Dr. Suppan International Institute

Der Netzwerk Insider

Juli 2004

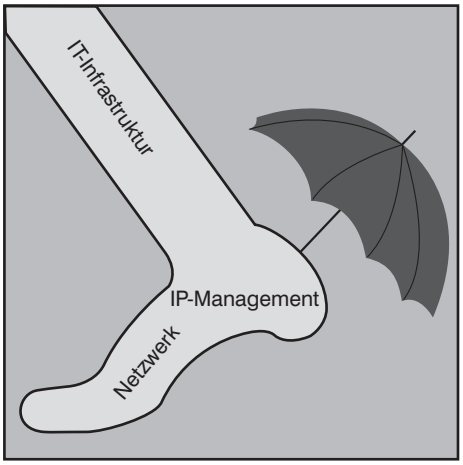
Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

IP-Management: „Achilles Ferse und Umbrella Technologie“

von Markus Holländer

Eine Reihe von Support-Einsätzen hat gezeigt, dass das IP-Management (DHCP - Dynamic Host Configuration Protocol, DNS - Domain Name System, NetBIOS-Namensauflösung) häufiger die Achilles Ferse in der Unternehmens-IT ist. Dabei ist es doch eine Umbrella Technologie, die für sehr viele Bereiche elementar wichtig ist. Das Thema ist eigentlich bekannt, doch wird es immer mehr in den Hintergrund gedrängt, um neuen Diensten und Anforderungen gerecht zu werden. Dabei wird immer wieder vergessen, dass diese neuen Themenfelder in den meisten Fällen auf dem IP-Management beruhen.



Damit Sie auch morgen noch von der Stelle kommen!

Zum Einstieg zwei Beispiele, die diese Situation verdeutlichen:

Innerhalb des ersten Szenarios befand sich der Kunde in der Migration von Windows NT 4.0 zum Active Directory (Version 2, Windows Server 2003) und beim Rollout von Windows XP. Eine vereinfachte Darstellung der Struktur ist der Abbildung 1 zu entnehmen. In diesem Szenario besteht die „neue“ Welt aus einer Gesamtstruktur (forest) des Active Directory und die „alte Welt“ aus mehreren Windows NT Domänen.

weiter auf Seite 14

Zweitthema

Einzug der LAN-Technologie in den WAN-Bereich

von Dr. - Ing. Behrooz Moayeri

Da die standortübergreifende Kommunikation für fast jegliche Art von Organisationen (Unternehmen, öffentliche Verwaltung etc.) immer größere Bedeutung erlangt, werden mit hohem Tempo neue, schnellere, sicherere und effizientere Verfahren für Wide Area Networks (WAN) entwickelt. Das visionäre Ziel aller dieser Entwicklungen ist die Befreiung der IT vom Diktat der Geografie. Informationen und IT-Ressourcen sollen unabhängig vom Standort allen Anwendern im Unternehmensnetz zur Verfügung stehen. Dies ist das Gebot der überall festzustellenden Trends der:

- Virtualisierung: Entkopplung der IT-Arbeitsplätze von „Arbeitsplätzen“ im engeren geografischen Sinne
- Konsolidierung: Kosteneinsparung durch Konzentration von technischen und personellen IT-Ressourcen auf wenige Standorte
- Flexibilität: Möglichkeit der schnellen Reaktion auf Änderungen in der Organisation sowohl innerhalb von Unternehmen als auch bei der Kooperation zwischen Unternehmen.

weiter auf Seite 6

Top-Event

Netzwerk-, System- und Service-Management Forum 2004

auf Seite 4

Zum Geleit

Innovation und Kreativität ergänzen traditionelle Management-Architekturen

auf Seite 2

Report des Monats

Design-Varianten Lokaler Netzwerke im Vergleich

auf Seite 11

Zum Geleit

Innovation und Kreativität ergänzen traditionelle Management-Architekturen

IT- und Netzwerk-Architekturen sind im Wandel. Viele dieser Entwicklungen wurden in den letzten Insider-Ausgaben und im Insider-Online beschrieben. Herausragend sind sicher die Trends im Bereich Sprach-Integration in Netzwerke, Sicherheits-Zonen-Modelle mit automatischer Anomalie-Erkennung, immer stärkere Ausweitung der Umsetzung wichtiger Geschäftsprozesse durch Webapplikationen, internationale Kollaboration in dem Sinne, dass jeder Mitarbeiter an jedem Ort an jedem wichtigen Geschäftsprozess teilhaben kann.

Und wieder einmal stellt sich die Frage, ob unsere bestehenden Netzwerk- und System-Management-Lösungen die geeigneten Hilfsmittel für den Betrieb dieser neuen Architekturen und Anwendungen bieten. Immerhin nimmt die Integration von IT und Geschäftsprozessen immer weiter zu, gerade die Bereiche Webapplikationen und Kollaboration zeigen dies. Damit wird die gesamte IT mehr denn je zur Achillesferse unserer Unternehmen. Der sichere und performante Betrieb wichtiger Geschäftsprozesse basiert auf der Tragfähigkeit unserer Management-Lösungen.

Wie tragfähig sind die bestehenden Management-Lösungen wirklich? Besteht Handlungsbedarf?

Dazu ist festzustellen:

- Jeder, der eine saubere Kern-Architektur mit Monitoring, Eventhierarchie, Regelbasierten Bewertungen, Eventkonsole, Visualisierungen, Reports etc. aufgebaut hat, kann der Entwicklung mit Gelassenheit begegnen. Die Professionalität der Architektur drückt sich genau in dem Aspekt aus, neue Datenquellen ergänzen und bestehende Visualisierungen anpassen zu können, allerdings sind gerade auf der Visualisierungsebene wichtige funktionale Erweiterungen notwendig.

- Aber: neue Funktionsbereiche kommen hinzu und bestehende Schwerpunkte verschieben sich. Dementsprechend sind funktionale Ergänzungen der bisherigen Lösung unvermeidbar. Als Beispiel sei die Darstellung vereinbarter Service-Level inklusive Soll-Ist-Visualisierung und ihre Zuordnung zu Verträgen genannt.

- Parallel verändert sich das Mengengerüst. Bestehende Regelwerke müssen angepasst und konsolidiert werden. Mit der Einführung von Service-Management entsteht zudem der Bedarf, Korrelations- und Filterbedingungen individuell einzelnen Service-Sichten zuordnen zu können, so dass ein Managed Objekt Teil völlig unterschiedlicher Regeln in verschiedenen Service-Sichten sein kann.

Was bedeutet dies im Einzelnen, was ist zu tun, welche neuen Funktionen müssen umgesetzt werden:

- Das Event-Management bedarf eines Redesigns und einer Straffung, sonst droht der Verlust von Übersicht und Kontrolle. Bei der Überarbeitung von Filter- und Korrelationsregeln ist zu prüfen, ob diese Service-spezifisch definiert werden sollten

- Netzwerk-Management muss deutlich modifiziert werden: Voice-Integration, WLAN´s und die Integration von Fertigungs-Netzwerken erfordern weitergehende Lösungen. Speziell im Bereich Performance- und Netzwerk-Service-Management machen universelle Management-Lösungen kaum noch Sinn, da es sein kann, dass das Netzwerk für einen Anwendungsbereich völlig ohne Probleme arbeitet, aber für eine neue Anwendung so nicht zu nutzen ist.

- Da sich immer mehr und immer verschiedenere Anwendungen und Technologiebereiche immer mehr auf wenige zentrale Technologien abstützen (Netzwerke, Server, IP, Webtechniken) ist die Einführung von Technologie- und Anwendungsspezifischem Service-Management unvermeidbar. Nur so kann auf zentralen Infrastrukturen die Betriebssituation einzelner Anwendungsbereiche differenziert überwacht und gesteuert werden. Dabei muss es möglich sein, nicht nur verschiedene Services mit individuellen Regelsätzen zu administrieren, es muss auch möglich sein, dies verschiedenen Vertragssichten zuordnen zu können. So kann ein Managed Objekt nicht nur Teil verschiedener Service-Sichten mit unterschiedlichen Regeln sein, Service-Sichten können auch Vertrags-individuell sein, wenn Verträge unterschiedliche Anforderungen an identische Services stellen

- Die permanente Ausweitung von Security-Lösungen, die immer stärkere Einbindung von Sicherheits-Lösungen in Netzwerk-Strukturen, die Schaffung getrennt steuerbarer Sicherheits-Zonen erfordert ein separates Sicherheits-Management, das von der Anomalie-Erkennung über die effiziente Gegenreaktion bis zur Wiederherstellung des Regelbetriebs reicht. Ziel muss es sein, bedrohte IT-Zonen gezielt wegschalten und reaktivieren zu können und dabei ein Maximum an nutzbarem Testbetrieb aufrecht zu erhalten

- Management-Portale haben sich als ideales Instrument der Zielgruppenoptimierten Betriebs- und Service-Information in den Mittelpunkt vieler Projekte gestellt. Die Umsetzung einer flexiblen Architektur mit Zielgruppenoptimierten Informations-Modellen und Realzeitbasierter Information kennzeichnen hier die technischen Herausforderungen

Dies sind nur ausgewählte Beispiele, die die zurzeit stattfindenden Änderungen im Netzwerk- und System-Management charakterisieren. In Summe sind viele neue Anforderungen und Einzelfunktionen im Gespräch.

Natürlich entsteht durch diese Entwicklungen auch wieder eine Architekturfrage. Wie schon zuvor ausgeführt, können derartige

Innovation und Kreativität ergänzen traditionelle Management-Architekturen

Entwicklungen in einer sauber definierten und gepflegten Architektur ohne Probleme umgesetzt werden. Im Endeffekt repräsentieren sie neue Datenquellen, neue Reaktionsschemata und neue Sichten.

Wer jedoch beim Aufbau seiner Management-Lösung versäumt hat, eine saubere und vor allem Produkt-neutrale Architektur zu definieren, die den Daten- und Funktionsfluss zwischen den Funktionsbereichen des Managements regelt, der kann angesichts der neuen Herausforderungen durchaus zu einem kompletten Redesign seiner Management-Lösung gezwungen sein. Dies muss nicht bedeuten, dass Produkte auszutauschen sind, aber eine Neukonfiguration der bestehenden Produktwelt kann eine Notwendigkeit sein. Hier hat sich in den Projekten der letzten Monate gezeigt, dass es sich aber einem bestimmten Grad an historisch gewachsenen Konfigurations-Labyrinthen nicht lohnt, ein weiteres Labyrinth hinzu zu fügen. In der Regel ist die völlige Neuaufsetzung der wirtschaftlichste, aber auch schnellste Weg zu einer geeigneten Lösung.

Unser Netzwerk-, System- und Service-Management Forum 2004 ist auch in diesem Jahr unser absoluter Top-Kongress. Auf diesem Forum gehen wir auf diese Entwicklungen ein und stellen absolut exklusive Analysen zu den genannten Themen vor.

So erhalten alle Teilnehmer exklusiv und nur auf diesem Forum unsere Analyse über neue und innovative Produkte, die sich als ideale Ergänzung bestehender Management-Architekturen anbieten.

Weitere Analysen sind aufgesetzt, um sie mit den neuesten Top-Informationen aus dem Bereich Netzwerk-, System- und Service-Management zu versorgen.

Beachten Sie die aktuell laufende Frühbucher-Phase. Ich würde mich freuen, Sie auf dem Forum begrüßen zu können. Auch in diesem Jahr trifft sich hier die deutsche Management-Branche.

Ihr
Dr. Jürgen Suppan

12% Frühbucherrabatt bis 31.08.04

Netzwerk-, System- und Service-Management Forum 2004

Teilnahmegebühr vom 08.11. - 11.11.04 inklusive Tutorium am ersten Tag innerhalb der Frühbucherphase € 1.690,-- zzgl. MwSt. (regulär € 1.990,--zzgl. MwSt.)

Teilnahmegebühr vom 09.11. - 11.11.04 ohne Tutorium am ersten Tag innerhalb der Frühbucherphase € 1.430,-- zzgl. MwSt. (regulär € 1.690,--zzgl. MwSt.)

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

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk-, System- und Service-Management Forum 2004

Ich buche das Seminar
Netzwerk-, System- und Service-Management Forum 2004
vom 08.11. - 11.11.04

☐ **mit Tutorium € 1.690,-- zzgl. MwSt.**

☐ **ohne Tutorium € 1.430,-- zzgl. MwSt.**

mit Workshop (siehe Seite 4-5)
☐ **Workshop 1** ☐ **Workshop 6**
☐ **Workshop 2** ☐ **Workshop 7**
☐ **Workshop 3** ☐ **Workshop 8**
☐ **Workshop 4** ☐ **Workshop 9**
☐ **Workshop 5**

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Top-Event des Jahres

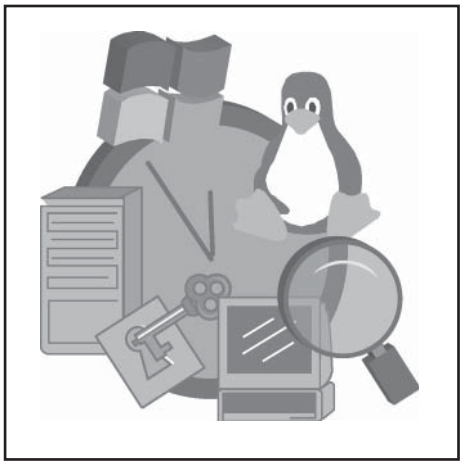
Netzwerk-, System- und Service-Management Forum 2004

IT- und Netzwerk-Architekturen sind im Wandel und erfordern erweiterte und innovative Management-Lösungen. Das Netzwerk-, System- und Service-Management Forum 2004 analysiert die neuesten Entwicklungen im Bereich Management, präsentiert aktuelle Projekt-Erfahrungen, diskutiert wichtige Trends und evaluiert die aktuelle Markt- und Produktsituation.

Schwerpunkt-Themen des Netzwerk-, System- und Service-Management Forums 2004 sind dementsprechend:

- Neupositionierung Netzwerk-Management: Netzwerk-Konvergenz erfordert erweiterte Lösungen
- Service-Management und stufenweise Integration von SLA´s
- Von der Anomalie-Erkennung über Intrusion Prevention zum Security-Operating
- Potenziale und innovative Funktionen neuer Service- und System-Management-Produkte in der Analyse
- Management von Geschäftsprozessen
- Aufbau von Management-Portalen
- Risiko-Management im IT-Betrieb
- User- und Identity-Management

Speziell zum Forum analysieren wir für



Sie: welche neuen, innovativen und kreativen Produkte gibt es, die ideal als Ergänzung bestehender Lösungen geeignet sind und einen echten Mehrwert bieten. Das Ergebnis wird exklusiv auf dem Forum präsentiert, jeder Teilnehmer erhält zudem ein kostenloses Exemplar des Analyse-Ergebnisses. Diese Analyse wird außerhalb des Forums nicht veröffentlicht werden und ist exklusiv für die Teilnehmer des Forums.

Auch in diesem Jahr erwartet Sie wieder ein herausragender Mix aus:

- Hintergrund-Analysen und Bewertungen aktueller Trends und Technologien
- Erfahrungsberichte aus erfolgreichen Projekten
- Diskussion herausragender Themen
- Live- und Vertiefungsworkshops zu den Top-Themen
- Begleitende Fachausstellung

Top-Informationen mit direkter Umsetzbarkeit in der Praxis haben in den letzten Jahren dazu geführt, dass sich diese Veranstaltung zu einem herausragenden und beliebten Treffpunkt der deutschen IT- und Management-Szene entwickelt hat. Viele treue Stammkunden speziell dieser Veranstaltung belegen die hohe Qualität, Aktualität und den Bezug zur Praxis.

Details entnehmen Sie bitte dem Programm: www.comconsult-akademie.de In den nächsten Wochen werden wir Sie über ausgewählte Teilthemen des Forums informieren, um Ihnen auch einen ersten Eindruck über die aktuellen Entwicklungen zu geben.

Programmübersicht

Montag, den 8.11.2004: Trends, Hintergründe, Analysen (Tutorium)

Trends 2005: IT-Architekturen im Wandel: wie tragfähig sind bestehende Management-Lösungen

- Netzwerk-Konvergenz: totale Konzentration auf eine Infrastruktur
- Voice-Integration: pro und kontra
- Megatrend Kollaboration: Einfluss auf Architekturen
- Integration von Produktionsumgebunge und Warenlogistik: wo sind die Grenzen
- Was müssen Server und Clienten leisten, welche Technologie setzt sich durch
- Die Wireless-Revolution: neue Systemarchitekturen stellen neue Anforderungen
- Sicherheits-Lösungen: Status Quo
- Tragfähigkeit bestehender Management-Lösungen
- Welche Management-Bereiche gewinnen an Bedeutung
- Positionierung: Netzwerk-Management, Service-Management, Security-Management

Dr. Jürgen Suppan, ComConsult Research

Netzwerk-Trends: wie weit werden uns neue Technologien bringen

- Neue Technologien bedingen neue Strukturen wann kommt es?
- Multigigabit Ethernets
- Multigigabit WANs
- Der Weg zu Gigabit WLANs
- Konsequenzen für Nutzung und Management

Dr. F.-J. Kauffels, Unternehmensberater

Netzwerk-Redesign: neue Anwendungen erfordern neue Strukturen

- Grenzen traditioneller Netzwerke
- Neue Anforderungen: Voice, Fertigungs-Integration, Security, WLAN
- Verfügbare Design- und Struktur-Technologien in der Analyse
- Spezialthema: Voice-ready Netzwerk-Design
- Spezialthema: Handhabung stark verschiedener Anforderungen innerhalb eines Netzwerks
- Beispiele und Empfehlungen

Dipl.-Inform. Petra Borowka, UBN

Der Veranstalter behält sich Änderungen im Programm vor!

Netzwerk-, System- und Service-Management Forum 2004

Dienstag, den 9.11.2004: Technologien in der Analyse

Neue Management-Produkte in der Analyse: Potenziale und innovative Funktionen neuer Service- und System-Management-Produkte
- Bedarf für innovative Lösungen
- Ergänzung bestehender Lösungen durch intelligente Zusatzfunktionen
- Ausgewählte Produkte in der Analyse
- Bewertung und Empfehlungen

Dipl.- Kfm. Martin Woyke, ComConsult Kommunikationstechnik

Management von Geschäftsprozessen und Aufbau von Management-Portalen
- Service-Abbildung in traditionellen Management-Architekturen
- Innovative Funktionen
- Effiziente Arbeitsoberflächen für Administratoren, Operatoren und Management
- Integration von SLA-Definitionen und Metriken
- Das Management-Portal: Schlüssel zur Projekt-Anerkennung
- Beispiele und Empfehlungen

Nils Meyer, Computer Associates

Sicherheit in den Netzwerken einer Privatbank
- Projektziele
- Aufbau einer Policy
- IDS-Grobkonzept
- Anforderungen an Produkte
- Auswahl geeigneter Produkte
- Netzbasierte Intrusion Prevention Produkte
- Kosten, Betrieb, Sicherheitsstatus
- Bewertung und Ausblick

Ralf Felden, HSBC Trinkaus & Burkhardt

Operational Business Risks und deren Management durch NSM und IT Service Prozesse nach best practices
- Risikomanagement heißt zuerst Risikoidentifikation: welche IT Services sind für die Business Prozesse Ihrer Kunden wichtig?
- Basel II und IT Service Management: die Zusammenhänge erkennen und nutzen
- Schwachstellenanalyse: wie Service Bäume und Fehler Bäume helfen, die wichtigen Systeme richtig abzusichern
- Gegenmaßnahmen festlegen und kontinuierlich managen: Tooleinsatz und proaktives Arbeiten setzt wirksame IT Service Prozesse voraus

Jürgen Dierlamm, Microfin

Security von Web-Applikationen
- Webapplikationen dominieren neue Software-Architekturen
- Neue Angriffsformen auf Applikationsebene
- Gravierende Sicherheits-Mängel: Ergebnisse einer Studie
- Alternative Lösungsansätze
- Traditionelle Firewall-Technik und ihre Grenzen
- Empfehlungen zur Umsetzung

Detlef Weidenhammer, GAI NetConsult

Performance und Service-Level-Management
- Bedarfsanalyse
- Architekturen und Varianten
- Aktuelle Entwicklungen
- Typische Lösungsansätze

Dr. F.-J. Kauffels, Unternehmensberater

Mittwoch, den 10.11.2004: Workshop-Tag

Die Durchführung der Workshops wird am Teilnehmerinteresse ausgerichtet. Bitte wählen Sie aus den Workshops drei aus. Die Workshopzeiten sind von 9:00 - 12:00 Uhr, von 13:00 - 16:00 Uhr und von 16:00-19:00 Uhr.

Workshop 1: Neuestes aus Messtechnik und Analyse
Workshop 2: Service-Management
Workshop 3: Neue Technologien in geswitchten Netzwerken: wie werden sie gemanaged
Workshop 4: Netzwerk-Management-Plattformen im Live-Vergleich
Workshop 5: IT Service Continuity Management nach ITIL: wie proaktives Problem Management nach ITIL und System Management helfen, Notfälle zu vermeiden
Workshop 6: Wireless-Technologien in der Analyse
Workshop 7: Management von Services und Geschäftsprozessen: Business Process Management im Live-Vergleich
Workshop 8: Security-Operating: Sicherheits-Risiken im Griff
Workshop 9: Trennung von Benutzer-Gruppen in Netzwerken

Donnerstag, den 11.11.2004

Business-Process-Management 2004
- Themenüberblick
- Marktübersicht und Wachstumsprognose
- Analystenbewertungen und Kundeneinschätzungen
- Darsteller der Keyplayer und deren Fokus
- Erfahrungen aus dem Projektgeschäft
- Empfehlungen

Ralf Horstmann, ComConsult Kommunikationstechnik

Secure Networks: sichere Netzwerke anstatt Netzwerk-Sicherheit
- Authentisierung und Advanced Policy Management
- Verschiedenste Authentisierungsmethoden und Policies auf einen Blick
- Kombination von IDS und Policy Management zu einem verteilten IPS
- Ein selbstverteidigendes Netzwerk in der Praxis
- Endpoint Security Integration: wie mache ich das Endsystem sicher und kopple dies mit der Netzwerkauthentisierung

Markus Nispel, Enterasys Networks

Redesign Netzwerk-Management: was eine moderne Lösung leisten muss
- Beispiel-Szenario: Management einer konvergenten Vernetzung
- Lösungs-Szenario mit theGuard! System Management Suite
- Architektonische Details
  - o Basis-Architektur und Objektmodell
  - o Topologie- und Verbindungs-Management
  - o Korrelation
  - o SLA-Management
  - o Aufbau eines Management-Portals

Georg Kieferl, Realtech AG

IP-Management: Eckpunkte einer professionellen Planung
- IP-Management: die Achilles-Ferse der Unternehmen
- Server, Applikationen, Benutzerverwaltung: neue Anforderungen
- K.O.-Kriterium: Dynamik gefordert
- IP-Management als Umbrella-Technologie
- Notwendigkeit der Integration mit Verzeichnisdiensten am Beispiel Active Directory
  - o Integrierte Gestaltung von DNS, DHCP und Directory Service
  - o Gegenseitige Konsequenzen und Anforderungen
- Plattformen integrieren: Unix und Windows, zwei Philosophien treffen aufeinander
- Lösungsansätze und Erfahrungen

Markus Holländer, ComConsult Beratung und Planung

User- und Identity-Management

N.N.

Zweitthema

Einzug der LAN-Technologie in den WAN-Bereich

Fortsetzung von Seite 1

Dr. Behrooz Moayeri (moayeri@comconsult.com) ist Mitglied der Geschäftsleitung der ComConsult Beratung und Planung GmbH, Aachen. Er hat in den letzten 15 Jahren zahlreiche Unternehmen und Organisationen bei der Konzipierung von IT-Infrastruktur-Konzepten, u. a. beim Aufbau standortübergreifender Netze, beraten.

Der vorliegende Beitrag befasst sich mit zum Teil bahnbrechenden neuen Entwicklungen im WAN-Bereich, die in einem Wort als die Aufhebung der Grenzen zwischen Local, Metroplitan und Wide Area Networks (LAN, MAN und WAN) bezeichnet werden können. LAN-Technologie findet Einzug in den Weitverkehrsbereich.

Dabei sollen WAN immer noch bezahlbar bleiben. Also müssen Synergien her, die nur Provider mit einer Mehrzahl an Kunden herstellen können. Der Provider stellt eine Infrastruktur zur Verfügung, die von mehreren Kunden genutzt wird (s. Abbildung 1).

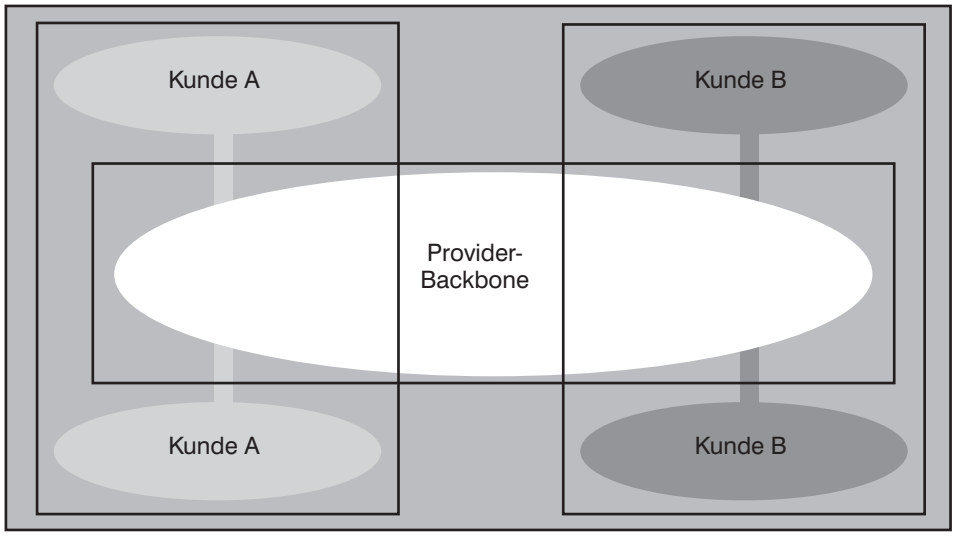


Abbildung 1: Nutzung der Provider-Infrastruktur durch mehrere Kunden

Relevante Standards

Die drei ausschlaggebenden Standardisierungsgremien für neue WAN-Technologien:

- Internet Engineering Task Force (IETF)
- Institute of Electrical and Electronic Engineers (IEEE)
- International Telecommunication Union – Telecommunication Standardization Sector (ITU-T)

Neben diesen Gremien sind auch die Aktivitäten des Metro Ethernet Forum (MEF) zu erwähnen.

Konvergenz auf Ethernet-Ebene

Nachdem die Konvergenz von IT-Infrastrukturen in Form der Nutzung des Internet Protocol (IP) für alle Kommunikationstypen (Daten, Sprache, Video, Storage, Industrieanwendungen) in den letzten Jahren zum unaufhaltsamen Trend geworden ist, haben wir es nun mit einer neuen Konvergenz zu tun: die Ethernet-Konvergenz. Ethernet wurde zwar ursprünglich als Technologie für Local Area Networks (LAN) konzipiert, ist aber zurzeit dabei, auch in den Weitverkehrsbereich (Wide Area Networks, WAN) einzuziehen. Stadtnetze auf reiner Ethernet-Basis, zum Beispiel mit einem Backbone auf Basis von Gigabit Ethernet (GE), sind keine Seltenheit mehr und sind sogar auf dem Wege, zur Regel bei MAN (Metropolitan Area Networks) zu werden.

Nun werden von den Herstellern und den Standardisierungsgremien aber auch Verfahren entwickelt, mit denen die Domäne von Ethernet noch weiter ausgedehnt wird. Ethernet wird zu einer LAN/MAN/WAN-Technologie.

Eine ganze Reihe von Projekten innerhalb von ITU-T befasst sich mit dem Einsatz von Ethernet im WAN-Bereich, darunter die Empfehlung G.7041 unter den Namen Generic Framing Procedure (GFP).[1] Dabei werden die Ethernet-Rahmen über ein synchrones hierarchisches Netz wie SDH (Synchronous Digital Hierarchy) übertragen. Das Rahmenformat von Ethernet wird beibehalten, nicht jedoch die bei Ethernet typischen „runden" Bitraten. Anstatt dieser werden die bei SDH üblichen Bitraten verwendet.

Dabei wird Folgendes nicht übertragen:

- Spanning Tree BPDUs
- Frames an reservierte Multicast-Adressen
- LACP Frames
- Slow Protocol (Typ 8809)
- PAUSE Frames
- MAC Control Frames (Typ 8808)
- Zu kurze oder zu lange Frames
- CRC-Fehler
- Alignment-Fehler

Der Vorteil dieses Verfahrens liegt in der weiteren Nutzung der synchronen optischen Netze, die einerseits dem Investiti-

[1] ITU-T Recommendation G.7041, Generic Framing Procedure, Dezember 2003

onsschutz Rechnung trägt und zum anderen die Möglichkeit gibt, die sehr robusten und auch auf Ausfälle sehr zuverlässig, schnell und selbstheilend reagierenden SDH-Mechanismen zu nutzen.

Neues von MPLS

Das Multiprotocol Label Switching (MPLS) ist bereits zum de facto Standard für neue WAN-Dienste der Provider geworden. MPLS erlaubt die Abbildung mehrerer Kundennetze (Virtual Private Networks, VPN) mit unabhängigen IP-Adress- und Routing-Konzepten auf ein und die selbe WAN-Infrastruktur, wobei bisher die standortübergreifende Kommunikation innerhalb von MPLS-VPN auf Layer-3-Routing basiert. Nun arbeitet die IETF am so genannten Virtual Private LAN Service (VPLS, Emulation von LAN über eine MPLS-Wolke), Virtual Private Wire Service (VPWS, Punkt-zu-Punkt-Verbindungen, u. a. Punkt-zu-Punkt-Ethernet-Verbindungen, über eine MPLS-Wolke) sowie IP-only L2 VPNs, einem Dienst, der IP-Endgeräten die Möglichkeit gibt, über eine MPLS-Wolke so zu kommunizieren, als ob sie an das selbe IP-Subnetz angeschlossen wären.[1]

Die Frage nach dem Nutzen solcher standortübergreifender IP-Subnetze ist schnell beantwortet: Wer kennt schon nicht die Anforderung, dass beispielsweise zwei Knoten eines Server-Clusters an unterschiedlichen Standorten aufgestellt werden? (s. Abbildung 2)

Normalerweise scheitert ein solches Vorhaben an den unterschiedlichen Adressbereichen in den beiden Standorten. Mit L2VPN wäre dieses Problem gelöst.

Neues von IEEE

Beim IEEE wird an der Anpassung des Bridging-Standards IEEE 802.1D sowie des Standards für Virtual LAN (VLAN), IEEE 802.1Q, an die Bedürfnisse von WAN gearbeitet. Darüber hinaus gibt es bereits seit 2003 den Standard für die Luftschnittstelle im Frequenzbereich 2 bis 11 GHz im Rahmen von „Wireless MAN“ gemäß IEEE 802.16 (Fixed Wireless)[2]. Access Points dieser Technologie könnten z. B. über DSL-Verbindungen an den nächstgelegenen Point of Presence (PoP) angeschlossen werden und eine Zelle versorgen (s. Abbildung 3). Die Größe einer solchen Zelle ist vom eingesetzten Verfahren und den Umgebungsbedingungen abhängig. Eine kreisförmige Zelle mit dem Radius von ca. 120 Metern würde einer Zellenfläche von ca. 0,05 km² entsprechen. Für eine Fläche von 100 km² würde der Provider bei einer vereinfachten Rechnung 2.000 Access Points benötigen.

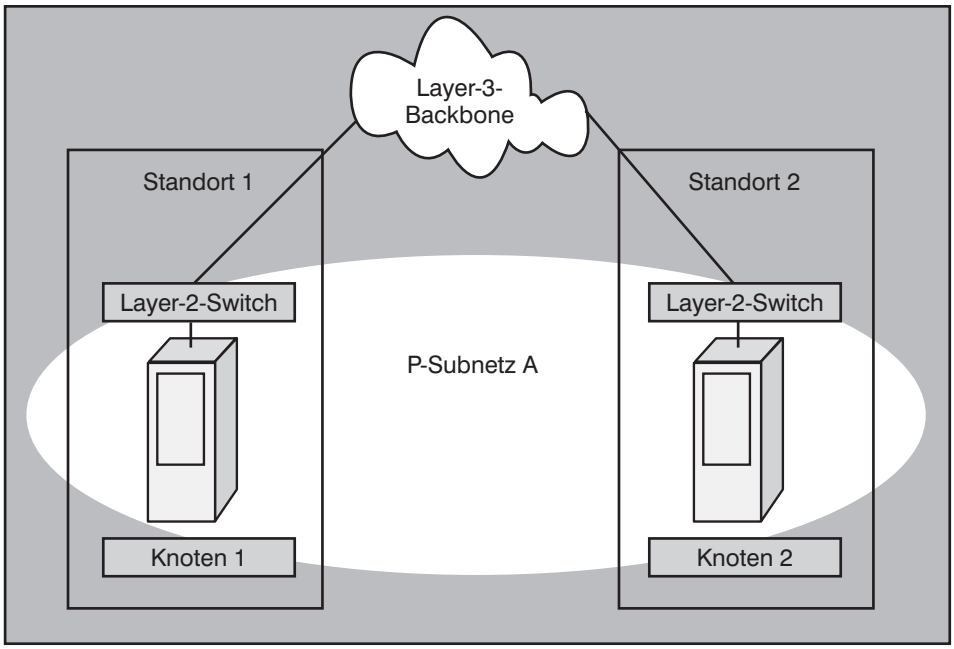


Abbildung 2: Standortübergreifende IP-Subnetze

Fortschritte macht die Arbeit für die künftige Spezifikation Ethernet in the First Mile (EFM), die später als IEEE 802.3ah verabschiedet wird. Dabei wird eine Kupferschnittstelle mit einer Reichweite von 2.700 m definiert. Die technische Basis dafür wird G.SHDSL sein. Im Rahmen des Projektes 802.3ah wird ebenfalls der Ansatz für das so genannte Ethernet Passive Optical Network (EPON) definiert. EPON soll mit ATM-basierenden Verfahren wie ATM Passive Optical Network) konkurrieren und preiswerter als diese sein.

Zu IEEE 802.17

Eine weitere wichtige Standardisierungsarbeit im Rahmen von IEEE ist die Entwicklung des Resilient Packet Ring (RPR), der im künftigen Standard IEEE 802.17 spezifiziert wird. Auf dieses Verfahren gehen wir im Folgenden etwas detaillierter ein.

Der Resilient Packet Ring (RPR) arbeitet ähnlich wie Token Ring und FDDI mit einer Ringtopologie. Dabei wird die im SDH-Bereich übliche redundante Struktur mit zwei gegenläufigen Ringen nachgebildet, mit dem Unterschied, dass es sich beim RPR um ein asynchrones Paket- und kein

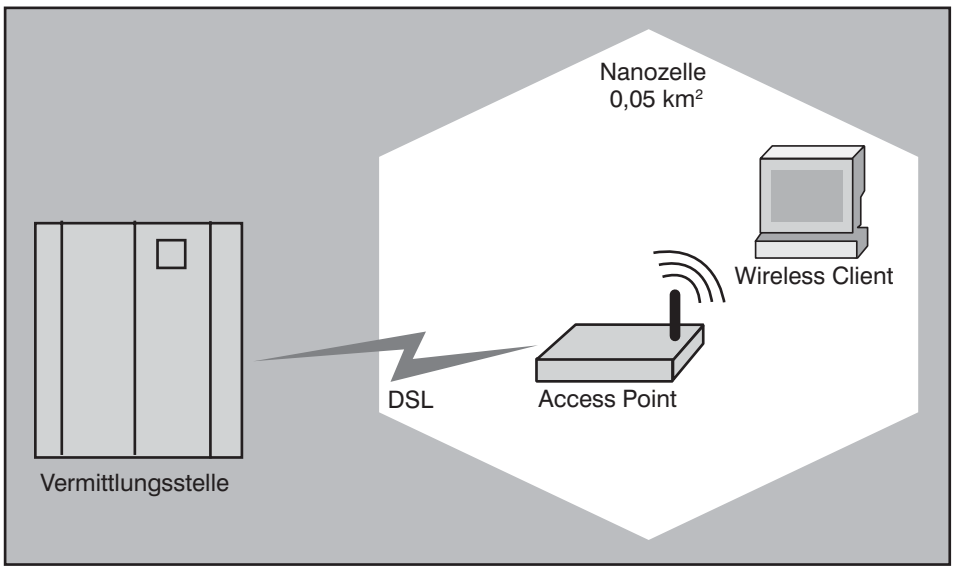


Abbildung 3: Fixed Wireless

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

[2] s. Air Interface for Fixed Broadband Wireless Access Systems, IEEE 802.16a.

Einzug der LAN-Technologie in den WAN-Bereich

synchrones Zeitmultiplexverfahren handelt. Im Prinzip ist RPR eine weitere Layer-2-Technologie im Rahmen von IEEE 802. Der Übergang zwischen RPR und anderen IEEE-802-basierten Netzen wie Ethernet ist somit sowohl auf der Ebene von Layer 2 (Bridging) als auch auf Routing-Ebene (Layer 3) möglich (s. Abbildung 4).

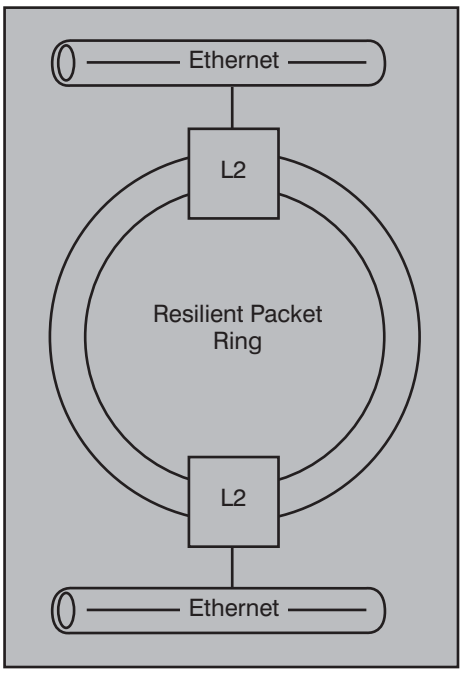


Abbildung 4: Resilient Packet Ring gemäß IEEE 802.17

Braucht man ein weiteres Layer-2-Verfahren? Reicht Ethernet nicht aus? Der Nachteil von Ethernet aus der Sicht der Verfechter von RPR liegt vor allem in den im Vergleich zu SDH fehlenden Funktionen wie schnelle und robuste Fail-over-Mechanismen sowie darin, dass es Ethernet an Fairness fehlt. Diejenigen, die Erfahrungen sowohl mit Token Ring als auch mit Ethernet gesammelt haben, berichten, dass ein Token Ring selbst bei nahezu Vollauslastung alle angeschlossenen Stationen fair und zuverlässig bedient hat. Dies kann Ethernet nicht. Ab einer bestimmten Auslastung wird Ethernet unfair und unzuverlässig. Da soll RPR helfen, indem er die Vorteile von Ethernet (Flexibilität und Vermeiden starrer Bandbreitezuordnungen wie unter SDH) mit den Vorteilen von SDH (schnelle Redundanzmechanismen und Zuverlässigkeit selbst bei hoher Auslastung) verbindet.

Im Unterschied zu Token Ring, bei dem erst der Sender das Paket vom Netz genommen hat, sieht RPR analog zur SAN-Technologie FibreChannel Arbitrated Loop (FC-AL) vor, dass der Empfänger das an ihn gerichtete Paket vom Ring entfernt. Dies hat den Vorteil, dass bei großen Netzausdehnungen der Ring besser ausgelastet werden kann. Broadcast-Pakete können natürlich auch beim RPR nur vom Sender „entsorgt“ werden. Damit Unicast-Pakete nicht endlos im Ring zirkulieren, gibt es beim RPR analog zu IP-Netzen ein Feld mit dem Namen time to live (TTL). Jede Station, die das Paket weiterleitet, dekrementiert den TTL-Wert. Ist die TTL ausgeschöpft, wird das Paket verworfen.

RPR nach dem bisherigen Entwurf vom November 2003 unterstützt die folgenden Verkehrsklassen:

- A0: Diese Klasse arbeitet mit der Reservierung von Bandbreite. Im ganzen Ring werden A0-Reservierungen im Rahmen von MAC-Frames bekannt gegeben. Damit ist jeder Station in der Lage zu kalkulieren, wie viel Bandbreite nach Abzug aller A0-Reservierungen übrig bleibt.

- A1: Auch für diese Klasse wird Bandbreite reserviert mit dem Unterschied, dass im Falle der Nichtnutzung der Bandbreite diese den anderen Anwendungen zur Verfügung steht.

- B-CIR (CIR steht für committed information rate): Dieser Verkehrstyp ist ungefähr mit den Permanent Virtual Connections (PVCs) vergleichbar, denen z. B. in einem Frame-Relay-Netz eine Bandbreite zugesichert wird. Bei Nichtnutzung dieser Bandbreite steht sie anderen Anwendungen zur Verfügung.

- B-EIR (EIR steht für excess information rate): Dieser Verkehrstyp ist ungefähr mit den Permanent Virtual Connections (PVCs) vergleichbar, denen z. B. in einem Frame-Relay-Netz eine Bandbreite in Aussicht gestellt wird, wenn die Netzressourcen dafür verfügbar sind.

- C: Diese Klasse entspricht einem Best-Effort-Dienst.

Die Klassen B-EIR und C werden als fairless eligible (FE) Klassen genannt, weil deren Verkehr den Richtlinien des RPR-eigenen Fairness-Algorithmus unterliegt.

In jeder Station ist für jeden gegenläufigen Ring ein so genannter Traffic Shaper implementiert, der dafür sorgt, dass der von der Station generierte Verkehr die nach Abzug des A0-Verkehrs übrig bleibende Restbandbreite zu keinem Zeitpunkt überschreitet. Darüber hinaus gibt es den so genannten Fairness Shaper, der die Durchsetzung der Fairness mittels Steuerung des FE-Verkehrs übernimmt.

Kein Prioritätensystem in Netzkomponenten kommt ohne differenzierte Warteschlangen aus. Daher arbeiten die RPR-Knoten mit den beiden Sendewarte-

schlangen Primary Transit Queue (PTQ) für die Verkehrsklassen A0 und A1 sowie Secondary Transit Queue (STQ) für die Verkehrsklassen B und C. Ein relativ komplexer Fairness-Algorithmus sorgt dafür, dass keine Station „aushungert“, sprich keine Situation eintritt, in der eine Station aufgrund der anderweitig intensiven Netzauslastung gar nicht zum Zuge kommt.

Der RPR geht auf eine Initiative von Herstellern wie Cisco Systems und Nortel Networks zurück. Vorgänger dieser Technologie sind proprietäre Verfahren, die in einigen Metro- und WAN-Komponenten einiger dieser Hersteller implementiert sind. Bisher sind diese herstellerspezifischen Verfahren auf kaum Akzeptanz gestoßen. Wird die Verabschiedung eines Standards etwas daran ändern? Möglicherweise nein, denn die Geschichte von IEEE 802 ist auch eine Geschichte von in Vergessenheit geratenden Verfahren. Wer erinnert sich noch an 802.4 (Token Bus) und 802.12 (100BaseAnyLAN)?

Eine Technologie, die einen echten Mehrwert bringt (wie im Falle von drahtlosen Verfahren), ist anders zu bewerten als ein Verfahren, das alte Konzepte im neuen Gewand wieder präsentiert. Aber meine eher skeptische Meinung zu RPR kann von so vielen Faktoren widerlegt werden, die nichts mit Vernunft, Effizienz und Wirtschaftlichkeit zu tun haben. Dazu zählt manchmal die Eigendynamik von Marketing-Maschinerien.

Fazit

Unabhängig davon, was man von dem einen oder anderen neuen WAN-Verfahren hält, steht fest, dass uns mit einer Reihe von Technologien neue Möglichkeiten gegeben werden, die Grenzen zwischen LAN und WAN aufzuweichen. Die standortübergreifenden Netze werden schneller und kosten (umgerechnet auf Bits pro Sekunde) immer weniger. Das bestätigen auch sensationelle Ergebnisse von neuesten WAN-Ausschreibungen, die wir im Auftrag unserer Kunden durchgeführt haben. Es lohnt sich, WAN-Konzepte auf den Prüfstand zu stellen.

Neues Seminar

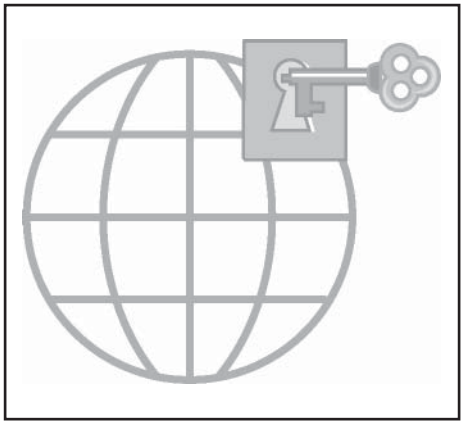
NEUES SEMINAR! Sicherheit von Web-Applikationen

Vom 29. November bis 01. Dezember 2004 veranstaltet die ComConsult Akademie erstmalig ihr neues Seminar „Sicherheit von Web-Applikationen“ im Excelsior Hotel in Berlin.

Aktuelle Untersuchungen zeigten, dass bis zu 90% aller Web-Applikationen unzureichend gesichert sind. Dieses neue Seminar zeigt Ihnen, worin Risiken bestehen und wie Sie Ihre Web-Applikationen optimal schützen.

Dieses Seminar zeigt typische Schwachstellen von Webanwendungen auf und stellt Schutzmaßnahmen von der Programmierung bis zum Betrieb vor. Dabei werden die verwendeten Angriffstechniken live vorgeführt und auch ein zur Abwehr geeignetes Web Application Security Gateway beispielhaft präsentiert.

Webanwendungen werden immer wichtiger, um über das Internet einen einfachen Zugriff auf Geschäftsvorgänge und -daten zu ermöglichen. Sie sind aber auch mit hohen Sicherheitsrisiken verbunden, da Lücken den Zugriff auf interne Daten und System ermöglichen können. Sicherheitsüberprüfungen ergaben bei über 70% der untersuchten Webanwendungen deutliche Mängel.



Herkömmliche Schutzvorkehrungen durch Firewalls können auf der Anwendungsebene bestenfalls offensichtlichen Missbrauch erkennen. Aktuelle Angriffe zielen aber gerade auf Schwachstellen innerhalb einer Anwendung. Ursache hierfür ist zumeist die mangelhafte Beachtung von Sicherheitsaspekten bei der Programmentwicklung.

In diesem Seminar lernen Sie
- wie die gefährlichsten Angriffe auf Webanwendungen funktionieren
- wie ein sicheres Applikationsdesign zu entwerfen

und umzusetzen ist
- welche Projektvorgaben bei der Erstellung einer sicheren Webanwendung gemacht werden sollten
- welchen Vorteil der Einsatz von Portallösungen bietet
- wie der Schutzbedarf einer Webanwendung die einzusetzenden Sicherheitsanforderungen bestimmt
- wie eine bereits vorhandene Webanwendung ohne Codezugriff auch noch nachträglich gesichert werden kann
- welche Auswahlkriterien an ein Web Application Security Gateway zu stellen sind
- welche zusätzlichen Schutzmaßnahmen für die Serverumgebung zu treffen sind

Referent:
Dipl.-Physiker Frank Breitschaft war nach seinem Studium der Physik in verschiedenen öffentlichen Rechenzentren tätig - zuletzt im Ressourcenzentrum des Deutschen Humangenomprojekts. Mittlerweile im Bereich Netzwerkentwicklung und Netzwerkberatung bei der GAI NetConsult GmbH in Berlin beschäftigt, liegt sein Schwerpunkt bei Konzeption und Betrieb von Netzwerken insbesondere unter Sicherheitsaspekten.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Sicherheit von Web-Applikationen

☐ Ich buche das Seminar
Sicherheit von Web-Applikationen

__ vom 29.11. - 01.12.04 in Berlin

(Preis € 1.690,-- zzgl. MwSt.)

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

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

Report des Monats

Design-Varianten Lokaler Netzwerke im Vergleich

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

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

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

Nach einer einleitenden Beschreibung häufiger Störfälle und ihrer Auswirkungen, erfolgt die Definition von Gefährdungsklassen für Netzwerkkomponenten und die entsprechende Einordnung typischer Systeme. Anhand dieser Gefährdungsklassen werden Kostenrahmen und notwendige Randbedingungen für Redundanzmaßnahmen charakterisiert.

In einem eigenen Kapitel werden dann umfangreiche, detaillierte Beispiele realer Netzwerke aus der breiten Praxiserfahrung der Autoren vorgestellt. Hier werden jeweils mehrere Netze aus den Bereichen Produktion, Dienstleistung und öffentliche Arbeitgeber skizziert und hierarchisch nach Netzwerkklassen geordnet.

Im Folgenden lesen Sie einen Auszug aus diesem Report

Bei redundant ausgelegten Netzen kommt es häufig vor, dass es verschiedene Wege von einem Router zu einem Netz gibt, die dieselben Kosten aufweisen. Der Router kann alle Wege nutzen und so eine Lastverteilung generieren. Man spricht in diesem Fall von Equal Cost Multipath Routing.

Die Abbildung auf der folgenden Seite zeigt ein Beispiel für eine Lastverteilung bei angenommenen gleichen Kosten. Während die ungeraden, roten Pakete den linken Weg nehmen, werden die grünen Pakete über den rechten transportiert.

Die Lastverteilung wird von jedem Router generiert, auf dem Weg durch ein Netz muss ein Router nicht wissen, ob er das Paket aufgrund von Lastverteilung erhalten hat oder ob alle Pakete einer Kommunikation über ihn geleitet werden. Aus diesem Grund ist es auch nicht nötig, dass alle Router darin übereinstimmen müssen, lastverteilt zu arbeiten.

Nicht alle Routingprotokolle sehen eine Lastverteilung explizit vor: während es bei OSPF bei der Entwicklung bedacht wurde, schweigt der RIP-Standard zu dem Thema. Da jedoch Lastverteilung über Wege mit gleichen Kosten niemals Probleme bezüglich Routing Loops machen kann, wird es von vielen Herstellern unterstützt. Zu einem Interoperabilitätsproblem zwischen Routern, die Lastverteilung unterstützen und solchen die es nicht tun, kommt es wegen der diesbezüglichen Unabhängigkeit der Router voneinander nicht.

Anders sieht das bei Wegen mit ungleichen Kosten aus, genannt Unequal Cost Multipath Routing. Bei den beiden behandelten Standardprotokollen ist das weder vorgesehen noch möglich. Hier besteht die Gefahr, dass es zu einem Routing Loop kommt, wenn sich beispielsweise zwei Router die Pakete gegenseitig immer wieder zuschicken. Das propietäre Enhanced Interior Gateway Protocol (EIGRP) und das Vorgängerprotokoll IGRP der Firma Cisco bieten diese Möglichkeit. Das Vorgehen wird in Kapitel 9.4.5 behandelt.
Für das Verfahren der Paketaufteilung kommen verschiedene Möglichkeiten in Betracht:

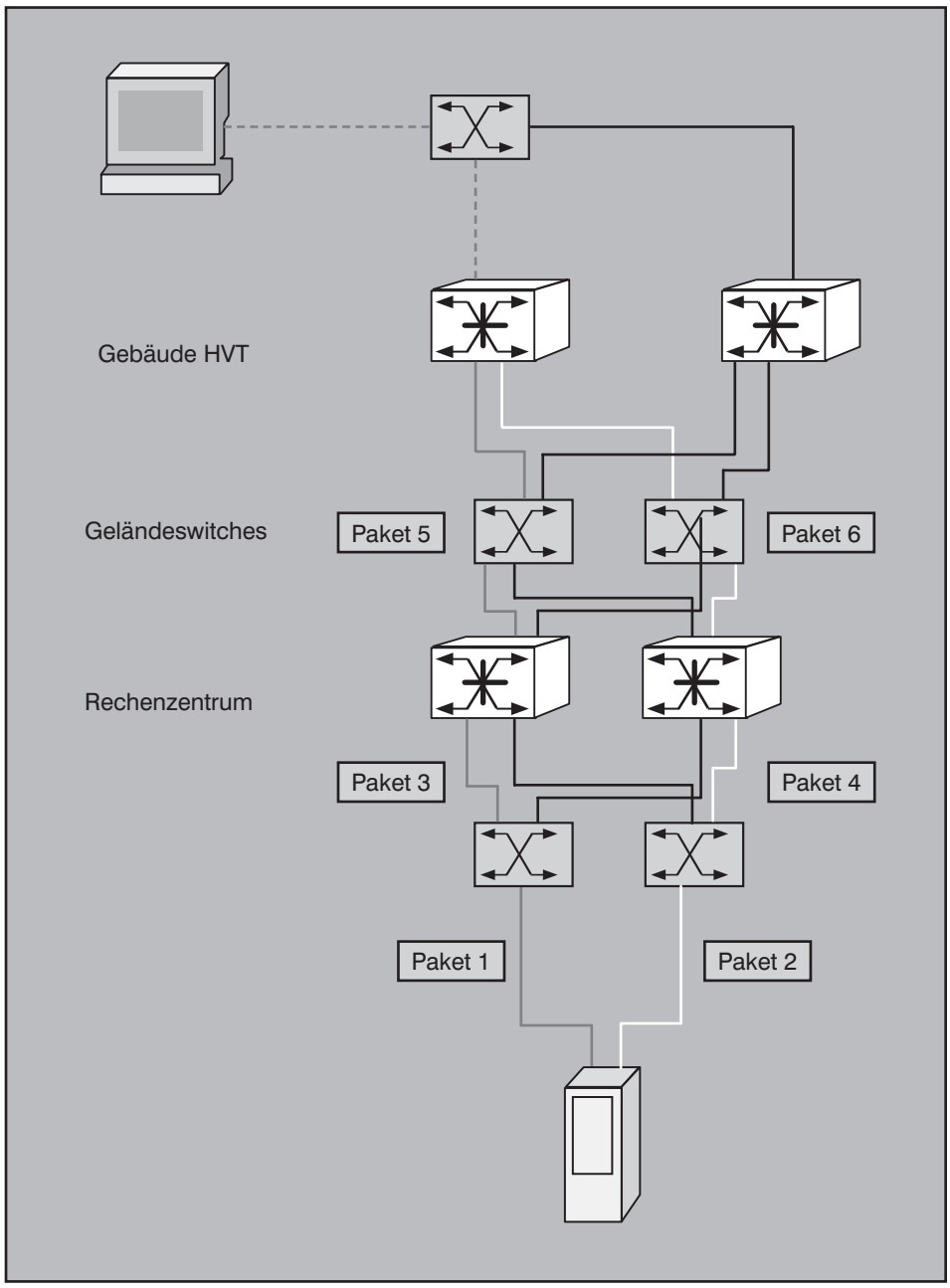
- Pro Paket (Packet-by-Packet)
- Nach Zieladresse (Destination)
- Nach Quell- und Zieladresse (Source-Destination)
- Nach Session (Source-Destination inkl. TCP/UDP-Portnummern)

Welche Möglichkeiten einem zur Verfügung stehen, variiert von Gerät zu Gerät und von Hersteller zu Hersteller. Allgemein lässt sagen: je größer (und teuerer) das Gerät ist, desto mehr Möglichkeiten stehen einem zur Verfügung. Häufig ist es bei den High-End-Layer-3-Switches möglich, das Verfahren mittels Konfigurationsparameter auszuwählen.

Verteilung pro Paket

Ein Router entscheidet pro Paket, entlang welchen Weges er es routet. Da viele Router und Layer-3-Switches wegen ihrer Hardware Architektur nicht dazu in der Lage sind, eine solche Entscheidung mit der nötigen Performance treffen zu können, ist diese Option, wenn konfigurierbar, mit Einbußen beim Durchsatz des Gerätes verbunden. Gerade ältere Modelle beherrschen keine paketbezogene Lastverteilung.

Design-Varianten Lokaler Netzwerke im Vergleich



Ein weiteres Problem ist, dass es dadurch zu unterschiedlichen Laufzeiten von Paketen kommt, die zum selben Datenstrom gehören. Der unterschiedliche Jitter kommt dadurch zustande, dass Pakete derselben Kommunikation auf unterschiedlichen Wegen unterschiedliche Router und Switches durchlaufen. Da Kosten sich zumeist nur an der zur Verfügung stehenden Bandbreite eines Weges orientieren, nicht aber an Geräte-internen Delays oder Auslastungen einzelner Zwischenrouter, kommt es zu unterschiedlichen Verzögerungen von Ende-zu-Ende von verschiedenen Wegen, was dann einen unterschiedlichen Abstand zwischen den Paketen, den Jitter, nach sich zieht. Das kann insbesondere dann zu einem Problem werden, wenn es sich um eine Jitter-sensitive Kommunikation wie Voice oder Video handelt.

In einem LAN mit modernen High-End-Layer-3-Switches sollte das heute nicht zu einem Problem führen, da sowohl das interne Delay vernachlässigt werden kann, insbesondere wenn gleich viele Switches auf allen Wegen durchlaufen werden, als auch bei einem auf Überkapazitäten beruhenden Netzdesign nicht mit langen Warteschlangen in den Geräten zu rechnen ist.

Anders ist das natürlich im WAN-Bereich, wo zum einen langsame Geräte in Form von klassischen Routern zum Einsatz kommen, zum anderen die Warteschlangen an Interfacen länger sind, da die zur Verfügung stehende Bandbreite deutlich geringer ist als im LAN-Bereich.

Noch ein Problem bei der Lastverteilung pro Paket ist, dass Pakete desselben Datenstroms sich auf dem Weg vom Sender zum Empfänger überholen können. Auch das kann bei bestimmten Applikationen zu Problemen führen, die dann durch andere Mechanismen aufgefangen werden müssen. Beispiel dafür sind über ein IP-Netz getunnelte SNA Pakete: hier muss beim Tunnel darauf geachtet werden, dass die richtige Paketreihenfolge am Tunnelausgang vom Router wieder hergestellt wird. Das heute am meisten verbreitete Protokoll ist DLSW; es beinhaltet solch einen Mechanismus, allerdings ist vereinzelt auch noch Remote Source Route Bridging im Einsatz, das bei Paketüberholungen zu einem Fehlverhalten führt.

Verteilung nach Zieladresse

Wird die Lastverteilung pro Zieladresse vorgenommen, so entscheidet der Router ausschließlich anhand der im IP-Header eingetragenen Zieladresse einmalig über den Weg. Erst ein Paket zu einer anderen Zieladresse würde auf einem anderen Weg gleicher Kosten übertragen werden. Das hat zur Konsequenz, dass auch Pakete von verschiedenen Sendern zum selben Ziel aus demselben Interface den Router verlassen. Eine einmal getroffene Zuordnung ist nur für eine bestimmte Zeit gültig. Sind lange keine Pakete mehr für ein bestimmtes Ziel vom Router weitergeleitet worden, timed der Eintrag aus und wird erst wieder neu generiert, wenn erneut ein Paket für dieses Ziel eintrifft.

Vorteil dieses Verfahrens ist, dass es, verglichen mit den weiter unten vorgestellten Verfahren, wenig Prozessoverhead generiert: der Router muss für die Routingentscheidung ohnehin die Zieladresse des IP-Pakete überprüfen, so dass für die Lastverteilung das Paket nicht weiter untersucht werden muss.

Ein weiterer Vorteil ist, dass sich Pakete zumindest theoretisch nicht überholen können. Das gilt allerdings nur, wenn alle Router zwischen Quelle und Ziel dieses Verfahren anwenden. Man sollte sich jedoch nicht darauf verlassen und lieber weitere Verfahren wie DLSW bei SNA Verkehr einsetzen, wenn eine Einhaltung der Reihenfolge gewährleistet sein muss.

Nachteil bei dieser Art der Lastverteilung, ist dass sie nicht zwangsläufig zu einem ausgewogenen Verhältnis der Paketverteilungen auf die möglichen Wege führt. Üb-

licher Weise finden Rechnerkommunkationen zwischen Clients und Servern statt. Meist gibt es Server (z. B. File-Server), mit denen erheblich mehr Daten ausgetauscht werden als mit anderen (z. B. Mail Server). Die Layer-3-Switches im HVT mit Anschluss zum Geländebackbone werden die Pakete bei dieser Art der Lastverteilung gemäß den angesprochenen Servern verteilen, was dazu führen kann, dass große Datenmengen zu einem File-Server entlang eines Weges geroutet werden, während die alternativen Wege nur wenig Daten transportieren, da ihnen zufällig nur die IP-Adressen gering belasteter Server zugeordnet wurden.

Dieses Verfahren ist also insbesondere dann ungeeignet, wenn man wenige Server hat, die ein hohes Lastaufkommen haben. Hat man in seinem Rechenzentrum hingegen sehr viele Server mit gemischtem Lastaufkommen, so kann dieses Verfahren gut zur Lastverteilung genutzt werden.

Verteilung nach Quell- und Zieladresse

Um den Nachteil der ungleichen Verteilung bei ausschließlicher Betrachtung der Zieladresse zu vermeiden, kann auch noch die Adresse des Senders bei der Lastverteilung mit berücksichtigt werden.

Damit wäre bei einer angenommenen Client-zu-Server Kommunikation nicht mehr allein die Adresse des Servers ausschlaggebend, sondern auch die Client-Adresse würde mit in Betracht gezogen. Das hätte zur Folge, dass die Lastverteilung auch wenn die meisten Daten zu einem oder wenigen Servern übermittelt werden, ausgewogener ist. Zumindest gilt das, wenn man davon ausgeht, dass die Daten von unterschiedlichen Clients aus übertragen werden.

Wie bei der Verteilung nach Zieladresse gilt auch hier, dass Pakete sich nicht überholen, wenn das Verfahren durchgängig in einem Netz eingesetzt wird. Allerdings ist es auch hier nicht ratsam, sich darauf zu verlassen, wenn eine strikte Reihenfolge eingehalten werden muss.

Als Nachteil bei der Verteilung nach Quell- und Zieladresse werden häufig so genannte Power-User angeführt, die den Hauptteil der Last generieren. In diesem Fall ist diese Verteilung, wie bei der Verteilung ausschließlich nach Zieladresse, ggf. wieder asymmetrisch. Man sollte sich jedoch fragen, ob man überhaupt Power-User hat und ob diese von der Anzahl her ernstzunehmender Weise zu einem Problem führen können. Wenn ja, so bleibt noch eine weitere Möglichkeit:

Verteilung nach Session

Zusätzlich zu den beiden Adressen im IP-Header werden auch noch die TCP- oder UDP-Portnummern des entsprechenden Layer-4-Headers mit berücksichtigt. Man spricht dann von einer Verteilung nach Session, da die Kombination aus IP-Adresse plus Portnummer einer Session entspricht.
Nachteil dieses Verfahrens ist, dass sehr weit in die Pakete hineingesehen werden muss, da die Portnummern erst nach dem gesamten IP-Header im Layer-4-Header eingetragen werden. Damit ist der Prozessoverhead bei diesem Verfahren am größten. Es ist eine Frage der Softwarearchitektur, ob der Overhead wirklich größer ist, wenn sowieso mit Access-Listen gearbeitet wird, die sich auch auf die Portnummern beziehen.

Ob in einem LAN diese Verteilung wirklich Vorteile gegenüber der Verteilung nach Quell- und Zieladresse bringt, ist fraglich. Hast man einige wenige Power-User so mag dieses Verfahren zu einer besseren Verteilung führen; im Regelfall wird man jedoch keine Unterschiede feststellen können.

Schwerpunktthema

IP-Management: „Achilles Ferse und Umbrella Technologie“

Integrierte Planung ist ein Muss!

Fortsetzung von Seite 1

Markus Holländer ist Competence Center Leiter Backoffice bei der ComConsult Beratung und Planung GmbH. Neben der Leitung des Competence Centers sind seine Hauptaktivitäten Projektleitungen und Konzipierungen im Bereich der Themen IP-Management, Verzeichnisdienste, Messaging und Clientmigrationen. Herr Holländer ist auch für die Entwicklung der Windows Server 2003 Seminare des Competence Centers in Zusammenarbeit mit der ComConsult Akademie verantwortlich und einer der Hauptreferenten. Zu erreichen unter: hollaender@comconsult.com

Hinzu kommt, dass die Exchange-Server innerhalb einer eigenen Domäne betrieben werden. Zwischen den relevanten Domänen bestehen entsprechende Vertrauensstellungen hinsichtlich der Authentifizierung. Im Bereich der NetBIOS Namensauflösung bestanden in der neuen und alten Welt jeweils mehrere WINS-Server (Windows Internet Name Service). Hinzu kam, dass in der alten Welt und insbesondere in der Domäne für Exchange auf diversen Servern – auch auf Domänenkontrollern – die lmhosts-Dateien genutzt wurden. Innerhalb der Definition der lmhosts-Dateien wurden u.a. auch die Einträge „#PRE“ (zur Bereitstellung der Informationen im NetBIOS-Namenscache) und „#DOM“ (zur Identifizierung von Domänenkontrollern) verwendet. Das Problem des Kunden war, dass Outlook Clients nicht auf Postfächer innerhalb der Exchange-Domäne zugreifen konnten. Recht schnell war klar, dass das Problem in der Namensauflösung zu suchen sei. Dies konnte auch nur in der NetBIOS Namensauflösung vorliegen, da ausschließlich mit den Exchange-Servern in der gesonderten Domäne darüber kommuniziert wurde. Die detaillierte Analyse ergab als erstes, dass es Probleme in der Replikation der WINS-Datenbanken gab. Angestrebt war eine sternförmige Topologie, wobei der „zentrale“ WINS-Server in der produktiven Active Directory Domäne positioniert war. Parallel wurde auch festgestellt, dass die lmhosts-Dateien in der alten Welt teilweise andere Einträge hatten als die WINS-Server dieser Domänen. Nachdem die Replikation im WINS-Umfeld korrigiert und die Inkonsistenz in diesem Bereich aufgehoben war, wurden die lmhosts-Dateien angepasst. Dabei wurden sämtliche Einträge entfernt, die durch WINS aufgelöst werden konnten. Dies führte auch dazu, dass nicht beide Verfahren gepflegt werden müssen. Ferner wurde darauf geachtet, dass in WINS nur absolut notwendige statische Einträge vorlagen und die gesamte Welt so dynamisch wie möglich arbeitete. Abschließend wurden die lmhosts-Dateien der Exchange-Domä-

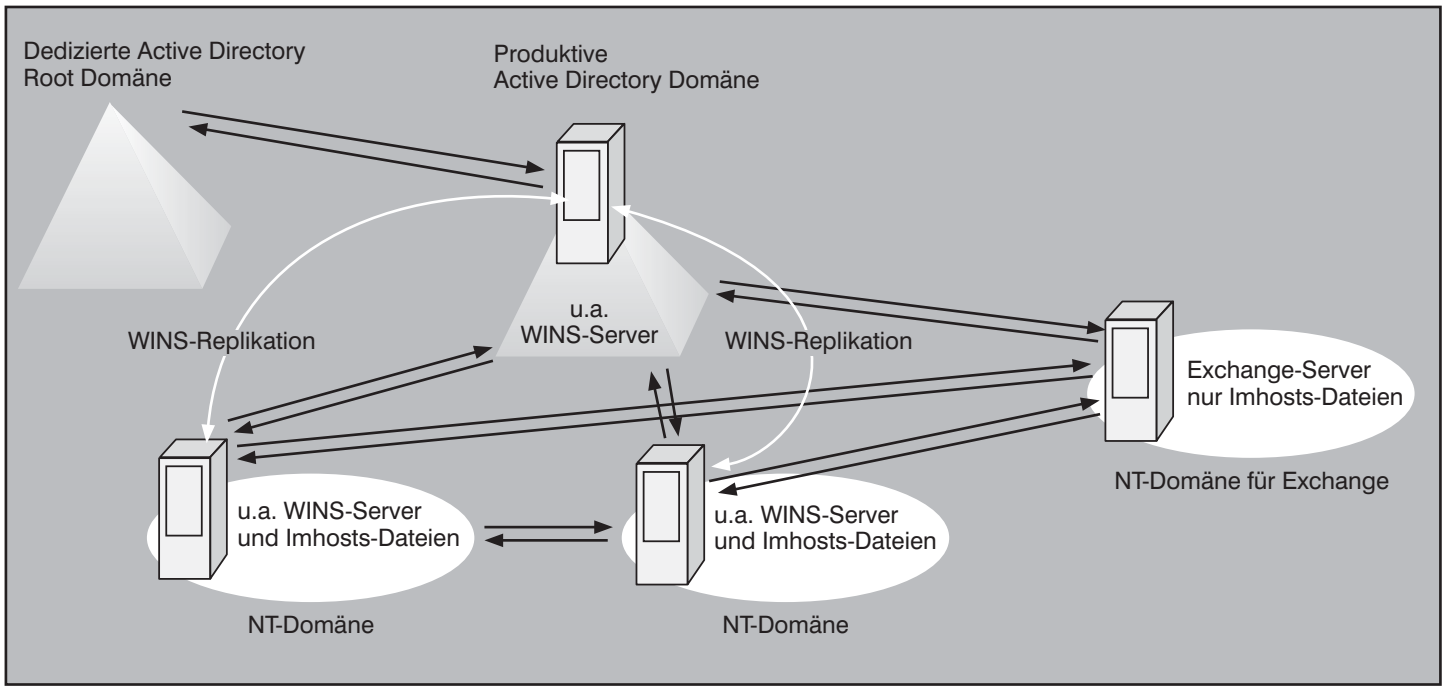


Abbildung 1: Szenario 1 Support

ne analysiert und Inkonsistenzen mit der bereinigten Landschaft behoben. Die Lösung des Problems lag im letzten Schritt. Ggf. hätte es ausgereicht, nur die lmhosts-Einträge innerhalb der Exchange-Domäne zu korrigieren, doch um überhaupt eine strukturierte Fehlersuche betreiben zu können, mussten die grob beschriebenen Schritte durchgeführt werden. Im Rahmen dieses Artikels kann sicherlich keine detaillierte Beschreibung erfolgen, doch sei noch ein Detail nachgeschoben: Es trat auch der Fehler auf, dass Namensabfragen falsch aufgelöst wurden, obwohl der WINS-Server die richtige Antwort kannte. Dies lag daran, dass lmhosts-Dateien inkl. #PRE-Eintrag genutzt wurden. Die Hybrid-Clients nutzten somit den Eintrag im NetBIOS-Namenscache, der durch den #PRE-Eintrag erzeugt wurde und kamen erst gar nicht bis zur WINS-Anfrage. (siehe Abbildung 1)

Im zweiten Szenario lag der Fall vor, dass eine Kunde das Active Directory implementiert hat, ohne eine ausreichende Abstimmung zwischen der Active Directory Gruppe und der Netzwerkbetreibergruppe – insbesondere für DNS – durchzuführen. Diese Situation, die auch oft aus politischen Gründen herbeigeführt wird, taucht doch das ein oder andere Mal in heutigen IT-Abteilungen auf. Das Problem für den Kunden lag dann in falschen Konfigurationen in beiden Welten und führte zu nicht unerheblichen Aufwänden hinsichtlich der Korrektur. Dieses Beispiel, welches nicht näher betrachtet wird, zeigt, dass neben technischen Problemen auch die Politik eine Rolle spielen kann.

Beide geschilderten Szenarien verdeutlichen bereits, dass das IP-Management elementare Grundlagen liefert, dass zumindest für gewisse Szenarien eine Dynamik von Vorteil ist und dass auch die interne Unternehmenspolitik sehr negativen Einfluss haben kann. All dies sind Gründe, um sich mit der Thematik immer wieder zu beschäftigen, jedoch sind es sicher nicht die einzigen, sondern es kommen auch neue Anforderungen hinzu. Bevor jedoch auf diese Anforderungen eingegangen wird, eine kurze Definition, was im Rahmen dieses Artikels unter IP-Management verstanden wird.

Elementares

Die elementarsten Funktionen und die Motivation der drei wichtigen Dienste im IP-Management werden folgend noch einmal in Erinnerung gerufen: DHCP: TCP/IP (Transmission Control Protocol / Internet Protocol) ist weltweit die bevorzugte Netzwerkprotokollfamilie, die in den öffentlichen (Internet) und privaten (Intranet, LAN) Computernetzwerken Verwendung findet. Jedem Host, der über dieses Protokoll kommuniziert, muss eine eindeutige IP-Adresse zugewiesen werden, so dass von diesem Host aus mit anderen Instanzen im lokalen und in anderen Netzwerken kommuniziert werden kann. Mit Hilfe von DHCP, einem offenen Industriestandard (z.B. RFC [Requests for Comment)] 2131 „Dynamic Host Configuration Protocol“ und RFC 2132 „DHCP Options and BOOTP Vendor Extensions“ bei Windows 2000), der die Komplexität der Verwaltung von TCP/IP-basierten Netzwerken reduziert, ist eine dynamische Zuweisung und Aktualisierung der Adressen aus einem vorher definierten IP-Adressbereich möglich. Den Administratoren bleibt es erspart, auf sämtlichen Clients die IP-Adressen manuell zu konfigurieren. Natürlich kann man aber auch mit DHCP statische Adressen zuweisen. Weitere Kommunikationseinstellungen, wie z.B. das Standardgateway, sowie die Subnetzmaske und weitere definierbare Parameter, können über den DHCP-Dienst den Clients zugewiesen werden.
DNS: DNS ist einer der wichtigsten Dienste im Internet sowie in fast allen Unternehmensnetzen. DNS erleichtert die IP-Kommunikation, indem die Benutzer nicht die schwer zu merkende IP-Adresse eingeben, sondern so genannte „Friendly-Names“, die aus Buchstaben, Zahlen und dem Bindestrich „-“ als Sonderzeichen aufgebaut sein können (gilt z.Z. im Internet; je nach DNS-Implementierung können im Intranet jedoch auch verschiedene Zeichensätze verwendet werden, die zusätzliche Sonderzeichen enthalten, z.B. den „_“). Ebenfalls löst DNS auch IP-Adressen zu Namen auf (Reverse Lookup). Grundsätzlich teilt sich DNS in verschiedene Namensräume hierarchisch auf. Eine Alternative oder ggf. ein Zusatz im Bereich der DNS-Namen ist die Verwendung von so genannten „hosts-Dateien“, die textdateibasiert die elementarsten Funktionen bietet.

NetBIOS-Namensauflösung: Für die NetBIOS-Namensauflösung steht auch die Alternative mittels einer textbasierten Datei „lmhosts“ zur Verfügung, doch erfolgt in sehr vielen Fällen die Verwaltung mittels WINS (Windows Internet Name Service). Dieser Dienst ist ein weiterer Namensdienst, der in Windows-NT-Umgebungen eingesetzt wird. Ähnlich wie DNS wird WINS dazu verwendet, Namen in IP-Adressen aufzulösen – allerdings dient DNS der Auflösung von Host-Namen (FQDN - Fully Qualified Domain Name, z.B. server.comconsult.com oder www.comconsult.com), während mit Hilfe von WINS NetBIOS-Namen aufgelöst werden. Bei WINS ist zu beachten, dass von Beginn an bereits die Dynamik im Vordergrund stand. Es ist zwar

möglich, statische Einträge zur erstellen und somit auch zu nutzen, doch ist es in der Regel so, dass sich die Clients dynamisch registrieren.

Zusammengefasst kann also definiert werden, dass DHCP zur Verteilung von IP-Adressen (dynamisch/statisch) inkl. IP-Konfigurationsparameter und DNS sowie WINS zur Namensauflösung genutzt werden. Dies sind jedoch nur die elementarsten Funktionen. Allerdings zeigen nicht nur die Eingangsbeispiele, dass es in diesen Bereichen schon Probleme gibt. Eine weitere wichtige Funktion in den Bereichen DNS und WINS ist die Bereitstellung von Informationen zum Auffinden von Diensten. Im WINS-Umfeld sind dies insbesondere die Einträge für die Domäne (bzw. die Domänenkontroller – der so genannte 1C-Eintrag) und den Computersuchdienst für Windows (1B-Eintrag). Bei DNS existieren so genannte SRV-Records (Service-Records), die es erlauben, einen Dienst zu lokalisieren. Auf diese Thematik wird im weiteren Verlauf noch näher eingegangen. An dieser Stelle kann jedoch festgehalten werden, dass das IP-Management, sowie bis jetzt bereits beschrieben, ein wesentlicher Teil des Fundaments einer IT-Infrastruktur ist (siehe Abbildung 2). Ist dieses Fundament nicht bzw. nicht richtig funktionsfähig vorhanden, dann könnte sich die IT-Infrastruktur entsprechend Abbildung 3 darstellen.

Weitere Anforderungen

In heutigen IT-Umgebungen kommen aber weitere Anforderungen auf das IP-Management zu. Hierbei sind in erster Linie Themen im DNS zu nennen, insbesondere nachdem Microsoft ab der Version Windows 2000 hinsichtlich der Namensauflösung einen wesentlichen Strategiewechsel von WINS hin zu DNS als primären Dienst zur Namensauflösung (sowie weiterer Funktionalitäten) vollzogen hat. Das erste Thema im Bereich dieser Anforderungen ist die dynamische Aktualisierung bzw. das dynamische DNS (DDNS). Mit DNS auf Basis von Windows NT wurde kein DDNS unterstützt. Allerdings gab und gibt es eine Reihe von IP-Management-Tools, wie z.B. Vital QIP von Lucent, die diese Funktionalität schon seit Jahren zur Verfügung stellen. Es ist jedoch so, dass Microsoft mit dem genannten Strategiewechsel hin zu DNS andere Anforderungen an das IP-Management geschaffen hat. Hierzu zählt auch die Unterstützung der dynamischen Aktualisierung. Seit Windows 2000 wird DDNS auch bei Microsoft unterstützt, so dass geeignete DHCP-Server (oder auch Clientrechner mit Windows 2000 oder XP) im DNS die Einträge automatisiert aktualisieren können. Der DHCP-Server oder Client kann, je nach Konfiguration, sowohl die Forward-Einträge (A-Records, Auflösung des Computernamens in eine IP-Adresse) als auch die Reverse-Einträge (PTR-Records, Auflösung der IP-Adresse in einen Computernamen) im DNS veranlassen. Die dynamische Registrierung verläuft bei Windows 2000/XP Clients standardmäßig anders als bei älteren Windows-Clients oder anderen Clients. Windows 2000/XP Clients führen die dynamische Aktualisierung der A-Namen (Host-Namen) selbsttätig am Windows 2000 bzw. Windows Server 2003 DNS-Server direkt nach der IP-Lease-Bestätigung durch. Der DHCP-Server führt die dynamische Aktualisierung des PTR-Eintrages durch. Die dynamische Aktualisierung des PTR-Eintrages wird vom Client beim DHCP-Server beantragt (Option 81). Unterstützt der DHCP-Server diese Option nicht, aktualisiert der Client den Eintrag selbstständig. Dies gilt auch bei manueller Konfiguration des TCP/IP auf dem Client. Bei anderen Betriebsystemen außer Windows 2000/XP erfolgt wie bereits oben beschrieben die Lease-Anforderung und Lease-Bestätigung über den DHCP-Server, der dann anschließend die dynamische Aktualisierung des A-Namens und des PTR-Eintrages für die Clients im DNS veranlasst. Grundsätzlich kann festgehalten werden, dass mit dem DDNS auch die Dynamik in dieser Form der Namensauflösung Einzug gehalten hat. Im Gegensatz zu NetBIOS bzw. WINS kann jedoch die erforderliche Kommunikation serverbasiert (DHCP und DNS) erfolgen. Wird das Active Directory als Verzeichnisdienst genutzt oder ist dieses geplant, dann ist die Nut-

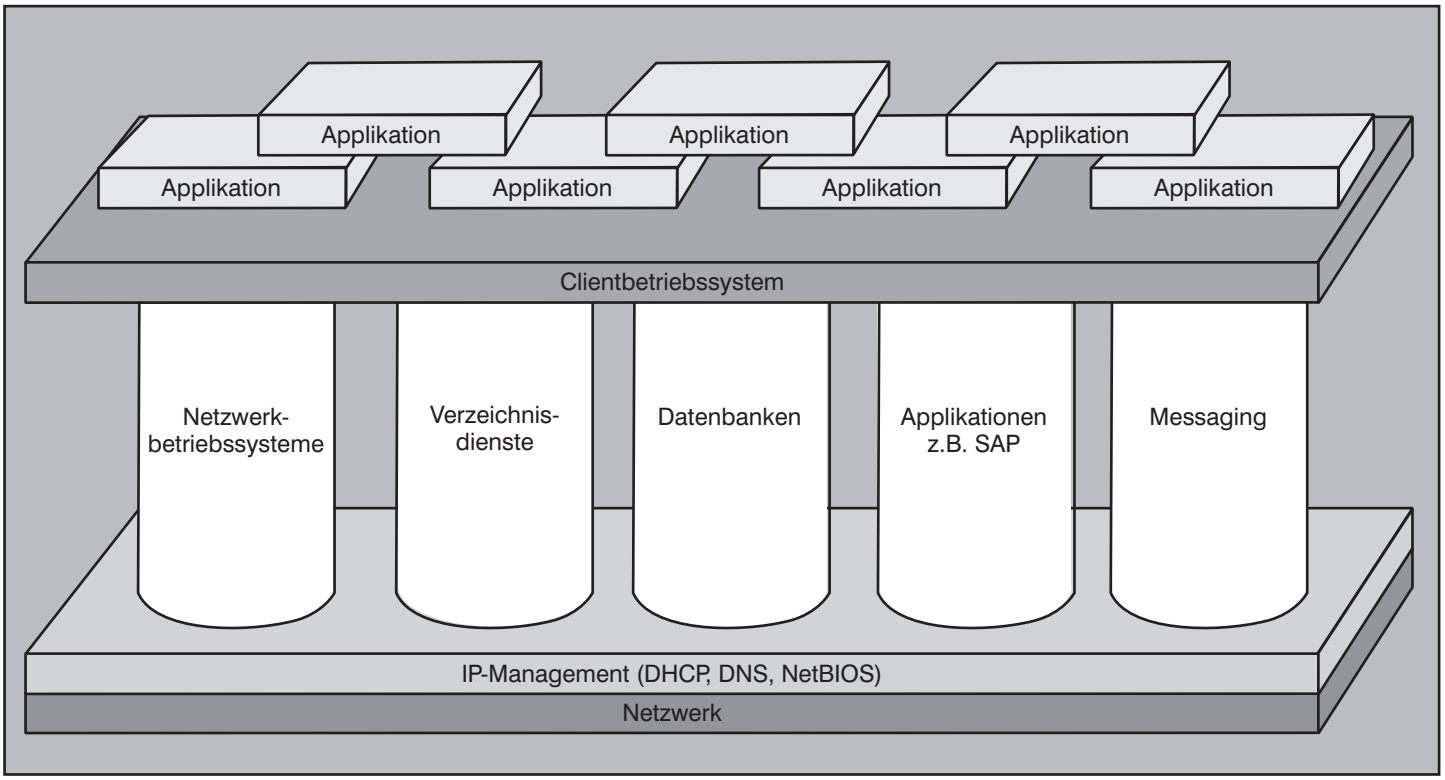


Abbildung 2: IP-Management eine Grundlage der IT-Infrastruktur

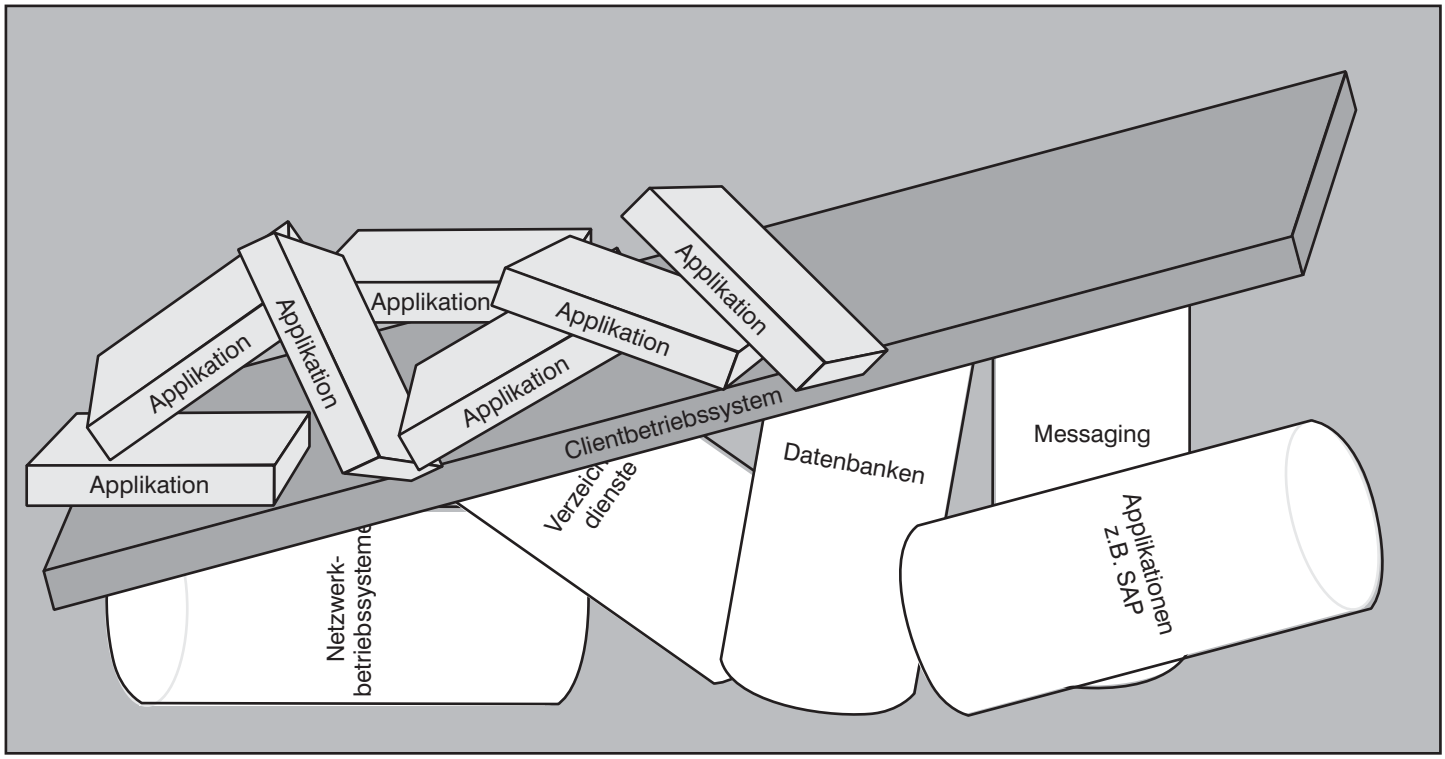


Abbildung 3: IT-Infrastruktur ohne IP-Management-Basis

zung des DDNS eigentlich unumgänglich, auch wenn theoretisch die Möglichkeit besteht, dies ohne Dynamik zu machen. Insgesamt wird die enge Bindung zwischen DNS und Active Directory in vielen Bereichen sichtbar, ein weiterer Punkt hierbei ist die sichere dynamische Aktualisierung mit dem Microsoft DNS-Server unter Windows 2000 bzw. Server 2003. Werden die Zoneninformationen des DNS im Active Directory Verzeichnisdienst gespeichert, dann kann diese sichere Aktualisierung implementiert werden. Dabei kann über eine Zugriffsliste (ACL – Access Control List) der Zone angegeben werden, welche Benutzer oder Computer Einträge in der Zone hinzufügen oder ändern können. In der Standardeinstellung können alle Mitglieder der Gruppe „Authentifizierte Benutzer“ Einträge erstellen. Durch die Verwendung der sicheren dynamischen Aktualisierung kann verhindert werden, dass „beliebige“ Systeme Änderungen im DNS durchführen. Außerdem kann verhindert werden, dass ein Host den Eintrag eines anderen Hosts ändert (jeder kann nur seinen eigenen DNS Record überschreiben). Dies ist für ein dynamisches System von entscheidendem Vorteil, da somit Fehlkonfigurationen minimiert werden.

Eine weitere Anforderung an die DNS-Implementierung ist die Unterstützung der bereits erwähnten SRV-Records. Grundsätzlich ermöglicht diese DNS-Abfrage das Auffinden eines oder mehrerer Server, die einen ähnlichen TCP/IP-Dienst anbieten. Derzeit wird diese Form der Einträge in der Hauptsache von so genannten „LDAP-Servern“ genutzt, wobei auch weitere Dienste wie z.B. http, ftp oder Kerberos diese Einträge nutzen können. Auch für diese Art der DNS-Einträge ist das Active Directory wieder der exzessivste Nutzer. Für das Active Directory stellt das DNS mittels dieser Einträge z.B. Informationen zum Auffinden von Domänenkontrollern zur Verfügung. Die SRV-Records werden ausführlich im Artikel „Active Directory und DNS, eine Welt“ im Netzwerk Insider vom August 2001 für Windows 2000 (Active Directory Version 1) erläutert.

Hinsichtlich der neuen Ansprüche an das DNS sind die gestiegenen Anforderungen an das Design der DNS-Implementierung natürlich ebenso wichtig, wie die neuen Funktionalitäten. An dieser Stelle werden nur einige Schlagwörter genannt, die im Kontext dieser Anforderungen zu betrachten sind: Interne DNS-Root, Conditional Forwarders und Stub Zones. Hinzu kommen erhöhte Anforderungen hinsichtlich der Verfügbarkeit und Flexibilität (Multi Master Replikation). Fasst man diesen Themenkomplex zusammen, dann ist festzuhalten, dass eine Reihe von Anforderungen an Gewicht gewonnen haben.

KO-Kriterien

Aber was sind die KO-Kriterien, die zu beachten sind? Dies kann natürlich nicht pauschal beantwortet werden und hängt entscheidend von den Diensten und Applikationen ab, die im jeweiligen Unternehmen vorhanden sind. Betrachtet man zwei immer wieder aktuelle Themen, dann kristallisiert sich jedoch ein Thema heraus. Möchte man eine dynamische Serverkonsolidierung durchführen, dann muss auch das IP-Management den Anforderungen dieser Dynamik entsprechen.

Dieser Anforderung wird nicht entsprochen, wenn auch nur eine der folgenden Situationen vorliegt:

1. manuelle Client-IP-Konfiguration (DHCP?),
2. statische Implementierungen auf Basis von lmhosts- oder host-Dateien (DNS,WINS?),
3. statische Einträge im WINS-Server-Umfeld,
4. keine Unterstützung bzw. Implementierung von DDNS, sondern manuelle Pflege.

Das andere Thema ist die Daten- und Funktionsverlagerung. Ähnlich der dynamischen Serverkonsolidierung ist auch hier Dynamik gefordert. Allerdings ist dies je nach Szenario noch wesentlich zeitkri-

tischer. Folgende Anhaltspunkte skizzieren wesentliche Rahmenparameter: Konfigurationsänderungen müssen schnell in der Landschaft repliziert werden (Beispiel: IP-Adresse für einen Applikationsserver muss geändert werden, es greifen aber alle Standorte und somit auch alle Clients darauf zu.), es muss durchgängig ein zentrales Management implementiert sein, ändern sich Anmeldeserver, so muss gewährleistet sein, dass diese auch angesprochen werden können (Service Records bei DNS, NetBIOS 1B und 1C Einträge), ändern sich Nameserver, dann muss das Design Redundanzen aufweisen. Wie diese beiden Szenarien, die Eingangsbeispiele und auch die bereits gemachten Ausführungen zum Active Directory zeigen, ist in vielen Fällen das globale KO-Kriterium die Dynamik! Dabei ist natürlich immer der Einzelfall zu betrachten, doch ist es in vielen Fällen tatsächlich so. Fasst man an dieser Stelle zusammen, dann ist festzuhalten, dass viele Dienste und Applikationen ein funktionierendes und meist dynamisches IP-Management als elementare Basis erfordern. Aber bleibt noch die Frage, warum es noch als Umbrella Technologie zu bezeichnen ist.

Umbrella Technologie

Zur Umbrella Technologie wird das IP-Management, weil es für sämtliche Plattenformen zur Verfügung gestellt werden muss (UNIX, LINUX, Windows, …), auf sämtlichen Plattformen betrieben werden kann, für sämtliche Komponenten von Bedeutung ist (Server, Clients, Speicher [z.B. NAS], aktive Komponenten, IP-Telefonie, …) und für sehr viele Dienste/Applikationen letztendlich eine Plattform liefert! Dies gilt in erster Linie für die Dienste DHCP und DNS. Hierbei sind auch mehrstufige Abhängigkeiten zu beachten. Ein Beispiel für diese mehrstufige Abhängigkeit ist die Standardisierung auf Basis von Windows XP. Zur Standardisierung im XP-Umfeld sind Gruppenrichtlinien (GPO – Group Policy Objects) ein Mittel zur Schaffung der erforderlichen Rahmenparameter. Gruppenrichtlinien wiederum können vollständig nur in Verbindung mit dem Active Directory genutzt werden und das Active Directory kann nur basierend auf DNS also dem IP-Management implementiert werden.

Die Thematik NetBIOS bzw. WINS ist im Kontext der Umbrella Technologie genauer zu betrachten. Eigentlich betrifft sie im Gegensatz zu DHCP und DNS meist nur den Microsoft-Teil der IT-Umgebungen in den Unternehmen, sollte jedoch im Sinne einer Teilmenge des Ganzen betrachtet werden. Je nachdem wie Microsoft-lastig die IT-Umgebungen sind, ist dies oft auch noch der größte Teil. In diesem Kontext muss man immer auch noch berücksichtigen, dass für viele Applikationen bis hin zu Microsoft eigenen Tools eine vorhandene NetBIOS-Namensauflösung mindestens von Vorteil oder sogar absolut erforderlich ist. In aktuellen Konzepten wird diesem Thema immer noch entscheidende Bedeutung zugemessen, auch wenn der primäre Dienst bei der Namensauflösung sicherlich DNS ist. Folgt man dieser Argumentationskette und ordnet auch die NetBIOS-Namensauflösung dem IP-Management als Umbrella Technologie zu, stellt sich als nächstes die Frage, wie die Vielfältigkeit dieser Technologie und die Anforderungen und Techniken in Einklang gebracht werden können. Dieses alles erfordert eine integrierte Planung, die alle Aspekte berücksichtigt.

Integrierte Planung

Bei der integrierten Planung stehen folgende Fragen bei den Vorüberlegungen bzw. beim Entwurf der globalen Strategie im Vordergrund: In erster Linie, welche Plattformen stehen zur Verfügung und welche Plattformen müssen bedient werden (ganz im Sinne der Umbrella Technologie)? Welche Verzeichnisdienste sind ggf. zu berücksichtigen? Welche Datenbanken stehen ggf. zur Verfügung? Welche weiteren Rahmenparameter der einzelnen Unternehmung sind zu berücksichtigen? Zur letzten Frage könnten z.B. die Antworten lauten, dass bereits ein IP-Management-Tool im Unternehmen etabliert ist oder dass ein Produkt auf Grund einer strategischen Partnerschaft gesetzt ist. Um diese integrierte Planung transparenter zu machen, wird im Folgenden die integrierte Planung des IP-Managements mit dem Active Directory beschrieben.

(*Kommentar des Autors: Es ist mir bewusst, dass einige Leser dieses Artikels aufgrund dieses Beispiels die Microsoftlastigkeit bemängeln werden, doch zeigt genau dieses Beispiel am besten die erforderliche integrierte Planung und die gegenseitigen Abhängigkeiten*.)

Folgende Rahmenparameter liegen dem Beispielszenario zu Grunde: Der fiktive Konzern besteht aus 2 Unternehmen. Die Clientlandschaft besteht fast ausschließlich aus Microsoft-Clients - ca. 4.000 (in der Hauptsache auf Basis von Windows NT und ein Teil auf Basis von Windows 2000 und XP), jedoch sind auch ein paar LINUX-Clients vorhanden. Die Serverlandschaft besteht zum einen aus Windows-Servern und zum anderen aus einigen UNIX- und LINUX-Servern. Aktuell werden in beiden Unternehmen diverse Windows NT-Domänen verwaltet und das IP-Management ist jeweils auf Basis der Microsoft-Dienste unter NT 4.0 implementiert. Als strategischer Verzeichnisdienst ist das Active Directory

IP-Management: „Achilles Ferse und Umbrella Technologie“

Version 2 (Windows Server 2003) vorgegeben. Dieses soll im Rahmen eines Projekts mit zentralem Ansatz, jedoch auch mit dezentraler Verwaltung implementiert werden.

DNS

Im Rahmen der integrierten Planung des Active Directory und des IP-Managements - insbesondere DNS - stellt sich als erstes die Frage, welche gegenseitigen Abhängigkeiten bestehen. Eine grundlegende Voraussetzung für das Active Directory ist, dass zu den einzelnen Active Directory Domänen gleichnamige DNS-Domänen vorhanden sein müssen. Insofern haben Design-Entscheidungen aus dem Active Directory direkten Einfluss auf das DNS-Design. An dieser Stelle stellt sich meist auch schon direkt die politische Frage, wer diese Domänen im DNS verwaltet. Geht es nach den Personen, die das Active Directory konzipieren, so wird eine Integration in deren Administrationshoheit favorisiert. Existiert eine eigene Abteilung für das Netzwerk, die auch das IP-Management administriert, wird dies meistens ganz anders gesehen. Welche Wahl die Richtige ist, bestimmen neben der Politik die Voraussetzungen, die im Unternehmen vorhanden sind. Es ist auch – eine entsprechende Konzipierung vorausgesetzt - ohne Probleme möglich, die Verwaltung der vom Active Directory benötigten Domänen ohne die Nutzung der Microsoft-Dienste zu implementieren. Letztendlich müssen die Schnittstellen definiert werden und die IP-Management-Implementierung muss natürlich die Anforderungen des Active Directory (SRV-Records, dynamische Aktualisierung etc.) unterstützen. Insofern könnte auch die Administration im Bereich der Netzwerk-Abteilung liegen. In solchen Szenarien ist somit auf alle Fälle auch die Netzwerk-Abteilung in die Active Directory Konzipierung entsprechend zu involvieren (siehe zweites Eingangsbeispiel). Grundsätzlich ist eine Aufteilung der DNS-Verwaltung nicht zu favorisieren, da dann mit Sicherheit Kompetenzgerangel zu erwarten ist. Aber zurück zum Beispielszenario: Da hier das IP-Management bereits auf Basis von Windows NT implementiert ist, bietet es sich an, auch die „neue Welt“ auf Basis der Windows-Dienste zu implementieren. Die erste Entscheidung im Rahmen der Active Directory Konzipierung ist, wie viele Gesamtstrukturen (forests, Wälder) bzw. wie viele Active Directory Root Domänen (nicht zu verwechseln mit der DNS Root Domänen) benötigt werden.

Hierbei sind die entscheidenden Kriterien:

1. Pro Gesamtstruktur gibt es ein Schema zur Definition von Objektklassen und Attributen.
2. Pro Gesamtstruktur existiert genau ein so genannter „Configuration Naming Context“ mit Informationen über die gesamte Infrastruktur (Domänen, Standorte, Standortverbindungen ...), der an alle Domänenkontroller inner halb der Gesamtstruktur repliziert wird.
3. Pro Gesamtstruktur existiert ein „Global Catalog“ mit ausgewählten Attributen.
4. Vertrauensstellungen innerhalb einer Gesamtstruktur werden automatisch (dcpromo-Prozess), transitiv und bidirektional angelegt.
5. Pro Gesamtstruktur kann nur genau eine Exchange 2000(3) Organisation integriert werden. (Für Exchange ist somit der Forest das entscheidende Kriterium!).

Meist ist die entscheidende Frage in wieweit sich ggf. Tochtergesellschaften oder weitere Standorte – insbesondere mit eigener IT-Verwaltung – integrieren lassen, denn für diese bedeutet dies den Verlust der absoluten Administrationshoheit. Neben den genannten Kriterien spielen technische Rahmenparameter wie z.B. die Anzahl der Benutzer oder Computer nur in sehr großen Unternehmen eine Rolle. Im Beispielszenario wurde sich für eine Gesamtstruktur entschieden, da alle Parameter passen und auch ggf. weitere Standorte zu integrieren sind. Auch wird mit der Implementierung einer Gesamtstruktur im Sinne einer zentralisierten Administration die beste Grundlage geschaffen. Für DNS lassen sich aus dieser für das Active Directory Konzept sicher sehr wichtigen Entscheidung noch wenige Rückschlüsse ziehen. Die Verwendung einer Gesamtstruktur gewährleistet nämlich nicht, dass nur ein Namensraum benötigt wird. Innerhalb einer Gesamtstruktur können verschiedene DNS-Namensräume integriert werden. Dies erfolgt durch die so genannten Active Directory Peer Domänen. Viel wichtiger für DNS sind die Entscheidungen, die im nächsten Schritt bei der Active Directory Konzipierung getroffen werden. An dieser Stelle wird die Anzahl der benötigten Domänen innerhalb der Gesamtstruktur definiert.

Bei der Definition der benötigen Domänen sollte immer zuerst das Modell mit nur einer (produktiven) Domäne geprüft werden.
Bei der Verwendung einer Domäne existieren folgende Vorteile:

1. Im Sinne eines zentralen Administrationsansatzes bietet dieses Modell die effizienteste Grundlage, selbst wenn mehrere Verwaltungspunkte bestehen sollen, da Administrationsdelegierungen durchgeführt werden können.
2. Die Authentifizierung erfolgt immer innerhalb einer Domäne, so dass jeder DC authentifizieren kann.
3. Der höchste Verwaltungspunkt für Gruppenrichtlinien zur Implementierung von Vorgaben und Einschränkungen für Benutzer und Computer ist die Domäne.
4. Eine einheitliche Sicherheitspolitik ist „leicht“ zu implementieren (z.B. Kennwort-Richtlinien). Allerdings muss hierbei erwähnt werden, dass für die Kontenrichtlinien auch nur ein Gruppenrichtliniensatz implementiert werden kann (siehe auch Nachteile).
5. Alle freigegebenen Ressourcen sind „leicht“ zu adressieren.
6. Der Aufwand für Hard- und Software ist im Vergleich zu mehreren Domänen geringer, da die Integration - die Implementierung einer entsprechenden Verfügbarkeit vorausgesetzt – von weniger Domänenkontrollern erforderlich ist, als bei Modellen mit mehreren Domänen.
7. Im Gegensatz zu NT sind mittels der so genannten Organisationseinheiten auch Strukturen innerhalb einer Domäne implementierbar – und dies wesentlich flexibler als mit mehreren Domänen.

Dieses Modell hat allerdings auch Nachteile:

1. Es sind keine unterschiedlichen Kontenrichtlinien (Kennwortlänge, -komplexität, alter etc.) implementierbar. Sollten unterschiedliche Kontenrichtlinien erforderlich sein, so ist dies meist der einzige technische Grund, warum mehrere Domänen konzipiert werden müssen.

2. Ausscheidende Unternehmensteilemüssen eine neue Struktur aufbauen (auch bei Gesamtstruktur). Dieser Punkt wird allerdings meist aus Sicht der konzipierenden Unternehmen vernachlässigt.

3. Oft ist es (sehr) fraglich, ob dies politisch durchsetzbar ist, da natürlich untergeordnete Administrationsbereiche, z.B. weitere Standorte, weitere Teile der Administrationshoheit (in Ergänzung zum Verlust durch eine Gesamtstruktur) verlieren. Insbesondere empfiehlt es sich, die Verwaltung der Domänenkontroller zu zentralisieren.

Weitere Parameter können nicht eindeutig als Vor- oder Nachteil gewertet werden, doch ist es in den meisten Fällen auch so,

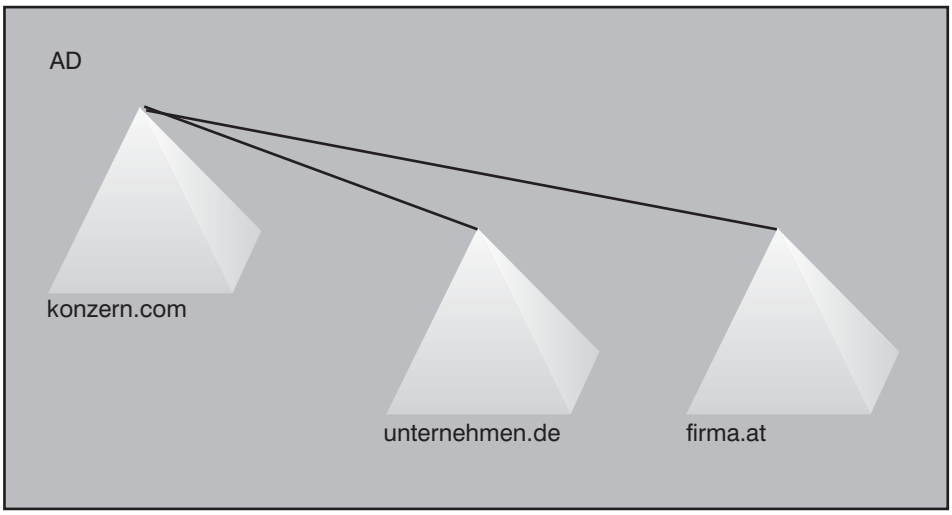


Abbildung 4: Gesamtstruktur und Domänen des Beispielszenarios

dass die Anzahl der Objekte innerhalb einer Domäne völlig ausreichen und dass nicht das Active Directory Anpassungen in der WAN-Struktur erfordert. Hierfür sind in der Regel andere Dienste verantwortlich. Betrachtet man jetzt das Beispielszenario, dann könnte tatsächlich die Implementierung von nur einer Domäne erforderlich sein. Ist jedoch angedacht, dass sich die beiden Unternehmen im Namensraum bzw. in der Benennung der Domäne unterscheiden, dann sind 2 (produktive) Domänen erforderlich. Für das Beispiel wird dieses angenommen. Anschließend stellt sich in der Regel noch die Frage, ob eine so genannte „dedizierte Active Directory Root Domäne“ implementiert wird. Dies wird im Rahmen dieses Artikels nicht näher betrachtet. Doch da die Implementierung einer solchen Root Domäne erhöhte Sicherheitsanforderungen erfüllt und insbesondere das Höchstmaß an Flexibilität gewährleistet, wird dies für das Beispielszenario angenommen. Mit fiktiven Namen versehen könnte sich die Gesamtstruktur für das Beispielszenario entsprechend Abbildung 4 darstellen.

Zu diesem Zeitpunkt sind die ersten Anforderungen an das DNS-Design definiert. Für das Beispielszenario werden somit 3 Domänen für die Namensräume konzern.com, unternehmen.de und firma.at. benötigt. Im Rahmen der integrierten Planung zu DNS stellt sich anschließend die Frage, ob und wenn ja wie das in bestehende Welten integriert werden kann. Am Anfang zu diesem Beispielszenario wurde ja bereits die politische Frage nach der Verwaltung der Domänen gestellt. Da aber für das Szenario entschieden wurde, dass die Verwaltung innerhalb der Microsoft-Welt erfolgt, stellt sich die Frage, ob für die anderen Betriebssysteme UNIX und LINUX weitere Namensräume berücksichtigt werden müssen oder ob diese Systeme in die definierten Namensräume integriert werden. Wird die Nutzung der Microsoft-Dienste konzipiert und implementiert, ist es in Projekten meist der Fall, dass diese Systeme jeweils zuerst in ihrem Namensraum bleiben und diese Namensräume in das DNS-Konzept integriert werden. Erst nach Abschluss der Einführung des Active Directory werden diese Systeme dann schrittweise (ggf. pro Server und/oder Dienst) in die „neuen“ Namensräume mi-

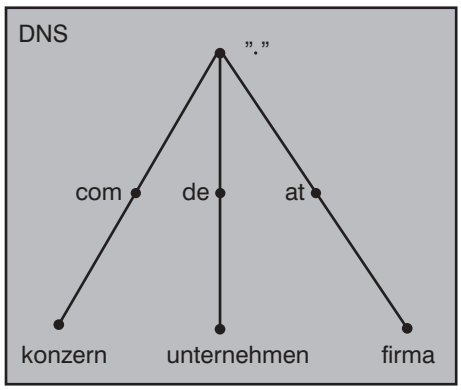


Abbildung 5: DNS Design des Beispielszenarios

griert (siehe auch Beispiel zur Dynamik). Für das Beispielszenario wird vom „best case“ ausgegangen und die Integration kann direkt in die vom Active Directory definierten Namensräume erfolgen. Entsprechend stellt sich die DNS-Struktur gemäß Abbildung 5 dar. In der Darstellung wurden auch die DNS-Root-Domäne sowie die Top-Level-Domänen (.com, .de, at) berücksichtigt.

Noch einmal der Hinweis: Aus Sicht des Active Directory bestehen natürlich die definierten Anforderungen hinsichtlich der (sicheren) dynamischen Aktualisierung und insbesondere der SRV-Records. Aber zurück zu DNS: Im nächsten Schritt ist zu prüfen, ob eine interne DNS-Root ver-

wendet wird. Wenn diese implementiert wird, dann geschieht dies meist aus dem Grund, dass die internen Namensräume völlig gegenüber dem Internet abgeschottet werden. Dies sollte allerdings nur dann erfolgen, wenn der Zugriff auf das Internet auf die proxyfähigen Dienste (z.B. http) beschränkt werden kann und wenn die Clients, die auch für nicht proxyfähige Dienste einen Internetzugriff benötigen, nicht auf zu viele Domänen zugreifen müssen. Für diese Clients können dann nämlich Techniken wie Condtional Forwarders oder Stub Zones eingesetzt werden. Werden diese Techniken benötigt, so erhöhen sich wiederum die Anforderungen an die DNS-Implementierung. Für Stub Zones ist nämlich beispielsweise mindestens Windows Server 2003 DNS oder alternativ BIND 9 erforderlich.

Völlige Integration

Betrachtet man wiederum das Beispielszenario, dann bestünde eine völlige Integration darin, dass Active Directory integrierte Zonen genutzt würden. Wird eine Verwendung festgelegt, dann generiert DNS somit Anforderungen an das Active Directory Konzept. Grundsätzlich sind folgende Parameter mit der Implementierung von Active Directory integrierten Zonen verbunden: Die Zonen inkl. Ihrer Einträge werden als Active Directory Objekte gespeichert und mit den Replikationsmechanismen des Active Directory repliziert. Hierbei stehen je nach Typ der Active Directory Zone entsprechende Optionen zur Verfügung. Zu beachten ist aber, dass der DNS-Server auf einem Domänencontroller ausgeführt werden muss. Besonders wichtig ist, dass die Verwendung der sicheren dynamischen Aktualisierung nur in Verbindung mit Active Directory integrierten Zonen erfolgen kann. Natürlich können auf anderen DNS-Servern Active Directory integrierte Zonen auch als sekundäre Zone und Stubzone gespeichert werden. Dies ist insbesondere von Bedeutung, wenn verschiedene Implementierungen parallel betrieben werden, sei es auch nur für eine Migrationsphase. In diesem Fall muss jedoch bereits bei der Planung der Namenskonventionen die Kompatibilität mit anderen DNS Implementierungen beachtet werden (RFC 1123). Ein entscheidender Vorteil Active Directory integrierter Zonen muss noch besonders herausgestellt werden: Bei Active Directory integrierten Zonen handelt es sich um primäre Zonen, das bedeutet, dass Aktualisierungen an jedem DNS-Server erfolgen können. Dies wird durch die im Active Directory verwendete Multi-Master-Replikation gewährleistet. Hieraus ergeben sich hinsichtlich des Designs bzw. insbesondere hinsichtlich der Serverpositionierung weitere Möglichkeiten. Unter Umständen kann dies auch dazu führen, dass aus dem Bereich DNS weitere Anforderungen hinsichtlich der Serverpositionierung an das Active Directory Konzept generiert werden.

Bevor das Augenmerk auf die beiden anderen Dienste des IP-Managements gerichtet wird, werden noch einmal die Anforderungen im Bereich DNS und Active Directory zusammengefasst. Das Active Directory generiert mit den benötigten Domänen Design-Anforderungen an das DNS. Ferner werden mit den SRV-Records und der dynamischen Aktualisierung Funktionsanforderungen an die DNS-Implementierung gestellt. Diese werden nochmals verschärft, wenn die sichere dynamische Aktualisierung verwendet werden soll. Umgekehrt werden aus der Verwendung der sicheren dynamischen Aktualisierung Design-Anforderungen hinsichtlich der Serverpositionierung an das Active Directory definiert. Das DNS generiert eigenständig Design-Anforderungen, wenn z.B. eine interne DNS-Root verwendet werden soll, was meist, mit weiteren Funktionsanforderungen an die DNS-Implementierung für Conditional Forwarders und Stubzones kombiniert wird. Diese kurze Zusammenfassung für den Teil DNS-Active Directory zeigt bereits eindeutig, dass eine integrierte Planung absolut erforderlich ist.

DHCP

Bei DHCP existieren nicht so viele direkte gegenseitige Abhängigkeiten zum Active Directory. Allerdings ist hier insbesondere die Dreiecksbeziehung (DHCP – DNS – Active Directory) von Bedeutung. Diese kommt nämlich spätestens „ins Spiel“, wenn die (sichere) dynamische Aktualisierung für Clients, die nicht auf Windows 2000 oder XP basieren, benötigt wird, da die Aktualisierung für solche DHCP Clients vom DHCP Server durchgeführt werden kann bzw. muss. Wie bereits beschrieben, könnte diese je nach Konzept aber auch

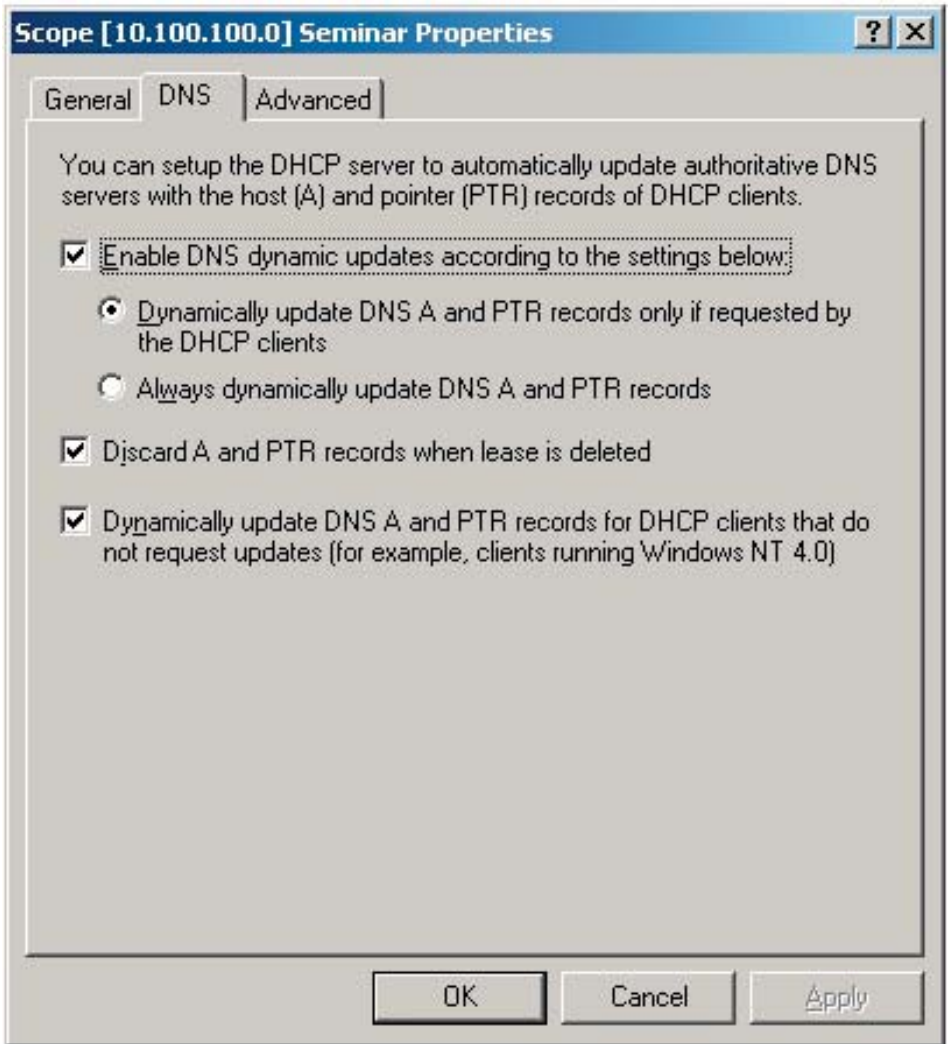


Abbildung 6: DNS-Konfigurationsparameter im DHCP

für Windows 2000/XP-Clients konzipiert werden. Grundsätzlich bietet ein Windows Server 2003 mit DHCP folgende Konfigurationsoptionen hinsichtlich DNS (siehe auch Abbildung 6 entsprechende Checkboxen).

Der DHCP-Server registriert und aktualisiert Clientinformationen mit den konfigurierten DNS-Servern gemäß den Clientanforderungen oder er registriert und aktualisiert Clientinformationen immer mit den konfigurierten DNS-Servern oder er registriert und aktualisiert nie die Clientinformationen mit den konfigurierten DNS-Servern oder er aktualisiert das DNS auch für Clients, die nicht die Betriebssysteme Windows 2000/XP ausführen. Konfigurierte DNS-Server sind die Server, die in den TCP/IP-Einstellungen für den DHCP-Server eingetragen sind. Die Einstellungen können für jeden Bereich (Scope) oder global auf Serverebene eingestellt werden. Läuft die Lease eines Clients aus, weil er im Netzwerk nicht mehr existiert oder eine Adresse aus einem anderen Bereich erhalten hat, dann veranlasst der DHCP-Server, den Eintrag zu löschen, sofern die Option „Forward-Lookups (Name zu Adresse) bei Ablauf des Lease löschen“ aktiviert wurde. Diese Funktion ermöglicht es, die Einträge im DNS so aktuell wie möglich zu halten und „veraltete“ Einträge zu verhindern.

Werden die Zonen dann noch als Active Directory integrierte Zonen gespeichert, dann existiert die oben genannte „Dreiecksbeziehung“: DHCP aktualisiert DNS und die Informationen sind im Active Directory gespeichert. Eine weitere Abhängigkeit des DHCP zum Active Directory ist ebenfalls noch zu beachten. Werden Windows 2000 oder Windows Server 2003 eingesetzt und auch das Active Directory verwendet, dann müssen die DHCP Server im Active Directory autorisiert werden. Ohne diese Autorisierung erfolgt keine Verteilung von IP-Adressen an die Clients. Letztendlich muss man zwar nur auswählen, dass der DHCP-Server autorisiert werden soll, doch besteht auch an diesem Punkt dadurch eine elementare Abhängigkeit.

Im Sinne einer integrierten Planung ist das Thema DHCP natürlich noch vielfältiger, auch wenn man nochmals das Beispielszenario betrachtet. Auch für die vorhandenen LINUX Clients müssen die entsprechenden Optionen definiert und verteilt werden. Ein Beispiel für diese Informationen könnten die Werte für NIS (Network Information Services) sein. Betrachtet man dann das Beispiel im Sinne einer integrierten Planung der LINUX Clients weiter, dann könnte im Rahmen dieses Szenarios die Implementierung der Services for UNIX von Microsoft erfolgen. Weitere Informationen hierzu siehe Kasten 1.

WINS

Zurück zur integrierten Planung des IP-Managements: Wie bereits beschrieben, wird auch das Thema NetBIOS-Namensauflösung als Teil dieser Planung gesehen. Betrachtet man das Beispielszenario, dann ist ein Einsatz von WINS sehr wahrscheinlich, nicht zuletzt unter dem Aspekt, dass die erforderliche Dynamik erzielt werden soll. Direkte Berührungspunkte mit dem Active Directory, wie im Sinne der beschriebenen Punkte für DNS, bestehen nicht in dieser Form. Allerdings stellt auch WINS neben der Namensauflösung für diese Welt verschiedene Informationen für die NetBIOS-Clients hinsichtlich der Domänen zur Verfügung. Dies sind insbesondere die bereits erwähnten Einträge 1C (für Domänenkontroller) und 1B (für den Domain Master Browser). Insofern sollte bei der Planung darauf geachtet werden, dass diese insbesondere hinsichtlich Serverpositionierung analog zur DNS-Planung erfolgt. Dieser de facto parallele Betrieb beider Welten zur (dynamischen) Namensauflösung hat noch einen Vorteil: Sollte tatsächlich der Fall eintreten, dass die NetBIOS-Namensauflösung im Unternehmen nicht mehr erforderlich ist, dann kann diese sehr leicht aus der Infrastruktur entfernt werden. Dies gestaltet sich schwieriger, wenn ggf. gegenseitige Abhängigkeiten bestehen. Andererseits ist die Anforderung an die Planung etwas höher, da unbedingt dafür Sorge getragen werden muss, dass beide Welten über identische Informationen verfügen.

Wie aus der Betrachtung des Beispielszenarios mit Active Directory zu ersehen, ist die integrierte Planung des IP-Managements unerlässlich. Dies ändert sich letztendlich auch nicht, wenn anstatt der IP-Management Dienste auf Basis von Windows mit Vital QIP ein noch umfassenderes Werkzeug eingesetzt wird.

QIP

Verändert man das Beispielszenario dahingehend, dass anstatt der Windows-Dienste das Produkt Vital QIP genutzt wird, dann ergeben sich im Überblick folgende Abhängigkeiten, die insbesondere eine integrierte Planung erforderlich machen. Die Design-Anforderungen aus dem Active Directory hinsichtlich der erforderlichen Domänen müssen ebenso berücksichtigt werden. Auch müssen die Funktionsanforderungen durch die Implementierung abgedeckt werden, hierbei sind ja in erster Linie die SRV-Records und die dynamische Aktualisierung zu beachten. Auch eine sichere dynamische Aktualisierung muss ggf. unterstützt werden (Vital QIP 6.1). In diesem Kontext ist zu beachten, dass als Front End DNS Server auch Windows 2000 Server mit Active Directory integrierten Zonen eingesetzt werden können, auch wenn dies bei einer Implementierung mit QIP meist nicht umgesetzt wird. Auch Design- und Funktionsanforderungen an das DNS selber, wie interne DNS-Root und Stubzones, können ebenfalls umgesetzt werden. Hinzu kommt bei QIP, dass die so genannten „Subnet Organisations“ mit den Sites (Standorten) innerhalb des Active Directory repliziert werden können. Dies ist eine zusätzliche Möglichkeit, die aber nochmals unterstreicht, dass eine integrierte Planung absolut erforderlich ist. Natürlich muss noch erwähnt werden, dass die Implementierung eines Tools wie QIP im Bereich des IP-Managements wesentlich mehr Funktionalitäten bietet als die Windows-Dienste. Grundsätzlich werden die Anforderungen abgedeckt und es stehen z.B. folgende zusätzliches Features zur Verfügung: Management heterogener Netze (verschiedene IP-Management Plattformen), eigenständige Datenbank im Hintergrund, besseres Reporting und Monitoring, Benutzer zu IP-Adressen- oder MAC-Adressen-Zuordnung (z.B. hinsichtlich Abrechnung) und diverse Zusatzmodule (SNMP oder API Toolkit). Andererseits muss aber auch erwähnt werden, dass das erforderliche Know-How zum Betrieb dieser umfassenderen Tools wesentlich größer sein muss und dass diese Tools auch ihren Preis haben.

Resümee

Im Rahmen des Artikels war erkennbar, dass das IP-Management einerseits leicht zur Achilles Ferse der Unternehmens IT werden kann, insbesondere wenn nicht die erforderliche Dynamik vorhanden ist, und andererseits eine Umbrella Technologie ist, die sich über weite Teile der IT-Infrastruktur spannt. Letztendlich ist das IP-Management so elementar wichtig, dass ihm auch weiterhin eine hohe Priorität zuzuordnen ist, auch wenn oft andere Dienste im Vordergrund stehen. Dieser hohe Stellenwert erfordert zwingend eine integrierte Planung, wie am Beispiel des Active Directory dargestellt wurde. Sollte dies nicht erfolgen, so findet man sich schnell in einer Situation wieder, wie in den Eingangsbeispielen beschrieben. (mh)

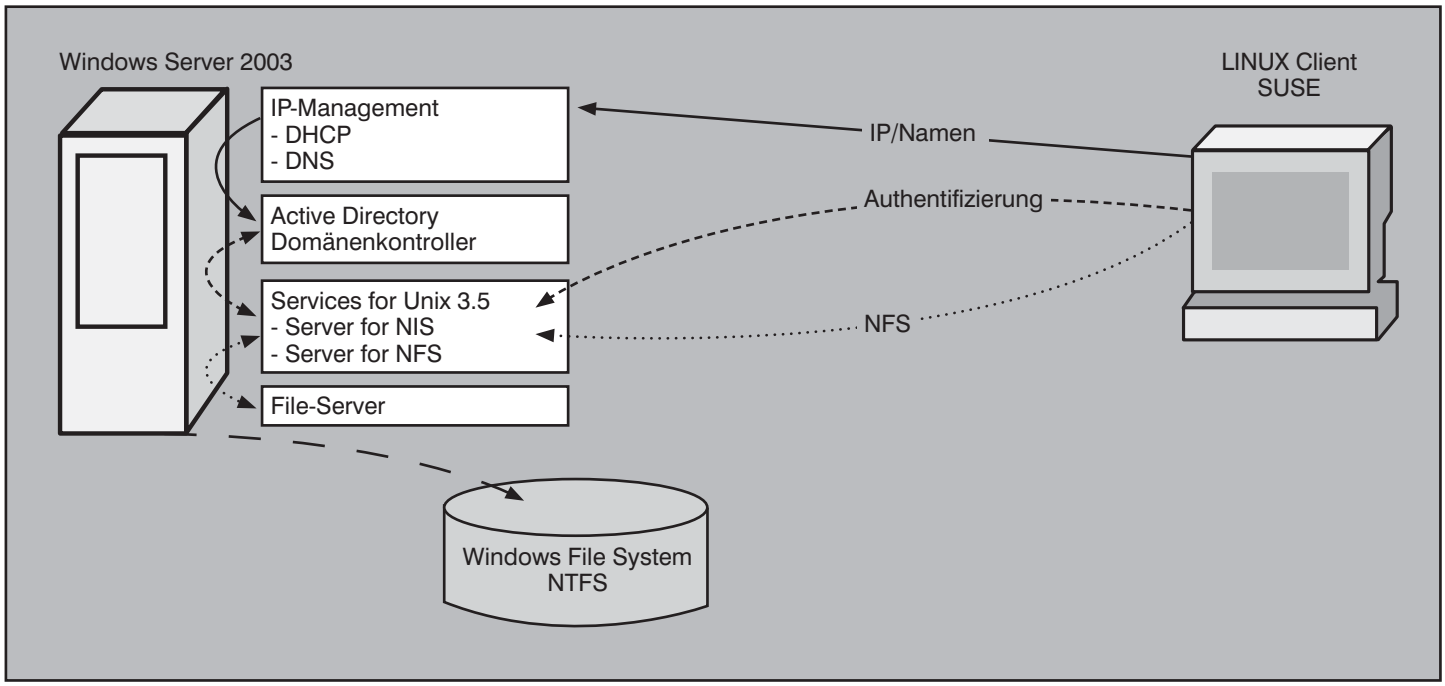


Abbildung 7: SFU Integration im Beispielszenario

KASTEN 1:

Services for UNIX

Im Rahmen des Artikels wurden die Services for UNIX (SFU) von Microsoft im Rahmen der integrierten Planung angesprochen. Folgend wird mit Orientierung am Beispielszenario des Artikels die Integration dieser Dienste grob betrachtet, da sie eine sehr gute Ergänzung darstellen und zukünftig immer häufiger zum Einsatz kommen werden. Vorweg noch die grundsätzlichen Möglichkeiten der SFU 3.5, die von den Microsoft Webseiten herunter geladen werden können (http://www.microsoft.com/windows/sfu/downloads/default.asp):

- Nutzung von UNIX (LINUX) Netzwerk Ressourcen
  - Client for NFS (Network File System): Dieses Tool ermöglicht Windows 2000, XP und Server 2003 den Zugriff auf NFS-Server.
  - Server for NFS: Ermöglicht NFS-Clients zu Zugriff auf Windows-Ressourcen mittels NFS.
  - Gateway for NFS: Ermöglicht Windows-Clients den Zugriff auf NFS-Ressourcen, wobei auf den Clients keine Software installiert werden muss. Das Tool läuft ausschließlich auf einem Windows 2000 Server bzw. Server 2003.
  - Server for PCNFS: Dieses Tool erlaubt Windows, als PCNFS Server zu agieren.
  - Netzwerk Administration
  - Telnet Client
  - Telnet Server
  - MMC Snap-in „Services for UNIX“
- Konten Management:
  - Server for NIS (Network Information Services): Dieses Tool ermöglicht es Windows 2000- oder Windows Server 2003- Domänenkontrollern, als primärer NIS-Server zu fungieren. Die Verwaltung der NIS-Domänen und Windows-Domänen erfolgt im Active Directory.
  - Password Synchronisation: Bidirektionale Kennwort Synchronisation für beide Plattformen.
  - User Name Mapping: Dieses Tool verbindet Windows und UNIX Benutzernamen, um es den Benutzern - ohne eine seperate Anmeldung in der UNIX-Welt - zu erlauben, sich mit einer NFS-Ressouce zu verbinden.
  - NIS Migration Wizard: Dies ist ein Tool, um UNIX NIS Informationen/ Daten in das Active Directory zu überführen.
- Interix: SFU 3.5 enthält die „Interix subsystem technology“ - eine Applikations- und Skripting-Umgebung.

Für das Beispielszenario könnte sich eine Integration der LINUX Clients entsprechend der vereinfachten Abbildung 7 darstellen.

Die LINUX-Clients erhalten über DHCP ihre IP-Adresse und die entsprechenden Konfigurationsparameter. Auch sorgt der DHCP-Server dafür, dass eine dynamische Registrierung im DNS erfolgt. Da im Beispielszenario Active Directory integrierte Zonen verwendet werden, könnte auch eine sichere dynamische Aktualisierung erfolgen. Ferner wird zur Authentifizierung mittels der SFU ein NIS-Server auf Basis von Windows Server 2003 implementiert. Dieser stellt den LINUX-Clients die entsprechenden Anmeldemöglichkeiten zur Verfügung. Die Informationen hinsichtlich NIS (NIS-Domäne und NIS-Server) werden den Clients mittels der DHCP-Optionen bereitgestellt. Die Verwaltung der NIS Informationen (Benutzer und Gruppen) erfolgt innerhalb des Active Directory im MMC Snap-In Benutzer und Computer (siehe Abbildung 8 für die Benutzer Attribute). Neben diesen Attributen, die die direkte Integration verdeutlichen, erfolgt natürlich auch die Verwaltung des Dienstes im MMC Snap-In für die Services for UNIX. An dieser Stelle wäre es beispielsweise auch möglich, Informationen zu NIS-Servern zu integrieren, die auf Basis von UNIX oder LINUX implementiert sind. Auch erfolgt in diesem Verwaltungswerkzeug die Zuordnung von Windows-Benutzern zu UNIX-Benutzern. Der Zugriff auf Dateien, die auf Windows-Servern gespeichert sind, könnte im Beispielszenario mittels eines NFS-Servers erfolgen.

Dies ist sicherlich nur ein kleines Beispiel, welches aber deutlich zeigt, dass wenn der Bogen etwas weiter gespannt wird, eine integrierte Planung umso erforderlicher

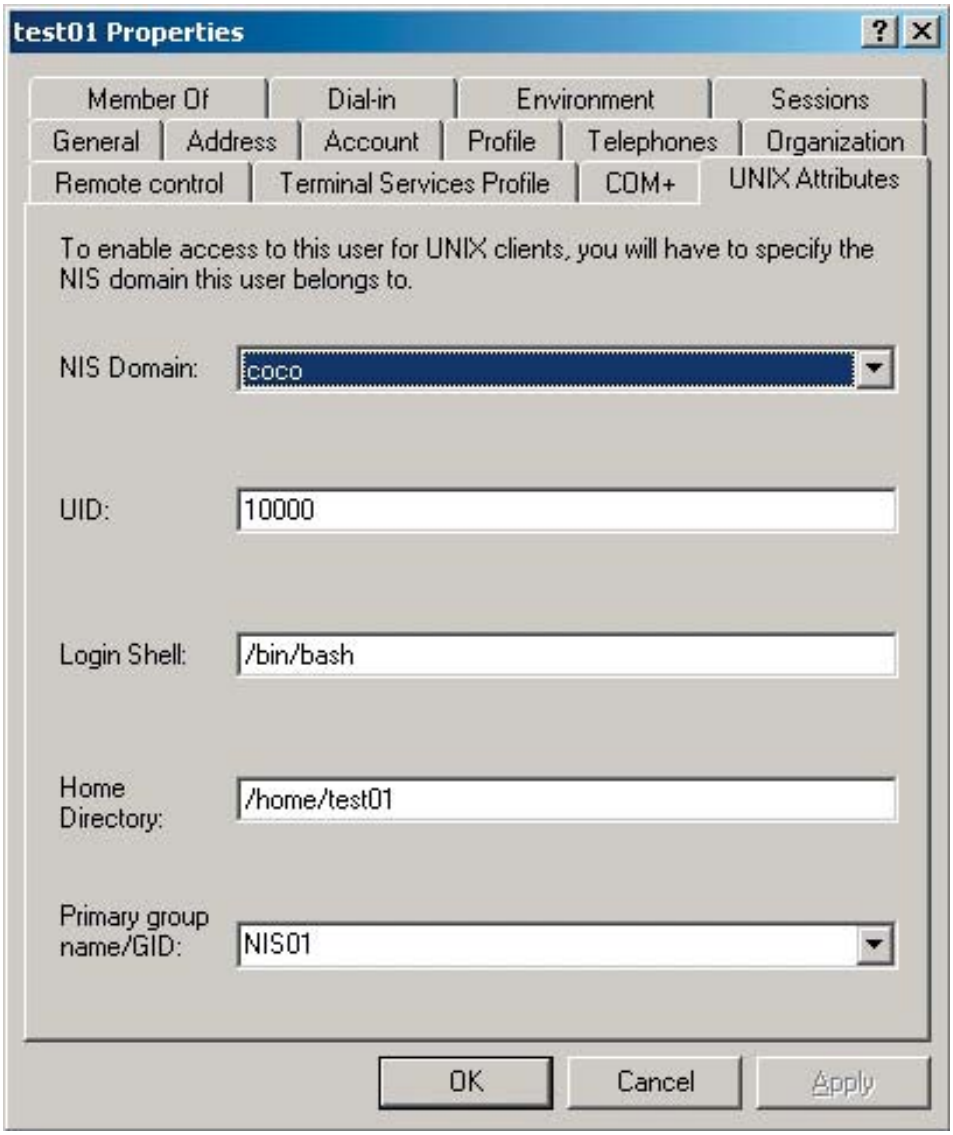


Abbildung 8: Verwaltung NIS-Attribute für Benutzer im Active Directory

wird. Zum einen stellt das IP-Management mit all den Integrationsaspekten wieder die entsprechende Basis zur Verfügung, ohne die auch dieses Szenario nicht bestehen könnte, und zum anderen erfolgt auch für die UNIX-Dienste eine Integration in das Active Directory. Diese geht sogar soweit, dass neben der Speicherung der Informationen für NIS die Administration integriert wurde. In Projekten hat die Implementierung der SFU bereits dafür gesorgt, dass andere Tools abgelöst wurden. Dies erfolgte meist im Sinne einer zentralisierten Administration (im Active Directory) und natürlich weil keine zusätzlichen Softwarekosten anfielen.

Betrachtet man die SFU gesondert, dann sollte beachtet werden, dass natürlich eine Reihe von guten Integrationsmöglichkeiten Richtung UNIX geboten werden, dass es aber immer noch zwei verschiedene Welten sind, was insbesondere beispielsweise hinsichtlich der Rechte ins Gewicht fällt. Auch ist entsprechendes Know-How für beide Welten erforderlich und es sind diverse Detailarbeiten nicht zu vergessen.

CCNE

ComConsult Certified Network Engineer

Lokale Netze
27.09. - 01.10.04 in Aachen
06.12. - 10.12.04 in Aachen

TCP/IP und SNMP
05.07. - 09.07.04 in Bonn
27.09. - 01.10.04 in Berlin
06.12. - 10.12.04 in Bonn

Internetworking
13.09. - 17.09.04 in Aachen
29.11. - 03.12.04 in Aachen

Ethernet Technologien - neuester Stand
13.09. - 17.09.04 in Aachen
29.11. - 03.12.04 in Aachen

Paketpreis für alle vier Seminare € 7.780.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--)

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting
in Lokalen Netzwerken - Grundlagen
05.07. - 09.07.04 in Aachen
08.11. - 12.11.04 in Aachen

Trouble Shooting
in geswitchten Ethernet-Umgebungen
06.09. - 10.09.04 in Aachen
22.11. - 26.11.04 in Aachen

Trouble Shooting
für TCP/IP- und Windows-Umgebungen
27.09. - 01.10.04 in Aachen

Paketpreis für alle drei Seminare mit Etherreal in Kombination mit Fluke Nettool € 7.500.-- zzgl. MwSt.
(Einzelpreise: je € 2.490.--)

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

CCSE

ComConsult Certified Security Expert

Sicherheitslösungen I:
Von den Einzelbausteinen zur integrierten Lösung
05.07. - 09.07.04 in Bonn
11.10. - 15.10.04 in Bonn

Sicherheitslösungen II:
IP-VPNs, der Kern einer Sicherheits-Infrastruktur
13.09. - 15.09.04 in Köln
15.11. - 17.11.04 in Köln

Sicherheitslösungen III:
19.07. - 23.07.04 in Aachen
04.10. - 08.10.04 in Aachen
06.12. - 10.12.04 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.de

Impressum

Verlag:
Dr. Suppan International institute b.v
Ahornenlaan 12
4493 DG Kamperland, Niederlande

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

Herausgeber und verantwortlich im Sinne des Presserechts:
Dr. Jürgen Suppan

Chefredakteur: Dr. Jürgen Suppan

Erscheinungweise: Monatlich, 12 Ausgaben im Jahr

Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service der ComConsult Akademie

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen