Dr. Suppan International Institute

Der Netzwerk Insider

Dezember 2004

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

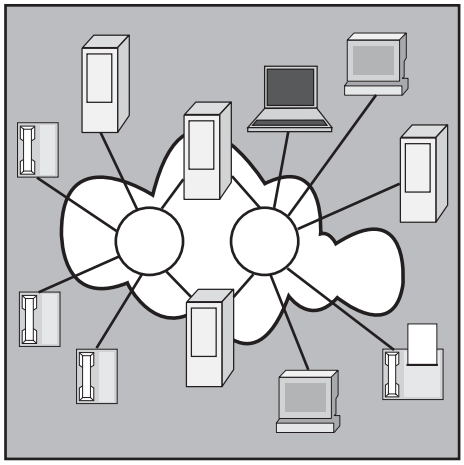
Wachsendes Interesse und verschiedene Verfahren für die Einteilung von LAN in getrennte Netze

von Dr. Behrooz Moayeri

Immer mehr Unternehmen, die in den letzten Jahren die so genannte „Perimeter Security“ realisiert, d. h. zwischen ihren LAN und anderen Netzen eine Trennung mittels Firewalls durchgeführt, das LAN selbst jedoch als einen zusammenhängenden Vertrauensbereich gestaltet haben, müssen nun ihr LAN in getrennte Netze aufteilen. Der folgende Beitrag geht auf die Gründe hierfür sowie auf die Verfahren für die Implementierung dieser Netztrennung ein.

Gründe für die Netztrennung

Für die Einteilung der LAN in verschiedene Vertrauensbereiche gibt es diverse Gründe. Einige dieser Gründe sind wie folgt:



- Immer mehr vormals von einem einzigen Unternehmen genutzte Gelände werden nun von mehreren Unternehmen mit verschiedenen Sicherheitsrichtlinien und -interessen genutzt, z. B. durch die Aufteilung von Firmen, Outsourcing und andere übergeordnete Entscheidungen. Viele Industrieparks sind entstanden, die eine Mehrzahl von zum Teil im Wettbewerb stehenden Unternehmen aufnehmen. Durch Outsourcing werden ganze Abteilungen und Unternehmensbereiche wie z. B. das IT Department auf andere Firmen übertragen. In einigen dieser Fälle besteht beiderseitiges Interesse an der Trennung der IT-Infrastrukturen.

weiter auf Seite 17

Zweitthema

WPP - Baustein zur Infrastrukturfähigkeit von WLANs

von Dr. Franz-Joachim Kauffels

Die neuen WLAN-Standards IEEE 802.11 a,h und n sowie die mittlerweile sinnvollere Klärung von Sicherheitsfragen machen vor dem Hintergrund sehr günstiger Preise die Etablierung von WLANs als Infrastrukturen auch als Ersatz konventioneller Verkabelung attraktiv. Allerdings sind noch sehr viele Fragen offen, u.a. die nach normierten Mess- und Testverfahren. Die neue Arbeitsgruppe WPP (Wireless Predictable Performance) von IEEE 802.11 und WiFi nimmt sich seit neuestem dieser Problematik an.

Die bisher dominierenden WLANs nach IEEE 802.11 b und g eignen sich gut für SOHO-Lösungen und andere überschaubare Bereiche. Die hohe Resonanz auf mobile Technologien allgemein und die gegenüber einer konventionellen Verkabelung nachweisbaren teilweise erheblichen Kostenvorteile führen zum Wunsch nach Einsatz von WLANs als Infrastruktur. Die neuen Standards nach IEEE 802.11 a,h und n sowie eine befriedigende Lösung der Sicherheitsproblematik bereiten hierzu den Weg. Allerdings gibt es noch erhebliche Lücken, auch weil die drahtlose Übertragungstechnologie an sich im LAN-Sektor noch relativ jung ist.

weiter auf Seite 6

Top-Event

Netzwerk-Redesign-Forum 2005

auf Seite 4

Zum Geleit

Netzwerk-Design muss sich neuen Herausforderungen stellen

auf Seite 2

Report des Monats

Neuer Report: Moderne Speichertechnologien

auf Seite 13

Zum Geleit

Netzwerk-Design muss sich neuen Herausforderungen stellen

Das Design unserer Netze ist in vielen Fällen mehrere Jahre alt, gleiches gilt für die dort eingesetzten Komponenten. Mit der noch immer weiter zunehmenden Bedeutung der Netzwerke als der zentralen IT-Infrastruktur stellt sich die Frage, ob die bestehenden Netzwerke dieser Rolle noch gerecht werden.

Folgende Grundfragen bieten sich zur Prüfung eines ggf. notwendigen Redesigns an:

Die Kapazitäts-Frage

Im LAN kann es je nach Alter der Komponenten bei vermehrtem Gigabit-Einsatz oder verstärkte Zentralisierung von Servern und Speicher notwenig sein, auf Komponenten mit höherer Switching-Kapazität umzurüsten. Auch der Einsatz von 10 Gigabit kann dies erforderlich machen, wenn die vorhandenen Komponenten dies zwar formal unterstützen, aber die damit gebotene 10 Gigabit-Integration nicht dem neuesten technischen Stand entspricht (zum Beispiel nur ein Bruchteil dieser Leistung wirklich durchsetzt).

Im WAN besteht der generelle Bedarf nach mehr Kapazität zur Standort-Kopplung, für Desaster-Recovery, zum Aufbau zentraler Data-Center, zur Umsetzung global benutzter Web-Applikationen usw. Da WAN-Kapazitäten in ihrer Nutzung stark preisgetrieben sind, wird es hier in den nächsten Jahren mit weiter fallenden Preisen insbesondere für 10 und 100 Mbit/s Internet-Zugänge zu einer neuen Architektur-Situation kommen. Die technische Grenze zwischen LAN und WAN wird immer schwerer abgrenzbar sein und mehr einem übergeordneten Design-Konzept folgen.

Die Out-of-Life-Frage

Für jede Produktfamilie kommt der Tag, an dem sich weitere Investitionen nicht mehr lohnen, sei es, weil die Familie abgekündigt ist oder die Abkündigung in den nächsten Monaten zu erwarten ist. Neue Produkte haben sich aber bereits den neuen Anforderungen angepasst und bieten veränderte Design-Möglich-

keiten. Diese Möglichkeiten würden verschenkt, wenn die alten Geräte einfach nur 1:1 ersetzt würden.

Die Design-Konzept-Frage

In der Vergangenheit gab es das typische Standard-LAN-Design: L3-Switches im Backbone, L2-Switches auf den Etagen. Unterschiede gab es in der Art der Redundanz-Verschaltung sowohl im L3 als auch im L2-Bereich. Das diesem Design zugrunde liegende Prinzip war: ein Design erfüllt die Ansprüche aller Anwendungen. Speziell im Backbone wurde nicht nach den Anforderungen der verschiedenen Einsatzbereiche differenziert. Nun zeigt sich, dass dieses Grundprinzip nicht in jedem Fall zu erhalten sein wird.

- Zwei Beispiele sollen das verdeutlichen:

  a) Es gibt Wireless-Lösungen, die ein eigenes Distribution-System parallel zum bestehenden Backbone-System aufbauen, um einen oder mehrere kontrollierte Übergänge zum Kabel-LAN zu schaffen. Insbesondere Controller-gesteuerte WLAN-Architekturen über mehrere Gebäude hinweg und Roaming zwischen Zellen kann ein Argument für ein derartiges Szenario sein.

  b) Mit dem stufenweisen Wegfall der Feldbusse im Produktionsbereich entsteht dort ein riesiger Ethernet-Layer-2-Bereich, der auch häufig über den Backbone mit anderen Gebäuden verschaltet werden muss. Hier sind neue Design-Lösungen gefordert, die aber häufig individuell sein werden, da gerade im Fertigungsbereich stark individuelle Anforderungen existieren können.

Die Quality-of-Service-Frage

In der Vergangenheit galt: QoS im LAN möglichst nicht benutzen. In der Tat konnte man ohne Probleme nachweisen, dass es in Verbindung mit Gigabit-Backbones in 99% aller Fälle keinerlei Notwendigkeit zur Priorisierung von einzelnen Anwendungen gegeben hat.

Mit Wireless LANs und auch anderen Bereichen kommen nun Technologien in unsere Netzwerk-Strukturen, die dem bisherigen Prinzip QoS durch Kapazität zu ersetzen, nicht mehr entsprechen. Sie haben keine ausreichenden Kapazitäten, um auf QoS-Mechanismen verzichten zu können. Dies führt sofort zu der generellen Designfrage, ob man isolierte QoS-Zellen für diese Technologien wünscht oder ein flächendeckendes Konzept anstrebt. Letzteres könnte auch für Voice in Verbindung mit LAN/WAN-Verbindungen zum Einsatz kommen.

Die IP-Backbone-Frage

Unser IP-Netzwerk ist der eigentliche Backbone unseres Unternehmens. Und dieser Backbone entwickelt sich immer mehr zum gemischten LAN/WAN-Backbone. Mit der Zunahme der Datenraten im WAN fällt zudem die Grenze zwischen den beiden Technologien. So stellen sich neue Fragen zum Thema Verfügbarkeit, Redundanz, weltweitem Zugang.

Die Sicherheit im Netzwerk-Frage

Das vielleicht momentan am kontroversesten diskutierte Thema. Wie weit sollen Sicherheits-Konzepte in das Netz-

Netzwerk-Design muss sich neuen Herausforderungen stellen

werk integriert werden? Ohne Frage steigen damit Komplexität, Intransparenz und ggf. auch der Betriebsaufwand.

- Zwei Szenarien sollen die aktuelle Diskussion verdeutlichen:

  Im ersten Szenario werden auf ein physikalisches Netzwerk mehrere logische abgebildet. Teilnehmer werden beim Zugang zum Netzwerk nach definierten Regeln den logischen Netzwerken zugewiesen und können nur in diesen kommunizieren. Mit diesem Konzept werden das Besucher-Problem und das Problem unsicherer Endgeräte gelöst. Diese kommen in separate Netzwerke und können keine anderen Teilnehmer infizieren.

  Das Grundproblem ist hier die Identifizierung der Teilnehmer. Eine Möglichkeit besteht in der Teilnehmer-Verwaltung über eine CMDB (Configuration Management Database), einer Lösung, die in Umgebungen bevorzugt wird, die einen hohen Sicherheitsstandard und eine zukünftige Zertifizierung anstreben. Ein Switch meldet eine neue MAC-Adresse zur CMDB und erhält von dort Anweisungen zur Handhabung. Eine zweite Möglichkeit besteht im Einsatz von IEEE 802.1x zur Benutzer-/Geräte-Identifizierung.

  Dieser Ansatz wird momentan immer populärer, da er technisch für Wireless Netzwerke sowieso benötigt wird und somit mit einer Infrastruktur alle notwendigen Fragen beantwortet werden können. In diesem Fall werden Geräte nach erfolgter 1x-Anmeldung einem logischen Netzwerk zugewiesen (siehe Enterasys).

  Im zweiten Szenario geht es um die Bildung getrennter Netzwerk-Zonen, die über Sicherheits-Appliances (z.B. Firewalls) verbunden werden und deren interner Verkehr über Anomalie-Erkennungs-Tools überwacht wird. Die Idee hinter diesem Konzept ist, dass im Falle eines erfolgreichen Angriffs, der betroffene Netzwerkbereich erkannt und in Quarantäne gesetzt wird.

Die Service-Level-Management-Frage

Mit der Konvergenz von Netzwerken im Sinne der Integration aller möglichen Anwendungsbereiche in einer zentralen Infrastruktur Netzwerk entsteht der Bedarf des Nachweises der Qualität für einzelne Anwendungsbereiche. So werden die Betreiber einer IP-Telefonie-Lösung völlig andere Anforderungen an das Netzwerk stellen als die Betreiber der Windows-Server.

Hier müssen Service-spezifische Überwachungs- und Management-Lösungen aufgebaut werden, die auch Service-spezifische Reaktionen zur Beseitigung erkannter Probleme ermöglichen. Dies ist häufig mit relativ einfachen Mechanismen möglich, die vorhandene Management-Plattformen ergänzen.

Die Verfügbarkeits-Frage

Immer häufiger tauchen Szenarien auf, in denen Netzwerk-Verfügbarkeiten deutlich besser als 99% gefordert werden. Dies ist nicht neu, konnte aber in der Vergangenheit häufig entkräftet werden. Die aktuellen Forderungen kommen häufig aus Technologien, die in der Tat auf eine hohe Netzwerk-Verfügbarkeit angewiesen sind. Auch hier sind vorrangig der Voice- und der Produktionsbereich zu nennen. Netzwerke können diese Anforderung erfüllen, benötigen dafür aber ein geeignetes Maschen-Design.

Die Prüf- und Analyse-Frage

Auch alte Netze können besser sein als ihr Ruf. Ggf. kann mit wenigen Verbesserungen bereits ein ausreichendes Leistungsniveau erreicht werden. Wie zuvor ausgeführt, reicht aber zur Prüfung keine allgemeingültige Messung aus. Die Messung muss Service-orientiert erfolgen. Viele der in diesem Zusammenhang in den gängigen Veröffentlichungen erwähnten Messungen sind dabei völlig unzureichend (zum Beispiel die Jitter-Messung zum Test der Voice-Eignung). Wir stellen zur Zeit für Sie zusammen: welche Messmethoden mit welchen Tools sind zur Eignungsprüfung bestehender, aber auch neu installierter Netzwerke besonders zu empfehlen.

Die Beantwortung dieser Fragen ist komplex. Sie ist abhängig von den bei Ihnen vorhandenen Anwendungsbereichen, von den eingesetzten Produkten und auch von der geografischen Verteilung des Unternehmens. ComConsult-Research hat deshalb in Zusammenarbeit mit anerkannten internationalen Top-Spezialisten für Sie analysiert:

- Wann besteht Bedarf für ein Redesign eines bestehenden Netzwerks?
- Welche neuen Design-Ansätze gibt es?
- Wie lassen sich die Anforderungen völlig verschiedener Anwendungsbereiche in einem Design integrieren?
- Wie entsteht Sicherheit im Netzwerk, welche der neuen Möglichkeiten sollte man nutzen welche nicht?
- Welche Konsequenzen haben speziell die Umsetzung von IP-Telefonie und Wireless in aktuellen Netzwerken?
- Wie passen Produkte und Design-Konzepte zusammen? Wie herstellerneutral sind die gegebenen Möglichkeiten? Welche Strategien verfolgen die einzelnen Hersteller?

Die Ergebnisse dieser Analysen stellen wir auf dem Redesign-Forum 2005 zur Diskussion. Auch sind alle namhaften Hersteller eingeladen, ihre aktuellen Design-Empfehlungen vorzustellen und zur Diskussion zu bringen.

Wir freuen uns auf lebhafte und kontroverse Diskussionen. Auch in 2005 wird das ComConsult Redesign-Forum der Treffpunkt der deutschen Netzwerkbranche werden.

In der Hoffnung, Sie dort begrüßen zu können

Ihr
Dr. Jürgen Suppan

Top-Event

Treffpunkt der Branche - Netzwerk-Redesign Forum 2005

Vom 18. - 21. April 2005 veranstaltet die ComConsult Akademie den Kongress „Netzwerk-Redesign Forum 2005“ in Königswinter. Der Kongress analysiert die aktuellsten Entwicklungen der Netzwerk-Technologie und bewertet Marktrends und Produktentwicklungen.

Wie entwickeln sich Netzwerke weiter? Wie sehen geeignete Strategien und Konzepte aus? Was passiert im Markt? Wo liegen Tücken und Fallstricke in aktuellen Technologien?

Die passenden Antworten liefert das Netzwerk Redesign Forum 2005, das seit 10 Jahren zu den Top-Events der Branche zählt.

Mit einer Mischung aus hochaktuellen Technologie-Vorträgen, den exklusiven Ergebnissen neuester Technologie-Untersuchungen sowie diversen Projekterfahrungen und vielen begleitenden Diskussionen und Gesprächen ist diese Veranstaltung ein Muss für jeden, der beruflich mit Netzwerken zu tun hat.

Im Mittelpunkt des Netzwerk-Redesign-Forums 2005 steht die Frage, wie das Design bestehender Netzwerke zur Erfüllung der immer weiter gehenden Kommunikations-Anforderungen verbessert werden kann.

Das Redesign-Forum 2005 bietet folgende hochaktuelle Themenblöcke:

Top-Analyse unseres Labors: neue Kommunikations-Anforderungen an Netzwerke

- Neue IT-Architekturen und ihre Anforderungen
- Globalisierung und Kommunikation
- Speicher-Technologien im Netzwerk
- Optimierter Client-Betrieb und die notwendigen Voraussetzungen
- IP-Telefonie, Konferenzschaltungen, Video/Multimedia/Dokument-Sharing
- RFID erweitert Netzwerk-Architekturen
- Logistik-Anwendungen im Netzwerk
- Produktions-Netzwerke und das Layer-2-Problem

Netzwerk-Redesign

- Bewertung eines bestehenden Netzwerk-Designs
- Design-Alternativen und ihre Nutzbarkeit
- Investitions-Sicherung
- Benutzertrennung im Netzwerk: Konzepte und Nutzbarkeit
- Service-Level-Orientierung im Design
- Voice-ready-networks: Design-Grundsätze und Anforderungen aus der Praxis
- Design-Konzepte im Vergleich: der neue Cisco Campus-Guide, Enterasys, Extreme

Standardisierung und Technologie-Entwicklung

- Was passiert hinter den Kulissen, was ist neu, wie relevant ist es?
- Welche neuen Standards sind verabschiedet, welche stehen vor der Tür?
- Was passiert in den Labors der Hersteller?

Optimierung des Netzwerk-Betriebs

- Wie kann ein Netzwerk besser betrieben werden?
- Was leisten neue Werkzeuge?
- Service-Level-Operating im Tagesbetrieb

Hersteller und Produkte

- Wie positionieren sich die Hersteller?
- Wie entwickeln sich wichtige Netzwerk-Produkte?
- Welche Vorteile können genutzt werden?

Sicherheit und Netzwerke

- Welchen Stellenwert haben Sicherheits-Lösungen im Netzwerk?
- Benutzeranmeldung im Netzwerk: welche Vorteile bietet das?
- Was leistet 802.1x, welche Projekterfahrungen existieren?
- Automatische Rechte- und Netzwerkzuordnung auf der Basis der Geräte- oder Benutzererkennung
- Was leistet eine Configuration Management Database CMDB? Generierung der Netzwerk-Konfiguration aus der CMDB?

WAN/Corporate Networks im Umbruch

- Was muss ein WAN in den nächsten Jahren leisten?
- Welche Realisierungs-Alternativen bestehen?
- Mehr Kapazität, mehr Verfügbarkeit, geringere Kosten?
- Remote Access: mit jedem Endgerät von jedem Ort mit optimaler Qualität?
- Standort-Verbindungen neu gestalten

IP-Telefonie erfolgreich einsetzen

- Neueste Entwicklungen in der Analyse
- Stellenwert des SIP-Standards! Ausrichtung am Standard oder Konzentration auf einen Hersteller?
- Investitions-Sicherung: welche Alternativen der Migration zur IP-Telefonie bestehen?
- Wer hat die beste Lösung? Siemens versus CISCO versus Alcatel!
- Präsenz-Telefonie: ein neuer Standard oder eine Modeerscheinung?

Wireless LANs

- Neue Wireless-Standards: wo steht 802.11 im Vergleich mit 802.15/16/20?
- Aufbau einer Wireless-Hierarchie
- Controller-basiertes Design verdrängt Standard-Access-Point-Design
- Redundanzkonzepte

Am 4. Tag bieten wir den Teilnehmern Ein-Tages-Intensiv-Trainings zu ausgesuchten Top-Themen. Dabei werden der Stand der Technik und der optimale Betrieb wichtiger Technologien intensiv über den ganzen Tag evaluiert. Die

Netzwerk-Redesign Forum 2005

Teilnehmer können dabei zwischen den Workshops wechseln.

Zurzeit sind folgende Intensiv-Trainings für den 4. Tag geplant:

- Voice-Ready-Networks
- Sicherheit im Netzwerk: neue Technologien sinnvoll einsetzen
- WAN-Redesign

Sie sehen, das Netzwerk Redesign Forum 2005 wird seinem Ruf als die führende deutsche Kongressveranstaltung zu Netzwerk-Technologien wieder voll gerecht. Mittlerweile im 10. Jahr wird sich hier auch 2005 die Branche treffen.

Die Mischung aus hersteller-neutralen Top-Referenten, den neuesten Technologie-Entwicklungen, hochaktuellen Projekterfahrungen und direkt umsetzbaren Empfehlungen aus der Praxis, einer hochaktuellen Ausstellung, der gleichzeitigen Anwesenheit vieler relevanter Hersteller hat diesen Kongress zum jährlichen Treffpunkt der Branche gemacht.
In den letzten Jahren war diese Veranstaltung immer ausgebucht. Als Mitglied des VIP-Verteilers haben Sie hiermit die einmalige Chance, sich bevorzugt einen Platz zu buchen bevor die öffentliche Werbung anläuft.

Als Dankeschön für die vertrauensvolle Zusammenarbeit gewähren wir Ihnen dabei bis zum 31.12.2004 den einmaligen VIP-Sonderrabatt von 12 %.

Die Buchung innerhalb der Frühbucherphase ist verbindlich, kann aber jederzeit auf andere Mitarbeiter Ihres Unternehmens übertragen werden. Die Teilnahmegebühren werden mit Auslauf der Frühbucherphase fällig.

Zögern Sie nicht und sichern Sie sich einen Platz auf unserer Top-Veranstaltung des Jahres 2005.

Auf dem Forum werden Sie von unserem Spitzen-Moderatoren begrüßt:

Dr. **Jürgen Suppan** gilt als einer der führenden deutschen Berater für Kommunikationstechnik. Unter seiner Leitung wurden diverse Netzwerkprojekte aller Größenordnungen erfolgreich umgesetzt. Seine Seminare zählen durch ihren didaktischen und lebendigen Aufbau und ihre Praxisnähe und Herstellerneutralität zu unseren erfolgreichsten Veranstaltungen.

Dr. **Franz-Joachim Kauffels** ist einer der erfahrensten und bekanntesten Referenten der gesamten Netzwerkszene (über 20 Fachbücher und unzählige Artikel) und bekannt für lebendige und mitreißende Seminare.

Netzwerk-Redesign-Forum 2005
Frühbucher-Rabatt bis 31.12.2004

Teilnahmegebühr vom 18.04. - 21.04.05 inklusive Workshop am letzten Tag innerhalb der Frühbucherphase € 1.750,- (regulär € 1.990,-).

Teilnahmegebühr vom 18.04. - 20.04.05 ohne Workshop am letzten Tag innerhalb der Frühbucherphase € 1.480,- (regulär € 1.690,-).

Alle Preise zzgl. MwSt. Die Buchung innerhalb der Frühbucherphase ist verbindlich.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk-Redesign Forum 2005

Ich buche den Kongress
Netzwerk-Redesign Forum 2005
vom 18.04. - 21.04.05 in Königswinter

☐ **mit Workshop € 1.750,- zzgl. MwSt.***
☐ **ohne Worksdop € 1.480,- zzgl. MwSt.***
***gültig bis 31.12.2004**

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

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ,Ort
eMail	Unterschrift

Zweitthema

WPP - Baustein zur Infrastrukturfähigkeit von WLANs

Fortsetzung von Seite 1

Dr. Franz-Joachim Kauffels ist einer der erfahrensten und bekanntesten Referenten der gesamten Netzwerkszene (über 20 Fachbücher und unzählige Artikel) und bekannt für lebendige und mitreißende Seminare.

Die Lücken findet man leicht, wenn man den Stand der konventionell verkabelten LAN-Technik und den Stand der professionellen flächendeckenden Funktechnik (Radio, GSM, UMTS ...) mit dem aktuellen Stand bei WLANs vergleicht.

Eine der erheblichsten Lücken gibt es hinsichtlich der Normierung von Messmethoden. „Wer misst misst Mist“ ist eine alte Weisheit. Wenn dann auch noch jeder misst, was er denkt, ist das Ergebnis sicherlich alles andere als nachvollziehbar.

Bisher war das Problem nicht so evident. Bei der Versorgung irgendeiner kleineren Fläche mit WLAN-Leistung hat es den Meisten bislang als Hauptkriterium ausgereicht, dass alle Empfänger in der Fläche irgend etwas empfangen konnten und dann war es gut. Dazu reichen ja auch diese einfachen Softwareinstrumente, wie sie serienmäßig mit WLAN-Adaptern ausgeliefert werden. Nur in bestimmten Umgebungen hat man sich weitergehende Gedanken, z.B. hinsichtlich verschiedener Störeinflüsse gemacht.

Bei der letzten großen IEEE 802.11-Konferenz in Vancouver ist eine Arbeitsgruppe gegründet worden, die sich endlich dieser Probleme systematisch annehmen will. Sie hat z.Zt. den Namen IEEE 802.11-WPP: Wireless Predictable Performance. Der Grundgedanke ist höchst konstruktiv: man möchte Methoden definieren, die es ermöglichen, eine WLAN-Umgebung aufzubauen und definiert durchzumessen und zwar so, dass die Leistung dieser WLAN-Umgebung sicher vorhersehbar ist.

Das entspricht der Vorgehensweise bei strukturierter Verkabelung. Man verwendet Komponenten, deren Eigenschaften man kennt und fügt sie in definierter Art und Weise entlang einer „Bauvorschrift“ zusammen. Damit erzeugt man eine Infrastruktur. Es folgt ein Abnahmeprozess, in dem eine Reihe von vorgeschriebenen Messungen ebenfalls nach eindeutigen Vorschriften vorgenommen wird. Die Ergebnisse der Messungen dokumentieren den Zustand des Systems und zeigen evtl. Schwachstellen auf, die nachgebessert werden müssen.

Dieses Verfahren ist mittlerweile seit vielen Jahren bewährt und eröffnet überhaupt erst die Möglichkeit für Infrastrukturanbieter, Kunden, die meist überhaupt nicht nachvollziehen können, was sie da einkaufen, Systeme zu verkaufen, die anschließend einer bestimmten Leistungsspezifikation genügen. Es schafft nicht nur Vertrags- und Gewährleistungssicherheit für die beteiligten Parteien, sondern ist mit dem Gesamtwerk der Spezifikationen so gestaltet, dass auch darüber hinausgehende Ansprüche, wie z.B. die Einhaltung gesetzlicher Störstrahlungsverordnungen, berücksichtigt werden. Es nützt auch allen beteiligten Herstellern als Hilfestellung beim Entwurf und der Weiterentwicklung entsprechender Produkte. Natürlich gibt es auch immer wieder Mängel und Probleme, die sind aber gegenüber dem Gesamterfolg vernachlässigbar.

Grundproblem: Komplexität

Wenn wir uns erinnern, hat es ungefähr ein Jahrzehnt gedauert, derartige Dinge zu entwickeln. Zu Beginn der verkabelten LANs hat jeder Hersteller gemacht, was er wollte. IBM war der erste Hersteller, der überhaupt so etwas wie eine Spezifikation für die Verkabelung definiert hat, mit mehr Lücken als Inhalt, aber immerhin. Es folgten die Standards nach EIA/TIA und schließlich ISO, die auch heute noch täglich weiterentwickelt werden. Aber erst seit wenigen Jahren sind auch nachvollziebare Messmethoden definiert.

Man kann nicht erwarten, dass dies jetzt bei WLANs alles plötzlich vom Himmel fällt. Es wird auch hier einige Jahre dauern, bis es Spezifikationen gibt, die es Herstellern ermöglichen, den Kunden Systeme anzubieten, die eine nachvollziehbare vorhersehbare Leistung im Sinne einer Infrastruktur haben. Aber man muss mit diesen Anstrengungen jetzt beginnen, auch weil die WLAN-Welle schneller rollt als alles, was wir bisher kennen.

Die Ausgangssituation ist indes viel ungünstiger. Bei einer verkabelten LAN-Lösung gewinnt man schon mit folgenden Messungen eine hohe Aussagekraft bezüglich der zu erwartenden Gesamtleistung:

- Dämpfung
- Delay
- Jitter
- Analyse von Fehlern (Jabber, ...)

Diese Messungen werden für die USA in den RFCs 2285, 2544 und 2889 festgelegt. Zusammen mit den bekannten Spezifikationen für die Verkabelung und der Einbeziehung des messbaren Verhaltens der Switches ergibt sich ein sinnvolles Gesamtbild. Länderspezifisch können noch einige weitere Messungen hinzukommen.

Es mag ungewöhnlich erscheinen, die Switches direkt mit einzubeziehen, aber der Kunde wünscht eine allgemeine Infrastrukturlösung und eine Aussage über deren Leistung. Dies wird auch manchmal getrennt behandelt.

Bei den WLANs gibt es allerdings keine Möglichkeit der getrennten Behandlung, denn die Access Points sind integraler Bestandteil des Grundsystems. Allerdings gibt es hier direkt einen ganzen Haufen von Messungen, die notwendig sind, um zu einigermaßen aussagekräftigen Ergebnissen im weiter oben genannten Sinne zu kommen:

WPP - Baustein zur Infrastrukturfähigkeit von WLANs

- Dämpfung
- Delay
- Jitter
- Einfluss der automatischen Ratenanpassung auf Dämpfung, Delay und Jitter
- Einfluss des Power Managements auf Dämpfung, Delay und Jitter
- Einfluss der Verschlüsselung auf Dämpfung, Delay und Jitter
- Einfluss der Überlappung von BSS (Zellen) auf Dämpfung, Delay und Jitter
- Einfluss von RTS/CTS auf Dämpfung, Delay und Jitter
- Einfluss der Fragmentierung auf Dämpfung, Delay und Jitter
- Leistung des Assoziationsvorgangs (Einbuchen)
- Leistung des Authorisierungsvorgangs
- Zeitbedarf beim Roaming
- Paketverlust beim Roaming
- Kontinuität von Sitzungen beim Roaming
- Benötigte Zeit für Ratenanpassung
- Paketverlust durch Ratenanpassung
- Übertragungsrate vs. Reichweite
- QoS
- Polling Performance
- Forwarding bei Contention auf dem Ethernet-Port des APs
- Leistung von WiFi Switches

Man sieht, dass ein Teil der Probleme darauf zurückzuführen ist, dass es sich eben um Funksysteme handelt und ein anderer Teil darauf, dass diese Funksysteme nur lückenhaft definiert sind. Man kann natürlich darauf hoffen, dass sich letzterer Teil irgendwann einmal ausdünnt, aber z.Zt. stehen wir klar an einem Punkt, wo die Entwicklung gerade erst begonnen hat. Alleine mit dem System IEEE 802.11 h kommen eine Reihe von Problembereichen hinzu, die z.B. die automatische Kanalwahl und deren Einfluss auf die Gesamtleistung betreffen. Mit den Systemen nach IEEE 802.11 n werden Koexistenzprobleme, automatische Ratenanpassung nach Systemgruppen und Probleme durch gewollte Mehrwegefunkübertragung mit orthogonalen Codes auf gleichen Frequenzen hinzukommen.

Der Start von WPP

In der ersten Sitzung der WPP-Gruppe waren gleichermaßen Betreiber und Chip-Hersteller vertreten. Die Chip-Hersteller haben bei WLANs die Rolle, die bei „normalen“ LANs von den Kabel- und Systemherstellern eingenommen wird. Für sie ist es vor allem wichtig, Leitlinien für die Entwicklung zu bekommen, denn die Standards lassen da einfach viel zu viele Fragen offen. Daher ist es auch nicht verwunderlich, dass Repräsentanten der WiFi anwesend waren. Immerhin ist das diejenige Gruppe, die dafür sorgt, dass man WLANs heute überhaupt benutzen kann.

Primäre Fragestellungen der WPP-Gruppe sind:

- Welchen Bedarf gibt es für 802.11 Metriken?
- Welche Probleme werden damit gelöst?
- Wer sind die primären Anwender hierfür?
- Wie sollte man vorgehen, um neue Metriken für Wireless zu schaffen?

Heute sind zwei wesentliche Ansätze für entsprechende Vorgehensweisen bekannt. IETF (BMWG) hat einen zweistufigen Ansatz für die Definitionen: ein Terminologie Dokument definiert alle relevanten funktionalen Charakteristika und ein Methodologie Dokument definiert die Vorgehensweise. Diese Methode ist am besten für Performance Testing geeignet. Der Ansatz vom ATM Forum bzw. heute Metro Ethernet Forum basiert auf ratifizierten Standard Dokumenten. Jede Test Definition bezieht sich auf Quelltext der Standards. Diese Methode ist am besten für Conformance Testing geeignet

IETF (BMWG) vollzieht einen objektorientierten Ansatz und definiert, um der Vielfalt der Systeme Herr werden zu können, zunächst einmal so genannte Schablonen (Templates).

Terminologie Definition Schablone

- Term, der definiert werden muss, z.B. Latenz
- Definition: die spezifische Definition für den Term. Discussion: eine kurze Dis-

Test Name	Name derived from reference document
Test Definition ID	A punctuated alphanumeric string assigned to each defined requirement and test procedure couple using the following convention: ‘one to three letter abbreviated source document name’ . ‘section number’ - ‘paragraph number in the section from which requirement is derived’. This number always figures as the last number of an ID. Ethernet Services Model=M; Ethernet Services Definitions=S; Traffic and Performance Parameters for SLSs=T. Example: M.6.1-4
Reference Document Source	Reference document and section (and paragraph when useful for clarity)
Test Type	Functional, Conformance, Interoperability or Performance
Test Status	Normative, optional, additional
Requirement Description	Brief description of the service requirement that the device must or should satisfy
Description of DUT/SUT	Type of Ethernet frame forwarding Device Under Test (DUT). Common designations used in this document are: CE Device (Customer Equipment Device); UNI Device (User Network Interface Device); MEN Device (Metro Ethernet Network Device). A UNI device may be considered as a kind of MEN ‘border’ device.
Test Object	Succinct description of test purpose
Test Bed Configuration	Succinct description of test bed configuration
Test Procedure	Succinct description of the test procedure with mention of the test stimulus and expected output
Units	Units can be time units, rates and counts in integers such as milliseconds, frames per second and numbers of frames transmitted or received. For the most part units used are defined in RFCs 2285, 2544, 2889
Variables	Variables such as frame length, test duration, numbers of interfaces under test must be described
Results	Description of the textual, numerical and/or graphical format in which to display test results
Remarks	Description of any particular observations that might effect the test result

Abbildung 1: Conformance Test Methods

WPP - Baustein zur Infrastrukturfähigkeit von WLANs

kussion über den Term, seine Anwendung und irgendwelche Restriktionen für die Messprozeduren.
- Maßeinheiten: die Einheiten in denen die Messungen für den Term beschrieben werden, falls anwendbar.
- Sachverhalte: Liste von Sachverhalten oder Bedingungen, die Einfluss auf diesen Term haben.
- Liste anderer Terme, die für die Diskussion dieses Terms relevant sind.

Methodologie Definition Schablone
- Ziele
- Setup Parameter
- Prozeduren
- Messungen, Berichtsformate

Die Abbildung 1 zeigt als Beispiel das Template für Conformance Test Methoden. Der Text wird absichtlich nicht übersetzt, damit der interessierte Leser einen Zusammenhang zu den Begriffen in der Originalliteratur finden kann.

Die WPP-Arbeitsgruppe hat natürlich die Aufgabe, die Problemstellungen nach Dringlichkeit zu sortieren. Die höchste Dringlichkeitsstufe haben hierbei sicherlich Bereiche, die man einfach als Konstruktionsmängel beschreiben könnte.

Konstruktionsmängel: Beispiel Roaming

Es geht primär bei den Arbeiten der WPP-Gruppe gar nicht so sehr um die Überwindung komplexer funktechnischer Probleme z.B. hinsichtlich der Einschätzung der Wellenausbreitung. Eine erste und besonders dringende Anforderung an WLAN-Messstandards ist das Ausräumen hausgemachter (Firmware) Probleme.

Der Bereich „Roaming“ ist ein praktisches Beispiel, welches zeigt, dass schlechte Leistung auf das Fehlen von Test Standards zurückzuführen ist.

Die Aussagen in den Standards, die es bislang von IEEE 802.11 gibt, zeigen ein frühkindliches Verständnis des Problems unter gleichzeitiger Ignoranz bestehender Lösungen (mit dem Handy klappt es doch meistens, oder?).

Beim Roamen macht ein 802.11 a/b/g/h Gerät: Disassoziation von einem AP, Suche nach einem stärkeren Signal von einem anderen AP, Asssoziation und Auth. an diesem AP und wenn dies erfolgreich war Wiederaufnahme der normalen Datenübertragung. Roaming kann scheitern an: transienten RF Bedingungen und der Zeit, die APs und Geräte für den vierstufigen Roaming Prozess benötigen.

Die Abbildung 2 zeigt einen Testaufbau für einen Roaming Test
Der Roaming Test soll folgende Zeit messen:
Total Roaming Time =
Decision Time + Switch Over Time

Die Decision Time ist die Zeit, die der NIC braucht, um damit aufzuhören, zu versuchen, Pakete an AP 1 zu schicken; nachdem das RF Signal nachgelassen hat. Die Switch Over Time ist die Zeit, die der NIC braucht , um seine Association mit AP2 zu vollenden, nachdem er mit dem Versuch aufgehört hat, Pakete an AP 1 zu schicken. Während der Decision Time erkennen die Karten das schwächer werdende Radiosignal und versuchen zunächst, sich mit langsameren Datenraten an die geänderten Bedingungen anzupassen. Die Switch Over Time endet, wenn der NIC das Ack vom AP auf den Association request erhält. Diese Zeit sollte nur dann aufgezeichnet werden, wenn der Datentransfer nach der Reassoziation wieder störungsfrei und normal verläuft. Man sieht sofort, dass vor allem die Entscheidungsverfahren hier eine wichtige Rolle spielen, nach denen eine Station bestimmt, ob das RF-Signal nur vorübergehend schwächelt oder durch die Erhöhung der Distanz vom AP nachlässt. Messergebnisse sind hier in erster Linie für Chipentwickler wichtig. Der Standard schweigt sich übr das Thema vollkommen aus.

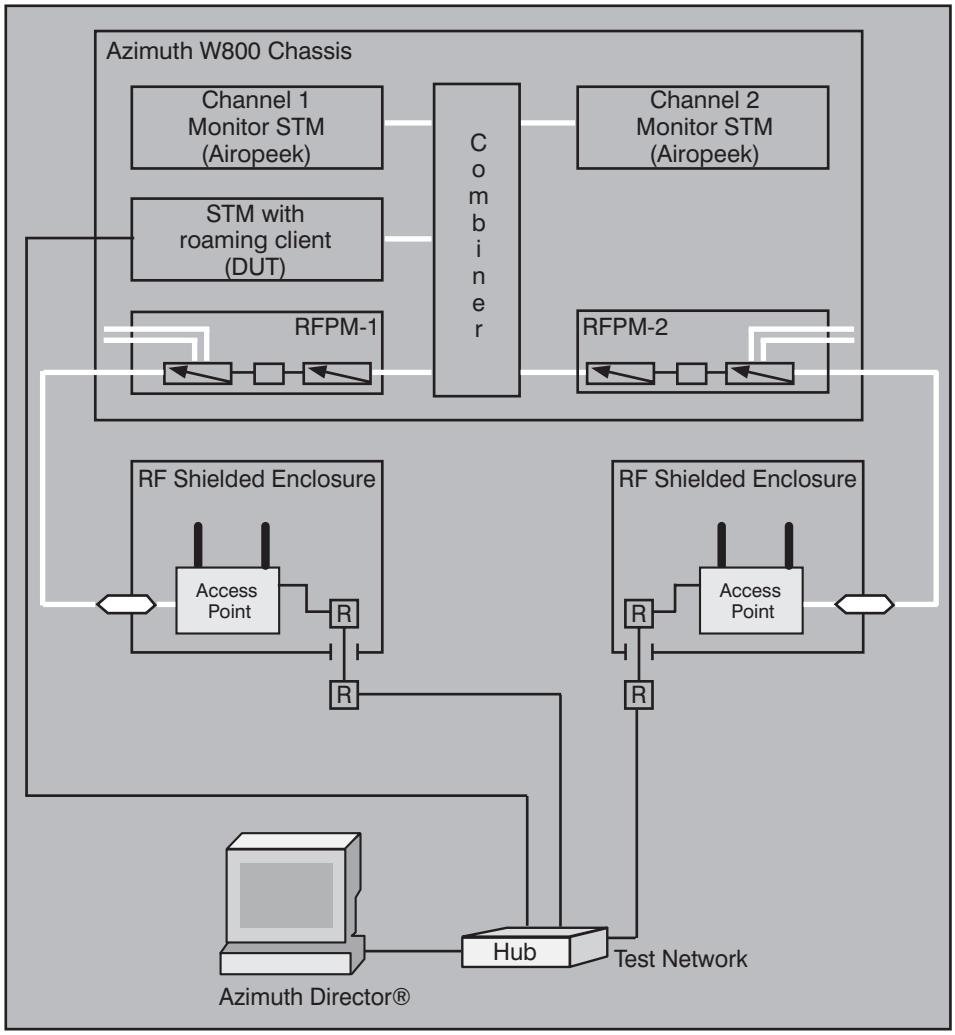


Abbildung 2: Test Konfiguration für Roaming Test

Wendet man den vorgenannten Test heute an, kommt man z.B. auf solche Ergebnisse, wie sie Abbildung 3 zeigt:

Die Ergebnisse sind schlichtweg erschütternd. Selbst die gutmütigste Verbindung wird nach einer halben Minute verzweifelt aufgeben. Anwendungen, die auch nur einen Hauch von Professionalität haben sollen, kann man mit diesen Ergebnissen schlichtweg knicken. „Hallo, unser VoIP over WLAN-Telefonat wird jetzt 12 Sekunden unterbrochen, weil ich einen Raum weiter gehe. Bitte leg nicht auf ...“

WPP - Baustein zur Infrastrukturfähigkeit von WLANs

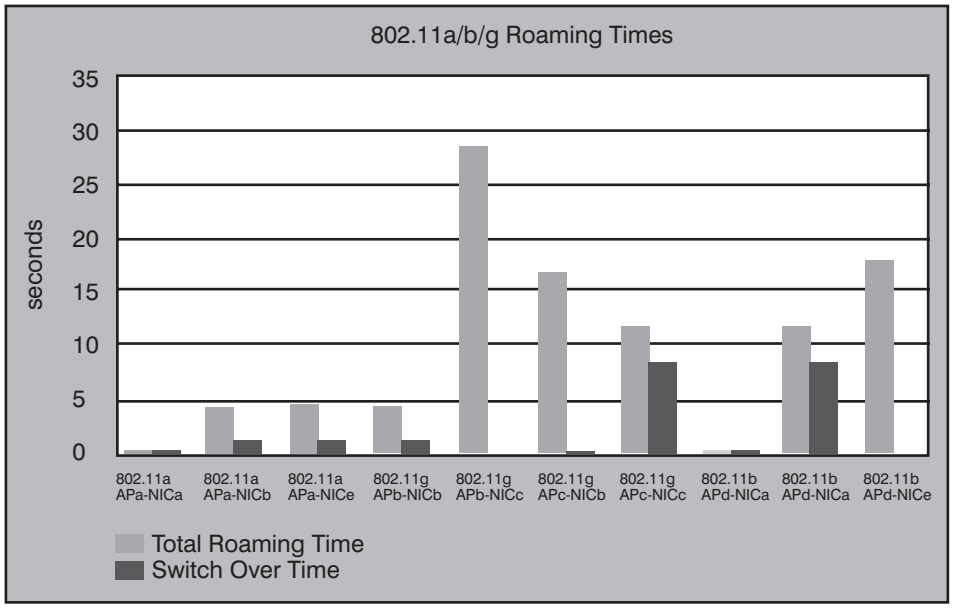


Abbildung 3: Test Resultate Roaming Test

Die Abbildung 4 zeigt nochmals die Schwankungsbreite. Das kann man einfach nicht hinnehmen!

Switch Over Times liegen minimal ca. 60 Millisekunden, Mittelwerte bei ca. 700 Millisekunden über alle Kombinationen und es gibt zwei Ausreißer, die über 8 Sekunden gebraucht haben. Mehrheitlich hat die Decision Time den größten Anteil an der Gesamtzeit für das Roaming. Paket Traces zeigen, dass die meisten Implementierungen der Verfahren für die automatische Ratenanpassung die Rate von 1 Mbps für einige Sekunden beibehalten, nachdem der Verlust des RF-Signals bemerkt wurde. Diese Algorithmen müssen für schnelles Roaming überarbeitet werden. Test Standards für das Messen von Roaming Zeiten können hierzu einen signifikanten Beitrag leisten, weil dann alle Hersteller und Nutzer einen gemeinsamen Satz Definitionen haben.

Was für Roaming gilt, gilt auch für viele andere Bereiche.

Es ist hier leider nicht der Platz vorhanden, auf mehr einzugehen, aber das können wir ja in den nächsten Monaten noch nachholen.

Ein weiterer wichtiger Bereich ist natürlich die Position des Kunden/Benutzers/Betreibers einer WLAN-Infrastruktur, die letztlich durch die Frage geprägt wird, was ein Wireless Service ist und wie man seine Qualität beurteilen und sichern kann.

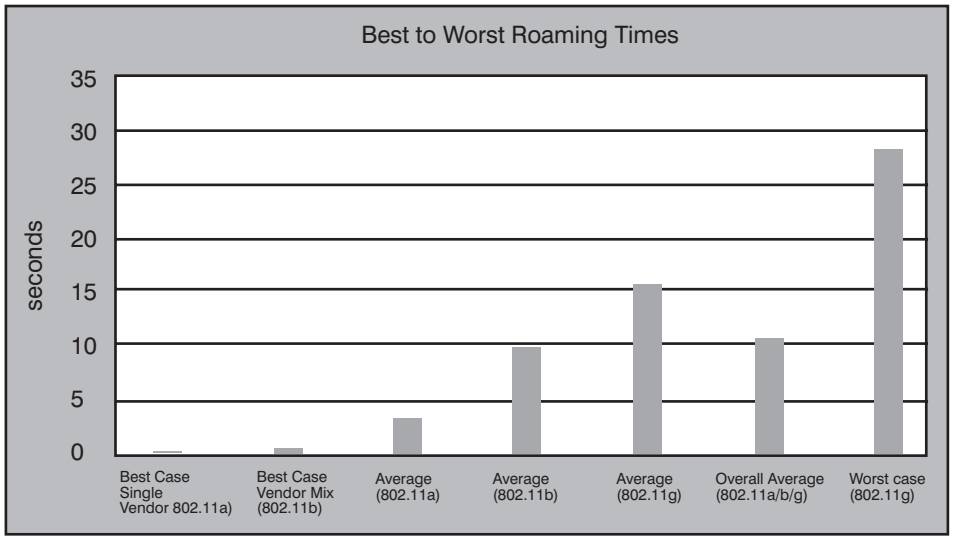


Abbildung 4: Schwankungsbreite Roaming Test

Kundenperspektive: Wireless Service

Den Betreiber eines Wireless Netzes werden die Innereien eines Roaming- oder sonstigen Algorithmus weniger interessieren. Er hat eine Population Benutzer mit einem Zoo von (mobilen) Endgeräten und eine Reihe von Anwendungen und Daten, mit denen diese Benutzer möglichst produktiv arbeiten sollen. Ihn interessiert, wie, zu welchen Kosten und mit welcher Qualität er Benutzer mit Anwendungen verbinden kann. Er fragt sich also z.B.:

- Was ist “Wireless Service”?
- Wie kann man ihn messen?
- Welche Faktoren haben Einfluss auf den Wireless Service?
- Wie kann man den Wireless Service verbessern?

Die Anforderung an WPP von der Kundenseite sind Hilfestellung bei der Beantwortung dieser Fragen. Der Kunde verfolgt dabei unterschiedliche Zieldimensionen, wie z.B.

Service Ziele:
- Mache Wireless Service äquivalent zu fest verdrahtetem
- Biete einzigartige mobile Services an

Betriebliche Ziele:
- Reduktion von Betriebskosten
- Minimierung von Support Personal

Es müssen dazu von WPP Kriterien gefunden werden, die die Erfahrung des individuellen Endbenutzers reflektieren und es muss Kriterien geben, mit denen man die unterschiedlichen Umgebungen – Enterprise, SOHO, Home - differenzieren kann.

Tests sind heute oft unkontrolliert und erzeugen fragwürdige Ergebnisse, die auch selten reproduzierbar sind. Tests isolieren heute das Feature, was getestet werden soll, nicht immer richtig. Tests können unbeabsichtigt die Grenzen der Spezifikation verlassen. Tests bilden die Last durch reale Benutzer ggf. nicht richtig nach und Tests nehmen oftmals keine Rücksicht auf andere Leistungsparameter. Die Spezifikationen haben sich seit IEEE 802.11b immer wieder ausgeweitet und die Tests haben nicht Schritt gehalten. So stellt sich immer wieder die bange Frage:
Vergleichen Tests Äpfel mit Birnen?

Von WPP erhofft man sich
- Die Entwicklung einer minimalen Menge von Test Metriken, die relevant für Schlüssel Performance Parameter (Robustheit, Durchsatz/Kapazität, Reichweite) sind

WPP - Baustein zur Infrastrukturfähigkeit von WLANs

- Die Entwicklung einer Menge von “Test Best Practices”, die reproduzierbare Resultate erzeugen, die richtige Balance zwischen Komplexität und Kosten haben und von der Industrie auch genutzt werden

Testkategorien für WPP

Ausgehend von einer Reihe von Graubereichen des Testens hat man sich auf eine Reihe von Testkategorien für WPP verständigt. Diese stellen - wie immer - einen Kompromiss aus den verschiedenen dargestellten Interessenperspektiven dar. Identifizierte Graubereiche sind z.B.

Durchsatz
- Wird der Durchsatz als MAC layer Payload gemessen? Auf IP layer? Auf TCP or UDP layer?
- Ein Gerät unter Test (DUT) mag bessere Ergebnisse an der PHY Layer als ein zweites DUT haben, aber z.B. schlechter werden, wenn z.B. der Rate Selection Algorithmus schlecht ist.
- Konsistenz in einem offenen Environment ist problematisch
  - Kann der Durchsatz in einer verkabelten Umgebung ohne Antenne gemessen werden?
  - Was ist, wenn das DUT eine Phased Array Antenne hat?
  - Was ist, wenn das DUT mini-PCI ist und keine Antenne hat?

Reichweite
- Was ist, wenn ein höherer TX Level Interferenzen in den Nachbarkanälen erzeugt und den Durchsatz eines benachbarten BSS negativ beinflusst?

Stromverbrauch
- Ist es nur der DC Verbrauch an der Schnittstelle der Karte?
- Solllte die CPU Last auch betrachtet werden, wenn die DUT den größten Teil ihrer Funktionalität auf ihrem Host-PC implementiert?

Roaming
- am schnellsten: 1 STA, 2 APs auf dem gleichen Kanal
- realistischer: AP rebootet, viele STAs roamen zum neuen AP auf einem neuen Kanal

Der geneigte Leser kann sich einen Spaß daraus machen, diese Liste beliebig zu verlängern.

Für jedes Endgerät wird es eine andere Gewichtung von Kriterien geben, siehe dazu Abbildung 5.

Bei der Definition von Testparametern für

	Durchsatz	Delay & Jitter	DC power	Roaming time
Laptop	++	+	++	+
AP	++	++	N/A	N/A
VoIP phone	0	+++	++	++

Abbildung 5: Gewichtung von Kriterien

WPP müssen Entscheidungen, welche Parameter nun betrachtet werden sollen, gefällt werden. Dazu gehört auch die Frage, wie die Leistungswahrnehmung des Benutzers in einen Satz reproduzierbarer Meßeinheiten transformiert werden kann z.B. hinsichtlich Durchsatz und Reichweite, Frame Latenz, Sichtbarkeit von APs, Delays bei Authent./Association und Roaming ohne Verlust von Verbindungen.
Z.Zt. diskutiert man folgende Messungen

Basis PHY/RF Messungen
Transmitter Parameter Messungen
- TX EVM oder Frame Error Rate (FER) mit Golden/Calibrated Receiver
- Carrier Unterdrückung
- Carrier Frequenzstabilität

Receiver Parameter Messungen
- RX FER vs. input power
- Flat channel (kontrolliert durch verkabelte und geschirmte Umgebung)
- Controlled frequency-selective channels (bekanntes Multipath power-delay Profil)

Antennen Messungen
- Gewinn vs. Azimuth und Winkel

MAC Layer Messungen
- Rate Adjustment Verhalten
- Spezifische Parameter? Test Bedingungen?

- Association und Roaming Verhalten
- Frame Latenz
- Layer-2 Durchsatz mit Verschlüsselung
- Wie viele verbrauchte Host CPU Zyklen?

Layer-4 Messungen
- UDP frame loss Rate und Latenz vs. Empfangsleistung
- flache oder frequenzselektive Kanäle?
- TCP Durchsatz vs. Empfangsleistung

Eine generelle Fragestellung betrifft Labor- vs. Open Air Messungen. Open-air Messungen sind immer Opfer unvollständig bekannter und über die Zeit variierender Multipath Power-Delay Profile, denn es gibt eine substantielle Variation bei 2.4 und 5.5 GHz über mehrere Zehntel msec.

TOP-KONGRESS 2005
Netzwerk-Redesign-Forum 2005

18.04. - 21.04.05
in Königswinter

Wie entwickeln sich Netzwerke weiter? Wie sehen geeignete Strategien und Konzepte aus? Was passiert im Markt? Wo liegen Tücken und Fallstricke in aktuellen Technologien? Die passenden Antworten liefert das Netzwerk Redesign Forum 2005, das seit 10 Jahren zu den Top-Events der Branche zählt.

Mit einer Mischung aus hochaktuellen Technologie-Vorträgen, den exklusiven Ergebnissen neuester Technologie-Untersuchungen sowie diversen Projekterfahrungen und vielen begleitenden Diskussionen und Gesprächen ist diese Veranstaltung ein Muss für jeden, der beruflich mit Netzwerken zu tun hat.

Moderator: Dr. Jürgen Suppan
Preise: € 1.750,-* zzgl. MwSt. inklusive Workshop
€ 1.480,-* zzgl. MwSt. ohne Workshop
*gültig bis 31.12.04, dann € 1.990,- und € 1690,- zzgl. MwSt.

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

WPP - Baustein zur Infrastrukturfähigkeit von WLANs

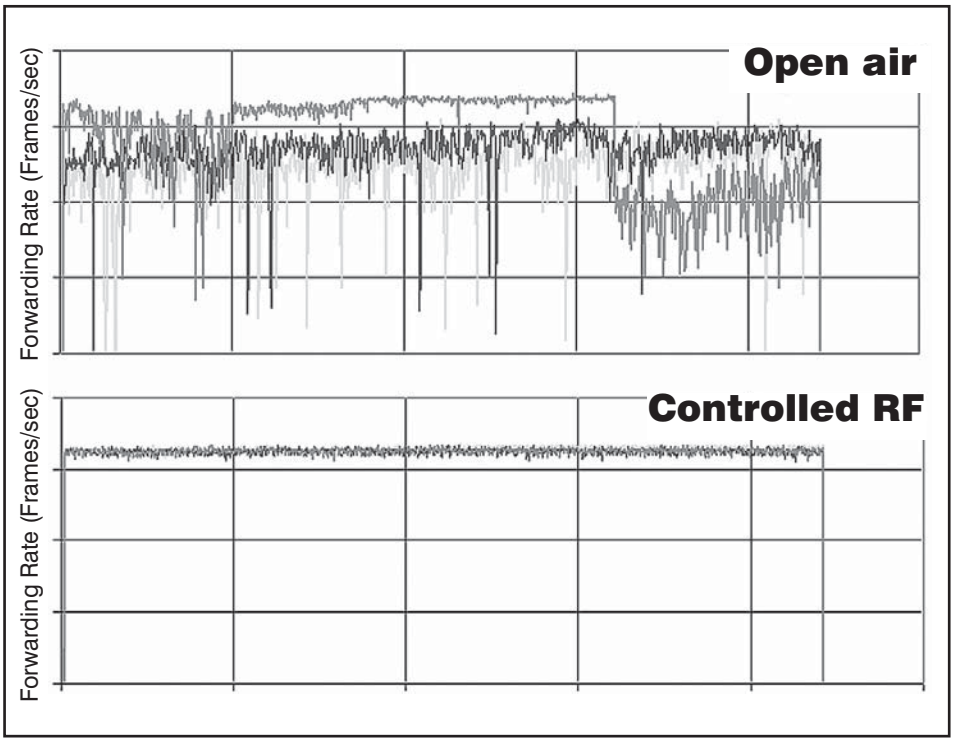


Abbildung 6: Forwarding Rate Messung

Die Multipath-Effekte können sogar dazu führen, dass Kanäle mit einem eigentlich höheren Verlust eine größere Kapazität als Kanäle mit einem eigentlich geringeren Verlust haben können. Die Kapazität eines Kanals kann sich sehr schnell ändern. Das ist ein noch größeres Problem für Systeme wie 802.11a/h and 802.11g, die eine große Anzahl möglicher Datenraten haben. Das Problem wird mit zukünftigen Standards immer schlimmer.

Was kann man tun? Es gibt die Empfehlung, so viele Messungen wie möglich mit Kabeln durchzuführen und die Ausführung von Open Air Messungen in einem Bereich, in dem die Distanz zwischen Transmitter und Receiver klein ist verglichen mit der Distanz zwischen sowohl Transmitter als auch Receiver und jedem anderen Objekt zu beschränken. Das ist hilfreich aber nicht ausreichend, da auch kleinste Reflexionen Auswirkungen auf die Kanalkapazität haben.

Der Ratschluss angesichts dieser Probleme kann nicht wirklich befriedigen. In der WPP-Gruppe gibt es eine Reihe von Praktikern, die sagen, man kann nur aufgeben und ein wirklich großes Ensemble von Messungen durchführen und Statistiken sammeln!

Die Abbildung 6 zeigt, wie sehr die Ergebnisse zwischen kontrollierter Umgebung und Open Air auseinander liegen können. Hier betrachten wir die Beispielmessung einer Forwarding-Rate, die natürlich in der kontrollierten Umgebung nahezu ideal verläuft.

Letztlich benötigt man beide Arten von Messungen. Nur in einer kontrollierten Umgebung lassen sich Feinheiten ausprobieren, wie z.B. unterschiedliche Arbeitsweisen von Algorithmen. Einen Benutzer wird es hingegen wenig freuen, wenn seine Verbindung in der täglichen Praxis holpert. Das Wissen, dass da irgendwo im Chip eigentlich wertvolle Algorithmen implementiert wurden, wird ihm kaum weiterhelfen. WPP muss also die notwendige Balance finden.

Zwischenfazit

Die Arbeiten von WPP haben gerade erst begonnen. Im Sinne stabiler WLAN-Infrastrukturen ist das sehr zu begrüßen und wir werden natürlich die Entwicklung von Ergebnissen genauestens beobachten. Der IT Manager fragt doch letztlich nur: “Wie gut funktionieren mobile Lösungen in meinem Unternehmen?”

Das heutige Dilemma besteht darin, dass Standard-Benchmarks für verdrahtete Umgebungen nicht die richtige Antwort geben. Die Verifikation von Funktionen und Leistungen im inherent unstabilen drahtlosen Raum verlangt nach neuen Methoden und Metriken und die Antwort auf diese Probleme sind neue Methoden für Testen und Messen jedes Aspekts von Wireless Protokollen. Allerdings steht eines schon heute fest: man braucht ca. 5 mal so viele Metriken wie bei traditionellem Ethernet!

Seminar und Report Wide Area Networks

21.02. - 23.02.05 in Köln

Dieses Seminar basiert auf den jüngsten Erfahrungen von Experten mit jahrelanger Erfahrung im Bereich der Konzipierung und Planung von WAN-Lösungen. Die Referenten kommen aus der Praxis und vermitteln Ihnen ihr Wissen sowohl bei der überprüfbaren Übertragung von Kommunikationsdiensten an Provider als auch beim Aufbau eigener Infrastrukturen im WAN-Bereich.

Report

Der neue Technologie-Report von ComConsult Research behandelt das gesamte Spektrum von den technologischen Grundlagen über Projekt- und Designplanung und Ausschreibungsdetails bis zu Betriebskonzepten und Management von WANs.

Referenten und Autoren: Dipl.-Inform. Andreas Meder, Dr.-Ing. Behrooz Moayeri
Preis: € 1.690,- zzgl. MwSt.

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

Seminar mit aktueller Studie

Storage-Netze: Technologie und Lösungen in der Analyse

Vom 11. - 13. April 2005 veranstaltet die ComConsult Akademie ihr hochaktuelles Seminar „Storage-Netze: Technologie und Lösungen in der Analyse“ in Bonn.

Die Zentralisierung von Speicher in der Form von Storage-Netzen ist die unverzichtbare Basis fast aller Konsolidierungs- und Optimierungs-Projekte. Die Vorteile reichen von der Kostensenkung über die flexiblere Nutzung bis hin zu vereinfachtem Backup und Disaster Recovery.

Die angebotenen Produkte basieren auf unterschiedlichen Technologien, selbst innerhalb einer Technologie ist Interoperabilität zwischen Herstellern nicht die Regel. So erfordert die Planung und Umsetzung von Storage-Netzen eine sorgfältige Analyse der konkurrierenden Lösungsansätze.

Dieses hochaktuelle Seminar arbeitet die verfügbaren Technologien und Produktansätze auf und analysiert ihre Nutzbarkeit und die damit erreichbare Lösungsqualität.

Im Einzelnen beinhaltet das Seminar folgende Themen:

- Storage-Netze: Stand der Technik, Entwicklungstrends, Motivation
- Standardisierung: wer macht was, was ist relevant
- Standards im Überblick: FibreChannel, SCSI, FCIP, Infiniband
- Reichweiten und Performance: wo liegen die Grenzen
- Lösungsansätze in der Analyse: DAS; NAS; SAN, iSCSI
- SAN-Lösungen: Technologie-Alternativen und Komponenten im Vergleich, für wen ist wann was geeignet
- Schlüsselfaktor Sicherheit: Zoning, Masking, ACLs
- Virtualisierung: was leistet sie, macht sie überhaupt Sinn, wo liegen Vor- und Nachteile
- Management: InBand kontra OutBand
- Migration: was ist zu beachten
- Datensicherung: Konzepte und Lösungen in der Analyse
- Hochverfügbarkeit: 2-Standort-Lösungen, Clustering, Disaster Recovery

Inhaltliche Themenschwerpunkte sind:

- Standards und Protokolle
- Varianten und deren Gegenüberstellung
- Darstellung der unterschiedlichen SAN-Topologien, die realisierbar sind
- SAN-Komponenten
- Sicherheit
- Virtualisierung auf den unterschiedlichen Ebenen
- Management
- Realisierbare Heterogenität
- Migration
- Datensicherung und - wiederherstellung
- Hochverfügbarkeit

Report zum Seminar

Moderne Speichertechnologien: Architekturen, Produkte und Migrationswege
Mit einer grundlegenden Einführung in die Protokolle und Architekturen von Speichernetzen, einer Vielzahl praxisnaher Designvorschlägen und der Vorstellung typischer, aktueller Produkte gehört dieser Report zu den herausragenden Standardwerken über Speichernetzwerke. Abgerundet wird der Bericht durch Kapitel über Management, Migrationswege und zur Datensicherung. Er ist damit für alle Planer und Betreiber von Rechenzentren und Datenspeichern ein absolutes Muss.

Fax-Antwort an ComConsult 02408/955-399

Paketanmeldung

Seminar mit aktueller Studie

☐ Ich melde mich zum Seminar „Storage-Netze: Technologie und Lösungen in der Analyse“ vom 11.04. - 13.04.05 in Bonn und bestelle zusätzlich den aktuellen Report „Moderne Speichertechnologien“ (25% Rabatt)
zum Preis von € 1.988,- zzgl. MwSt.

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

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

Report des Monats

NEUER REPORT!
Moderne Speichertechnologien:
Architekturen, Produkte und Migrationswege

ComConsult Research stellt den neuen Technologie Report über moderne Speichertechnologien vor. Mit einer grundlegenden Einführung in die Protokolle und Architekturen von Speichernetzen, einer Vielzahl praxisnaher Designvorschlägen und der Vorstellung typischer, aktueller Produkte gehört dieser Report zu den herausragenden Standardwerken über Speichernetzwerke. Abgerundet wird der Bericht durch Kapitel über Management, Migrationswege und zur Datensicherung. Er ist damit für alle Planer und Betreiber von Rechenzentren und Datenspeichern ein absolutes Muss.

Es folgt eine Leseprobe aus diesem Report:

FC-AL (Arbitrated Loop)

Für diese Topologie wird das Fibre Channel Arbitrated Loop Protokoll (FC-AL) eingesetzt. FC-AL hatte lange Zeit einen höheren Bekanntheitsgrad als FCP, obwohl dieses Protokoll jüngeren Datums ist. Dies lag daran, dass für dieses Protokoll sehr früh bereits Komponenten auf dem Markt verfügbar waren, bevor es überhaupt Switches oder Direktoren für FCP gab. FC-AL steht in seinen Funktionen den Funktionen des FCP einiges hinterher und daher sind die hierauf beruhenden Topologie für einen Netzaufbau ins Hintertreffen gegenüber den Switch-Topologien geraten ist.

Immer weniger Produkte unterstützen das Protokoll, die Topologie findet immer mehr Einzug in die Speichersysteme selbst. Solche Speichersysteme be-stehen aus Festplatten mit einer FC- statt SCSI-Schnittstelle und die Geräte werden in einem bzw. doppelten Loop angeordnet. (siehe Abbildung 1)

Diese Topologie basiert auf ein Entscheidungsverfahren (Arbitration) ähnlich wie beim Token-Ring-Verfahren. Der Port, der die Arbitration gewinnt, erhält den Medienzugriff und hat für die Transaktion die volle Bandbreite des AL zur Verfügung. Nach der Transaktion schließt der Port die temporäre Verbindung und stellt die Bandbreite anderen Stationen zur Verfügung. Nach jeder Datenübertragung wird erneut ausgehandelt, wer als nächstes den Zugriff auf das Medium erhält. Diese Arbitration generiert natürlich einen Overhead, der die Leistung des FC-AL reduziert. FC-AL ist also ein Shared Medium, bei dem sich die effektiv zur Verfügung gestellte Bandbreite pro Gerät mit steigender Anzahl der Geräte im Loop reduziert. Mit insgesamt 16 Geräten in einen Loop und die volle Bandbreite von 100 MB/s vorausgesetzt beträgt beispielsweise die effektive Bandbreite nur noch circa 6 MB/s.

Während der Transaktion werden die Daten von Port zu Port gesendet, wobei jeder Port überprüft, ob das Datenpaket für ihn bestimmt ist. Die Anzahl der Geräte in einem Loop ist beschränkt auf 126. Dies ist zurückzuführen auf die 8b/10b-Kodierung, die laufend die Running Disparity kontrolliert und entsprechende Characters mit passender Disparity für die Einhaltung der Kodierungsregel setzt. Daraus resultiert, dass lediglich 134 gültige Characters mit den Kodierungsregeln generiert werden können, wovon sieben Character für Sonderfunktionen verwendet werden. Es verblieben also 127 gültige Adressen für die Arbitrated Loop Port Address (AL-PA). Dies führt dazu, dass maximal 126 Adressen in einem Loop verwendet werden können. Die 127te oder genauer die erste der gültigen Adresse wird immer für den FL-Port (Fabric-Loop-Port eines Switches) verwendet, an welchem der Loop betrieben wird.

In diesem Fall spricht man von einem Public Loop. Ist der Loop in sich geschlossen ohne an einer Fabric angebunden zu sein, dann ist die Rede von einem Private Loop. Je kleiner der Wert der Adresse ist, desto eher gewinnt der Port bzw. die Adresse die Arbitration, da mit der Adresse eine Portpriorisierung verbunden ist. Daher besitzt in einem Public Loop der FL-Port die höchste Priorität, so dass dieser zu jeder Zeit die Arbitration gewinnt und der Switch dann weitere Aufgaben innerhalb der Fabric durchführen kann. In einem Public Loop werden den Ports im Loop über die ersten zwei Bytes der Portadresse der so genannte Fabric Loop Identifier mitgeteilt, welcher für alle Ports im Loop gleich ist. In einem Private Loop

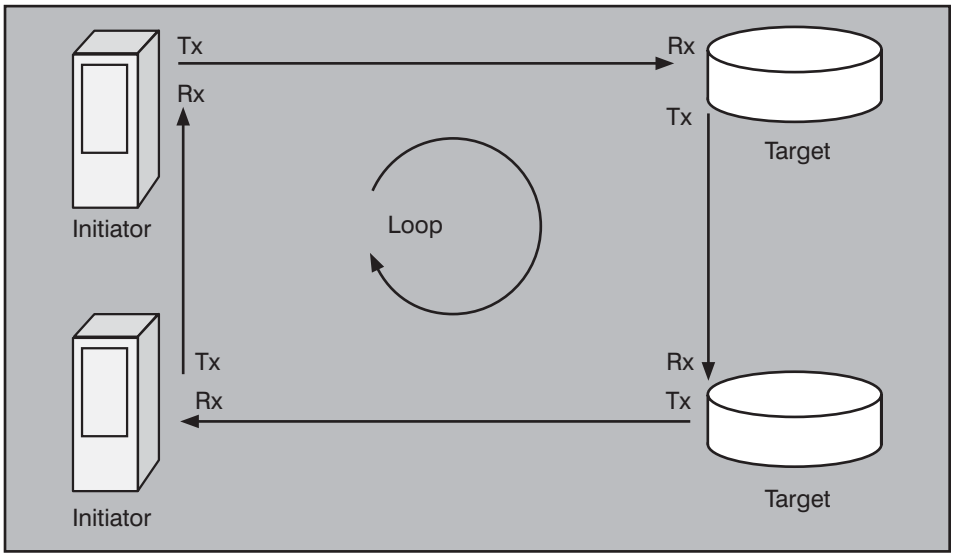


Abbildung 1: Loop-Verbindung

wird dieser Wert auf x0000 gesetzt. Das letzte Byte der Portadresse ist in beiden Fällen die AL-PA für den Port.

Trotz der Priorisierung garantiert das Protokoll, dass jeder sendewillige Port auch tatsächlich den Zugriff erhält. Kein Port muss also aufgrund einer höheren AL-PA „verhungern“. Über eine Fairness-Variable wird dieser Prozess gesteuert: Jeder NL-Port, der die Arbitration ge-wonnen und seine Daten übertragen hat, ist er erst dann wieder an der Reihe, wenn alle ande-ren sendewilligen NL-Ports ebenfalls ihre Daten übertragen haben. Das Zugriffsverfahren funktioniert im Wesentlichen wie folgt:

- Der sendewillige Port tut seine Absicht kund, indem er eine Anforderung ARB(x) (x entspricht der AL-PA) sendet. Dies kann er zwar auch machen, während ein anderer Teilnehmer im Besitz des Loops ist, aber nur zwischen jeweils zwei Rahmen.
- Empfängt der Teilnehmer seine eigene ARB(x), dann wechselt er in den ARB-won-Zustand.
- Empfängt ein anderer Teilnehmer den ARB(x), während er beabsichtigt selbst zu senden, dann wird die Priorität anhand der AL-PA verglichen.

Abhängig von der Anzahl der Teilnehmer im Loops kann dies länger dauern, da mit steigen-der Anzahl von Teilnehmern die Wahrscheinlichkeit wächst, dass mehrere zeitgleich Daten übertragen wollen.

Es ist beispielsweise sinnvoll, dass die Serversysteme, welche als Initiatoren arbeiten, auch eine niedrige AL-PA erhalten, die Speichersysteme (Targets) dagegen eine höhere Adresse, da diese nie eine Arbitration gewinnen müssen bzw. nie einen Zugriff auf das Medium selbständig versuchen werden.

Die AL-PA wird bei der Initialisierung des AL bestimmt und kann sich nach jeder Initialisierung oder bei einem Reset eines Gerätes ändern. Adresskonflikte können aufgrund dieser dynamischen Adressvergabe nur dann entstehen, wenn zwei zuvor unabhängige Loops miteinander verbunden werden. Hubs führen jedoch in der Regel bei einer Zusammenführung über eine Kaskadierung selbsttätig eine Schleifen-Initialisierung durch.

Es wird daher empfohlen, keinen Loop mit allzu vielen Ports aufzubauen, weil dies die Performance dramatisch senken kann. Darüber hinaus muss die Anzahl der Initiatoren in einem vernünftigen Verhältnis zu den Targets stehen. In der Praxis sind nicht mehr als vier bis sechs Initiatoren pro Loop üblich. (siehe Abbildung 2)

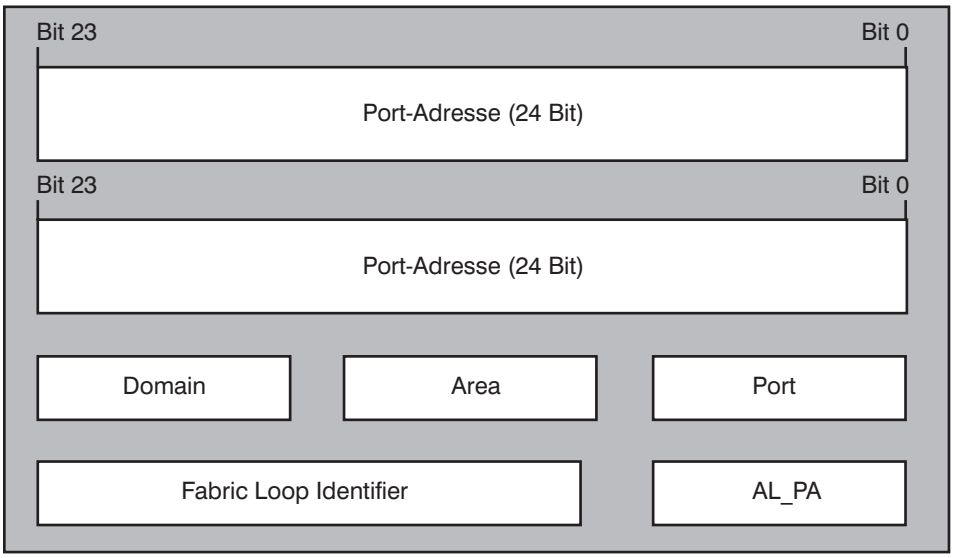


Abbildung 2: Aufbau der Portadresse für FC-AL

Die ersten AL-Varianten waren in der Tat eine Verkettung von mehreren Stationen mit dem Problem, dass die Entfernung einer Station oder die Unterbrechung des Kabels den gesamten AL beeinträchtigte. Heutzutage wird mittels FC-AL-Hubs physikalisch eine Sterntopologie aufgebaut, die sich logisch als Ringtopologie darstellt. Dies hat den Vorteil, dass die Hubs als Repeater fungieren können und auch bei Ausfalle eines NL-Ports den logischen Ring über eine Bypass-Schaltung geschlossen halten ohne den Loop zu beeinträchtigen. Der Hub verbindet dazu den Transmitter (Tx) des letzten Hubports mit dem Receiver (Rx) des ersten Ports. Eine Kaskadierung von Hubs ist ohne spezielle Kabel möglich. In einem Loop über mehrere kaskadierte Hubs zählt jeder Port innerhalb des Loops, also auch Ports, die zwischen einzelnen Hubs geschaltet sind. In der nachfolgenden Abbildung ist beispielhaft ein Loop über drei Hubs dargestellt. Es sind drei Initiatoren und sechs Targets angebunden. Tatsächlich werden jedoch 13 Ports adressiert. (siehe Abbildung 3)

Loop-Initialisierung

Die Loop-Initialisierung wird zur Aufnahmen von neuen Teilnehmern in eine Loop, zur Zuweisung von Adressen (AL-Pas), sowie bei einer Topologieänderung durchgeführt. Der eigentliche Prozess wird als loop initialization primitives (LIP) bezeichnet. Bevor eine Initialisierung außer aufgrund der zuvor genannten Gründe tatsächlich durchgeführt wird, sendet ein

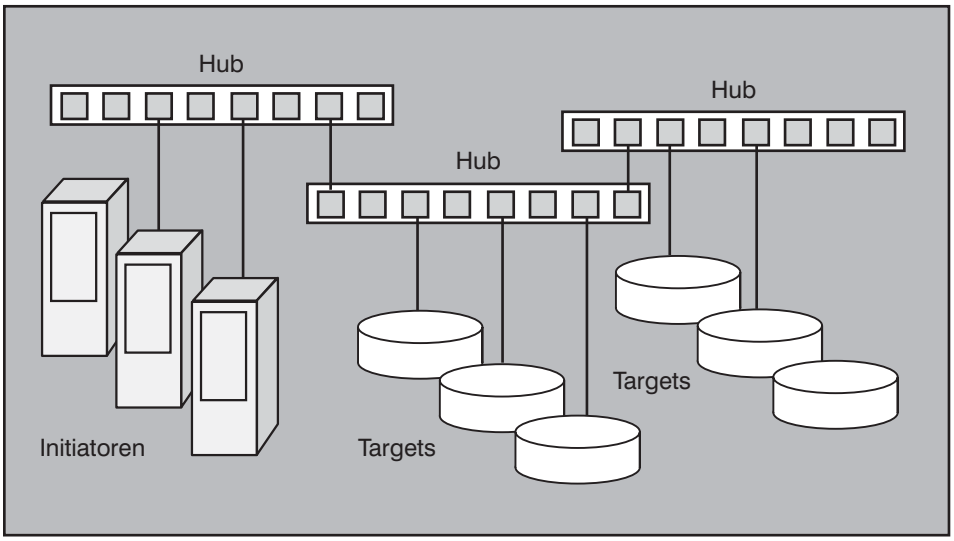


Abbildung 3: Hub-Kaskadierung

NL-Port mindestens 12 LIPs. Die Teilnehmer des Loops empfangen diese LIPs und gehen in den Open-Init-Zustand (Arbitrated Loop Open Initialize State). Alle laufenden Operationen werden dafür unterbrochen. Es wird ein temporary loop master mittels einer Loop Initialization Select Master Procedure (LISM) ausgewählt bzw. bestimmt. Dafür werden Frames als LISM-Signale von jedem Teilnehmer gesendet, wodurch jeder versucht Loop Master zu werden. Dafür werden die hexadezimalen Adresswerte des WWPN in dem LISM-Signal mit dem eigenen Adresswert verglichen und es wird ein LISM-Signal mit dem höheren Wert weitergeleitet und die eigenen LISM-siganle werden gestoppt.. Empfängt ein Teilnehmer ein LISM-Signal mit dem eigenen Wert, so ist dieser der Loop-Master. Dieser meldet dies den anderen Teilnehmern und im Anschluss erfolgt die Zuordnung der AL-PAs.

Um hier ständige Reinitialisierungen zu vermeiden, implementieren manche Hub-Hersteller Mechanismen zur Überbrückung von Stationen, die mehr als eine bestimmte Anzahl von Initialisierungsanforderungen pro Zeiteinheit schicken.
…

Sicherheit

Analog zu Mechanismen, die auf Serverebene implementiert sind und kontrollieren, welche Applikationen welche Geräte nutzen dürfen, ist es notwenig, ähnliche Maßnahmen in Speichernetzwerken zu implementieren. Ein im Server eingebauter HBA ermöglicht diesem den Zugriff auf entsprechende Geräte, in diesem Fall logische oder tatsächlich physikalische Festplatten eines Speichernetzwerkes. Dieser Zugriff muss sicherheitstechnisch betrachtet werden.

Hierfür wird zunächst auf eine Eigenart des Betriebssystems Windows in Bezug auf Plattenzugriffe hingewiesen. Wird ein Windowssystem an ein Speichernetzwerk angebunden, kann eine Festplatte eventuell über unterschiedliche Pfade angesprochen werden. Windows betrachtet eine solche Festplatte über jeden Pfad als separate neue Festplatte und geht dadurch von einer falschen Anzahl von Festplatten aus. Die nachfolgende Abbildung verdeutlicht dies. (siehe Abbildung 4)

Der Server verfügt über zwei HBAs, die an einen Switch angebunden sind. An diesen Switch ist ein Speichersystem angeschlossen, welches dem Windowsserver eine LUN zur Verfügung stellt. Diese Anbindung wird ebenfalls über zwei Pfade realisiert. In der Summe sieht das Windowssystem die eine LUN über vier Pfade

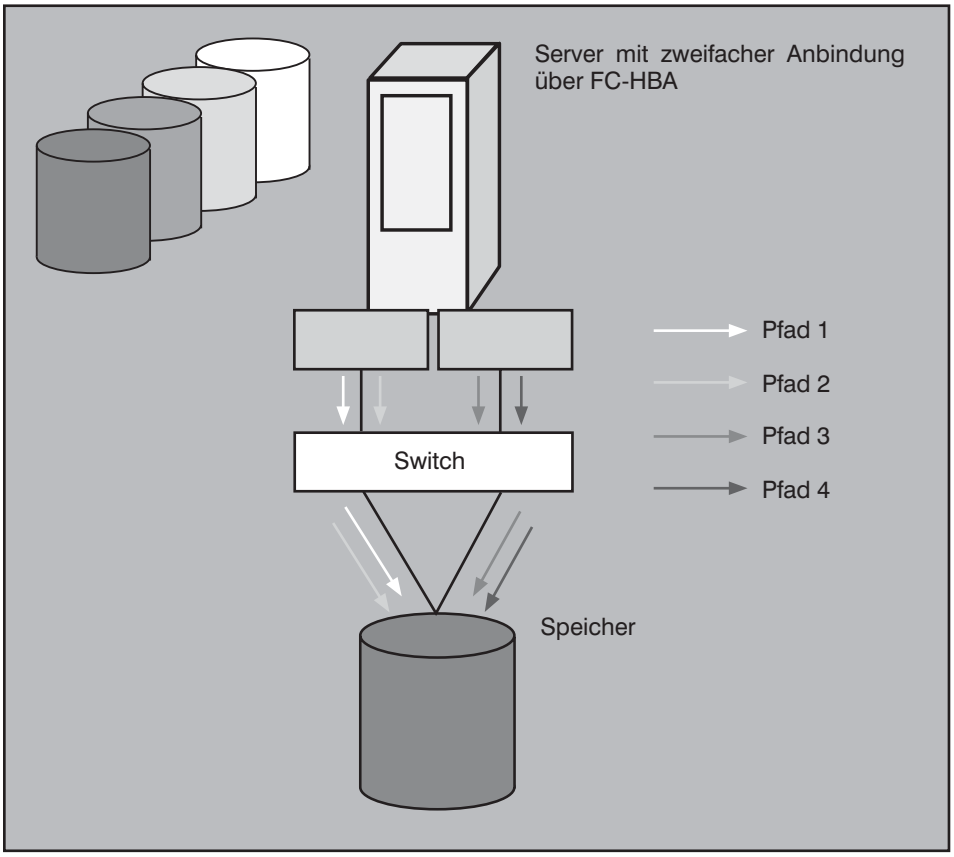


Abbildung 4: LUN-Ansicht eines Windowssystems

und interpretiert sie als vier eigenständige Festplatten. Diese Eigenart kann jedoch über separate Software, die weiter unten genauer betrachtet wird, gelöst werden.

Darüber hinaus schreibt jedes Windowssystem auf alle Festplatten, die gesehen werden, eine eigene Signatur. Dies gilt auch für alle LUNs, die für andere Windowssysteme oder für Ser-versysteme mit anderen Betriebssystemen vorgesehen sind. Bereits vorhandene Partitionie-rungen oder vorhandene Dateisysteme werden dabei ignoriert. Ohne entsprechende Sicher-heitsvorkehrungen führt dies definitiv zu Datenverlusten, weil vorhandenen Daten bei einem nicht autorisierten Zugriff überschrieben werden und damit verloren gehen.

Wie im Netzwerk und auf Betriebssystemebene verschiedene Mechanismen der irrtümlichen oder bewussten Veränderung von Daten und dem Verlust von Daten entgegenwirken, müssen auch in Speichernetzwerken geeignete Maßnahmen zum Schutz der Daten implementiert werden. Im Weiteren werden diese Maßnahmen detailliert betrachtet. Hierbei handelt es sich um das Zoning und das LUN-Masking, welches bereits in DAS-Umgebungen zum Einsatz kommt.

Zoning

Mittels Zoning werden logische Gruppen von Geräten bzw. Geräteteilen erstellt. Hierbei wer-den Switchports, HBA-Ports und Ports von Speichersystemen bzw. LUNs in so genannten Zonen zusammengefasst, um eine vereinfachte Zugriffsüberwachung und Zugriffssteuerung auf die Daten durchführen zu können. Geräten, die sich in einer gemeinsamen Zone befinden, wird die Kommunikation untereinander ermöglicht, während Geräten, die nicht aufgeführt sind, der Zugriff verweigert wird.

- Zonen werden auf den Switches innerhalb einer Fabric eingerichtet und konfiguriert.
- Zonen können sich über einen oder über mehrere Switches erstrecken.
- Änderungen an Zonen sind im laufenden Betrieb ohne Produktivunterbrechung möglich.
- Zoning kann nur in Speichernetzwerken, die über eine Fabric verfügen, implementiert werden.

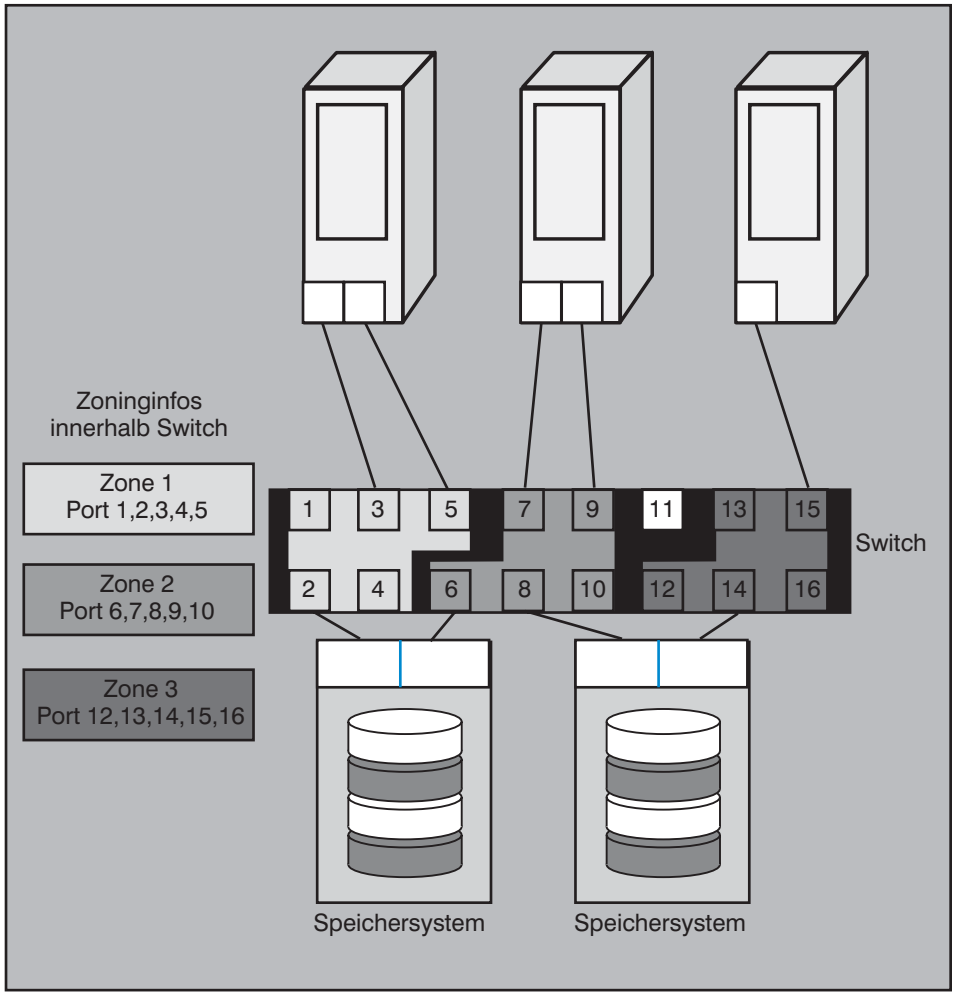


Abbildung 5: Beispiel für Hardzoning

Es gibt zwei grundsätzlich unterschiedliche Ansätze des Zonings: das Hard-Zoning, welches auch als Portzoning bezeichnet wird und das WWN-Zoning, welches wiederum auch als Softzoning bekannt ist.

Hard-Zoning

Mittels Hard-Zoning werden direkte strikte Zuordnungen zwischen Switchports definiert. Dies bedeutet, dass ein Port des Switches nur mit einem ganz bestimmten anderen Port dieses Switches oder eines anderen Switches innerhalb dieser Fabric Daten austauschen kann. Definiert man z.B. eine Zone mit Port 7 und 11, wobei an Port 7 ein Serversystem und an Port 11 ein Speichersubsystem (Speichersystem oder Tape-Library) angebunden ist, dann kann dieser Server nur über diesen Datenpfad (Serveradapter - Switchport 7 - Switchport 11 - Speichersystemadapter) eine Datenkommunikation aufbauen. Innerhalb des Switches wird der ent-sprechende Switchpoint für diesen Datenpfad aktiviert. Alle übrigen Ports dieser Fabric oder des Switches erhalten keine Kenntnis von der Datenkommunikation. Frames, die an ein Mitglied außerhalb der eigenen Zone gesendet werden, werden verworfen. Dieser Vorgang kann bei einigen Herstellern auch als Sicherheitsverletzung zu administrativen Zwecken protokolliert werden. Die nachfolgende Abbildung stellt das Hard-Zoning in einer Umgebung mit drei Zonen grafisch dar. (siehe Abbildung 5)

Fax-Antwort an ComConsult 02408/955-399

Bestellung Report

Moderne Speichertechnologien: Architekturen, Produkte und Migrationswege

☐ Ich bestelle den Report

Moderne Speichertechnologien
(Preis € 398.-- zzgl. MwSt. und Versand)
Erscheinungstermin Ende Dezember 2004

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

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

Schwerpunktthema

Wachsendes Interesse und verschiedene Verfahren für die Einteilung von LAN in getrennte Netze

Dr.-Ing. Behrooz Moayeri hat viele Großprojekte mit dem Schwerpunkt skalierbare Netze geleitet. Er gehört der Geschäftsleitung der ComConsult Beratung und Planung GmbH an und betätigt sich als Berater, Autor und Seminarleiter.

Fortsetzung von Seite 1

- In Fabriken umfasst die Vernetzung immer kritischere Bereiche wie die Steuerung von Fertigungsverfahren. Die für Büroumgebungen typischen Sicherheitsverfahren wie regelmäßige Virenschutz-Updates, fast wöchentliches Aufspielen von Security Hotfixes etc. können in den meisten Produktionsumgebungen nicht umgesetzt werden, z. B. weil der Hersteller einer Produktionsanlage zwar für Viren anfällige Betriebssysteme wie Windows verwendet, jedoch häufige Updates aus Sicherheitsgründen nicht vorgesehen hat. So waren in jüngster Vergangenheit einige Produktionsanlagen schadensstiftender Software schutzlos ausgeliefert. Viele Unternehmen erlitten dadurch gravierende Produktionsausfälle und trennen daher die Netze in ihrer Produktionsumgebung von anderen Bereichen wie z. B. dem Bürobereich.

- Zwar sind Wireless LAN mit den neuen Sicherheitsmechanismen nicht mehr so unsicher wie früher, aber viele Unternehmen halten eine Trennung zwischen der WLAN- und der LAN-Infrastruktur für sinnvoll, da z. B. von außen initiierte Denial-of-Service-Angriffe über Wireless LAN trotz der neuen Sicherheitsmechanismen möglich sind. Andere Motivationen dafür, WLAN sicherheitstechnisch anders zu behandeln als LAN, sind die Verwendung von WLAN als öffentliches Netz für Besucher aus anderen Firmen sowie die Aufstellung von WLAN Access Point in physikalisch nicht ausreichend zu schützenden Bereichen z. B. außerhalb von Gebäuden.

- Konventionelle Telekommunikationsanlagen weichen langsam aber sicher Voice over IP. Darin sehen viele Unternehmen das Risiko, dass sämtliche Angriffe und Sicherheitsprobleme, die es bisher in der Infrastruktur für Datenübertragung gegeben hat, nun auch die Telekommunikation betreffen. Einige Unternehmen versuchen, dieses Problem durch Trennung der Netze für VoIP und Daten in Griff zu bekommen.

Die Aufteilung von LAN in verschiedene Vertrauensbereiche kann auf diversen Ebenen implementiert werden. Je nach Sicherheitsanforderungen und -richtlinien, die Anlass zur Netztrennung geben, müssen sich die Netzverantwortlichen für eine der nachfolgend aufgeführten Varianten entscheiden.

Trennung auf der Ebene der passiven Infrastruktur

In einigen Fällen müssen nicht nur die zu unterschiedlichen Sicherheitsbereichen gehörenden Informationsströme, sondern auch die Zuständigkeiten für den Betrieb der zu trennenden Netze separiert werden. Zum Teil wird sogar gefordert, dass der eine Betreiber keinen Zugriff auf die aktive und passive Infrastruktur des vom anderen Betreiber verantworteten Netzes erhält. Konkret müssen z. B. getrennte Verteilerschränke und Schließsysteme vorgesehen werden. In diesen Fällen bleibt nichts anderes als die Trennung auf der Ebene der passiven Struktur (zusätzlich zur Trennung auf höheren Ebenen) übrig. Man kann dann höchstens Synergiepotenziale bei der Belegung von Technikräumen nutzen, vorausgesetzt, innerhalb dieser Technikräume werden getrennt gesicherte Schränke für die verschiedenen Bereiche aufgestellt.

Diese Art der Netztrennung stellt in der

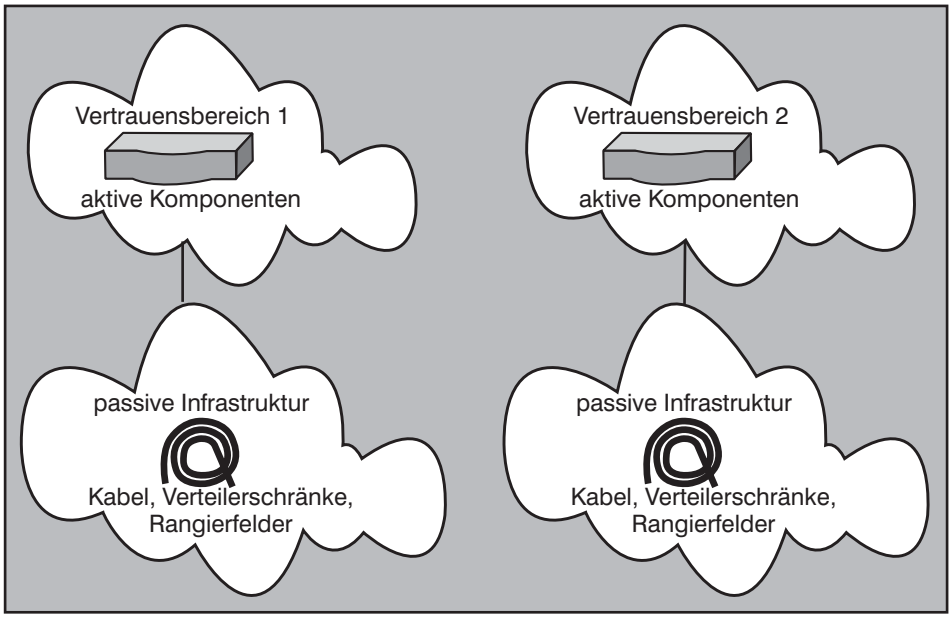


Abbildung 1: Getrennte passive und aktive Infrastruktur

Wachsendes Interesse und verschiedene Verfahren für die Einteilung von LAN in getrennte Netze

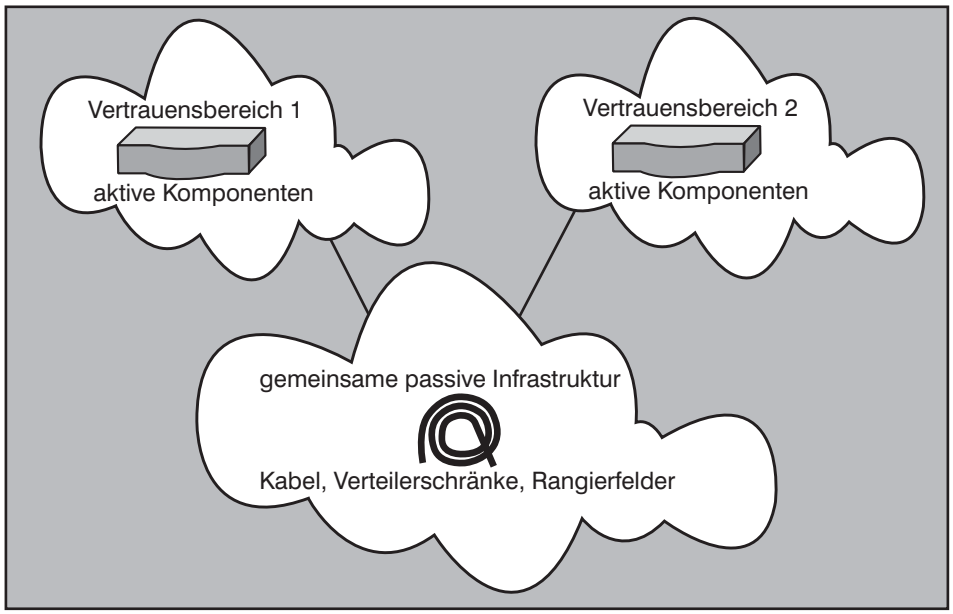


Abbildung 2: Getrennte aktive Komponenten, gemeinsame passive Infrastruktur

Regel keine technische, sondern eine wirtschaftliche Herausforderung dar. Sämtliche aktive und passive Bestandteile des Netzes müssen mehrfach beschafft und betrieben werden.

Trennung aller aktiven Bestandteile

Trennung aller aktiven Bestandteile: Viele Unternehmen akzeptieren zwar den gemeinsamen Zugriff verschiedener Betreiber auf die selbe passive Infrastruktur bzw. die Übertragung der Aufgaben im Zusammenhang mit der passiven Infrastruktur auf eine gemeinsame Instanz, nicht jedoch die gemeinsame Nutzung von aktiven Netzkomponenten. Dafür gibt es verschiedene Gründe wie die Befürchtung, dass die Risiken durch die gemeinsame Nutzung der gleichen aktiven Komponenten von den Informationsströmen verschiedener Vertrauensbereiche nicht vollständig ausgeschlossen werden können (was eine berechtigte Befürchtung ist). Werden beispielsweise die Netzkomponenten selbst von einem Wurm angegriffen, hilft die Trennung auf VLAN-Ebene meistens wenig. So werden zwar die selben passive Komponenten wie Verteilerschränke und Rangierfelder von verschiedenen Sicherheitsbereichen genutzt, jedoch getrennte aktive Netzkomponenten wie Switches und Router eingesetzt. In diesem Fall kann auch die Betriebszuständigkeit für diese aktiven Komponenten auf einfache Weise getrennt werden.

In einem solchen Szenario der Netztrennung ist die Definition der passiven Infrastruktur von entscheidender Bedeutung. Was zählt zur passiven, was zur aktiven Infrastruktur? Ist es akzeptabel, die passive Infrastruktur etwas großzügiger zu definieren und zum Beispiel rein optische Multiplexer diesem Teil der Infrastruktur zuzuordnen? Man stelle sich ein Gelände vor, in dem verschiedene Netzbereiche zu implementieren sind. Statt für die verschiedenen Bereiche im Geländebereich eigene Lichtwellenleiterpaare vorzusehen, kann man optische Multiplexer einsetzen, auf denen verschiedene Netzbereiche unterschiedliche Wellenlängen erhalten. Die Motivation für den Einsatz solcher Multiplexer besteht oft darin, den Aufwand für die Verlegung neuer Glasfaserkabel einzusparen, wenn die Fasern der vorhandenen Kabel ausgeschöpft sind. Wenn die verschiedenen Gebäude durch öffentliche Straßen etc. von einander getrennt sind, muss in der Regel Dark Fiber von Providern angemietet werden. Auch in solchen Szenarien ist es oft wirtschaftlicher, statt der Erhöhung der Zahl der Glasfasern optische Multiplexer einzusetzen.

Im dargestellten Beispiel verbindet ein optischer Backbone vier Gebäude miteinander. Der Backbone besteht aus vier optischen Multiplexern und der ringförmig angeordneten LWL-Verkabelung zwischen diesen. In jedem Gebäude sind die beiden zu trennenden Netzbereiche mit eigenen aktiven Komponenten vertreten. Die aktiven Komponenten jedes Vertrauensbereichs werden in jedem Gebäude mit einem Port des optischen Multiplexers verbunden, der für den Bereich vorgesehen ist. (siehe Abbildung 3)

Es ist in einem solchen Szenario zu klären, wem der Betrieb der optischen Multiplexer zu übertragen ist. Solche Multiplexer weisen zwar keine sehr hohe Änderungsdynamik auf wie herkömmliche Netzkomponenten, müssen aber genauso wie die-

Sicherheits-Lösungen: Von den Einzelbausteinen

14.02. - 18.02.05 in Bonn

Dieses Seminar vermittelt, aus welchen Bausteinen eine effiziente Sicherheits-Lösung aufgebaut wird, welche Bausteine unverzichtbar sind und wie diese Bausteine konfiguriert werden. Jeder einzelne Baustein wird detailliert erklärt und in seinen Potenzialen beschrieben. An vielen typischen Einsatzszenarien wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt.

Referenten: Dipl.-Inform. Andreas Meder, Dipl.-Ing. Hans Peter Mohn
Preis: € 2.290,- zzgl. MwSt.

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

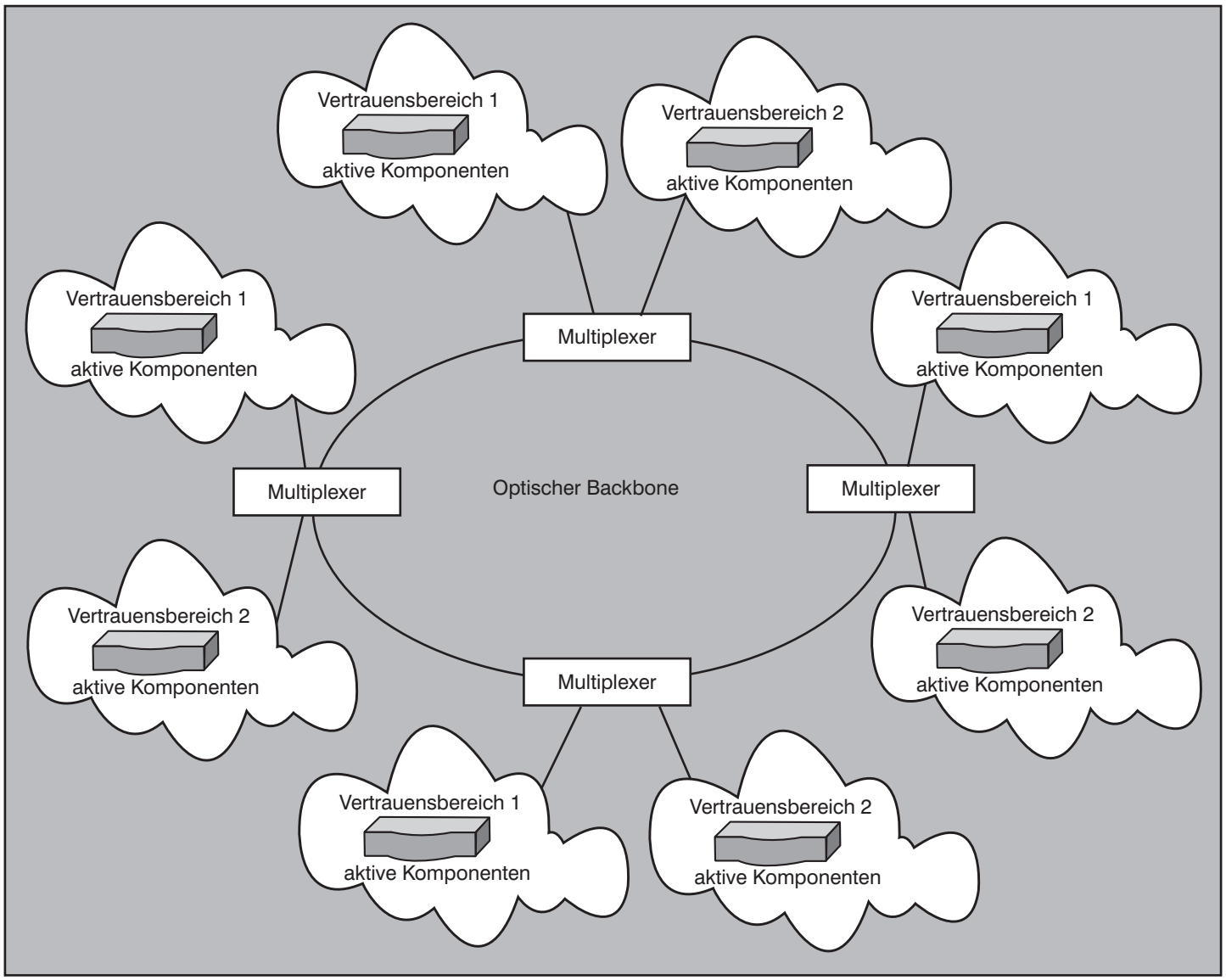


Abbildung 3: Einsatz optischer Multiplexer

se überwacht und gewartet werden.

Trennung auf VLAN-Ebene

Aus wirtschaftlichen Gründen versuchen viele Unternehmen, den durchgängigen Einsatz getrennter aktiver Komponenten für verschiedene Sicherheitsbereiche zu vermeiden und bei aktiven Komponenten Synergieeffekte zu nutzen.

Meistens bedeutet dies die Definition getrennter Virtueller LAN auf der Basis der selben aktiven Komponenten. Somit können verschiedene Ports eines Layer-2-Switches zu unterschiedlichen Vertrauensbereichen gehören, vorausgesetzt, alle Vertrauensbereiche einigen sich auf einen Modus für den Betrieb und den Zugriff auf den Layer-2-Switch selbst. Die zu diesen verschiedenen Ports gehörenden Pakete werden auf den Verbindungen des Switches zu anderen Netzkomponenten gemäß dem Standard IEEE 802.1Q unterschiedlich markiert. Technisch bedeutet dies, dass eine durchgängige Layer-2-Struktur realisiert wird.

Zu einer solchen Struktur gehört bei Bedarf nach ausfallsicheren Netzen der Redundanzmechanismus der Schicht 2, d. h. Spanning Tree (nach dem konventionellen Verfahren gemäß dem Standard IEEE 802.1D oder dem leistungsfähigeren Verfahren gemäß dem Standard IE-EE 802.1w).

Die Aufteilung der Layer-2-Infrastruktur in verschiedene VLAN ist ein Verfahren zur Netztrennung und unabhängig davon, wie die verschiedenen VLAN miteinander verbunden werden (falls eine VLAN-übergreifende Kommunikation erforderlich ist). (siehe Abbildung 4)

Die Bildung von VLAN ist eines der in Unternehmensnetzen verbreitetsten Verfahren, um Netzbereiche voneinander zu trennen. Jeder Netzadministrator, der bei der Konfiguration von LAN-Switches nicht ganz unerfahren ist, kann VLAN einrichten und Switch-Ports den VLAN zuordnen. In Netzen bis zu einer bestimmten Größenordnung verursacht ein solches Netzdesign keine besonderen Herausforderungen an den Betreiber.

Gleichwohl weisen Konzepte auf der Basis des exzessiven Einsatzes von VLAN zur Netztrennung einige Einschränkungen auf:

- Broadcast-Stürme, die in einem Vertrauensbereich entstehen, können sich auf die Verfügbarkeit der gemeinsamen

Wachsendes Interesse und verschiedene Verfahren für die Einteilung von LAN in getrennte Netze

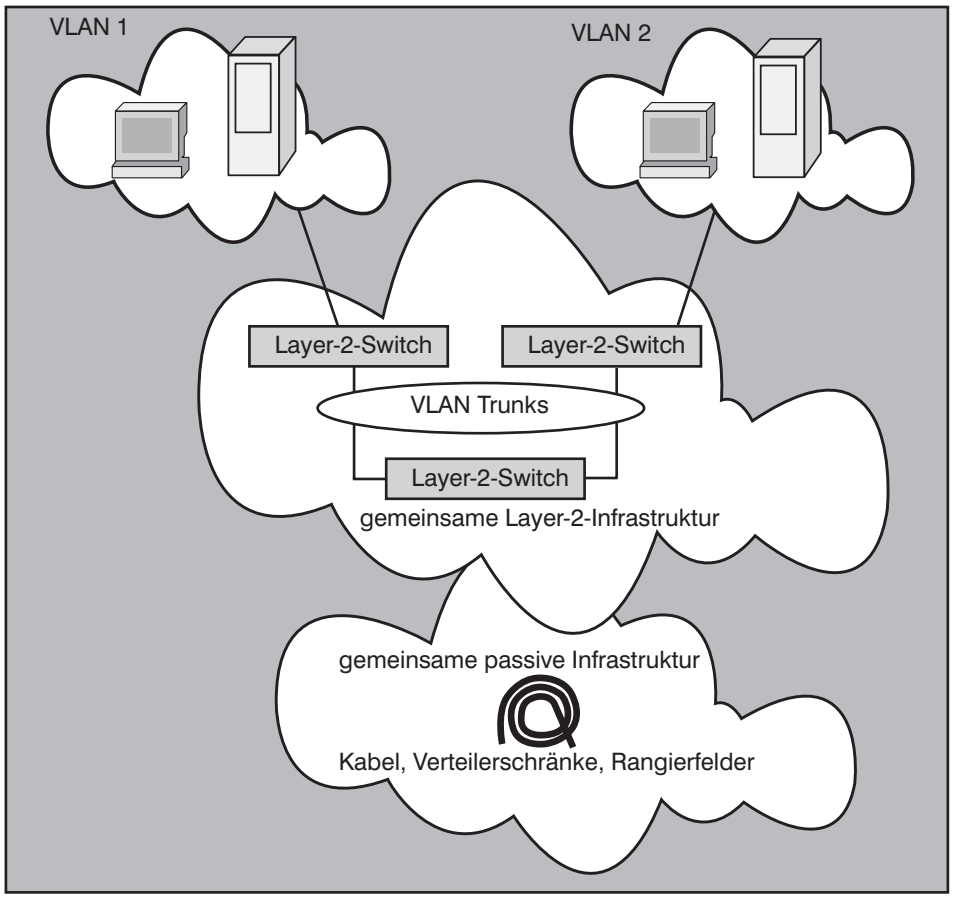


Abbildung 4: VLAN-Trennung

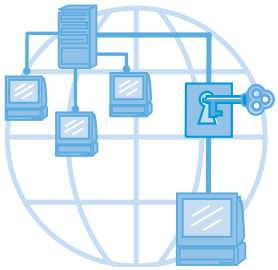
Layer-2-Infrastruktur für die anderen Vertrauensbereiche negativ auswirken. Zwar ist es bei manchen Netzkomponenten möglich, Höchstgrenzen für die Übertragung von Broadcasts zu setzen, jedoch unterstützen die am meisten verbreiteten preiswerten Layer-2-Switches solche Funktionen in der Regel nicht.

- Die Flutung von Unicasts durch die Fehlkonfiguration von Servern oder ähnliche Ursachen kann ein weiteres Problem darstellen, das in einem VLAN entsteht und andere VLAN mit beeinträchtigt. Zwar ist es bei einigen (bei Weitem nicht allen) Netzkomponenten möglich, die von einem VLAN beanspruchte Netzkapazität zu begrenzen, jedoch ist von der Aktivierung eines solchen Mechanismus aus mehreren Gründen abzuraten. Erstens können dadurch in Phasen von Verkehrsspitzen Pakete verloren gehen. Zweitens büßt das Netz Synergiepotenziale ein, weil künstliche Grenzen für die Dynamik des Verkehrs gesetzt werden (als ob man zwischen verschiedenen Spuren einer Autobahn eine bauliche Trennung vorsehen würde).

- Viren und Würmer, die sich in einem VLAN ausbreiten, legen unter Umständen die auch von anderen VLAN genutzten aktiven Netzkomponenten lahm.

- Im Falle der Notwendigkeit redundanter Netzstrukturen führt in den meisten Layer-2-Netzen an Spanning Tree kein Weg vorbei. Obwohl die neue im Standard IEEE 802.1w spezifizierte Variante von Spanning Tree einen wesentlichen Nachteil der alten Variante, nämlich die langsame Konvergenz bei Netzänderungen, behoben hat, bleiben einige mit Spanning Tree verbundene Probleme weiter bestehen. Dazu zählt zum Beispiel der Umstand, dass manchmal eine verlorene BPDU (Bridge Protocol Data Unit, ein Paket, in dem Steuerungsinformationen gemäß Spanning Tree enthalten sind) aus, um ein ganzes Netz zu destabilisieren. Spanning Tree muss von den Prozessoren der Netzkomponenten mit oberster Priorität bearbeitet werden und konkurriert somit mit anderen Netzsteuerungsmechanismen wie Routing-Protokollen. Es kommt daher hin und wieder vor, dass sich durch Spanning-Tree-Probleme entstehende instabile Zustände im Netz über Layer-2-Brodcast-Domänen hinaus ausbreiten. Deshalb wird allgemein empfohlen, die Zahl der Komponenten in einer Spanning-Tree-Domäne zu begrenzen.

Sicherheits-Lösungen: IP-VPNs



28.02. - 02.03.05
in Bonn

VPN-Technologie hat sich zu einer der wichtigsten Technologien innerhalb von Netzwerken entwickelt. Dabei reicht die Einsatz-Spannbreite von der Standort-Kopplung über Remote Access bis zur sicheren Notebook-Kommunikation und zur Absicherung von Wireless LAN´s. Diese Vielfalt macht den Stellenwert dieser Technologie deutlich. Ebenso vielfältig wie die Nutzungsformen sind die Realisierungs-Alternativen und die Integration in bestehende Netzwerk-Infrastrukturen. Aufgaben wie die optimale Kombination eines VPN-Servers mit Firewall/Routing/NAT oder die Klärung der Microsoft-spezifischen Fragen auf den Client-PC´s (Interoperabilität, Anmeldung, Namensauflösung) sind typisch für die Komplexität der VPN-Nutzung.

Referenten: Dipl.-Inform. Andreas Meder, Alexander Zarenko
Preis: € 1.690,- zzgl. MwSt.

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

Wachsendes Interesse und verschiedene Verfahren für die Einteilung von LAN in getrennte Netze

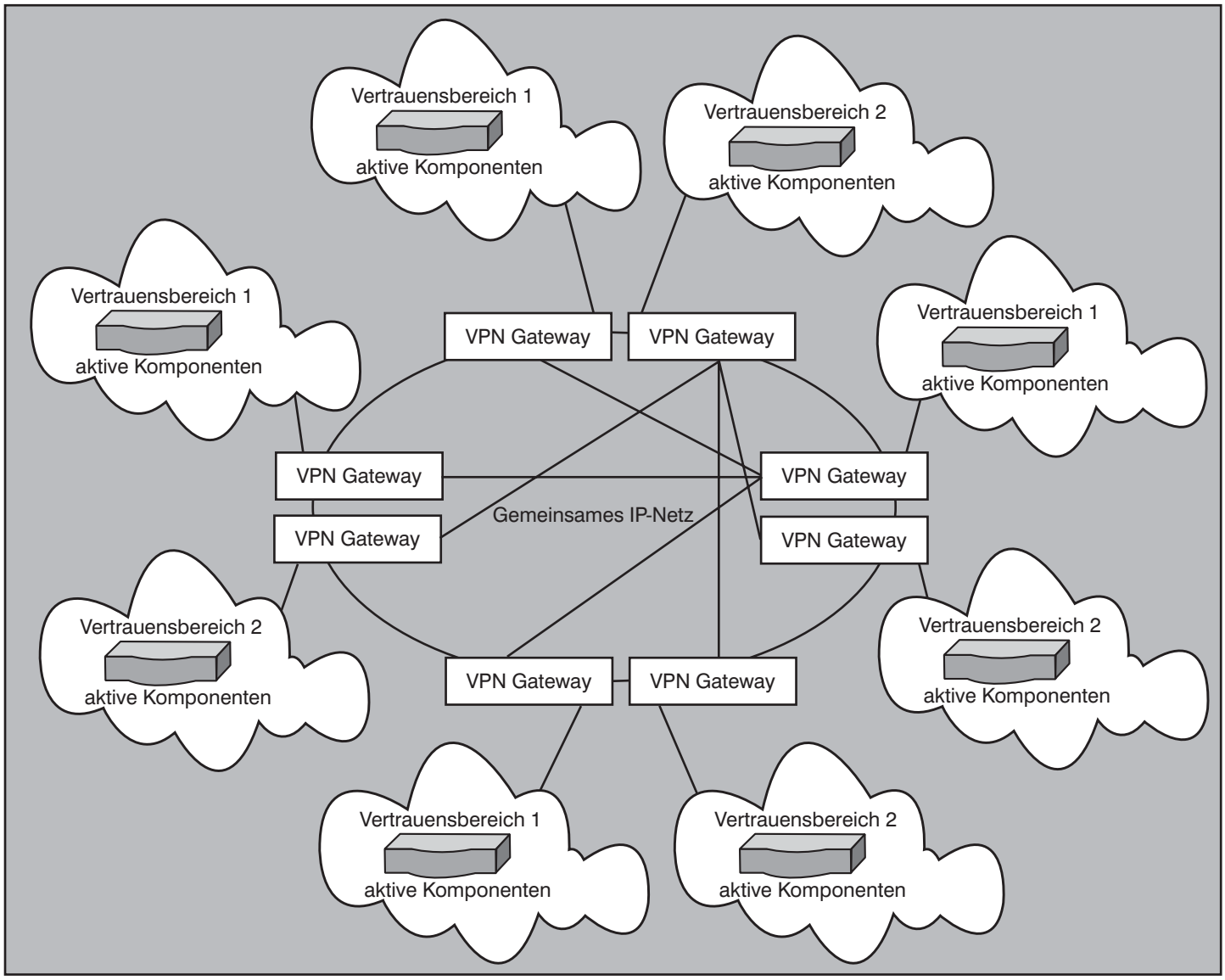


Abbildung 5: Nutzung eines gemeinsamen IP-Netzes durch verschiedene VPN

- Ab einer bestimmten Größe des Netzes und der Zahl der VLAN ist die manuelle Einrichtung von Änderung an VLAN-Zuordnungen zu aufwändig und fehleranfällig. Viele Netzbetreiber greifen daher zum Hilfsmittel proprietärer Protokolle, über die sich die Netzkomponenten Informationen über VLAN-Zuordnungen austauschen. Solche hersteller-spezifische Mechanismen bergen die Gefahr der Abhängigkeit von einem einzigen Hersteller in sich. Komponenten verschiedener Hersteller können in solchen Netzen nicht gemischt werden. Man ist auf die Verwendung der Produkte eines Herstellers angewiesen, was strategisch vom Nachteil sein kann.

- Allgemein sind gemeinsam genutzte aktive Komponenten mit dem Problem verbunden, dass der Betreiber Wartungsarbeiten mit den Verantwortlichen für alle VLAN abstimmen muss. Oft werden deshalb überhaupt keine Wartungsfenster für solche Arbeiten wie Software Updates gefunden. Deshalb ziehen es einige Netzbetreiber vor, zumindest im Access-Bereich auf die VLAN-Trennung zu verzichten und dort jedes Netz auf der Basis eigener Komponenten zu implementieren. Da Access-Switches meistens nicht redundant ausgeführt werden, sind Wartungsarbeiten an diesen Switches mit einer Service-Unterbrechung verbunden, die im Falle des Verzichts auf deren gemeinsame Nutzung durch verschiedene Bereiche nur mit einem Bereich abgestimmt werden muss. Die Kosten für Access-Switches sind meistens relativ niedrig, sodass die Aufstellung getrennter Access-Komponenten für verschiedene Netzbereiche wirtschaftlich vertretbar ist. Übergeordnete Komponenten im Distribution- und Core-Bereich werden häufig redundant ausgelegt, so dass Wartungsarbeiten nicht zwangsläufig mit Service-Unterbrechungen einhergehen. Diese zentralen Komponenten können von verschiedenen zu trennenden Bereichen gemeinsam genutzt werden, ohne dass dies an der Problematik der Wartungsfenster scheitern muss. Aber auf solchen zentralen Komponenten werden häufig Layer-3-Funktionen benötigt, sodass dort die Netztrennung auf VLAN-Ebene nicht ausreicht.

Vor dem Hintergrund dieser Einschränkungen ist die Netztrennung auf VLAN-Ebene in vielen Fällen zumindest nicht ausreichend.

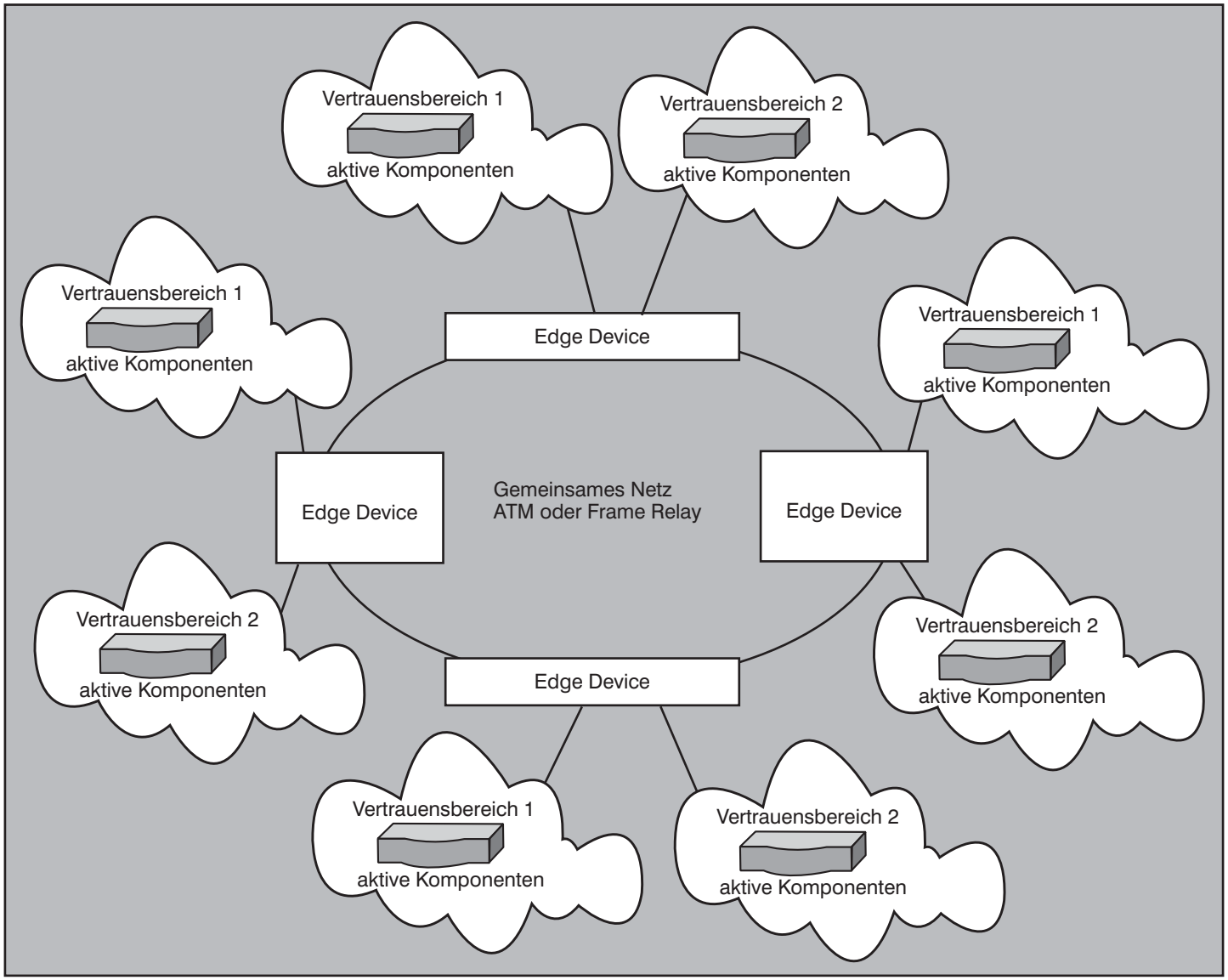


Abbildung 6: Gemeinsamer Layer-2-Backbone

Trennung auf VPN-Ebene

Verschiedene Vertrauensbereiche können auf verschiedene Virtual Private Networks (VPN) abgebildet werden. Das gängigste Verfahren für die VPN-Bildung ist IPsec. Dabei werden über die selbe IP-Infrastruktur verschlüsselte Tunnels aufgebaut. Die Trennung der Informationsströme erfolgt mittels Authentifizierung beim Anschluss an die VPN sowie durch Verschlüsselung. (siehe Abbildung 5)

Im dargestellten Beispiel nutzen zwei verschiedene VPN, auf die zwei verschiedene Vertrauensbereiche abgebildet sind, ein gemeinsames IP-Netz als Transportmedium. Durch dieses gemeinsame Netz werden Tunnel aufgebaut, deren Endpunkte als VPN Gateways bezeichnet werden. Diese verschlüsseln den Verkehr des angeschlossenen Vertrauensbereiches und übertragen den verschlüsselten Verkehr zu anderen Gateways des selben Vertrauensbereiches, die wiederum den Verkehr entschlüsseln. Alle VPN Gateways eines Vertrauensbereiches können beispielsweise sternförmig an einen zentralen Gateway des selben Bereiches angeschlossen sein.

Der Nachteil dieses Verfahrens liegt vor allem in den Kosten für die Beschaffung und den Betrieb von VPN-Komponenten sowie den Leistungseinbußen durch Verschlüsselung. Dieser Nachteil gilt nicht für einige andere VPN-Verfahren, die aus dem Providerbereich stammen. Im Providerbereich gibt es als Standardfall die Forderung, dass verschiedene Kunden die selbe Infrastruktur nutzen, ohne dass ihre Netze sich gegenseitig sehen oder stören können. Dieser Forderung sind die Provider jahrelang gerecht geworden, indem sie durch ein gemeinsames Layer-2-Netz auf der Basis von Frame Relay (FR) oder ATM (Asynchronous Transfer Mode) für jeden Kunden dedizierte Verbindungen aufgebaut haben. Die Endpunkte dieser Verbindungen sind ausschließlich für einen Kunden (einen Vertrauensbereich) vorgesehene Layer-3-Komponenten. (siehe Abbildung 6)

Auch in einigen Campusnetzen sind Netztrennungsverfahren auf der Basis von ATM zum Einsatz gekommen. So können zum Beispiel verschiedene Emulated LAN (ELAN) auf der Basis des selben ATM-Netzes als logisch getrennte, jedoch auf der selben physikalischen Plattform beruhende Layer-2-Backbones für getrennte Netzbereiche fungieren.

Wachsendes Interesse und verschiedene Verfahren für die Einteilung von LAN in getrennte Netze

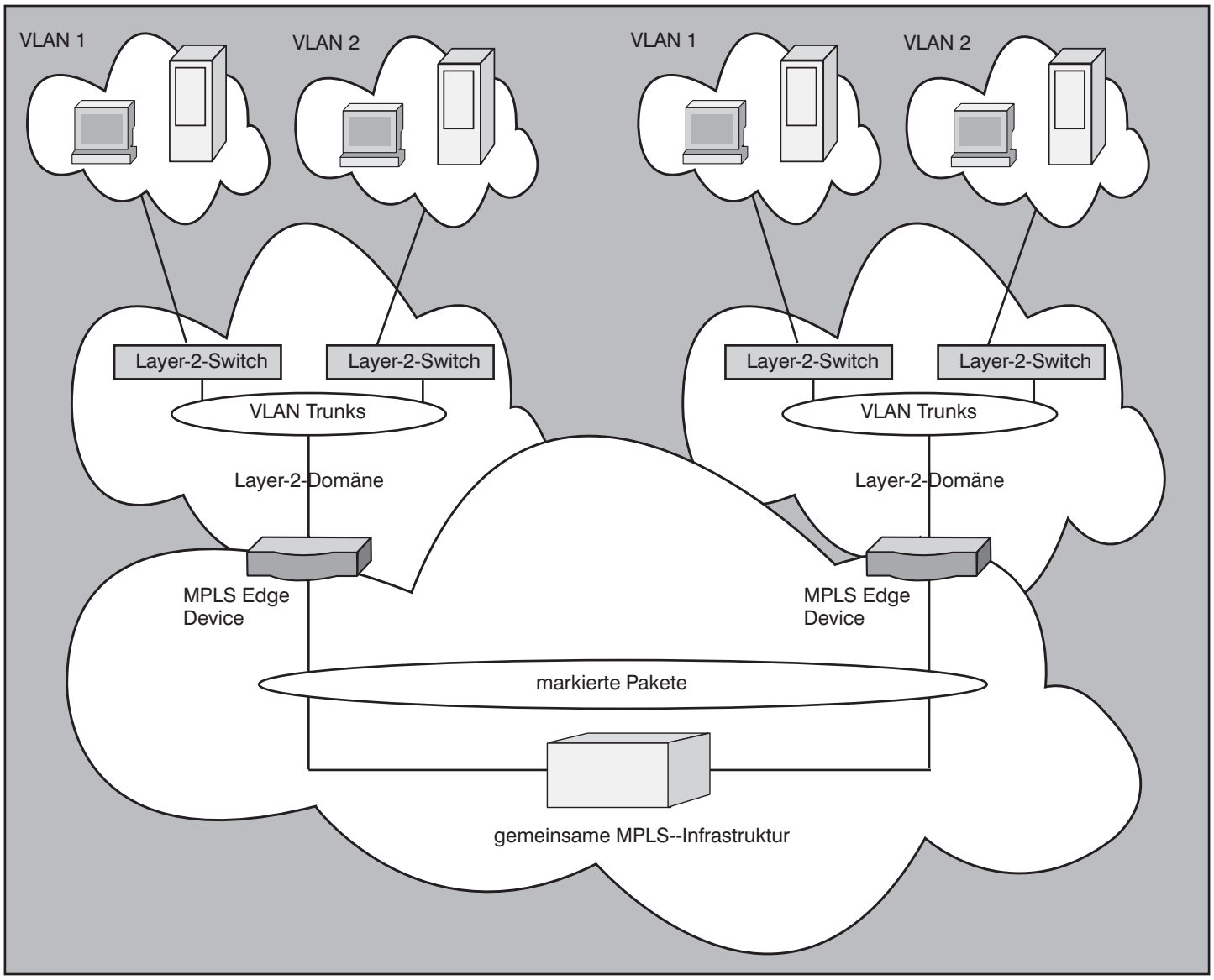


Abbildung 7: Kombination aus MPLS und VLAN

VPN auf Layer-2-Basis haben den Nachteil, dass der Backbone-Bereich nicht flexibel in dem Sinne aufgebaut werden kann, dass je nach Stand der Technik eine Mischung von Layer-2-Verfahren zum Einsatz kommt. Ein ATM-Netz bleibt ein ATM-Netz, bis es durch ein anderes Netz abgelöst wird. Layer-2-VPN sind zu starr und unflexibel. Außerdem ist der Aufbau eines vermaschten VPN auf der Basis von oft eingesetzten Permanent Virtual Circuits (PVC) in einem ATM- oder FR-Netz mit einem nicht zu vernachlässigenden Konfigurationsaufwand verbunden. Diesbezüglich besser sind solche Verfahren wie LAN Emulation oder MPLS einzustufen, die von vornherein in einem ELAN bzw. VPN eine Any-to-any-Kommunikation unterstützen. LAN Emulation hat jedoch andere Probleme, insbesondere hinsichtlich der Skalierbarkeit und Komplexität, weshalb dieses Verfahren als absterbende Technologie gilt.

Bei Providern ist mittlerweile das Verfahren Multiprotocol Label Switching (MPLS) Stand der Technik der Netztrennung. Dieses Verfahren sieht analog zu VLAN und ELAN vor, dass die zu verschiedenen VPN gehörenden Pakete bei der Übertragung über die IP-Infrastruktur unterschiedlich markiert werden. Der Nachteil von MPLS besteht darin, dass Layer-2-Komponenten, die in den meisten LAN den Access-Bereich dominieren, MPLS nicht unterstützen. So muss MPLS zusammen mit anderen Verfahren eingesetzt werden, wenn damit ein LAN in unterschiedliche Sicherheitsbereiche aufzuteilen ist. Denkbar ist die Kombination von MPLS im Bereich der Layer-3- und VLAN im Bereich der Layer-2-Komponenten. Das Netz wird beispielsweise in einen MPLS-Backbone und angeschlossene Layer-2-Domänen aufgeteilt (es kann sich dabei um das Geländebackbone bzw. um die Gebäudenetze handeln). Im MPLS-Backbone werden in der Anzahl der benötigten getrennten Vertrauensbereiche VPN gebildet. Einem solchen VPN wird pro Layer-2-Domäne die entsprechende VLAN-Schnittstelle der zuständigen Layer-3-Komponente zugewiesen. (siehe Abbildung 7)

Bisher stellt ein MPLS-Backbone immer eine Layer-3-Routing-Instanz dar. Werden zwei Standorte des selben VPN über ein MPLS-Netz miteinander verbunden, gibt es zwischen diesen beiden Standorten eine Layer-3- und keine Layer-2-Kopplung. Dies kann zum Beispiel im Vergleich zu einem standortübergreifendem VLAN den Nachteil bedeuten, dass bestimmte Verfahren nicht

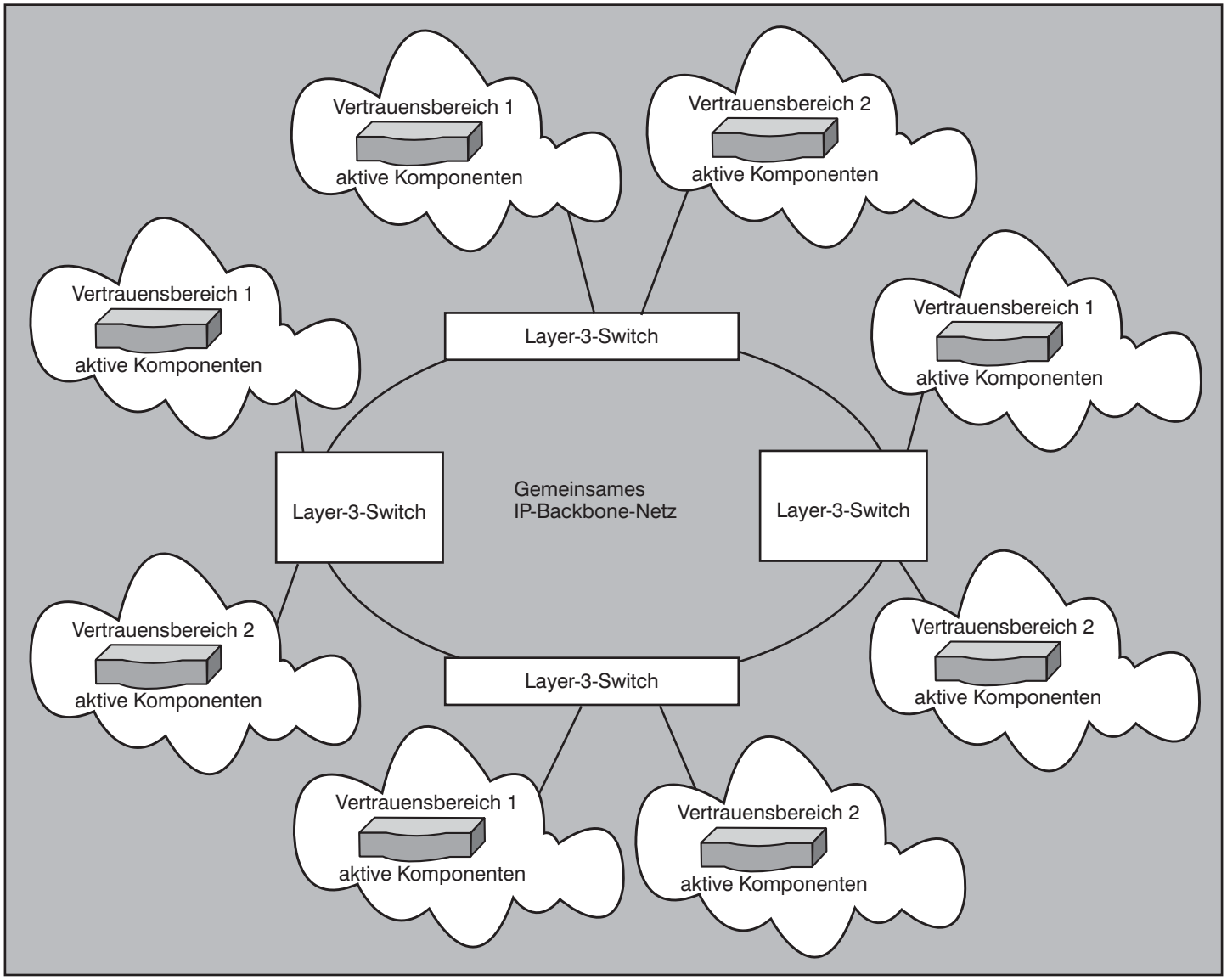


Abbildung 8: Layer-3-Kopplung zwischen Netzbereichen

unterstützt werden. Zu solchen Verfahren gehören beispielsweise Cluster-Mechanismen, die allein deshalb eine Layer-2-Verbindung zwischen den Standorten benötigen, weil ein und die selbe IP-Adresse von einem Knoten am ersten Standort zu einem Knoten am zweiten Standort wandern muss. Viele Server-Cluster werden so aufgebaut.

MPLS unterstützt bisher solche Anforderungen nicht. Dieser Nachholbedarf wurde bereits von den für die MPLS-Standardisierung zuständigen Gremien innerhalb der Internet Engineering Task Force (IETF) erkannt. Nun arbeitet die IETF am so genannten Virtual Private LAN Service (VPLS, Emulation von LAN über eine MPLS-Wolke), Virtual Private Wire Service (VPWS, Punkt-zu-Punkt-Verbindungen, u. a. Punkt-zu-Punkt-Ethernet-Verbindungen, über eine MPLS-Wolke) sowie IP-only L2 VPNs, einem Dienst, der IP-Endgeräten die Möglichkeit gibt, über eine MPLS-Wolke so zu kommunizieren, als ob sie an das selbe IP-Subnetz angeschlossen wären.[1]

Wie bereits erwähnt, löst die reine Netztrennung noch nicht das Problem, wie die so getrennten Netzbereiche miteinander kommunizieren. So wie es die Netztrennung auf verschiedenen Ebenen gibt, sind auch Kopplungsverfahren auf verschiedenen Ebenen denkbar.

Unabhängig von den Verfahren für die Trennung der Netzbereiche ist häufig das Problem zu lösen, dass diese Netzbereiche trotz der die Netztrennung veranlassenden Sicherheitsrichtlinien gekoppelt werden müssen. Entweder besteht Bedarf nach direkter Kommunikation zwischen den getrennten Netzen, oder von diesen Netzen aus müssen gemeinsame Dienste wie z. B. Internet-Kommunikation genutzt werden. Die Kopplung verschiedener Teilnetze kann auf verschiedenen Ebenen erfolgen.

Layer-3-Kopplung

In einigen Fällen, insbesondere dann, wenn es zwischen den getrennten Netzbereichen sehr vielfältige und häufige Änderungen aufweisende Kommunikationsbeziehungen gibt und sich die Sicherheitsrichtlinien in den verschiedenen Bereichen nicht gravierend unterscheiden, verbindet man die verschiedenen Bereiche über einfache Layer-3-Kopplungen miteinander. Konkret bedeutet dies, dass jeder Bereich auf ein eigenes IP-Subnetz oder eigene IP-Subnetze eines gemeinsamen großen IP-Netzes abgebildet wird. Die verschiedenen Bereiche sind somit

[1] siehe Beschreibung von Layer 2 Virtual Private Networks (l2vpn) unter: http://www.ietf.org/html.charters/l2vpn-charter.html

Wachsendes Interesse und verschiedene Verfahren für die Einteilung von LAN in getrennte Netze

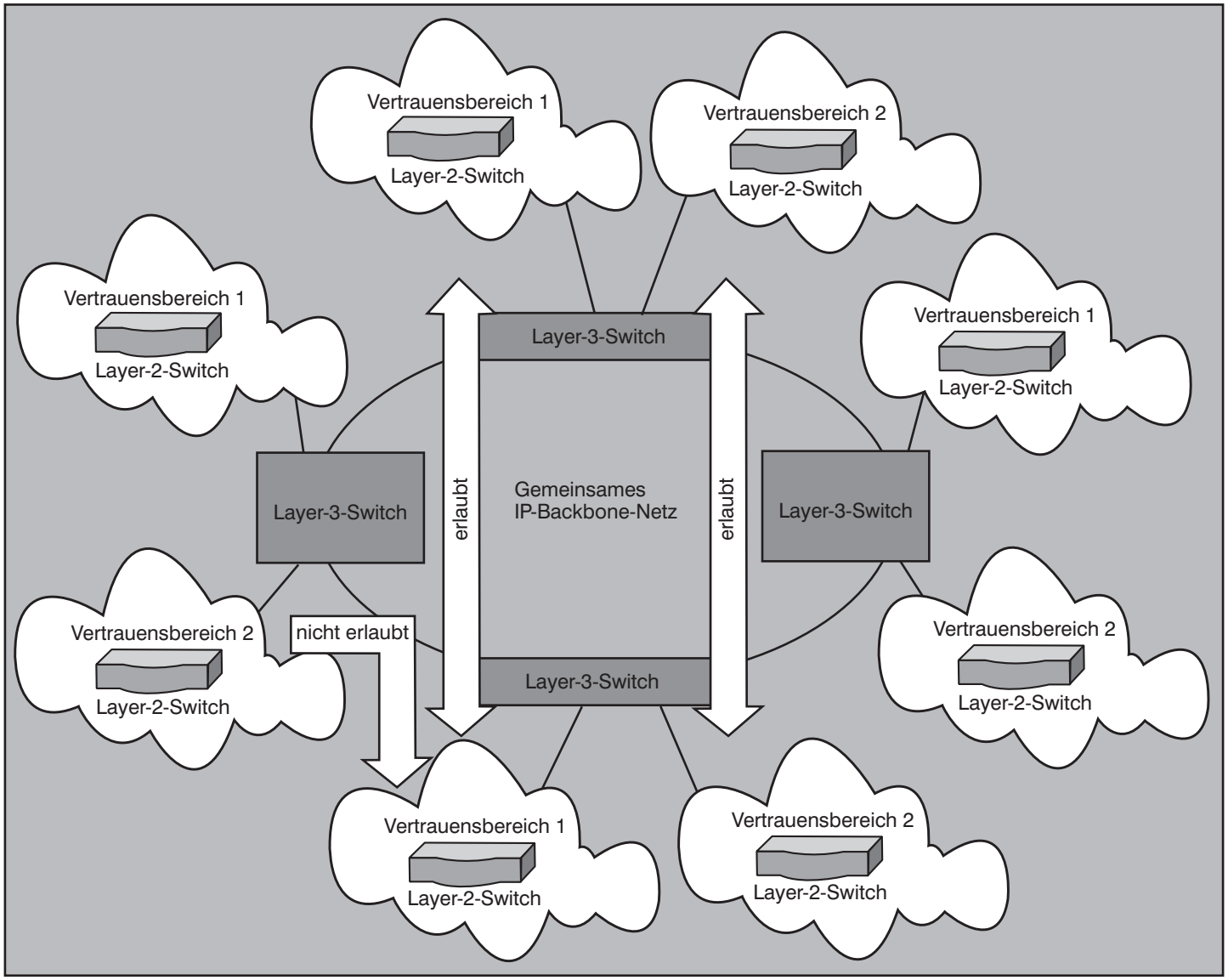


Abbildung 9: Einsatz von Paketfiltern

nicht stark voneinander getrennt, so dass sich z. B. Viren von einem zum anderen Bereich ausbreiten können. Gewisse Risiken können trotzdem reduziert werden, wie z. B. die durch Layer-2-Netzprobleme oder Broadcast Storms verursachten Risiken. (siehe Abbildung 8)

Einige Unternehmen trennen auf diese Art beispielsweise ihre Büro- von ihrer Produktionsumgebung. Büroendgeräte wie PC werden nicht an die selben Layer-2-Switches angeschlossen, die der Vernetzung von Endgeräten in der Produktion wie z. B. Robotter und Steuerungen dienen. In einigen Fällen wird eine Produktionsanlage 1:1 auf ein IP-Subnetz bzw. eine Broadcast-Domäne abgebildet. Diese Broadcast-Domäne nimmt ausschließlich Endgeräte der Produktionsanlage auf und ist über Layer-3-Switches mit anderen Subnetzen verbunden, zum Beispiel mit zentralen Rechnern, mit denen alle Produktionsanlagen im Netz kommunizieren müssen.

Wenn keine weiteren Maßnahmen ergriffen werden, kann in einem solchen Netz jedes Endgerät eines Vertrauensbereiches mit jedem anderen Endgerät eines anderen Vertrauensbereiches kommunizieren. Dies bedeutet, dass es sich bei der reinen Layer-3-Kopplung um ein Verfahren handelt, das die Netztrennung eigentlich weitgehend aufhebt.

Kopplung über Paketfilter

Die meisten Unternehmen stufen über gemeinsame Layer-3-Komponenten gekoppelte IP-Subnetze nur dann als verschiedene Sicherheitsbereiche ein, wenn mindestens einige Filterregeln und Zugriffslisten für die Einschränkung der bereichsübergreifenden Kommunikationsbeziehungen sorgen.

Technisch wäre eine solche Maßnahme als Paketfilter zu bezeichnen. Ein Paketfilter vergleicht die von einem zum anderen Subnetz zu übertragenden Pakete mit vordefinierten Mustern. Je nach Übereinstimmung mit diesen Mustern werden die Pakete entweder übertragen oder blockiert. Die für die Definition der Paketmuster verwendeten Masken können auf verschiedene Merkmale des Paketes angewandt werden. Meistens werden IP-Adressen oder Teile davon, die Protokollkennung im IP-Header oder Portnummern im TCP/UDP-Header als Masken verwendet. Paketfilter können entweder auf der Basis von Layer-3-Switches oder Routern oder mittels

Firewall-Systeme realisiert werden. (siehe Abbildung 9)

Im dargestellten Beispiel werden auf den Layer-3-Switches Regeln definiert, die für die Entscheidung über die Übertragung von Paketen ausschlaggebend sind. Beispielsweise kann vorgegeben werden, dass aus dem Vertrauensbereich 2 (zum Beispiel einer Büroumgebung) aus keine TCP-Verbindungen mit Endgeräten des Vertrauensbereichs 1 aufgebaut werden dürfen. Dies wird technisch so umgesetzt, dass jedes Paket, das dem Muster des ersten Paketes einer TCP-Verbindung entspricht, nur in einer Richtung übertragen werden darf. Das erste Paket einer TCP-Verbindung weist eine einmalige Belegung der so genannte SYN- und ACK-Flags (zwei Bits im TCP-Header) auf, die in keinem der folgenden Paketen einer Verbindung verwendet wird. Durch die Vorgabe, dass Pakete dieses Musters nur in einer Richtung übertragen werden dürfen, kann erzwungen werden, dass TCP-Verbindungen nur in einer Richtung auf-gebaut werden können. Gleichzeitig können zum Beispiel UDP- oder ICMP-Pakete völlig von der Übertragung ausgeschlossen werden.

Bei Filterregeln, die in der Bedienersyntax der Netzkomponenten häufig als Access Control Lists (ACL) bezeichnet werden, kann man zwischen positiven und negativen Filtern unterscheiden. Entweder man lässt alle Kommunikation bis auf die ausdrücklich verbotenen Kommunikationsbeziehungen zu oder umgekehrt, das heißt eine Kommunikationsbeziehung wird nur dann unterstützt, wenn sie explizit zugelassen wird.

Die größte Herausforderung bei der Arbeit mit ACL besteht darin, die Übersicht zu behalten und keine derart komplexen Regelwerke zu definieren, die in der Praxis des Netzbetriebs unbeherrschbar sind. Einige Unternehmen wenden zur Bewahrung von übersichtlichen Regeln ein IP-Adressschema an, das die Abbildung sowohl geografischer als auch organisatorischer Gegebenheiten unterstützt. Das folgende Beispiel verdeutlicht dieses Verfahren:

Ein Netz wird unter Anwendung privater Adressen mit IP-Subnetzen aus dem Bereich 10.0.0.0 bis 10.255.255.255 versorgt. Das zweite Oktett der IP-Adresse kann zu einem geografischen und das dritte Oktett zu einem organisatorischen Merkmal werden. So kann zum Beispiel einem geografischen Bereich der Adressraum 10.1.0.0 und darin jedem organisatorischen Bereich ein eigenes Subnetz zugeordnet werden, zum Beispiel 10.1.1.0 dem Vertrauensbereich 1, 10.1.2.0 dem Vertrauensbereich 2 etc. Die Filterregeln in jedem geografischen Bereich können dann bis auf das unterschiedliche zweite Oktett identisch sein, beispielsweise 10.x.1.0 kann Verbindungen mit 10.x.2.0 aufnehmen, umgekehrt jedoch nicht.

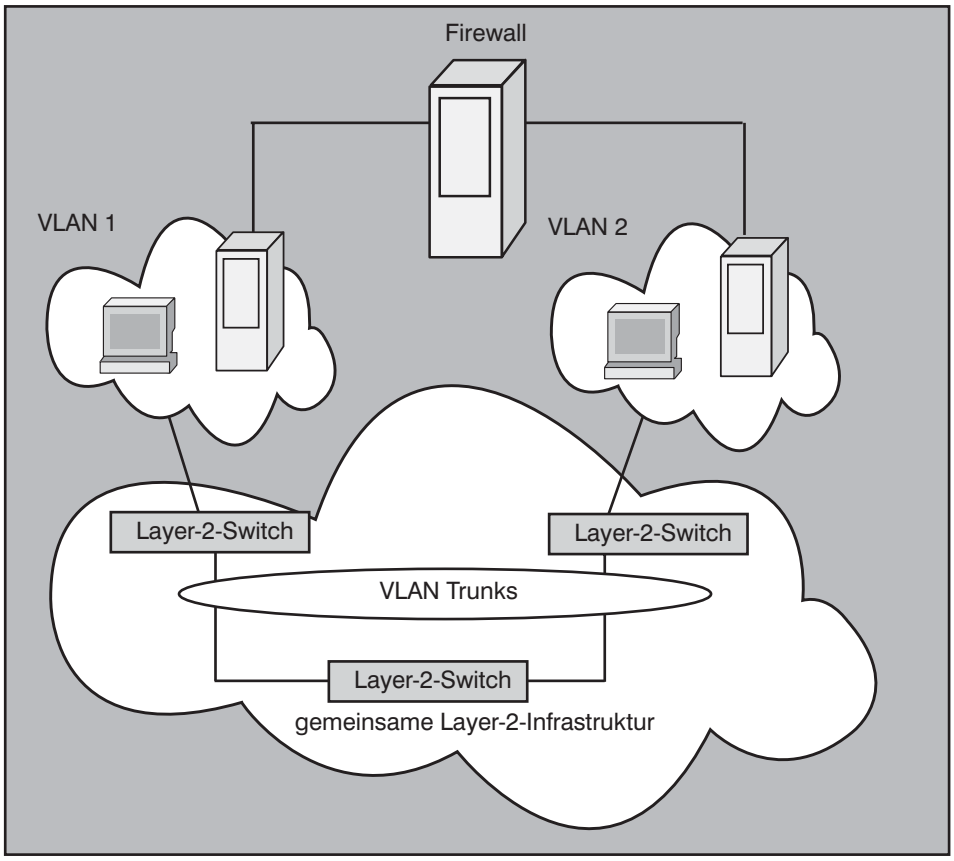


Abbildung 10: Kopplung mittels Firewalls

Problematisch wird ein solcher Ansatz dann, wenn aufgrund von Adressengpässen eine solche zweidimensionale Aufteilung des Adressraums nicht möglich ist. Dann kann man zwar immer noch eine feinere Strukturierung des Adressraums anwenden, indem man beispielsweise ein Oktett in zwei jeweils aus vier Bits bestehende Hälften unterteilt, die erste Hälfte für die geografische Strukturierung und die zweite Hälfte für die organisatorische Strukturierung verwendet, aber die Übersichtlichkeit wird dadurch sicherlich reduziert.

Kopplung auf Firewall-Ebene

Der wichtigste Vorteil von Firewalls liegt darin, dass sie über die reine Paketfilterung hinaus komplexere Überprüfungsmechanismen anbieten, die in dem Fall eingesetzt werden können, wenn bei bestimmten Kommunikationsbeziehungen die reine Prüfung auf Paketebene als Sicherheitsmechanismus nicht ausreicht. Ein Firewall-System kann unter Umständen für bestimmte Protokolle eine Überprüfung auf Paketebene und bei anderen Entscheidungshilfen auf Anwendungsebene anwenden, wozu ein Layer-3-Switch oder Router in der Regel nicht in der Lage ist. Darunter sind zu erwähnen:

- Kopplung mit Prüfung auf Verbindungsebene: Einige Firewalls unterstützen das Konzept der so genannten Stateful Inspection. Dabei wird überprüft, ob ein Paket zum Kontext einer bereits aufgebauten, zulässigen Verbindung passt. Nur solche Pakete werden durchgelassen. Das Firewall-System ist in dem Sinne „statusbewusst“, dass es den Status aufgebauter Verbindungen kennt.

- Kopplung mittels Application Level Gateways (ALG): Als ALG bezeichnet man solche Firewalls oder Gateways, welche die Kommunikation zwischen zwei verschiedenen Netzen nur im Rahmen einer bestimmten Applikation zulassen. Ein E-Mail Relay ist ein ein-faches Beispiel für einen ALG. Ein anderes Beispiel ist ein HTTP Proxy, der auf der Applikationsebene sowohl eine Authentifizierung als auch Prüfungen des zu übertragenden Inhalts vornehmen kann.

Wachsendes Interesse und verschiedene Verfahren für die Einteilung von LAN in getrennte Netze

Einige Unternehmen setzen zum Beispiel Firewalls ein, um getrennte Vertrauensbereiche wie die Büro- und die Produktionsumgebung oder die Daten- und die Sprachumgebung miteinander zu koppeln. (siehe Abbildung 10)

Zum Beispiel können sämtliche IP-Telefone in einem Netz einem und alle Datenendgeräte einem anderen VLAN zugeordnet werden. Ein Firewall-System kann dann die beiden Bereiche miteinander koppeln, da diverse Kommunikationsbeziehungen zwischen den beiden Bereichen notwendig sind. So muss z. B. ein Unified-Messaging-Server (UM-Server) sowohl mit dem IP-Telefonie-Server als auch mit dem E-Mail-Server kommunizieren. Der Telefonieserver muss dem Telefonie-VLAN und der E-Mail-Server dem Daten-VLAN zugeordnet werden. Der UM-Server kann alternativ an die folgenden Bereiche angeschlossen werden:

- An den Telefoniebereich: Dann muss eine Firewall-Regel dafür sorgen, dass zum Beispiel Voice Mails als Dateianhänge von E-Mail-Nachrichten vom UM-Server zum E-Mail-Server gelangen.
- An den Datenbereich: Dann ist dafür zu sorgen, dass die Signalisierung zwischen dem UM-Server und dem Telefoniebereich sowie die Übertragung von Voice-Nachrichten vom Telefoniebereich zum UM-Server über das Firewall-System unterstützt wird.
- An einen dritten Bereich, der sowohl mit dem Daten- als auch mit dem Telefoniebereich kommuniziert.

Ein anderes Beispiel ist die Trennung zwischen der Büro- und der Produktionsumgebung, die oft über Firewalls miteinander verbunden sind. Auch in diesem Beispiel muss dafür gesorgt werden, dass sämtliche bereichsübergreifende Kommunikationsbeziehungen auf Firewallregeln abgebildet werden, ohne dass die Firewalls durch zu allgemeine Regeln überflüssig werden.

Schwierigkeiten in der Praxis

Dem Leser wird kaum entgangen sein, dass die o. g. Kopplungsverfahren in der Reihenfolge eines steigenden Sicherheitsniveaus geordnet sind. ALG gelten als die Koppelelemente mit dem höchsten Sicherheitsniveau, weil sie anders als alle anderen aufgeführten Hilfsmittel auf der Ebene von Anwendungen agieren und somit Angriffe erkennen und abwehren können, die auf den unterhalb der Applikationsebene liegenden Levels nicht erkennbar sind. Zugleich können die ALG jedoch auch Prüfungen auf niedrigeren Ebenen durchführen und zum Beispiel die Kommunikation mit bestimmten IP-Adressen oder Protokollen unterbinden. Ein ALG überträgt keine Pakete von einem zum anderen Netz, sondern gilt als Kommunikationsendpunkt auf beiden Seiten. So werden viele Risiken durch die Paketübertragung von einem zum anderen Netz erst gar nicht entstehen.

Die Kehrseite der Medaille ist, dass für die meisten Anwendungen kein ALG verfügbar ist. Insbesondere bei der unternehmensinternen Kommunikation werden im großen Maße auch Protokolle und Anwendungen verwendet, die keinem etablierten Marktstandard entsprechen. Gerade für solche Kommunikationsbeziehungen fehlen ALG, während die gängigsten Protokolle, die bei der Kommunikation über das Internet verwendet werden, in der Regel mittels ALG abgesichert werden können.

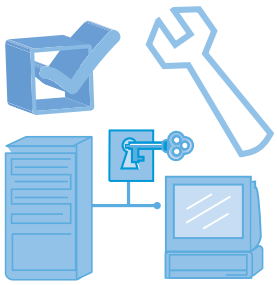
Deshalb ist es bei vielen Unternehmen üblich, die Perimeter Security mittels ALG und die Trennung des internen Netzes in verschiedene Bereiche mithilfe von Paketfiltern zu implementieren.

Nach der bisherigen Betrachtung ist es zwar möglich, Verfahren für die Netztrennung mit Verfahren für die Kopplung zu kombinieren und somit den Anforderungen für die Unterteilung von LAN in verschiedene Vertrauensbereiche gerecht zu werden, aber diese Betrachtung wäre unvollständig, wenn wir nicht auf Schwierigkeiten in der Praxis hinweisen würden. Exemplarisch gehen wir auf einige Probleme ein, die im Zusammenhang mit dem Einsatz von VoIP entstehen können.

Muss die Sprachübertragung über IP auch zwischen verschiedenen Vertrauensbereichen unterstützt werden, liegt die Herausforderung darin, Firewall-Regeln sowohl für Hard- als auch für Soft-Phones zu definieren. Dabei sind mindestens folgende Kommunikationsbeziehungen zu berücksichtigen:

- Der Sprachtransport über das Real-time Transport Protocol (RTP) muss zwischen beliebigen zwei Endgeräten sowie diesen und beliebigen Gateways unterstützt werden, es sei denn, verschiedene Vertrauensbereiche werden mittels Proxy-Systeme gekoppelt, die zwischen den VoIP-Endgeräten in verschiedenen Bereichen vermitteln. Die Schwierigkeit bei RTP besteht darin, dass die Portnummern dynamisch ausgehandelt werden.
- Eine weitere Schwierigkeit besteht darin, dass für die meisten gängigen VoIP-Signalisierungsprotokolle, die bei der Steuerung von IP-Telefonen durch Telefonieserver verwendet werden, keine Proxies verfügbar sind und einige dieser Signalisierungsverfahren dynamische, verschachtelte Verbindungen nutzen.
- IP-Telefone beziehen in der Regel ihre IP-Adressen von DHCP-Servern. Entweder muss pro Vertrauensbereich mindestens

Sicherheits-Lösungen: Planung und praktische Konfiguration



18.04. - 22.04.05
in Aachen

Dieses einmalige Seminar vermittelt intensiv innerhalb von 5 Tagen den praktischen Umgang mit Firewall, VPN, Windows-Sicherheit und WLAN-Sicherheit. Im Rahmen von praktischen Live-Übungen werden typische Konfigurationen analysiert und vermittelt. Als Übungsbasis stehen typische Produkte des Marktes zur Verfügung, die vermittelten Konfigurationen sind aber nicht produktspezifisch sondern auf jedes ähnliche Produkt direkt übertragbar. Die Teilnehmer werden so in die Lage versetzt, dieses Wissen direkt nach dem Seminar aktiv in der Praxis einzusetzen.

Referent: Heiko Kieckbusch, Dipl.-Inform. Andreas Meder,
Dipl.-Ing. Hans Peter Mohn, Alexander Zarenko
Preis: € 2.290,- zzgl. MwSt.

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

Wachsendes Interesse und verschiedene Verfahren für die Einteilung von LAN in getrennte Netze

ein DHCP-Server oder eine Firewall-Regel für DHCP-Kommunikation vorgesehen werden.

- Werden die Telefone von zentraler Stelle aus gemanaget, ist sicherzustellen, dass beispielsweise SNMP-Kommunikation zwischen dieser zentralen Stelle und den Endgeräten möglich ist.

Kann man Hard-Phones unter Umständen noch an der IP-Adresse erkennen, gilt dies für Soft-Phones nicht. Zu den o. g. Schwierigkeiten kommt bei Soft-Phones hinzu, dass ein Soft-Phone wie jede andere Anwendung auf einem Datenendgerät (in der Regel einem PC) die IP-Adresse des Endgerätes nutzt und somit anhand der IP-Adresse nicht erkennbar ist.

Mangels „VoIP-bewusster“ Firewalls, insbesondere im Bereich der im VoIP-Markt noch dominierenden herstellerspezifischen Signalisierungsverfahren, besteht die Lösung für diese Probleme meistens in der aus Security-Sicht nicht optimalen Öffnung von Adress- und Portbereichen bei der Kommunikation zwischen verschiedenen Teilnetzen.

Fazit

Ein zunehmender Bedarf nach Einteilung von LAN in verschiedene Vertrauensbereiche ist feststellbar, sei es aufgrund organisatorischer Veränderungen oder wegen der unterschiedlich zu behandelnden Netze in Büro- und Produktionsumgebungen, bei drahtgebundenen und drahtlosen Verfahren und durch die Verbreitung von VoIP. Sowohl für die Trennung als auch für die Kopplung der verschiedenen Netzbereiche sind unterschiedliche Verfahren denkbar, die miteinander kombiniert werden können.

Die Entscheidung für ein Verfahren ist von den Sicherheits- und sonstigen Anforderungen (Wirtschaftlichkeit, Managebarkeit, Leistungsfähigkeit) in einer bestimmten Umgebung abhängig. Netzverantwortliche, die ein Konzept für Netztrennung und die Kopplung der getrennten Netze ausarbeiten, müssen rechtzeitig die genannten Anforderungen aufnehmen und bei der Entscheidung für jedes Verfahren die Schwierigkeiten berücksichtigen, die es z. B. in der Praxis der Netztrennung bei gleichzeitiger Unterstützung neuer Peer-to-Peer-Anwendungen wie Voice gibt.

In jedem Fall geht die Trennung eines LAN in unterschiedliche Vertrauensbereiche mit einem Redesign größeren Ausmaßes einher.

AKTUELLER REPORT

Design-Varianten Lokaler Netzwerke im Vergleich

Die aktuelle Studie analysiert detaillierte Beispiele realer Netzwerke unter zukunftsstrategischen, technologischen und kostenmäßigen Gesichtspunkten und zeigt auf, dass neue kostengünstige und hochperformante Designvarianten eine Reihe sinnvoller Alternativen zu den von den Herstellern vermarkteten, sternförmig redundanten Layer-3-Konzepten darstellen.

Zum Inhalt

- Das Design Lokaler Netzwerke ist historisch gewachsen und bedarf in vielen Fällen einer Optimierung.
- Moderne Switching-Verfahren in Kombination mit modernen Switching-Architekturen ermöglichen eine wirtschaftliche Optimierung und eine deutliche Senkung der Betriebskosten.
- Die zunehmende Verbreitung von Gigabit-Ethernet im Endgerätebereich und die Erweiterung der Backbone-Kapazitäten erfordern eine Neukalkulation der Buchungsfaktoren und ein entsprechendes Redesign.
- Service-Level-Zusagen für Netzwerke werden vermehrt gefordert, insbesondere für kritische Anwendungen und Sprachübertragungen. Aktuelle Design-Verfahren bieten eine Reihe sinnvoller Alternativen.
- Der steigende Kostendruck zwingt die Betreiber, über Alternativen zu den von den Herstellern vermarkteten, sternförmig redundanten Layer-3-Konzepten nachzudenken.
- Neue Standards bieten seit Kurzem kostengünstige und hochperformante Designvarianten an.

Vor diesem Hintergrund analysiert die aktuelle Studie von ComConsult-Research die bestehenden Design-Varianten Lokaler Netzwerke unter zukunftsstrategischen, technologischen und kostenmäßigen Gesichtspunkten. Sie bildet die ideale Basis für ein Redesign bestehender Netzwerke, aber auch eine optimale Grundlage für jede Neuplanung.

Die Studie zeigt auf:
- welche Design-Alternativen existieren
- was sich in den letzten Monaten geändert hat
- was in den nächsten Monaten noch kommen wird
- wie mit modernen Verfahren und aktuellen Produkten ein optimales Netzwerk-Design entsteht

Autoren: Markus Schaub, Dipl.-Inform. Petra Borowka
Preis: € 398,- plus Porto und Versand zzgl. MwSt.

Buchen Sie über unsere Web-Seite **www.comconsult-research.com**

CCNE

ComConsult Certified Network Engineer

Lokale Netze
21.02. - 25.02.05 in Aachen
25.04. - 29.04.05 in Aachen
27.06. - 01.07.05 in Aachen
12.09. - 16.09.05 in Aachen
28.11. - 02.12.05 in Aachen

Internetworking
13.12. - 17.12.04 in Aachen
28.02. - 04.03.05 in Aachen
30.05. - 03.06.05 in Aachen
26.09. - 30.09.05 in Aachen
28.11. - 02.12.05 in Aachen

TCP/IP und SNMP
11.04. - 15.04.05 in Berlin
20.06. - 25.06.05 in Köln
26.09. - 30.09.05 in Berlin
21.11. - 25.11.05 in Bonn

Ethernet Technologien - neuester Stand
14.03. - 18.03.05 in Aachen
20.06. - 24.06.05 in Aachen
19.09. - 23.09.05 in Aachen
14.11. - 18.11.05 in Aachen

Paketpreis für alle vier Seminare € 8.170.-- 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
21.02. - 25.02.05 in Aachen
06.06. - 10.06.05 in Aachen
12.09. - 16.09.05 in Aachen
07.11. - 11.11.05 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen
14.02. - 18.02.05 in Aachen
30.05. - 03.06.05 in Aachen
24.10. - 28.10.05 in Aachen

Trouble Shooting in geswitchten Ethernet-Umgebungen
11.04. - 15.04.05 in Aachen
04.07. - 08.07.05 in Aachen
17.10. - 21.10.05 in Aachen
28.11. - 02.12.05 in Aachen

Paketpreis für alle drei Seminare € 7.500.-- zzgl. MwSt.
(Einzelpreise: je € 2.490.--)

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

CCSE

ComConsult Certified Security Expert

Sicherheitslösungen I: Von den Einzelbausteinen zur integrierten Lösung
14.02. - 18.02.05 in Bonn
25.04. - 29.04.05 in Bonn
06.06. - 10.06.05 in Köln
26.09. - 30.09.05 in Nürnberg

Sicherheitslösungen II: IP-VPNs, der Kern einer Sicherheits-Infrastruktur
28.02. - 02.03.05 in Bonn
30.05. - 01.06.05 in Köln
19.09. - 21.09.05 in Bonn
07.11. - 09.11.05 in Köln

Sicherheitslösungen III: Planung und praktische Konfiguration
18.04. - 22.04.05 in Aachen
27.06. - 01.07.05 in Aachen
17.10. - 21.10.05 in Aachen
05.12. - 09.12.05 in Aachen

Paketpreis für alle drei Seminare € 5.330.-- zzgl. MwSt.
(Einzelpreise: € 2.290.-- / € 1.690.-- / € 2.290.--)

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

Impressum

Verlag:
Dr. Suppan International institute b.v
Ahornenlaan 12
4493 DG Kamperland, Niederlande
BTW-Nr.: NL 808 482 683 B01
Handelsregister Nr. 22044734 0000

Telefon (0049)02408/955-400
Fax (0049)02408/955-399
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

Erscheinungweise: 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
© Dr. Suppan International Institute b.v.