung zu verhindern, sind diverse Queuing- und Schedu-

ling-Verfahren denkbar, z. B. Fair Queuing, womit jeder Warteschlange ein bestimmter Anteil der Ressourcen zur Verfügung gestellt wird. Solche Mechanismen müssen vor allem dann eingesetzt werden, wenn die maximal mögliche aggregierte Bitrate des zu priorisierenden Verkehrs (z.B. Voice over IP) einen signifikanten Anteil der verfügbaren Netzressourcen ausmacht, so dass eine statische Priorisierung negative Auswirkungen auf andere Anwendungen haben könnte. In Bereichen, in denen beispielsweise die maximal denkbare Voice-over-IP-Bitrate einen signifikanten Anteil der verfügbaren Netzressourcen ausmacht, muss in der Regel eine Begrenzung der für VoIP zur Verfügung stehenden Netzkapazität vorgenommen werden. Erfahrungsgemäß ist dies in Weitverkehrsnetzen (WAN) der Fall, jedoch nicht in lokalen Netzen (LAN), da hier in der Regel deutlich mehr Bandbreite zur Verfügung steht als erforderlich ist.

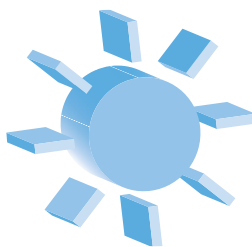
Netzlastverläufe weisen in der Regel Schwankungen auf. Um die Effizienz eines Netzes zu erhöhen, kann durch Traffic Shaping die Übertragung von Paketen bis zur Verfügbarkeit von mehr Ressourcen verzögert oder abgewiesen werden (Dropping). Solche Maßnahmen sind in LANs nicht sinnvoll. Im WAN können solche Maßnahmen jedoch erforderlich sein, z. B. um das Verkehrsaufkommen einer von einem Carrier unterstützten Committed In-

formation Rate (CIR) anzupassen. Solche Maßnahmen sollten in direktem Zusammenhang mit Queuing und Scheduling vorgenommen werden, damit zeitkritische Anwendungen nicht darunter leiden.

Die Reservierung von Ressourcen besteht darin, dass vor dem Aufbau einer verbindungsorientierten Anwendung (Session) das Netz entweder automatisch oder von den Anwendungen selbst erfährt, dass bestimmte Ressourcen für die entsprechende Anwendung zu reservieren sind. Diese Reservierung wird entlang des Übertragungspfades vom Netz vorgenommen. Im Zusammenhang mit VoIP sind solche Maßnahmen in LANs nicht sinnvoll. Generell wird davon ausgegangen, dass der verbindungsorientierte Reservierungsansatz sehr komplex sei und nur dann durchzuführen wäre, wenn andere QoS-Mechanismen nicht möglich sind. Ohne Admission Control ist der Reservierungsansatz jedoch undenkbar. Das Netz muss über die reservierten Ressourcen Buch führen und neue Reservierungen nur dann durchführen, wenn entsprechende Ressourcen verfügbar sind. Andernfalls müssen Reservierungswünsche abgewiesen werden (Admission Control). Im Zusammenhang mit VoIP ist Admission Control zum Beispiel ein Bestandteil der Aufgabe eines Gatekeepers und nur beim Übergang zu WANs sinnvoll.

Sommerschule 2006

19.06. - 23.06.06
in Aachen



Auch in diesem Jahr bietet die Sommerschule wieder den Intensiv-Update auf den neuesten Stand der Netzwerk-Technik, zeigt neue Nutzungs-Potenziale, diskutiert Änderungen im Design, analysiert aktuelle Produkttrends. Damit wendet sich die Sommerschule speziell an erfahrene Teilnehmer/Innen, die den Betrieb ihrer bestehenden Netzwerke weiter optimieren und neue Entwicklungen und Technologien kennenlernen wollen.

Die Sommerschule 2006 bietet folgende Schwerpunkte:

Der Cisco-Design-Guide in der Analyse; Mobile Kommunikation; Privacy und Sicherheit bei der mobilen Kommunikation; Bluetooth-Sicherheit in der Praxis; Netzwerk-Design 2006; Das Session-Initiation Protokoll SIP in der Analyse; Auswahl neuer Switch-Systeme für den Workgroup-Bereich; Videoüberwachung über IP; Einsatz von Netzwerk-basierten IPS; Wireless-Networks; Sicherheit in der IP-Telefonie; Identity und Access-Management an einem Projektbeispiel; Von 802.1X zur Anmeldung von Benutzern und Trennung von Benutzergruppen; Quality of Service in Netzwerken professionell nutzen

Moderation: Markus Schaub

Preis: € 2.290,- zzgl. MwSt.



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

Quality of Service

Oberhalb der IP-Ebene stehen als Schicht-4-Protokolle im Grunde nur die beiden Transportprotokolle User Datagram Protocol (UDP) und Transmission Control Protocol (TCP) zur Verfügung. Für die Übertragung von zeitkritischen Daten wird in der Regel auf UDP zurückgegriffen, da TCP aufgrund vielfältiger Mechanismen zu große Verzögerungen mit sich bringen würde. UDP verzichtet gänzlich auf QoS-Mechanismen, weswegen höhere Protokolle diese Aufgaben übernehmen müssen. Die beiden wichtigsten Vertreter dieser Protokolle sind das Real-Time Protocol (RTP) und das Real-Time Control Protocol (RTCP).

Quality of Service in Local Area Networks

Lokal Area Networks (LAN) haben bis heute eine weltweite Verbreitung gefunden, die im Bereich der Kommunikationsnetze sicherlich nur noch von Telefonnetzen übertroffen wird. Aus Bürogebäuden, Verwaltungen und Produktionsstätten sind derartige Netze nicht mehr wegzudenken. Selbst in Hotels, Wohnungen und privaten Häusern trifft man häufig auf LANs oder Komponenten davon. Die inzwischen mit großem Abstand erfolgreichste Technologie für lokale Netze ist Ethernet nach IEEE 802.3.

Die für Ethernet relevanten Standards von IEEE 802.3 sehen selbst keine QoS-Mechanismen vor. Daher muss ein Layer-2-Frame (Rahmen) um einen zusätzlichen „Tag“ führen (IEEE 802.1Q). Dabei kann es sich um einen VLAN-tagged Frame handeln, aus dem sowohl die VLAN-Zuordnung als auch die Priorität hervorgeht, oder um einen Priority-tagged Frame, der nur die Priorität enthält. Ein solcher Tag ist immer vier Bytes lang. Die ersten beiden Bytes sind bei allen bisherigen Implementierungen identisch (8100) und kennzeichnen das verwendete Tag-Protokoll. Die beiden letzten Bytes im Tag umfassen die User Priority (UP), den Canonical Frame Indicator und die Virtual LAN ID.

Ein Layer-2-Switch kann aufgrund der über das Netz signalisierten Informationen oder der eigenen Konfigurationsvorgaben UP-Werte neu vergeben. Dabei ist ein UP-Wert von 0 der Standardwert und ein UP-Wert von 7 gleichbedeutend mit der höchsten Priorität. Auf dem Markt verfügbare Netzkomponenten unterscheiden sich u. a. in der Anzahl der verschiedenen Warteschlangen, die in den Komponenten implementiert sind. Je nach verfügbarer Anzahl solcher Warteschlangen für die Weiterleitung von Paketen empfiehlt das IEEE eine entsprechende Aufteilung der Verkehrsklassen auf die Warteschlan-

gen. Bei Verfügbarkeit von nur zwei Warteschlangen in der Netzkomponente wird empfohlen, lediglich zwischen den Verkehrsklassen Best Effort und Voice zu unterscheiden, da die höchsten QoS-Anforderungen in lokalen Netzen heutzutage durch Voice-over-IP-Technologien (VoIP) gestellt werden.

VoIP stellt sehr hohe Ansprüche an geringe Verzögerungen und Varianzen bei der Zwischenankunftszeit von Paketen. Insbesondere die Paketlaufzeit stellt hohe Ansprüche an die subjektiv empfundene Qualität der Sprachübertragung. International wird hier von einem Grenzwert von 150 ms ausgegangen. Dabei muss aber berücksichtigt werden, dass diese Latenz nicht nur durch den Transport innerhalb des Netzes entsteht, sondern auch Rechenzeit für die Kodierung und Dekodierung an den jeweiligen Endstellen erforderlich ist. Um diesen Wert zu erreichen, werden auch in LANs sehr häufig QoS-Maßnahmen ergriffen. Nicht selten ist aber z. B. ein PC über einen Mini-Switch in einem IP-Telefon an das Netz angeschlossen. Daher muss das IP-Telefon den VoIP-Verkehr gegenüber dem Datenverkehr intern priorisieren. Darüber hinaus können für die verschiedenen Klassen unterschiedliche Class Of Service Werte (COS) vom IP Phone gesetzt werden. Dabei wird das ggf. vorhandene COS-Feld im Paket des angeschlossenen PCs überschrieben.

Sofern es einen separaten Anschluss von IP-Telefonen und anderen Endgeräten gibt, könnten die Ports als Trusted Port definiert werden, welche zum Anschluss der IP-Telefone genutzt werden. D. h. der Access-Switch akzeptiert an diesen Ports das gesetzte COS-Feld und handelt danach (Zuordnung der VoIP-Pakete zur Priority Queue). Die anderen Ports werden als untrusted konfiguriert, d. h. sämtlicher eingelesener Verkehr an diesen Ports wird der Default-Queue zugeordnet. Die Anwendung dieses Modells setzt entweder eine Umkonfiguration der Switches bei Umzügen oder eine einheitliche Zuordnung voraus (Beispiel: Ports 1 bis 12 sind trusted und dienen dem Anschluss der Telefone, während die Ports 13 bis 24 untrusted sind und dem Anschluss anderer Endgeräte dienen). Alternativ könnten alle Ports als trusted konfiguriert werden, so dass die von den PC-Anwendungen gesetzten Werte im COS-Feld vom Access-Switch unverändert akzeptiert werden. Dies kann möglicherweise die Priorisierung des VoIP-Verkehrs gegenüber dem Datenverkehr aufheben, wenn bestimmte Anwendungen einen priorisierten COS-Wert setzen.

Bei der Priorisierung des Verkehrs im Netz stellt sich daher die Frage, ob den Endgeräten vertraut wird oder die entsprechenden Felder explizit von den Netzkomponenten gesetzt werden. Im ersten Fall ist die Priorisierung des Voice-Verkehrs nicht sichergestellt. Im zweiten Fall sind Umzüge, Neuanschlüsse und Änderungen mit Umkonfigurationen verbunden, oder es müssen feste Port-Bereiche für verschiedene Endgerätetypen reserviert werden. In dem zweiten Fall ist aber z.B. die Priorisierung von Voice-Verkehr (Soft-Phone) des PCs nicht möglich. Um sich diese aufwändige Konfiguration und Wartung zu ersparen, wird QoS häufig auch mittels einer im Verhältnis zum durchschnittlichen Verkehrsaufkommen vielfachen Übertragungskapazität (Overprovisioning) gewährleistet. Nicht wenige Experten rechnen jedoch vor, dass ein bis zu 15-faches Overprovisioning erforderlich ist, um Paketverluste gänzlich zu vermeiden. Welcher dieser Standpunkte nun zutreffend ist, lässt sich derzeit nicht eindeutig verifizieren. Oft herrschen jedoch Argumente vor, die eher kommerzielle Hintergründe haben als dass sie wissenschaftlich belegbar sind.

Sowohl Gegner als auch Befürworter von Overprovisioning machen sich die Verfahren der Warteschlangentheorie zu nutze, um nachzuweisen oder zu widerlegen, dass z.B. die Anforderungen von VoIP durch die Sicherstellung eines ausreichenden Netzdurchsatzes zu erfüllen sind. Die Position der Befürworter basiert darauf, dass es nach der Warteraumtheorie möglich ist, durch die Erhöhung der Bedienrate (Netzkapazität) die Länge einer Warteschlange zu einem sehr hohen Anteil der Zeit (bis auf tendenziell infinitesimale Restwahrscheinlichkeiten) unterhalb eines bestimmten Schwellenwertes zu halten. Im Umkehrschluss bedeutet dies, dass Paketlaufzeiten in einem Netz eine Funktion der Netzauslastung sind. Bleibt die Netzauslastung unterhalb eines bestimmten Schwellenwertes, übertreffen die Paketlaufzeiten quasi nie, oder genauer, nur mit einer tendenziell infinitesimalen Wahrscheinlichkeit den für VoIP kritischen Schwellenwert. Nach dieser Argumentation reicht es also aus, zur Sicherstellung der Sprachqualität die Netzauslastung in den betroffenen Bereichen stets unterhalb eines Schwellenwertes zu halten.

In sehr vielen Veröffentlichungen über die Warteraumtheorie werden exponential verteilte Zwischenankunftszeiten (Poisson-Verteilung) für die eintreffenden Pakete und so genannte M/M/1-Warteschlangen zugrunde gelegt. Grund dafür ist die relativ einfache Berechenbarkeit, die sich

Quality of Service

aus dieser Annahme heraus ergibt. Die Poisson-Verteilung ist jedoch gedächtnislos. Demnach ist es nicht möglich, anhand der bereits vergangenen Wartezeit eine Aussage darüber zu machen, wann das nächste Paket eintrifft. Die Poisson-Verteilung gilt nur für (seltene) Ereignisse, die voneinander unabhängig eintreffen. Genau das trifft aber für lokale Netze nicht zu. Denn beispielsweise ist die Ankunft von Ethernet-Frames oder IP-Paketen, die vom Aufruf einer Webseite oder von einem File-Transfer herrühren, natürlich nicht voneinander unabhängig. Vielmehr lassen sich sehr genaue Aussagen über die Zwischenankunftszeiten machen, sodass die Ergebnisse aufgrund einer angenommenen Poisson-Verteilung nicht mehr zu halten sind.

Wenn überhaupt, ist die Nutzung der Poisson-Verteilung nur für Netze bzw. Netzabschnitte mit sehr vielen, unterschiedlichen Nutzern zulässig und auch da eigentlich nur dann, wenn nicht Frames oder Pakete betrachtet werden, sondern höhere Ebenen des Protokollstapels, also etwa Sessions. Ausschließlich aufgrund sehr großer Nutzerzahlen mit völlig heterogenen Anwendungen kann davon ausgegangen werden, dass keine Aussage über die Poisson-basierte Ankunft von Paketen gemacht werden kann. Dementsprechend kann aber nur an einem Knoten in einem Kernnetz eine solche Situation vorkommen. Je weiter man die Betrachtung an den Rand eines großen Netzes verschiebt, desto mehr hängt das Verkehrsaufkommen vom Verhalten der bzw. des Benutzers und deren/dessen Anwendungen ab.

In einem lokalen Netz müsste man den Verkehr, der unmittelbar an einem Client entsteht, in irgendeiner Weise modellieren können, um mithilfe der Warteraumtheorie eine analytische Betrachtung des Verkehrsaufkommens durchführen zu können. Gleichzeitig müsste aber die Berechenbarkeit des Gesamtmodells gewährleistet bleiben. Ohne eine Einschränkung auf wenige Anwendungen und ein äußerst deterministisches Nutzerverhalten scheidet ein analytisches Verfahren jedoch aus.

Eine Alternative zur analytischen Herangehensweise wäre die Simulation von Netzen. Dazu gibt es im wissenschaftlichen Bereich bereits umfangreiche Erfahrungen, insbesondere für Weitverkehrsnetze. Simulationen erreichen heute eine extreme Realitätsnähe, ohne dazu immense Rechenleistung zu benötigen. Damit ließen sich selbst große, komplexe lokale Netze simulieren und Engpässe frühzeitig entde-

cken. Aber auch hier ist das Nutzerverhalten der kritische Punkt. Zwar ließen sich unterschiedliche Nutzerprofile oder zufälliges Nutzerverhalten integrieren, aber es bleibt der Schwachpunkt jeder Prognose.

Befürworter von QoS im LAN werden möglicherweise das folgende oder ähnliche Beispiel heran ziehen, um zu zeigen, dass es doch seltene Fälle gibt, die QoS erforderlich machen. Angenommen, an einem Switch einer Firma mit 24 Fast-Ethernet-Ports und einem Gigabit-Ethernet-Uplink sind 20 Clients angeschlossen, die alle regelmäßig die jeweiligen E-Mail-Postfächer ihrer Benutzer abfragen. Schickt nun der Chef eine wichtige E-Mail mit einem Attachment von mehreren Megabyte an alle, dann wird der Switch in den nächsten Sekunden nichts anderes mehr über den Downlink empfangen als dieses Attachment - vorausgesetzt, dass der Mail-Server der Firma schnell genug ist. Sollte in derselben Zeit noch jemand versuchen, über diesen Switch ein Voice-over-IP-Telefon zu betreiben, könnte es eng werden.

Bei diesem Beispiel ist jedoch einiges zu bedenken: Auch wenn wir annehmen, dass alle Mail-Clients gleichzeitig das Attachment herunterladen (was in der Regel nicht der Fall ist), kann der Mail-Server mindestens auf Netzwerkebene nur sequenziell arbeiten, d.h. zu einer bestimmten Zeit immer nur ein Paket sen-

den. Der Mail-Server, dessen Engpass in der Regel die Festplatten-I/O-Geschwindigkeit und andere interne Prozesse sind, wird – auch wenn er sehr schnell ist – gemäß TCP von den langsamen Clients gebremst; d.h. er sendet zum Beispiel ein typisches TCP-Window von 8 KBytes d.h. 64 kbit und belegt damit auf der Fast-Ethernet-Anbindung des Clients fuer 0,64 Millisekunden die Leitung zu einem Client. Dann wird auf das Acknowledgement des Clients gewartet. Während dieser Zeit, die mindestens mehrere Millisekunden dauert, herrscht Funkstille auf der Leitung, da der Client damit beschäftigt ist, das TCP-Window einzuordnen, das Acknowledgement zu erstellen etc.. Dieser Vorgang dauert in der Realität weit mehr als 20 Mikrosekunden. In dieser Zeit kann ein VoIP-Paket (17,5 Mikrosekunden) mühelos verschickt werden. Das nächste VoIP-Paket muss dann erst 20 Millisekunden später in dieselbe Richtung geschickt werden, so dass der Mail-Server weitere TCP-Windows verschicken und auf die Bestätigung warten kann. Nach weiteren ca. 30 TCP Windows steht wieder ein VoIP-Paket an, und so weiter und so fort.

Das Beispiel zeigt, dass UDP durch die Congestion Control von TCP einen Vorteil bei der Übertragung über ein gemeinsames Medium besitzt. Wirklich problematisch wird es daher erst, wenn eine oder mehrere UDP-basierte Anwendungen

REPORT

Quality of Service in modernen Infrastrukturen - Standards und Architekturen

Dieser Report bietet allen Betreibern von Netzen einen vollständigen Überblick über aktuelle QoS-Verfahren sowohl im LAN als auch in Wireless LANs und in WANs. Darüber hinaus werden alle Entscheider in die Lage versetzt, den



Nutzen von Maßnahmen in QoS-Techniken abzuschätzen und mit alternativen Lösungen zu vergleichen. Sie erhalten aktuellste Informationen, die vor dem Hintergrund der zunehmenden Integration von VoIP-Telefonie und der verstärkten Konvergenz von Büro- und Produktionsnetzen bei keinem Netzwerkexperten fehlen darf.

Auto: Dr. Frank Imhoff
Preis: € 398,- zzgl. MwSt. und Versand



Bestellen Sie über unsere Web-Seite www.comconsult-research.de

Quality of Service

gleichzeitig große Datenmengen senden. Es gibt jedoch kaum vorstellbare Anwendungsszenarien dafür. Denkbar wäre z.B. eine Videoübertragung mit hoher Bandbreite, die innerhalb eines Subnetzes per Broadcast statt per Multicast versendet wird.

Trotz aller Gegenbeispiele zeigt jedoch die Erfahrung, dass moderates Overprovisioning völlig hinreichend ist. Messungen zeigen, dass selbst ohne explizite Bereitstellung von Overprovisioning vollständig geschaltete LANs ausreichende Reserven für Voice over IP bieten. Bei diesen Messungen ist jedoch auf eine hinreichende Granularität der Messintervalle zu achten. Denn häufig lassen sich zwar die Belastungen einzelner Ports an Routern oder großen Switches abfragen, jedoch werden diese Werte in Minuten- oder sogar Fünf-Minuten-Intervallen ermittelt. Das sind aber deutlich zu große Messintervalle, denn Fünf-Minuten-Mittelwerte geben keine Auskunft darüber, welche Spitzenbelastungen über welchen Zeitraum existieren. Eine Spitzenbelastung bzw. völlige Auslastung einer Netzkomponente über mehrere Sekunden hinweg ist aber völlig inakzeptabel, wenn man bedenkt, dass Verzögerungszeiten von mehr als 300 ms bei VoIP schon als sehr störend empfunden werden.

Um eine realistische Grundlage für die Beurteilung zu haben, ob ein produktives Netz z.B. für VoIP geeignet ist, bleiben Messungen unerlässlich. Konkrete Beispiele aus der regelmäßigen Beratungspraxis zeigen jedoch, dass ein gut struktu-

riertes und vollständig geschaltetes Netz in der Regel ohne QoS-Maßnahmen für VoIP geeignet ist. Selbst unter Labor-Bedingungen ist es kaum möglich, den Voice-Verkehr nachhaltig zu stören. Die Gründe dafür sind vor allem bei den Eigenschaften des überwiegend genutzten TCP als Transport-Protokoll im Netz zu suchen. Im Folgenden soll auf diese Gründe und eine Reihe von Messungen eingegangen werden. Als Maß für die Qualität der Sprachübertragung wird bei diesen Versuchen der Mean Opinion Score (MOS) benutzt. Dabei wird die Sprachübertragung mit Noten von 5 (exzellent) bis 1 (schlecht) subjektiv beurteilt.

Einfluss der TCP-Verkehrslast auf die Sprachqualität

Die meisten Anwendungen verwenden heute TCP. Grund dafür ist nicht zuletzt, dass es Mechanismen zur Fehlerbehandlung, zur Flusskontrolle (Flow Control) und zur Vermeidung von Überlastsituationen (Congestion) enthält. Ursprünglich waren diese Mechanismen noch weitaus wichtiger als heute, da die Übertragungsmedien wesentlich fehleranfälliger waren als heutige Glasfaser- und Kupferkabel und über geringere Bandbreiten verfügten. Obwohl diese Schwierigkeiten in modernen Kommunikationsnetzen kaum noch ein größeres Problem darstellen, blieb TCP bisher unangefochten weit verbreitet.

Es stellt sich nun die Frage, wie sich die Übertragung vieler TCP-Verbindungen über denselben Netzwerkpfad auf

die Übertragung von VoIP auswirkt, da zur Übertragung von VoIP in der Regel ja kein TCP, sondern das verbindungslose User Datagramm Protocol (UDP) verwendet wird. Es muss also geklärt werden, wie sich die Mechanismen von TCP zur Vermeidung von Congestion gegenüber UDP-Daten verhalten und welche Parameter dazu führen, dass die UDP-Daten verloren gehen oder so stark verzögert werden, dass die Übertragung von VoIP nicht mehr sinnvoll möglich ist. Dazu wurde zunächst der in Abbildung 1 dargestellte Versuchsaufbau gewählt.

Kern des Versuchsaufbaus sind zwei Fast-Ethernet-Switches vom Typ HP Procurve 2512, die mit jeweils 24 Fast-Ethernet-Ports ausgestattet sind. Die beiden Switches sind über eine Fast-Ethernet-Verbindung miteinander verbunden. Mithilfe zweier Lastgeneratoren (PC1 und PC2) werden mehrere TCP-Streams erzeugt und an die entsprechenden Lastempfänger (PC3 und PC4) gesendet. Neben den Lastgeneratoren bzw. Empfängern sind jeweils noch ein Messrechner und ein Telefon an die Switches angeschlossen.

Zunächst wurden mit dieser Konfiguration fünf TCP-Ströme von jeweils 4 Mbit/s von PC2 zu PC4 gesandt. PC1 hat zudem drei Datenströme von 10 Mbit/s und eine variable Anzahl von Datenströmen mit 5 Mbit/s generiert. Damit wurde eine Grundlast von acht Verbindungen mit etwa 50 Mbit/s generiert, die sich mühelos über die Fast-Ethernet-Verbindung übertragen ließ. Die stufenweise Erhöhung dieser Grundlast mit bis zu 24 weiteren Verbindungen zog jedoch keine

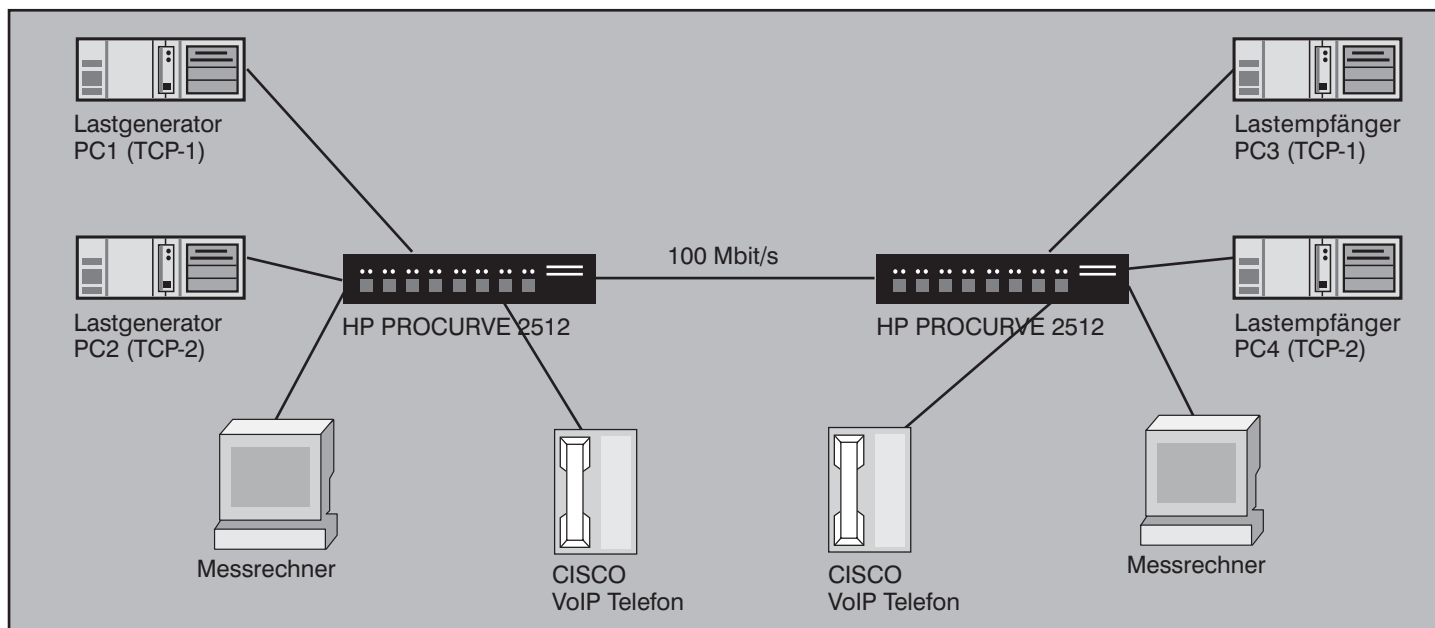


Abbildung 1: Versuchsaufbau

Quality of Service

lineare Erhöhung der Übertragungslast der Fast-Ethernet-Verbindung nach sich, sondern erreichte bei etwa 85 Mbit/s Durchsatz einen Höhepunkt. Abbildung 2 zeigt den Verlauf des Gesamtdurchsatzes und verdeutlicht den Einfluss der Mechanismen zur Vermeidung von Congestion.

Der Grund für die Grenze von ca. 85 Mbit/s sind die Flow Control und Congestion Avoidance Mechanismen von TCP, die eine Überlastung einzelner Abschnitte des Netzes bzw. eines Empfängers vermeiden sollen. Die Menge der übertragenen Daten muss daher zwischen den kommunizierenden Rechnern abgestimmt werden. Diese Algorithmen führen bei der Betrachtung einer TCP-Verbindung zu einer Sägezahn-Kurve. Nach jedem Paketverlust wird die Übertragungsrates zunächst gesenkt, um dann wieder schrittweise anzusteigen, bis zum nächsten Paketverlust. Welche Auswirkungen die unterschiedlichen Algorithmen in einem Netz auf eine parallel verlaufende VoIP-Verbindung haben, ist analytisch schwer zu fassen. Daher mussten Messungen durchgeführt werden, bei denen mehrere TCP-Verbindungen parallel existierten.

Um trotz der Effekte die Sprachqualität über die belastete Verbindung hinweg messen zu können, wurden zwei Messrechner mit IxChariot genutzt. Mithilfe der beiden VoIP-Telefone vom Typ Cisco IP Phone 7960 konnte zudem die Sprachqualität subjektiv beurteilt werden. Zur Kodierung der Sprache wurde ein G.711 µLAW Codec mit dem maximalen MOS-

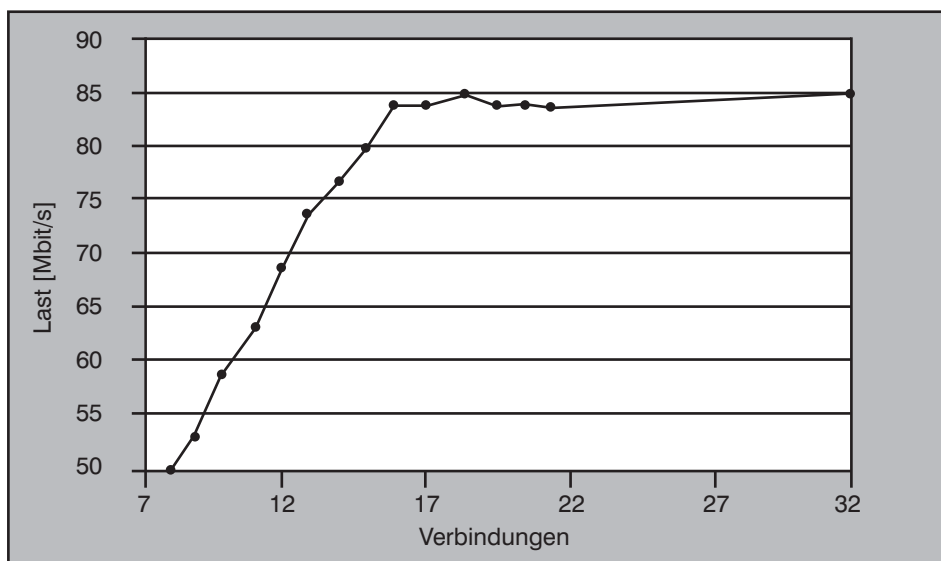


Abbildung 2: Last-Verlauf der Fast-Ethernet-Verbindung

Wert von 4,4 verwendet. Die Messungen wurden mit einem Querverkehr zwischen 50 und 85 Mbit/s in Schritten von ca. 5 Mbit/s jeweils rund fünf Minuten lang durchgeführt. Die Ergebnisse sind in Tabelle 1 zusammengefasst.

Last von 85 Mbit/s erleidet die VoIP-Übertragung Paketverluste von mehr als einem Prozent. Das sind zwar keine guten MOS-Werte mehr, eine Kommunikation ist damit aber nach wie vor möglich.

Es ist zu erkennen, dass die Sprachqualität nicht unmittelbar von der Last abhängt. Selbst unter der maximal mit TCP erreichbaren Last von rund 85 Mbit/s sind immer noch zufrieden stellende MOS-Werte zu messen. Der Mittelwert sinkt kaum unter 4, so lange die Anzahl der TCP-Verbindungen unter 20 bleibt. Erst bei mehr als 20 TCP Verbindungen mit der maximalen

Grund für dieses Verhalten ist die Flusssteuerung des TCP-Protokolls. Diese Flusssteuerung versucht, die Übertragungsgeschwindigkeit einer TCP-Verbindung bis zu einem Maximalwert zu erhöhen. Erst wenn ein Paket z.B. vom Switch verworfen werden muss, weil die Verbindung überlastet ist und der zugehörige Buffer überläuft, wird diese Erhöhung gestoppt. Das geschieht dadurch, dass der

| Last [Mbit/s] | | | Verbindungen | | | MOS | | | Übertragung | |
|---------------|-----|------|--------------|-----|------|------------|---------|---------|------------------|-------------|
| PC1 | PC2 | Ges. | PC1 | PC2 | Ges. | Mittelwert | Minimum | Maximum | Paketverlust [%] | Jitter [ms] |
| 30 | 20 | 50 | 3 | 5 | 8 | 4,37 | 4,37 | 4,37 | 0,00 | 0,02 |
| 34 | 19 | 53 | 4 | 5 | 9 | 4,37 | 4,37 | 4,37 | 0,00 | 0,07 |
| 39 | 20 | 59 | 5 | 5 | 10 | 4,37 | 4,37 | 4,37 | 0,00 | 0,10 |
| 44 | 19 | 63 | 6 | 5 | 11 | 4,37 | 4,37 | 4,37 | 0,00 | 0,21 |
| 49 | 19 | 68 | 7 | 5 | 12 | 4,36 | 3,80 | 4,37 | 0,01 | 0,66 |
| 54 | 19 | 73 | 8 | 5 | 13 | 4,31 | 3,80 | 4,37 | 0,07 | 0,76 |
| 59 | 17 | 76 | 9 | 5 | 14 | 4,20 | 3,23 | 4,37 | 0,19 | 0,92 |
| 62 | 18 | 80 | 10 | 5 | 15 | 4,11 | 2,88 | 4,37 | 0,29 | 0,98 |
| 66 | 18 | 84 | 11 | 5 | 16 | 4,07 | 2,83 | 4,37 | 0,35 | 1,05 |
| 67 | 17 | 84 | 12 | 5 | 17 | 3,92 | 2,83 | 4,37 | 0,53 | 0,99 |
| 69 | 16 | 85 | 13 | 5 | 18 | 3,86 | 2,56 | 4,37 | 0,61 | 1,04 |
| 71 | 13 | 84 | 14 | 5 | 19 | 3,59 | 2,23 | 4,37 | 0,97 | 1,05 |
| 72 | 12 | 84 | 15 | 5 | 20 | 3,44 | 2,37 | 4,37 | 1,12 | 1,06 |
| 73 | 11 | 84 | 16 | 5 | 21 | 3,29 | 2,36 | 4,37 | 1,37 | 1,04 |
| 60 | 25 | 85 | 16 | 16 | 32 | 2,97 | 1,86 | 4,37 | 2,05 | 1,03 |

Tabelle 1: Messergebnisse mit TCP-Verkehrslast

Quality of Service

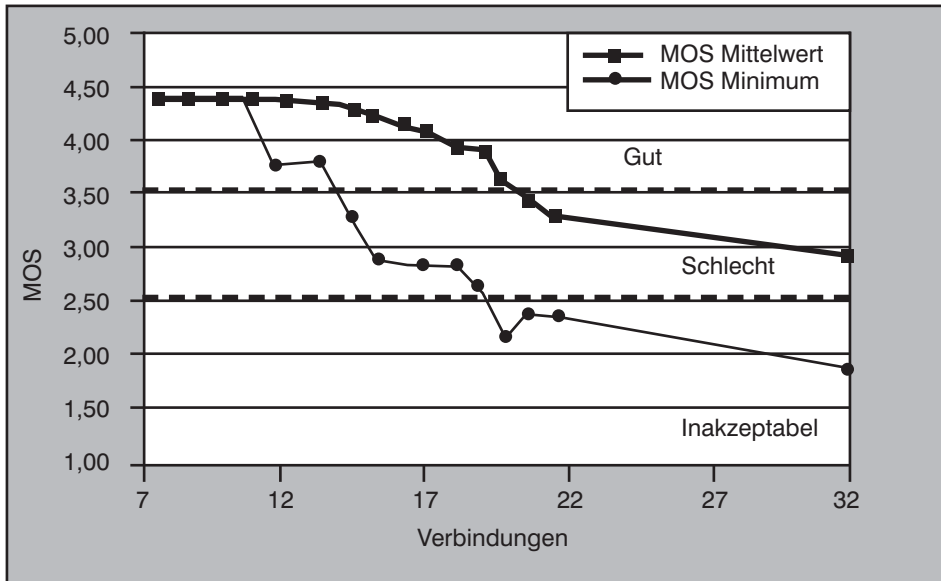


Abbildung 3: Last-Verlauf der Fast-Ethernet-Verbindung

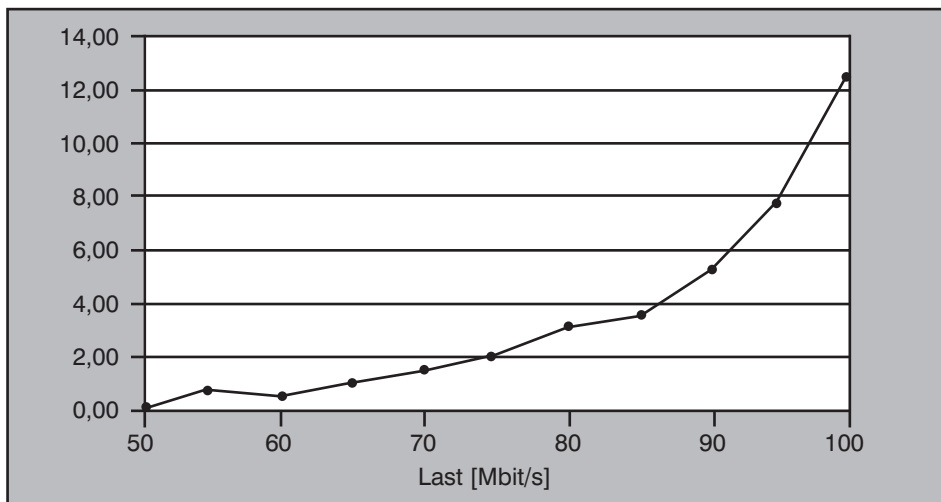


Abbildung 4: Last-Verlauf der Fast-Ethernet-Verbindung

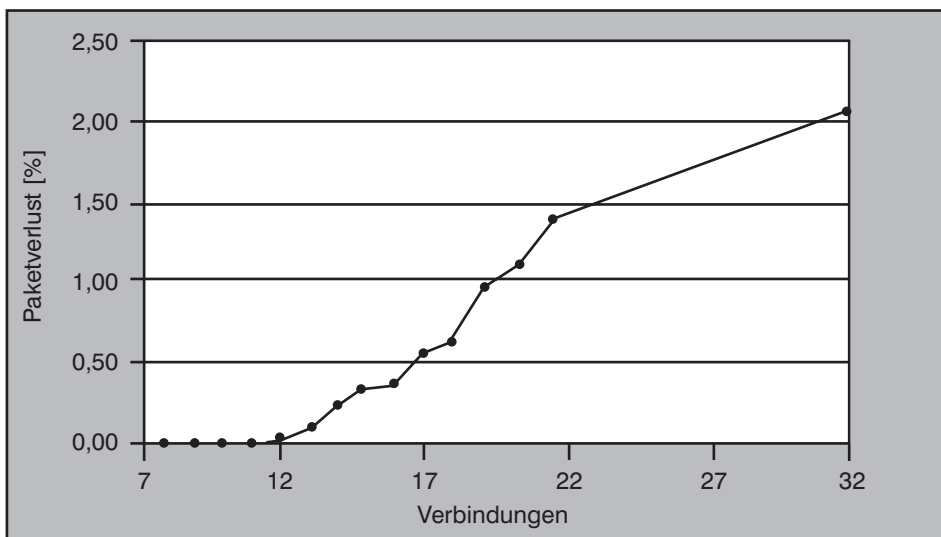


Abbildung 5: Paketverluste einer VoIP-Verbindungen bei TCP-Last

Empfänger den Paketverlust bemerkt und das entsprechende Acknowledgement nicht senden kann. Daraufhin setzt der Sender die Sendeleistung herunter und überträgt die Daten erneut. Wird eine Leitung mit wenigen TCP-Verbindungen voll belegt, bleibt durch das Warten auf die Bestätigung des Empfängers immer noch genug Zeit, um die konkurrierenden UDP-Daten zu übertragen. Mit steigender Anzahl der TCP Verbindungen wächst jedoch auch die Verlustwahrscheinlichkeit für die UDP-Übertragung, da immer mehr Pakete von verschiedenen Verbindungen zur Übertragung anstehen. Mit zunehmendem Paketverlust der UDP-Übertragung sinkt dann auch der MOS-Wert. Der Verlauf ist in Abbildung 3 gezeichnet.

Bei 20 konkurrierenden TCP-Verbindungen sinkt der mittlere MOS-Wert unter 3,5 und wird damit schlecht. Der minimale MOS-Wert sinkt gleichzeitig unter 2,5. Damit steht fest, dass eine Leitung nicht gleichzeitig mit mehr als 20 intensiv genutzten TCP-Verbindungen belastet sein sollte, wenn darüber noch VoIP in akzeptabler Qualität übertragen werden muss. In der Praxis dürften häufig noch viel mehr TCP-Verbindungen über einen Uplink verlaufen, da z.B. komplexe Webseiten mit Java-Bestandteilen gleich mehrere TCP-Verbindungen erforderlich machen, jedoch sind diese Verbindungen selten besonders belastet, so dass die eine Fast-Ethernet-Verbindung immer noch genug Reserve bieten sollte.

Weitere Versuche wurden so durchgeführt, dass die zu Beginn einer TCP-Verbindung entstehenden Effekte berücksichtigt werden konnten. Im Verlauf eines Gesprächs sind dazu u.a. 32 TCP-Streams oder UDP-Streams mit der Gesamtbandbreite von 64 Mbit/s gleichzeitig gestartet worden. Bei diesem Experiment sind subjektiv keine Störungen der Sprache zu verzeichnen gewesen. Einschwingvorgänge von TCP-Verbindungen sind offenbar nicht kritisch, sofern noch genug Bandbreite für VoIP zur Verfügung steht.

Einfluss der UDP-Verkehrslast auf die Sprachqualität

Anders stellt sich die Situation bei einer hohen Verkehrslast durch UDP-Verkehr dar. Bei UDP handelt es sich um einen verbindungslosen Dienst, der keine gesicherte Übertragung und keine Flusskontrolle bietet. UDP stellt lediglich einen Transportdienst für höhere Protokolle wie u.a. das Trivial File Transfer Protocol (TFTP), der Domain Name Services (DNS) oder das Lightweight Directory Access Protocol (LDAP) zur Verfügung.

Quality of Service

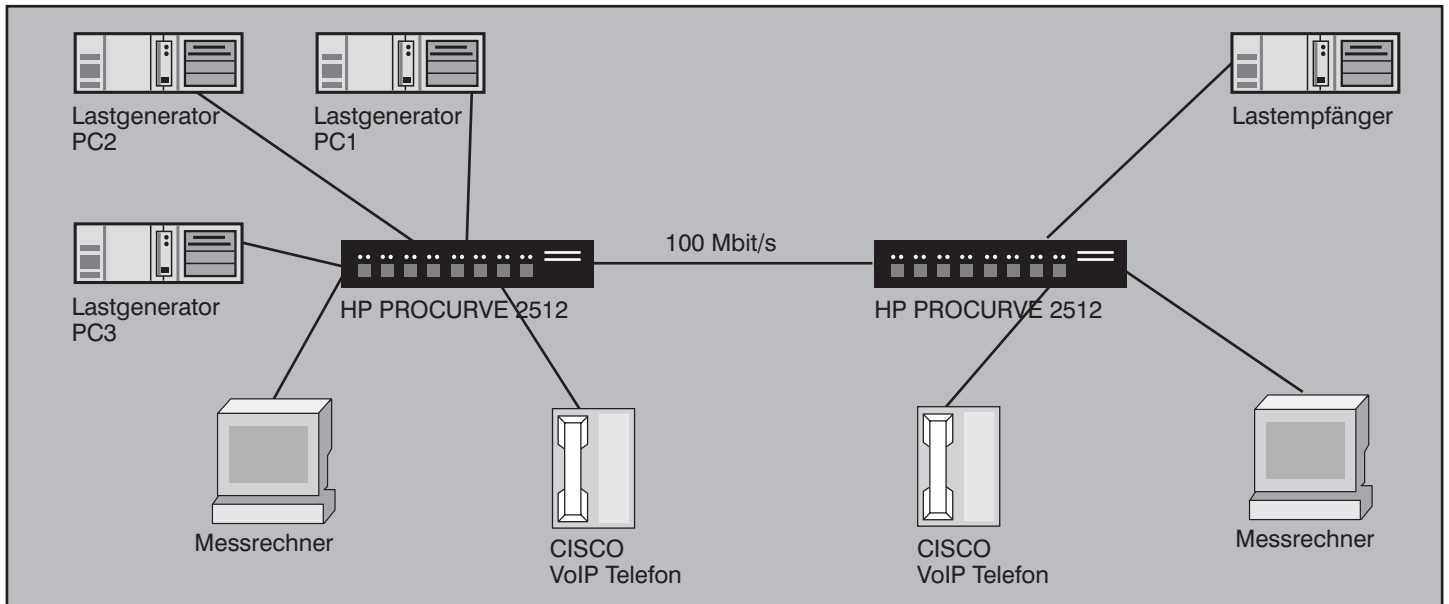


Abbildung 6: Zur Messung von UDP-Last eingesetzter Versuchsaufbau

| Last [Mbit/s] | | | | MOS | | | Übertragung | |
|---------------|-----|-----|------|------------|---------|---------|------------------|-------------|
| PC1 | PC2 | PC3 | Ges. | Mittelwert | Minimum | Maximum | Paketverlust [%] | Jitter [ms] |
| 0 | 32 | 18 | 50 | 4,43 | 3,79 | 4,37 | 0,03 | 0,00 |
| 5 | 32 | 18 | 55 | 4,26 | 3,23 | 4,37 | 0,44 | 0,44 |
| 10 | 32 | 18 | 60 | 4,05 | 2,83 | 4,37 | 0,38 | 0,60 |
| 15 | 32 | 18 | 65 | 3,54 | 2,06 | 4,37 | 1,05 | 0,90 |
| 20 | 32 | 18 | 70 | 3,34 | 2,07 | 4,37 | 1,41 | 1,07 |
| 25 | 32 | 18 | 75 | 2,97 | 1,26 | 4,37 | 2,04 | 1,24 |
| 30 | 32 | 18 | 80 | 2,62 | 1,00 | 4,37 | 2,85 | 1,33 |
| 35 | 32 | 18 | 85 | 2,37 | 1,25 | 3,80 | 3,41 | 1,45 |
| 40 | 32 | 18 | 90 | 1,86 | 1,00 | 2,90 | 4,99 | 1,82 |
| 45 | 32 | 18 | 95 | 1,18 | 1,00 | 2,23 | 7,70 | 1,70 |
| 50 | 32 | 18 | 100 | 1,00 | 1,00 | 1,01 | 12,57 | 1,64 |

Tabelle 2: Messungen der Sprachqualität bei UDP-Verkehr

Welcher prozentuale Anteil an Paketverlusten eine Sprachverbindung gemessen an der Auslastung einer Leitung durch UDP-Datenströme mit sich bringt, ist in Abbildung 4 dargestellt.

Im Vergleich dazu ist in Abbildung 5 der Paketverlust der Sprachübertragung in der Abhängigkeit von der Anzahl der TCP-Verbindungen unter größtmöglicher Last dargestellt. Dabei zeigt sich deutlich, dass die UDP-Datenströme sehr viel mehr Paketverluste bei einer parallel verlaufenden VoIP-Verbindung anrichten als durch TCP-Connections überhaupt erreicht werden kann.

Legt man die in Abbildung 3 erzielten Ergebnisse zugrunde, ergibt sich, dass eine

durchweg gute Sprachverbindung maximal 20 parallele TCP-Verbindungen unter voller Last verkraftet. Das entspricht beim Vergleich mit Abbildung 5 einem maximalen Paketverlust der VoIP-Verbindung von nur einem Prozent. Aus Abbildung 4 ergibt sich jedoch für einen anteiligen Paketverlust von einem Prozent eine maximale Auslastung von kaum mehr als 60 Prozent.

Zusammenfassend lässt sich damit feststellen, dass eine Belastung von UDP-Strömen nicht mehr als 60 Prozent erreichen sollte, um den MOS-Wert einer parallel übertragenen VoIP-Kommunikation nicht wesentlich unter 3,5 fallen zu lassen.

Zur Berechnung der Sprachqualität einer durch UDP belasteten Fast-Ethernet-Verbindung wurde der in Abbildung 6 dargestellte Versuchsaufbau gewählt. Die beiden Lastgeneratoren PC2, PC3 haben mithilfe der Software IP-Traffic eine Grundlast von 50 Mbit/s erzeugt, indem 16 bzw. neun unabhängige UDP-Streams mit jeweils 2 Mbit/s und Paketgrößen zwischen 128 bis 6460 Bytes erzeugt haben. Der dritte Lastgenerator (PC1) erzeugte bis zu zehn Streams mit jeweils 5 Mbit/s. Diese Daten wurden über die 100 Mbit/s Fast-Ethernet-Leitung zum Lastempfänger gesendet. (siehe Abbildung 6)

Zur Messung der Sprachqualität wurden zwei Messrechner benutzt, die mit dem Programm IxChariot die Qualität der belasteten Verbindung zwischen den beiden Switches gemessen haben. Um einen möglichst objektiven Eindruck zu gewinnen, wurden zudem noch zwei Cisco VoIP-Telefone angeschlossen. Die Sprache wurde mit dem G.711 µLAW Codec mit dem maximalen MOS-Wert von 4,4 kodiert. Die Messungen wurden mit der Gesamtlast zwischen 50 und 100 Mbit/s in Schritten von 5 Mbit/s jeweils fünf Minuten lang durchgeführt. Die Ergebnisse sind in der Tabelle 2 zusammengefasst.

Die ermittelten Daten zeigen deutlich, dass die Qualität der übertragenen Sprache mit der steigenden Last abfällt. Bei einer Last von über 65 Mbit/s ist die Sprachqualität im Mittel als schlecht einzustufen, ab ca. 82 Mbit/s als inakzeptabel. Wichtig ist aber auch die MOS-Minimumkurve, die die Sprachqualität in kurzen Abschnitten betrachtet und daher in keinem Fall in den inakzeptablen Bereich absinken. Die Gren-

Quality of Service

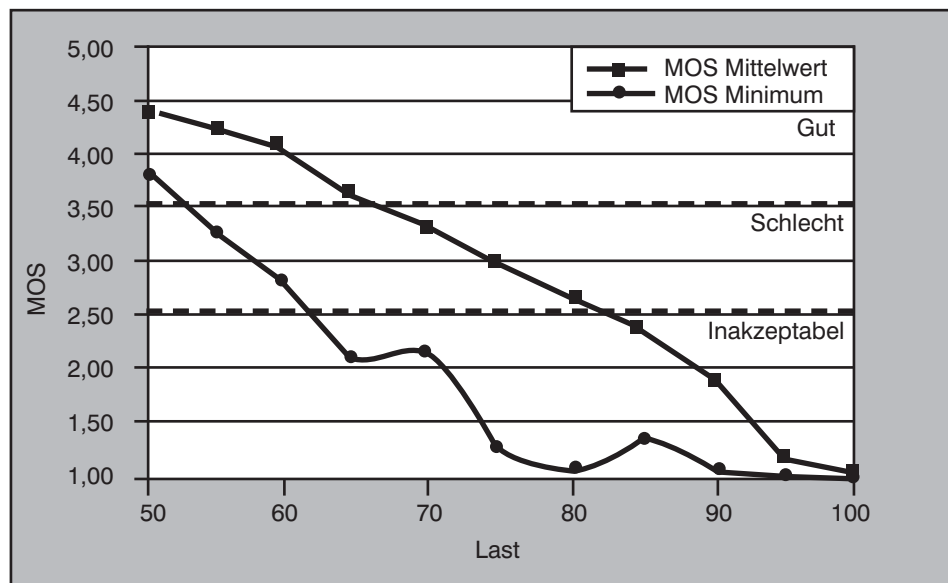


Abbildung 7: Einfluss von UDP-Verkehr auf die Sprachqualität

ze der akzeptablen Gesamtlast liegt daher schon bei ca. 62 Mbit/s. Um sicher zu gehen, wäre sogar ein Grenzwert von 52 Mbit/s vorzusehen, damit die VoIP-Nutzer unter unregelmäßig auftretenden Störungen leiden. Bei der subjektiven Betrachtung mithilfe der VoIP-Telefone konnte diese Feststellung bestätigt werden.

In der Praxis werden jedoch nur selten reine UDP- oder reine TCP-Verkehre über eine Trunk-Verbindung auftreten. In der Regel wird immer eine Mischung auftreten. Jedoch wird in herkömmlichen Netzen wesentlich häufiger mit TCP-Verbindungen als mit UDP zu rechnen sein. Das liegt vorwiegend daran, dass die Kommunikation von Zugriffen auf Webseiten oder Fileserver und Datenbanken dominiert wird, die ausschließlich TCP-Verbindungen nutzen. Eine Ausnahme stellen natürlich dedizierte Leitungen z.B. für die Kommunikation über virtuelle Private Netze (VPN) oder für reine VoIP-Kommunikation dar.

Fazit

Nahezu alle Hersteller von Netzkomponenten bieten inzwischen auch für LANs Lösungen zur Unterstützung von QoS an. Hauptargument für die Einführung von QoS in LANs sind Einsparungen, die bei der Erstbeschaffung im Vergleich zu Overprovisioning anfallen. Dieses Kostenargument ist aufgrund des ständigen Preisverfalls auch von sehr hochwertigen Netzkomponenten und Gigabit-Technologien aber kaum noch zu halten, so dass viele LAN-Betreiber selbst bei Einführung von zeitkritischen Applikationen wie VoIP den Weg des Overprovisioning statt der Einstellung von QoS in den Netzkompo-

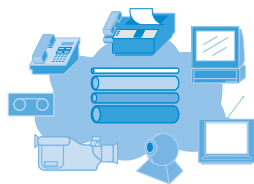
nenten gehen. Die Präferenz für eine solche Vorgehensweise basiert auch auf den negativen Erfahrungen mit QoS-Mechanismen. Die Hersteller von Netzkomponenten arbeiten seit Jahren an komplexeren Lösungen für die Sicherstellung der QoS. Viele dieser Lösungen sind aufgrund der Komplexität und der daraus resultierenden mangelnden Akzeptanz bereits verworfen worden.

Selbst beim relativ simplen DiffServ-Ansatz ist eine komplexe Konfiguration der Netzkomponenten für die Erkennung und Zuordnung der Datenströme zu Prioritätsklassen sowie für die differenzierte Behandlung dieser Klassen erforderlich. Da eine solche manuelle Konfiguration jeder Netzkomponente in einem großen Netz kaum praktikabel ist, arbeiten die Hersteller an so genannten Policy-Konzepten. Im Rahmen dieser Konzepte werden die für QoS erforderlichen Konfigurationsvorgaben zentral an einer Konsole festgelegt und von dieser Konsole aus auf die Netzkomponenten verteilt. Jedoch lassen sich auch damit kaum bössartige Benutzer oder Anwendungen davon abhalten, Prioritätsregelungen zu missbrauchen. Das ist nur auf Kosten der Flexibilität eines Netzes zu gewährleisten (z.B. feste Zuordnung einzelner Geräte zu den Ports eines Switches).

Inzwischen sind vielfältige, z. T. hoch komplexe Proirisierungsmechanismen implementiert worden. Mathematische Untersuchungen belegen jedoch, dass nur die höheren Prioritätsklassen in den Genuss einer leicht verbesserten Durchsatz- und Wartezeitsituation kommen. Allen übrigen Prioritätsklassen drohen empfindliche Nachteile, die deren Performance im Vergleich zu nicht-priorisierten Klassen um ein Vielfaches verschlechtert.

SEMINAR

Quality of Service - QoS 16.10. - 17.10.06 in Köln



Dieses 2-tägige Seminar befasst sich mit Quality of Service (QoS) in LAN, WAN und WLAN. Sie lernen, wann QoS erforderlich ist, welche QoS-Standards es gibt, wie eine beherrschbare Architektur aussieht und wie QoS funktioniert.

Die Hersteller von Netzkomponenten arbeiten seit Jahren an Lösungen für die Sicherstellung der QoS. Viele dieser Lösungen sind aufgrund ihrer Komplexität bereits verworfen worden. Auch im Fall des einfachsten QoS-Modells der differenzierten Behandlung von wenigen Verkehrsklassen ist eine komplexe Konfiguration von Netzkomponenten erforderlich.

Ist jedoch die Strategie des „Überangebots“ an Netzkapazität aufgrund der technischen und wirtschaftlichen Rahmenbedingungen nicht umsetzbar, führt an QoS-Maßnahmen kein Weg vorbei.

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



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

Quality of Service

Aus der Entwicklung ähnlicher Priorisierungsmechanismen für Betriebssysteme (Stichwort: Scheduling) ist bekannt, dass die Wahl einer falschen Bearbeitungsstrategie für die verschiedenen Prioritätsklassen mit erheblichen Nachteilen für die niedrigeren Prioritätsklassen verbunden sein kann und im Extremfall sogar eine Blockade dieser Klassen möglich ist. Da jedoch das Verhalten von Anwendungen im Netz extrem dynamisch ist, muss zur Vermeidung dieser Probleme die Bearbeitungsstrategie von Warteschlangen ständig angepasst werden. Dies ist im realen Betrieb der Netze nicht praktikabel. Die Einstellung von QoS-Mechanismen und Policy-Konzepten führt darüber hinaus zu einer sehr komplexen Fehlersuche, zu einer starken Herstellerabhängigkeit durch inkompatible Ansätze und zu erheblich höherem Wartungsaufwand.

Im Gegensatz zu Priorisierungsmaßnahmen zeichnet sich ab, dass mithilfe eines moderaten Overprovisioning, also der Überdimensionierung des Netzes, mindestens ebenso gute Resultate erzielt werden können. Dabei ist jedoch zu beachten:

- Netze und Switch-Systeme müssen konsequent unterhalb der maximal möglichen Auslastung betrieben werden. In der Regel wird hier eine maximale Auslastung von 70 % empfohlen. Diese Auslastung muss durch permanente Überwachung und durch die Einführung von Schwellenwerten sichergestellt werden.
- Messungen der Auslastung müssen regelmäßig durchgeführt werden. Auf keinen Fall reichen dafür Mittelwerte über einen Zeitraum von einer Minute und mehr.
- Die Verwendung von Shared Media, Hubs und älteren Switches scheidet aus, da hierdurch allzu leicht Engpässe auftreten.
- Sehr große Netze sollten sinnvoll strukturiert sein. Dazu gehört eine hinsichtlich Kapazität möglichst abgestimmte Auslegung verschiedener Netzbereiche und Hierarchiestufen. Die Struktur darf möglichst keine Single-Points-of-Failure enthalten, welche auch im Normalbetrieb zu Flaschenhälsen werden können.
- In heutigen LANs sind Gigabit- und Multigigabit-Technologien erforderlich, um dem steigenden Übertragungsaufkommen gerecht zu werden.

Messungen in mittleren und großen Netzen haben gezeigt, dass die heute üblichen Netze völlig ausreichende Reserven bieten, um ohne weiteres VoIP einzuführen. Selbst mit der Erzeugung künstlicher Last ist nur selten eine erhebliche Beeinträchtigung der VoIP-Qualität zu verzeichnen.

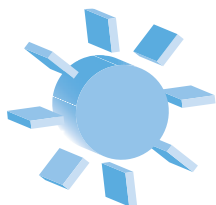
Die Nutzung von Overprovisioning im LAN hat neben den VoIP-spezifischen QoS-Aspekten wie geringer Delay oder Jitter in der Regel auch noch den Vorteil, dass für die herkömmliche Datenkommunikation Redundanzen aufgebaut werden und eine bessere Skalierbarkeit des Netzes gewährleistet ist. Beim Ausfall eines einzelnen Knotens finden dadurch meistens keine nennenswerten Beeinträchtigungen statt. Kommen weitere Endgeräte hinzu, sind ebenfalls keine grundlegenden Änderungen des Netzes notwendig. Zudem können sehr viele Wartungs- und Ausbaumaßnahmen durchgeführt werden, ohne

dass ganze Bereiche abgeschaltet oder vom restlichen Netz getrennt werden müssen.

Größter Vorteil eines moderaten Overprovisioning ist jedoch der stark vereinfachte Betrieb, da keine komplexe und aufwändige Parametrierung sowie eine dauernde Pflege oder restriktive Handhabung der Anschlussverteilung erforderlich ist. Diese Vereinfachung wiegt die geringfügig höheren Kosten bei der Erstbeschaffung angesichts der Dominanz der Betriebskosten (insbesondere der Personalkosten) mehr.

Natürlich gelten diese Ergebnisse nicht generell. Es ist durchaus denkbar, dass unter besonderen Umständen auch besondere Maßnahmen zur Sicherstellung einer Dienstgüte erforderlich sind. Es ist aber zu erwarten, dass unter diesen Umständen andere Probleme zugrunde liegen und einer Lösung bedürfen.

Sommerschule 2006



19.06. - 23.06.06
in Aachen

Auch in diesem Jahr bietet die Sommerschule wieder den Intensiv-Update auf den neuesten Stand der Netzwerk-Technik, zeigt neue Nutzungs-Potenziale, diskutiert Änderungen im Design, analysiert aktuelle Produktrends. Damit wendet sich die Sommerschule speziell an erfahrene Teilnehmer/Innen, die den Betrieb ihrer bestehenden Netzwerke weiter optimieren und neue Entwicklungen und Technologien kennen lernen wollen.

Die Sommerschule 2006 bietet folgende Schwerpunkte:

- Der Cisco-Design-Guide in der Analyse
- Mobile Kommunikation
- Privacy und Sicherheit bei der mobilen Kommunikation
- Bluetooth-Sicherheit in der Praxis
- Netzwerk-Design 2006
- Das Session-Initiation Protokoll SIP in der Analyse
- Auswahl neuer Switch-Systeme für den Workgroup-Bereich
- Videoüberwachung über IP
- Einsatz von Netzwerk-basierten IPS
- Wireless-Networks
- Sicherheit in der IP-Telefonie
- Identity und Access-Management an einem Projektbeispiel,
- Von 802.1X zur Anmeldung von Benutzern und Trennung von Benutzergruppen
- Quality of Service in Netzwerken professionell nutzen

Moderation: Markus Schaub
Preis: € 2.290,- zzgl. MwSt.



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

Neues Seminar

Troubleshooting Exchange Server 2003

Inkl. Neuerungen durch Exchange Server 2003 Service Pack 2

Die ComConsult Akademie veranstaltet vom 16. - 17. Oktober erstmalig ihr neues Seminar „Troubleshooting Exchange Server 2003“ in Aachen.

Im Vergleich zu seinen Vorgängern bietet Exchange Server 2003 ein enormes Leistungspotential und ist dazu geeignet tausende Postfächer auf einem einzigen Serversystem zu verwalten. Gerade bei solch hoch skalierten Systemen ist eine hohe Verfügbarkeit unabdingbar und für den Fall eines katastrophalen Datenverlusts eine schnelle und sichere Wiederherstellung entscheidend.

Gleichzeitig steigt das Nachrichtenaufkommen stetig sowohl organisationsintern als auch im Austausch mit dem globalen Internet. Ein großer Prozentsatz der aus dem Internet stammenden Nachrichten ist dabei unerwünscht und zum Teil virulent, was die gestellten Anforderungen an die Verfügbarkeit der Kommunikationsdienste gefährdet und die Wahrscheinlichkeit eines Datenverlusts erhöht.

Analog zum Seminar „Troubleshooting Windows Server 2003 Active Directory inkl. Neuerungen zu Windows Server 2003 R2“ stellt auch dieses Seminar ei-



nen Mix aus Know-How-Auffrischungen, Live-Demonstrationen und Praxis dar und knüpft teilweise an die dort behandelten Themen an.

Dieses Seminar ruft bewährte Technologien der Exchange Server-Produkte nochmals bei den Teilnehmern in Erinnerung und zeigt anhand dieses Know-How effiziente Maßnahmen zur Sicherung, Reparatur und Wiederherstellung von Exchange-Daten auf. Des Weiteren werden die Möglichkeiten betrachtet, die Exchange

Server 2003 mit integriertem Service Pack 2 bietet, um dem wachsenden Problem zu begegnen, welches durch die Flut unerwünschter Nachrichten entsteht.

In diesem Seminar lernen Sie

- Die Exchange Datenspeicherung und Transaktionsprotokollierung
- Die Exchange Datensicherung mit dem Windows Sicherungsprogramm und weiterer Microsoft-Tools in verschiedenen Situationen
- Die Reparatur von beschädigten Exchange Daten
- Die Exchange-Datenwiederherstellung mit dem Windows Sicherungsprogramm und von Microsoft erhältlichen Tools
- Der Einsatz und die Konfiguration der in Exchange integrierten Mechanismen zur Abwehr unerwünschter Nachrichten

Durch das Seminar führt Sie Dipl.-Ing. Peter Kleynen. Herr Kleynen ist seit 2004 als freier Mitarbeiter bei der ComConsult Beratung und Planung GmbH als Berater im Competence Center BackOffice tätig. Zu seinen Kernkompetenzen zählen der Entwurf von Active Directory- und Exchange-Umgebungen sowie deren Implementierung und Migration.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Troubleshooting Exchange Server 2003

Ich buche das Seminar

Troubleshooting Exchange Server 2003

vom 16. - 17.10.06 in Aachen

zum Preis von € 1.390,- zzgl. MwSt.

Vorname _____

Nachname _____

Bitte reservieren Sie für mich ein Hotelzimmer

vom _____ bis _____ 06

Firma _____

Telefon/Fax _____

Straße _____

PLZ, Ort _____

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

eMail _____

Unterschrift _____

Planung für Voice over IP

Evaluierung von Architekturen und Details zur Realisierung

Der Technologie-Report von ComConsult Research erarbeitet einen Leitfaden zur Umsetzung von IP-Telephonie in der Praxis. Alternativen werden verglichen, bekannte Probleme aufgezeigt und erfolgreiche Konzepte vermittelt. Der Autor blickt auf langjährige Erfahrungen bei der Konzipierung und der Planung von Netzen und Kommunikationslösungen zurück und gibt mit vielen Tipps und Tricks sein Wissen und seine Betriebserfahrung aus aktuellen Projekten an die Leser weiter.

Im Folgenden stellen wir Ihnen einen Auszug als Leseprobe zur Verfügung:

1.1. Redundanzkonzept für zentrale Komponenten

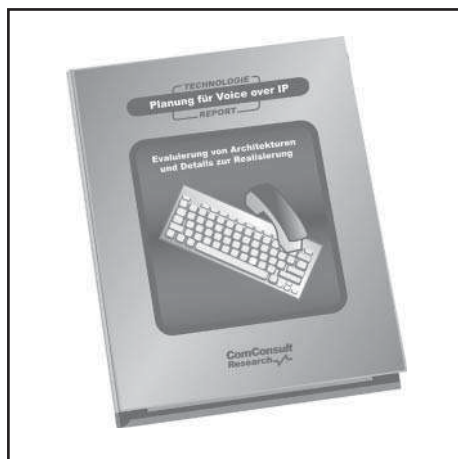
Jede VoIP-Umgebung benötigt zentrale Komponenten, von denen die Verfügbarkeit der gesamten VoIP-Umgebung oder bestimmter Dienste dieser Umgebung abhängig ist. Um die Verfügbarkeit dieser Komponenten zu erhöhen, sind Maßnahmen erforderlich, die im Abschnitt 2.4 bereits dargestellt wurden. Die Auswirkungen dieser Maßnahmen auf die LAN-Architektur sind Gegenstand dieses Abschnitts.

1.1.1. Redundanter Anschluss von Servern

Server, die bestimmte Dienste in einer VoIP-Umgebung anbieten, können redundant an das Netz angeschlossen werden, indem jeder Server mindestens zwei Netzanschlüsse aufnimmt, die mit unterschiedlichen Switches verbunden werden. Damit dieses Redundanzkonzept wirksam ist, müssen in der Regel die Netzanschlüsse des Servers demselben IP-Subnetz, d. h. demselben VLAN, zugeordnet werden. (siehe Abbildung 1)

Das dargestellte Design ist die Grundlage der meisten angewandten Verfahren. Zwischen den dargestellten beiden Ports, an die der Server angeschlossen ist, muss eine Layer-2-Verbindung bestehen. Dies kann z. B. durch die nachfolgend dargestellte Netzstruktur erreicht werden. (siehe Abbildung 2)

Die beiden Switches, an die der Server angeschlossen ist, müssen folgende Ports mit unterschiedlichen Konfigurationen aufnehmen:



• Ports der Verbindung zwischen zwei Layer-2-Switches bzw. zwischen zwei Layer-2-Switch-Instanzen in zwei kombinierten Layer-2/3-Switches. Diese Ports sind deshalb erforderlich, weil sich das IP-Subnetz des Servers aus Redundanzgründen auf mindestens zwei Layer-2-Switches erstrecken muss.

- Ports der Kategorie 3 sind reine Layer-3-Switchports, d. h. dort besteht eine 1:1-Zuordnung zwischen dem physikalischen Port und der IP-Schnittstelle des Layer-3-Switches. Diese Ports dienen der Verbindung zwischen den Layer-3-Instanzen auf den Server-Switches.

- Ports der dargestellten Kategorie 1 dienen als gebridgedete Ports dem Anschluss von Servern. Diese Ports werden dem Server-VLAN zugeordnet und werden von manchen Herstellern als Layer-2-Switchports bezeichnet.

- Ports der Kategorie 4 sind wie die der dritten Kategorie Layer-3-Ports und werden zur Verbindung der Serverswitches mit übergeordneten Layer-3-Backbones verwendet.

Das dargestellte Design ist eine der möglichen Netzstrukturvarianten, welche die Anforderung der redundanten Anbindung von Servern erfüllen.

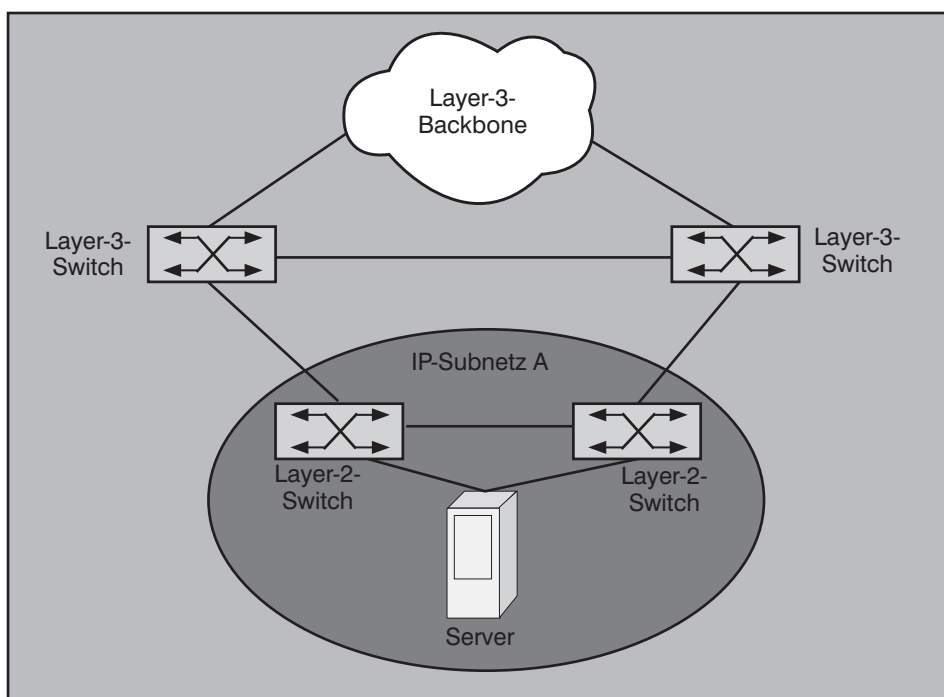


Abbildung 1: Redundanter Serveranschluss in einem IP-Subnetz

Planung für Voice over IP

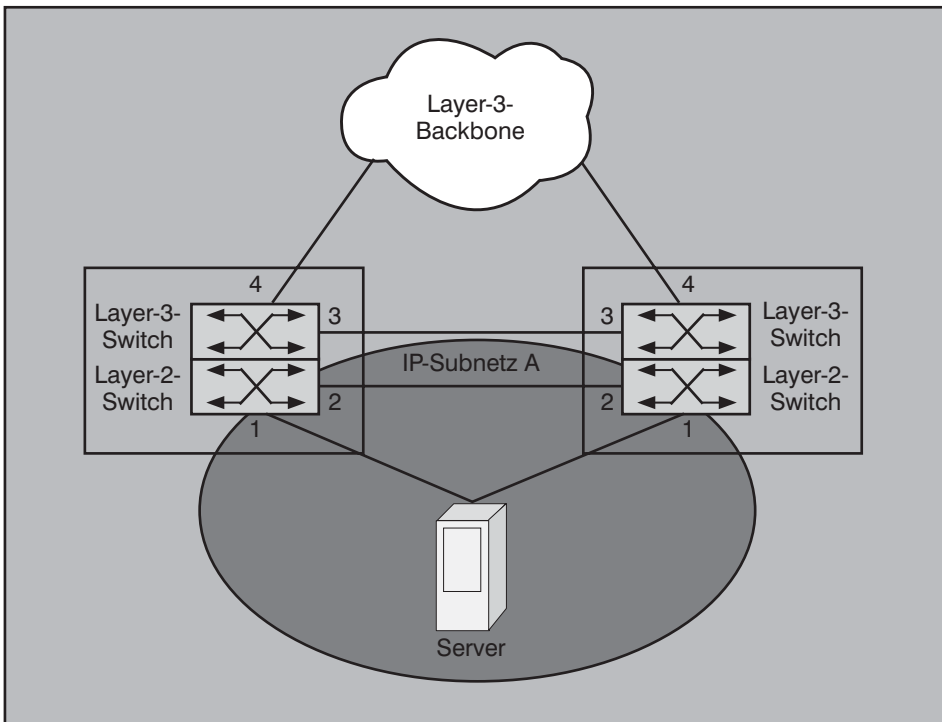


Abbildung 2: Unterschiedlich konfigurierte Ports in einem Serverswitch

1.1.2. Redundante Auslegung von Servern

Im Abschnitt 2.4 wurde auch die redundante Auslegung von Telefonieservern als Mechanismus für die Erhöhung der Verfügbarkeit von VoIP-Umgebungen dargestellt. In vielen Umgebungen reicht es nicht aus, die Netzinfrastruktur einschließlich der Netzanbindung von Servern redundant auszuliegen. Eine solche Be-

schränkung der Redundanz auf das Netz würde die Ausfälle der Server selbst nicht abdecken. Durch die zunehmende Standardisierung und Stabilisierung der Redundanzverfahren im Netzbereich verlagert sich die Wahrscheinlichkeit potenzieller Ausfälle in Richtung der Server. Daher werden Lösungen für die redundante Auslegung von Telefonieservern von den Herstellern angeboten. Allein der Vorteil der

größeren Unabhängigkeit von Wartungsfenstern bei Software Updates und anderen Änderungen ist häufig die Motivation, solche Lösungen einzusetzen.

Das erste Modell für die redundante Auslegung eines Telefonieservers ist in Abbildung 3 dargestellt.

Bei den beiden dargestellten Servern handelt es sich um zwei Instanzen im Netz, die über dieselbe virtuelle IP-Adresse und in der Regel auch dieselbe virtuelle MAC-Adresse erreichbar sind. Im Normalfall sind die virtuelle IP- und die virtuelle MAC-Adresse dem einem der beiden Server, dem so genannten aktiven Server, zugeordnet. Fällt dieser aus oder wird er vom Netz getrennt, bemerkt der zweite dargestellte Server, der so genannte Standby-Server, diesen Ausfall und beansprucht die virtuelle IP- und MAC-Adresse für sich. Da die Konfiguration der beiden Server synchronisiert ist, bleiben die von den Servern angebotenen Dienste verfügbar.

Aufgrund der Verwendung derselben IP- (und unter Umständen MAC-)Adresse von zwei Servern, die sinnvollerweise an zwei verschiedene Switches angeschlossen werden, gelten für die Konfiguration dieser Switches dieselben Überlegungen wie im Abschnitt 4.2.1 dargestellt, d. h. zwischen den beiden Serverswitches muss eine Layer-2-Verbindung bestehen.

Das dargestellte IP-Telefon adressiert in diesem Szenario den Telefonieserver immer unter derselben virtuellen IP-Adresse,

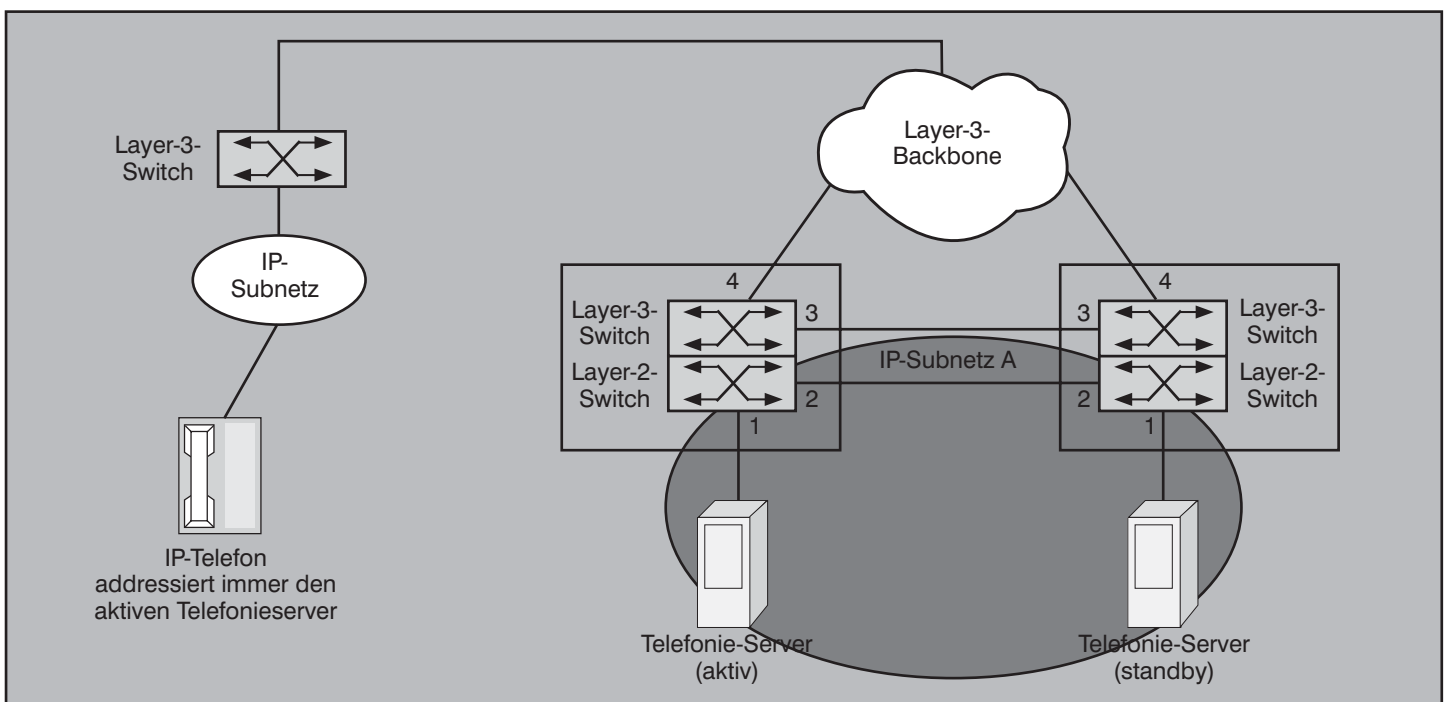


Abbildung 3: Serverredundanz, Modell 1

Planung für Voice over IP

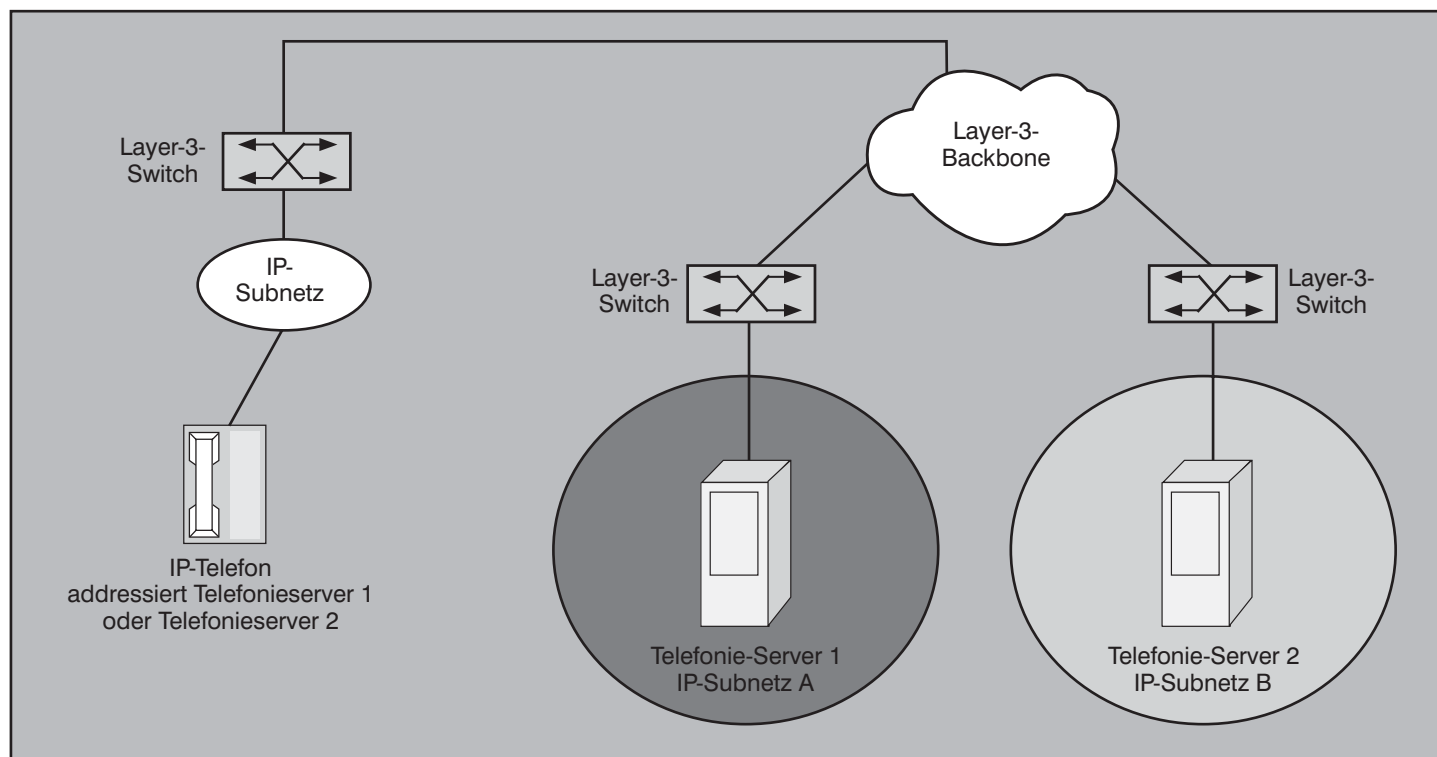


Abbildung 4: Serverredundanz, Modell 2

deren Erreichbarkeit nicht von der Verfügbarkeit eines einzigen physikalischen Servers abhängig ist.

Dieses Modell wird von einigen Herstellern von Telefonieservern unterstützt. Andere Hersteller gestalten ihr Redundanzkonzept nach dem folgenden Verfahren. (siehe Abbildung 4)

Dabei bieten die beiden dargestellten Telefonieserver dieselben Dienste (und werden laufend synchronisiert). Es handelt sich um zwei unabhängige Instanzen im Netz, die auch über unterschiedliche IP-Adressen erreichbar sind. Die beiden Server können (müssen aber nicht) unterschiedlichen Subnetzen zugeordnet werden. Entscheidend ist, dass den VoIP-Endgeräten wie IP-Telefonen, aber auch Gateways, beide Telefonieserver bekannt gemacht werden. Die Clients (d. h. IP-Telefone oder Gateways) selbst bemerken den Ausfall eines Servers dadurch, dass der Server auf ihre Anfragen nicht antwortet, und richten sich an den anderen Server.

1.1.3. Redundante Auslegung von Gateways

Eine VoIP-Architektur kann vorsehen, dass z. B. für die Kommunikation über das PSTN wahlweise oder aus Redundanzgründen verschiedene Gateways zum Einsatz kommen, wobei diese Gateways auch an unterschiedlichen Standorten im IP-Netz aufgestellt sein können. Dies bedeutet, dass in der Regel die redundan-

te Auslegung von Gateways auch derart möglich sein muss, dass ein Gateway in einem anderen IP-Subnetz die Funktion eines ausgefallenen Gateways übernehmen kann. (siehe Abbildung 5)

Dieses Modell entspricht dem im Abschnitt 4.2.2 dargestellten zweiten Modell für die redundante Auslegung von Servern, d. h. die Endgeräte müssen wahlweise den einen oder anderen Gateway für denselben

15% Rabatt bei Seminarteilnahme



IP-Telefonie: Vorbereitung, Migration, Management

26.06. - 28.06.06 in Aachen

Die Referenten dieses 3-tägigen Seminars vermitteln ihre jahrelangen Projekt-Erfahrungen bei der Nutzung und des Betriebs von IP-Telefonie sowie bei der Durchführung hochkomplexer Projekte in diesem Umfeld.

Jedes Unternehmen muss die IP-Telefonie in ihre IT- und TK-Planungen einbeziehen. Die Netze sind für IP-Telefonie vorzubereiten, Produkte auszuwählen, Migrationspläne fertig zu stellen und das Betriebs- und Management-Konzept für die IP-Telefonie-Umgebung auszuarbeiten. Alle diese Arbeiten können mittlerweile von den Erfahrungen eines breiten Spektrums von IP-Telefonie-Projekten von einigen Dutzend bis mehrere Tausend IP-Telefonen profitieren.

Teilnehmer an diesem Seminar können die hier vorgestellte Studie zum Sonderpreis von nur € 338,- zzgl. MwSt. erwerben.

Referent: Dr.-Ing. Behrooz Moayeri
Preis: € 1.690,- zzgl. MwSt.



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

Planung für Voice over IP

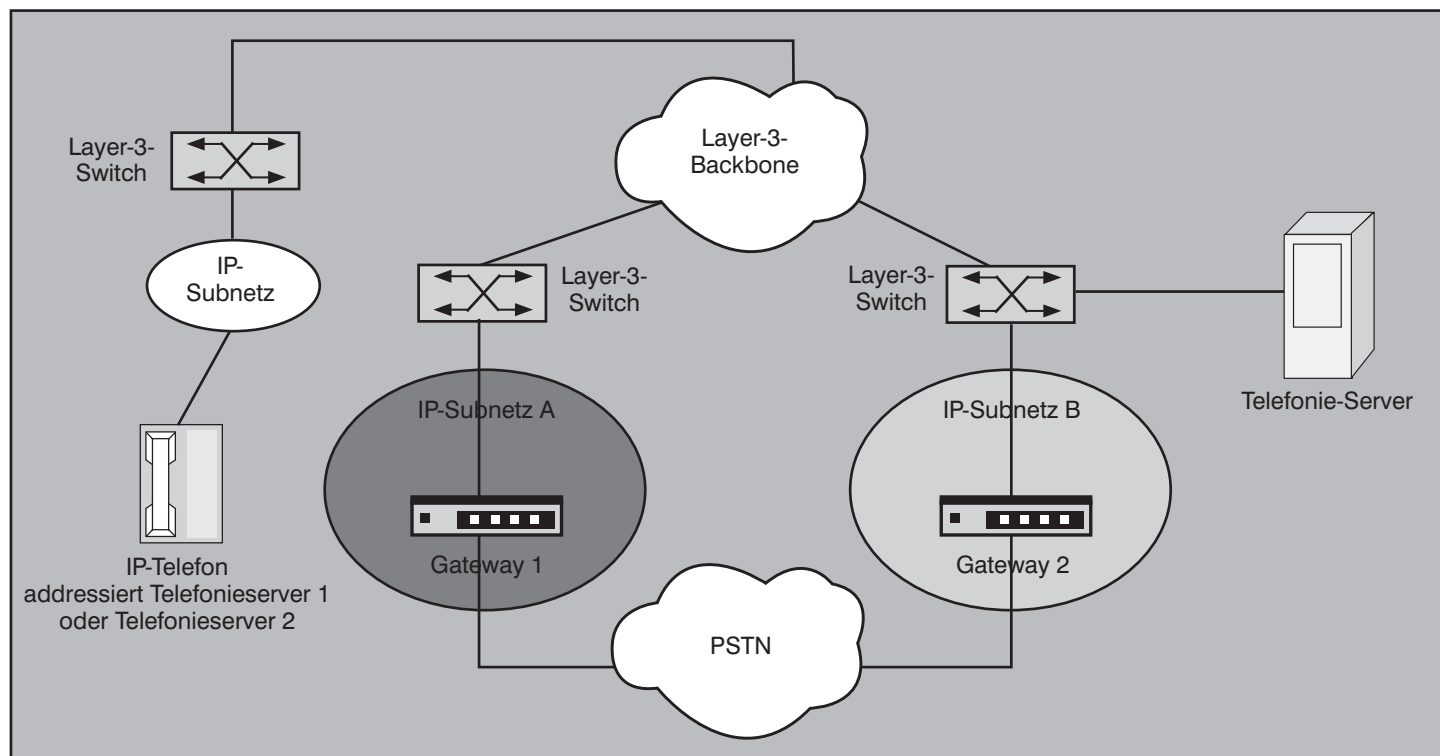


Abbildung 5: Gateway-Redundanz

Dienst adressieren. Dies wird in der Regel dadurch erreicht, dass sich die Endgeräte beim Verbindungsaufbau an den Telefonieserver wenden. Dieser teilt den Endgeräten die IP-Adresse des Gateways mit. Dabei wird die Erreichbarkeit der Gateways und die Verfügbarkeit der von ihnen angebotenen Dienste vom Telefonieserver durch permanente Überwachung überprüft. Fällt ein Gateway aus, wird dies vom Telefonieserver bemerkt, worauf hin er die Adresse des Gateways den Endgeräten auf Anfrage nicht mehr mitteilt. Verliert

ein Gateway den Anschluss an das Netz, das er mit dem IP-Netz verbindet, meldet er sich beim Telefonieserver ab. Auch dies wirkt sich so aus, dass die Adresse des Gateways nicht mehr vom Telefonieserver propagiert wird.

Wenn die VoIP-Umgebung eines Unternehmens wie dargestellt über zwei Gateways mit dem PSTN verbunden ist, werden in der Regel über das PSTN kommende Rufe vom Provider auf die beiden Gateways verteilt. Verliert der Gateway

die Verbindung zum IP-Netz, signalisiert er dieses Problem an den Switch im Providernetz, sodass vom PSTN kommende Rufe nicht mehr zum Gateway geroutet werden. Fällt der Gateway aus, bemerkt der Provider-Switch den Ausfall der Verbindung und adressiert den Gateway nicht mehr.

Es wird auf jeden Fall empfohlen, diese Mechanismen zu testen (siehe auch Kapitel 8).

Fax-Antwort an ComConsult 02408/955-399

Bestellung

Planung für Voice over IP

Ich bestelle den Report
Planung für Voice over IP
 (Preis € 398.-- zzgl. MwSt. und Versand)

Vorname _____


Nachname _____

Firma _____

Telefon/Fax _____

Straße _____

PLZ,Ort _____

 Bestellen Sie über unsere Web-Seite
www.comconsult-research.de

eMail _____

Unterschrift _____

Schwerpunktthema

Auswahl von Access-Switches in modernen Datennetzen

Fortsetzung von Seite 1



Dipl.-Ing. Hartmut Kell ist spezialisiert auf die Datenkommunikation in lokalen Netzen und kann auf eine mehr als 15-jährige Berufserfahrung in diesem Bereich verweisen. Als langjähriger Mitarbeiter der ComConsult Beratung und Planung GmbH hat er umfangreiche Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken gesammelt. Ergänzend zu diesen projektbezogenen Arbeiten vermittelt Herr Kell sein umfangreiches Fachwissen in Form von Fachpublikationen und Seminaren.



Dipl.-Ing. Harald Krause arbeitet seit der Firmengründung 1995 für die ComConsult Beratung und Planung GmbH. Er ist Senior-Consultant im Competence Center Netze und plant aktive und passive Netzwerkinfrastrukturen.

Modular oder nicht-modular

Eine der ältesten Kernanforderungen bei der Auswahl von Komponenten im Access-Bereich stellt die Frage nach einer modularen bzw. nicht-modularen Bauform dar. Bereits zu Hochzeiten der Hub-Technologie standen viele bei der Planung vor der Schwierigkeit, eine Entscheidung zwischen multifunktionalen, modularen Geräten und einfacheren, nicht-modularen Geräten zu treffen; dies hat sich im Prinzip bis heute nicht geändert.

Alle renommierten Hersteller bieten Switch-Systeme an, die weit über 200 Endgeräte an einem einzelnen Gehäuse anschließen können. Die Vorteile dieser hochkonzentrierten Geräte liegen im Wesentlichen darin, dass

- nur eine IP-Adresse für das SNMP-Management vorzusehen ist (das Netzwerk wird in Punkto Management überschaubarer);
- die Anzahl von Software-Updates auf den Koppellementen gering bleibt;
- einige Hochleistungsfunktionen (vor allem im Bereich der RMON-Überwa-

chung) nur hier vollständig zur Verfügung stehen;

- die eventuell notwendige Backbone-Anbindung eines derartigen High-Density-Switches (HD-Switch) über einen einzigen physikalischen Kanal (2 Fasern) bzw. 2 Kanäle bei Redundanz realisiert werden kann;
- die IP-Strukturierung der physikalischen Strukturierung entspricht, ohne dass Switch-übergreifende VLANs gebildet werden müssen.

Diesen Vorteilen stehen jedoch auch Nachteile gegenüber:

Der Switch stellt bei hoher Portanzahl einen extremen Single-Point-of-Failure dar. Fällt das Gerät aus, so sind zwangsläufig 200 LAN-Teilnehmer oder mehr, je nach Ausbaustufe, nicht mehr in der Lage, eine Datenkommunikation zu betreiben. Die Hersteller versuchen zwar, diesen Single-Point-of-Failure durch Verbesserung der Komponenten und Redundanz einzelner elementarer Bauteile (Management, Controller, Power-Supply, Backplane) zu beseitigen, was jedoch nichts daran ändert, dass der Ausfall eines derart komplexen Systems zu einer Kommunikationsunter-

brechung der gesamten angeschlossenen Clients führt. In einzelnen Projekten konnte bei dieser Betrachtung die Erfahrung gemacht werden, dass dem Netzwerk-Betreiber gar nicht klar wurde, wie hoch diese Ausfall-Gefahr tatsächlich ist. Durch Vereinbarung von Service-Verträgen mit vertraglich zugesicherten Austauschzeiten von weniger als 2 Stunden wog man sich in Sicherheit, vergaß aber vollkommen die Praxisnähe. Es ist denkbar naiv zu glauben, dass ein modulares Gerät wie z.B. ein Catalyst 4510 mit einer Maximalbestückung von ca. 400 Ports in einem derartigen Zeitintervall ausgetauscht werden kann. Insbesondere dann, wenn die typische Alltagsschludrigkeit zu einem Chaos in der Kabelrangierung führt und erst einmal x hundert Anschlussschnüre (am besten nicht beschriftet und nicht dokumentiert) „abgeklemmt“ werden müssen, artet solch ein Austausch in einem Super-GAU aus. Natürlich wird von einigen Herstellern hervorgehoben, dass die Chassis vollkommen passiv sind und nicht ausfallen können; doch was ist mit dem Fall einer geplanten Wartung des gesamten Systems, was ist bei Austausch eines einzelnen ausgefallenen Moduls, welches sich hinter einem undurchdringlichen „Vorhang“ von Anschlussschnüren befindet? (siehe Abbildung 1)

Auswahl von Access-Switches in modernen Datennetzen

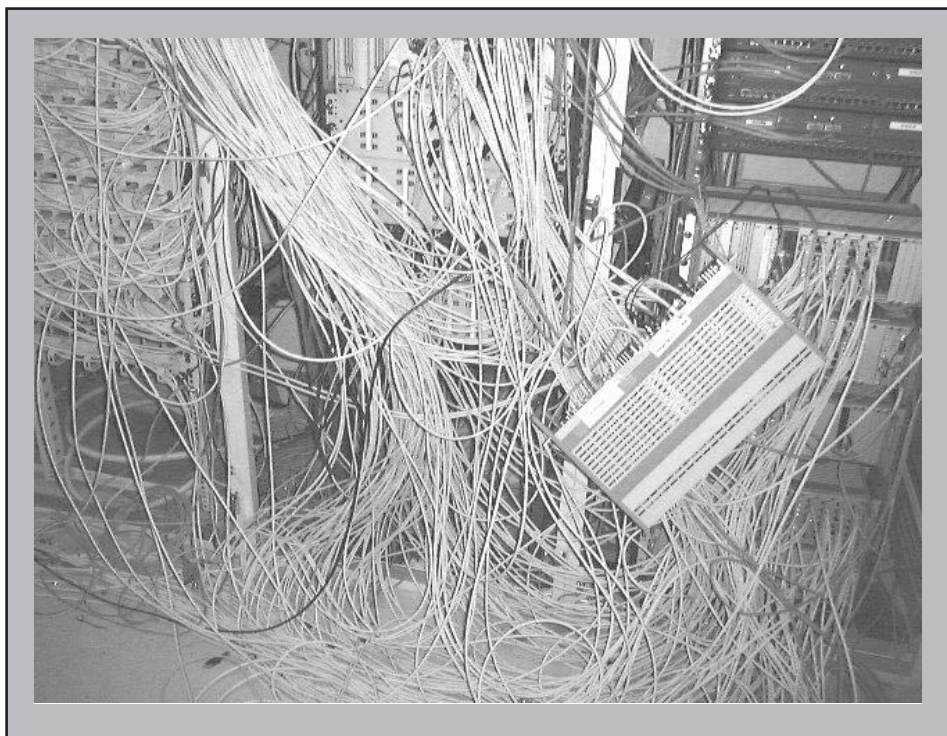


Abbildung 1: Typischer Zustand eines (alltäglichen) Verteilers

Der entscheidende Nachteil besteht aber darin, dass bei korrekter Planung eines hochkapazitiven, modularen Switches mit redundanten Netzteilen und redundanten Controller- oder Supervisory-Modulen dies in der Regel zu einer deutlichen Verteuerung des Gesamtsystems führt. Über 80 % aller Planungen, bei denen eine Kostengegenüberstellung zwischen den beiden Varianten durchgeführt wurde, führte zu einem klaren wirtschaftlichen Nachteil für die modularen Varianten (dazu siehe auch Artikel im Netzwerk-Insider August 2004).

Eine Alternative zu den großen Switch-Einheiten besteht darin, mehrere völlig autarke, kleinere, fest konfigurierte Desktop-Switches (maximal 96 Ports) zur Versorgung der Endgeräte vorzusehen. Als typischer Anwendungsbereich wird hierfür bekanntermaßen ein kleinerer Etagenverteiler angegeben. Jedoch auch in zentralen Verteilern, in denen mehrere hundert Endgeräte angeschlossen werden, können diese Desktop-Switches Vorteile bieten:

- Fällt einer der Switches aus, so sind lediglich 48 Endgeräte davon betroffen. Bei Nutzung einer mittleren Größe für diese Desktop-Switches sind sogar nur 24 Endgeräte involviert. Mit diesen Einheiten lassen sich durchaus Austauschzeiten von 30 Minuten realisieren. Dies setzt aber weiter voraus, dass ein „ordentliches Anfahren“ der einzelnen Einheiten mit den Rangierkabeln von der

Seite oder von unten über ein Rangierpanel vorgesehen wird.

- Nicht-modulare Komponenten sind wesentlich günstiger als modulare, z.T. redundant ausgelegte Einheiten. Alleine die Interface-Module der modularen Geräte sind deutlich teurer als ein vergleichbarer Desktop-Switch.
- Eine Aufrüstung der Datenrate und Port-Anzahl im Verteiler ist bei Stand-Alone-Systemen einfacher und kostengünstiger als bei modularen Systemen. Letztere müssen dafür zumindest hinsichtlich der Backplane vorbereitet sein.
- Nicht-modulare Komponenten erlauben eine sehr einfache Bildung von kleinen Arbeitsgruppen als eigenständige Netze. Bei einer Wahl von Systemen mit geringer Portdichte (typisch mit 12 Ports) kann gegebenenfalls auf eine Bildung von VLANs auf den Access-Switches verzichtet werden.
- Es lassen sich wesentlich gezielter neue Funktionalitäten über den Einbau von neuen Switches einführen. Typisches Beispiel ist die Power-over-Ethernet-Fähigkeit: Sukzessive können veraltete Switches ohne PoE durch komplett neue, modernere Systeme mit PoE ersetzt oder erweitert werden.
- Eine strikte Trennung der Netzwerk-

Hardware, wie sie z.B. bei Einführung von Netzen zur Gebäudeüberwachung in Zukunft denkbar sein werden, ist wesentlich einfacher durchzuführen.

Dagegen stehen jedoch auch Nachteile einer verteilten Lösung mit nicht-modularen Switches:

- Es ist nicht gesichert, dass die Hersteller für alle Komponenten eine vollständige RMON-Funktionalität über die ersten 4 RMON1-Gruppen (Mini-RMON) hinweg gewährleisten. Zu diesem Punkt könnte man in eine sehr ausschweifende Diskussion gelangen, ob überhaupt derartige Intelligenz im Access-Bereich gebraucht wird. Die Erfahrung zeigt, dass nur die wenigsten Netzwerk-Administratoren selbst die Minimalfunktionen im RMON-Bereich permanent nutzen.
- Zur Anbindung der Desktop-Switches sind mehrere physikalische Leitungskanäle (i. d. R. Glasfaserpaare) notwendig, bzw. die vorhandene Infrastruktur muss dafür vorbereitet sein. Dies lässt sich nur durch Bildung von Stacks umgehen, auf die später noch im Artikel eingegangen werden soll.
- Es ist von mehreren mit SNMP zu überwachenden Geräten auszugehen, und die Managementstruktur wird komplexer (Ausnahme: proprietäre Lösungen mit Stacking, bei denen eine über Management ansprechbare Basiseinheit definiert ist und die Erweiterungseinheiten über diese erreicht werden).
- Die Bandbreite innerhalb eines gestackten bzw. geclusterten Zusammenschlusses von mehreren Desktop-Switches ist auf das Switch-übergreifende Zugangsverfahren begrenzt und erreicht nicht die Qualität einer Backplane in einem modularen Switch. Da die Bildung dieser Cluster proprietär verläuft, können fremde Systeme nicht integriert werden, dies darf aber nicht als Nachteil im Vergleich zu modularen Systemen gesehen werden, da auch hier kein Modulaustausch zwischen fremden Systemen möglich ist.
- Die redundante Strom-Versorgung ist bei modularen Systemen einfacher (nicht unbedingt preiswerter), dazu später mehr.
- Firmware- und Software-Updates sind bei mehreren Einzelgeräten betriebstechnisch aufwendiger, was aber durch moderne Software-Verteilungsmechanismen kompensiert werden kann.

Auswahl von Access-Switches in modernen Datennetzen

- Zum Teil werden bestimmte und insbesondere innovative Funktionen der „großen“ modularen Switches für die nicht- modularen Komponenten mit einer zeitlichen Verzögerung von mehreren Monaten oder gar nicht angeboten.
- Es müssen bei Vermeidung von Stacks und von Switch-übergreifenden VLANs viele kleine IP-Subnetze am Verteilungs-Switch per hierarchischem Routing zusammengefasst werden.

Die Desktop-Switch-Lösung weist zwar quantitativ die meisten Nachteile auf, aber es ist zu hinterfragen,

- ob ein länger andauernder Netzausfall für hundert oder mehr Clients als Resultat der Störung einer großen modularen Komponente akzeptiert werden kann;
- ob die eingeschränkte Funktionalität im Access-Bereich wirklich von Relevanz ist;
- ob die durch Einsatz von autarken Geräten gewonnene Flexibilität diesen Mangel an Funktionalität nicht aufwiegt.

Wie bereits gesagt, wurden in den meisten Projekten nicht-modulare Systeme eingesetzt und dieser Trend zeichnet sich auch weiterhin ab.

Bereitgestellte Datenrate im Access-Bereich

Dem Ende der 90er Jahre aufgetretenen Ruf nach immer höheren Datenraten, auch im Access-Bereich, folgte im neuen Jahrzehnt eine zunehmende Besinnung auf die wirklich benötigte Performance. Dieser „Rückschritt“ konnte insbesondere auch durch die zunehmende Forderung nach WLAN nicht ausbleiben: Wie können im leitungsgelassenen Bereich Datenraten von bis zu 1 Gbit/s am Arbeitsplatz gefordert und gleichzeitig über eine Ablösung der Datenverkabelung durch Einsatz von WLAN mit maximal 54 Mbit/s (Brutto!) nachgedacht werden? Diese Unvereinbarkeit erkannten die meisten Planer und Netzwerk-Betreiber, aktuelle Umfragen im Rahmen der ComConsult-Seminare führen zum Ergebnis, dass nicht einmal 50 % der Teilnehmer einen flächendeckenden Bedarf nach 100 Mbit/s am Arbeitsplatz sehen. ComConsult Beratung und Planung sind keine Projekte bekannt, bei denen insbesondere die nicht ausreichende Datenrate am Endgerät Auslöser einer Netzwerk-Sanierung war (Annahme: Netz mit Switches). Als Beispiel sei ein Netz-

werk im Universitätsumfeld genannt, welches bis heute mit 10 Mbit/s für die meisten Netzwerkteilnehmer operiert und erst jetzt, im Zusammenhang mit wesentlichen Umbaumaßnahmen auch eine Erhöhung der Datenrate berücksichtigen wird. Dieser Ernüchterung bei den Anforderungen an hohe, aktuell und kurzfristig benötigte Datenraten steht natürlich die Frage gegenüber, ob es innerhalb des Nutzungszeitraumes der angeschafften Komponenten nicht dennoch zu einem Bedarf nach mehr als 100 Mbit/s kommen kann. Um diese Frage zu beantworten ist zunächst einmal der erwartete Nutzungszeitraum zu definieren. Wurde dieser

Wert in früheren Analysen aufgrund des erwarteten, kurzfristig anstehenden höheren Datenratenbedarfs bei ca. 3 bis maximal 5 Jahren gesehen, so orientiert sich heute der Nutzungszeitraum im Wesentlichen an sich verändernden Anforderungen bei den Funktionen. Dazu zwei Beispiele:

IEEE 802.1X: Die Bedrohung durch nicht-authentifizierte Netzwerk-Teilnehmer wird massiv erst seit Ende 2001 diskutiert und stellt auch heute noch einen Hauptteil der Planung von sicheren Netzen dar. Komponenten, die somit 2001/2002 geplant wurden, haben nicht zwangsläufig alle dieses

| Kostenvergleich 10/100/1000er-Switch (keine modulare Einheiten) | | | | | | | |
|---|---------------|-------------------|-------|-------------|-----------|-------------|-----------|
| Hersteller | Systemfamilie | Anzahl Ports | L2/L3 | mit PoE | | ohne PoE | |
| | | | | Systempreis | Portpreis | Systempreis | Portpreis |
| Hersteller 1 | 1 | 24 x 10/100* | L2 | 3.040 € | 127 € | 2.400 € | 100 € |
| | 1 | 24 x 10/100* | L2 | 5.200 € | 108 € | 4.000 € | 83 € |
| | 2 | 24 x 10/100* | L2 | 4.630 € | 193 € | 3.990 € | 166 € |
| | 2 | 48 x 10/100* | L2 | 6.790 € | 141 € | 5.590 € | 116 € |
| | 3 | 24 x 10/100/1000* | L3 | 6.240 € | 260 € | 5.600 € | 233 € |
| | 3 | 48 x 10/100/1000* | L3 | 12.400 € | 258 € | 11.200 € | 233 € |
| Hersteller 2 | 4 | 24 x 10/100* | L2 | | | 1.305 € | 54 € |
| | 1 | 12 x 100/1000* | L3 | | | 3.316 € | 276 € |
| | 1 | 24 x 10/100/1000* | L3 | | | 4.146 € | 173 € |
| | 2 | 24 x 10/100* | L2 | 2.071 € | 173 € | 1.324 € | 55 € |
| | 3 | 24 x 10/100* | L2 | | | 98 € | 4 € |
| Hersteller 3 | 4 | 48 x 10/100* | L2 | 2.523 € | 53 € | | |
| | 1 | 24 x 10/100* | L3 | | | 1.391 € | 58 € |
| Hersteller 4 | 2 | 22 x 10/100/1000* | L2 | | | 2.391 € | 109 € |
| | 1 | 24 x 10/100* | L2 | | | 161 € | 7 € |
| | 2 | 16 x 10/100* | L2 | | | 238 € | 15 € |
| | 3 | 24 x 10/100* | L3 | | | 820 € | 34 € |
| Hersteller 5 | 4 | 24 x 10/100/1000* | L3 | | | 1.394 € | 58 € |
| | 1 | 24 x 10/100* | L2 | | | 375 € | 16 € |
| | 2 | 24 x 10/100/1000* | L2 | | | 930 € | 39 € |
| | 3 | 24 x 10/100* | L2 | 1.385 € | 58 € | | |
| | 4 | 20 x 10/100/1000* | L2 | 2.636 € | 132 € | | |

* ohne GBIC oder SFP
Systeme des Herstellers mit nicht vergleichbaren Funktionen werden durch unterschiedliche Zahlen gekennzeichnet

Tabelle 1: relativer Kostenunterschied zwischen 10/100- und 10/100/1000er-Switches

Auswahl von Access-Switches in modernen Datennetzen

Feature und eine nachträgliche Forderung nach Erhöhung der Sicherheit muss zu einem Austausch dieser Switches nach ca. 4 bis 5 Jahren führen (weitere Details zu 802.1X im letzten Teil des Artikels).

PoE nach IEEE 802.3af: Der diesbezügliche Standard wurde erst Mitte 2003 verabschiedet, auch hier würde bei hinzugekommener Anforderung nach dieser Funktionalität ein Austausch der älteren Switches nach ca. 3 Jahren notwendig werden.

Beide Fälle machen deutlich, dass der Anspruch, Systeme auszuwählen, die garantiert alle Funktionalitäten in einem Zeitraum von 3 bis 5 Jahre bereitstellen, nicht erfüllt werden kann. Dieses Wissen hilft bei einer vorausschauenden Planung bezüglich des Bedarfs nach hohen Datenraten: Wer nicht der Überzeugung ist, dass in den nächsten 3 bis 5 Jahren eine sehr hohe Übertragungsrate, wohlgemerkt eine flächendeckend hohe Übertragungsrate benötigt wird, kann Mehrkosten durch Beschaffung von Switches mit 1000BaseT vermeiden. Insbesondere der Einsatz von preisgünstigen nicht-modularen Systemen erlaubt eine sanfte Aufrüstung des Netzes bei Bedarf nach ersten Anschlüssen mit 1000 Mbit/s. Doch wie sehen die Mehrkosten zum aktuellen Zeitpunkt aus? Dazu Tabelle 1 mit dem relativen Preisunterschied vergleichbarer Systeme verschiedener Hersteller.

Kann dieser Argumentationskette zugestimmt werden, so erübrigt sich die Frage nach Access-Switches mit einer Endgerätedatenrate von 10 Gbit/s, Switches mit diesen Datenraten auf Basis von Kupfer werden – sofern sich die Historie der letzten 15 Jahre wiederholt - mindestens in den nächsten 10 Jahren nicht im Access-Bereich zu sehen sein.

Deshalb ist es nicht verwunderlich, dass aktuelle Planungen von neuen Netzen mit einem realistisch eingeschätzten Nutzungszeitraum weiterhin auf Basis von Komponenten mit maximal 100 Mbit/s pro Endgeräteport durchgeführt werden.

Im Uplink-Bereich stellt sich glücklicherweise diese Problematik nicht, denn dank der Modularität von SFP- und GBIC-Technik lässt sich die Datenrate den aktuellen Bedürfnissen anpassen. Festzustellen ist, dass durch die Verdrängung der GBIC-Technologie mit den breiteren SC-Connectoren durch die SFP-Technologie mit dem wesentlich kleineren LC-Connector auch bei 1 Höheneinheit flachen Access-Switches automatisch mehr Platz vorhanden ist und die Hersteller in der Zwi-

schenzeit bei neuen Systemen auf 4 statt 2 Uplink-Ports umsteigen. Da bei einem Einsatz von Switches z.B. mit 24 Ports 1000BaseT und einer 10-fachen Überbuchung bereits 2,4 Gbit/s im Uplink notwendig wären, wird klar, dass selbst ein Trunk mit 2 x 1 Gbit/s nicht ausreichend ist. Demzufolge ist insbesondere bei Switches mit Gbit-Endgeräteanschlüssen die Anzahl von 4 x 10Gbit/s-Uplinks sehr sinnvoll (unabhängig von der oben diskutierten Frage wann 1000 Mbit/s am Arbeitsplatz notwendig sein wird).

Stacking-Funktionalität

Bereits seit den Anfangszeiten der Switching-Technologie gibt es die Möglichkeit, mehrere kleinere Systeme (Standardportanzahl 12, 24 oder 48 Ports) in einem Verteiler ohne zusätzliches Gehäuse zusammenzuschalten. Dieses Zusammenschalten bedeutete nicht das übliche Kaskadieren (Hintereinanderschalten) von mehreren Switches mit Hilfe von einfachen Verbindungskabeln und eines Standardzugangsverfahrens wie z.B. 1000BaseSX, sondern das Zusammenfassen von mehreren, grundsätzlich vollkommen autarken Einheiten zu einem Gebilde mit einer zentralen Intelligenz. Der geläufigste Name für diese Verschaltung ist Stack oder Cluster. Da im Laufe der Zeit bei einigen Herstellern das einzelne, stapelbare Gerät auch als Stack bezeichnet wurde ist dieser Begriff nicht ganz eindeutig, im Artikel wird deshalb für den ganzen Sta-

pel der Begriff „Cluster“ bevorzugt. Unbeachtet der geringfügigen Unterschiede bei den verschiedenen Herstellern ist das Grundprinzip in der Regel gleich. Mit Hilfe von Spezialkabel und speziellen Ports werden die Geräte in der Regel als Stern (z.B. bei der Ursprungsvariante von 3Com) oder als Kette (Daisy-Chaining) miteinander verschaltet, eine Kette kann als Loop geschlossen werden und steigert damit die Ausfallsicherheit des Clusters. Die speziellen Stacking-Ports verhindern ein Mischen von verschiedenen Herstellern oder auch verschiedener Systeme des gleichen Herstellers innerhalb eines Clusters. Insbesondere im Falle von Switches mit verschiedenen Funktionen, z.B. mit oder ohne Power over Ethernet, ist das System-Portfolio des Herstellers genau zu untersuchen, welches innerhalb eines Clusters gemischt eingesetzt werden soll. Zu beachten ist, dass die Anschlussports für diese Spezialkabel sich meistens auf der Rückseite des Gerätes befinden, und damit insbesondere in Verteilerschränken, bei denen der hintere Zugang erschwert ist, Änderungen an der Cluster-Verkabelung sehr unhandlich sind. Die Spezialkabel gibt es nicht in beliebigen Längen, meist werden Typen mit maximal 3 bis 5 Meter Länge angeboten, dies erschwert die Bildung von Clustern über mehrere Schränke hinweg. (siehe Abbildung 2)

Eine Einheit wird als Zentraleinheit definiert (stack commander, Basis-, Mas-

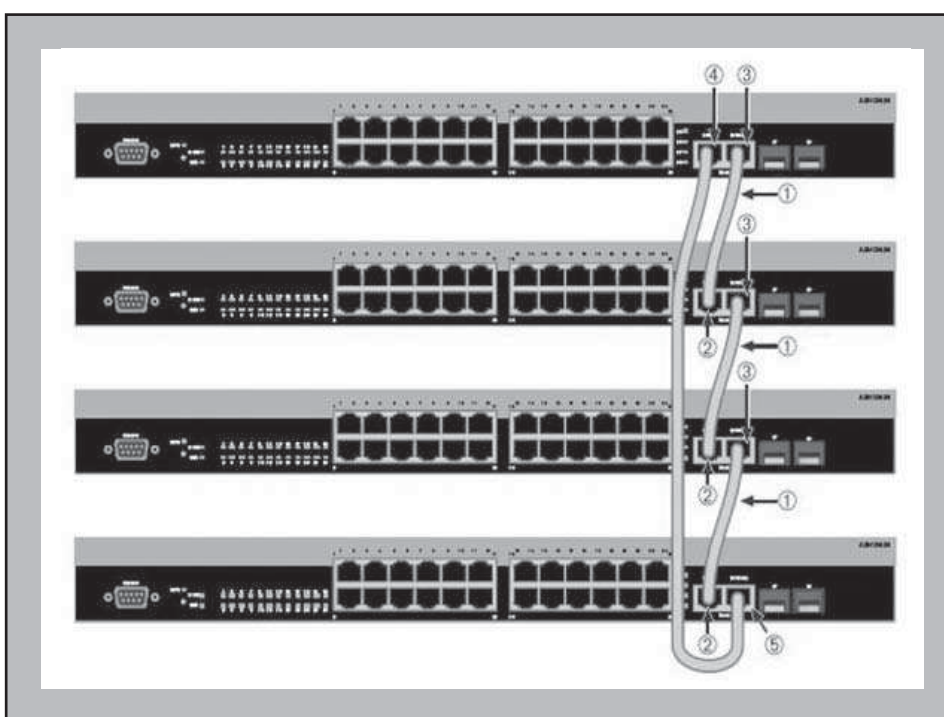


Abbildung 2: Beispiel für Ring-Schaltung in einem Stack/Cluster (Enterasys)

Auswahl von Access-Switches in modernen Datennetzen

ter- oder Managereinheit) und übernimmt die SNMP-Konfigurierbarkeit und Überwachung des kompletten Clusters. An die Basiseinheit werden die anderen Einheiten (Erweiterungseinheiten) angeschlossen. Der Cluster erscheint bei der Management-Überwachung als eine Einheit, zum Teil erfolgt durch die Definition des Masters eine automatische Deaktivierung der Consolen-Ports der untergeordneten Einheiten. Bei vielen Herstellern wird der Cluster über eine einzige IP-Adresse angesprochen. Neben der Möglichkeit, die Mastereinheit gezielt vorzugeben (z.B. bei HP ProCurve Stack Management) gibt es aber auch Systeme (z.B. Cisco Catalyst 3750), bei denen nur der Einschaltvorgang der Stromversorgung der einzelnen Geräte darüber entscheidet, wer Master wird und wer nicht. Viele Hersteller bieten auch die Möglichkeit, den Master redundant auszulegen, um im Falle seines Ausfalls den Cluster nicht kommunikationsunfähig werden zu lassen (Achtung: der stack commander bei HP kann z.B. nicht redundant ausgelegt werden). Interessant wird die Frage nach dem redundanten Anschluss eines Clusters an die übergeordnete Switch-Komponente, z.B. dem oder den Distribution-Switches. Zum Vergleich: Modulare Geräte lassen unter Einsatz von entsprechenden Redundanzmechanismen wie z.B. Spanning Tree, Rapid Spanning Tree, HSRP/VRRP oder auch proprietären Lösungen eine Zweifach-Anbindung zu. Da ein Cluster sich wie ein einziges Gerät verhalten soll, wäre es denkbar, dass auch der Cluster zweifach angeschlossen werden kann. Im Optimalfall wird man die beiden Uplinks an dem obersten und untersten Switch des Clusters anschließen. Doch wie verhält sich der Cluster in dem Fall, wo z.B. einer der mittleren Switches ausfällt, oder was passiert, wenn nur das Uplink-GBIC ausfällt, der Switch selber aber intakt bleibt? Erstaunlicherweise sind die diesbezüglichen Informationen der Hersteller zum Teil sehr spärlich, und ComConsult-Erfahrungen wie auch Erfahrungen von Kunden bestätigen, dass diese Problematik nicht trivial ist. Unsere Empfehlung geht da hin, dass man bei Nutzung einer derartigen, durchaus nützlichen Funktion ausführlichste Tests im Vorfeld bereits bei der Produktauswahl planen sollte.

Insbesondere bei einzelnen Features ist Vorsicht walten zu lassen: Sind die Features bei den einzelnen Geräten verfügbar, so besteht die Gefahr, dass dies im Cluster und insbesondere in einem Cluster mit verschiedenen Geräten nicht mehr genutzt werden können. Dazu Beispiele für den Hersteller Nortel: In einem Cluster ohne das Gerät BayStack 450 lassen sich

nach Aussage von konkurrierenden Herstellern bis zu 256 VLANs und 8 Spanning Tree-Instanzen einrichten; befindet sich dieses Gerät im Cluster, reduziert sich die Leistungsfähigkeit auf 64 VLANs und eine Spanning Tree-Instanz. Auch MAC-basierende VLANs sind dann nicht mehr möglich.

Der übliche Cluster beschränkt sich auf einen einzigen Verteiler bzw. einer Gruppe lokal zusammengehörender Switches, mit dem „expandable Resilient Networking“ XRN von 3Com gibt es jedoch auch eine Variante, die den Cluster über mehrere, räumlich getrennte Verteiler hinweg abbilden kann. Damit geht dieser Ansatz über eine reine Lösung für Stacking-Technologien hinaus und er wird als Alternative zu klassischen Core-Lösungen gesehen. XNR setzt ganz konkrete neuere Produkte des Herstellers voraus und führt zu einer Einschränkung der Funktionalität wie z.B. VLAN-Anzahl oder ARP-Table-Größe im Vergleich zu den anderen Stack-Lösungen. Noch problematischer ist dagegen der Ansatz, dass man mit der Ausdehnung des Clusters über ein proprietäres Verfahren eine Herstellerbindung einführt, die kritisch zu bewerten ist. Kann man im Betrieb eines Netzes noch sehr gut damit leben, dass innerhalb eines Clusters im Verteilerschrank keine Freiheit existiert, die dort eingesetzten Switches durch Fremd-

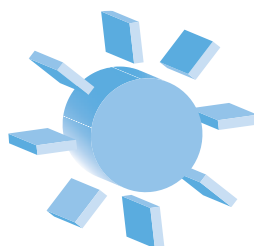
produkte (fremder Hersteller oder des gleichen Herstellers) auszutauschen, so ist diese Einschränkung innerhalb eines ganzen LANs nicht zu akzeptieren. Insbesondere der oben bereits beschriebene Weg einer sanften Migration durch sukzessiven Austausch von Switches z.B. nach 3 bis 5 Jahren würde sehr erschwert.

Die maximal mögliche Bandbreite innerhalb des Clusters unterscheidet sich sehr stark zwischen den Herstellern und auch innerhalb der Produkte eines Herstellers, beispielsweise bietet das System GigaStack von Cisco eine maximale Bandbreite von 1 Gbit/s full duplex, das System StackWise dagegen erreicht 32 Gbit/s.

Neben der zentralen Administration bietet ein Cluster einen weiteren Pluspunkt im Vergleich zu der Einzelanbindung der Switches an die übergeordnete Instanz, es wird eine erhebliche Menge an Glasfasern und Gigabit-Ports eingespart. Ein Verteiler mit 8 Access-Switches würde zur redundanten Anbindung 32 Fasern benötigen, bei einem 8-fach-Cluster reduziert sich dies auf 4 Fasern. Beide Varianten sind jedoch in einem weiteren entscheidenden Punkt nicht gleichwertig: ein einziger Uplink für 8 Switches wird mit einer wesentlich höheren Überbuchung betrieben als die 8 Uplinks der einzelnen Switches.

Sommerschule 2006

19.06. - 23.06.06
in Aachen



Auch in diesem Jahr bietet die Sommerschule wieder den Intensiv-Update auf den neuesten Stand der Netzwerk-Technik, zeigt neue Nutzungs-Potenziale, diskutiert Änderungen im Design, analysiert aktuelle Produktrends. Damit wendet sich die Sommerschule speziell an erfahrene Teilnehmer/Innen, die den Betrieb ihrer bestehenden Netzwerke weiter optimieren und neue Entwicklungen und Technologien kennen lernen wollen.

Die Sommerschule 2006 bietet folgende Schwerpunkte:

Der Cisco-Design-Guide in der Analyse; Mobile Kommunikation; Privacy und Sicherheit bei der mobilen Kommunikation; Bluetooth-Sicherheit in der Praxis; Netzwerk-Design 2006; Das Session-Initiation Protokoll SIP in der Analyse; Auswahl neuer Switch-Systeme für den Workgroup-Bereich; Videoüberwachung über IP; Einsatz von Netzwerk-basierten IPS; Wireless-Networks; Sicherheit in der IP-Telefonie; Identity und Access-Management an einem Projektbeispiel; Von 802.1X zur Anmeldung von Benutzern und Trennung von Benutzergruppen; Quality of Service in Netzwerken professionell nutzen

Moderation: Markus Schaub

Preis: € 2.290,- zzgl. MwSt.



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

Auswahl von Access-Switches in modernen Datennetzen

Power over Ethernet

Eine der ersten Fragen, die sich bei der Entscheidung für ein Access-Switch-System stellt, bezieht sich auf den zu erwartenden Zeitpunkt der Bereitstellung von Power over Ethernet. Grundsätzlich bieten fast alle Hersteller innerhalb einer Systemfamilie Geräte mit und ohne PoE an und es ist zu erwarten, dass in naher Zukunft diese Funktion genauso grundsätzlich dazu gehört wie beispielsweise eine automatische Erkennung der Datenrate. Der Stand heute ist jedoch, dass nicht-modulare Access-Switches im Durchschnitt 10 bis 20 € pro Port teurer sind. Gibt es sinnvolle Alternativen zu PoE-Switches? Bekannt sind so genannte Midspan-Geräte, die zwischen Switch (ohne PoE) und dem Endgerät geschaltet werden; diese Lösung führt in der Regel zu keiner unmittelbaren Kostenersparnis, denn der Unterschied zwischen Endspan-Switches und „normalen“ Switches mit zusätzlichem Midspan ist nicht sehr groß. Im Gegen-

teil: Durch weiteren, zusätzlichen Platz, der für die Midspan-Geräte benötigt wird, erhöht sich der Bedarf an Schrankkapazität, was im Extremfall zu größeren Technikräumen führt, und dieser Platz ist entweder gar nicht verfügbar oder sehr teuer. (siehe Abbildung 3)

Ein weiterer Nachteil besteht darin, dass derzeit Midspan-Technik nur für eine 8-adrige Verkabelung und für 10/100-Mbit/s normiert ist (eine Erweiterung ist in der überarbeiteten Version der IEEE 802.3af vorgesehen). Man könnte die Frage stellen, wer in den nächsten 3-5 Jahren für seine Endgeräte (Powered Devices) PoE mit 1000 Mbit/s benötigt? Es gibt zwar kaum Endgeräte, die 1.000 Mbit/s und PoE benötigen, was aber ist z.B. mit Planungen, die aufgrund von zu geringer Anzahl von Anschlussdosen VoIP-Telefone mit integriertem Switch einsetzen müssen? Die Möglichkeit, dass sich „hinter“ dem Telefon Endgeräte mit einem Bedarf nach 1.000 Mbit/s befinden, kann in vie-

len Fällen nicht ausgeschlossen werden und dann wäre PoE in Kombination mit 1000BaseT von großem Nutzen. Auf den ersten Eindruck scheint es so, als würde Midspan-Technik nur mit Nachteilen verbunden sein; schauen wir uns daher die Argumente gegen Endspan-Switches näher an.

Es beginnt bereits damit, dass PoE-Switches in den meisten Fällen schwerer und größer sind. Das Gewicht mag keine Rolle spielen, die Größe jedoch aus der eigenen Erfahrung schon. In einem konkreten Projekt wurden sowohl Wandverteilerschränke und Standard-Access aufeinander abgestimmt und ausgeschrieben. Nach der Installation der Schränke entschied man sich für modernere PoE-Switches der gleichen Systemfamilie und war der Meinung, dass bei gleicher Höhe diese 1:1 in den Schränken eingebaut werden könnten. Irrtum: die PoE-Switches waren fast 10 cm tiefer und jeder, der die Platzverhältnisse in einem Wandverteilerschrank kennt, weiß, welche Probleme das mit sich bringen kann. Weiterhelfen konnte im betrachteten Fall der Austausch der Stromkabel: statt der üblichen Kabel mit einem gerade abgehenden Kaltgerätestecker wurde eine gewinkelte Version verwendet.

Ein nächster, häufig vertretender Kritikpunkt an Endspan-Geräten besteht darin, dass die erhöhte Wärmewirkung in diesen Switches zu einer Verringerung der MTBF (Mean Time Between Failure) führt und deshalb Stromversorgung der Endgeräte und Switching-Technologie entkoppelt werden sollten (Hinweis auf den Netzwerk-Insider Mai 2006, der die Bedeutung der unterschiedlichen MTBF-Werte erläutert). Anhand der nachfolgenden Produktbeispiele lässt sich dieser Unterschied, der Unterschied zwischen verschiedenen Herstellern und auch der Einfluss der komplexeren Elektronik bei 1000 Mbit/s sehr gut veranschaulichen:

- Der Catalyst 3750-24TS (10/100 Mbit/s ohne PoE) kommt auf eine MTBF von ca. 294.000 h, das entsprechende gleichwertige System mit PoE Catalyst 3750-24PS dagegen nur auf 210.000 h.
- Der Catalyst 3750G-24T (10/100/1000 Mbit/s ohne PoE) kommt auf eine MTBF von ca. 210.000 h, der 3750G-24PS (10/100/1000 Mbit/s mit PoE) hat 182.000 h.
- Der Enterasys C2G124-24 (10/100/1000 Mbit/s ohne PoE) kommt auf eine MTBF von ca. 195.000 h, der C2G134-24P (10/100/1000 Mbit/s mit PoE) dagegen nur auf ca. 145.000 h.

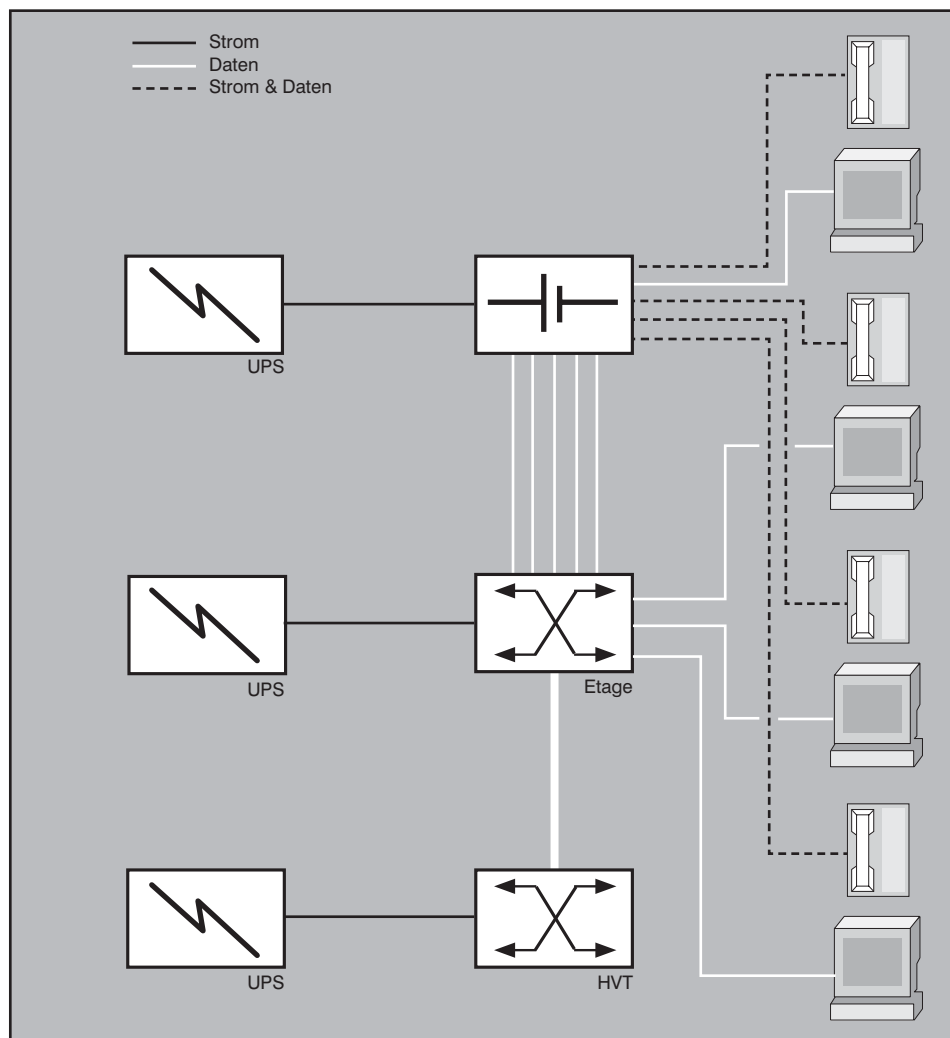


Abbildung 3: Lösungsansatz Midspan-Technik (Quelle: Markus Schaub, ComConsult Reserach)

Auswahl von Access-Switches in modernen Datennetzen

- Der Netgear GSM7224 mit 24 Ports 10/100/1000 Mbit/s und PoE kommt sogar nur auf 58.000 h, der Layer-3-Switch mit 24 Ports 10/100 Mbit/s ohne PoE hat 117.000 h.

Die Lebensdauer zwischen Switches mit/ ohne PoE unterscheidet sich im Durchschnitt um 30 %, auch der Einsatz von Switches mit 10/100/1000 Mbit/s reduziert die MTBF in einer ähnlichen Größenordnung. Unter dem Aspekt der MTBF wäre also eine sehr ungünstige Konstellation ein Switch mit PoE und 10/100/1000 Mbit/s. Wie lassen sich solche MTBF-Zeiten in eine anschauliche Größenordnung bringen, denn 117.000 h entsprechen ungefähr 13 Jahren, und wer wird einen Switch schon 13 Jahre nutzen. Dazu ein weiteres Beispiel: Der einigen wohl noch bekannte Sternkoppler ASGE der Firma Hirschmann ist ein System, was Ende der 80er bis Anfang der 90er Jahre sehr weit verbreitet war und zum Teil heute noch im Einsatz ist. Diesem sehr robusten Gerät kann man eine Nutzungszeit von 10 bis 15 Jahren attestieren. Die vom Hersteller im Datenblatt angegebene MTBF beträgt je nach Ausführung weit über 1.000.000 h!

Ein weiterer Vergleich: Über die folgende Formel lässt sich die statistisch zu erwartende Anzahl der fehlerhaften Systeme pro Nutzungszeitraum ausrechnen:

$$\text{Fehlerrate} = \frac{\text{Systemanzahl} \times \text{Betriebsstunden}}{\text{MTBF}}$$

Wieder der Vergleich zwischen einem hochwertigen Switch und einem Low-Cost-Produkt:

- Bei Betrachtung einer Betriebsdauer von 1 Jahr kommt es bei 100 eingesetzten Catalyst 3750G-24P statistisch gesehen zu 4 fehlerhaften Systemen.
- Bei der gleichen Menge und dem gleichen Zeitraum müsste man beim Netgear GSM7224 mit 14 fehlerhaften Systemen rechnen.

Es gibt bei Vertretern der Midspan-Idee Lösungsansätze, welche den Einbau von Midspan-Geräten unmittelbar im Bereich der Rangierfelder (also weg aus dem „aktiven Schrank“) vorsehen; die Midspan-Geräte werden also zu einem Bestandteil der „passiven“ Infrastruktur. Die Wärme entwickelnden Netzteile würden dabei aus den aktiven Schränken ausgegliedert und die MTBF der Switches erhöht sich. Die Stromversorgung wird Gegenstand einer sich eher langsam verändernden Umgebung (der Verkabelung) und dies ermöglicht eine einfachere Anpassung von spe-

ziellen Switch-Funktionalitäten, die nicht unbedingt mit PoE-Switches angeboten werden. Ein Vertreter dieser Idee ist beispielsweise der aus der Verkabelung bekannte Hersteller Panduit. Es werden Patchpanels (Stand heute: nur Kategorie 5e) mit integriertem PoE angeboten, die statt der herkömmlichen passiven Patchpanels eingebaut werden und die Datenanschlüsse zu den Arbeitsplätzen aufnehmen; ein größerer Platzbedarf wäre demnach nicht notwendig. Die Beurteilung dieser Technik unter Betrachtung der Forderung nach einer neutralen und hochqualitativen Verkabelung soll an dieser Stelle nicht weiter erfolgen. Midspan erlaubt eine wesentliche sanftere Einführung von PoE, da gezielt der Bedarf nach PoE sukzessive durch den Betreiber befriedigt werden kann; eine sofortige Anschaffung von Endspan-Switches wäre nicht notwendig. Bei einer Entscheidung zu Endspan-Switches darf man sich ohnehin nicht von der Anzahl der physikalischen Ports in die Irre führen lassen, in vielen Fällen unterstützen die Systeme bei einer Bereitstellung der maximalen Leistungsklasse (15,4 Watt) nur ca. 50% der Ports! Beispiel: Der Cisco Catalyst 3750-48 PS besitzt 48 Endgeräteports, kann aber nur 24 mit maximaler PoE-Leistung versehen. Wird sogar ein redundantes Netzteil benötigt, so sollte man sehr genau die Systemeinschränkungen der Hersteller lesen, insbesondere beim Aufbau eines hoch verfügbaren Stacks mit redundanter Stromversorgung ist gewissenhaft zu prüfen, wie sich der Stack im Falle eines Netzteilausfalls verhält.

In diesem Zusammenhang sei darauf hingewiesen, dass bei vielen Herstellern die Auslagerung der redundanten Netzteile zu einer „Scheinredundanz“ führt. Es lassen sich häufig zwar alle Switches in einem Verteilerschrank an diese externe Einheit anschließen, aber es kann nur der Ausfall eines einzigen Netzteiltes eines einzigen Switches abgefangen werden. Fällt beispielsweise der gesamte Stromkreis der angeschlossenen Switches aus, so versorgt die üblicherweise am zweiten Stromkreis angeschlossene redundante Einheit nur einen einzigen Switch weiter mit Ersatzstrom (in der Regel ein Gleichstrom)!

Was ist von Access-Switches mit höherer Ausgangsleistung zu halten, die Norm beabsichtigt eine Erhöhung von 15 Watt auf 30 Watt pro Port? Bei dieser Erweiterung stellt sich aus Sicht der Autoren erst recht die Frage, wer diese Funktion innerhalb des kurzfristig anstehenden Nutzungszeitraumes braucht; in Einzelfällen ist dies denkbar, wird man aber deshalb alle Switches damit ausstatten? Hat jemand über die Kon-

sequenzen im Zusammenhang mit der notwendigen Infrastruktur oder Steckerqualität nachgedacht? Fakt ist, dass bereits heute viele gegebene Technikrauminfrastrukturen mit der Zuführung einer ausreichenden 230-Volt-Stromzuführungen und Abführung der Wärme Probleme haben. Die Aufrüstung der Stromversorgung ist in der Regel dabei das kleinere Problem, aber die Abführung der Wärme bereitet erfahrungsgemäß sehr große Schwierigkeiten. Dazu folgende Ausführung: Die Hersteller von Switches geben vielfach in ihren Datenblättern eine so genannte BTU/h (British Thermal Unit = Energieeinheit über Zeitraum von 1 Stunde) an, aus der sich über die Formel $1 \text{ Watt} = 1 \text{ BTU} \cdot 1055 / 3600$ die abzuführende Wärmeleistung ausrechnen lässt. 1000 BTU/h entsprechen demzufolge einer Wärmeleistung von 293 Watt (Achtung, nicht gleich elektrischer Leistung in Watt). Dazu ein paar Vergleichswerte:

- Eine nichtmodulare Midspan-Einheit mit 24 Ports kommt auf ca. 40 Watt Wärmeleistung
(Produktbeispiel PH24/NN)
- Eine nichtmodulare Midspan-Einheit mit 48 Ports kommt auf ca. 80 Watt Wärmeleistung
(Produktbeispiel Systemax)
- Eine nichtmodulare Endspan-Einheit mit 24 Ports kommt auf 120 Watt Wärmeleistung, die Stromaufnahmeleistung liegt bei ca. 500 Watt
(Produktbeispiel Catalyst 3750-24PS)

Die dazugehörigen BTU-Werte wurden bei Switches der aktuellen PoE-Spezifikation (maximal 15 Watt pro Port) ermittelt, eine Erhöhung der Wärmeleistung bei den geplanten 30 Watt könnte in einem Technikraum mit „nur“ 240 Ports theoretisch zu 6,4 kW Wärmeleistung führen (bei Midspan Schätzung: 1,4 kW).

Kommt man im Laufe der Planung zum Ergebnis, dass nicht jeder Datenport PoE erfordert, so stellt Midspan unter Berücksichtigung aller Nachteile eine durchaus überlegenswerte Alternative zu Endspan-Switches dar. In diesem Fall sollte man sich jedoch Gedanken zur Kennzeichnung des Dienstes PoE am Arbeitsplatz machen; Dosensysteme mit austauschbaren Kennzeichnungen z.B. Farbmarkierungen wären von Vorteil.

Portanzahl

Die Möglichkeit zum Durchschleifen von Ports bei Einsatz von VoIP-Telefonen führt zu einer Planungsunsicherheit bei der Be-

Auswahl von Access-Switches in modernen Datennetzen

stimmung der Portanzahl und setzt sich insbesondere bei der Frage der erörterten notwendigen Anzahl und Art von PoE-Ports fort. Basiert die Planung der Access-Switches auf der Annahme eines Einsatzes von VoIP-Telefonen mit integrierem Switch, so besteht bei einer zeitversetzten Einführung von VoIP die Gefahr, dass man gezwungen ist, genau solche Telefone einzusetzen und gegebenenfalls Telefone mit besseren Funktionen, aber ohne zweiten Anschluss nicht in die enge Wahl nehmen kann. Ebenfalls schränkt man sich bei der Netzwerkgestaltung ein; viele Kunden gehen dazu über, aus organisatorischen Gründen ein eigenständiges Netz mit eigenständiger Hardware für die Sprache einzurichten (Verzicht auf VLANs), auch dieses wäre bei nicht ausreichender Portanzahl ohne Nachrüstung nicht möglich. Es stehen also folgende Varianten zur Verfügung:

- Variante 1: Orientierung am aktuellen Anforderungsminimum
- Variante 2: Orientierung an den höchsten zu erwartenden Anforderungen und Portmengen

Aus Sicht der Autoren ist Variante 2, insbesondere angesichts der Kosten einer zu hohen Portmenge, in vielen Fällen zu verneinen. Warum: Zum einen versperrt man sich die Möglichkeit, zukünftige, möglicherweise für VoIP besonders nützliche Features einsetzen zu können (falls diese nicht über Upgrades bereitgestellt werden können), zum Anderen investiert man in Hardware, die zum späteren Einsatzzeitpunkt veraltet ist. Es ist erstaunlich, wie schwer sich Netzwerkplaner mit der Idee tun, gerade im Access-Bereich in kurzen Nutzungszeiträumen zu denken und durch Einsatz von einsatzoptimierten Komponenten das Netzwerk wirtschaftlich zu optimieren.

In diesem Zusammenhang soll ein kaum bekannter, durchaus prüfenswerter Lösungsansatz vorgestellt werden. Dieser sieht die kabeltechnische Aufschaltung aller am Arbeitsplatz bzw. in den Büros möglichen Datenanschlüsse, also aller Dosen vor. Scheint dies Idee zunächst sehr abwegig zu sein (es müssen ja viel zu viele Access Switches eingebaut werden), so sollte man sich einmal Gedanken über die Vorteile machen. Die Technikschränke werden einmal komplett mit ausreichender Anzahl von Access Switches ausgestattet und alles wird rangiert. Vorteil 1: Es können Rangierschnüre mit optimaler, in der Regel sehr kurzer Länge eingesetzt werden; zu kurze oder zu lange Schnüre gibt es nicht mehr. Re-

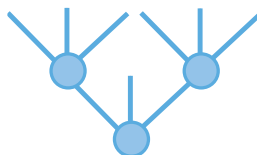
serven im Schrank zur Unterbringung von Überlängen werden nicht benötigt, „Vorhänge“ aus herabhängenden Kabeln verschwinden. Vorteil 2: Als Konsequenz muss während des Betriebs - außer im Fehlerfall (defekte Komponenten) - niemals wieder jemand an den Schränken, Rangierungen oder Switches etwas ändern. Im Idealfall werden die Schränke über Jahre hinweg nicht mehr geöffnet und bleiben in einem aufgeräumten Zustand. Diese Methode steigert die Verfügbarkeit des Netzes erheblich: wer kennt nicht die typischen Fehler verursacht durch Fehlrangierungen oder nicht nachgehaltene Dokumentation. Vorteil 3: Das sonst im Betrieb des Netzes übliche Auf- und Umrangieren entfällt; es muss niemand mehr unterwegs sein, um Ports im Verteiler in Betrieb zu nehmen. Ein Aktivieren und Deaktivieren des Ports ist natürlich weiterhin möglich, erfolgt dann eben halt per Konfiguration am Switch. In einem konkreten Projekt der ComConsult Beratung und Planung wurde das Einsparpotential, bestehend aus reduziertem personellen Aufwand bei Betrieb und Fehlersuche, den Mehrkosten der Access-Switches gegenübergestellt und es wurde sich zu Gunsten der Komplettaktivierung entschieden. Stellt also die „billige“ Komplettverschaltung aller Dosen mit 10/100er-Switches ohne PoE eine Alternative dar?

Quality of Service

Seit einigen Jahren wird heftig darüber diskutiert, ob QoS-Maßnahmen innerhalb eines modernen LAN überhaupt erforderlich sind. Ein Teil der Experten sieht eine großzügig ausgelegte Übertragungskapazität (Overprovisioning) des Netzes als völlig hinreichend an, um selbst QoS-Anforderungen von Voice-over-IP gerecht zu werden. Andere Experten streiten das mit dem Hinweis auf diverse Engpässe in lokalen Netzen vehement ab. Die Autoren können sich sehr gut daran erinnern, dass beispielsweise bereits Ende der 90er-Jahre von namhaften Herstellern prognostiziert wurde, eine Einführung von VoIP sei nur unter Zuhilfenahme von QoS möglich und jeder Verzicht darauf oder die Einführung von einfachen Layer-2-Switches ein Fehler sein wird. Entspricht dies wirklich dem generellen heutigen Netzdesign aller VoIP-Anlagen, laufen diese nur in Netzen mit QoS?

Da im vorliegenden Netzwerk-Insider in einem eigenen Artikel von Dr. Imhoff sehr ausführlich auf diese Thematik, insbesondere auf die Vor- und Nachteile des Overprovisioning eingegangen wird verzichtet dieser Artikel auf eine weitere Analyse der Techniken im Bereich des Quality of Service.

SEMINAR



Ethernet Technologien neuester Stand 25.09. - 29.09.06 in Aachen

Ethernet ist die führende LAN-Technologie. Unterschiedlichste Anwendungsbereiche von der Sprache über Daten bis zur Fertigung basieren auf Ethernet und beeinflussen sowohl dessen Design als auch den Betrieb. Ergänzt wird Ethernet um Wireless-LAN's. Diese können je nach Bedarf in unterschiedlichster Form eingebunden und konfiguriert werden.

Dieses Seminar stellt die neuesten Ethernet- und Wireless-Varianten vor und zeigt, nach welchen Regeln und Auslegungsvorschriften diese zu konfigurieren sind. Mit besonderem Blick auf die Praxis werden Komponenten- und Kabeltechnik erläutert, auch wichtige Betriebsfragen werden vorgestellt. Im Besonderen wird die Bedeutung der IP-Telefonie für die Gestaltung von Ethernet-LANs analysiert. Abgerundet wird das Seminar um wichtige Fragen des Trouble-Shootings.

Referenten: Dipl.-Inform. Oliver Flüs, Dipl.-Ing. Hartmut Kell,
Dipl.-Ing. Harald Krause, Dr.-Ing. Joachim Wetzlar
Preis: € 2.290,- zzgl. MwSt.



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

Auswahl von Access-Switches in modernen Datennetzen

Sinnvolle Abwehrmechanismen

Als „sicher“ verstehen die Autoren solche Access-Switches, die Abwehrmechanismen gegen typische Angriffsszenarien auf das aktive Datennetz - z.B. gegen Angriffe auf die Netzwerkverfügbarkeit (Denial of Service) - oder gegen Angriffe auf übertragene Daten - z.B. Abhören oder Fälschen von Daten - bereitstellen. Die Leistungsfähigkeit hinsichtlich dieser Sicherheit von Access-Switches kann in folgende 3 Teilgebiete unterteilt werden:

1. Schutz gegen unberechtigten Zugang zu Konfigurationsschnittstellen des Switches
2. Schutz gegen ungewolltes Aktivieren von Endgeräten an Zugangsschnittstellen
3. Schutz gegen Störung der Switch-Funktionalität

Die verfügbaren und typischen Schutzmechanismen zu den einzelnen Sicherheitsaspekten werden im Folgenden unabhängig von projekt- oder anwenderspezifischen Anforderungen beschrieben.

Unabhängig von allen weiteren Betrachtungen ist zur Absicherung des Datennetzes im Access-Bereich festzustellen, dass ein mechanischer Schutz der Access-Switches unabdingbar ist. Access-Switches müssen für einen sicheren Betrieb in abgeschlossenen Schränken oder Räumen untergebracht werden, die einen Zugriff unberechtigter Personen auf die Switches wirksam unterbinden. Dies ist die zwingende Voraussetzung dafür, dass die im Folgenden beschriebenen Switch-internen Sicherheitsmechanismen nicht umgangen werden können (z.B. durch Zugriff über die i.d.R. vorhandene Outband-Konfigurationsschnittstelle). Gleiches gilt für Standard-Passwörter, die zwingend auf individuelle Werte umzustellen sind.

Schutz der Konfigurationsschnittstellen

Die Konfiguration von Access-Switches wird häufig über eine Telnet-Verbindung auf die Management-Instanz des Switches durchgeführt. Ein wesentlicher Nachteil von Telnet-Zugriffen ist, dass das Telnet-Protokoll nicht verschlüsselte Login-Namen und Passwörter überträgt. Damit sind aus mitgeschnittenen Telnet-Sessions ohne große Mühe mit freiverfügbaren Analysatoren Anmeldenamen und Passwörter dekodierbar. Hat ein Angreifer diese Informationen zur Hand, kann er quasi alle denkbaren Sicherheitsmechanismen schnell ausschalten.

Daher sollte zur Absicherung der Konfiguration eine verschlüsselte Übertragung von Konfigurationskommandos stattfinden. Diese Verschlüsselung ist z.B. mit wenig Aufwand über das Secure-Shell-Protocol (SSH) erreichbar. Die an den Switch zu stellende Anforderung ist, dass er eine SSH-Server-Funktion unterstützt und dass der konfigurierende Anwender eine Terminal-Emulations-Software mit SSH-Unterstützung verwendet (z.B. TerraTerm oder PuTTY als FreeWare). Über den verschlüsselten Kanal wird dann die Terminal (Telnet) Verbindung verschlüsselt durchgeführt.

Gleiches wie für das Telnet-Protokoll gilt für die Version 1 des Simple-Network-Management-Protokolls (SNMP). Das SNMP-Protokoll verwendet als Authentifizierungsmerkmal einen so genannten Community-String, der als Passwort interpretiert werden kann. Aus einer mitgeschnittenen SNMPv1-Kommunikation kann aus jedem Befehlspaket der Community-String auslesen und für Angriffe verwenden. Eine Abhilfe bieten die neueren Versionen, insbesondere Version 3 des SNMP-Protokolls (SNMPv3). Diese Version bietet durch eine Verschlüsselung und Integritätsprüfung der Daten eine gute Absicherung gegen Abhören oder auch Manipulationen von Management-Informationen. Neben einer SNMPv3 Unterstützung durch den Switch ist zu ge-

währleisten, dass auch die konfigurierende Station – also die Netzwerk-Management-Software - das SNMPv3 unterstützt, da ansonsten auf eine niedrigere Version ohne ausreichende Verschlüsselung und Integritätsprüfung zurückgegriffen werden muss.

Eine besondere Option des Schutzes der Switch-Konfiguration wird von verschiedenen Layer-2-Access-Switches in Form von Layer-3-Zugangssperren (Layer-3-ACL) für den Zugriff auf die Telnet- oder SNMP-Schnittstelle bereitgestellt. Dabei lässt der Switch die Konfiguration über Telnet oder SNMP nur für solche Absender zu, die in der ACL vorgegeben sind, so dass das Ausspionieren von Passwörtern nur für denjenigen Angreifer eine Angriffsmöglichkeit bietet, der gleichzeitig in der Lage ist, die konfigurierten Quelladressen zu übernehmen.

Als ein weiterer Schutzmechanismus für die Konfigurationsschnittstellen kann die Authentifizierung von Teilnehmern an der Telnet-Schnittstelle gegen einen Authentifizierungs-Server eingestuft werden (z.B. RADIUS oder TACACS). Die Authentifizierung gegen einen Authentifizierungs-Server bietet folgenden Vorteil: Es können personengebundene Administratorenkonten eingerichtet und mit Berechtigungen versehen werden. Diese bietet die Möglichkeit, personenbezogenen administrativen

REPORT

Quality of Service in modernen Infrastrukturen - Standards und Architekturen

Dieser Report bietet allen Betreibern von Netzen einen vollständigen Überblick über aktuelle QoS-Verfahren sowohl im LAN als auch in Wireless LANs und in WANs. Darüber hinaus werden alle Entscheider in die Lage versetzt, den Nutzen von Maßnahmen in QoS-Techniken abzuschätzen und mit alternativen Lösungen zu vergleichen. Sie erhalten aktuellste Informationen, die vor dem Hintergrund der zunehmenden Integration von VoIP-Telefonie und der verstärkten Konvergenz von Büro- und Produktionsnetzen bei keinem Netzwerkexperten fehlen darf.

Autor: Dr. Frank Imhoff
Preis: € 398,- zzgl. MwSt. und Versand



Bestellen Sie über unsere Web-Seite www.comconsult-research.de

Auswahl von Access-Switches in modernen Datennetzen

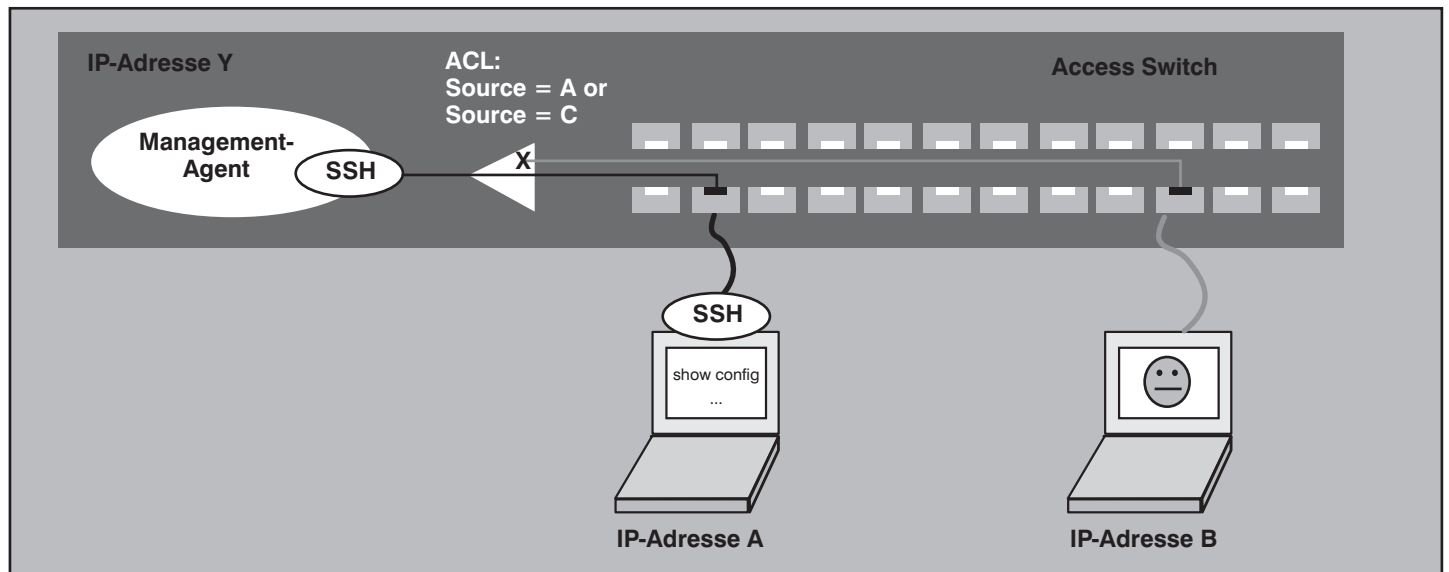


Abbildung 4: Schutz der Managementagenten

Zugang zu gewähren oder auch wieder zu entziehen oder z.B. auch auf Syslog-Servern (sofern der Switch eine Syslog-Funktion unterstützt) sehr detailliert aufzuzeichnen, welcher Administrator wann welche Änderungen durchgeführt hat. Das leider häufig übliche Abspeichern von Anwendernamen und Passwörtern auf dem Access-Switch führt in der Praxis häufig dazu, dass die Abstufung von Administratorenkonten früher oder später ganz aufgegeben wird und dass alle Administratoren sich ein Paar von Username/Password teilen. Die Anmeldeinformationen werden stetig weiter verteilt und einem immer größeren Administratorenkreis bekannt gemacht. Eine selektive Rechtevergabe oder -Entziehung ist nicht mehr möglich.

Wichtige Schutzfunktionen für die Konfigurationsschnittstellen können also zusammengefasst werden als:

- SSH-Verschlüsselung für den Telnet-Zugang
- Unterstützung von SNMPv3
- Unterstützen von IP-Sperllisten (ACL) für die Telnet- oder SNMP-Schnittstelle
- RADIUS- oder TACACS-Authentifizierung für die Telnet-Schnittstelle

„Sichere“ Access-Switches schützen ihre Management-Agenten durch verschlüsselte Übertragung von Management-Kommunikation und zusätzlich durch Vorgabe von zulässigen Quell-Adressen für den administrativen Zugriff. (siehe Abbildung 4)

Schutz gegen ungewolltes Aktivieren von Endgeräten an Zugangsschnittstellen

Bedingt durch die ausschließliche Verwendung von standardisierten Ethernet/IP-Schnittstellen steigt das Risiko, unberechtigte Standardsysteme (PC mit Open-Source-Software oder Freeware-Tools) am LAN anzuschließen und für Spionage oder die Störung von Services zu nutzen. Daher ist es heute für viele Netzwerkbetreiber ein Anliegen, die Zugangsschnittstellen der Access-Switches (im Folgenden auch als Access-Ports bezeichnet) so zu konfigurieren, dass eine Aktivierung unberechtigter Teilnehmer verhindert wird.

Als ältestes Schutzverfahren gegen einen unberechtigten Anschluss an Access-Switches kann die manuelle Konfiguration der MAC-Adresse pro Port eingestuft werden. Die meisten Access-Switches ermöglichen eine Zuordnung von erlaubten MAC-Adressen der Forwarding-Tables. Nur noch die zugewiesenen MAC-Adressen je Port können dann kommunizieren. Allerdings zeigen Umfragen im Kreis der ComConsult-Kunden, dass der administrative Aufwand, bei jedem Umzug von Teilnehmern bzw. Netzwerk-Hardware im Netz eine Änderung der relativ kryptischen MAC-Konfiguration durchzuführen, abgelehnt wird. Daher ist dieses Verfahren nur in kleineren und wenig dynamischen Umgebungen sinnvoll einsetzbar.

Eleganter, aber immer noch nicht ausreichend skalierbar, ist eine Konfiguration von MAC-Zugangssperllisten (MAC-ACL). Im Switch wird hierfür eine eigenständige

Liste aller erlaubten MAC-Adressen konfiguriert und als Ingress-Filter verwendet, d.h. nur Pakete mit solchen Absender-MAC-Adressen, die in der ACL vorhanden sind, werden vom Switch angenommen. Der Vorteil gegenüber der Methode der portbezogenen MAC-Adressen besteht dabei in der Möglichkeit, eine einheitliche Zugangssperlliste aller zulässigen MAC-Adressen zu pflegen und auf alle Switches zu verteilen. Aber auch hier bleibt ein zwar reduzierter, aber dennoch nicht unerheblicher Administrationsaufwand bestehen, so dass auch dieses Verfahren nur in kleinen Netzen angewendet werden kann.

Ein standardisiertes Verfahren zur Absicherung von LANs mit hohem Sicherheitsniveau ist mit dem seit 2001 normierten IEEE-802.1X-Verfahren gegeben. Das IEEE-802.1X-Verfahren zwingt Endgeräte vor der Freischaltung eines Access-Ports zu einer aktiven Authentifizierung. Der Switch baut dafür mit dem sich für Netzzugang bewerbenden Endgerät eine Authentifizierungskommunikation über das Extensible Authentication Protocol (EAP) auf und leitet die Authentifizierungsantworten des Endgeräts an einen Authentifizierungs-Server im LAN (z.B. ein RADIUS-Server) weiter. Wenn der Authentifizierungs-Server zu einem positiven Authentifizierungsergebnis kommt, schaltet der Switch den Access-Port frei, ansonsten bleibt dieser gesperrt, oder je nach Hersteller auch nur eingeschränkt nutzbar. Auch eine authentifizierungsabhängige Zuweisung des Endgeräts zu dedizierten VLANs ist bei einigen Produkten möglich und nur Endgeräten, die eine aktive Authentifizierung gegen einen zentralen Au-

Auswahl von Access-Switches in modernen Datennetzen

thentifizierungs-Server bestehen, wird der Access-Port frei geschaltet. (siehe Abb. 5) Die Autoren erwarten, dass das IEEE-802.1X-Verfahren in einigen Jahren zu einem intensiv genutzten Standard werden wird. Stand heute muss - leider - gesagt werden, dass die Verbreitung im kabelgebundenen LAN noch nicht allzu weit gediehen ist. Dies liegt vermutlich im Wesentlichen an der nicht geringen Komplexität des Verfahrens, der immer noch fehlenden Unterstützung von IEEE-802.1X bei vielen nicht-teilnehmergebundenen Endgeräten wie z.B. Druckern oder IP-Telefonen und Problemen bei verschiedenen Sondertechniken wie z.B. PXE-Boot oder Reihenschaltung von IP-Telefon und PC.

Aufgrund der heutigen Probleme mit IEEE-802.1X muss daher noch auf längere Zeit eine Übergangslösung für nicht-802.1X-fähige Endgeräte gefunden werden. Als eine wesentliche Anforderung neben der Unterstützung von IEEE-802.1X muss daher die Unterstützung eines zusätzlichen Verfahrens für die Authentifizierung von nicht-802.1X-fähigen Endgeräten gefordert werden. Die Authentifizierung von nicht-802.1X-Endgeräten kann zum Beispiel erreicht werden, wenn der Access-Switch zusätzlich zur EAP-Authentifizierung des 802.1X-Verfahrens die MAC-Adresse des Endgeräts ausliest und an den Authentifizierungs-Server als Authentifizierungsmerkmal überträgt. Dies ermöglicht einen Mischbetrieb, in dem 802.1X-fähige Endgeräte über eine aktive Authentifizierung z.B. mit Username/Passwort oder X.509-Zertifikaten authentifiziert werden, während nicht-802.1X-fähige Endgeräte über ihre MAC-Adresse authentifiziert werden. Diese MAC-Adresse-basierte Authentifizierung wird von einigen Herstellern als MAC-RADIUS bezeichnet. Ein optimaler Mischbetrieb wird erreicht, wenn MAC-Adresse-basierte Authentifizierung und 802.1X-Authentifizierung parallel am Switch greifen und dabei dem Authentifizierungs-Server anhand der bei ihm hinterlegten Authentifizierungsmerkmale vorgegeben werden kann, welches Authentifizierungsverfahren angewendet werden soll. Eine Entweder-/Oder-Vorgabe von IEEE-802.1X-Authentifizierung am Access-Switch selbst sollte aufgrund des Konfigurationsaufwands möglichst vermieden werden.

Übrigens kann auch ohne IEEE-802.1X ein Schutz des LANs mit MAC-Adresse-basierter Authentifizierung erreicht werden, wenn diese über einen zentralen Authentifizierungs-Server realisiert wird (z.B. als MAC-RADIUS). Die zulässigen MAC-Adressen im LAN werden einmalig auf dem Authentifizierungs-Server konfigu-

riert werden und können dann netzweit Zugang erlangen. Dieses Verfahren bietet demnach eine große Skalierbarkeit und wesentliche administrative Vorzüge gegenüber MAC-ACLs und statisch konfigurierten MAC-Adressen auf dem Access-Switch.

Abschließend sei darauf hingewiesen, dass einige Hersteller von Access-Switches besondere Funktionen für die „plug-and-play“-Aktivierung von IP-Telefonen implementiert haben. Dazu gehören z.B. die Unterstützung automatischer VLAN-Auswahlung am Access-Port (dient zur automatisierten Aktivierung von VLAN-Tagging für Voice- und Daten-VLANs auf einem Port, an dem beide VLANs für ein IP-Telefon mit nachgeschaltetem PC benötigt werden) oder die automatische Umgehung von IEEE-802.1X-Authentifizierung für IP-Telefone z.B. durch besondere Erkennungspakete, besondere MAC-Adressen oder SIP-Registrar-Pakete. Für eine Absicherung des Netzes ist es notwendig, dass alle diese proprietären „Tricks“ ausgeschaltet werden können müssen und diese nur soweit genutzt werden, wie sie zwischen Sicherheit und dem VoIP-Betrieb als Konsens vereinbar sind.

Die notwendigen Schutzmaßnahmen zur Abwehr unberechtigter Zugänge zum LAN sind also:

- Konfigurierbarkeit von zulässigen MAC-Adressen pro Access-Port oder MAC-ACL
- Unterstützung von IEEE-802.1X
- Unterstützung von MAC-basierter Authentifizierung von Teilnehmern gegen einen Authentifizierungs-Server (z.B. RADIUS)
- gleichzeitige Unterstützung von IEEE-802.1X und MAC-Authentifizierung pro Access-Port
- Abschaltbarkeit von solchen „plug-and-play“-Funktionen bei der Aktivierung von IP-Telefonen, die ein Sicherheitsrisiko darstellen

Schutz gegen Störung der Switch-Funktionalität

Eine letzte Betrachtung sei der Abwehr von Denial-of-Service-Angriffen gegen die Access-Switches gewidmet.

Layer-2-Access-Switches können und werden verglichen mit Layer-3-Backbone-Switches oder Routern als vergleichsweise dumme Netzwerkknoten konfiguriert

und betrieben. Aufwändige Funktionen auf den Access-Switches sollten aufgrund der i.d.R. großen Zahl von Access-Switches im Netz möglichst vermieden und auf zentralen Switches abgebildet werden. Dann ist es möglich, die meisten Prozesse auf dem Access-Switch (z.B. das Lernen von MAC-Adressen und die Vermittlung anhand der MAC-Adressen) durch Hardware-Bausteine des Switches in sehr großer Performance und Stabilität abzuwickeln. Dennoch: auch bei wenig komplexer Konfiguration gibt es einige Prozesse, die auf dem Access-Switch als Software auf einem zentralen Prozessor ablaufen. Dazu gehören in der Regel alle Management-Prozesse aber typischerweise auch Spanning-Tree-Berechnungen und teilweise auch die Behandlung von Broad- oder Multicast. Den Autoren sind verschiedene Fälle bekannt, in denen durch Flutung von Access-Switches mit Broad- oder Multicast-Paketen oder exzessiven Anfragen an z.B. http-Services der Management-Instanzen auch einfach konfigurierte Layer-2-Switches so überlastet wurden, dass der Switch schließlich seine Paketvermittlung einstellte und einen Reboot benötigte. Daher muss zweierlei gefordert werden:

1. Alle prozessorintensiven Verfahren (z.B. http-Server oder sonstige aufwändige Management-Funktionen) müssen selektiv abschaltbar sein, um die Angriffsfläche zu minimieren.
2. Switches, welche die Bearbeitung (Vervielfältigung) von Broad- oder Multicast über einen zentralen Prozessor erledigen, müssen Verfahren zum Schutz gegen eine Prozessorüberlastung bieten (z.B. Broad- oder Multicast-Reduction).

Weiterhin besteht ein unter „Hackern“ verbreitetes Angriffsmuster darin, dass ein Access-Switch mit einer Vielzahl von Paketen unterschiedlicher Absender-MAC-Adressen geflutet wird (MAC-Flooding). Viele Switches versuchen, alle auftretenden MAC-Adressen in ihrer Forwarding-Table zu speichern. Die typischen Konsequenzen sind dabei ein Überlauf der Forwarding-Table und dann z.B. das Kolabieren der Switching-Funktion. Auch eine vollständige Überfüllung der Forwarding-Table mit nicht-relevanten Einträgen ist möglich, die ihrerseits zu Folge hat, dass der Switch im Weiteren wie ein Repeater alle eingehenden Pakete an allen Ports flutet, da er nicht mehr sinnvoll beurteilen kann, welcher Teilnehmer über welchen Port erreicht werden kann. Es ist daher als positiv einzuschätzen, wenn der Switch einen Schutzmechanismus bietet, der bei zu vielen auftretenden MAC-Adressen an einzelnen Access-Ports diese ent-

Auswahl von Access-Switches in modernen Datennetzen

weder sperrt oder das MAC-Learning für diesen Port gezielt unterbinden kann. Allerdings ist hierbei wie bei den meisten proprietären Leistungsmerkmalen insbesondere in großen Layer-2-Netzen Vorsicht geboten, da ja eine Vielzahl von auftretenden Absender-MAC-Adressen an einem Port nicht zwangsläufig einen Angriff darstellen muss, sondern auch auf jedem Uplink-Port möglich ist.

Als letzte Funktion sei auf den nicht unwichtigen Schutz des Spanning-Tree-Verfahrens (STP) hingewiesen. Der Konventionelle Spanning-Tree nach IEEE-802.1D datiert noch aus der „Steinzeit“ der Bridging-Technik und konvergiert relativ schwerfällig im Bereich von 30-60 Sekunden. Große Layer-2-Netze können bei häufigem Auftreten von STP-Topology-Changes leicht dazu gebracht werden, dass die Topologie dauerhaft durch den STP blockiert wird und ein Switching nicht mehr möglich ist. Topology-Changes können dabei auch durch böswilliges Einspielen falscher Bridge-Protocoll-Data-Units (BPDU) „simuliert“ werden. Der modernere Rapid-Spanning-Tree nach IEEE-802.1w (RSTP) sollte diesbezüglich grundsätzlich etwas weniger anfällig sein, konkrete Erfahrungsberichte liegen den Autoren jedoch nicht vor.

Sinnvoll ist daher die Option Access-Switches so zu konfigurieren, dass sie solche

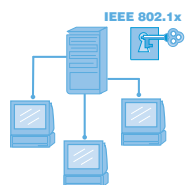
Access-Ports, auf denen wider Erwarten BPDUs empfangen werden, automatisch deaktivieren. Damit hat ein Einspielen schadhafter BPDUs keine Wirkung mehr. Mehr noch: Durch dieses Leistungsmerkmal kann eine „Vervielfachung“ eines Access-Ports durch einen verdeckt, heimlich oder unangemeldet angeschlossenen Switch verhindert werden. Das Bereitstellen zusätzlicher, nicht gewollter Access-Ports wird unterbunden, solange der unberechtigt angeschlossene Switch das STP/RSTP-Protokoll verwendet (dies ist typischerweise für die meisten Switches gegeben). Der „vervielfachte“ Access-Port wird dann automatisch deaktiviert.

Wünschenswerte Funktionen zum Schutz der Switching-Funktionen sind zusammengefasst also:

- selektive Abschaltbarkeit aller prozessorintensiven Leistungsmerkmale
- Unterstützung von Schutzmechanismen gegen Broad- oder Multicast-Stürme,
- Unterstützung einer Erkennung und eines Schutz gegen MAC-Flooding
- Unterstützung einer einschaltbaren automatischen Deaktivierung von Access-Ports, bei Empfang von BPDUs.

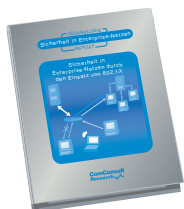
Fazit

Aus Sicht der Autoren sollte sich die Auswahl an Switches für den Access-Bereich unbedingt am erwarteten Nutzungs- bzw. Abschreibungszeitraum orientieren, dem Lockruf der Hersteller nach noch besseren, noch moderneren, noch zukunftssicheren Systemen sollte man nur sehr bedacht folgen. Es müssen nicht unbedingt Systeme beschafft werden, die mehr als 5 oder 10 Jahre halten. Stattdessen ist zu erwarten, dass die notwendige Bereitstellung heute noch nicht benötigter oder bekannter Funktionen eher zu einem Austausch der Systeme führen wird als die Haltbarkeit der Geräte; nichtsdestotrotz hat man bei der Auswahl der Systeme einen erheblichen Einfluss auf die Ausfallrate (MTBF) und kann darüber die Verfügbarkeit von Netzwerkdiensten maßgeblich beeinflussen. Features wie PoE oder auch eine hohe Datenrate von 1.000 MBit/s für alle Endgeräteports wirken negativ auf die MTBF-Zeiten und müssen derzeit noch zu einem höheren Preis eingekauft werden. Sicherheitsfunktionen werden in Zukunft immer wichtiger und müssen bei der Auswahl von Access-Switches berücksichtigt werden. Dagegen ist die Notwendigkeit von aufwändigen QoS-Funktionen bei ausreichender Bandbreite zum heutigen Standpunkt für die meisten Netze kaum erkennbar.

Paketangebot**Sicherheit im LAN mit IEEE 802.1X****25.09. - 26.09.06 in Neuss**

Dieses 2-tägige Seminar vermittelt den optimalen Umgang mit IEEE 802.1X, erläutert die Einsatzvarianten, beschreibt die gegebenen Fallstricke und liefert die ideale Basis zur Vorbereitung eines Einsatzes.

Einzelpreis: € 1.390,- zzgl. MwSt.

**Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X**

Sie erhalten mit diesem Report ein umfassendes Grundlagenwerk, das Sie bei der Auswahl und beim Aufbau einer 802.1X-basierende Sicherheitslösung unterstützt, auf die verborgenen Fallstricke dieses Frameworks aufmerksam macht und wesentliche Betriebsaspekte offen legt.

Einzelpreis: € 398,- zzgl. MwSt. und Versand

Bei Buchung des Seminars „Sicherheit im LAN mit IEEE 802.1X“, bieten wir Ihnen den neuen Report „Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X“ (März 2006) zu einem Sonderpreis an. Statt regulär € 398,- zahlen Sie nur € 338,- (alle Preise zzgl. MwSt.)

Autor des Reports: Dipl.-Math. Cornelius Höchel-Winter - Referenten des Seminars: Dr. Simon Hoff, Dipl.-Ing. Harald Krause
 Paketpreis: € 1.728,- zzgl. MwSt.

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

Aktuelle Veranstaltungen

Sommerschule 2006, 19.06. - 23.06.06 in Aachen

Auch in diesem Jahr bietet die Sommerschule wieder den Intensiv-Update auf den neuesten Stand der Netzwerk-Technik, zeigt neue Nutzungs-Potenziale, diskutiert Änderungen im Design, analysiert aktuelle Produktrends. Damit wendet sich die Sommerschule 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.

Trouble Shooting in konvergenten Netzwerken, 19.06. - 23.06.06 in Aachen

Dieses Seminar vermittelt das notwendige Hintergrundwissen über die typischen Fehler, erklärt ihre Erscheinungsformen im laufenden Betrieb und trainiert systematisch ihre Diagnose und Beseitigung. Dabei wird die Theorie mit praktischen Übungen und vielen Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen.

Preis: € 2.490,- zzgl. MwSt.

Sicherheit 2: VPN Virtuelle Private Netze: Planung, Konfiguration, Betrieb, 19.06. - 21.06.06 in Aachen

VPN-Technologie sind ein unverzichtbarer Teil jeder Netzwerk-Sicherheits-Lösung. Ebenso vielfältig wie die Nutzungsformen sind die Realisierungs-Alternativen und die Integration in bestehende Netzwerk-Infrastrukturen. Dieses 3-tägige Seminar bewertet die bestehenden Alternativen und gibt direkt in der Praxis umsetzbare Empfehlungen zur optimalen Nutzung von VPN-Technologien.

Preis: € 2.290,- zzgl. MwSt.

IP-Telefonie: Vorbereitung, Migration, Management, 26.06. - 28.06.06 in Aachen

Die Referenten dieses 3-tägigen Seminars vermitteln ihre jahrelangen Projekt-Erfahrungen bei der Nutzung und des Betriebs von IP-Telefonie sowie bei der Durchführung hochkomplexer Projekte in diesem Umfeld.

Preis: € 1.690,- zzgl. MwSt.

Lokale Netze für Einsteiger, 26.06. - 30.06.06 in Aachen

Dieses 5-tägige Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Dabei werden sowohl die notwendigen theoretischen Hintergrundkenntnisse vermittelt als auch der praktische Aufbau und der Betrieb eines LANs erläutert.

Preis: € 2.290,- zzgl. MwSt.

Grundlagen des Trouble Shooting in Lokalen Netzwerken, 04.09. - 08.09.06 in Aachen

Dieses Seminar vermittelt, welche Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind, wie man mit diesen Fehlersituationen analysiert und wie dabei methodisch vorgegangen wird, um in kürzester Zeit zu einem Ergebnis zu kommen.

Preis: € 2.490,- zzgl. MwSt.

Wireless LAN, 11.09. - 15.09.06 in Bonn

Dieses 5-tägige Seminar erklärt die Arbeitsweise von WLANs und beschreibt typische Einsatzszenarien von der Ergänzung bestehender LANs bis hin zur kompletten WLAN-Infrastruktur. Die letzten beiden Tage sind optional buchbar und liefern vertiefte Kenntnisse zur Planung, Konfiguration und Betrieb von flächendeckenden sicheren WLAN und Hotspots, ergänzt durch praktische Beispiele und Demonstrationen.

Preis: € 2.290,- zzgl. MwSt.

Sicherheit 1: Kernbausteine einer erfolgreichen Sicherheits-Lösung, 11.09. - 15.09.06 in Bonn

Dieses 5-Tages-Seminar identifiziert die herausragenden Gefahrenbereiche für Firewalls, Webserver, Clienten, Mailsysteme und Netzwerke und zeigt detailliert effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. An vielen typischen Einsatzszenarien wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt.

Preis: € 2.290,- zzgl. MwSt.

Internetworking: optimales Netzwerk-Design mit Switching und Routing, 11.09. - 15.09.06 in Aachen

Dieses 5-Tages-Intensiv-Seminar vermittelt dem Einsteiger Methoden und Technologien zur erfolgreichen Strukturierung von Enterprise Netzwerken. Dabei wird das komplette Spektrum vom L2/L3 Switching über Redundanz/Routing bis hin zu Themen wie VLAN, WLAN-Integration, Multicast-Routing, VPN, MPLS, abgedeckt. Es werden sowohl die theoretischen Hintergrundkenntnisse als auch die Konsequenzen für den praktischen Betrieb von Netzwerken dargestellt. Fallstudien und Gruppenübungen mit Planungsbeispiel vermitteln Informationen, die in der Praxis sofort umgesetzt werden können.

Preis: € 2.290,- zzgl. MwSt.

Cisco Router erfolgreich einsetzen für Fortgeschrittene, 18.09. - 22.09.06 in Aachen

Dieses 5-tägige Intensiv-Seminar wendet sich an Fortgeschrittene und hilft das Potenzial von Cisco Routern optimal auszuschöpfen sowie typische Fehler in der Konfiguration zu vermeiden. Es beinhaltet aktive Konfigurations-Übungen mit Cisco 2600 Routern in Kleinstgruppen. Schwerpunkt in diesem Seminar sind Redundanzkonzepte auf Layer 3.

Preis: € 2.350,- zzgl. MwSt.

IP-Telefonie evaluieren, planen, betreiben, 25.09. - 27.09.06 in Neuss

Dieses 3-tägige Seminar evaluiert Technologien und Produkte gegenüber den in der Praxis bestehenden Anforderungen. Es vermittelt die technischen Grundlagen, beschreibt die Arbeitsweise wichtiger Produkte, analysiert typische Nutzungsformen und gibt eine Prognose für die Marktsituation und weitere Entwicklung. Die Situation etablierter Hersteller wie Alcatel, Avaya/Tenovis, Cisco, Nortel und Siemens inklusive des Leistungsumfangs ihrer Produkte wird bewertet.

Preis: € 1.690,- zzgl. MwSt.

CCNE

ComConsult Certified Network Engineer

Lokale Netze

26.06. - 30.06.06 in Aachen
23.10. - 27.10.06 in Neuss
04.12. - 08.12.06 in Aachen

Internetworking

11.09. - 15.09.06 in Aachen
13.11. - 17.11.06 in Aachen

TCP/IP und SNMP

25.09. - 29.09.06 in Köln
27.11. - 01.12.06 in Berlin

Ethernet Technologien - neuester Stand

25.09. - 29.09.06 in Aachen
27.11. - 01.12.06 in Aachen

Paketpreis für alle vier Seminare € 8.244.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--)



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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen

04.09. - 08.09.06 in Aachen
06.11. - 10.11.06 in Aachen

Trouble Shooting in gewichteten Ethernet-Umgebungen

19.06. - 23.06.06 in Aachen
18.09. - 22.09.06 in Aachen
13.11. - 17.11.06 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen

16.10. - 20.10.06 in Aachen

Paketpreis für alle drei Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen“ € 6.990.-- zzgl. MwSt.
(Einzelpreise: je € 2.490.--)



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

CCSE

ComConsult Certified Security Expert

Sicherheit 1: Kernbausteine einer erfolgreichen Sicherheits-Lösung

11.09. - 15.09.06 in Bonn

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewall, VPN, Windows-Clients, WLANs

23.10. - 27.10.06 in Aachen

Sicherheit 2: VPN Virtuelle Private Netze: Planung, Konfiguration, Betrieb

19.06. - 21.06.06 in Aachen
25.09. - 27.09.06 in Köln

Paketpreis für alle drei Seminare und Report „VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung“ € 5.990.-- zzgl. MwSt. (Einzelpreise: € 2.290.-- / € 1.690.-- / € 2.290.-- / Report 398.--)



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

Impressum

Verlag:
ComConsult Technology Information Ltd.
121 Paton Rd.
RD1
Richmond
New Zealand
GST Number 84-302-181
Registration number 1260709
Phone: 0064 3 5444632
Fax: 0064 3 5444237

German Hot-line of ComConsult-Research: 02408-955300
E-Mail: insider@comconsult-akademie.de
<http://www.comconsult-research.de>

Herausgeber und verantwortlich im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungsweise: Monatlich, 12 Ausgaben im Jahr
Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service der ComConsult Akademie

Für unverlangte eingesandte Manuskripte wird keine Haftung übernommen
Nachdruck, auch auszugsweise nur mit Genehmigung des Verlages
© ComConsult Research