ComConsult Research

# Der Netzwerk Insider

Juni 2005

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

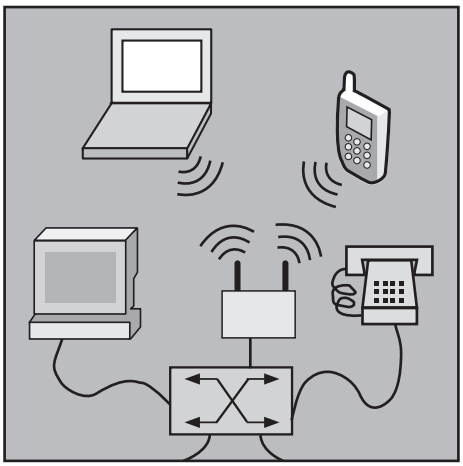
Schwerpunktthema

# Technologietrends für Enterprise Redesign: Wireline und Wireless für PAN, LAN, MAN, RAN

**von Dipl.-Inform. Petra Borowka - Teil 3**

In den vorangegangenen zwei Teilen haben wir die verschiedenen aktuellen Wireless und Wireline Technologien beschrieben und anhand wesentlicher Design-Kriterien bewertet. Dieser Artikel befasst sich mit der strukturierten Integration beider Welten sowie angemessener Provisionierung von Sicherheit und Dienstgüte.

Für ein strukturiertes Redesign von Enterprise Netzwerken haben wir ein allgemeingültiges Konzept enwickelt, das einerseits hierarchisch aufgebaut ist, andererseits ein angemessenes Maß an Design-Flexibilität zur Betriebs- und Kostenoptimierung ermöglicht.



**4. Strukturiertes Netzdesign zur Integration von Wireless und Wireline: LND**

**4.1 Flexible Netzstrukturen für angemessene Skalierbarkeit und Verfügbarkeit: LND-Xn**

**Schrittweise hierarchische Integration von Wireless**
Es gelten nach wie vor die in vielen Praxis-Projekten erprobten Design-Grundsätze:

weiter auf Seite 19

Zweitthema

# Schnelle Konvergenz im Access-Bereich

**von Dipl.-Ing. Harald Krause**

Im Rahmen des (Re-)Designs eines lokalen Netzes ist in der Regel zu entscheiden, wie die Endanwender im so genannten Access-Bereich an das übergeordnete Netzwerk angebunden werden. Aufgrund der immer weiter fortschreitenden Automatisierung von Geschäftsvorgängen im LAN und den daraus resultierenden steigenden Anforderungen an die Verfügbarkeit von Netzwerkdiensten werden die Access-Switches dabei bevorzugt redundant an das übergeordnete Netz - sprich die Distribution-Switches (oder in kleineren Netzen: die Backbone-Switches) - angebunden.

weiter auf Seite 10

Sonderveranstaltung

## Business Service Management ExpertDays 2005

auf Seite 5

Zum Geleit

## Wireless-Technologie-Phasen: Aktionsplan gefordert

auf Seite 2

Report des Monats

## Planung für Voice over IP

auf Seite 17

Zum Geleit

# Wireless-Technologie-Phasen: Aktionsplan gefordert

Wireless-Technologien entwickeln sich in Technologie-Phasen, die sich inhaltlich deutlich unterscheiden. Für jeden Anwender entsteht somit die Aufgabe, eine für sein Unternehmen optimierte Implementierungsstrategie zu finden. Diese Strategie muss Investitionen sichern und technische Nachteile und Sackgassen vermeiden. Ergebnis muss dann u.a. ein konkreter Aktionsplan sein, der insbesondere darauf ausgelegt ist, ein solides technisches Fundament für den zukünftigen Ausbau und die Folgephasen zu schaffen.

Grob zusammengefasst sehen wir zur Zeit drei relevante Entwicklungsphasen von Wireless-Technologien:

Phase 1: Client-dominierte WLAN-Technologien

Die in den Clients implementierten WLAN-Technologien bestimmen und begrenzen den WLAN-Einsatz. Neue Technologien und wichtige Verbesserungen werden durch die fehlende Client-Kompatibilität ausgebremst.

Phase 2: Erste professionelle Nutzung, aber mit weiter bestehenden Bandbreiten-Einschränkungen

Clients haben sich soweit weiter entwickelt, dass zumindest im Bereich der Sicherheit einheitliche Standards einhaltbar sind. Das Thema Mobilität prägt zunehmend das Design WLANs.

Phase 3: Voll professionelle Nutzung und Aufhebung der Bandbreiten-Einschränkungen

Neue Technologien bieten Bandbreiten, die dem Kabel-Anschluss für normale Büro-Arbeitsplätze vergleichbar sind. Mobile Teilnehmer prägen das Netzwerk und erfordern Flächendeckung.

In der aktuell dominierenden Phase 1 prägt die in den Client-Systemen implementierte Technik die Netzwerke. Im Bereich der Notebooks besteht dabei durch eine Wahlmöglichkeit, die auch

über den häufig eingesetzten Centrino-Chipsatz hinaus geht. Bei vielen anderen Client-Typen, wie zum Beispiel Handscannern und WLAN-Telefonen, besteht die Wahl und Gestaltungsmöglichkeit häufig nicht. Dies gilt sowohl für die eingesetzte Wireless-LAN-Basis-Technologie als auch für das umsetzbare Sicherheitsniveau.

Typisch für die Phase 1 sind folgende Merkmale:

- Hoher Anteil von IEEE 802.11b Teilnehmern
- Kleiner, aber zunehmender Anteil von IEEE 802.11g-Teilnehmern
- Keine oder nur geringe Nutzung von IEEE 802.11a
- Mischbetrieb aus 11b und 11g beeinträchtigt die Gesamtleistung stark
- WEP ist weiter stark präsent, WPA wenn überhaupt, dann mit Pre-Shared-Keys (die theoretisch mit einer Dictionary Attacke angegriffen werden können)
- Störungen aus anderen Anwendungen, die ebenfalls im 2,4 GHz-Bereich laufen, nehmen immer weiter zu und stellen eine stabile Nutzung von 11b und 11g ernsthaft in Frage

Bewertet man diese Situation, dann ist festzustellen, dass die Phase 1 somit durch 3 Kernmängel geprägt ist:

- Die Wireless-Nutzung ist bedingt durch die bestehenden WEP-Teilnehmer unsicher (natürlich kann für Notebook-dominierte Zellen eine sicherere Lösung gefunden werden)
- Die nutzbare Bandbreite ist durch den Mischbetrieb von IEEE 802.11b und IEEE 802.11g unzureichend
- Die Stabilität ist bedingt durch die Interferenzen mit anderen Anwendungen nicht gewährleistet

Speziell die Sicherheits-Problematik ist durch eine zunehmende Diskrepanz gekennzeichnet. Auf der einen Seite haben Standards wie IEEE 802.11i / WPA II im Prinzip alle bestehenden Sicherheitsprobleme gelöst. Sie führen bei korrekter Umsetzung dazu, dass Wireless LANs mit zu den sichersten existierenden Netzwerken überhaupt gehören würden. Auf der anderen Seite erschweren Teilnehmer, die diesen Standard nicht untersützen, die flächendeckende Umsetzung.

Es darf bei der Diskussion des Themas Sicherheit allerdings auch nicht verschwiegen werden, dass viele Unternehmen gar nicht in der Lage wären, den vollen Ausbaugrad der höchsten Sicherheitsstufe umzusetzen. Die dazu notwendige Sicherheitsarchitektur mit einer zentralen Anmeldung erfordert Vorleistungen zum Beispiel im Bereich der Benutzerverwaltung, der zentralisierten Konfigurationsverwaltung von Endgeräten und der Directory-Dienste, die in vielen Fällen erst noch geleistet werden müssen. Diese Vorarbeiten können sich durchaus über einen Zeitraum von 1 bis 2 Jahren erstrecken, je nach Größe des Unternehmens.

Wireless LANs entwickeln sich technisch mit dem Markt weiter (deshalb ja auch die Einteilung in Entwicklungsphasen). Diese Weiterentwicklung wird dazu führen, dass die angebotenen Produkte in den nächsten 12 Monaten weitgehend den Wechsel in die Phase 2 vollziehen werden.

Dementsprechend müssen hier folgende Handlungsempfehlungen abgeleitet werden:

- Bei einer Entscheidung für den Kauf von Client-Systemen muss die Fähigkeit zur Unterstützung aller WLAN-Standards, also auch von IEEE 802.11a/h ein Kernkriterium mit Ausschlusswirkung sein

- Auch wenn der volle Einsatz von IEEE 802.11i momentan nicht möglich sein sollte, sollte mit dem Aufbau einer geeigneten Sicherheits-Infrastruktur sofort begonnen werden, da dieser Aufbau Zeit kostet.

Der Einstieg in Phase 2 ist gleichzeitig ein Einstieg in den 5 GHz-Bereich. In den USA ist die entsprechende Diskussion relativ intensiv, da hier bereits erhebliche Probleme durch Interferenzen mit anderen 2,4 GHz-Anwendungen existieren (dies betrifft in den USA auch den Konsumer-Bereich, da einige sehr populäre Funktelefone im 2,4 GHz-Band arbeiten; der starke Drang von Konsumer-Technik in Richtung Wireless wie zum Beispiel auf der CES in Las Vegas zu sehen könnte hier sehr kurzfistig zu einem hohen Druck in Richtung IEEE 802.11a/h führen, dafür spricht auch die aktuelle Normung zu IEEE 802.11n).

Phase 2 wird im Wesentlichen durch folgende Eigenschaften geprägt:

- Konzentration auf 5 GHz und IEEE 802.11a/h (WiFi hat endlich die Konformitätstests für 11h freigegeben, so dass hier jetzt Bewegung zu erwarten ist), Nutzung von 11g und 11b nur im Sinne einer Rückwärtskompatibilität mit abnehmender Bedeutung

- Starke und zunehmende Orientierung an mobilen Client-Systemen, daraus abgeleitet

  - Zunehmende Flächendeckung
  - Zellüberlappung
  - Handover auch für Layer-3 ohne Unterbechung der Applikation

- Einsatz von IEEE 802.11i / WPA II im Rahmen einer Sicherheits-Infrastruktur

Das herausragende Kernmerkmal der Phase 2 ist der zunehmende Bedarf an zentraler Kontrolle. Hier hat sich in den letzten Monaten ein Technologiewechsel immer stärker heraus gearbeitet. Dementsprechend wird zentrale Kontrolle umfassen:

- Wechsel auf eine Switch-basierte Architektur, bei der die Intelligenz vom Access Point in den Switch verlagert wird. Ein Switch steuert eine Menge von Access Points, es entsteht ein zentraler Kontroll- und Konfigurationspunkt

- Dies ist nicht neu, entsprechende Produkte gibt es schon seit längerem (siehe Vernier, Trapeze, Chantry, Aruba etc). Neu ist, dass dabei der Umfang der Kontroll- und Steuerungsfunktionen immer weiter ausgebaut wird. Ziel ist es, auf eine aufwändige Einmessung einer Fläche verzichten zu können und ein System zu schaffen, das sich selbst an die Umgebung adaptiert, also auch auf Änderungen im Umfeld (Umbauten, andere Art der Möblierung) und auf Störungen dynamisch reagieren kann. Typische Steuerungs-Funktionen umfassen:

  - Wahl des Kanals
  - Wahl der Signalstärke
  - Erkennung unzulässiger Access-Points

- In Kombination mit der Client-Software auf den PCs wird diese dynamische Auslegung der Funkzellen dann mit einer dynamischen AP-Wahl auf Seiten der Clients kombiniert. Client-Systeme kommen so in die Lage, auch nach Lastgesichtspunkten den für sie optimalen Acces-Point auszuwählen. Damit wird die nutzbare Kapazität einer Installation gerade auch im Vergleich zu den einfachen traditionellen Access-Point-Installationen massiv erhöht

Eine Alternative zu dieser Entwicklung, die als ein Kompromiss betrachtet werden kann, ist der Ansatz, eine zentrale Management-Applikation mit normalen, traditionellen Access-Points zu kombinieren. Dieser Ansatz wird speziell von AirWave betrieben und auch von wichtigen Herstellern unterstützt (Hewlett Packard, Linksys, Lancom, …). Der Nachteil dieses Ansatzes könnte auf Dauer im Bereich des Verlust-freien Layer-3-Roamings liegen. Der Vorteil liegt in der Einhaltung von offenen internationalen Standards. Denn leider haben alle anderen zentralisierten Lösungen auf Switch-Basis den gravierenden Nachteil der Hersteller-Bindung und Nicht-Standard-Basierung (ein Kompromiss ist von Trapeze gekommen, die ihre Software für die Access Points offen gelegt haben, aber auch das ist kein Ersatz für einen Standard). Gerade diese Hersteller-Bindung von Switch-basierten Lösungen erfordert aber eben auch eine schnelle Entscheidung. Ansonsten können hohe Fehlinvestitionen die Folge sein. Wer bereits in einem erheblichen Ausmaß in Access Points investiert hat, für den ist der Ansatz von AirWave der geeignetste Ansatz zur Investitions-Sicherung.

Was bleibt dann noch für Phase 3?

Nun, die wesentlichen Mängel der Phase 2 bestehen in 2 Bereichen:

- Noch nicht unbedingt Flächendeckung, damit Nachteile zum Beispiel in der Umsetzung von Voice over WLAN. Man mache sich da nichts vor. Jeder, der IP-Telefonie einsetzt, wird auf Dauer eindeutig diesen Weg gegenüber einer DECT-Lösung bevorzugen. Voice over WLAN ist auf 5 Jahre gesehen eine unvermeidliche Flächentechnologie mit sehr hoher Bedeutung

- Bandbreitenengpässe. Auch mit einer Kapazitätsoptimierung der Access-Points durch ein dynamisches und lastorientiertes Anmeldeverfahren der Clients werden Bandbreitenengpässe weiter bestehen bleiben so lange Wireless Netzwerke auf 11a/h basieren

Dementsprechend besteht Phase 3 aus folgenden Kernelementen:

- Ausbau der Bandbreite durch Standards wie 11n oder weitere Folgestandards. Leider orientiert sich 11n zu sehr am Bedarf der Konsumertechnik. So ist momentan das Hauptziel von 11n, eine flächendeckende HDTV-Versorgung in einem Einfamilienhaus zu erreichen. Dafür sind eine sehr stabile Übertragung und mehr als 60 Mbit/s Nutzdatenrate erforderlich (40 Mbit/s für Video, der Rest für Daten, MP3 u.a.)

- Flächendeckende Mobilität mit unterbrechungsfreiem Layer-3-Handover

- Architektur-Ergänzung im Sekundärbereich und ggf. auch im Primärbereich durch WiMAX

Die Entwicklung des Wireless-Marktes in diesen Phasen kann als relativ sicher angesehen werden. Im Endeffekt ist der Übergang zu Phase 2 gerade im Gange. Es fehlen eigentlich nur die Client-Systeme und der Wechsel auf 5 GHz.

Ansonsten ist der Markt in Summe in einer Bereinigungsphase. Die innovativen Startups werden zunehmend durch die Großen übernommen oder im Rahmen langjähriger OEM-Verträge fest gebunden. Diese Konsolidierung wird im Bereich der professionellen Anbieter nicht

mehr als vier oder fünf dominanten Anbieter zurück lassen. Auch dies ist ein klares Zeichen dafür, dass sich der Markt dem Ende der Phase 1 nähert.

Welcher Aktionsplan kann jetzt daraus abgeleitet werden? Im Kern können folgende Empfehlungen als Basis der Weiterentwicklung der Wireless-Technologien gegeben werden:

- Sofortiger Start zum Aufbau einer Sicherheits-Infrastruktur. Diese sollte sowohl WLANs als auch Kabelgebundene LANs abdecken. Da dieser Aufbau zeitaufwändig sein kann, sollte eine entsprechende Entscheidung sofort gefällt werden
- Ausrichtung aller Neubeschaffungen auf 5 GHz
- Umwandlung der Einzelinstallation von Acess-Points in eine zentral gesteuerte Architektur, sei es mit Wireless-Switches oder mit AirWave. Je später dieser Wechsel vollzogen wird, desto teurer wird er werden. Da er in jedem Fall kommt, sind hier Sofort-Entscheidungen über den richtigen Weg erforderlich
- Ausrichtung auf mobile Clients

Die Entscheidung für den richtigen Weg kann im Einzelfall durch die Abhängigkeit von einzelnen Herstellern, durch Umgebungsbedingungen oder begrenzte Projektbudgets sehr komplex sein.

Aus diesem Grund empfehlen wir speziell zu diesem Thema:

- Die Sommerschule 2005 mit Schwerpunkten zu Wireless und zur Umsetzung von Sicherheits-Infrastrukturen in Netzwerken
- Unser Wireless-Seminar, das auf alle angesprochenen Fragen detailliert eingeht

Ihr
Dr. Jürgen Suppan

Sonderveranstaltung

# Business Service Management ExpertDays 2005

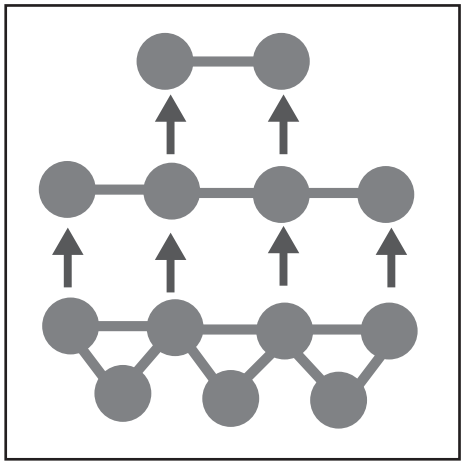
Die ComConsult Akademie veranstaltet vom 27.06. - 28.06.05 erstmalig die „Business Service Management ExpertDays 2005“ in Köln.

Mit den Business Service Management (BSM) ExpertDays 2005 wollen wir Ihnen erstmalig die Gelegenheit geben, das marktbestimmende Thema Business Service Management neutral und kompetent aufbereitet in komprimierter Form zu durchleuchten.

Die BSM ExpertDays 2005 analysieren die aktuellsten Entwicklungen im Business Service Management und bewerten Markttrends und Produktentwicklungen.

Im Mittelpunkt der BSM ExpertDays 2005 stehen u.a. die folgenden Fragen

- Was ist Business Service Management? Für wen lohnt sich Business Service Management?
- Ist Business Service Management wirklich etwas Neues oder nur ein neuer Begriff für alte Ideen?
- Wie unterscheidet sich Business Service Management von früheren System- und Service-Management-Ansätzen?
- Was sind die Kernmerkmale einer Business Service Management Architektur?
- Wie setzt man ein Business Service Management Projekt auf? Worauf muss man hier besonders achten?
- Welche Produktstrategien verfolgen die Key Player auf dem Business Service Management Markt? Gibt es hier Unterschiede?



Die BSM ExpertDays 2005 bieten Ihnen hochaktuelle Aussagen in Form von

- Neutrale Meinungen zum BSM-Markt hochkarätiger Analysten, seiner aktuellen Stellung und zukünftigen Entwicklung,
- Erfahrungsberichte von Kunden, die sich mit BSM bereits beschäftigt haben oder aktuell in der Einführungsphase sind,
- Hersteller-Statements zu zukünftigen Produkt- und Marktstrategien,
- Projektberichte aktueller Implementierungen.

Aufgrund der Aktualität und Internationalität werden einzelne Vorträge in englischer Sprache gehalten!

Die Business Service Management Expert Days geben Ihnen Gelegenheit, sich in Vorträgen und Diskussionen durch ausgesuchte BSM-Experten in kürzester Zeit auf den neuesten Stand dieses aktuellen Themas zu bringen.

Erstmalig ist es gelungen, die wesentlichen Keyplayer des wachsenden BSM Marktes zusammen zu bringen:

Von der ComConsult Kommunikationstechnik Martin Woyke, Geschäftsführer (deutsch), Ralf Horstmann, Abteilungsleiter IT Enteprise Management und Strategieberater für BSM Themen (deutsch) Heiko Soldan, Abteilungsleiter Vertrieb und Strategieberater zu CMDB Themen (deutsch).
Weiterhin Aria Naderi, Senior Consultant der BMC und Strategieberater für BSM Lösungen mit BMC Service Impact Manager (deutsch) Urs Hardekopf, Sales Director Germany der Firma Oblicore (deutsch) Steve Gadd, Product Manager Managed Objects Formula (englisch) Will Cappelli, Gartner Analyst mit Themenschwerpunkt BSM + CMDB (englisch) Dan Tabor, BSM Specialist Micromuse Netcool (englisch) Robert Roblin, CEO der Firma Collation zum Thema automatische Service Inventarisierung (englisch).

Fax-Antwort an ComConsult 02408/955-399

# Anmeldung

## Business Service Management ExpertDays 2005

☐ Ich buche das Seminar **Business Service Management ExpertDays 2005**
vom 27.06. - 28.06.05 in Köln
zum Preis von € 1.490,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____05

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

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

## Business Service Management ExpertDays 2005 - Programmübersicht

In dieser einmaligen Veranstaltung werden anerkannte Strategieberater und Analysten Sie fundiert und praxisnah über Lösungsansätze von der Auswahl einer BSM-Architektur über die aktuelle Marktentwicklung bis zu Realisierungsempfehlungen informieren. Die Herstellervorträge orientieren sich an bereits realisierten Kundenprojekten, die seit mindestens 6 Monaten erfolgreich den Produktionsstatus erreicht haben und liefern Ihnen exklusiv Informationen zu den folgenden Punkten:

- Architekturbild des Kunden
  - Mengengerüste der Kundenumgebung
  - Lösungsbeschreibung
  - Beschreibung der umgebenden Systeme und Integrationen
    - Netzwerk Management
    - System Management
    - UHD
    - ...
- Darstellung des Projektmeilensteinplans
  - Welche Projektziele wurden verfolgt?
  - Welche Projektziele wurden erreicht?
- Mit welcher Methode wurde BSM beim Kunden initiiert?
- Welche Argumente waren für die Entscheidung ausschlaggebend?
- ROI Rechnung des Kunden
- Welche Budgets musste der Kunde einplanen
  - Lizenzkosten + Mengengerüste der Lösung
  - Externe Dienstleistungsaufwände (Personentage + Kosten)
  - Interne Aufwände (Personentage)
- Wie wurden die Prozessbeschreibungen ermittelt?
- Wie wurden die Prozessbeschreibungen in das System übertragen?
- Mit welcher Methode erkennt der Kunde Änderungen in Prozessen / Infrastruktur / Verträgen / SLA's?
- Wie fließen diese Änderungen in das BSM-System ein und werden aktualisiert?
- Welche zeitlichen Abläufe liegen den Pflegeprozessen zugrunde?
- Welche weiteren Schritte sind geplant?

### Montag, den 27.06.2005

**9:00 bis 9:15 Uhr**
**Begrüßung**
*Dipl.-Kfm. Martin Woyke, ComConsult Kommunikationstechnik*

**9:15 bis 10:00 Uhr**
**BSM Marktübersicht , Plazierung**
*Ralf Horstmann, ComConsult Kommunikationstechnik*

**10:00 bis 11:00 Uhr**
**BMC BSM Strategie / Referenzprojekt**
*Aria Naderi, BMC*

**11:30 bis 12:30 Uhr**
**Oblicore Guarantee / Referenzprojektvorstellung**
*Urs Hardekopf, Oblicore*

**14:00 bis 15:00 Uhr**
**Vorgehensweise bei der Einführung einer BSM Strategie/PoC**
*Kundenvortrag*

**15:00 bis 16:00 Uhr**
**Formula BSM + BSCM / Referenzprojektvorstellung**
*Steve Gadd, ManagedObjects*

**16:30 bis 17:30 Uhr**
**Analystenmeinung zu BSM Konsolen**
*Will Cappelli, Gartner*

**11:00 - 11:30 Uhr Kaffeepause**
**12:30 - 14:00 Uhr Mittagspause**
**16:00 - 16:30 Uhr Kaffeepause**
**ab 18:00 Uhr Happy Hour**

### Dienstag, den 28.06.2005

**9:00 bis 10:00 Uhr**
**CMDB im BSM Umfeld - strategische Plazierung + Markt + PoC**
*Ralf Horstmann, ComConsult Kommunikationstechnik*

**11:00 bis 11:00 Uhr**
**Netcool/RAD / Referenzprojektvorstellung**
*Dan Tabor, Micromuse*

**11:30 bis 12:30 Uhr**
**Collation Configia Application Discovery / Referenzprojekt**
*Robert Roblin, Collation*

**14:00 bis 15:00 Uhr**
**AixBOMS CMDB / Referenzprojekt**
*Heiko Soldan, ComConsult Kommunikationstechnik*

**15:00 bis 16:00 Uhr**
**Analystenmeinung zur CMDB**
*Will Cappelli, Gartner*

**16:00 bis 16:30 Uhr**
**Fazit und Zusammenfassung, Ausblick 2005 / 2006**
*Dipl.-Kfm. Martin Woyke, ComConsult Kommunikationstechnik*

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

Änderungen im Programm behält sich der Veranstalter

Neues Seminar aus der Praxis

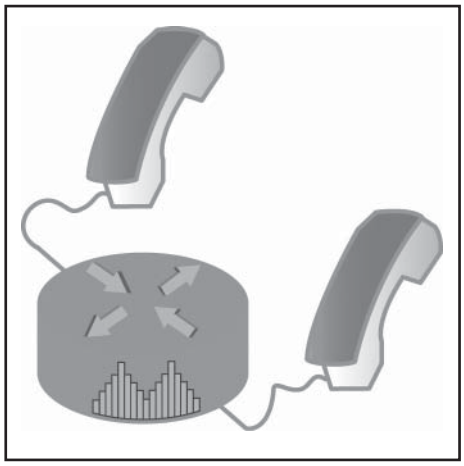
# Konzeption, Rollout und Betrieb einer IP-Telefonie-Lösung

## basierend auf dem Cisco-CallManager in einem großen Netzwerk

Die ComConsult Akademie veranstaltet vom 26.09. - 27.09.05 erstmalig ihr neues Seminar „Konzeption, Rollout und Betrieb einer IP-Telefonie-Lösung basierend auf dem Cisco-CallManager in einem großen Netzwerk“ in Bonn.

Wie finde ich das für mein Unternehmen am besten geeignete Produkt für IP-Telefonie? So einfach die Frage ist, so komplex ist die Antwort. Zwar ermöglichen Studien wie die Produktanalyse von ComConsult-Research einen Produktvergleich auf einem hohen Niveau, doch zur letzten Entscheidung sind Erfahrungen aus dem Praxis-einsatz der Produkte unverzichtbar. Insbesondere gilt dies, da gerade IP-Telefonie-Produkte in der Regel um zusätzliche Funktionen und Spezialprodukte ergänzt werden.

Dieses Seminar beschreibt eine Telefonie-Komplettlösung auf Basis des Cisco-Call Managers in einer Umgebung mit mehreren tausend Telefonen. In dem Mix aus Erfahrungsberichten, der Darstellung von Verfahren, technischen Hintergründen und Beispielen zu Systemkonfigurationen und eigenen Entwicklungen betrachten die Referenten die wichtigsten Facetten des Projektes und gehen



unter anderem auf folgende Fragestellungen ein:

- Wie war die Ausgangslage?
- Welche Gründe führten zur Produktentscheidung?
- Können die benötigten Leistungsmerkmale erfüllt werden?
- Was bedeutet Konfiguration der Lösung in der Praxis?
- Wo muss das Produkt durch Zusatzprodukte ergänzt werden?
- Welche Architektur ist sinnvoll?
- Wie kann Verfügbarkeit sichergestellt werden?
- Welche Anforderungen ans Netzwerk entstehen?
- Was ist bei Migration und Rollout zu beachten?
- Wie haben die Benutzer reagiert, was war positiv, was negativ?
- Wie aufwändig und komplex ist der Betrieb?
- ROI Betrachtung
- Empfehlungen für andere Projekte

Dieses Seminar bietet einen einmaligen Überblick zu Pro und Contra zum Einsatz des Call Managers.

Durch das Seminar führen Karl-Heinz Hommen-Menz und Axel Schemberg, die beide seit vielen Jahren im Rechenzentrum der Finanzverwaltung Nordrhein-Westfalen beschäftigt und freiberuflich als freie Dozenten tätig sind. Profitieren sie von den mehrjährigen Praxiserfahrungen der beiden Referenten, stellen Sie Ihre Fragen und setzen Sie die Erkenntnisse aus diesem Seminar erfolgreich in Ihren Projekten ein.

Fax-Antwort an ComConsult 02408/955-399

# Anmeldung

## IP-Telefonie-Lösung: Konzeption, Rollout und Betrieb

☐ Ich buche das Seminar **IP-Telefonie-Lösung: Konzeption, Rollout und Betrieb**
vom 26.09. - 27.09.05 in Bonn
zum Preis von € 1.390,- zzgl. MwSt.
☐ Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____05

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

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

Sonderveranstaltung

# IP-Telefonie: Markt und Produkte in der Analyse

Die Auswahl eines geeigneten Produkts für IP-Telefonie ist für jedes Unternehmen nicht leicht:

- Hersteller haben ihre Strategien, Produkte und Ankündigungen mehrfach geändert
- Produkt-Architekturen sind komplex, insbesondere in redundanten Standort-übergreifenden Situationen
- Die gleiche Komplexität betrifft die Umsetzung von Sicherheits-Konzepten, die gerade bei IP-Telefonie elementar sind
- Neue Standards wie SIP verändern Produkte und Architekturen
- Neue Funktionsbereiche wie Multipunkt-Audio und Video-Konferenzen, Kollaboration oder Präsenzbasierte Team-Funktionen erfordern die Kenntnis der zukünftigen Weiterentwicklung der Produkte

An dieser Stelle setzt diese hochaktuelle Sonderveranstaltung an, die Sie umfassend in Markt und Produkte einführt.

Sie erfahren in diesem Seminar:

- Was IP-Telefonie-Produkte leisten
- Worauf Sie bei der Auswahl achten müssen
- Wo typische Schwachstellen und Probleme liegen
- Welche Strategien ausgewählte Hersteller verfolgen
- Welche Erfahrungen ausgewählte Anwender gemacht haben

Es erwartet Sie eine herausragende Veranstaltung, die Sie auf keinen Fall versäumen sollten, wenn Sie sich für IP-Telefonie interessieren. Die Veranstaltung steht unter der Leitung von Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke, unter deren Leitung auch die großen Marktanalysen über Alcatel, CISCO und Siemens entstanden sind. Als Teilnehmer an der Veranstaltung können Sie diese Markt-Analysen zu einem sehr attraktiven Sonderpreis erwerben.

Durch die Veranstaltung führt Sie Dipl.-Inform. Petra Borowka, Unternehmensberatung UBN.

## Programmübersicht

### Montag, den 20.06.2005

**10:00 bis 11:00 Uhr**
**Einführung: IP-Telefonie und ihre Varianten: wie funktioniert sie, welche Alternativen hat der Kunde zur Auswahl**

- Die verfügbaren Standards
- Grundprinzipien und Protokolle
- Komponenten einer Lösung: VoIP Endgeräte, VoIP-Server, VoIP Gateways und ihre Netzanbindung

*Dipl.-Inform. Petra Borowka, UBN*

**11:15 bis 12:30 Uhr**
**Architekturen, Einsatz-Konzepte**

- Klassische TK
- Zentrale Hybrid-Anlage
- Dezentrale Hybridlösung
- Reine Soft-PBX
- Beispiel-Szenarien: Single-PBX, Filial-Situation, Teleworker; Mehrstandort-Konzepte

*Dipl.-Inform. Petra Borowka, UBN*

**13:30 bis 14:00 Uhr**
**Evaluierung von VoIP Lösungen, Kriterien**

- Projekterfahrungen
- Funktionale Bewertung
- Strategische Bewertung
- Total Cost Ansatz
- Evaluierungs-Bereiche: Architektur, Endgerät, TK-Server, Leistungsmerkmale, weiterführende Funktionen, Zusatzanwendungen

*Dipl.-Inform. Petra Borowka, UBN*

**14:00 bis 15:00 Uhr**
**Anwendervortrag: Rollout- und Bestriebserfahrungen mit IP-Telefonie von Cisco**

- Komponenten der Lösung in der Finanzverwaltung NRW
- Voraussetzungen im LAN und WAN
- Einige wesentliche Funktionen / Highlights für die Anwender
- Installations-, Konfigurations- und Rolloutprozess
- Stand des Rollouts
- Wo liegen die Probleme
- Was verursachte den meisten Aufwand
- Wie aufwändig ist der Betrieb
- Sind Erwartungen an Kostensenkung erfüllt worden

*Karl-Heinz Hommen-Menz, RZF*

**15:15 bis 16:15 Uhr**
**Produkte, Strategie, Marktposition**

- Alcatel
- Cisco
- Siemens

*Dipl.-Inform. Petra Borowka, UBN*

**16:30 bis 17:30 Uhr**
**Report-Ergebnisse: Alcatel vs. Cisco vs. Siemens Teil 1**

- Bewertungs-Kriterien
- Technische Bewertung:
  - Architektur
  - Leistungsmerkmale
  - Weiterführende Funktionen

*Dipl.-Inform. Petra Borowka, UBN*

**11:00 - 11:15 Uhr Kaffeepause 12:30 - 13:30 Uhr Mittagspause 15:00 - 15:15 Uhr Kaffeepause ab 18:00 Uhr Happy Hour**

IP-Telefonie: Markt und Produkte in der Analyse

## Dienstag, den 21.06.2005

**9:00 bis 10:00 Uhr**
**Report-Ergebnisse:**
**Alcatel vs. Cisco vs. Siemens Teil 2**
- Kostenbewertung:
  - Zwei RFI-Projekte
  - Lösungen
  - Kostenvergleich

*Dipl.-Inform. Petra Borowka, UBN*

**10:00 bis 11:00 Uhr**
**Anwendervortrag:**
**Praxiserfahrungen mit IP-Telefonie von Siemens**
- Wie hoch war der Konfigurationsaufwand
- Wie aufwendig ist der Betrieb
- Sind Erwartungen an Kostensenkung erfüllt worden
- Wie zufrieden sind die Anwender

*Heinz Lebeck, LTU*

**11:15 bis 12:30 Uhr**
**Produkte, Strategie, Marktposition**
- Avaya, Mitel , Nortel

*Dipl.-Inform. Petra Borowka, UBN*

**13:30 bis 14:45 Uhr**
**Zusatzanwendungen und ihre Bedeutung**
- Unified Messaging / Unified Communication
- Call Center
- Kollaboration
- Einsatz-Szenarien
- Worauf ist beim Einsatz zu achten?

*Dipl.-Inform. Petra Borowka, UBN*

**15:00 bis 15:30 Uhr**
**Projekt-Vorstellung des RFI**
- Projektumgebung
- Anforderungen
- Mengengerüst

*Dipl.-Inform. Petra Borowka, UBN*

Hersteller präsentieren ihre Lösungen an einem vorgegebenen Projektbeispiel
Eingeladen sind: Alcatel, Avaya, Cisco, Mitel, Nortel, Siemens

**15:45 bis 16:30 Uhr**
**RFI Präsentation der Alcatel-Lösung**

*Dr. Jörg Fischer, Alcatel*

**16:30 bis 17:15 Uhr**
**Präsentation der Avaya-Lösung**

*Stefan Neumann, Avaya / Tenovis*

**11:00 - 11:15 Uhr Kaffeepause** **12:30 - 13:30 Uhr Mittagspause** **14:45 - 15:00 Uhr Kaffeepause**

## Mittwoch, den 22.06.2005

**9:00 bis 9:45 Uhr**
**RFI Präsentation der Cisco-Lösung**

*Joachim Baumann, Cisco*

**9:45 bis 10:30 Uhr**
**RFI Präsentation der Mitel-Lösung**

*Eric Vocke, Mitel*

**10:45 bis 11:30 Uhr**
**RFI Präsentation der Nortel-Lösung**

*Dipl.-Ing. Göran Friedl,Nortel Networks*

**11:30 bis 12:15 Uhr**
**RFI Präsentation der Siemens-Lösung**

*Dr. Ralf Tyras, Siemens*

**12:15 bis 12:45 und 13:45 bis 14:15 Uhr**
**SIP: Der Telefonie-Standard der Zukunft in der kritischen Analyse**
- Arbeitsweise und Anlagen-Architektur
- SIP-Clients
  - Softclients, Hardclients, Multimedia-Clients
- Funktionserweiterungen Instant Messaging und Presence
- Einsatz-Beispiele: Alcatel OTUC, Nortel MCS 5100, Siemens OpenScape
- Erfahrungen aus dem German SIP Center

*Dipl.-Inform. Petra Borowka, UBN*

**14:15 bis 15:00 Uhr**
**Implementierungs-Aspekte für Voice-ready Netzwerke**
- Anforderungen (Delay, Verlust, Jitter)
- Netzwerk-Voraussetzungen
- Pover over Ethernet
- Voice-VLAN's ja oder nein?
- Quality of Service: Priorisierung
- Sicherheits-Überlegungen

*Dipl.-Inform. Petra Borowka, UBN*

Änderungen im Programm behält sich der Veranstalter vor!

**10:30 - 10:45 Uhr Kaffeepause** **12:45 - 13:45 Uhr Mittagspause** **15:00 Uhr Ende der Veranstaltung**

Fax-Antwort an ComConsult 02408/955-399

# Anmeldung IP-Telefonie: Markt und Produkte in der Analyse

☐ Ich buche das Seminar **IP-Telefonie: Markt und Produkte in der Analyse**
vom 20.06. - 22.06.05 in Bonn
zum Preis von € 1.990,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____05

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

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

Zweitthema

# Schnelle Konvergenz im Access-Bereich

Fortsetzung von Seite 1

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

Bild 1 zeigt eine solche redundante Anbindung der Access-Switches an die Distribution-Switches. Für diese redundante Verschaltung muss jedoch ein Verfahren ausgesucht und implementiert werden, das die redundanten Uplinks steuert. Hier bieten die Hersteller verschiedene Verfahren an, die mit hoher Bandbreiteneffizienz und sehr schnellen Umschaltzeiten werben.

Im Folgenden werden vier Lösungen für die Redundanzverschaltung betrachtet und hinsichtlich ihrer Leistungsfähigkeit analysiert und bewertet. Die vier Lösungen stehen stellvertretend für eine nahezu unbegrenzte Zahl von denkbaren und herstellerspezifischen Lösungen. Es soll an diesen stellvertretenden Ansätzen gezeigt werden, welche Umschaltzeiten heute möglich sind und wie typischerweise die entsprechenden Designs bewertet werden können.

### Anforderungen an das Konvergenzverhalten des Netzes

Zunächst ist jedoch zu hinterfragen, was der Netzbetreiber eigentlich vom Netz erwartet. In der Verschaltung nach Bild 1 wäre ein Steuerungsverfahren optimal, das folgendes leistet:

1. Im Normalfall werden beide Uplinks eines Access-Switches aktiv genutzt (Load-Sharing).

2. Fällt einer der Uplinks oder ein ganzer Distribution-Switch aus, so erkennen der Access-Switch und das übrige Netz diesen Ausfall und schicken den Datenverkehr nur noch über verbleibende Systeme. Die Umschaltung geschieht so schnell, dass sie von den Anwendern nicht bemerkt wird. Ist der ausgefallene Link oder Switch wieder betriebsbereit, soll automatisch der ursprüngliche Betriebszustand wieder aufgenommen werden.

3. Das Verfahren lässt sich optimal kontrollieren und steuern. Eine Pfadanalyse ermöglicht das Verfolgen von Kommunikationspfaden und das Auffinden von Störungen.

Die Frage, wie schnell das Netzwerk bei einer Störung umschalten muss, hängt von der Nutzung ab. Für die meisten TCP-basierten Applikationen reichen Umschaltzeiten im Bereich von 10 Sekunden aus, da in diesem Bereich in der Regel noch kein TCP-Timeout auftritt und daher die Applikationen nach dem Umschaltvorgang weiterlaufen. Es sind jedoch auch TCP-Applikationen bekannt, die in bestimmten Betriebssituationen bereits nach wenigen Sekunden Unterbrechungszeit eine Applikationsstörung erleiden. Im Falle von IP-Telefonie wird die Erwartungshaltung an die Umschaltzeit im Netz vermutlich im Bereich von wenigen Sekunden liegen; eine hörbare Gesprächsunterbrechung von 10 Sekunden wird wohl kaum akzeptiert werden.

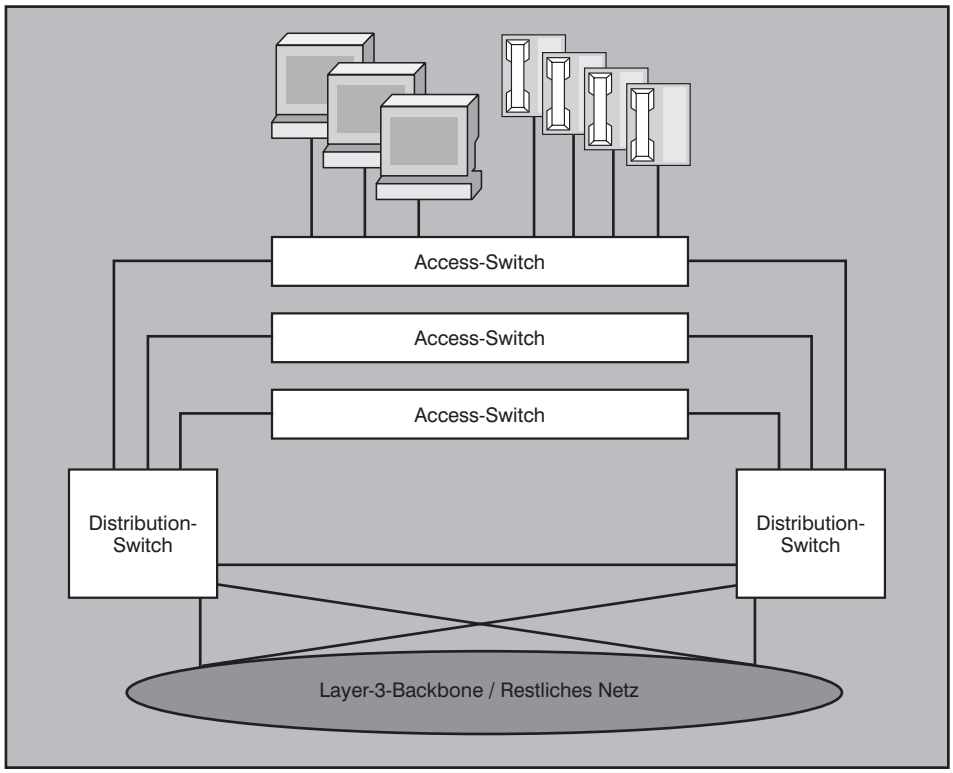



Bild 1: Redundante Anbindung von Access-Switches an das übergeordnete Netz

### Rapid-Spanning-Tree und VRRP

Bild 2 zeigt eine typische Technik für die Steuerung der Redundanzen mit standardisierten Protokollen und einer Layer-2-Ausprägung des gesamten Access-Bereichs. Ein oder mehrere Access-Switches werden als Broadcast-Domäne auf den Distribution-Switches zusammengefasst.

Rapid-Spanning-Tree (RSTP) steuert die Bildung einer schleifenfreien Struktur auf Layer-2, indem von einem Root-Switch aus ein schleifenfreier Baum über alle Switches gespannt wird. Fällt eine der Verbindungen zwischen den Access-Switches und dem Root-Switch aus, sorgt RSTP für eine schnelle Aktivierung einer Ausweichstrecke im Bereich von Sekundenbruchteilen durch das Konzept der vorberechneten alternativen Ports („alternate port“).

Bei Ausfall des Root-Switches werden zunächst alle Access-Switches ihre redundanten Uplinks am zweiten Distribution-Switch ebenfalls innerhalb Sekundenbruchteilen aktivieren. Da die verbleibende Topologie schleifenfrei ist, aber eine neue Root-Bridge ermittelt werden muss, benötigt die Rekonfiguration des Baumes nun noch maximal zweimal die Zeit für das Austauschen eines BPDU, also in Summe 4 Sekunden (RSTP-Default-Wert, eine Beschleunigung ist möglich, aber nicht zu empfehlen).

Zusätzlich zum RSTP-Verfahren für die Steuerung der Layer-2-Struktur ist zusätzlich noch eine Absicherung des Routers zu erreichen, damit den Endgeräten bei einer Störung weiterhin ein Weg aus dem Netz angeboten werden kann. Hierfür wird auf den beiden Distribution-Switches jeweils eine eigenständige Routing-Instanz konfiguriert, wobei sich die zwei Routing-Instanzen über das Virtual Routing Redunancy Protocol (VRRP) gegenseitig absichern. Im Normalbetrieb stellt eine der beiden Routing-Instanzen das Default-Gateway für die Endgeräte im Access-Bereich dar. Unter VRRP wird diese Routing-Instanz als „Master“ bezeichnet. Der Master beantwortet ARP-Requests der Endgeräte mit einer VRRP-spezifischen, virtuellen MAC-Adresse. Die Endgeräte schicken nun alle nach außen gerichteten Pakete für die Weitervermittlung an die virtuelle MAC-Adresse. Der Master-Router schickt regelmäßig (Standard: 1x pro Sekunde) Hello-Pakete ins Access-Netz, die den zweiten Router (unter VRRP als „Backup“ bezeichnet) informieren, dass der Master-Router aktiv ist. Erhält der Backup-Router drei aufeinanderfolgende Hello-Pakete nicht, geht er davon aus, dass der Master-Router ausgefallen ist. Er übernimmt dann die Master-Funktion und damit auch die virtuelle VRRP-MAC-Adresse. Für die Endgeräte ändert sich dabei nichts. Es gelangen lediglich für bis zu 4 Sekunden keine Pakete nach außen.

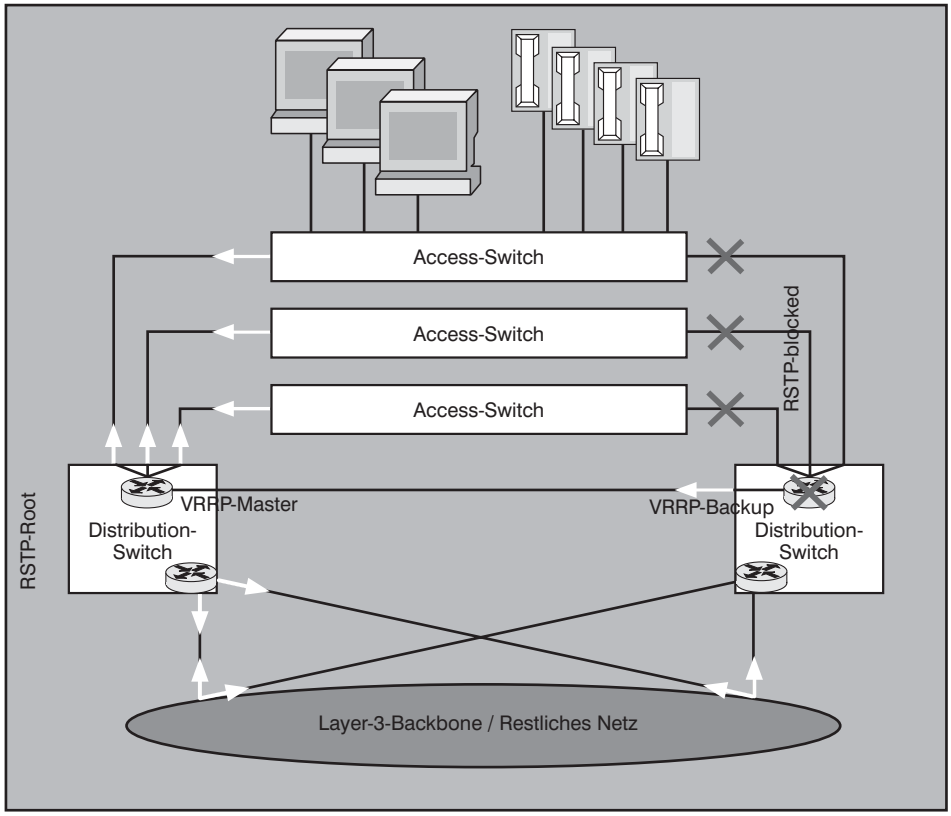



Bild 2: Steuerung der Redundanz mit VRRP und RSTP

Bei Ausfall eines Distribution-Switches ist außerdem noch zu berücksichtigen, dass im Layer-3-Backbone eine Änderung der Wegewahl notwendig ist. Bei einer Verschaltung wie in Bild 2 gezeigt und Verwendung von Open Path Shortest First (OSPF) mit Equal Cost Multi-Path (ECMP) kann diese Änderung der Wegewahl zeitlich stark begrenzt werden, da durch ECMP alternative Routen bereits in der Routing-Tabelle vorhanden sind und weil durch die redundante Anbindung der Distribution-Switches an den Backbone der Ausfall eines der Distribution-Switches durch das Fluten entsprechender Link-State-Advertisments (LSA) in Sekundenbruchteilen propagiert wird. Typischerweise werden in solchen Konstellationen im OSPF Umschaltzeiten im Bereich von ca. 1 Sekunde erreicht. Es sei darauf hingewiesen, dass hier auch wesentlich längere Umschaltzeiten entstehen können, wenn z.B. aufgrund einer unsymmetrischen Verschaltung kein ECMP realisiert werden kann oder mehr als 2 Router über ein Layer-2-Netz im Backbone gekoppelt werden (Routing-Neighborhood).

### Split Multi-Link Trunking und Routed Split Multi-Link Trunking

Der Hersteller NortelNetworks wirbt intensiv mit einer Redundanztechnik, die als Split Multi-Link Trunking (SMLT) bezeichnet wird. Diese überträgt die Link-Aggregation gemäß IEEE-802.3ad auf ein Dreieck von Switches. Kann Link-Aggregation nach IEEE-802.3ad zunächst nur zwischen 2 Switches realisiert werden, so kann mit NortelNetwork’s SMLT ein aggregierter Link auch von einem Access- zu zwei Distirbution-Switches aufgespannt werden, sofern zwischen den zwei Distribution-Switches ein InterSwitch Trunk (IST) aufgespannt wird, über den auf Basis eines proprietären Protokolls ein Abgleich der Distribution-Switches erfolgt.

Durch diese Technik ist der Rapid-Spanning-Tree wie zuvor beschrieben verzichtbar, da das Netz sich verhält, als wären die Access-Switches über eine Bündelung ihrer Uplinks und damit ohne Layer-2-Schleifen an einen einzigen Distribution-Switch angeschlossen. Besonders vorteilhaft ist dabei, dass jeweils beide Uplinks der Access-Switches im Normalbetrieb vollständig bidirektional genutzt werden können, während bei RSTP jeweils ein Uplink blockiert wird. Die installierte Bandbreite kann demnach optimal ausgenutzt werden.

Bild 3 zeigt die Verschaltung unter Einsatz von SMLT und des IST. In dieser Darstellung ist erkennbar, dass auf dem IST ein besonderes Verfahren eingesetzt sein muss, das dafür sorgt, einerseits die Link-Aggregation zwischen den beiden Distribution-Switches abzugleichen und andererseits die Schleifenbildung im Netz zu verhindern. Der IST ist NortelNetworks-proprietär und nach Kenntnis des Autors nicht mit anderen Herstellern kompatibel. Die Access-Switches sind allerdings rein nach IEEE-802.3ad-Standard konfiguriert und können somit von beliebigen Herstellern stammen.

NortelNetworks bietet zusätzlich Lösungen an, um die Konvergenz im Layer-3-Bereich zu beschleunigen. Eine dieser Lösungen besteht darin, auch die Routing-Instanzen auf den Distribution-Switches über den IST abzugleichen und so für Routing-Redundanz zu sorgen. Dabei werden zunächst zwei unabhängige Router konfiguriert, deren Routing-Tabellen und sonstige Eigenschaften aber durch Einbindung in den IST abgeglichen werden. Diese Lösung wird wegen der Nutzung des IST als RSMLT (Routed Split Multi-Link Trunking) bezeichnet. Jeder Router verarbeitet dabei auf Basis der abgeglichenen Routing-Tabellen auch solche Pakete, die an seinen Nachbarn im IST adressiert sind. Werden die Distribution-Switches wie in Bild 3 gezeigt an einen Backbone-Switch angeschlossen, der ebenfalls RSMLT-basiert ist, so reguliert das RSMLT-Verfahren sowohl die Redundanz bezüglich des Default-Gateways der Endgeräte wie auch die Redundanz in der Backbone-Anbindung (OSPF), da jeder Router im IST-Pärchen jeweils alle ein- und ausgehenden Pakete routen kann.

Die Umschaltzeiten bei Ausfall eines Uplinks oder eines Distribution-Switches liegen bei parallelem Einsatz von SMLT und RSMLT wie in Bild 3 gezeigt nach Herstellerangaben im Bereich von 1 Sekunde oder darunter. Dem Autor sind bestätigende Messwerte nur für das SMLT-Verfahren, nicht jedoch für das RSMLT-Verfahren bekannt.

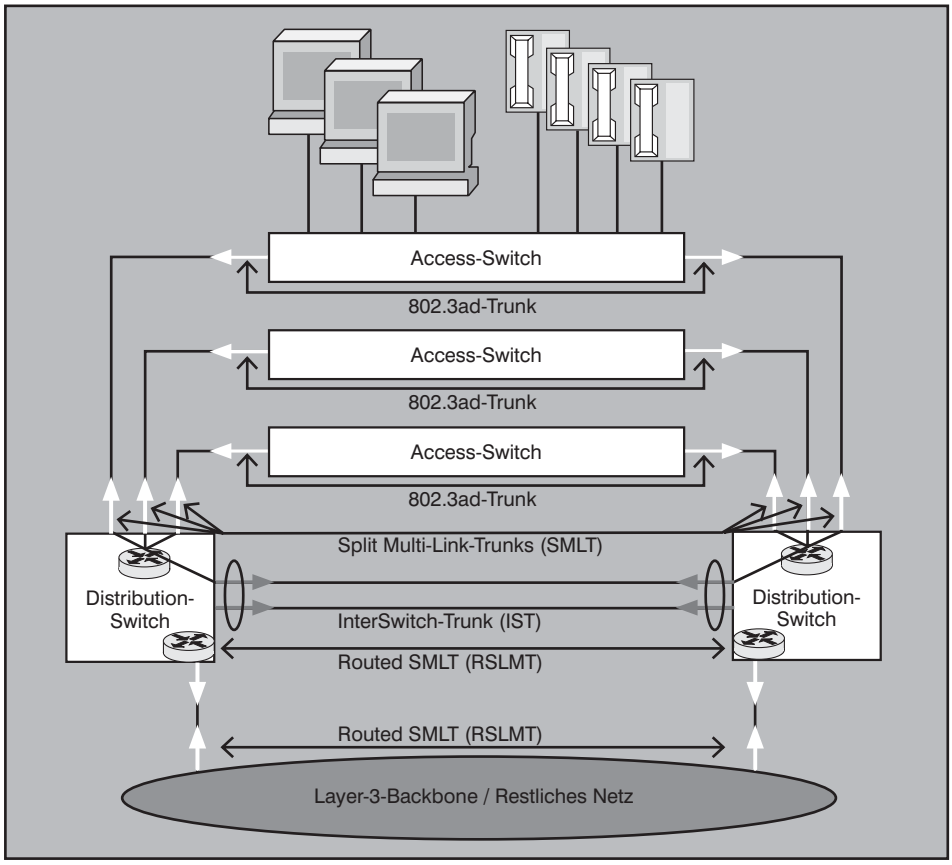



Bild 3: Einsatz von NortelNetworks SMLT und RSMLT für die Steuerung der Redundanz

### VRRP mit Verzicht auf Spanning-Tree

Eine Variation der zuvor erläuterten Designs entsteht, indem auf Layer-2-Strukturen in den Access-Bereichen so weit verzichtet wird, dass jeder Access-Switch ein eigenes IP-Netz darstellt und an den Distribution-Switches auf einem Routing-Inferface abgeschlossen wird. Dadurch können nun im Access-Bereich keine Layer-2-Schleifen mehr entstehen und es kann auf ein entsprechendes Layer-2-Steuerverfahren verzichtet werden.

Bild 4 zeigt diese Art der Layer-3-Microsegmentierung. Diese Verschaltung ist zunächst für viele Umgebungen nicht umsetzbar, da immer noch nicht-routing-fähige oder nicht-IP-Protokolle eingesetzt werden oder die Netzwerkdesigner eine Layer-2-Strukturierung als Designziel anstreben. Dennoch existieren für das beschriebene Design viele dem Autor bekannte Beispiele, die sich gute Betreibbarkeit und hohe Stabilität auszeichnen. Dies gilt übrigens auch bei Einsatz anderer Router-Redundanzverfahren wie Cisco HSRP oder Foundry VRRPE.

Das Umschaltverhalten der in Bild 4 gezeigten Konstellation entspricht derjenigen der zuvor dargestellten RSTP-/VRRP-Lösung, nur dass nun der RSTP-Anteil entfällt und bei jeder Störung direkt VRRP und OSPF greifen. Die Umschaltzeiten sind dabei identisch wie zuvor beschrieben (maximal 4 Sekunden für VRRP und ca. 1 Sekunde für OSPF).

Der Vorteil dieser Lösung liegt zunächst darin, dass auf Basis von standardisierten Protokollen ein Verzicht auf RSTP durchgeführt werden kann und dass gleichzeitig die Uplinks der Access-Switches im Normalfalle nicht blockiert betrieben werden. Allerdings gilt die Blockierungsfreiheit nur für die Kommunikationsrichtung vom Distribution-Switch zum Access-Switch. Der Access-Switch schickt alle nach außen gerichteten Pakete an den VRRP-Master, also nur einen der beiden Distribution-Switches. Der hierdurch entstehende Nachteil ist jedoch akzeptabel, wenn ohnehin wesentlich mehr Informationen vom Netz zu den Endgeräten als umgekehrt übertragen werden. Ein solches Kommunikationsprofil dominiert in den meisten Access-Bereiche der Unternehmensnetze.

### GLBP - eine Erweiterung von HSRP

Um die Bandbreiten-Ineffizienz von VRRP zu umgehen, haben verschiedene Hersteller proprietäre Erweiterungen eingeführt. Eine davon wurde von Cisco Systems unter dem Namen Gateway Load Balancing Protocol (GLBP) eingeführt. Dieses Verfahren setzt auf dem ebenfalls Cisco-proprietären Hot Standby Redundancy Protocol (HSRP) auf und erweitert dessen Funktionalität um eine Lastverteilung und eine Parametrierbarkeit der Timerwerte im Millisekundenbereich.

HSRP funktioniert grundsätzlich sehr ähnlich wie das zuvor beschriebene VRRP jedoch mit verschiedenen Detailunterschieden, die hier nicht weiter betrachtet

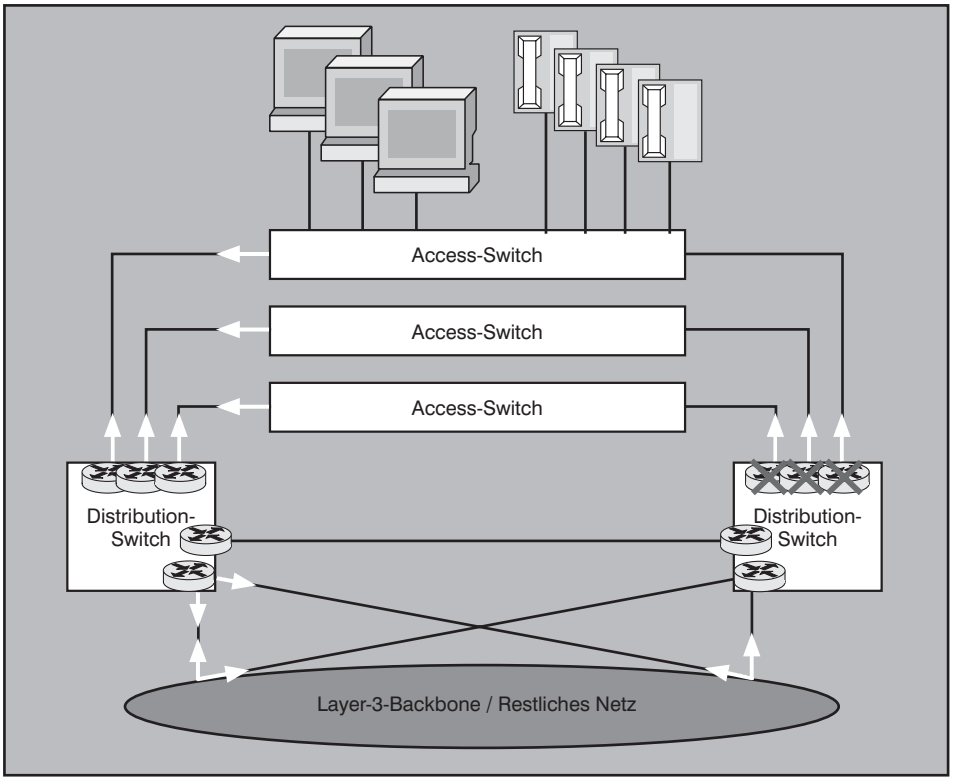



Bild 4: Verzicht auf Layer-2-Strukturen und Einsatz von VRRP für die Steuerung der Redundanz

werden sollen. Es ist möglich, die HSRP-Timer-Werte so einzustellen, dass ein Ausfall des HSRP-Active-Routers ebenfalls nach maximal 4 Sekunden erkannt und behoben wird (Hersteller-Default-Wert: 10 Sekunden).

GLBP führt nun zusätzlich eine Lastverteilung zwischen den beteiligten Routern ein, indem nicht nur eine, sondern bis zu vier virtuelle MAC-Adressen verwendet werden, die den teilnehmenden Routern fest zugewiesen werden. Dafür wird bei GLBP zunächst ein so genanntes Active Virtual Gateway (AVG) gewählt, das die virtuellen MAC-Adressen verwaltet und den teilnehmenden Routern zuweist. Die Lastverteilung wird dann dadurch erreicht, dass die ARP-Requests der Clients vom AVG nach einem einstellbaren Algorithmus mit den verschiedenen virtuellen MAC-Adressen beantwortet werden. Die Endgeräte im Access-Bereich werden dadurch hinsichtlich ihres Default-Gateways auf die teilnehmenden Router aufgeteilt und jeder Router übernimmt für einen Teil der Endgeräte die Funktion der Paket-Vermittlung ins übergeordnete Layer-3-Netz. Das Verfahren ist für die Endgeräte wie VRRP auch transparent, das heißt, sie verwenden alle eine einzige IP-Adresse für das Default-Gateway.

Wird nun in der zuvor beschriebenen VRRP-Verschaltung VRRP durch GLBP ersetzt und werden die Timer-Werte des GLBP entsprechend scharf eingestellt, so wird eine Lastverteilung auf die Distribution-Switches erzielt und zusätzlich sind für die Gateway-Redundanz nun auch Umschaltzeiten im Bereich von 1 Sekunde erreichbar. Bild 5 zeigt diese Konstellation. Da es sich um ein vergleichsweise neues Verfahren handelt, das zudem nur für einen Teil der Routing-Komponenten des Herstellers Cisco Systems implementiert ist, sind dem Autor noch keine Praxiswerte zur Stabilität bei verschärften Umschaltzeiten bekannt (Im Hersteller-Default ist das Timing von GLBP identisch mit demjenigen von HSRP).

### Entscheidung für eine Lösung

Die beschriebenen Verfahren zur redundanten Absicherung des Access-Bereichs stellen wie gesagt eine Auswahl einer unüberschaubaren Vielzahl an Lösungen dar. Ein gutes Netzwerkkonzept muss zwischen den gezeigten und weiteren möglichen Lösungen das Optimum ermitteln.

Bezüglich der Umschaltzeiten sind die proprietären Verfahren in der Regel im Vorteil, wie Tabelle 1 zeigt. Die proprietären Verfahren erreichen das gewünschte Umschaltverhalten vollständig. Standardisierte Verfahren schalten in Extremsituationen langsamer.

Eine vollständige Nutzung aller installierten Bandbreiten ist nur mit den proprietären Verfahren möglich, wie ebenfalls in Tabelle 1 erkennbar. Die proprietären

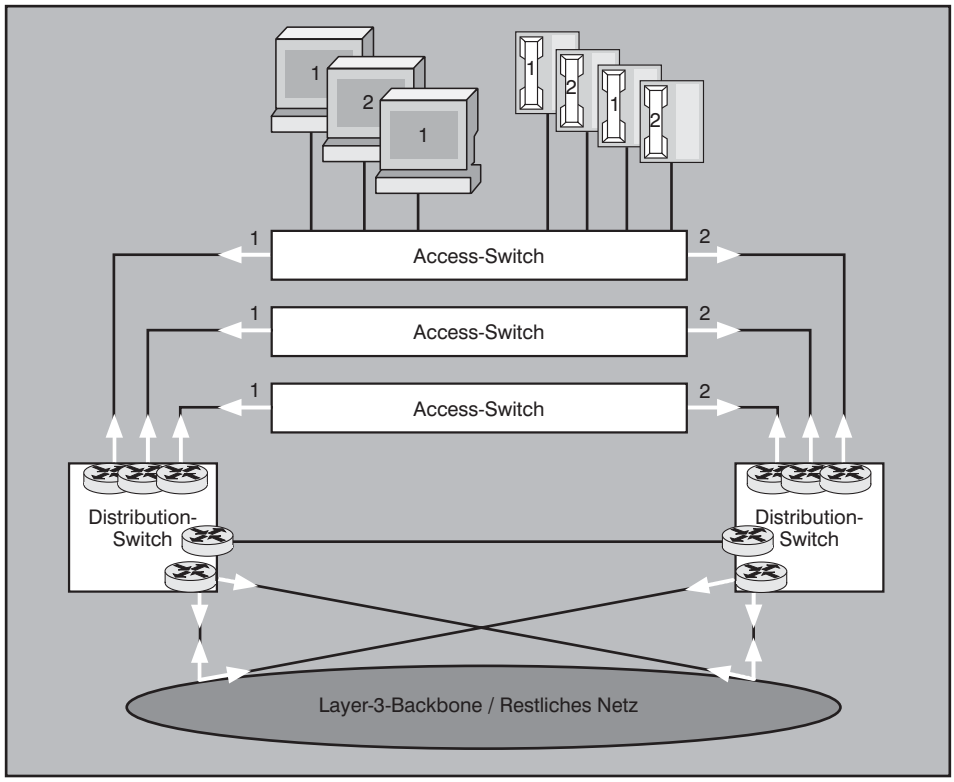



Bild 5: Einsatz von GLBP für eine bandbreiteneffizientere Steuerung der Redundanz

| | Maximale Umschaltzeit bei ungünsstiger Störung | Bandbreitennutzung im Normalbetrieb |
|---|---|---|
| RSTP mit VRRP | ≤ 4 Sekunden | 50% |
| SMLT mit RSMLT | ≤ 1 Sekunde * | 100% |
| VRRP ohne STP | ≤ 4 Sekunden | Richtung Backbone: 50%<br>Richtung Acces-Switch: 100% |
| BLBP ohne STP | ≤ 1 Sekunde * | 100% |

Tabelle 1: Umschaltzeiten der diskutierten Verfahren * Herstellerangaben

Verfahren nutzen im Normalbetrieb bis zu100% der Bandbreite aus. Die VRRP-Lösung nutzt die Bandbreiten abhängig von der Kommunikationsrichtung halb oder vollständig, während Spanning-Tree-Verfahren bei redundanter Verschaltung immer 50% der Bandbreite blockieren.

Die Betreibbarkeit der NortelNetwork-Verfahren SMLT und RSMLT sind aus Sicht des Autors kritisch zu bewerten, da Kommunikationspfade - wenn überhaupt - nur mühsam bestimmt werden können. Dieses Problem haftet allen Link-Aggregation-Techniken an. Das RSTP-Design bietet den Nachteil, dass drei Verfahren (RSTP, VRRP und OSPF) koordiniert und im Fehlerfalle analysiert werden müssen. Außerdem bieten die Switches für RSTP in der Regel keine aggregierte Auskunft über die gesamte Layer-2-Topologie an. Daher sind bezüglich der Betreibbarkeit die beiden Layer-3-microsegmentierten Lösungen auf Basis von VRRP und GLBP als optimal zu bewerten.

Die Entscheidung für oder gegen eines der Verfahren ist sicherlich individuell zu treffen. Proprietäre Verfahren sind in manchen Umgebungen tabu und sollten nach Einschätzung des Autors aufgrund der schlechteren Vorhersagbarkeit des Verhaltens nur zurückhaltend und nur bei zwingenden Gründen eingesetzt werden.

Andererseits sind viele Umgebungen per se herstellerhomogen aufgebaut oder erfordern aufgrund der technischen Aufstellung des Betreibers die Unterstützung des Herstellers und erlauben daher auch den Einsatz proprietärer Verfahren. Wenn also sehr schnelle Umschaltzeiten oder eine möglichst hohe Bandbreiten-Effizienz im Vordergrund stehen, so sind proprietäre Verfahren unter bestimmten Bedingungen im Vorteil.

### Literaturhinweise


1. NortelNetworks, eliminate single points of failure, Whitepaper, 03.06.2004 http://www.nortel.com/products/01/passport/8600_rss/collateral/nn108460-060304.pdf
2. IEEE, IEEE Std 802.1w-2001, Amendment to IEEE Std 802.1D, 14.06.2001
3. Cisco Systems, GLBP Gateway Load Balancing Protocol, Product Feature Guide, 19.10.2004 http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a00801541c8
4. Cisco Systems, Gateway Load Balancing Protocol Overview, Whitepaper, 22.09.2004 http://www.cisco.com/en/US/partner/tech/tk869/tk769/technologies_white_paper0900aecd801790a3.shtml
5. Cisco Systems, Understanding Rapid Spanning Tree Protocol, Whitepaper, 04.03.2005 http://www.cisco.com/en/US/partner/tech/tk389/tk621/technologies_white_paper09186a0080094cfa.shtml

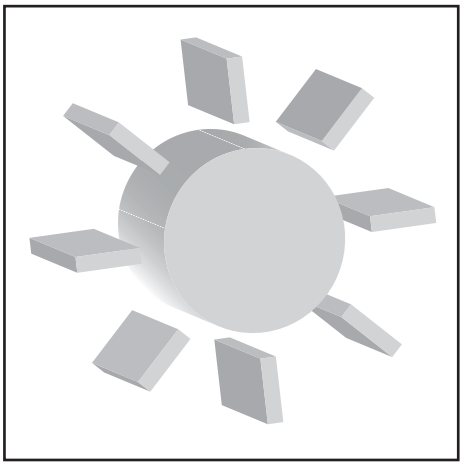
Top-Sommer-Veranstaltung

# Sommerschule 2005 - Intensiv-Update auf den letzten Stand der Netzwerk-Technik Netzwerk-Design im Brennpunkt

Vom 04.-08. Juli veranstaltet die ComConsult Akademie ihre diesjährige Sommerschule in Aachen.

Netzwerke unterliegen einer permanenten Weiterentwicklung. Der aktuelle Design-Wettbewerb von ComConsult-Research, an dem sich nahezu alle führenden Hersteller beteiligten, unterstreicht dies sehr stark. Vor allem der Wunsch nach Benutzertrennung und nach kürzeren Konvergenzzeiten hat zu starken Änderungen im Backbonedesign, aber auch in den eingesetzten Verfahren geführt. Produkte haben sich entsprechend geändert. Moderne Switch-Systeme bieten einen deutlichen Zugewinn an Gestaltungsfunktionalität für leistungsstarke und sichere Netzwerke.

Die Sommerschule 2005 greift die aktuellsten Entwicklungen auf, stellt die wichtigsten Trends zur Diskussion und gibt Empfehlungen zur Weiterentwicklung und Verbesserung bestehender Netzwerke. Einige wichtige Themen in der Übersicht:



- Verändertes Campus-Design und Segmentierung
- Konvergente Netzwerke und ihre Konsequenzen
- Quality of Service als Basis einer Verkehrstrennungs-Strategie
- Ausdehnung Layer-3 bis in den Edge-Bereich
- Voice-Ready Netzwerke: was heißt das
- Sicherheit im Netzwerk und seine praktische Umsetzung: 802.1x und aufsetzende Gestaltungen
- Wireless-LAN-Architekturen und Integration
- Rechenzentren im Web und Änderungen im WAN-Design

Die Sommerschule 2005 bietet den 5-Tages-Intensiv-Update auf den letzten Stand der Netzwerk-Technik. Wir haben für Sie die aktuellen Entwicklungen analysiert, Erfahrungen aus Labor und gerade abgeschlossenen Projekten eingearbeitet und daraus eine Auswahl aus den zur Zeit anliegenden Top-Themen getroffen.

Zur Sicherstellung der Diskussionsfähigkeit und einer interaktiven Kommunikation haben wir die Teilnehmerzahl begrenzt. Zögern Sie deshalb nicht, sich schnell einen Platz in dieser herausragenden Veranstaltung zu sichern.

## Montag, der 4.7.2005

**Neue Netzwerk-Technologien und ihr zukünftiger Einfluss auf das Design und die Nutzung von Netzwerken**
- Was sich im Bedarf ändert
- Mehr Bandbreite und ihre Verwendung
- Hierchische Architekturen
- Zonen und Sicherheits-Konzepte
- Neue Wireless-Technologien: WiMAX

*Dipl.-Inform. Petra Borowka, UBN*

**Netzwerk-Konvergenz und seine Handhabung in der Praxis**
- Herausforderung: Integration Sprache, Daten, Produktion, Logistik, Meldetechnik
- Unterschiede in den Anforderungen
- Power over LAN
- VLAN-Technologie 2005: wann und wie einsetzen
- Quality of Service
- IP-Adressierung unter Druck
- Anschluss von PC und Telefon am Arbeitsplatz
- Herausforderung Sicherheit
- Kosten

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

## Dienstag, der 5.7.2005

**Netzwerk-Design im Umbruch**
- LAN-Redesign
  - Neues Campus-Design
  - Senkung der Konvergenzzeiten: neue Verfahren in der Übersicht
  - Quality of Service als Basis einer Verkehrstrennung?
  - Service-Level-Betrieb
- Integration-Aufgaben und ihre strukturelle Lösung
  - WLAN-Integration
  - Voice-Integration
- Struktur und Empfehlungen für ein Redesign
  - Strukturbausteine
  - Wesentliche Design-Regeln

*Dipl.-Inform. Petra Borowka, UBN*

**Der ComConsult Research-Design-Wettbewerb**
- Vorgegebenes Szenario
- Design-Alternativen der Hersteller
- Analyse: welche Verfahren liegen im Trend
- Analyse: wie ändern sich Switch-Produkte
- Vorstellung der besten Designs und herausragender Design-Elemente
- Zusammenfassung und Bewertung
- Empfehlungen für die Teilnehmer

*Dipl.-Inform. Petra Borowka, UBN*

Sommerschule 2005

## Mittwoch, der 6.7.2005

**Rechenzentrum im Web: Funktionselemente und Umsetzung globaler Datacenter als Basis des Redesigns von Wide Area Networks**

- Globale Strukturen, Daten und Dienste als zentrales Datacenter-Angebot
- Trends für die zukünftige WAN-Nutzung und ihre Auswirkungen auf das Design
- Messungen aus aktuellen Projekten
- Eigenrealisierung: wann sinnvoll, wann nicht
- Internet-VPN als Alternative zu MPLS, ATM und Frame Relay
- QoS-Angebote der Carrier
- Tipps für Ausschreibungen

*Dipl.-Inform. Andreas Meder, ComConsult Beratung und Planung GmbH*

**Sicherheit im Netzwerk: Verfahren, Strategien und Konzepte**

- Zugangssteuerung und Rechtezuweisung durch Einsatz von 802.1x
- Weitergehende Konzepte: Bildung virtueller Benutzergruppen
- Typische Problembeispiele und ihre Handhabung: Trennung von PC und Telefon
- Varianten der Trennung von Vertrauensbereichen: VLAN, MPLS, Virteulle Router und ACL in der vergleichenden Analyse
- Verschlüsselung Ende-zu-Ende: ist das machbar und für welche Anwendungen gilt das
- Intrusion Detection und Prevention
- Anomalie-Erkennung
- Sicherheit im WLAN und seine praxisgerechte Umsetzung

*Dr. Simon Hoff, ComConsult Beratung und Planung GmbH*

## Donnerstag, der 7.7.2005

**IP-Telefonie in der Praxis**

- Migration: von alt nach neu, aber wie
- Erfahrungen aus Ausschreibungen und Migrationsprojekten
- Wie Voice-tauglich sind bestehende Netzwerke: Ergebnisse aus Einmessungen und laufenden Projekten
- Mehrpunkt-Konferenztechnik und ihre Umsetzung
- Planungsansätze
- Projekterfahrungen
- Wirtschaftlichkeit
- Voice im WAN versus Voice über öffentliche Provider-Netzwerke: welcher Weg ist sinnvoller?

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

**Produkte, Hersteller, Trends**

- Alcatel, Cisco und Siemens im Vergleich
- Wohin geht der Trend
- Wo werden wir in 1 bis 3 Jahren stehen
- Wo liegen Grenzen der Entwicklung

*Dipl.-Inform. Petra Borowka, UBN*

**Der zukünftige Mega-Standard SIP**

- Struktur und Arbeitsweise von SIP
- Testbericht und Erfahrungen mit SIP-Clients und SIP-Servern
- SIP als Basis für Multimedia-Lösungen: Vision oder Realität?
- Problembereich NAT-Traversal
- Empfehlungen und Diskussion

*Markus Schaub, ComConsult-Research, German-SIP-Center*

## Freitag, der 8.7.2005

**Wireless-Networks**

- Varianten
- Nutzbarkeit neuer Technologien
- Controller-based Architekturen und ihre Vorteile
- Dynamische Frequenz- und Kanalwahl
- Dynamische Steuerung der Sendeleistung
- Roaming: Stand der Technik
- Voice im WLAN: Stand der Technik und Ausblick
- Architekturen
- Produkte
- Planung und Design
- Betrieb
- Sicherheit in Netzwerken

*Dr. Simon Hoff, ComConsult Beratung und Planung GmbH*

Änderung im Programm behält sich der Veranstalter vor!

Fax-Antwort an ComConsult 02408/955-399

# Anmeldung
# Sommerschule 2005

☐ Ich buche das Seminar
**Sommerschule 2005**
vom 04.07. - 08.07.05 in Aachen
zum Preis von € 2.290,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____05

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

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

Report des Monats

# Planung für Voice over IP

## Evaluierung von Architekturen und Details zur Realisierung

Der aktuelle Technologie-Report von ComConsult Research erarbeitet einen Leitfaden zur Umsetzung von IP-Telephonie in der Praxis. Lesen Sie im Folgenden einen Ausschnitt aus dieser Studie.

### 5.1 Methoden für das Konfigurationsmanagement

Diverse Methoden können für das Konfigurationsmanagement von IP-Telefonen eingesetzt werden, z. B.:

- Die Änderung der Konfigurationsdateien auf einem Bootserver (z. B. TFTP-Server) entweder individuell für jedes Telefon oder generell für alle Telefone ist die wichtigste Methode, um die Konfiguration einer Vielzahl von IP-Telefonen zu managen.
- Am Telefon selbst können mittels der fest vorgegebenen und konfigurierbaren Tasten beispielsweise menügesteuert Einstellungen vorgenommen werden. Diese Methode ist in einigen Fällen der Fehlersuche vor Ort nützlich.
- Falls ein Telnet-Server auf dem IP-Telefon unterstützt wird, greifen viele Administratoren zum Werkzeug des Zugriffs über das Netz, um auf einem VoIP-Endgerät beispielsweise gezielt Fehlersuche zu betreiben.

**1.1 Konfigurationsparameter**

Die an einem IP-Telefon einzustellenden Konfigurationsparameter sind z. B.:

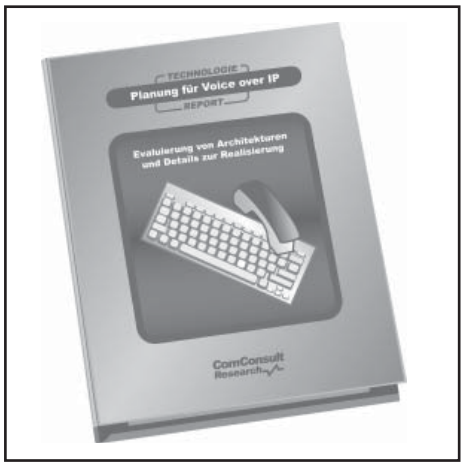
- Netzeinstellungen, u. a. Ethernet-Einstellungen,
- spezielle VoIP-Settings wie SIP-Parameter etc.,
- allgemeine Geräteeinstellungen wie Datum, Uhrzeit, Zeitzone, Sommer-zeit/ Winterzeit.

Im Folgenden wird auf einige dieser Parameter eingegangen.

**1.1.1 Anschlussmodelle**

Für die Netzeinstellungen an IP-Telefonen ist die Unterscheidung zwischen den in Abbildung 5.1 dargestellten Anschlussmodellen relevant (siehe auch Abschnitt 4.1).

Wenn das IP-Telefon einen integrierten Miniswitch beinhaltet, können das Telefon und der an den Miniswitch angeschlossene PC in einem VLAN betrieben werden. Alternativ können das IP-Telefon und der PC aber auch zwei separaten VLANs an-




gehören. In diesem Fall muss der im IP-Telefon integrierte Miniswitch VLAN Tagging gemäß IEEE 802.1Q unterstützen.

Wenn das IP-Telefon über keinen integrierten Miniswitch verfügt, sind die folgenden Fälle zu unterscheiden:

- Telefon und PC am selben Access-Switch und im selben VLAN,
- Telefon und PC am selben Access-Switch, aber in separaten VLANs,
- Telefon und PC an separaten Access-Switches, jedoch im selben VLAN,
- Telefon und PC an separaten Access-Switches und in separaten VLANs.

Die Vor- und Nachteile der Zuordnung von Daten- und Sprachendgeräten zu denselben bzw. unterschiedlichen VLANs sind bereits im Abschnitt 4.1 dargestellt worden, weshalb im Folgenden nur auf die unterschiedlichen physikalischen Anschlussmodelle eingegangen wird.

**1.1.2 Layer-2-Einstellungen**

Einige der folgenden Layer-2-Parameter können je nach Produkt auf IP-Telefonen eingestellt werden:

- VLAN-ID: Wenn der im IP-Telefon integrierte Miniswitch IEEE 802.1Q unterstützt, muss die VLAN-ID gesetzt werden. Bei manchen Konfigurationen wird diese VLAN-ID jedoch von der Einstellung am Access-Switch überschrieben. In diesen Fällen ist die Einstellung am Telefon irrelevant. Bei manchen Produkten wird zwischen administrativem und operativem VLAN unterschieden. Manche Access-Switches können dem Telefon die VLAN-ID vorgeben. Dies ist in der Regel nur dann möglich, wenn der Access-Switch und das IP-Telefon vom selben Hersteller stammen, weil das Protokoll zur Einstellung der VLAN-ID durch den Access-Switch proprietär ist.
- MAC-Adressen können bei IP-Telefonen in der Regel nicht verändert werden, weil sie bei veränderlichen IP-Adressen als Identifikationsmerkmal von IP-Telefonen dienen.
- Ethernet-Einstellungen pro Port (es sind mehr als ein Port zu berücksichtigen, wenn im IP-Telefon ein Miniswitch integriert ist):
  - Einstellung der Bitrate auf 100 Mbit/ s oder 10 Mbit/s oder automatische Aushandlung
  - Einstellung des Duplexmodus auf Vollduplex oder Halbduplex oder automatische Aushandlung

Die folgenden Vorgaben für die Ethernet-Einstellungen auf der Strecke zwischen dem Access-Switch auf der einen und dem Endgerät bzw. IP-Telefon auf der anderen Seite haben sich in der Praxis bewährt:

- Einstellung der Bitrate auf 100 Mbit/s im Normalfall und auf 10 Mbit/s, wenn der Access-Switch, die Verkabelung oder das IP-Telefon 100 Mbit/s nicht unterstützen.
- Im Normalfall wird am IP-Telefon und am Switch Auto Negotiation aktiviert und somit erreicht, dass 100 Mbit/s full duplex automatisch eingestellt wird. Ausnahmen von dieser Regel sind wie folgt:
  - Wenn Implementierungsfehler dazu führen, dass der Negotiation-Prozess fehlerhaft ist und zu unterschiedlichen Duplex-Einstellungen an den beiden Enden des Links führt, wird am Endgerät 100 Mbit/s half duplex fest eingestellt. Die feste Einstellung auf Vollduplex würde mit der Gefahr von Duplex Mismatch verbunden sein, weil bei Ausbleiben der Negotiation Response ein Gerät auf Halbduplex zurückfällt und somit Situationen entstehen können, in denen Duplex Mismatch herrscht.
  - Bei Mischverkabelung in einem Gebäude (Mischung von 100-Mbit- und Nicht-100-Mbit-fähiger Verkabelung)

werden die Access-Switchports im Gebäude auf 100 Mbit/s half duplex bzw. 10 Mbit/s half duplex eingestellt.

Diese verschiedenen Szenarien gehen aus der folgenden Abbildung hervor:

Analog können für die Strecke zwischen IP-Telefon und daran angeschlossenem Datenendgerät folgende Festlegungen getroffen werden:

- Einstellung der Bitrate auf 100 Mbit/s im Normalfall und auf 10 Mbit/s, wenn der PC oder das IP-Telefon 100 Mbit/s nicht unterstützen
- Im Normalfall wird am IP-Telefon und PC Auto Negotiation aktiviert und somit erreicht, dass 100 Mbit/s full duplex automatisch eingestellt wird. Ausnahmen sind wie folgt:
  - Wenn Implementierungsfehler dazu führen, dass der Negotiation-Prozess fehlerhaft ist und zu unterschiedlichen Duplex-Einstellungen an den beiden Enden des Links führt, wird am PC 100 Mbit/s half duplex fest eingestellt. Dabei kann am IP-Telefon, falls möglich, auch 100 Mbit/s half duplex eingestellt werden. Anderenfalls ist das Belassen des Telefons in der Standardeinstellung auf Autonegotiation unproblematisch, weil die Kombination von „auto duplex“ am einen und „half duplex“ am anderen Ende eines Links in der Regel keinen Duplex Mismatch verursacht.
  - Wenn aufgrund der nicht 100-Mbit-fähigen Verkabelung im Gebäude die Strecke zwischen Access-Switch und IP-Telefon auf 10 Mbit/s eingestellt wird, muss auch am Endgerät die Einstellung 10 Mbit/s half duplex vorgenommen werden.

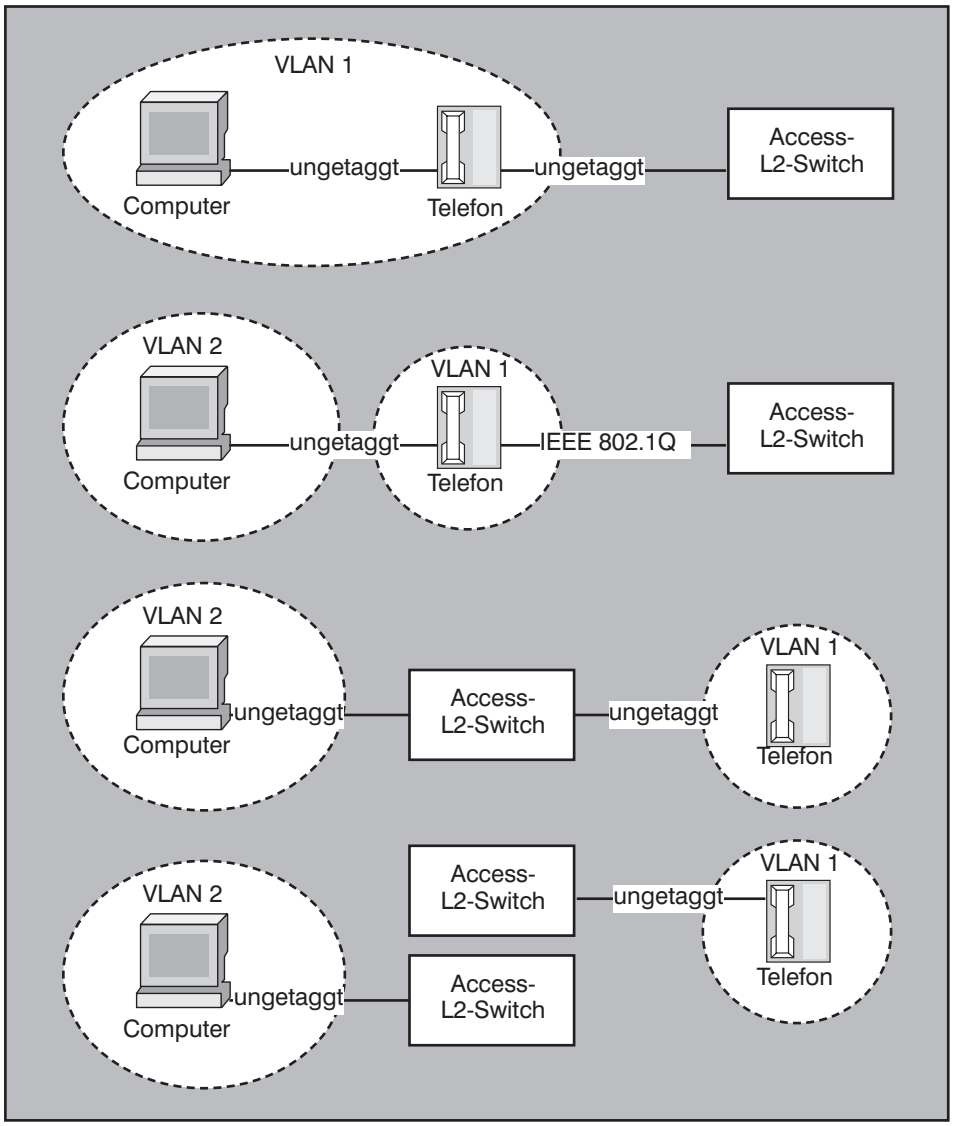



Abbildung 5.1: Anschlussmodelle für IP-Telefone

Schwerpunktthema

# Technologie-trends für Enterprise Redesign: Wireline und Wireless für PAN, LAN, MAN, RAN

Teil 3 - Fortsetzung von Seite 1

Dipl. Inform. Petra Borowka leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern für Kommunikationstechnik. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen und ist seit vielen Jahren Referentin der ComConsult Akademie. Ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt.

- KISS Prinzip
- Deterministisches Verhalten
- Steuerbarkeit und Beherrschbarkeit
- Gewichtung der unverzichtbaren und wichtigen Funktionen gegenüber Ergänzungsfunktionen
  1. Verfügbarkeit
  2. Kapazität
  3. Sicherheit
  4. Quality of Service
  5. Überwachung, Management
- Strukturiertes Design mit bewährten Basisverfahren auf Layer-2 und Layer-3
- Nutzung von Standards und Vereinheitlichung

Das Design-Konzept heißt LND (Layered Network Design), wobei ein spezielles Netzwerk hierarchisch in Design-Ebenen für den Front End Bereich (Endgeräte), den Backbone (Kernnetz) und den Backend Bereich (Server, Speicher) gegliedert wird. In jeder Design-Ebene kann bedarfsgerecht eine sternförmige Struktur (S) oder ringförmige/vermaschte Struktur (R) aufgebaut werden. Je nach Größe des Netzwerks sind dies unterschiedlich viele Ebenen, die allgemeine Bezeichnung eines LND-Designs ist daher

**LND-Xn** mit
X = S, R
n = integer

wobei X die Struktur angibt (S für sternförmig, R für ringförmig) und n für die Anzahl der Design-Ebenen steht (im Regelfall liegt n zwischen 3 und 7). Nachfolgend geben wir ein Beispiel für ein LND-X5 Netzwerk: mit den Design-Ebenen EACCB: Edge, Access, Concentrator, Core, Backend.

Die Edge Ebene besteht im gezeigten Beispiel aus mobilen Endgeräten mit GSM oder WLAN Anschuss und non-Ethernet Produktions-Endgeräten (SPS, Mess-Stationen, Laborgeräte o.ä.). Der Access Bereich besteht aus der äußersten Ebene mit einfachen Ethernet Komponenten, an die Wireline Endgeräte oder Anschaltkomponenten zur Kopplung von non-Ethernet und Ethernet angebunden werden wie WLAN Access Points, Feldbus-Ethernet Verbindungs-Systeme oder Dual homed Systeme.

Für Netzwerke, die einerseits verschiedene Technologien integrieren müssen, sei es Wireline und Wireless oder Echtzeit- und non-Echtzeit, andererseits hohe Anforderungen an Robustheit und Verfügbarkeit haben, werden spezielle Design-Konfigurationen verwendet, die wir als SIRENED, (Structured Integrated REsilient NEtwork Design) bezeichnen.

**SIRENE Design für robuste Netzwerke**

SIRENED beinhaltet mindestens die nachfolgenden Elemente:

- Erhöhte Verfügbarkeit durch Redundanz mit automatischer Fehlerumschaltung, typischerweise als 2er Stern, 3er Ring oder 4er Ring
- Angemessene Leistungs-Provisionierung durch Berechnung der Kapazität in Relation zur benötigten Antwortzeit, um sowohl die benötigte Datenrate als auch die benötigte Antwortzeit zu erreichen
- Flexible Skalierbarkeit hinsichtlich Mengengerüst und Integration neuer Dienste wie Mobilität oder Konvergenz von Daten, Sprache und Video
- Überwachungs- und Diagnose-Funktionalität
- Reduzierung von Komplexität und somit Erreichung von Betriebsoptimierung durch:
  - einheitliche und eingeschränkte Kombination verschiedener Verfahren (STP, RSTP, MSTP, LAG, OSPF, VRRP, GLBP, MPLS, BGP, Port Security, VPN, RAS, .... u.v.a.m.)
  - optimierte Kaskadierung
  - soweit möglich Bevorzugung von FO (Failover) gegenüber LB (Load Balancing)
  - Kosten-Nutzen-Abwägung hinsichtlich Layer-2 vs. Layer-3: handhabbare aber nicht zu kleine L2 Bereiche (Broadcast Domänen), Kopplung von Layer-3 Bereichen mit dynamischem OSPF Routing

**CoSIRENED Design für Service Level Netzwerke**

Für weitergehende Anforderungen zur Einhaltung von Service Level Agreements, z.B. hinsichtlich Sicherheit und Quality of Service / effizienter Ressourcen-Nutzung haben wir eine Erweiterung des SIRENE Designs definiert: Controlled Structured Integrated REsilient NEtwork Design (Co-SIRENED). Hier wird das robuste Basis-Netzwerk je Design-Ebene und Teilnetzwerk kontrolliert um Service Level Funktionen erweitert:

- Im Bereich Sicherheit führt dies zur Einführung von Schutzzonen-Konzepten, innerhalb derer in abgestufter Form ein Login für nicht-authentifizierte Mitglieder oder Mitglieder einer bestimmten Benutzergruppe eingeschränkt oder gar nicht möglich ist.
- Im Bereich Effizienz führt es zur gezielten Abstimmung der Ressourcen aufeinander, insbesondere
  - Server
  - Netzkomponenten
  - passive Infrastruktur
  - Provisionierung: bei Bedarf Priorisierung in Kombination mit Bandbreiten-Limitierung

Abbildung 4.1 zeigt als erstes Beispiel ein LND-RS5 SIRENED (5 Ebenen, mit gemischter Ring- und Stern-Redundanz) Netzwerk mit WLAN Access Points und Feldbus-Systemen im Edge Bereich, welches bewusst so gewählt wurde, dass nicht überall Höchst-Anforderungen vorliegen: Zur Anschaltung der WLAN Access Points wurde Ring-Redundanz geplant, da keine hohe Leistung erforderlich ist, denn die WLAN AP's benötigen lediglich 54 Mbit Shared als Maximalleistung zum Access Bereich ein. Weiterhin wurde eine nicht-redundante Anbindung der Feldbus-Ebene vorgesehen, da nur gelegentlicher Datenaustausch erforderlich und die Access Ebene nicht an Steuer- und Regelprozessen beteiligt ist. Die Verfügbarkeits-Anforderung der zentralen Dienste und somit auch des Backbone führte zu einem redundanten Doppelstern-Design der Concentrator-Ebene im Büro-Umfeld, aus den zuvor genannten Gründen zu einem halbredundanten Stern-Design der Concentrator-Ebenen die die Produktion mit dem Büro-Umfeld verbindet. Das Kernnetz wurde zur Absicherung der Verfügbarkeit zentraler Dienste mit zwei Chassis ausgelegt, an die je nach Anforderung eine vollredundante oder halbredundante Anbindung der Concentrator-Ebene erfolgt, und die ausreichende Skalierbarkeit haben, um einen Ausbau zur flächendeckend vollredundanten Anbindung aller Bereiche an das Kernnetz zu ermöglichen. Passend zum Edge Bereich und Concentrator Bereich sind nicht alle Server vollredundant angebunden. Die nicht-redundant angebundenen Server werden hälftig auf beide Core-Chassis verteilt, wodurch sich eine Halbredundanz ergibt. Als Backend Netzwerk zur Anbindung von Speicherkomponenten sind Fibre Channel Komponenten im Einsatz.

**Nutzung der vorhandenen Infrastruktur**

Ganz Europa ist von den Wireless Verfechtern erobert - alle Kabel auf den Müll? Mitnichten! Es gibt da ein paar kleine Ausnahmen:

Erstens: Im Gegensatz zu Unkenrufen, dass in drei Jahren alle Neuplaner von Verkabelungssystemen in eine Zwangsverwahrung genommen werden, vertreten wir an dieser Stelle eine andere Sichtweise: Nutzen Sie Ihre vorhandene Infrastruktur weiter, da sie in vielen Fällen hierfür geeignet ist und Wireline Systeme nicht innerhalb der nächsten 3 Jahre flächendeckend durch Wireless Komponenten ab-

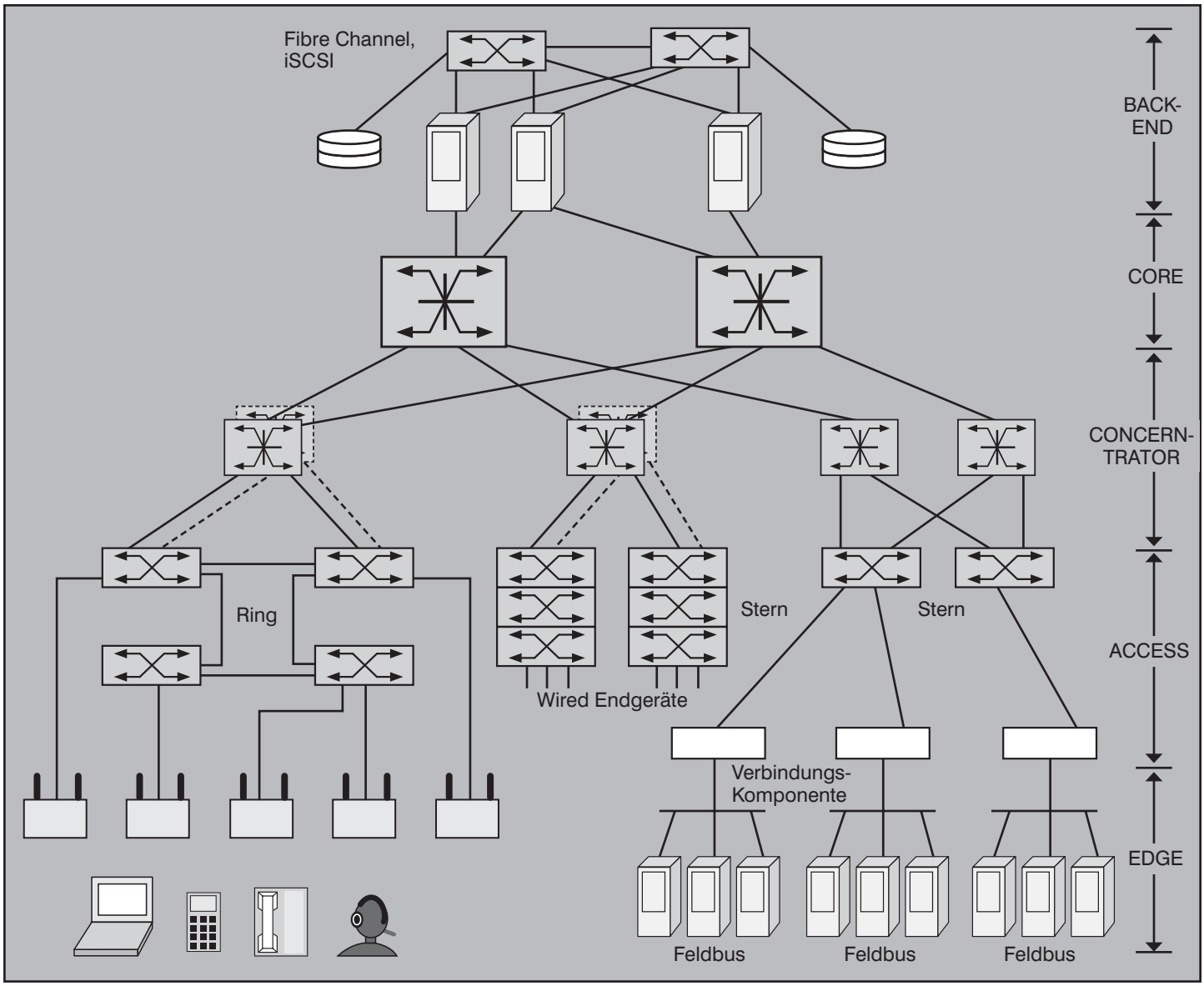



Abbildung 4.1: Beispiel 1, LND-RS5 SIRENED Netzwerk mit WLAN auf der Edge Ebene

lösbar sein werden. Die aktuellen Trends sprechen dafür, dass im Kupferbereich weiterhin bei einem Bedarf von bis zu 10 Gbit am Endgerät Twisted Pair genutzt werden wird (allerdings dann 300 MHz TP Kabel der Link Klasse E / Kategorie 6). Multimode Fasern sind mit zunehmender Verfügbarkeit der ursprünglich ungeliebten Normschnittstelle 10GBase-LX4 immerhin in normaler Güte (500 MHz * km) für Entfernungen bis zu 300 m mit 10 Gbit nutzbar.

Zweitens: Sollen zusätzlich zu allen PC's auch die Telefone in ein IP Netzwerk integriert werden ohne jedoch die Anzahl verfügbarer Switchports zu erhöhen, so können Telefon und PC über den Miniswitch im Telefon kaskadiert werden (siehe Abbildung 4.2). Ein eher visionärer Ansatz wäre an dieser Stelle, die DV-Endgeräte auf WLAN umzurüsten (inklusive der damit verbundenen Leistungs-Einschränkungen!) und so die freiwerdenden Ports für IP Telefone ohne Kaskadierung nutzbar zu machen (siehe Abbildung 4.3). Damit werden Sie sich bei den PC-Benutzern unbeliebt machen. Komplementär dazu ließen sich alle IP Telefone als WLAN Telefone implementieren (siehe Abbildung 4.4), was wiederum verkabelte Anschlussports für die Telefone spart (aber die Sicherheitslücke öffnet, da VoWLAN Telefone aktuell noch kein WPA2 unterstützen! Und zu QoS Implementierung zwingt, da WLAN's aktuell noch als Shared LAN's arbeiten). Damit werden Sie sich bei den Telefon Benutzern unbeliebt machen. Ansatz zwei und drei wollen wir wegen der bekannten Einschränkungen hier noch nicht als ernsthaft zu empfehlende Alternativen verstanden wissen.

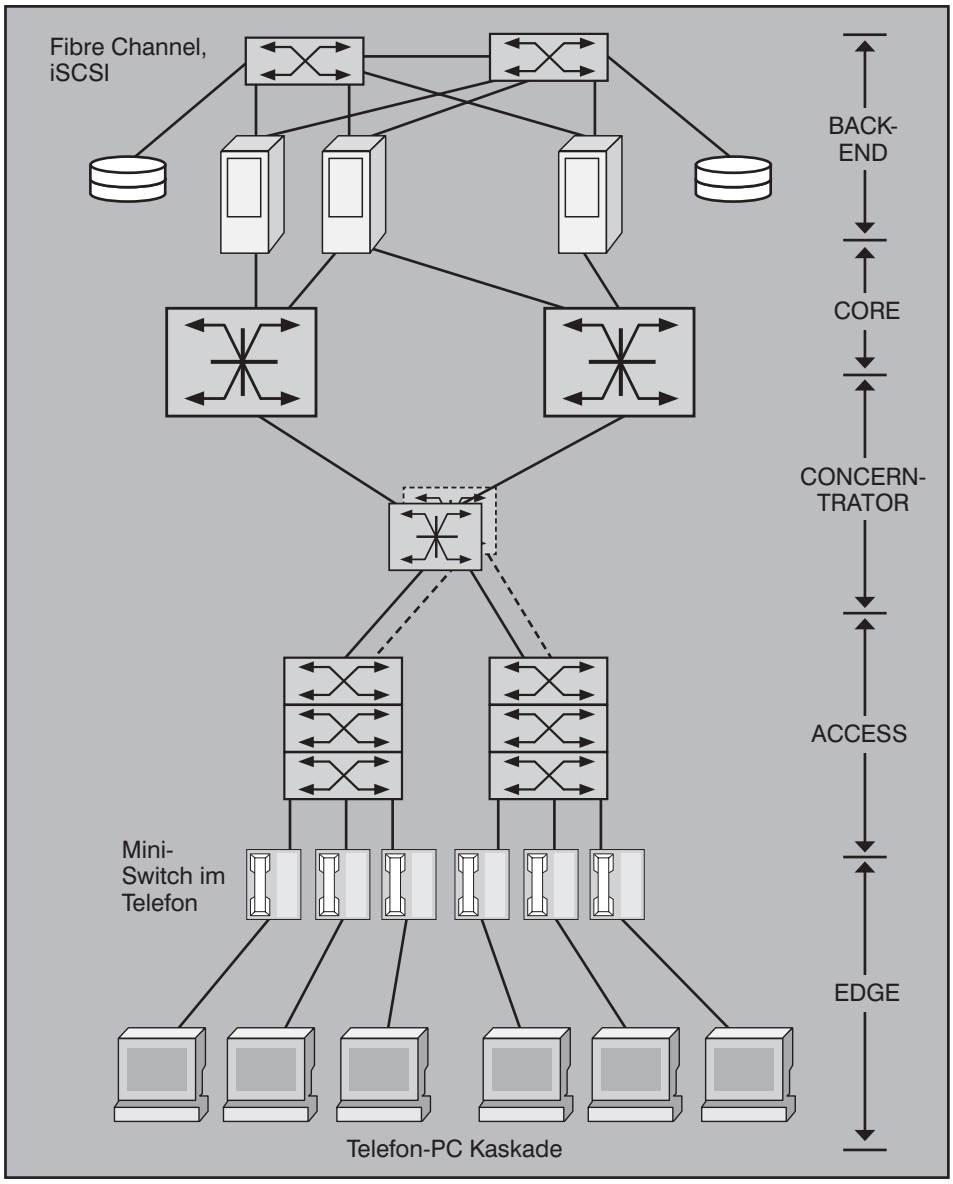



Abbildung 4.2: Abbildung 4.2: PC-Telefon Kaskadierung

Die Anzahl benötigter IP Adressen lässt sich bei allen drei Lösungen nicht reduzieren. Eine Reduktion der benötigten IP Adressen wäre beim Einsatz von Softphones möglich, die jedoch oft aus anderen technischen und funktionalen Gründen nicht zum Einsatz kommen.

Drittens: Soweit Wireless Technologie in einem Standort-Netzwerk integriert werden soll, erfolgt derzeit standardmäßig eine WLAN Anbindung an mindestens das Kernnetz (Concentrator/Core Ebene), speziell an Ethernet Switches. Selbst bei Reduzierung der benötigten verkabelten Anschluss-Ports muss nach wie vor eine flächendeckende verkabelte Infrastruktur erhalten bleiben, da ja die Access Points zum jetzigen Zeitpunkt an Wireline Ethernet angeschlossen werden müssen. Falls Wireless LAN als Ablöse-Technologie für Ethernet implementiert werden soll, so müssen die AP's auch noch redundant angebunden werden, was wiederum die Anzahl verkabelter Anschlussports erhöht.

### 4.2 Redundanzkonzepte mit Wireless und Wireline

Als WLAN-Redundanz-Konzepte hatten wir in Teil 2 die Möglichkeiten mit Dual Radio, Dual AP, Dual Ethernet oder Spanning Tree aufgezeigt. An dieser Stelle zeigen wir Möglichkeiten der Integration von Wireless und Wireline Teilnetzen in einem redundanten Gesamt-Design.

In Beispiel 2 (siehe Abbildung 4.5) wird, als Zukunfts-Perspektive, die ringförmige Ethernet-Anschaltung zum Anschluss mobiler Endgeräte Access-Bereich durch Wireless Technologie ersetzt und somit ein rein sternförmiges Design auf allen Ebenen gewählt (LND-S5). Dies ist mit heutigen Produkten nicht verfügbar, da eine Kaskadierung und Rapid Spanning Tree (RST) von WLAN Access Points nicht sowie „alter" Spanning Tree (STP) kaum unterstützt wird und WiMAX Komponenten noch nicht verfügbar sind. Verfügbar sind jedoch inzwischen Access Points mit doppelter Ethernet Schnittstelle die angegebenen WLAN Switches auf der Concentrator Ebene, die schnelles Roaming innerhalb der Access Points ermöglichen, die am selben WLAN Switch angebunden sind und je nach Hersteller zusätzliche Management- und Ansteuerungs-Funktionen unterstützen.

Alternativ hierzu wird in Beispiel 3 (siehe Abbildung 4.6) zum Anschluss mobiler Endgeräte im Access-Bereich aus Kostengründen ein ringförmiges Design

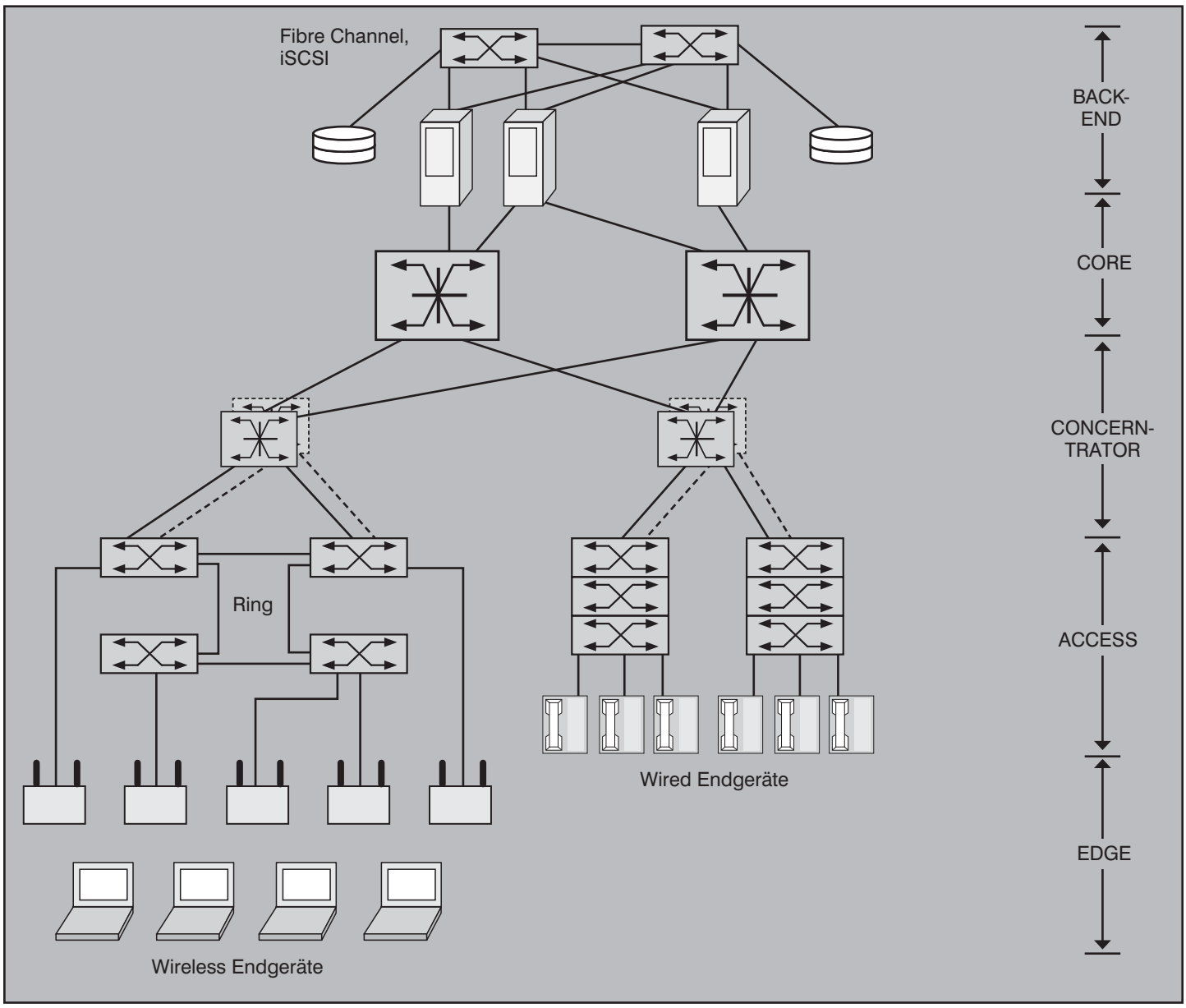



Abbildung 4.3: WLAN PC's und Wireline Telefone

vorgesehen (LND-RS5). Solche Konfigurationsmöglichkeiten werden mittels Standardverfahren möglich sein, wenn vermaschtes WLAN (IEEE 802.11r und 802.11s) oder vermaschtes WiMAX verfügbar werden. Alternativ zu WLAN Switches haben wir hier WLAN Server / Controller vorgesehen, die ein schnelles Layer-3 Roaming oder aber Tunneling mit Beibehaltung des bei Login zugeordneten IP Subnetzes innerhalb des gesamten Standorts ermöglichen.

### 4.3 Service-Level-Orientierung: Bedarf nach Benutzertrennung

Aktuell werden verschiedentlich Argumente oder Anforderungen genannt, die eine Absonderung spezieller Benutzergruppen vom allgemeinen Netzwerk nahe legen oder erfordern, insbesondere unter den Aspekten

- Sicherheit
- Verfügbarkeit
- Leistung, Quality of Service (Durchsatz, Antwortzeit, Verlustrate)

Einige Beispiele für solche Benutzergruppen sind

- Telefone (Durchsatz, Antwortzeit, Sicherheit)
- Wireless Benutzer (Sicherheit)
- Management und Überwachung (Verfügbarkeit, Sicherheit)
- Produktionsnetze, SPS'en (Verfügbarkeit, Antwortzeit)
- Objektschutz (Verfügbarkeit)

**Port-basierte VLAN's**

Ein oft vermarkteter Ansatz zur Umsetzung solcher Anforderungen ist die Definition separater VLAN's, die dann mit unterschiedlicher Funktionalität an das Datennetz gekoppelt sind, im einfachsten Fall mittels Routing / Layer-3 Switching, im komplexeren Fall mittels Firewall-Verbindung, im Extremfall völlig isoliert. Der letztgenannte Fall bedeutet, dass keinerlei integrierte Daten- / TK-Anwendungen zwischen dem isolierten VLAN und dem „Normalnetz" möglich sind, die auf Server wie Datenserver, Verzeichnisse, DNS-

Dienst, DHCP-Dienst, Datenbanken, Telefonieserver etc. zugreifen sondern lediglich Webzugang erhalten oder ebenfalls durch völlig separierte Server bedient werden. Als Konsequenz ergibt sich eine entsprechend reduzierte Funktionalität. Dafür ist die erreichbare Sicherheits-Abschottung relativ hoch. Eine weitere Hoffnung ist, mit separaten VLAN's einen einfachen Ansatz für implizite Priorisierung gefunden zu haben (Policy: Bearbeite alle Pakete mit dem VLAN Tag 122 mit der Priorität „Hoch").

Die genannten VLAN's lassen sich über feste Portzuordnung konfigurieren, indem alle Switchports, an denen bestimmte Endgeräte angebunden sind, einem entsprechenden VLAN zugeordnet und alle weiter kaskadierten Uplinks als getagte Verbindungen konfiguriert werden. Wird eine kaskadierte Lösung PC - Telefon eingesetzt, so muss gegebenenfalls ab dem Miniswitch im Telefon bis zum nächsten Layer-3 Switch Tagging (T) konfiguriert werden. Kaskadierte Anschaltung mit Konfiguration separater VLAN's erfordert, nicht-kaskadierte Anschaltung vermeidet Tagging im Telefon-Miniswitch. Sind lediglich die Handapparate (Hardphones) als separate VLAN's abgetrennt und alle anderen Geräte gebäude-orientierten IP Subnetzen/ VLAN's zugeordnet, lässt sich die notwendige Übersichtlichkeit noch näherungsweise erreichen. Dennoch ist der Anfang einer VLAN Zersplitterung innerhalb einer Etage und etagenübergreifend erkennbar. Diese Trennung lässt sich jedoch auf weitere Benutzergruppen, z.B. WLAN Geräte, Gast-User, Externe u.ä. ausdehnen. Vielfach wird dies aufgrund erhöhter Sicherheitsanforderungen insbesondere für WLAN-Einsatz so gefordert.

Im Normalfall wird jedes VLAN einem eigenen IP Subnetz zugeordnet, so dass die Einrichtung separater VLAN's gleichzeitig die Einrichtung von separaten IP-Subnetzen für alle entsprechenden Benutzergruppen bedeutet. Die resultierende Zersplitterung wird in diesem Fall deutlich größer und verschärft sich mit fortlaufender Betriebszeit.

Darüber hinaus ist die Lösung nicht generisch einsetzbar, denn an dieser Stelle

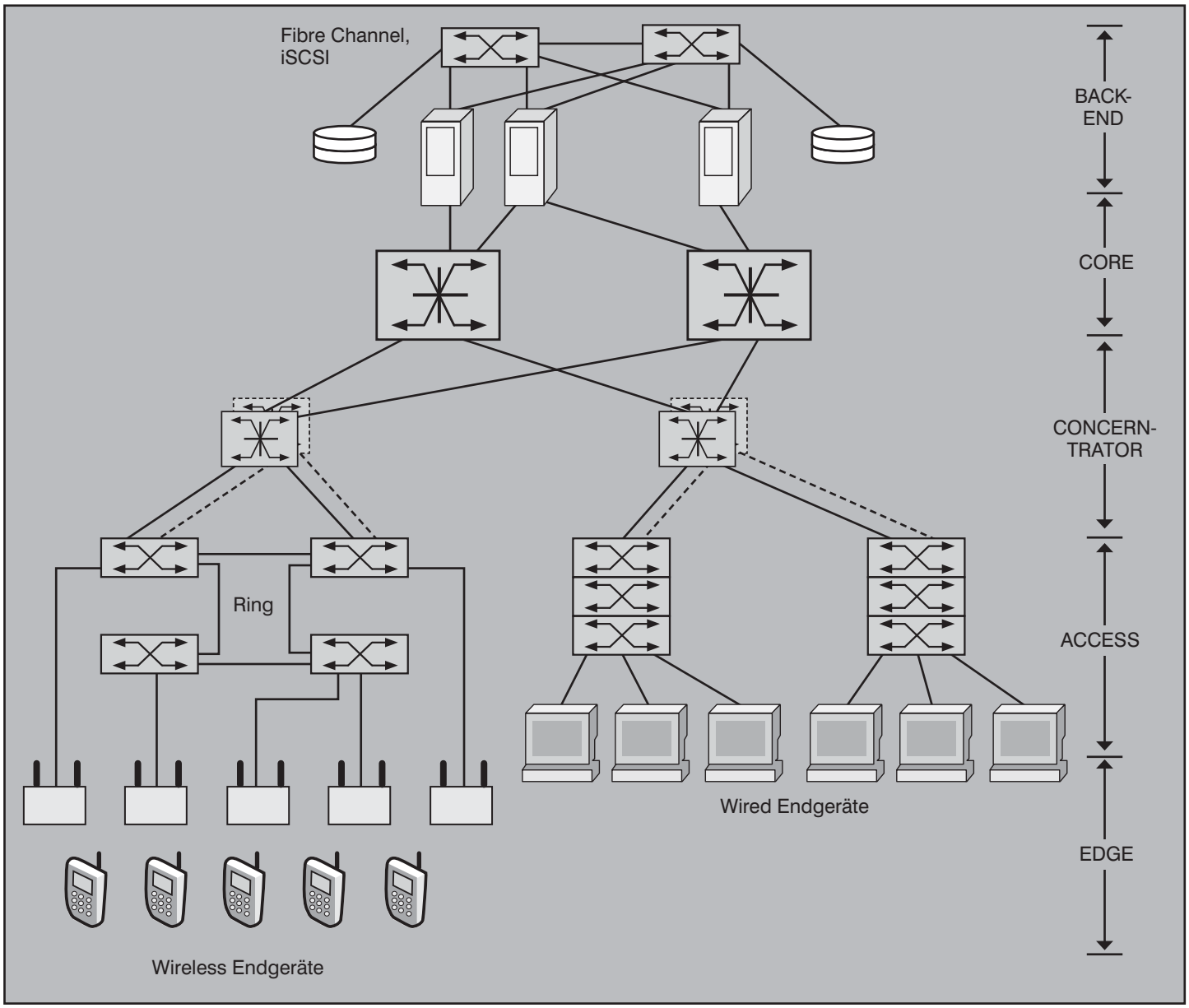



Abbildung 4.4: WLAN Telefone und Wireline PC's

sind einige Fragen zu klären, deren Antwort jeweils projektspezifisch gefunden werden muss, insbesondere:

- Welchem VLAN/IP Subnetz werden Ethernet PC‘s, und Laptops und mit Softphone zugeordnet?
- Welchem VLAN werden WLAN Telefone zugeordnet?
- Welchem VLAN werden WLAN Laptops und WLAN PDA‘s mit Softphone zugeordnet?
- Welchem VLAN werden Bildschirmtelefone mit Webzugang zugeordnet?

Zur Steigerung der Übersichtlichkeit kann hier die VLAN-Zuordnung mit festen Ports verbunden werden: Eine denkbare, noch einigermaßen übersichtliche Lösung kann das Vorhalten fester Ports je Etagenswitch für Wireless und Monitoring sein, z.B. immer der Port 24 oder 48 für Monitoring, Ports 17-23 oder 41-47 für den Anschluss von WLAN Access Points, auch wenn diese dann nicht in jedem Fall aktiv genutzt werden. Als Erweiterung kann festgelegt werden, dass die Zuordnung von WLAN Telefonen zum Wireless VLAN, die Zuordnung von IP Handapparaten zu separaten Telefonie-VLAN‘s und die Zuordnung aller Softphones zu den jeweiligen allgemeinen Etagen-Subnetzen (sowohl bei Wireless als auch bei Wired Laptops / PC‘s) erfolgt. Allerdings wird schon aus der Grafik ersichtlich, dass diese Lösung zu einer deutlichen VLAN-Zersplitterung und erzwungenem Tagging für alle Uplinks führt. Zudem entsteht für Telefonie eine Zwei-Klassen-Gesellschaft, in der Softphones anders behandelt werden als Hardphones, da sie den jeweiligen „Daten-Subnetzen“ zugeordnet werden. Der pragmatische aber generische Ansatz ist hier, auf eine VLAN-Zuordnung zu verzichten und Telefone, PC‘s mit Softphone, und PC‘s ohne Softphone gleichermaßen dem jeweils für diesen Etagenbereich vorgesehenen IP Subnetz zuzuordnen.

Eine Reduzierung der VLAN Zersplitterung ist möglich (siehe Abbildung 4.7 und Abbildung 4.8), wenn für die Ethernet-Anschaltung der WLAN Access Points in jedem Verteiler ein separater Ethernet Switch vorgehalten wird (Kostenfaktor: hier wird Übersichtlichkeit mit Mehrinvestition bezahlt). Bei flächendeckender WLAN Ausstattung bietet sich diese Lösung geradezu an, da hier eine entsprechende Anzahl Switchports benötigt wird.

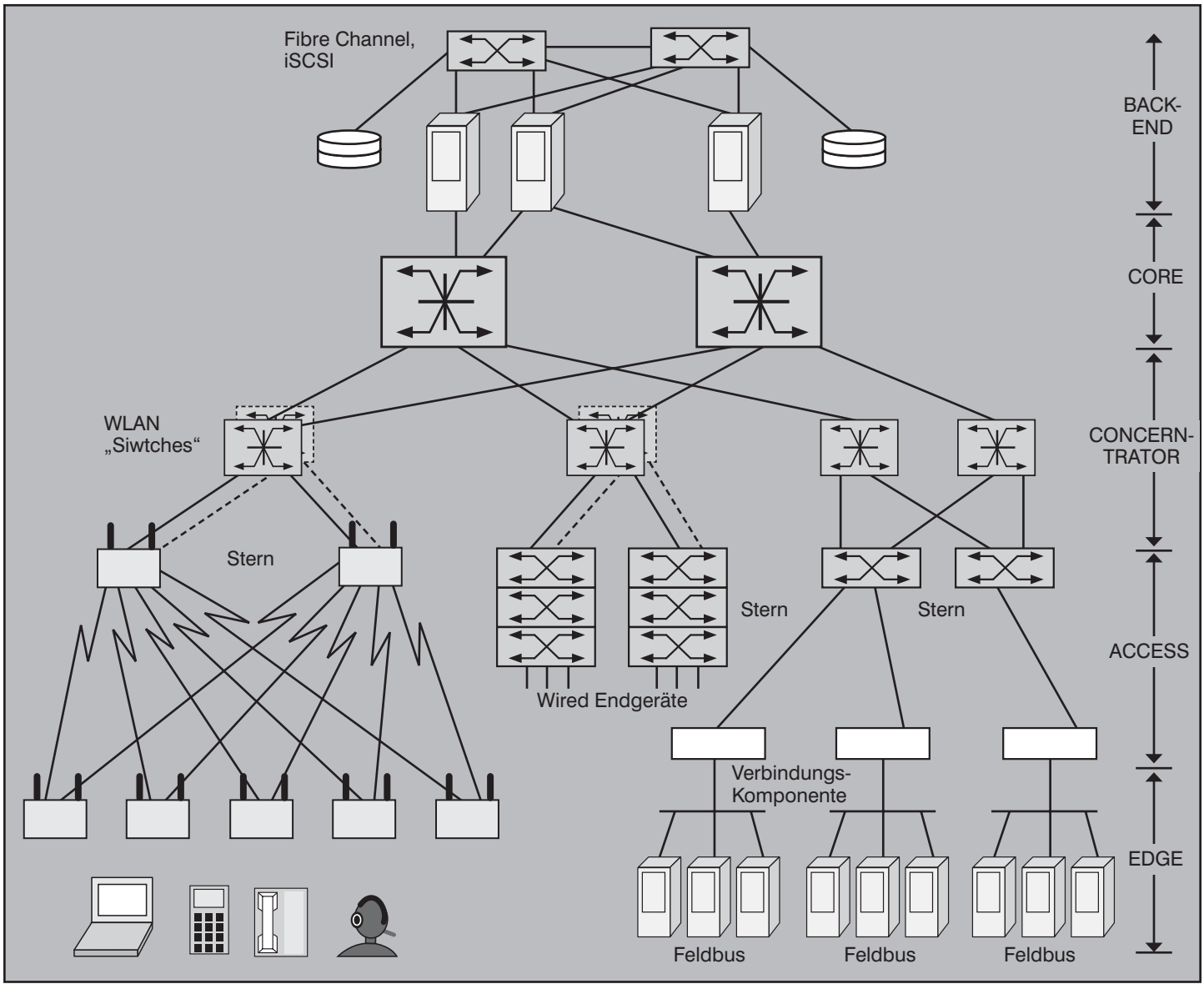



Abbildung 4.5: Beispiel 2, LND-S5 SIRENED Netzwerk mit sternförmig redundantem WLAN auf der Edge Ebene und Access Ebene

Allerdings empfehlen wir hier vorzugsweise den Einsatz identischer Switchtypen wie zur Anbindung der Wireline Endgeräte, da der Einsatz separater „WLAN Switches“ die Betriebskomplexität erhöht.

**Automatische VLAN-Zuordnung (AVA)**
Als Alternative für die Zuweisung von VLAN‘s durch feste Portzuordnung können einige IP Telefonie-Lösungen eine automatische VLAN-Zuordnung für Telefone vornehmen, sobald der Switch an der MAC-Adresse (Hersteller OUI!) erkennt, dass das angebundene Endgerät ein Telefon ist. Gleiches gilt für eine automatische VLAN-Zuordnung durch doppelte DHCP-Anfragen oder durch den RADIUS Server in Kombination mit Authentifizierung nach dem IEEE Standard 802.1X (Port Security). Beide Alternativen führen jedoch wiederum zu der schon zuvor genannten Zwei-Klassen-Gesellschaft für Hardphones und Softphones und stellen somit keine generische Lösung dar.

### 4.4 Integration von Quality of Service

Zusammen mit der Integration von Wireless Technologien in Enterprise Netzwerken stellt sich erneut die Frage nach Dienstgüte für kritische und wichtige Anwendungen. IEEE 802.11 / Wi-Fi hat hier noch keinen Standard verabschiedet, in der Praxis lizensieren eine Reihe von Herstellern für Sprache über WLAN (VoWLAN) das SpectraLink Priorisierungsverfahren (SVP SpectraLink Voice Priority). IEEE 802.16 / WiMAX hat in die 802.16d-2004 Spezifikation Priorisierungs-Funktionalität eingebracht, Produkte sind jedoch erstens aktuell noch nicht verfügbar, zweitens ist ihr Einsatz im Inhaus-Bereich aufgrund der vergleichsweise zu 802.11 hohen EMV-Abstrahlwerte fraglich.

Die grundsätzlichen Techniken für Klassifizierung, Priorisierung und Reservierung in Ethernet Netzwerken haben wir in den Netzwerk Insider Ausgaben Juni und August 2004 im Beitrag „Design von Voice-Ready Netzwerken“ beschrieben.

Da bei einer unbegrenzten Priorisierung und hoher Verkehrslast der priorisierten Anwendungen andere, unwichtigere Anwendungen erheblich benachteiligt werden können, nennen wir diese Priorisierung „PgH“ (Prinzip der guten Hoffnung). Sinnvoll ist, die Priorisierung stets mit einer Bandbreitenlimitierung zu kombinieren, die für

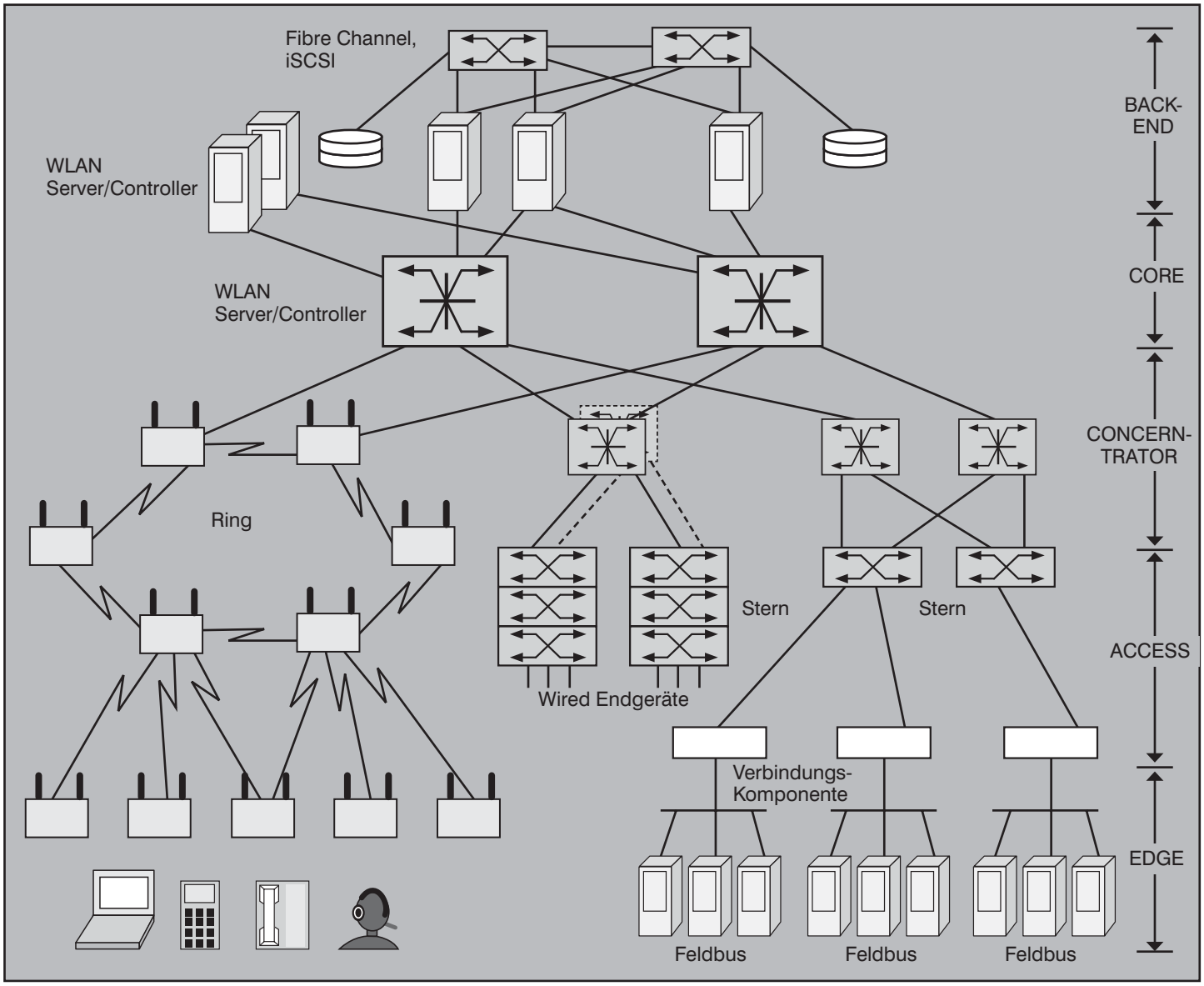



Abbildung 4.6: Beispiel 3, LND-RS5 SIRENED Netzwerk mit ringförmig redundantem WLAN auf der Edge Ebene und Access Ebene

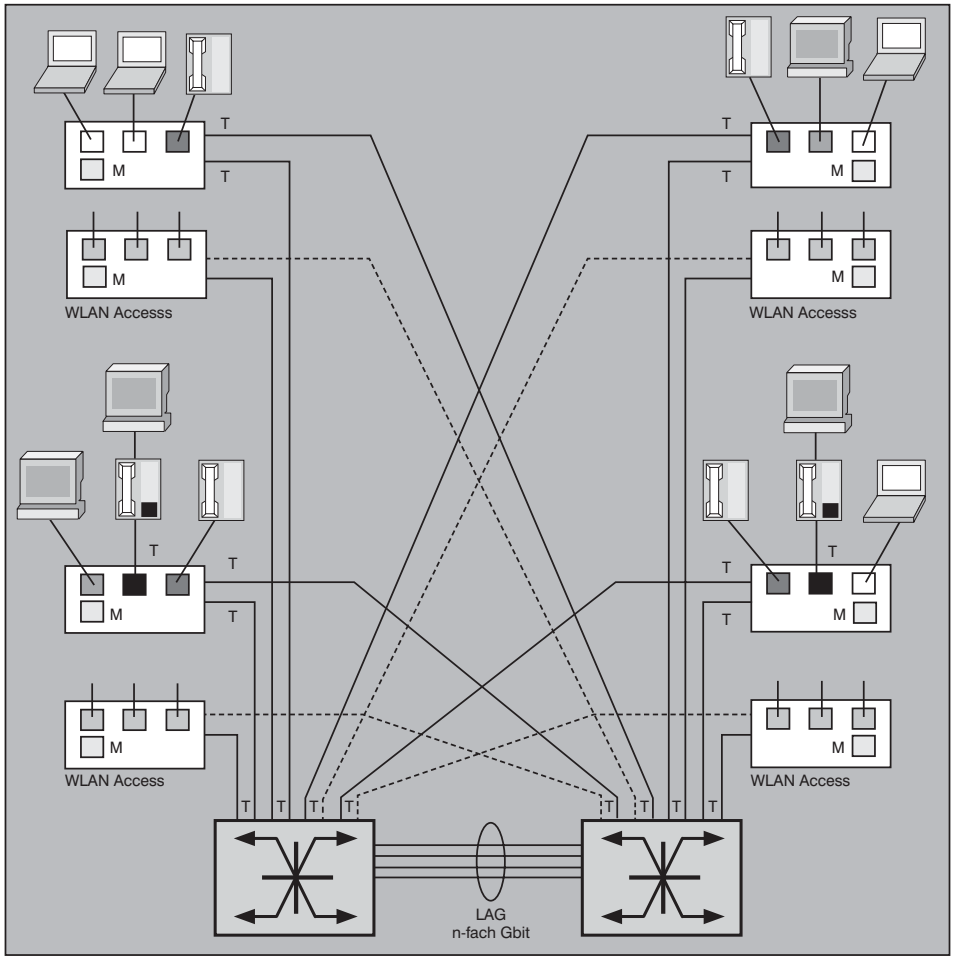



Abbildung 4.7: Benutzergruppen-Trennung durch VLAN's in Kombination mit separaten Switches

andere Anwendungen ausreichend Bandbreite übrig lässt wie in Abbildung 4.9 gezeigt. Diese Priorisierung nenne wir „PgM" (Prinzip des gesunden Misstrauens). Die Limitierung splittet die entsprechende Verbindung logisch in zwei Kanäle, einen Kanal mit limitierter Bandbreite für die priorisierte Anwendung, einen Kanal mit der restlichen Bandbreite für die anderen Anwendungen.

Soweit möglich sollte indirekte Priorisierung (Klassifizierung aufgrund TCP/UDP Portnummer oder anderer Paket-Informationen) erfolgen, um eine Markierung zu vermeiden. Dies ist jedoch mangels well-known Portnummern für Telefonie, Video und andere RTP-basierte Anwendungen nicht möglich. Soll eine Priorisierung solcher Anwendungen erreicht werden, die überdies von unterschiedlichen Endgeräte-Typen genutzt werden wie z.B. IP Telefonie, so ist die einzige generische, d.h. auf alle Handapparate, PDA's und Softphones anwendbare Lösung das Setzen von Priorisierungs-Bits im IP und MAC Header durch die Anwendung bzw. das Endgerät selbst. Aber auch diese Lösung hat einen Haken: In den beteiligten Switches muss explizite Priorisierung aktiviert werden, d.h. Lesen des Headers, Auswertung etwa gesetzter Priorisierungs-Bits und entsprechend hochpriorige oder niederpriorige Bearbeitung des Paketes. Dies öffnet jedoch kreativen Benutzern ein Scheunentor, die beliebige andere Anwendungen (mit Tools, die aus dem Internet herunterladbar sind) ebenfalls so konfigurieren, dass die Priorisierungs-Bits auf einen hohen Wert gesetzt werden. Hier gibt es keine technische Lösung, da selbst die ausgefeiltesten Policy- und Filter-Regeln abgesehen vom immensen Betriebsaufwand nicht alle Anwendungen einfangen werden. Übrig bleibt hier der Pragmatiker-Ansatz: Hinzunehmen, dass einige wenige kreative Benutzer die Regeln brechen. Erfahrungsgemäß ist die Anzahl dieser Benutzer in vielen Unternehmen niedrig.

Abschließend fassen wir die nach unserer Erfahrung vorhandenen Vor- und Nachteile beim Einsatz von Priorisierung zur Erreichung / Verbesserung von Quality of Service zusammen:

Vorteile:
- kurze Antwortzeiten für kritische Applikationen
- relativ gute Antwortzeiten für wichtige Applikationen
- Vermeidung von Investition in Überkapazität („nächste Ausbaustufe")
- Einsparung von Kosten im WAN durch Vermeidung von Hochrüstungen

Nachteile:
- höhere Kosten der aktiven Netzwerk-Komponenten („Full Function Switch")
- schlechte Antwortzeiten für unwichtige Applikationen
- hohe Betriebskomplexität
- bei Einsatz vieler QoS Regeln unübersichtliche aktive Konfiguration
- laufender Aufwand durch „Re-Engineering" und Anpassung
- fehlende Überwachbarkeit, keine Rückkopplung zwischen Policy und Monitoring

### 4.5 Integration von Sicherheitskonzepten

Nicht nur mit der Integration von Wireless Technologie und remote Access sind die Sicherheits-Anforderungen an Netzwerk-Komponenten, Netzwerk-Zugang und Netzwerk-Betrieb gestiegen. In vielen Umgebungen ist ein unkontrolliertes Login nicht-authentifizierter Benutzer (z.B. über eine „offene" Anschlussdose an der Wand oder über einen „schnell eben angeschlossenen Access Point" nicht mehr akzeptabel. Die zunehmende Anzahl von Angriffen, Viren und Würmern und die daraus resultierenden Schäden zwingen sowohl Anwender als auch Hersteller, an abgestimmten Konzepten vom Endsystem über NIC, Access Switch, Backbone, RZ-Zugang bis hin zum Server und der darauf laufenden Anwendung zu arbeiten. Hierzu zählt sicherlich der Einsatz von Verfahren und Schutzmechanismen wie

- Antiviren Software, Intrusion Detection / Protection Systeme (IDS / IPS)
- Wi-Fi WPA2 / IEEE 802.11i für Authentifizierung und Verschlüsselung in 802.11 Wireless LANs
- IEEE 802.1X (Port Security) für Authentifizierung von Benutzern und Endgeräten, auch im Wireline LAN
- IPsec in Verbindung mit VPN-Lösungen für remote Zugang
- SRTP (Secure RTP, RFC 3711) für Voice oder Video über IP
- Ende-zu-Ende Herstellerlösungen: NAC, NAP, TES
- TNC der TCG (Trusted Network Connect, Trusted Computing Group)

Über die Bedeutung und Funktionsweise von IEEE 802.1X (Port Security), SRTP und IPsec als Sicherheits-Standards für

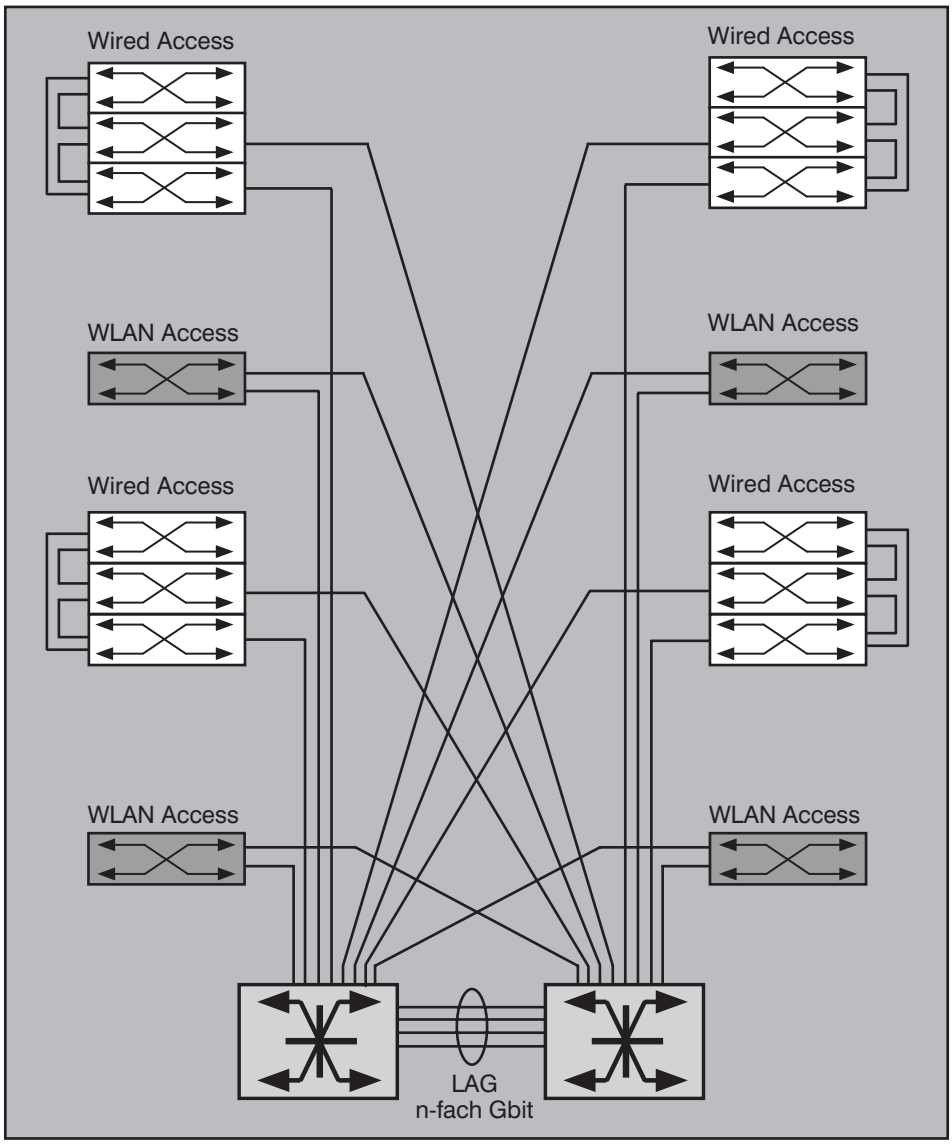



Abbildung 4.8: Trennung von WLAN und Wireline VLAN's in Kombination mit separaten Switches

Authentifizierung und Verschlüsselung wurden im Netzwerk Insider verschiedene Beiträge veröffentlicht, daher werden wir beides an dieser Stelle nicht weiter vertiefen, sondern auf weiterführende Entwicklungen eingehen. Derzeit ist ein Trend erkennbar, auf allen Ebenen und in allen Komponenten Software-Teile und Module gegen Angriffe zu installieren. Die Frage stellt sich jedoch, inwieweit es wirtschaftlich vernünftig ist, sowohl den Netzwerkübergang zwischen internem und externem Netz als auch Endsysteme als auch Server als auch alle Netzwerk-Komponenten mit solcher Software auszustatten. Falls der Betreiber sich hierzu entschließt, hat er in jedem Fall das Problem, dass Virenscanner im Endsystem nicht mit der IDS Software auf den LAN Switches und Routern und diese nicht mit dem eingesetzten Firewall Management zusammenspielen. Alle drei Schutzmechanismen haben keine Rückkopplung zu dynamischen Regeln bei IEEE 802.1X, so dass hier verschiedenste Betriebsbaustellen entstehen, die alle separat verwaltet werden müssen.

In einer solchen Betriebsumgebung wird es zunehmend wichtiger, dass verseuchte Endgeräte oder Endgeräte, die nicht auf dem neuesten Softwarestand der Sicherheits-Software laufen, auch und besonders dann, wenn sie zugelassenen internen Benutzern gehören, sofort vom Produktivnetz-Zugang abgeschottet werden, denn: Diese Geräte umgehen aufgrund ihres direkten LAN-Zugangs und des Status ihrer Benutzer jede Perimeter-Kontrolle völlig!

Interessanterweise versuchen aktuell sowohl Netzwerk-Hersteller wie Cisco als auch Hersteller von Endbenutzer-Software wie Microsoft, allgemeine Lösungsansätze zu finden: Cisco's NAC (Network Admission Control) und Microsoft's NAP (Network Admission Protection) bilden eine Kontroll-Barriere für jeden PC, der ans Netz will. Beide Hersteller haben API's verfügbar gemacht, auf deren Basis AV, Patch Management, Personal Firewall und andere Sicherheits-Software integriert werden könnten. Symantec, McAfee, Trend Micro und einige andere mehr sind Partner sowohl im Cisco- als auch im Microsoft-Entwicklungsprogramm.

NAC und NAP arbeiten beide nach folgendem Prinzip: Ein Agent auf dem Endsystem (Host-Agent) sucht dort nach entsprechender Software wie AV, Patches, Personal Firewall o.ä. Der Agent sendet einen Status-Bericht über die vorgefundene Umgebung an einen Policy Server, der den vorgefundenen Status mit den festgelegten Sicherheits-Richtlinien / Freigaben abgleicht und entsprechende weitere Aktionen veranlasst (erfolgreiches Login, Aufspielen von Sicherheits-Software, Zugangsverweigerung etc.). Sowohl NAC als auch NAP arbeiten mit Dritthersteller-Software zusammen, die das Vorhandensein und den Status / Patchlevel der eingesetzten AV-Produkte überprüft, bei Bedarf Sicherheits-Meldungen absetzt und im Netz nach entsprechenden Patches sucht, um sie auf das nicht sicherheitskonforme Endgerät aufzuspielen. PC's, die dem Standard entsprechen, können ein erfolgreiches Netzlogin durchführen, alle anderen werden in eine gesicherte Quarantäne-Zone verwiesen oder vollständig vom Zugang abgeblockt.

**NAC**

Ciscos NAC stützt sich wesentlich auf 802.1X ab und erfordert daher einen Supplicant auf jedem Gerät, das ans Netzwerk angeschaltet werden soll, einschließlich Drucker, Plotter und anderer Peripherie-Komponenten. Eine Ende-zu-Ende NAC-Lösung (siehe Abbildung 4.10) fängt mit einem Cisco Trust Agenten (CTA) auf dem Endsystem an, der für Windows 2000, NT und XP verfügbar ist (es gibt Pläne für Windows Server 2003, Red Hat Linux und Unix). Dies ist die Agenten-Software, die über das Cisco-API die zuvor genannten Status-Informationen sammelt und an den Cisco Secure Access Control Server (ACS), einen RADIUS Server, weitermeldet. Zwischen Client und Server steht ein Cisco-Switch, der als Policy Enforcement Komponente arbeitet und gemäß 802.1X mit dem Client EAPoL und mit dem ACS Server RADIUS redet. Der ACS Server koordiniert sich mit 3rd Party Policy Servern hinsichtlich Informationen über AV-Updates, Patches usw. und gibt dann eine

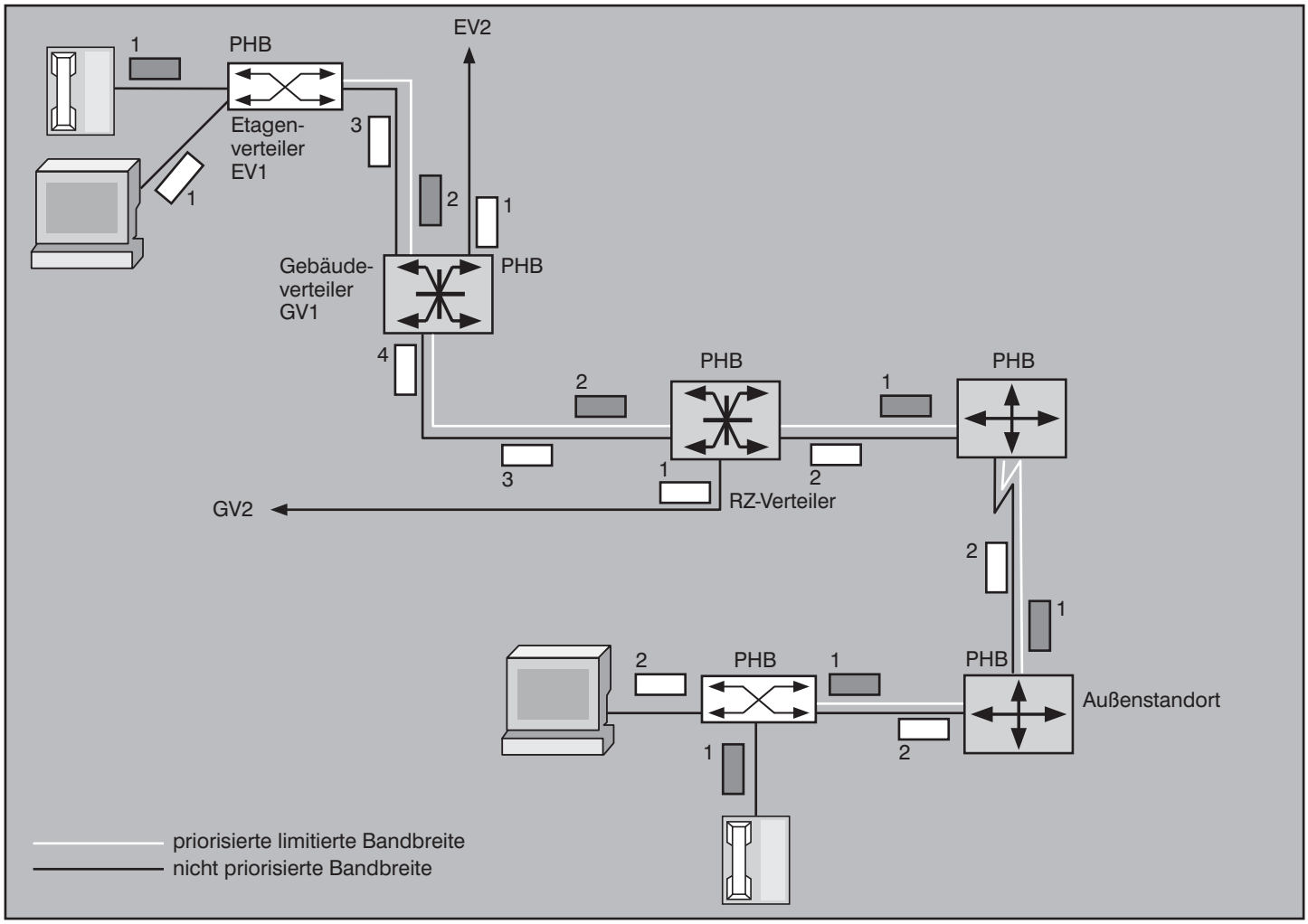



Abbildung 4.9: Qos-Implementierung mittels limitierter Priorisierung, „PgM“

Rückmeldung an den Switch, die die auszuführende Policy Aktion enthält, nämlich ein Login durchzuführen, eingeschränkt durchzuführen oder zu verweigern. Die Durchsetzung der Sicherheitsrichtlinien (PEP, Policy Enforcement Point) obliegt bei NAC immer einer Netzwerk-Komponente (Access-Switch, Backbone-Switch, Router).

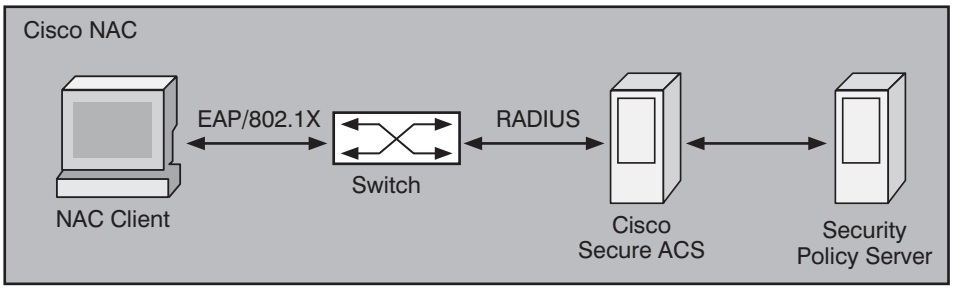



Abbildung 4.10: Cisco‘s Network Admission Control

**NAP**

Microsoft‘s NAP (siehe Abbildung 4.11) benötigt als zentrale Kontrollkomponente einen DHCP Server mit einer Windows Zusatz-Software, dem Quarantäne Enforcement Server (QES). Der Agent auf dem Endsystem (Client) heißt Quarantäne Agent (QA), ist - natürlich - in das Betriebssystem eingebettet und läuft unter Windows XP SP2. Das zuvor genannte entsprechende Microsoft API ermöglicht es 3rd Party Software, mit dem QA zu kommunizieren.

NAP funktioniert folgendermaßen: Sobald der PC vom DHCP Server eine gültige IP-Konfiguration haben will, fragt der DHCP Server den Quarantäne Agenten des PC‘s nach dem vorgefundenen Sicherheits-Status. Der DHCP Server gibt die Antwort des QA mittels RADIUS Paketen an den Microsoft Internet Authentication Service (IAS) weiter. Der IAS gleicht die Status Information mit verschiedenen Regeln ab, die in so genannten System Health Vektoren (SHV) gespeichert sind. SHV‘s arbeiten ihrerseits als Policy Server, die 3rd Party Agenten wie AV-Programme handhaben. Ja nach Antwort der SHV‘s weist der IAS Server den DHCP Server an, dem PC eine IP Adresse zu geben, die vollen Netzwerk-Zugang erlaubt oder den PC in eine Quarantäne-Zone (separates IP Subnetz / VLAN!) schickt. Die angekündigte neue Version des Microsoft Systems Management Server (SMS), die Softwareverteilung und Patch-Verteilung automatisiert, wird NAP-kompatibel sein.

**TES**

Trusted End System von Enterasys Networks hat eine Agenten-basierte Varian-

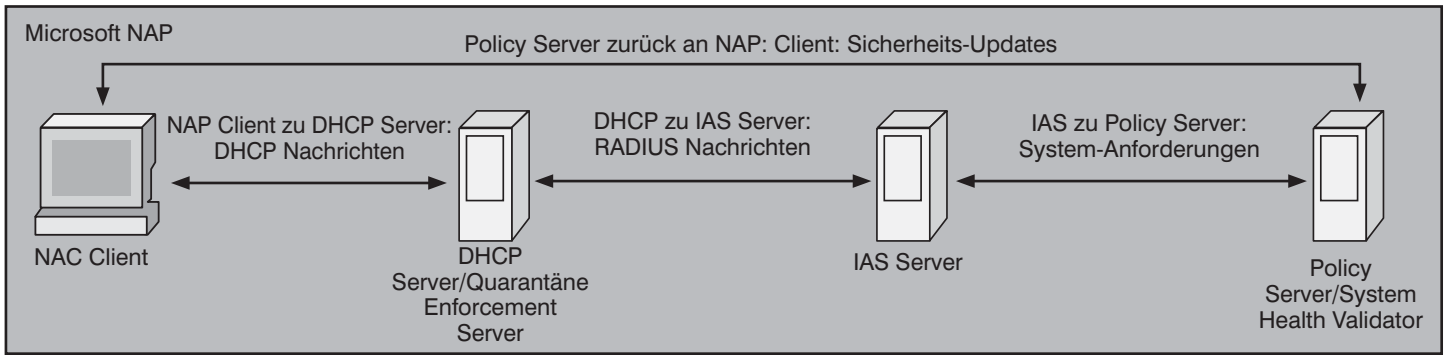



Abbildung 4.11: Microsoft's Network Admission Protection

te (AB Agent-Based) und eine Agenten-lose Variante (NB Network-Based). TES-AB arbeitet mit Software-Komponenten von Sygate und Zonelabs zusammen, nutzt IEEE 802.1X und funktioniert ähnlich wie NAC. Bei der agentenlosen Variante TES-NB wird der Benutzer, ggf. gezielt aufgrund einer vorhergehenden Klassifizierung mittels IDS-System und Policy-Regeln, zunächst in eine Scan-Umgebung geführt und dort z.B. durch einen Nessus Vulnerability Scan oder Bindview einer Sicherheitskontrolle unterworfen. Je nach Ergebnis der Kontrolle bzw. vorgefundenem Sicherheits-Status wird der Netzwerk-Zugriff gewährt, eingeschränkt oder abgelehnt. Enterasys, Sygate und Zonelabs sind Mitglieder der TCG, so dass eine gewisse Wahrscheinlichkeit für eine TNC-konformen Weiterentwicklung der TES Lösung besteht. Weitere Netzwerk-Hersteller, die für Policy Enforcement bei Endsystemen mit Sygate zusammenarbeiten, sind Alcatel, Extreme Networks, Foundry und HP.

**Entscheidung für eine Hersteller-Lösung?**

Bevor Sie sich jedoch als Anwender / Betreiber für eine der Hersteller-Lösungen entscheiden, bedenken Sie, dass beide Ansätze noch im Anfangsstadium stecken und proprietär sind. NAC läuft zur Zeit nur auf den Cisco Router Plattformen, für den Catalyst 6500 ist ein Upgrade für Sommer 2005 angekündigt. Microsoft will sich sogar bis 2007 Zeit lassen, denn dann soll die neue Windows-Serverplattform mit dem aktuellen Codenamen Longhorn verfügbar werden. Sowohl Cisco als auch Microsoft haben angekündigt, dass NAC und NAP (irgendwann, Anm. d. Autorin) zueinander kompatibel sein werden, so dass Policy Enforcement Entscheidungen beider Lösungen entsprechend von Microsoft und auch Cisco Komponenten gehandhabt werden können.

**TCG / TNC**

An diesem Punkt bietet sich die TCG (Trusted Computing Group) mit ihrer im Mai 2004 gegründeten TNC Initiative (Trusted Network Connect) als neutrale dritte Alternative an, der sich neben Software-Häusern wie Checkpoint, Sygate und Symantec auch schon Hardware-Hersteller wie Enterasys Networks, Extreme Networks, Foundry, Fujitsu, HP IBM, Intel oder Juniper Networks angeschlossen haben. Die TNC Gruppe will im Wesentlichen ein Gegengewicht gegen die Cisco und Microsoft Marktmacht bilden. (Im April hat allerdings auch Microsoft seinen Beitritt zur TNC-Gruppe angekündigt.) Eine solche Lösung ist insbesondere für non-Microsoft Endsysteme wie PDA's, WLAN Telefone, IP-Handapparate u.ä. interessant.

TNC ist eine Untergruppe der TCG und hat eine offene Architektur auf Basis von Industrie-Spezifikationen erarbeitet, die

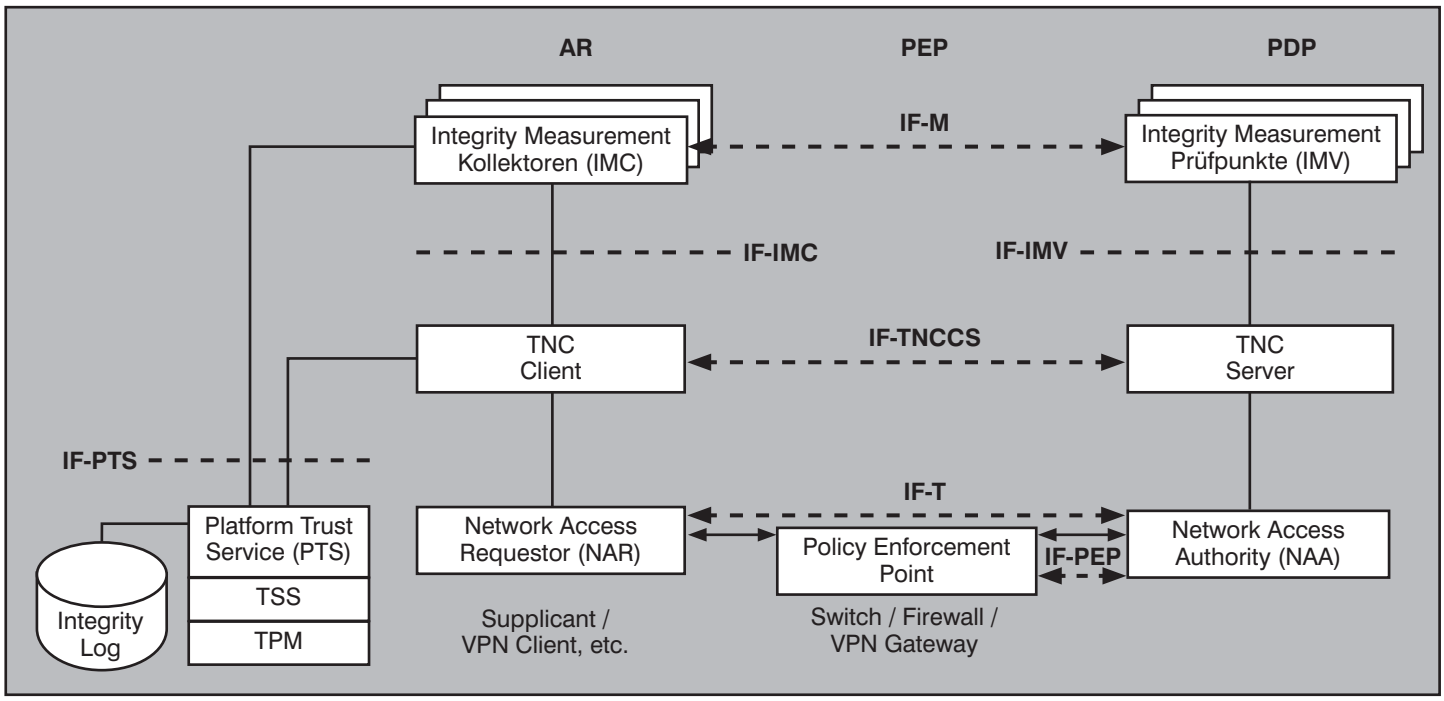



Abbildung 4.12: TNC-Architektur

Netzwerk-Administratoren in die Lage versetzt, den Sichterheits-Status von Endgeräten zu prüfen und die Einhaltung von Sicherheits-Vorgaben / Richtlinien für den Netzzugang dieser Endgeräte zu erzwingen (Policy Enforcement). Hierzu gehört:

- Bestimmung des Sicherheits-Levels und der Regelkonformität von Benutzern und Geräten, die einen Netzzugang haben wollen
- Provisionierung eines angemessenen Netzzugangs auf der Basis der vorgefundenen Sicherheits-Konformität; hierzu gehört vollfunktionaler Zugang, teilfunktionaler Zugang, Zugang zu einem abgeschlossenen (gesicherten) Bereich und Zugangsverweigerung

Die TNC Architektur inklusive des optionalen TPM ist in Abbildung 4.12 dargestellt. Der Client ist der Access Requestor (AR), der Server der Policy Decision Point (PDP) und damit letztendlich die Netzzugangs-Autorität für den Client (NAA Network Access Authority). Die gepunkteten Linien sind Standard-Schnittstellen (Protokolle und API's). Die Komponenten des Client bzw. Access Requestor (AR) sind Integrity Measurement Kollektoren, der TNC Client und der Network Access Requestor (802.1X Supplicant, VPN Client o.ä.). IF-PTS (Platform Trust Service) ist die Schnittstelle zur TPM Hardware. Die IMC Schnittstelle (IF-IMC) erlaubt Herstellern von Sicherheits-Software, Plug-In Module mit ihrer Endsystem Software (AV, Personal Firewall etc.) zu entwickeln. Der Policy Enforcement Point (PEP) zwischen AR und PDP überwacht den Zugang zum geschützten Netzwerk. Vielfach wird der Access Switch als PEP betrachtet (bei Microsoft NAP ist dies der DHCP Server). Er leitet Nachrichten (von IF-M und IF-TNCCS) mit Hilfe eines Transport Protokolls (IF-T) wie EAP-TTLS oder PEAP weiter, wodurch der Ablauf der Authentifizierungs-Sequenz zwischen TNC-Client und TNC-Server ermöglicht wird. Der Server bzw. Policy Decision Point (PDP) trifft die Entscheidungen über den Netzzugang jedes Client auf der Basis des für das Client-Systems vorgefundenen Sicherheits-Status. Er nutzt hierfür einerseits die IMV-Schnittstelle (IF-IMV) zur Kommunikation mit Policy-Auswertungs Plug-In's, andererseits nutzt er die PEP-Schnittstelle (IF-PEP), um den Policy Enforcement Point zu informieren, in welcher Form der Netzzugang für einen bestimmten Client (AR) zuzulassen ist.

Die TNC-Architektur und zwei der Einzelspezifikationen (IF-IMC, IF-IMV) wurden am 3. Mai 2005 veröffentlicht, die noch fehlenden Spezifikationen sollen noch in 2005 veröffentlicht werden. Die ersten Entwicklungen werden schon vorab implementiert.

Die TNC Architektur benutzt EAP und TLS, was wiederum den Einsatz von IEEE 802.1X und IPsec oder SSL VPN's ermöglicht. Zusätzlich wird mit Trusted Platform Module (TPM) eine „Trusted Hardware" spezifiziert. Dies ist ein Chip auf dem PC Board, der als „Root-of-Trust" für weitergehende Systemaktivitäten dient. Der TPM-Chip kann z.B. benutzt werden, um während eines so genannten TNC Handshake zu prüfen, welche Software auf einem PC läuft. Abbildung 4.13 zeigt, wie eine Authentifizierung und Autorisierung mit TNC abläuft, auch hier findet die Authentifizierung nach dem Client-Server Prinzip statt:

1. Der TNC-Server auf dem Policy Decision Point (PDP) initiiert eine Sicherheits-Prüfung.
2. Der TNC-Client (Agent) sammelt Sicherheits-Informationen von den Integrity Measurement Collectoren (IMC's).
3. Der TNC-Client (Agent) gibt über einen zwischengeschalteten Policy Enforcement Point (PEP) die gesammelten Informationen an den TNC Server weiter

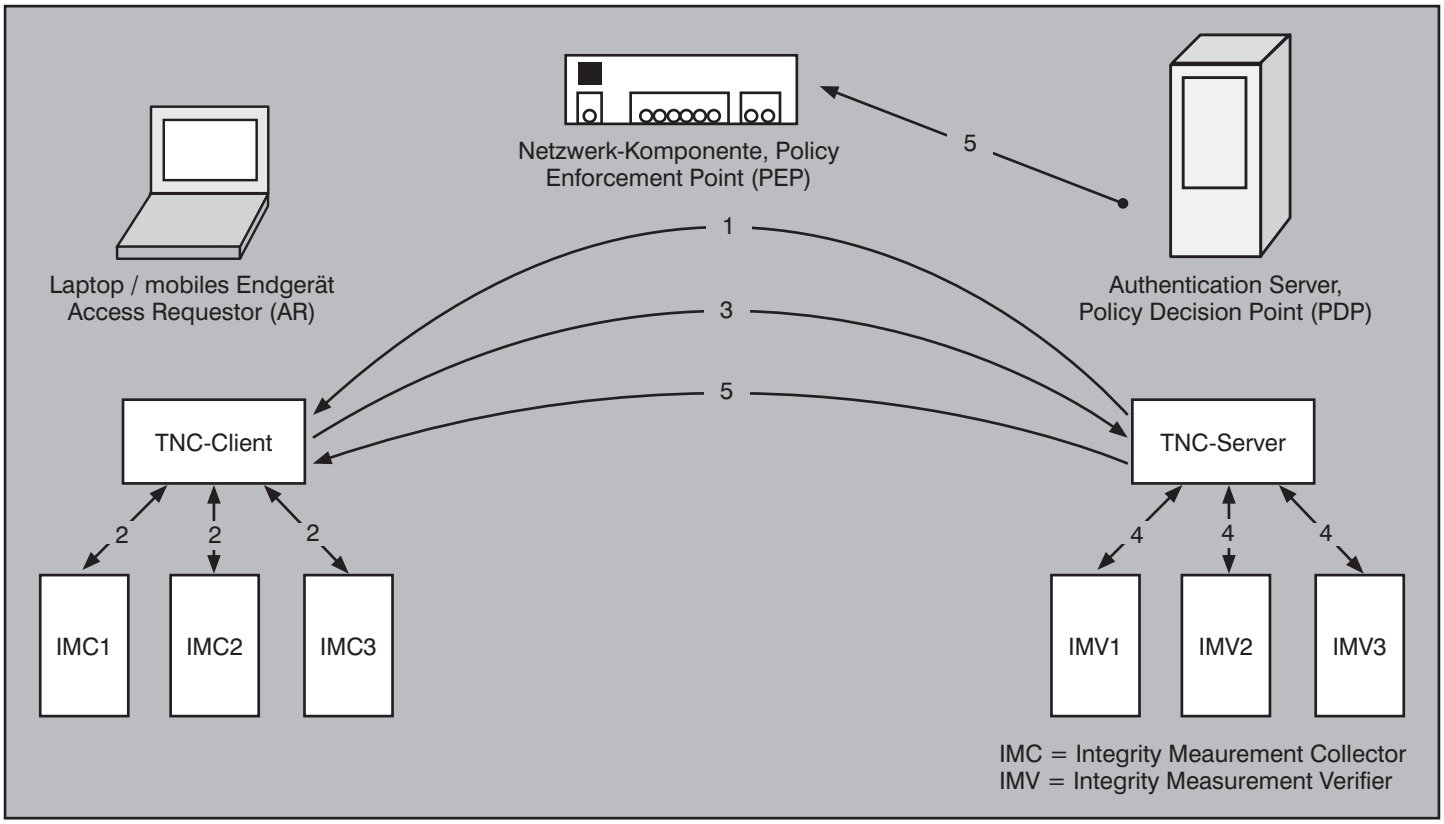



Abbildung 4.13: Zugangskontrolle mit TNC Agenten und Servern

4. Der TNC-Server trifft die letztliche Zugangs-Entscheidung, sendet diese zum PEP und über diesen an den AR

Falls die Sicherheitsüberprüfung erfolgreich verläuft, gewährt der PEP dem AR Zugang zu dem geschützten Netzwerk (im Regelfall vollfunktional), falls die Sicherheitsüberprüfung erfolglos verläuft, platziert der PEP den AR in einer Quarantäne Zone, in der eine Anpassung des Client an die Sicherheits-Richtlinien (z.B. Behebung der Sicherheits-Löcher, Aufspielen der erforderlichen Patches) vorgenommen werden kann oder in der der Client vom weiteren Netzwerk-Zugang abgeschottet wird.

**Fazit zum Sicherheitstrend**

Die TNC Initiative zeichnet sich aktuell als einziger Multivendor-Ansatz ab. Mit der Verfügbarkeit einer kompletten Spezifikation ist bis Ende 2005 zu rechnen, die Verfügbarkeit von TNC konformen Produkten wird entsprechend bis 2006 auf sich warten lassen. Wie weit sich Microsoft der Initiative anschließt oder letztlich doch eine herstellereigene Lösung auf den Markt bringt, bleibt abzuwarten. Betreiber, die sich bis dahin für eine spezielle Hersteller-Lösung entscheiden, müssen davon ausgehen, dass diese Lösung in sich geschlossen und inkompatibel zu Multivendor-Produkten bleiben wird. Die dauerhafte Marktdominanz einer der genannten Lösungen ist derzeit nicht absehbar. Die besten Chancen hierfür räumen wir der TNC-Lösung ein, insbesondere auch weil sie auf den aktuell etablierten Sicherheits-Standards aufsetzt.

### 4.6 Integration von Policies und Benutzer-Rollen

Der Einsatz von Regeln und Benutzer-Rollen zur feingranularen Steuerung des Netzwerk-Betriebs ist nicht neu, aber im Zusammenhang mit Wireless Sicherheit und einer Weiterentwicklung der Sicherheits- und Quality of Service Diskussionen in Richtung Service Level Agreement erneut in die Diskussion eingetreten: Die Zielsetzung von Policies sind

- Erkennen unerwünschter Verkehrslasten oder Angriffe
- Unterdrückung unerwünschter Verkehrslasten
- Festlegung „erlaubter“ Nutzung von Diensten / Anwendungen (Nutzungs-Profile)
- Explizite Provisionierung von Leistung und Dienstgüte

Der allgemeine Policy-Ansatz führt eine Klassifizierung von Paketen oder Authentifizierungs-Wünschen und –Sequenzen durch, wobei das Ergebnis der Klassifizierung nachfolgende Aktionen auf der Basis hinterlegter Regeln festlegt. Insofern können Policies auch als Weiterentwicklung von ACL‘s (Access Control Listen) mit verbesserter Bedienoberfläche betrachtet werden. Klassifizierungsfaktoren und Aktions-Regeln können fest oder variabel / dynamisch (z.B. nach Zeit und Ort) gültig sein (siehe Abbildung 4.14). Neu ist hierbei die dynamische Anpassung von Policies, quasi als Rückkopplung aufgrund speziell aufgetretener Verkehrsmuster, die als unerwünschte Verkehrsmuster klassifiziert worden sind.

**Klassifizierung**

Die Klassifizierung von Paketen kann auf

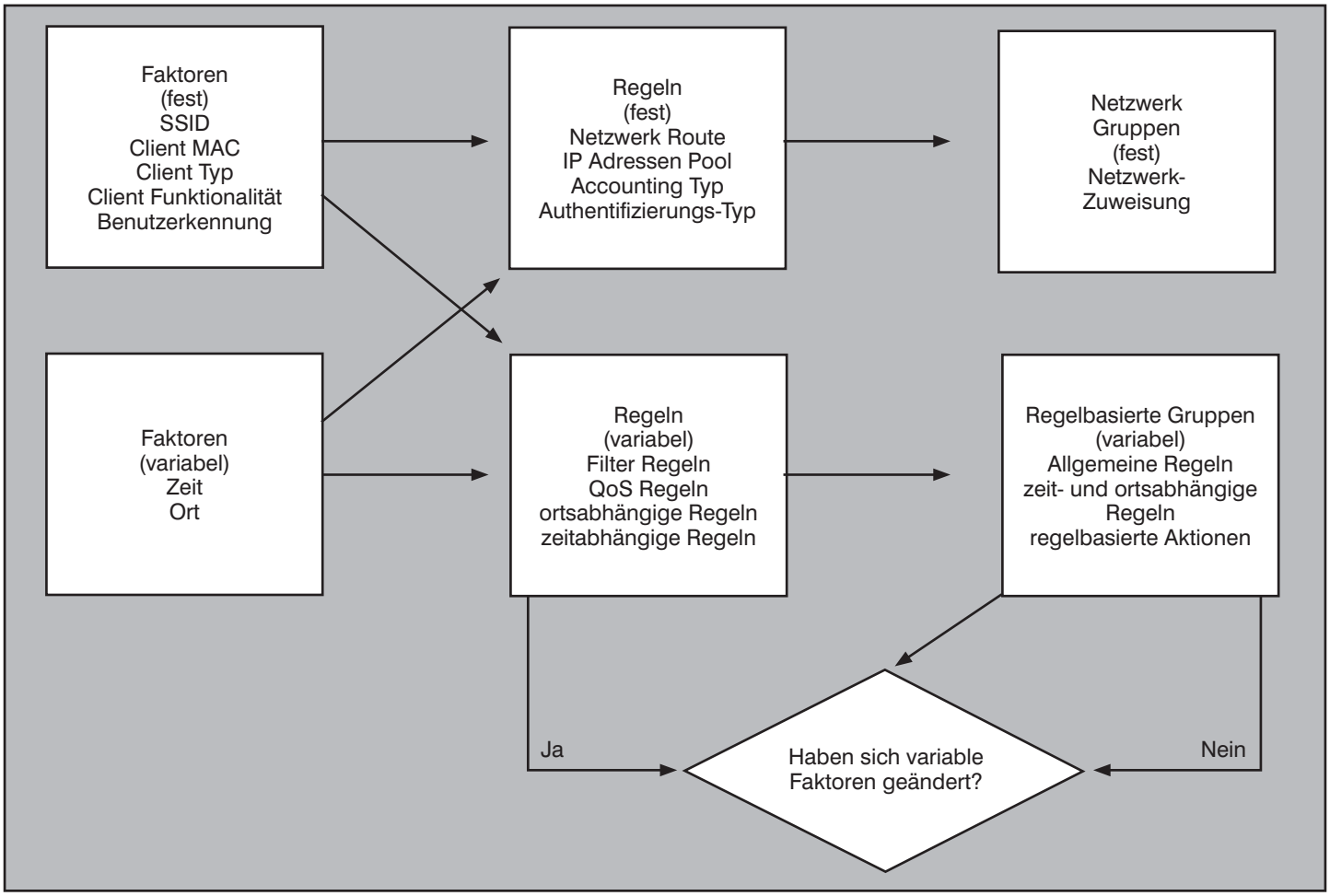



Abbildung 4.14: Flussdiagramm für eine regelbasierte Paketbearbeitung

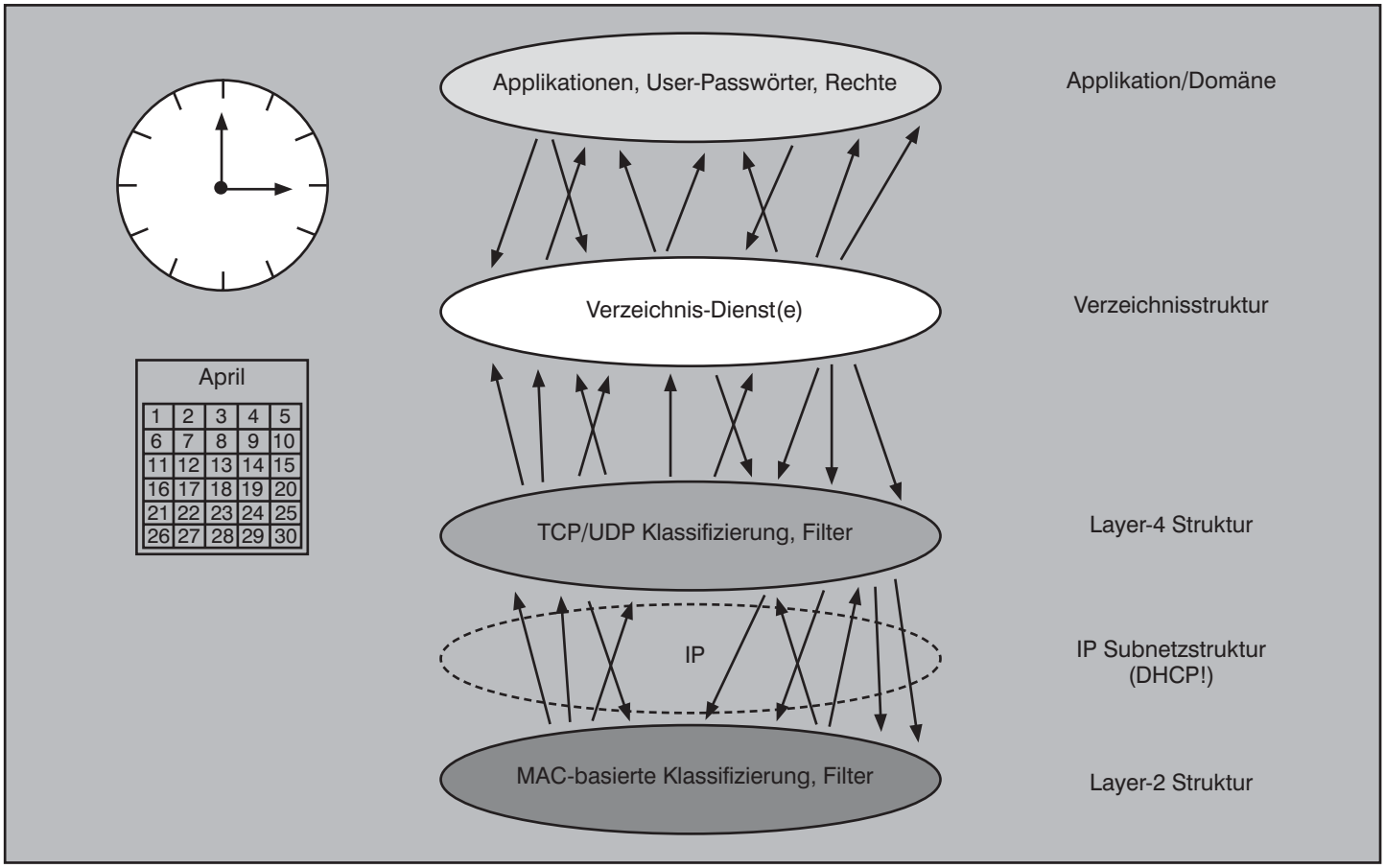



Abbildung 4.15: Klassifizierungs-Schichten und deren wechselseitige Zugriffe aufeinander

der Link Ebene, IP Ebene, Transport Ebene (TCP/UDP) oder Applikations-Ebene erfolgen. Auf der Link-Ebene stehen MAC-Adresse, MAC Prefix (OUI) und Ethernet Typfeld / LSAP zur Verfügung. Auf der IP-Ebene steht die IP Adresse zur Verfügung, die jedoch inzwischen zum Glück nicht mehr im Fokus von Klassifizierungen steht, da selbst hartnäckige Verfechter separater VLAN's auf Basis von IP-Adressen immer mehr erkennen, dass diese keine generische Lösung darstellen. Auf Transport-Ebene stehen die TCP und UDP Portnummern sowie die Protokoll-Nummer zur Verfügung. Dies lässt sich für alle Anwendungen heranziehen, die mit well-known Portnummern arbeiten, nicht jedoch für RTP-Anwendungen wie Telefonie oder Video, da diese dynamische Portnummern verwenden, die sie beim Verbindungsaufbau aushandeln. Auf der Applikations-Ebene lassen sich URL's, Passwörter, konfigurierte Rechte oder auch die genutzte Verzeichnisstruktur zur Klassifizierung verwenden. Natürlich lassen sich Klassifizierungen auch um Datum und Uhrzeit-Angaben des Zugriffs erweitern. Problematisch für eine geordnete Klassifizierung sind jedoch die verzahnten Referenzen verschiedener Anwendungen auf verschiedene Protokoll-Ebenen wie Link-Ebene, Transport-Ebene und Applikations-Ebene, die sich vielfach wechselseitig überschneiden und in keine hierarchische Ordnung passen wollen: Verschiedene MAC-Adressen nutzen dieselbe TCP Portnummer und umgekehrt, verschiedene Portnummern nutzen gleiche Verzeichnisstrukturen und umgekehrt, verschiedene Verzeichnisstrukturen nutzen gleiche Applikationen und umgekehrt (siehe hierzu Abbildung 4.15).

**Aktionen**
Typische Aktionen sind Erlauben (Forward), bedingt erlauben (Forward + Condition, z.B. zusammen mit Bandbreitenlimitierung erlauben), VLAN-Zuordnung d.h. IP Subnetz-Zuordnung vornehmen, Nachricht versenden (z.B. an Netzwerk-Administrator, Policy Server), isolieren (einer Quarantäne-Zone oder einem „Gast-VLAN" zuweisen), verwerfen (Discard) oder jede sinnvolle Kombination der zuvor genannten Aktionen.

**Rollen**
Werden Klassifikationen und Aktionen unter Anwendung mehrerer Regeln gruppiert, können so genannte „Dienste" entstehen, die Kombination mehrerer Dienste wird in einigen Konzepten als „Rolle" bezeichnet. Allgemein lassen sich Dienste und Rollen mit Skripten vergleichen. Einem einzelnen Benutzer lassen sich dann eine oder mehrere Rollen zuordnen. Abbildung 4.16 zeigt ein übersichtliches Beispiel für den Einsatz von Rollen: Der Vertrieb nutzt SAP mit hoher Priorität, die Entwicklung Citrix mit hoher Priorität und (normalen) Internet-Zugang, die Verwaltung Internet-Zugang. Alle drei Benutzergruppen haben keine Berechtigung, SNMP zu nutzen. Die Dienste „SAP mit hoher Priorität", „kein SNMP", „Citrix mit hoher Priorität" und „Internet Zugang" wurden mit nur 12 Regeln erstellt. Das gezeigte Beispiel ist klein und fein und übersichtlich. Wir geben daher ein Gegenbeispiel und unterstellen hierfür:

- 15 Abteilungen
- je Abteilung 10 Dienste
- je Dienst 3 Regeln

Daraus ergibt sich
15 x 10 x 3 = 450 Policies
kombiniert mit
- Zeitsteuerung und Vertretungsregelung (Faktor 2)

ergibt dies
15 x 10 x 3 x 2 = 900 Policies

Das Beispiel macht deutlich, dass inner-

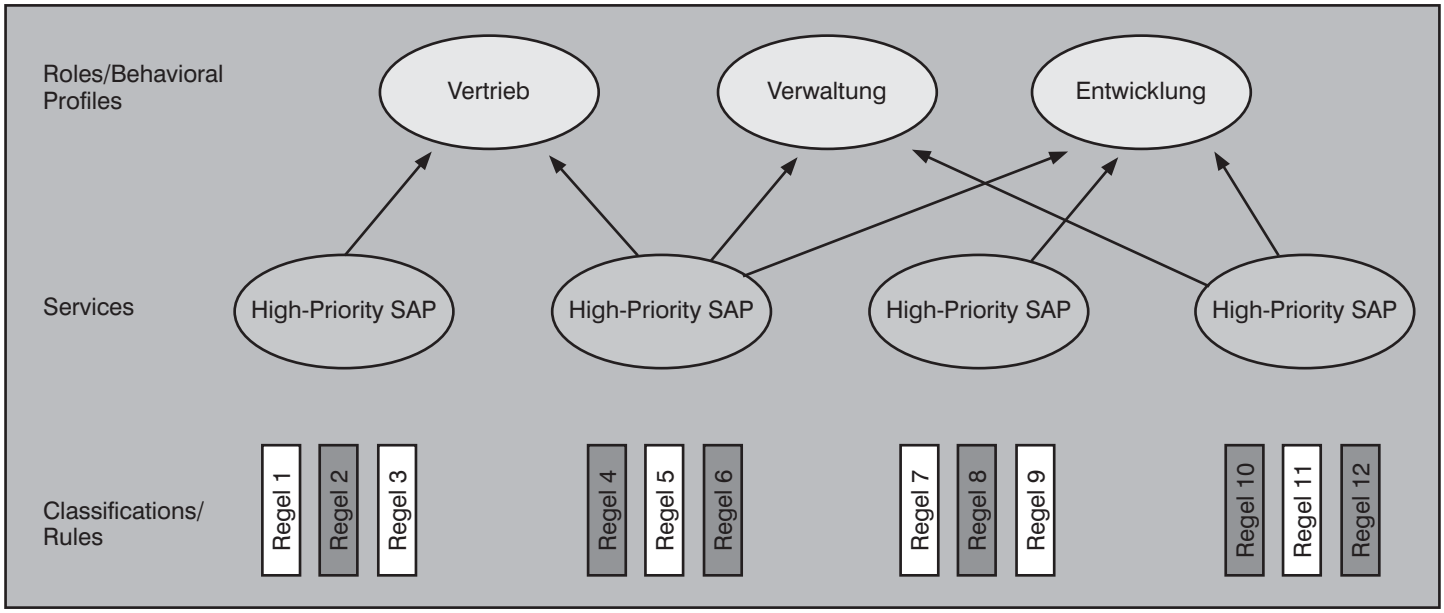



Abbildung 4.16: Beispiele für Rollen /Skripte

halb weniger Betriebsjahre „historisch gewachsene“ Policies schnell sehr unübersichtlich werden können, insbesondere wenn sie unter dem Zeitdruck des „normalen Alltagsgeschäfts“ schlecht oder nicht dokumentiert sind. Dies erinnert an die Praxis historisch gewachsener ACL-Listen: In einem Fall hatten wir einen Kunden, der bei Übernahme der Router-ACL seines Vorgängers 2000 sehr rudimentär dokumentierte ACL-Einträge vorfand (!). Die Auflösung dieses Puzzels dürfen wir an dieser Stelle nicht allgemein bekannt geben, schreiben Sie uns bei Interesse hierzu eine Mail (petra.borowka@ubn.de).

**Offene Punkte bei Policies**

Abgesehen von Leistungs-Aspekten (Welche Ihrer Netzwerk-Komponenten leistet die Inspektion aller Flows mit wire speed?) führt die Festlegung der erlaubten Nutzung zu einer statischen Umgebung. Die Einrichtung von Quarantäne-Zonen muss mandantenfähig sein, da es nicht passieren sollte, dass verschiedene, der Quarantäne zwangszugeordnete Benutzer sich gegenseitig ausspionieren oder angreifen. Last but not least sind in größeren Umgebungen die Auswirkungen auf den Help Desk zu bedenken, der sich mit allen Anrufen von Benutzern befassen muss, welche aufgrund vergessener Passwörter, vergessener Updates oder ähnlicher Vergesslichkeiten kurzerhand in Quarantäne gepackt wurden.

Unsere Empfehlung an dieser Stelle:

- Beschränkung auf möglichst wenige Policies
- Beschränkung auf Negativ-Policies zur Unterdrückung unerwünschter Verkehrslasten
- Wichtigkeit dynamischer Rückkopplung zwischen Klassifizierung und Policies beachten

**IEEE 802.1X als Basis für Policy Enforcement**

Mit steigendem Risiko-Bewusstsein hinsichtlich des ungesicherten Netzwerkzugangs von Endsystemen wird 802.1X von mehreren Initiativen als Basis für weitergehende Anwendungen mit Policy Enforcement genutzt, die den Netzzugang für einzelne Benutzer oder einzelne Endgeräte vollfunktional erlauben, eingeschränkt erlauben oder verweigern. Typische Prüfpunkte sind hierbei AV-Signaturen, Patch-Level, Virenfreiheit oder ähnliches. Geräte, die nicht den geforderten Sicherheits-Richtlinien / Standards entsprechen, werden vom Netzzugang ausgeschlos-

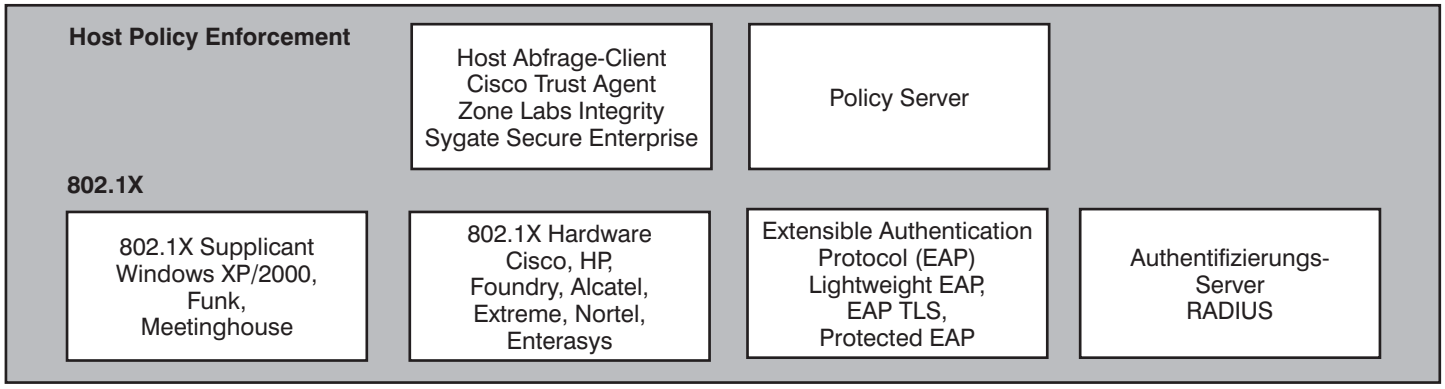



Abbildung 4.17: IEEE 802.1X als Basis für Policy Enforcement

sen. Voraussetzungen für eine 802.1X Implementierung sind jedoch

- Angemessene Unterteilung des Netzwerks in VLAN's
- Einheitliche Verzeichnis- und Namenskonventionen, konsistentes Management / Schema für Benutzerkennungen
- Portbezogene Konfiguration der genutzten Authentifizierung (802.1X, webbasiert, MAC-basiert)
- Risiko-Abschätzung hinsichtlich entstehender Sicherheits-Löcher bei Ausnahmeregeln (z.B. fest authentifizierte Ports für den Anschluss von Monitoren oder Probes)

Die Übersicht in Abbildung 4.17 zeigt das Zusammenspiel von Policy Enforcement Produkten und 802.1X Komponenten.

**Co-SIRENE Design für SLA-Netze**

Abschließend zeigen wir ein Einsatz-Beispiel für LND (Layered Netzwerk Design) mit der Co-SIRENED Erweiterung für SLA-Netzwerke. Für jede EACCB Ebene (Edge, Access, Concentrator, Core, Backend) wird entsprechend des Bedarfs selektiv Sicherheits-Funktionalität implementiert:

- Edge: Zwingend Sicherheits-Funktionalität mit Authentifizierung und Verschlüsselung für WLAN, für IP Telefonie bei Bedarf mit Authentifizierung sowie bei weitergehendem Bedarf mit Verschlüsselung
- Access: Authentifizierung in allen Bereichen mit Gast-Zugang, bei Bedarf ACL/ Policy Einsatz
- Concentrator, Core: bei Bedarf ACL/Policy Einsatz
- Backend: Autorisierung zum Core

Für jede Ebene wird entsprechend des Bedarfs sehr selektiv QoS-Funktionalität und Sicherheits-Funktionalität implementiert:

- Edge: bei Bedarf direkte Priorisierung mittels Markierung der IP Bits und MAC Bits durch die Endgeräte
- Access, Concentrator, Core: Klassifizierung, Priorisierung, Bandbreitenkontrolle
- Backend: Bedarf direkte Priorisierung mittels Markierung der IP Bits und MAC Bits durch die Server

Im gezeigten Beispiel (s. Abb. 4.18) wird der Edge-Bereich, soweit er Wireless LAN ist, sowohl mit Sicherheits-Funktionalität als auch mit QoS-Funktionalität implementiert (QoS-Funktionalität aufgrund der Shared LAN Eigenschaften), der nachgelagerte Access Bereich ist mit Sicherheits-Funktionalität ausgestattet, um etwaige Lücken im Edge-Bereich zu schließen, nicht jedoch mit QoS-Funktionalität, da es sich um voll geswitchte (dedizierte) Verbindungen handelt. Im verkabelten Kernnetz und Backend wurde auf weitergehende SLA-Steuerung ganz verzichtet.

**5. Fazit**

Nachfolgend fassen wir konzeptuelle und strategische Empfehlungen sowie Do's und Dont's zusammen.

**Konzeptuelle Empfehlungen:**

- Verwenden Sie das KISS Prinzip: Keep It Simple and Stupid
- Setzen Sie Standards ein - manchmal gilt es auch, auf Standards zu WARTEN!
- Generische Lösungen für Mobilität, Telefonie und Sicherheit sind vorzuziehen, vermeiden Sie Speziallösungen
- Setzen Sie ein solides Strukturkonzept ein, das flexibel erweiterbar ist: LND-

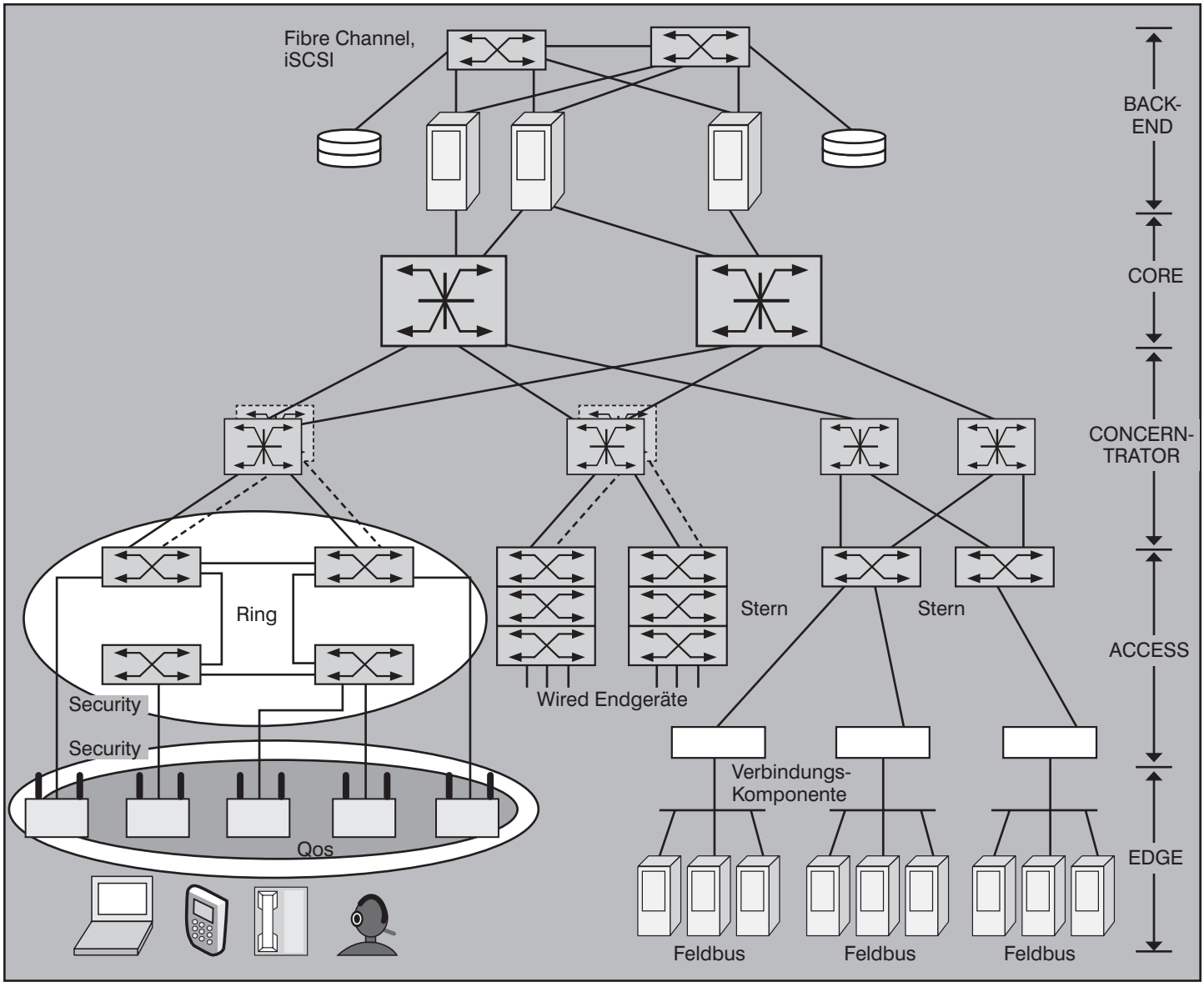



Abbildung 4.18: Beispiel-Netzwerk für ein LND-RS-5 Co-SIRENE Design

SR, CoSIRENE, Anwendung der LND-Kriterien
- „If your Network is solid like a rock, the rest doesn't matter" (Quelle: Cisco Systems)

**Strategische Empfehlungen:**
- Verlassen Sie sich auf den Gegenpol zu Mode-Marketing - das 4er Kleeblatt: Bedarfsanalyse, Gewichtung, Evaluierung, Entscheidung
- Berücksichtigen Sie strategische Aspekte wie Zukunftssicherheit, Marktposition, Innovation
- Legen Sie einen Total Cost Ansatz zugrunde: Was bringt langfristige Vorteile?

**Do's and Dont's**
- Verkabelung: Bei Redesigns Monomode, hochwertiges Kupfer (mind. Kat. 6)
- Vermeiden: Server-Engpässe, auch für TK-Server!
- Netzwerk: 10 Gbit Ethernet-Einatz mindestens als Option
- Vermeiden: Überbuchte Switcharchitekturen, überbuchte Module im Backbone
- PoE einplanen: Hersteller, Produkte, Klimatisierung, USV, Verkabelung (1:1 !)
- Integration von Wireline und Wireless berücksichtigen: Hersteller, Management
- Vorsicht bei Lastverteilung
- Zielsetzung Benutzergruppen: Minimierung von VLAN's
- Zielsetzung QoS: Minimierung von QoS-Regeln, Priorisierung zusammen mit Bandbreitenlimitierung
- Zielsetzung Policies: Übersichtliche Policies, eher negativ (drop) als positiv (wanted usage)
- Klärung: Policies im Endgerät oder Policies in den Netzkomponenten
- Sicherheitszonen: Angemessene Lösung, WLAN/Voice berücksichtigen, aber Vermeidung der „Voice-Hysterie"
- Überwachung, Management, Administration mit hohem Stellenwert versehen
- Permanent-Überwachung: Messpunkte definieren, Ende-Ende Monitoring implementieren
- Vermeiden: Wahlloser Technologie-Mix von 802.11, Bluetooth, WiMAX, WEP, WPA, MAC-Authentifizierung, 802.11X, HSRP, VRRP, GLBP
- Vermeiden: Subnetz-Zerstückelung
- Vermeiden bei Geländekonzepten: „Distribution Layer" in kleinen Gebäuden
- Vermeiden: Gebäude-übergreifende VLAN's

### 6. Abkürzungen

| | |
|---|---|
| ACL | Access Control Liste |
| ACS | Access Control Server |
| API | Application Programming Interface |
| AV | Antivirus |
| AVA | Automatic VLAN Assignment |
| BGP | Border Gateway Protocol |
| CoSIRENED | Controlled Structured Integrated REsilient NEtwork Design |
| CTA | Cisco Trust Agent |
| DHCP | Dynamic Host Configuration Protocol |
| EAP | Extensible Authentication Protocol |
| EAPoL | EAP over LAN |
| GLBP | Gateway Load Balancing Protocol |
| GSM | Global System for Mobile Communication |
| HSRP | Hot Standby Router Protocol |
| IAS | Internet Authentication Service |
| IDS | Intrusion Detection System |
| IEEE | Institute of Electrical and Electronics Engineers |
| IMC | Integrity Measurement Collector |
| IMV | Integrity Measurement Vector |
| IPS | Intrusion Protection System |
| LAG | Link Aggregation Group |
| LND | Layered Network Design |
| LSAP | Logical Link Service Access Point |
| MAC | Media Access Control |
| MHz | Megahertz |
| MPLS | Multiprotocol Label Switch |
| MSTP | Multiple Spanning Tree Algorithm or Protocol |
| NAA | Network Access Authority |
| NAC | Network Admission Control |
| NAP | Network Admission Protection |
| NAR | Network Access Requestor |
| OSPF | Open Shortest Path First |
| OUI | Organizational Unique Identifier (erste 3 Byte einer MAC-Adresse) |
| PDA | Personal Digital Assistant |
| PDP | Policy Decision Point |
| PEP | Policy Enforcement Point |
| PTS | Platform Trust Service |
| QA | Quarantäne Agent (Quarantine Agent) |
| QES | Quarantäne Enforcement Server (Quarantine Enforcement Server) |
| QoS | Quality of Service |
| RADIUS | Remote Authentication Dial In User Service |
| RAS | Remote Access Server |
| RSTP | Rapid Spanning Tree Protocol |
| SHV | System Health Validator |
| SIRENED | Structured Integrated REsilient NEtwork Design |
| SMS | Systems Management Server |
| SPS | Speicherprogrammierbare Steuerung |
| SRTP | Secure RTP |
| STP | Spanning Tree Protocol |
| SVP | SpectraLink Voice Priority (SpectraLink) |
| TCG | Trusted Computing Group |
| TCP | Transmission Control Protocol |
| TNCCS | Trusted Network Connection Client-Server |
| TP | Twisted Pair |
| TPM | Trusted Platform Module |
| TSS | TCG Software Stack |
| UDP | User Datagram Protocol |
| URL | Universal Resource Locator |
| USV | Unterbrechungsfreie Stromversorgung |
| VLAN | Virtual LAN |
| VoWLAN | Voice over WLAN |
| VPN | Virtual Private Network |
| VRRP | Virtual Router Redundancy Protocol |
| WEP | Wired Equivalent Privacy |
| WiMAX | Worldwide Interoperability for Microwave Access |
| WLAN | Wireless LAN |
| WPA | Wi-Fi Protected Access |

CCNE

## ComConsult Certified Network Engineer

**Lokale Netze**
27.06. - 01.07.05 in Aachen
12.09. - 16.09.05 in Aachen
28.11. - 02.12.05 in Aachen

**TCP/IP und SNMP**
20.06. - 24.06.05 in Köln
26.09. - 30.09.05 in Berlin
14.11. - 18.11.05 in Bonn

**Internetworking**
26.09. - 30.09.05 in Aachen
28.11. - 02.12.05 in Aachen

**Ethernet Technologien - neuester Stand**
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**
12.09. - 16.09.05 in Aachen
07.11. - 11.11.05 in Aachen

**Trouble Shooting für TCP/IP- und Windows-Umgebungen**
24.10. - 28.10.05 in Aachen

**Trouble Shooting in geswitchten Ethernet-Umgebungen**
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**
26.09. - 30.09.05 in Nürnberg

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

**Sicherheitslösungen III: Planung und praktische Konfiguration**
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:
ComConsult Technology Information Ltd.
121 Paton Rd.
RD1
Richmond
New Zealand
GST Number 84-302-181
Registration number 1260709
Phone: 0064 3 5444632
Fax: 0064 3 5444237

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

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