Dr. Suppan International Institute

Der Netzwerk Insider

August 2001

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Active Directory und DNS – eine Welt?

von Markus Holländer und Lars Kuhl

Ein Großteil der Unternehmen, die ernsthaft den Schritt zu Windows 2000 und damit auch zum Active Directory anstreben, planen die Migration für das 2. Halbjahr 2001 bzw. für das 1. Halbjahr 2002. Projekt- und Seminarerfahrung zeigen jedoch, dass viele diesen Schritt unterschätzen, insbesondere was die Ausmaße der Migration betrifft und dass bereits bei den Grundlagen entscheidende Fehler gemacht werden. Eine dieser Grundlagen ist DNS – von dem das Active Directory ganz entscheidend abhängig ist.

Neben diesem technischen Aspekt, auf dem in diesen Artikel näher eingegangen wird, besitzt das Thema DNS und Active Directory aber auch politische Brisanz. In der Vergangenheit bzw. heute oft noch aktuell basiert die Namensauflösung von Windows NT auf NetBIOS (WINS) und die "Microsoft-Truppe" kann ihr eigenes

Es ist angerichtet:
Active Directory und DNS – eine Welt

"Süppchen" kochen. Mit der Wandlung weg von NetBIOS hin zu DNS wurde auch politisch einiger Zündstoff generiert, denn DNS-Namensauflösung und Strukturen sind klassische UNIX- oder Netzbetriebs-Administrationsbereiche. Die von Microsoft favorisierte Vorstellung, dass die DNS-Administration - zumindest die, die das Active Directory betrifft, auch in einer MS-Welt läuft, wird von den wenigsten klassischen DNS-Administratoren geteilt. Andererseits schafft es Microsoft durch geschicktes Marketing immer wieder, Entscheider vorweg so zu vereinnahmen, dass globale Entscheidungen wie die Einführung von Windows 2000 bereits getroffen worden sind und somit dieser Zündstoff entstehen kann. Nicht dass die Einführung des Active Directory als eine schlechte Entscheidung angesehen wird, doch manchmal müssen die technischen Gründe im Projekt nachgeschoben werden.

weiter Seite 8

Zum Geleit

Was müssen Netzwerk-Produkte leisten, wo stehen die Hersteller ?

Der Netzwerkmarkt ist in einer erheblichen Unruhe. Die Hersteller stehen angesichts starker Umsatzeinbrüche und zum Teil massiver Verluste in der bisher größten Herausforderung der Netzwerk-Geschichte.

Es ist keine Frage, dass der Markt sich wieder fangen wird. Dazu ist der mittelfristige Bedarf nach Kommunikationslösungen zu groß. Man denke nur an den bisher kaum erschlossenen Markt der privaten Netze (home networks). Und auch im Bereich der industriellen Kunden und Behörden besteht noch ein erheblicher Investitionsbedarf innerhalb der nächsten 3 bis 5 Jahre.

Technologienveränderungen im Server- und Speicher-Bereich werden zwangsläufig zu einem weiteren Investitionsschub im Netzwerkbereich führen. Trotzdem wird nicht jeder der heutigen Anbieter die nächsten 3 Jahre überleben.

Entscheiden werden

- die richtige Produktstrategie
- die Preisgestaltung
- Wartungs- und Service-Konzeptionen
- die Absatzgestaltung
- eine klare und eindeutige Identität

Die eigentliche Bedrohung der Hersteller kommt dabei m.E. nicht aus dem vorübergehenden Rückgang der Nachfrage sondern aus den starken Änderungen der technischen Anforderungen an Produkte. Mit der Frage, welche Detailtechnologie in Zukunft gefordert wird, sind erhebliche Risiken verbunden. Wer auf die falsche Technik setzt, der kann aufgrund der hohen Entwicklungskosten schnell vor dem Aus stehen (siehe CoreBuilder und 3Com). Auch kann sich die Entscheidung der Hersteller, die Produktion zu anderen Unternehmen auszulagern, angesichts der damit verbundenen vertraglichen Abnahmeverpflichtungen bei einer falschen Einschätzung des Marktes zu einem Bumerang entwickeln.

weiter Seite 2

Was müssen Netzwerk-Produkte leisten, wo stehen die Hersteller?

Fortsetzung von Seite 1

Die Historie der letzten 20 Jahre hat gezeigt, dass sich im Markt nur durchsetzt, was

- dem direkten Bedarf des Anwenders entspricht
- einfach ist
- wenig kostet.

Spannend ist, dass die meisten Hersteller in den letzten 12 bis 18 Monaten Technologien gefördert haben, die dieser Erkenntnis widersprechen:

- Voice over IP
- Quality of Service
- Policy Networking

Der Grund für diese Strategie der Hersteller ist einleuchtend. Die aufwendige Konfiguration dieser neuen Technologien ist im Tagesbetrieb nur mit einem geeigneten Tool realisierbar. Dieses führt aber zwangsläufig zu einer Bindung an den jeweiligen Hersteller und zu der konsequenten Nutzung aller Produkte eines Herstellers (strategisch geradezu mustergültig im Hause CISCO umgesetzt).

Trotzdem ist für mich immer wieder überraschend, wie stark die Hersteller die Interessen des Anwenders vernachlässigen. Wichtige technische Entwicklungen geraten so in das Risiko, vom Markt nicht angenommen zu werden.

Ein gutes Beispiel hierfür ist Voice-over-IP. Es ist offensichtlich, dass eine Kosteneinsparung im Bereich der Basis-Telefoniefunktionen in bereits bestehenden Infrastrukturen kaum zu erzielen sein wird. Trotzdem kann Voice-over-IP wesentliche Vorteile bringen, wenn man Funktionen wie kleine Call-Center (ACD), CTI und Unified Messaging als Teil einer integrierten Lösung ansieht.

Derartige Lösungen waren bisher zu teuer und zu kompliziert, um sie einer breiten Nutzung zuzuführen. Voice-over-IP würde die Chance bieten, dies zu ändern.

Wir haben dies für uns in der ComConsult Akademie umgesetzt und auf der Basis dieser Technologien eine völlig neue Kommunikations-Infrastruktur aufgebaut. Und wir sind begeistert. Die organisatorischen und wirtschaftlichen Vorteile sind erheblich. Nur betrachtet man die Masse der angebotenen Produkte in diesem Bereich, dann wäre dieser Weg für uns mit diesen Produkten nicht möglich gewesen.

Warum?

Weil sie teuer und kompliziert sind, obwohl sie auf Voice-over-IP beruhen.

Worin liegt denn dann noch der Vorteil gegenüber einer traditionellen TK-Lösung?

Auf der einen Seite jammern die Hersteller über die mangelnde Nachfrage nach Voice-over-IP, auf der anderen Seite kümmern sie sich nicht um den Bedarf des Anwenders. Dann müssen sie sich nicht wundern, dass dieser die Produkte nicht kauft.

Warum ist das so?

Zum einen verstehen offensichtlich nicht alle Hersteller die gegebenen Anforderungen, zum anderen beinhalten die Anforderungen im Kern eine Software-technische Lösung. Die meisten der Netzwerk-Hersteller haben ihre Stärke aber im Bereich der Hardware und der hardwarenahen Software. Somit geraten sie in ein logistisches und strukturelles Problem, wollten sie die Anforderungen mit ihren Produkten umsetzen. Auch nutzt die späte Erkenntnis, was der Markt wirklich fordert, wenig, wenn bereits eine Produktarchitektur festgelegt wurde, die für die Umsetzung umfangreicher Software-Lösungen nicht geeignet ist bzw. dabei nicht skalieren würde.

Geht man von der Grundforderung aus, dass ein Netzwerk

- einfach sein muss
- von alleine laufen sollte
- nicht ausfallen sollte

kommt man auf eine andere Gewichtung der technischen Eigenschaften, die ein modernes Netzwerk-Produkt haben sollte. Es sollte:

- einfach und preiswert sein
- Schnittstellen für die aktuellen Ethernet-Technologien haben
- ein Produktportfolio bieten, das einerseits
  - Produkte zur Realisierung eines hochverfügbaren Netzwerk-Kerns inklusive der entsprechenden Server-Anbindungen
  - und andererseits preiswerte Massenprodukte für die Anbindung von Endgeräten beinhaltet.

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

Gestaltung:
Zweipfennig

Erscheinungsweise:
Monatlich,
12 Ausgaben im Jahr

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

Für unverlangt
eingesandte Manuskripte
wird keine Haftung übernommen

Was müssen Netzwerk-Produkte leisten, wo stehen die Hersteller?

In diesem Sinne halte ich folgende Entwicklungen des Marktes für wirklich wichtig:

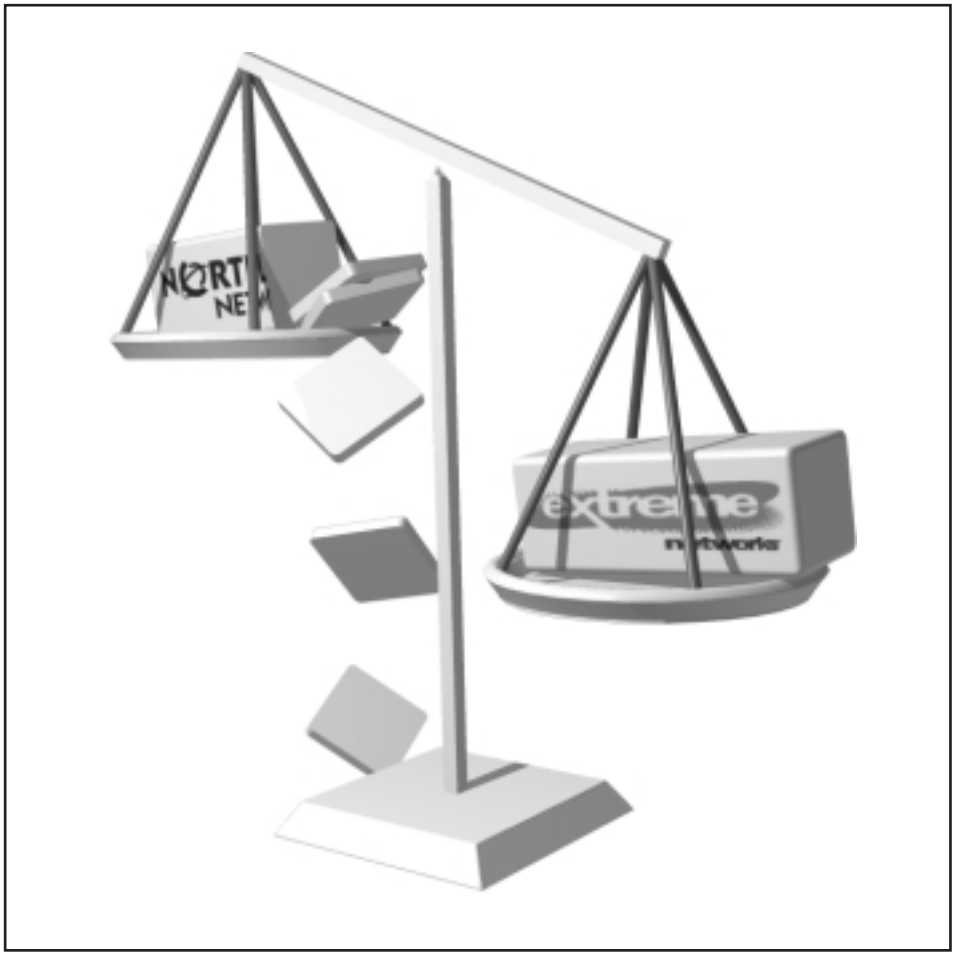
- die Entwicklung von Etagen-/Workgroup-Switches, die eine austauschbare Netzwerk-Grundfunktionalität zu einem günstigen Preis an die Endgeräte bringen. (ein gutes Beispiel sind die Produkte von HP mit dem Ein-Chip-Design)
- Wartungsfreiheit für derartige Massenprodukte (siehe HP)
- ein zunehmendes Angebot an kleinen Layer-3-Switch-Systemen für den Kernbereich kleinerer Unternehmen zu einem wesentlich niedrigeren Preis als bisher (CISCO bewegt sich in diese Richtung, wie die letzten Ankündigungen in der 29xx und 35xx-Serie zeigen)
- ein zunehmendes Angebot von Gigabit-Ethernet Schnittstellen für das Endgerät (siehe ebenfalls CISCO, natürlich auch Extreme)
- die Umsetzbarkeit von 10-Gigabit-Ethernet im Gelände innerhalb der nächsten 3 Jahre (die Gesamt-Schaltkapazität des Switches muss das zulassen!)
- die Weiterentwicklung einfacher Redundanzverfahren wie Spanning Tree und Link Aggregation

Hintergrund dieser Bewertung wichtiger Eigenschaften ist meine grundsätzliche Strategie:

- die Konfiguration wichtiger Verfahren für Redundanz, Loadsharing und Fehlertrennung auf den Kernbereich eines Netzwerks (Server-Zugang, Gelände) zu konzentrieren
- die Netzwerk-Komponenten zur Versorgung der Endgeräte auf den Etagen wie Repeater zu behandeln und möglichst einfach zu konfigurieren.

Spannend ist dabei, dass derartig konfigurierte Netzwerke

- einfach sind
- preiswert sind (insbesondere, wenn preiswerte Layer-3-Systeme verfügbar sind)
- alle Anforderungen an Quality of Service erfüllen.



Betrachtet man das Produktangebot der großen Hersteller, so liegt in dieser Grundfrage, was ein Netzwerk-Produkt wirklich leisten muss, mehr Sprengstoff als in der Frage, wie hoch die Nachfrage des Marktes ist.

Die traditionellen Hersteller haben sich meines Erachtens in den letzten Jahren unnötig technisch verzettelt und unter dem Ziel, die Kundenbindung durch technische Abhängigkeiten zu erhöhen, gefährliche Irrwege eingeschlagen. Dass der Weg in Richtung "komplex und teuer" nicht der vom Markt akzeptierte ist, hat schon die ATM-Historie gezeigt.

Dies gibt zur Zeit Herstellern, die Produktionserfahrungen unter dem Prinzip "einfach und kostengünstig" haben, die Chance Teile des Marktes zu erobern. Gleichzeitig sind derartige Produkte auch optimal für den Home Networking Markt geeignet.

Fazit: der Netzwerk-Markt wird sich weiterentwickeln.

Wir sind längst noch nicht am Ende der Entwicklung angekommen. Die notwendigen Weiterentwicklungen und die zukünftigen Anforderungen können ja klar benannt werden. Aber: es ist durchaus unklar, wer die Gewinner sein werden.

Aus meiner Sicht können die Gewinner nur die Hersteller sein, die ihre Produkte am Bedarf der Kunden orientieren und das Prinzip "einfach und preiswert" weiter verfolgen. Wichtig ist auch eine klare und eindeutige Identität (siehe Extreme). Hersteller, die meinen, auf erhebliche Marktsegmente einfach verzichten zu können, weil sie ihnen nicht lukrativ genug erscheinen, werden einen hohen Preis für diese Arroganz bezahlen (siehe Nortel).

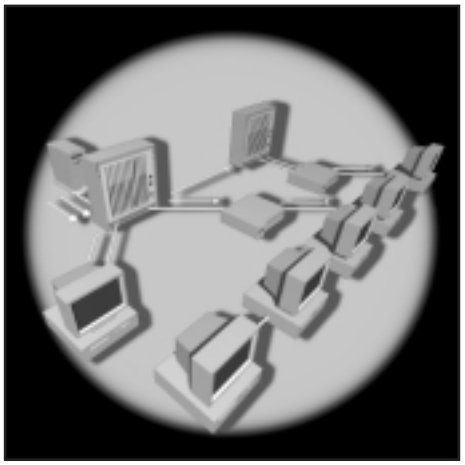
Ihr
Dr. Jürgen Suppan

Aktueller Kongress

Top-Highlights und brandheiße Information: Netzwerk- und System-Management Forum 2001

Vom 5. bis 8. November veranstaltet die ComConsult Akademie das Netzwerk- und System-Management Forum 2001 im Maritim Hotel Königswinter.

Unter der Leitung und Moderation der international anerkannten Management-experten Dr. Jürgen Suppan und Dr. Franz-Joachim Kauffels wird den Teilnehmern in dieser einzigartigen und äusserst beliebten Veranstaltung eine Top-Mischung aus Experten-Vorträgen, Anwender-Erfahrungsberichten, Live-Workshops mit direkter Gegenüberstellung wichtiger Produkte und einer begleitenden Ausstellung geboten.



Dieses Konzept hat in den letzten Jahren mit dazu geführt, dass diese Veranstaltung immer ausgebucht war und sich zu dem Treffpunkt der deutschen Management-Szene entwickelt hat.

Auch in diesem Jahr besteht wieder die Möglichkeit, das Forum 4-tägig mit Tutorium am ersten Tag, oder 3-tägig ohne das Tutorium zu buchen. Angesichts der Überbuchung in den Vorjahren ist eine rasche Anmeldung allen Interessenten, die sich ihren Teilnahmeplatz sichern wollen dringend empfohlen. Bis zum 31. August besteht darüber hinaus die Möglichkeit vom Frühbucherrabatt zu profitieren.

Die Themen-Schwerpunkte des diesjährigen Netzwerk- und System-Management Forums werden sein:

Aktueller Stand der Netzwerk- und System-Management-Technologie

- Was ist neu?
- Wie haben sich die Produkte entwickelt?
- Was werden neue Versionen bringen?

Aktueller Stand der Netzwerk- und IT-Systemtechnik

- Was ist neu, was kommt innerhalb der nächsten 3 Jahre?
- Was bedeutet das für die Management-Lösungen?

Service-Level-Management mit Live-Vergleich der führenden Tools:

- Was ist Service-Level Management?
- Wie wird es realisiert?
- Was bieten die Produkte?
- Welche Projekterfahrungen liegen vor?

IP-Technologie im Jahr 2001 und ihre Konsequenzen für Netzwerk- und System Management

- Ipv6 steht direkt vor der Tür (Druck der Smartphones, aktuelles CISCO-Announcement)
- Migration von Ipv4 zu Ipv6, wie sieht das aus?
- Was bedeutet das für die Switches?
- Wie werden IP-Netze optimal verwaltet?

DNS, DHCP usw.

- Welche Vorteile bietet ein Directory Dienst in diesem Zusammenhang?

Die neue Management-Technologie: Impact-Analyse

- Wie funktioniert sie?
- Was bringt sie?
- In welchen Produkten ist sie vorhanden?

Management von Switch-Systemen und QoS-Lösungen

- Switch-Systeme haben die Basis für Netzwerk-Management und Protokoll-Analyse stark verändert. Die Einführung von QoS-Lösungen ist nur in Kombination mit einem geeigneten Management möglich. Wie sehen die aktuellen Lösungen für Switch-Management aus?

Methodenuntersuchung:

- Wie kann mit möglichst wenig Arbeit möglichst viel Kontrolle über Netzwerke und Server in möglichst kurzer Zeit erreicht werden, welche Vorgehensweisen und Tools haben sich bewärt, welche nicht?

Organisatorische Rahmenbedingungen:

- Welche betrieblichen Abläufe sind für den erfolgreichen Einsatz von Netzwerk- und System-Management-Lösungen zu empfehlen bzw. mindestens erforderlich? Welche Instanzen müssen diskutiert werden, wie arbeiten diese zusammen, welche Tools optimieren speziell die Zusammenarbeit zwischen den Betriebsinstanzen?

Anzeige

10 % Vorbuchungs-Rabatt bis zum 31.08.01

Netzwerk- und System-Management Forum 2001

05.11. - 08.11.01 in Königswinter

Für Besucher unserer bisherigen Management-Veranstaltungen bzw. für die Teilnehmer am VIP-Verteiler bieten wir in diesem Jahr exklusiv eine Vorbuchungsphase für das Forum bis zum 31.08.2001 an. Vorteile für Sie:

- **Sie sichern sich Ihren Teilnahmeplatz**
- **Sie erhalten einen Vorzugs-Rabatt von 10 %**
  4 Tage (mit Tutorium) zum Preis von EUR 1.610,-- statt 1.790,-- zzgl. MwSt.
  3 Tage (ohne Tutorium) zum Preis von EUR 1.430,-- statt 1.590,-- zzgl. MwSt.

Die Buchung ist verbindlich, kann aber jederzeit auf andere Mitarbeiter Ihres Unternehmens übertragen werden.

Bitte buchen Sie per
eMail: akademie@comconsult.de oder via Internet www.comconsult-akademie.de

In der Hoffnung, Sie in Könisgwinter begrüßen zu können,
mit freundlichen Grüßen

Ihr Team der
ComConsult Akademie

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk- und System-Management Forum 2001

Ich melde mich an zum
Netzwerk- und System- Mangement Forum 2001 in Königswinter

☐ vom 05.11. - 08.11.01 **(mit Tutorium)**
zum Preis von EUR 1.610,-- zzgl. MwSt.

☐ vom 06.11. - 08.11.01 **(ohne Tutorium)**
zum Preis von EUR 1.430,-- zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer im Maritim Königswinter

von _____ bis _____
(Übernachtung/Frühstück DM 211,--)

Name	Vorname
Firma	Abteilung
Position	Funktion
Straße	PLZ, Ort
Telefon	Fax
eMail	Unterschrift

Faxen Sie einfach diesen Abschnitt an **02408/955-399** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de**

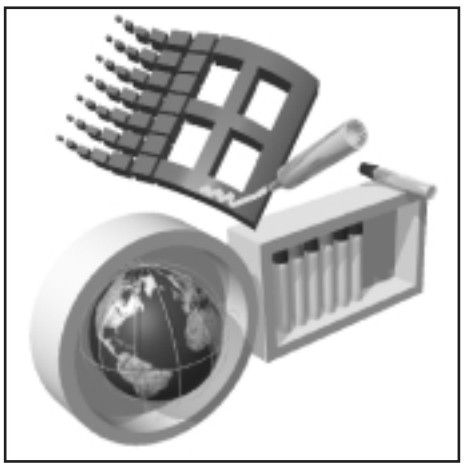
Seminare zum Schwerpunktthema

Zusatztermine: "DNS-/IP-Design für" und "Design Windows 2000 Active Directory"

Die Seminare der Reihe "Windows 2000 Active Directory" erfreuen sich eines überaus großen Zuspruchs und sind teilweise weit vor Seminarbeginn schon völlig ausgebucht. In dieser Situation bietet die ComConsult Akademie jetzt zwei Zusatztermine für die Seminare "DNS-/IP-Design für Windows 2000 Active Directory" (vom 4. bis 6. September im Maritim Hotel Königswinter) und "Design Windows 2000 Active Directory" (vom 10. bis 12. September 2001 im Holiday Inn Bonn).

Das Seminar "DNS-/IP-Design für Windows 2000 Active Directory behandelt in konzentrierter Form die Implementierungsgrundlagen aus dem IP-Bereich für Windows 2000 bzw. für das Active Directory. Dabei spielt DNS die Hauptrolle, wobei auch insbesondere die dynamische Verbindung zum DHCP betrachtet wird. Die Teilnehmer lernen in diesem Seminar die Grundlagen zu DNS als Auffrischung in komprimierter Form; welche aktuellen DNS-Serverimplementierungen auf dem Markt sind, insbesondere aus dem Hause Microsoft, aber auch die anderer Hersteller; welche DNS-Funktionen vom AD benötigt werden und wie Sie ein AD-DNS-Projekt strukturieren und durchführen.

Nachdem die Grundlagen für das Design des AD vermittelt wurden, befasst sich das Seminar "Design Windows 2000 Active Directory" mit dem eigentlichen Design des AD. Es werden die entsprechenden Kenntnisse aus dem vorangegangenen Seminar vorausgesetzt, wobei ein Besuch nicht zwingend erforderlich ist. Dieses Seminar vermittelt, unterstützt durch den Praxisbezug zu Projekten in diesem Umfeld, wie das AD zu strukturieren ist. Insbesondere dabei wird großen Wert auf den Entwurf der strategischen Komponenten (Domäne, Standort) gelegt. Neben dem theoretischen Vortrags- und Diskussionsteils wird ein Beispiel einer fiktiven Unternehmung dargestellt. Dies bedeutet, dass wichtige Designentscheidungen jeweils leichter nachvollzogen werden können. Ebenfalls wird die Dokumentation, die mehrfach Bestandteil des Seminars ist, an diesem Beispiel mit Hilfe von Visio 2000 erläutert. Ein weiteres Highlight ist die Präsentation des Windows-2000-Implementierung-Proj-ektplanentwurfs, in dem zum Abschluss des Seminars die Komplexität und die wichtigsten Meilensteine erläutert werden. Die Bereiche "Strukturen schaffen" und "AD und andere Verzeichnisdienste" orientieren sich an diesem Projektplan.



Die Referenten der ComConsult Beratung und Planung verfügen über entsprechende praktische Erfahrung aus einer Vielzahl von Projekten.

Markus Holländer ist Kompetenz Center Leiter Backoffice und besitzt langjährige Projekterfahrung im Design und im Betrieb von Windows NT und Windows 2000, sowie weiterer Backoffice Produkte. Er hat zahlreiche Projekte privater und öffentlicher Auftraggeber in diesem Umfeld erfolgreich geleitet.

Dipl.-Ing. Lars Kuhl ist im Backoffice Kompetenz Center als Berater für die Konzipierung und Umsetzung von Migrationsprojekten auf Windows NT 4 und Windows 2000 beschäftigt. Seine Kenntnisse hat er in der Projektarbeit und der Migration von Netzwerken bei Kunden erworben.

Dipl.-Inform. Michael van Laaks Schwerpunkte in der Konzipierung und Umsetzung von Migrationsprojekten auf Windows NT 4 und Windows 2000 sind Domänen-, IP-Management- und (Fern-) Administrationskonzepte.

Frank Neunzig (MCSE) besitzt mehrjährige Erfahrung und praktische Kenntnisse in den Bereichen Windows NT und Windows 2000, sowie weiterer Backoffice Produkte.

"plan – build – run" Windows 2000 Active Directory Seminarreihe

Der Windows 2000 Server beinhaltet eine Reihe von sehr leistungsstarken Möglichkeiten, den Betrieb von Servern und TCP/IP-Netzen zu vereinfachen und zu signifikanten Kosteneinsparungen zu kommen. Eine Reihe von sehr erfolgreichen Projekten hat bestätigt, dass hier ein erhebliches Potenzial gegenüber den bisherigen Lösungen besteht. Das eigentlich neue und somit auch der Grund für die vielen Vorteile, die Windows 2000 betriebstechnisch bietet, ist die Kombination einer Reihe von Verwaltungsdiensten mit einem zentralen Directory Service mit einer gleichzeitigen Integration in eine TCP/IP-Kommunikationswelt. Um die gegebenen Vorteile nutzen zu können, sind detallierte Kenntnisse einerseits der Technik des Windows 2000 Directory Services und andererseits seiner methodischen Nutzung erforderlich. Zur Vermittlung dieser Kenntnisse haben wir eine komplette Seminarreihe konzipiert, die mit aufeinander aufbauenden Seminaren aus der Planung und Konzeptionierung bis zum Betrieb von Windows 2000 Active Directory führen.

Im einzelnen besteht die Windows 2000 Active Directory Seminarreihe aus den Seminaren:

1. DNS-/IP-Design für Windows 2000 Active Directory
2. Design Windows 2000 Active Directory
3. Migration zu Windows 2000 Active Directory
4. Betrieb von Windows 2000 Active Directory

Die Seminare sind grundsätzlich unabhängig voneinander, jedoch ist es von Vorteil, wenn bei der Teilnahme an mehreren Seminaren die Reihenfolge eingehalten wird.

Windows 2000 Active Directory

DNS-/IP-Design für Windows 2000 Active Directory
Inhalt

Grundlagen des Domain Name System (DNS)
- Warum DNS? • Domain-Name-Space, Domain-Name, Internet-Domain-Name-Space
- Zonen • DNS-Server-Varianten • Delegierungen
- Clientkommunikation • DNS-Datenbank, DNS-Dateien
- DNS intern und extern • Dynamisches DNS
- Service-Records • Verbindungen zu DHCP und WINS

DNS-Server Implementierungen
- Windows NT 4.0 Server • Alternativen
- Windows 2000 Server - Neuerungen
- Active Directory Integration • Multiple-Master-Replikation
- Delegierungen • Primäre DNS-Server • Sicherheit
- SRV-Einträge • Verbindungen zu DHCP und WINS

AD-Anforderungen an DNS
- AD-Domäne gleich DNS-Domäne
- DNS-Domäne ungleich AD-Domäne • SRV-Einträge

DNS-Vorbereitung auf die Einführung vom AD
- Ist-Analyse • Zielvorstellungen • Migration

Fallbeispiel: DNS-Migration zur Einführung von Windows 2000

Design Windows 2000 Active Directory
Inhalt

Grundlagen des Active Directory
- X.500, Schema, DAP, LDAP: Objektklassen und Attribute
- Active Directory: Logische Struktur, Physikalische Struktur, Gruppenrichtlinien

Strukturen schaffen
- Erforderliche Active-Directory-Kompenenten
- Active Directory Rootdomänen/Gesamtstrukturplan
- Domänenmodelle für die einzelnen Rootdomänen
- Organisationseinheiten (OUs)
- Standorte/Sites
- Domänenkontroller

Active Directory und andere Verzeichnisdienste (Exchange 5.5)
- Vergleich der Standortdefinition
- Analyse der Synchronisationsmöglichkeiten
- Objekte für die Verzeichnissynchronisation
- Einsatzplanung des ADC (Active Directory Connectors)
- Dokumentation der Verzeichnisreplikation

Strukturen sichern – Sicherheitsmechanismen

Projektplanentwurf Windows 2000 Implementierung

ComConsult Akademie – Telefax: 02408/955-399

Fax-Antwort
Windows 2000 Active Directory

Ich melde mich an zum Zusatztermin
☐ 04. - 06.09.01 **DNS-/IP-Design für Windows 2000 Active Directory**
☐ 10. - 12.09.01 **Design Windows 2000 Active Directory**
zum Preis von je EUR 1590,-- zzgl. MwSt.

☐ Ich buche die Seminarreihe **plan - build - run Windows 2000 Active Directory** zum Paket-Preis von EUR 4.990,-- zzgl. MwSt. (statt regulär EUR 5.760,--)
1. ☐ 04. - 06.09.01* ☐ 24. - 26.09.01
2. ☐ 10. - 12.09.01 ☐ 05. - 07.11.01
3. ☐ 27. - 28.09.01 ☐ 26. - 27.11.01
4. ☐ 01. - 02.10.01 ☐ 06. - 07.12.01

☐ Bitte buchen Sie ein Zimmer im Holiday Inn Bonn/ * Maritim Hotel Königswinter

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **akademie@comconsult.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de**

☐ Senden Sie mir bitte unverbindlich detailliertes Informationsmaterial über die vier Seminare der **plan - build - run Windows 2000 Active Directory** -Seminarreihe:
1. **DNS-/IP-Design für Windows 2000 Active Directory**
2. **Design Windows 2000 Active Directory**
3. **Migration zu Windows 2000 Active Directory**
4. **Betrieb von Windows 2000 Active Directory** zu

Name _____ Vorname _____

Firma, Abteilung _____ Position, Funktion _____

Abteilung _____ Funktion _____

Straße _____ PLZ, Ort _____

Telefon _____ Fax _____

eMail _____ Unterschrift _____

Active Directory und DNS – eine Welt?

Das Autorenteam

Markus Holländer (MCSD) ist Kompetenz Center Leiter Backoffice bei der ComConsult Beratung und Planung GmbH.

Dipl.-Ing. Lars Kuhl ist bei der ComConsult Beratung und Planung GmbH im Backoffice Kompetenz Center als Berater für die Konzipierung und Umsetzung von Migrationsprojekten auf Windows NT 4 und Windows 2000 beschäftigt.

Grundsätzlich ist es empfehlenswert in einer frühen Phase des Projektes oder sogar im Vorfeld alle relevanten Bereiche an einen Tisch zu bringen, also der Kreis, der für das AD verantwortlich ist, die aktuellen DNS-Administratoren und auch das Sicherheitsteam, denn dies ist ebenfalls durch das DNS/AD-Design betroffen, da Sicherheitsbereiche definiert werden. In Projekten gab es bereits elementare Design-Enscheidungen, die nur auf Sicherheitsaspekten beruhten und eigentlich nicht von AD-Designer gewünscht waren, doch dazu später mehr. Eine wichtige Vorraussetzung und ein Thema dieser Runde ist, dass jede Active Directory Domäne eine gleichnamige DNS-Domäne benötigt.

Somit stellen sich in dieser frühen Phase folgende Fragestellungen:

- Welche DNS-Domänen benötige ich für das AD?
- Ist das DNS-Domänen-Design gleich dem AD-Domänen-Design?
- Nimmt man bestehende Domänen oder definiert neue bzw. kann man seine vorhandene Struktur verwenden oder was ist zu verändern?
- Welche DNS-Serverimplementierung verwendet man, kann man die bestehende Implementierung verwenden, muss man updaten oder etwas völlig neues aufbauen?

Es ist natürlich so, dass man nicht für jede DNS-Domäne eine AD-Domäne benötigt, doch wird das DNS-Design zumindest durch das AD beeinflusst. Somit scheint die Ausgangsfrage "AD und DNS – eine Welt?" geklärt - es kommt immer auf die Blickrichtung an. Aus der DNS-Sicht ist es "nur" ein Teil, aus AD-Sicht scheint es eine Welt zu sein. Zur Klärung obiger Fragestellungen beschreiben folgende Abschnitte Ansätze, Anforderungen und Vorschläge.

1 Anforderungen aus dem Active Directory an das DNS

Windows 2000 und Active Directory verwenden DNS für die Namensauflösung. Ohne eine DNS-Infrastruktur kann das Active Directory nicht implementiert werden. Die Domänenstruktur des Active Directory spiegelt sich im DNS wider, da für die Bezeichnung von Active Directory Domänen DNS-Namen verwendet werden.
Nachfolgend wird dargestellt, wie die Namensauflösung unter Windows 2000 abläuft und in welcher Weise Active Directory das DNS verwendet. Weiterhin wird beschrieben, welche Anforderungen an eine DNS-Implementierung seitens des Active Directory für ein einwandfreies Arbeiten gestellt werden.

1.1 Namensauflösung bei Windows 2000

Die Namensauflösung unter Windows 2000 unterscheidet sich erheblich von der unter Windows NT. Bei Windows NT gilt als Grundregel, dass vor der DNS-Namensauflösung zuerst eine NetBIOS Namensauflösung versucht wird. Windows 2000 verwendet für die Namensauflösung zuerst das DNS.

Ist eine Namesauflösung erforderlich, so wird zuerst vom Windows 2000 System überprüft, ob es sich um einen FQDN (Fully Qualified Domain Name) handelt wie beispielsweise www.comconsult.com. oder um einen unvollständigen Namen mit einer oder mehreren Komponenten (sap1 oder sap1.comconsult). Bevor eine DNS-Abfrage gestartet wird, wird zunächst der Cache des Windows 2000 Systems überprüft, ob die benötigten Informationen bereits lokal gespeichert sind.

Soll ein FQDN abgefragt werden, so kann der Name direkt an den DNS-Server weitergegeben werden. Die Abfrage eines unvollständigen Namens kann über DNS nur dann erfolgen, wenn der Name zu einem FQDN vervollständigt wird, da DNS-Server nur Abfragen für FQDN beantworten können. Bei unvollständigen Namen mit mehren Komponenten wird nur ein Punkt an den Namen angehängt, bevor der Name als FQDN an den DNS-Server übergeben wird. Bei einem unvollständigen Namen mit nur einer Komponente müssen für die Vervollständigung zum FQDN zwei Situationen je nach Konfiguration des Windows 2000 Clients unterschieden werden.

1. Auf dem Client wurde keine Liste von Domänensuffixen in der TCP/IP Konfiguration definiert. Wenn dies der Fall ist, wird das primäre DNS-Suffix angehängt, um einen FQDN an den DNS-Server übergeben zu können.

   Anmerkung: Das primäre DNS-Suffix eines Windows 2000 Clients entspricht dem DNS-Namen der Active Directory Domäne, in der das Computerkonto des Clients existiert.

2. Ist eine Liste von Domänensuffixen definiert, so erfolgt eine systematische DNS-Abfrage mit den verschiedenen Suffixen. Die Suffixe werden gemäß der konfigurierten Reihenfolge angehängt.

Die Domänensuffixe können in den erweiterten TCP/IP Eigenschaften (Bild 1) konfiguriert werden und es kann auch die Verwendungsreihenfolge bestimmt werden. Es stehen mehrere Konfigurationsmöglichkeiten zur Verfügung:

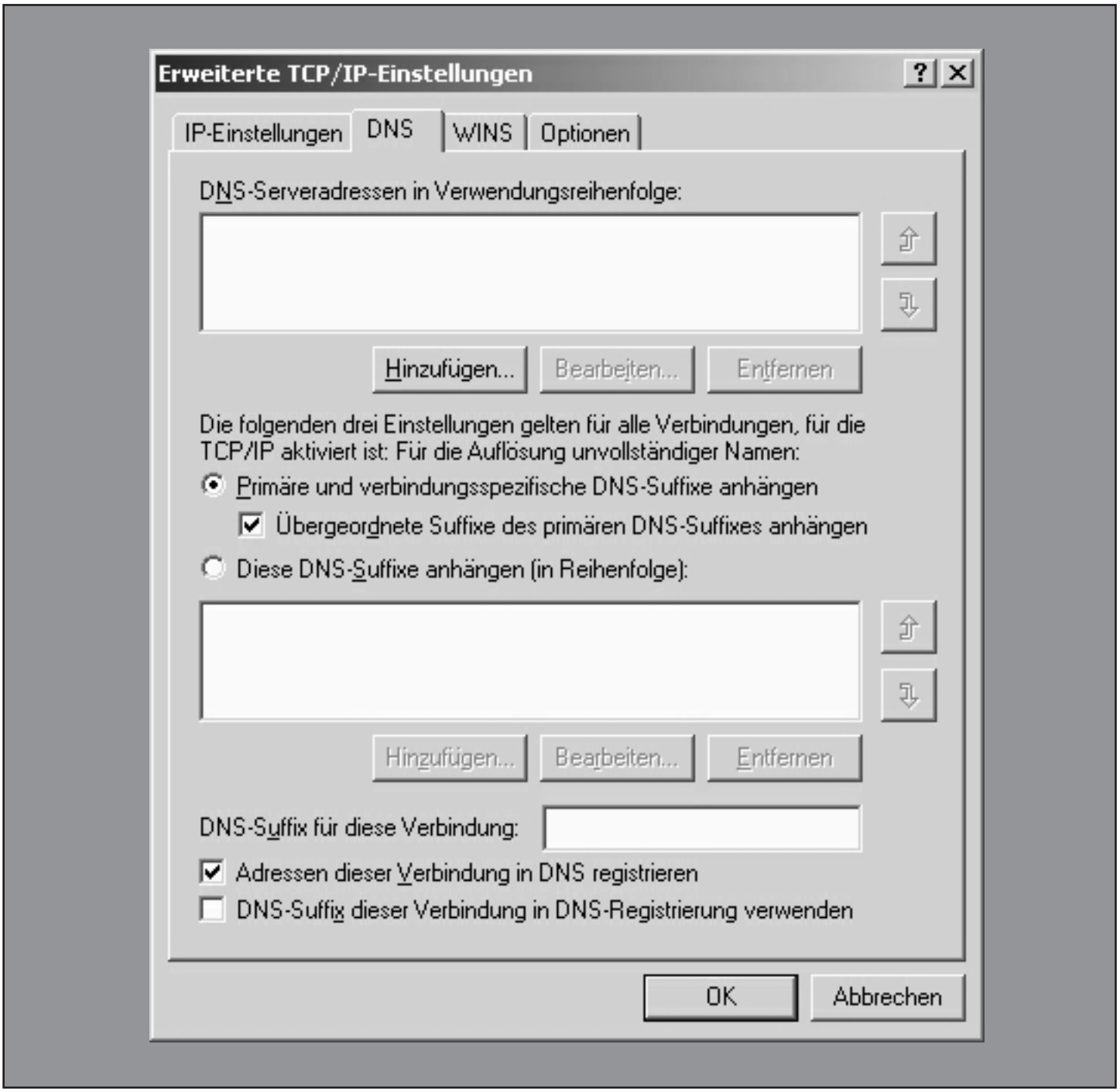
- Primäre und verbindungsspezifische Suffixe anhängen

Zunächst wird das primäre Domänensuffix angehängt. Scheitert diese Abfrage, so wird das für die Netzwerkkarte konfigurierte verbindungsspezifische Suffix aus dem Feld "DNS Suffix für diese Verbindung" dem unvollständigen Namen angehängt.

- Diese Suffixe anhängen (in Reihenfolge)

  Hier können Suffixe eingetragen werden, die anstelle des primären bzw. verbindungsspezifischen Suffixes verwendet werden. Die Reihenfolge, in der diese Suffixe verwendet werden sollen kann beeinflusst werden.

Bild 1 Erweiterte TCP/IP Einstellungen eines Windows 2000 Clients



- Übergeordnete Suffixe des primären Suffix anhängen

  Ist diese Option aktiviert, so werden vor dem verbindungsspezifischen Suffix alle dem primären Suffix übergeordneten (aus hierarchischer DNS Sicht) Suffixe angehängt.

  Lautet das primäre Suffix beispielweise auf aachen.deutschland.comconsult.com so lauten die übergeordneten Suffixe wie folgt: deutschland.comconsult.com; comconsult.com. Die übergeordneten Suffixe der TLDs (Top Level Domains = com, net, de, edu, ...) werden nicht angehängt, da dies aus Sicht der Administrationshoheit dieser Domänen keinen Sinn macht.

1.2 DNS Server Unterstützung für "SRV-Einträge"

Das Active Directory von Windows 2000 beruht darauf, dass

- für die Dienste, die von Domänencontrollern zur Verfügung gestellt werden (LDAP, Kerberos, globaler Katalog, etc.) im DNS entsprechende Einträge vorhanden sind und
- dass Clients diese Informationen von einem DNS-Server abrufen können.

Hierzu greift Windows 2000 im DNS auf spezielle Ressourceneinträge des Typs SRV (Dienstressourceneintrag) zurück, die in RFC 2782 und RFC 2052 beschrieben sind.

Mit Hilfe der SRV-Einträge kann der Standort eines Servers für einen bestimmten Dienst oder ein Protokoll in der Domäne bestimmt werden. Die SRV-Einträge beginnen typischerweise mit einem Unterstrich "_". Nachdem ein Windows 2000 Server zum Domänencontroller heraufgestuft wurde, wird von dem auf jedem Server laufenden Dienst "Netlogon" bei jedem Dienststart automatisch versucht, mehrere SRV-Einträge dynamisch im DNS zu registrieren. Active Directory Clients rufen genau diese SRV-Einträge im DNS ab, um die Server lokalisieren zu können, die einen entsprechenden Dienst ausführen (etwa bei der Anmeldung an einer Domäne).

Da jeder Active Directory Domänencontroller beim Start des Netlogon-Dienstes versucht, die ihm zugeordneten SRV-Einträge automatisch beim DNS-Server zu registrieren, sollte der DNS-Server die dynamische Aktualisierung unterstützen. Dies ist jedoch nicht zwingend erforderlich, da die entsprechenden SRV-Einträge auch manuell (oder auch halbautomatisch mit Hilfe eines Skriptes) in das DNS eingepflegt werden können. Auf jedem Domänencontroller ist im Verzeichnis %systemroot%\system32\config die Datei netlogon.dns gespeichert, in der die aktuellen SRV-Einträge BIND-konform hinterlegt sind. Ein Administrator kann diese Datei verwenden, um die darin enthaltenen Einträge in das DNS zu importieren. Ein skriptgesteuerter Import auf einen Microsoft DNS-Server kann mittels des Tools dnscmd.exe aus den Windows 2000 Support Tools oder dem Windows NT Server Ressource Kit erfolgen. Wird die dynamische DNS-Aktualisierung nicht verwendet, so müssen die entsprechenden SRV-Einträge bei jeder Änderung (Verlagerung eines Dienstes auf einen anderen Domänencontroller, Hinzukommen eines neuen Domänencontrollers, Änderung der Site-Topologie, etc.) im Active Directory aktualisiert werden. SRV-Einträge werden sowohl vom Windows 2000- als auch vom Windows NT 4.0(ab Service Pack 4)- DNS-Server unterstützt.

1.3 SRV-Einträge

Aus Sicht des DNS sind die SRV-Einträge der zentrale Dreh- und Angelpunkt für das Active Directory. Da das Active Directory ohne SRV-Einträge nicht lauffähig ist, wird nachfolgend das Format dieser Einträge beschrieben und alle für das Active Directory relevanten SRV-Einträge werden erläutert (siehe Kasten 1: SRV-Einträge für das Active Directory).

Kasten 1a SRV-Einträge für das Active Directory

Ein Domänencontroller, der der erste Domänencontroller der Gesamtstruktur ist und der mit Windows NT kompatiblen Berechtigungen (PDC-Emulation) konfiguriert wird, würde die nachfolgenden SRV-Einträge im DNS registrieren (hier sind nur die Felder _Dienst._Protokoll.Name aufgeführt, da die anderen Felder alle gleich besetzt wären):

_ldap._tcp.<DnsDomainName>

Ermöglicht einem Client, einen LDAP-Server in der durch <DnsDomainName> angegebenen Domäne zu finden. Wird von allen Windows 2000 Domänencontrollern registriert.

_ldap._tcp.<Standortname>._sites.<DnsDomainName>

Ermöglicht einem Client, einen LDAP-Server in der durch <DnsDomainName> angegebenen Domäne am Standort <Standortname> zu finden. Wird von allen Windows 2000 Domänencontrollern registriert.

_ldap._tcp.dc._msdcs.<DnsDomainName>

Ermöglicht einem Client, einen Domänencontroller (dc) der durch <DnsDomainName> angegebenen Domäne zu finden. Wird von allen Windows 2000 Domänencontrollern registriert.

_ldap._tcp.<Standortname>._sites.dc._msdcs.<DnsDomainName>

Ermöglicht einem Client, einen Domänencontroller der durch <DnsDomainName> angegebenen Domäne am Standort <Standortname> zu finden. Wird von allen Windows 2000 Domänencontrollern registriert.

_ldap._tcp.pdc._msdcs.<DnsDomainName>

Ermöglicht einem Client, den primären Domänencontroller (pdc) der durch <DnsDomainName> angegebenen "gemischten Domäne" zu finden. Nur der PDC Emulationsmaster registriert diesen Namen.

_ldap._tcp.gc._msdcs.<DnsForestName>

Ermöglicht einem Client, einen globalen Katalogserver (gc) für die Gesamtstruktur zu finden. Nur ein Domänencontroller, der als globaler Katalogserver der Gesamtstruktur mit dem Namen <DnsForestName> dient, registriert diesen Namen.

_ldap._tcp.<Standortname>._sites.gc._msdcs.<DnsForestName>

Ermöglicht einem Client, einen globalen Katalogserver für die Gesamtstruktur zu finden, der sich am Standort <Standortname> befindet. Nur ein Domänencontroller, der als globaler Katalogserver der Gesamtstruktur mit dem Namen <DnsForestName> dient, registriert diesen Namen.

_gc._tcp.<DnsForestName>

Ermöglicht einem Client, einen globalen Katalogserver für die Gesamtstruktur zu finden. Nur ein LDAP-Server, der den globalen Katalog der Gesamtstruktur mit dem Namen <DnsForestName> bedient, registriert diesen Namen. Der Server ist nicht unbedingt ein Domänencontroller.

_gc._tcp.<Standortname>._sites.<DnsForestName>.

Ermöglicht einem Client, einen globalen Katalogserver für die Gesamtstruktur zu finden, der sich am Standort <Standortname> befindet. Nur ein LDAP-Server, der den globalen Katalog der Gesamtstruktur mit dem Namen <DnsForestName> bedient, registriert diesen Namen. Der Server ist nicht unbedingt ein Domänencontroller.

_ldap._tcp.<DomainGuid>.domains._msdcs.<DnsForestName>.

Ermöglicht einem Client, einen Domänencontroller in einer Domäne mit einem GUID (Globally Unique Identifier) <DomainGuid> zu finden.

_kerberos._tcp.<DnsDomainName>

Ermöglicht einem Client, ein Kerberos-Schlüsselverteilungscenter (Key Distribution Center, KDC) für die Domäne zu finden. Alle Domänencontroller, die den Kerberos-Dienst anbieten, registrieren diesen Namen. Der Server ist nicht notwendigerweise ein Domänencontroller. Wird von allen Windows 2000 Domänencontrollern registriert, auf denen der KDC Dienst ausgeführt wird.

_kerberos._udp.<DnsDomainName>

Entspricht _kerberos._tcp.<DnsDomainName>, nur wird UDP impliziert.

_kerberos._tcp.<Standortname>._sites.<DnsDomainName>

Ermöglicht einem Client, ein Kerberos-Schlüsselverteilungscenter für die Domäne mit dem Namen <DnsDomainName> zu finden, das sich am Standort <Standortname> befindet. Der Server ist nicht notwendigerweise ein Domänencontroller. Wird von allen Windows 2000 Domänencontrollern registriert, auf denen der KDC Dienst ausgeführt wird.

Kasten 1b SRV-Einträge für das Active Directory

_kerberos._tcp.dc._msdcs.<DnsDomainName>

Ermöglicht einem Client, einen Domänencontroller zu finden, auf dem ein Windows 2000-basiertes Kerberos-Schlüsselverteilungscenter für die Domäne mit dem Namen <DnsDomainName> ausgeführt wird. Wird von allen Windows 2000 Domänencontrollern registriert, auf denen der KDC Dienst ausgeführt wird.

_kerberos._tcp.<Standortname>._sites.dc._msdcs.<DnsDomainName>

Ermöglicht einem Client, einen Domänencontroller zu finden, auf dem ein Windows 2000-basiertes Kerberos-Schlüsselverteilungscenter für die Domäne mit dem Namen <DnsDomainName> ausgeführt wird und der sich am Standort mit dem Namen <Standortname> befindet. Wird von allen Windows 2000 Domänencontrollern registriert, auf denen der KDC Dienst ausgeführt wird.

_kpasswd._tcp.<DnsDomainName>

Ermöglicht einem Client, einen Kerberos-Kennwortänderungsserver für die Domäne zu finden. Alle Server, die den Kerberos-Kennwortänderungsdienst anbieten, registrieren diesen Namen. Der Server ist nicht notwendigerweise ein Domänencontroller. Alle Windows 2000 Domänencontroller, auf denen der Kerberos KDC-Dienst ausgeführt wird, registrieren diesen Namen.

_kpasswd._udp.<DnsDomainName>

Entspricht _kpasswd._tcp.<DnsDomainName>, nur wird UDP impliziert.

Kasten 1c SRV-Einträge für das Active Directory

Für SRV-Einträge wird das folgende Format verwendet:

_Dienst._Protokoll.Name TTL Klasse SRV Priorität Gewichtung Port Ziel

- Das Feld _Dienst legt den Namen des Dienstes fest [LDAP (_ldap), globaler Katalog (_gc), Kerberos (_kerberos)].
- Über das Feld _Prokokoll wird das verwendete Protokoll festgelegt (z. B. TCP oder UDP).
- Das Feld Name bestimmt den (Active Directory) Domänennamen, auf den sich der Ressourceneintrag bezieht.
- Das Feld TTL gibt die Gültigkeitsdauer (Time To Live) an, wie viele Sekunden der DNS-Server oder der Auflösungsdienst diesen Eintrag zwischenspeichern soll.
- Das Feld Klasse definiert die Protokollfamilie (IN für das Internetsystem).
- Durch das Feld Priorität wird die Rangfolge für den Host bestimmt. Bieten mehrere Hosts den gleichen Dienst an, so wird vom Client der Host mit der niedrigsten Priorität angesprochen. (Prioritätswert: von 0 bis 65535)
- Mit Hilfe des Feldes Gewichtung kann ein Lastenausgleich erzielt werden. Ist das Prioritätsfeld für zwei oder mehr Einträge in der Domäne gleich, so versuchen Clients häufiger auf die Einträge mit der höheren Gewichtung zuzugreifen. (Gewichtungswert: 0 bis 65535)
- Mit dem Feld Port wird der Anschluss für den Dienst auf dem Host spezifiziert.
- Das Feld Ziel gibt den FQDN des Hosts an, der den Dienst anbietet.Bei genauerer Betrachtung der aufgelisteten SRV-Einträge (siehe Kasten) fällt auf, dass in einigen Einträgen die Komponente .<Standortname>._sites enthalten ist, die die im Active Directory definierten Standorte (Sites) wiedergibt. Mit Hilfe dieser Komponente ist es möglich, den Host zu ermitteln, der sich im gleichen Standort wie der anfragende Client/ Server befindet.

Die Teildomäne _msdcs hält Informationen für die Suche nach Domänencontrollern vor, die in der Domäne / Gesamtstruktur Windows 2000-spezifische Rollen übernehmen. Dies sind Domänencontroller (dc), Globaler Katalogserver (gc) und Primärer Domänencontroller Emulator (PDC-Emulator). Innerhalb dieser Teildomäne, ist auch die Suche nach der GUID der Domäne (Globally Unique Identifier, wird vom Active Directory jedem neuen Objekt zugewiesen; ist ein 128 Bit Wert; wird zur Identifikation verwendet) möglich, für den Fall, dass die Domäne umbenannt wurde. Eine Domänen-Namensänderung sollte nur im aller äußersten Notfall geschehen und widerspricht der ersten Anforderung, dass eine AD-Domäne eine gleichnamige DNS-Domäne benötigt.

Active Directory verwendet spezielle SRV-Einträge, die Informationen über Dienste in der Gesamtstruktur <DnsForestName> bereitstellen. Diese Informationen werden dazu benötigt, damit Replikationspartner einander finden und Clients die Globalen Katalog-Server lokalisieren können und sie werden in der DNS-Domäne _msdcs.<DnsForestName> gespeichert. Diese Informationen müssen in der in der Gesamtstruktur zur Verfügung gestellt werden und daher sollte diese Domäne nach Möglichkeit auf allen DNS-Servern der Gesamtstruktur zur Verfügung gestellt werden (siehe Bild 2: Verteilung der delegierten Domäne _msdcs). In der DNS-Domäne Konzern.de wurde eine Delegierung der DNS-Domäne _msdcs.Konzern.de (diese entspricht der Domäne _msdcs.<DnsForestName>) vorgenommen, um eine eigene Zone für diese Domäne zu erhalten, die dann als sekundäre Zone auf alle weiteren DNS-Server der Gesamtstruktur repliziert wird. Diese Vorgehensweise ist nicht zwingend erforderlich, reduziert jedoch ggf. deutlich die standortübergreifenden DNS-Abfragen.

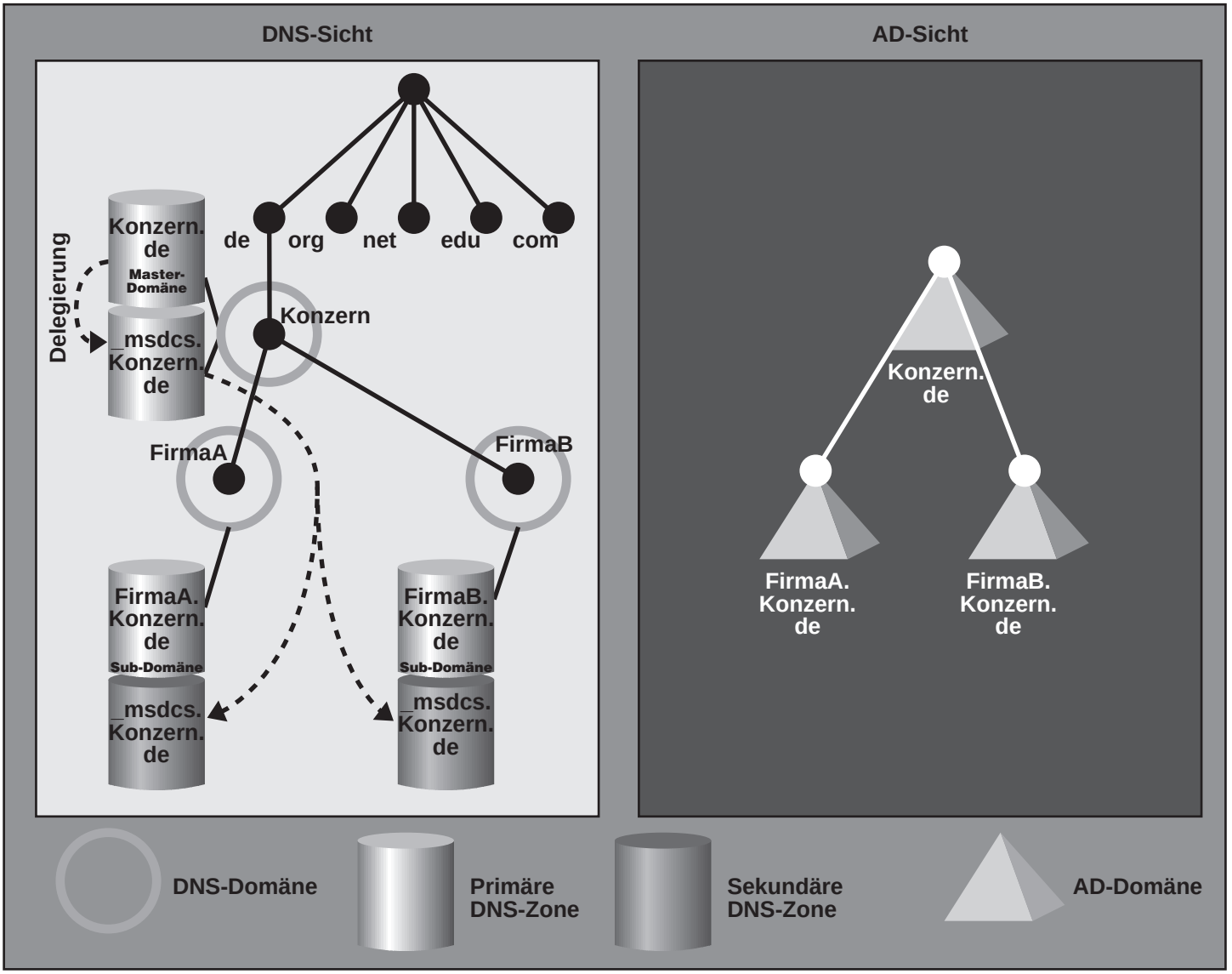


Bild 2 Verteilung der delegierten Domäne _msdcs

Vom Netlogon-Dienst eines Domänencontrollers werden bei dessen Start noch weitere Einträge im DNS hinzugefügt. Dies sind nur A-Ressourceneinträge, die von LDAP-Clients verwendet werden können, die keine SRV-Einträge unterstützen.

- DnsDomainName
  Ermöglicht einem Client, einen beliebigen Domänencontroller in der Domäne über eine normale A-Eintragssuche zu finden.

- gc._msdcs.<DnsForestName>
  Ermöglicht einem Client, einen beliebigen globalen Katalog in der Gesamtstruktur über eine normale A-Eintragssuche zu finden.

- <DsaGuid>._msdcs.<DnsForestName>
  Ermöglicht einem Client, einen beliebigen Domänencontroller in der Gesamtstruktur über eine normale A-Eintragssuche zu finden. Die einzigen bekannten Informationen zum Domänencontroller sind der GUID für den Domänencontroller und der Name der Gesamtstruktur, in der sich der Domänencontroller befindet. Dieser Name wird verwendet, um die mögliche Umbenennung eines Domänencontrollers zu vereinfachen.

Fazit

Die DNS-Server-Implementierung für das Active Directory muss zwingend SRV-Einträge unterstützen. Ist dies nicht der Fall, kann das Active Directory nicht verwendet werden. Das dynamische DNS Update muss von der DNS-Server-Implementierung nicht unterstützt werden, ist aber zumindest für den Bereich der SRV-Einträge äußerst empfehlenswert und minimiert insgesamt den administrativen Aufwand. Fasst man an dieser Stelle zusammen, so kann definiert werden, dass es zwei zwingende Anforderungen gibt a) SRV-Einträge müssen unterstützt werden und b) für eine AD-Domäne benötigt man eine gleichnamige DNS-Domäne. Eine je nach DNS-Implementierung zu bewertende fast zwingende Anforderung ist jedoch zusätzlich die Dynamik, die zumindest für Teilbereiche erforderlich ist.

Nachdem nun die grundsätzlichen Anforderungen seitens des AD definiert wurden, sollte im nächsten Schritt die Planung des Namensraums für das Inter- und Intranet folgen. Dies ist sicherlich auch ein Thema für die eingangs beschriebene Runde, die dann auch noch um politische Entscheider erweitert werden sollte.

2
Namensraum intern / extern

Bei der DNS Planung sollte grundsätzlich sichergestellt werden, dass der Entwurf die folgenden Anforderungen erfüllt:

- Nur der öffentliche Teil des Namensraums der Organisation sollte im Internet sichtbar gemacht werden. Dies dient dem Schutz vor unerwünschten externen Angriffen.
- Allen Clients sollte ermöglicht werden, sowohl die öffentlichen als auch die privaten Ressourcen der Organisation auflösen zu können.
- Clientcomputer, die einen Zugriff auf das Internet benötigen, sollten alle Internetnamen auflösen können.

2.1
Entwerfen einer DNS-Benennungsstrategie für Active-Directory / Internet

Die DNS-Namensauflösung wird für die IP-basierte Kommunikation sowohl im Internet (öffentliches Netzwerk) als auch im Intranet (privates Netzwerk) verwendet.

Viele Firmen präsentieren sich heutzutage im Internet. Um dies zu ermöglichen, ist es notwendig, dass die Firmen eine registrierte DNS-Stammdomäne besitzen. Diese Stammdomäne kann bei der ICANN (Internet Corporation for Assigned Names and Numbers) registriert werden. Durch die Registrierung wird die weltweite Eindeutigkeit aller DNS-Namen gewährleistet. Weiterhin erhält man durch die Registrierung die Befugnis zur Verwaltung einer eigenen Hierarchie mit untergeordneten Domänen, Zonen und Hosts innerhalb der Stammdomäne.

In einem Windows 2000 Netzwerk (privates Netzwerk) legt Active Directory DNS-Standards bei der Benennung von Domänen, Servern und Diensten zugrunde. Active Directory verwendet zudem DNS als Domänensuchdienst.

Wird beabsichtigt, die Organisation im Internet darzustellen, so ist zu entscheiden, ob die intern zugänglichen Ressourcen (privates Netzwerk) von solchen Ressourcen getrennt werden, auf die ein externer Zugriff möglich ist (öffentliches Netzwerk), oder ob dies nicht der Fall sein soll. Nachfolgend werden drei unterschiedliche Ansätze vorgestellt, sowie deren Vor- und Nachteile dargestellt.

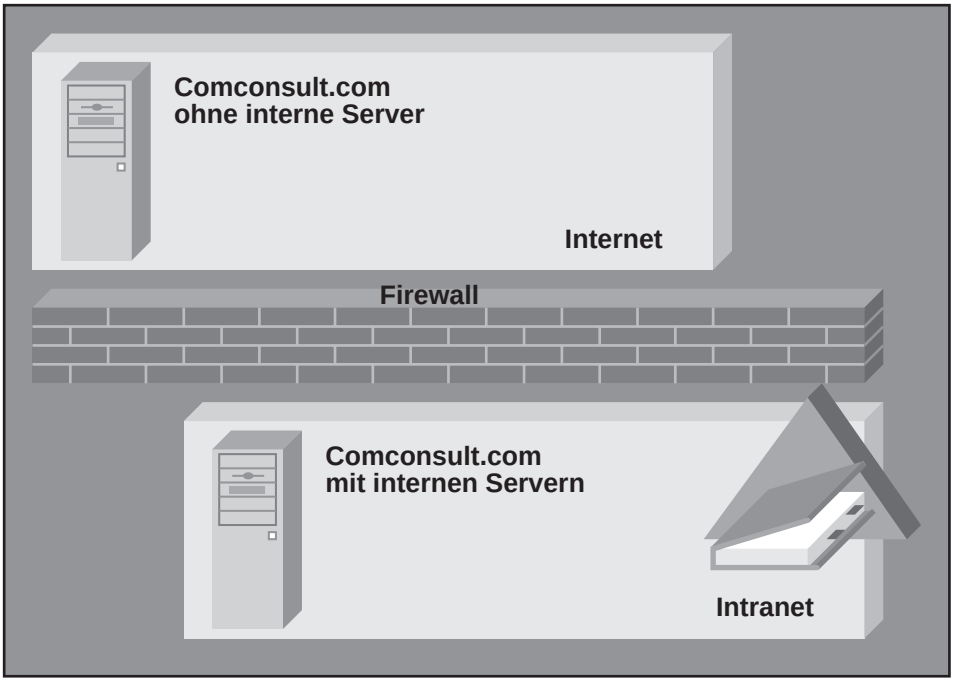


Bild 3 Gleiche Namen für Inter-/Intranet

Verwendung des gleichen Domänennamens für Internet & Intranet

Für das öffentliche und das private Netzwerk können gleiche Domänennamen verwendet werden, wobei die Trennung der beiden Bereiche hierbei sichergestellt sein sollte.

In der oben dargestelltem Konstellation verwaltet der DNS-Server im öffentlichen Netzwerk nur Einträge von Hosts, die vom Internet her zugänglich sind. Die DNS-Server im internen Netzwerk verwalten Ressourceneinträge, die allen internen Hosts zur Verfügung gestellt werden (incl. aller Active Directory-spezifischen Einträge).

Bei Verwendung dieser Konstellation ergeben sich folgende Auswirkungen:

- Die Benutzer brauchen sich nur einen Domänennamen zu merken, um auf Ressourcen im Internet bzw. im privaten Netzwerk zuzugreifen.
- Es muss nur eine Domäne (hier: Comconsult.com) registriert werden.
- Es wird eine erhöhte Administration des DNS benötigt, um sicherzustellen, dass auf den Servern alle relevanten Einträge – aber auch nur diese – zur Verfügung stehen. Es muss sichergestellt werden, das keine Informationen des privaten Netzwerkes nach außen gelangen.
- Die Konfiguration der Firewall wird komplexer, wenn das private Netzwerk vor dem Zugriff über das Internet geschützt werden soll.
- Die Datensynchronisierung kann aufwendiger werden, wenn externe Ressourcen ins private Netzwerk gespiegelt werden.

Verwendung einer delegierten untergeordneten Domäne für das Intranet

Anstatt den registrierten, externen DNS-Domänennamen der Organisation als Stammdomäne des Active Directory zu verwenden, kann auch eine untergeordnete Domäne als Stamm für das Active Directory dienen. Die registrierte Domäne wird hierbei für das öffentliche Netzwerk verwendet.

Diese Aufteilung hat folgende Auswirkungen:

- Active Directory-Daten verbleiben in der entsprechenden Domäne bzw. Domänenstruktur.
- Es wird ein zusammenhängender Namensraum bereitgestellt, der für Administratoren und Benutzer weniger verwirrend ist.

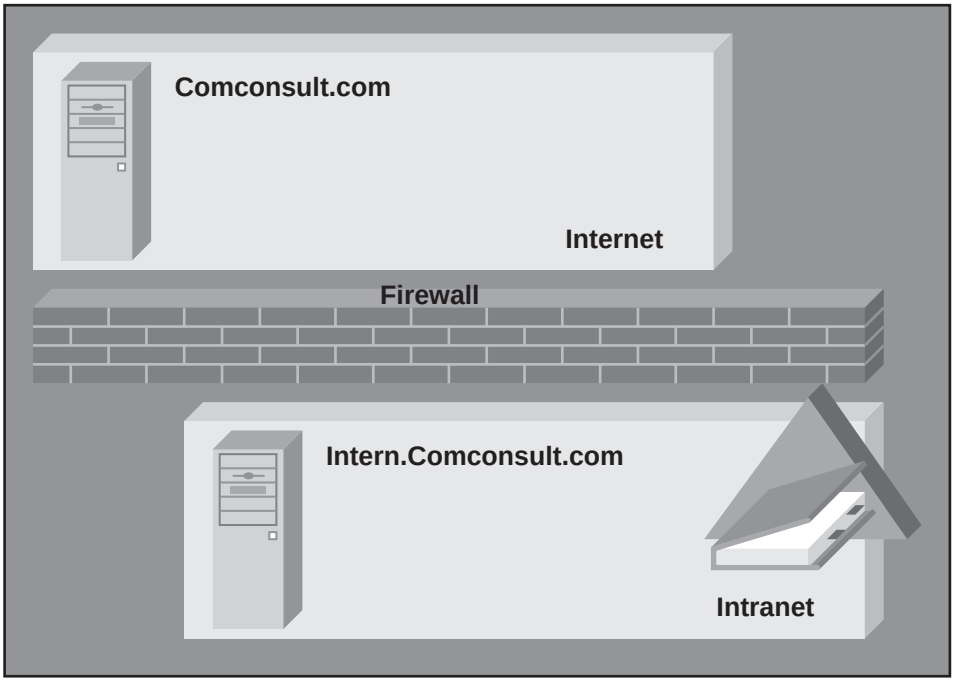


Bild 4 Delegierte untergeordnete Domäne für das Intranet

- Es muss nur die externe Domäne registriert werden.
- Für die delegierte Active Directory Domäne wird ein eigener DNS-Server benötigt. Die schon vorhandenen Server für die Internetdomäne können beibehalten werden.
- Die Active Directory Namensstruktur ist länger, da sie erst auf der dritten Ebene beginnt.

Verwendung unterschiedlicher DNS-Namen für Internet & Intranet

Es ist weiterhin möglich, vollkommen unterschiedliche Domänennamen für das öffentliche und das private Netzwerk zu verwenden.

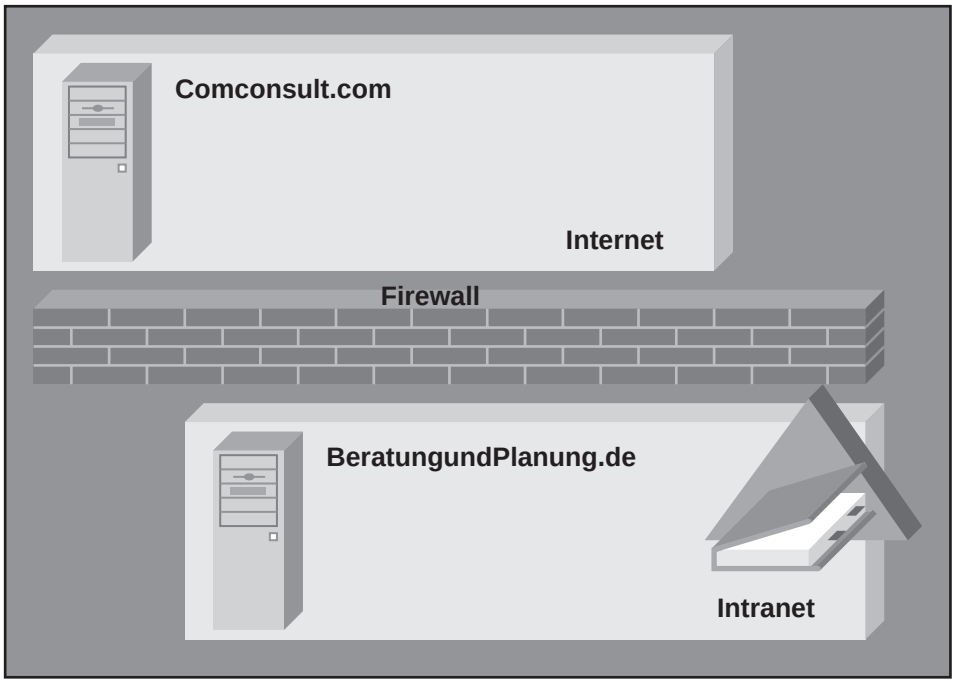
Durch die Verwendung unterschiedlicher DNS-Namen für das öffentliche und das private Netzwerk erfolgt eine saubere Trennung der externen von den internen Ressourcen.

Will man den Clients ermöglichen, externe Namen sowohl für die Organisation als auch für andere Internethosts aufzulösen, so kann man die internen DNS-Server so konfigurieren, dass sie alle Anforderungen, die sie nicht auflösen können, an den externen DNS-Server weiterleiten. Bei Verwendung von Proxy-Clients muss eine Ausschlussliste definiert werden.

Die Verwendung unterschiedlicher DNS-Namen für das öffentliche und das private Netzwerk hat folgende Auswirkungen:

- Eine klare Trennung zwischen den privaten und öffentliche Ressourcen hat zur Folge, dass Ressourcen leichter verwaltet und geschützt werden können.
- Es muss (formell) nur die Domäne für das öffentliche Netzwerk registriert werden. Es wird jedoch empfohlen, auch den DNS-Namen der internen Domäne registrieren zu lassen, da ungewiss ist, welche Anforderungen (z.B. durch neue Betriebssysteme, etc.) in Zukunft gestellt werden.
- Die interne Namenshierarchie wird bei Zugriffen über das Internet nicht offen gelegt.
- Unter Verwendung des externen Domänennamens ist es nicht möglich vom Internet aus auf die internen Ressourcen zuzugreifen.
- Die unterschiedlichen Namen können bei einigen Benutzern zu Verwirrungen führen, wenn diese versuchen über das Internet auf eine Unternehmensressource zuzugreifen.
- Der administrative Aufwand kann steigen, da es z.B. Unterschiede zwischen den E-Mail-Namen und den Active Directory Namen eines Benutzers gibt.

Bild 5 Unterschiedliche Namen für Inter-/Intranet



2.2 Verwendung eines internen DNS-Stamms

Für die Fälle, dass das Intranet nicht mit dem Internet verbunden ist oder eine Internetnamensauflösung über einen anderen Weg als über den DNS-Server für das Active Directory bereitgestellt werden kann (z.B. bei Verwendung von Proxy-Servern), besteht die Möglichkeit der Verwendung eines internen DNS-Stamms (der Punkt "."). Damit wird der private Namensraum genauso strukturiert, wie dies auch im Internet der Fall ist: Es gibt im privaten Namensraum eine Stammdomäne ".", je nach Konfiguration eine oder mehrere Top-Level-Domänen (de, edu, com, etc.) sowie die Domänen des Active Directory.

Bei dieser Konstellation wäre es möglich, für die Active Directory Stammdomäne einen DNS-Namen zu wählen, der einer frei wählbaren Top-Level-Domäne entspricht (z.B. ADComconsult.).

Da es keine Interaktion zwischen den DNS-Servern für das Active Directory und DNS-Servern im Internet gibt, kann der Name frei gewählt werden und muss sich nicht an den Top-Level-Domänen des Internets orientieren. Der DNS-Stamm (also der Punkt ".") kann jedoch nicht als DNS-Name für die Active Directory Stammdomäne verwendet werden.

Vorteilhaft an der Verwendung einer internen DNS-Stammdomäne ist, dass alle untergeordneten internen DNS-Server so konfiguriert werden können, dass sie DNS-Abfragen, die sie nicht aufgrund ihrer vorgehaltenen Zonen oder ihres Caches beantworten können, ohne den Eintrag eines Forwarders an die Server weiterleiten, die die Stammzone vorhalten (Stammserver).

Welche Server die Stammserver sind, ist dem DNS-Server aus der Datei cache.dns, die sich im Ordner %systemroot%\system32\dns (bei Windows) befindet, oder aus dem Active Directory bekannt.

In der Standardeinstellung eines Windows 2000 DNS-Servers werden die Hinweise auf die Stammserver aus dem Active Directory oder falls dort keine Informationen vorhanden sind aus der Datei cache.dns entnommen.

Die Hinweise auf die Stammserver werden bei der Installation des DNS-Servers bzw. des Active Directory eigenständig angelegt. Sie können aber auch manuell editiert werden.

3 Design-Entscheidungen und Lösungsansätze

Nach der Definition der Inter-/Intranetstruktur und ggf. der Verwendung des internen Punktes, folgt die entscheidende Designphase. Genau in dieser Phase werden häufig Fehler gemacht, die im derzeitigen Release von Windows 2000 Active Directory nicht mehr so leicht zu beheben sind, denn nur bei der Konfiguration der Domänencontroller (dcpromo.exe) können Strukturen definiert werden. Änderungen an bestehenden Strukturen können derzeit nur durch Neuinstallationen der Domänen erfolgen. Bei der Implementierung des AD muss immer die "oberste" Domäne zuerst installiert werden, also beispielsweise comconsult.com. Möchte man weitere Subdomänen implementieren, wie z.B. backoffice.comconsult.com, so kann dies nur geschehen, wenn die "oberste" Domäne, nämlich die AD-Root-Domäne (comconsult.com), vorhanden ist. Weitere Subdomänen erfordern immer die nächst höhere Domäne.

Eine Namensänderung der AD-Root-Domäne hat prinzipiell zur Folge, dass die gesamte Struktur neu aufgebaut werden muss.

Entscheidend für die AD-Domänenintegration sind die ersten Eingabemasken des dcpromo ("Assistent zum Installieren von Active Directory"), in denen man folgendes festlegen kann:

- Im ersten Fenster kann man definieren, ob man eine neue Domäne anlegen möchte oder ob der DC zu einer bestehenden Domäne hinzugefügt werden soll.
- Im zweiten Fenster kann man definieren, ob man eine neue Domänenstruktur oder eine neue untergeordnete Domäne (Subdomäne) erstellen möchte, vorausgesetzt, man hat im ersten Fenster das Anlegen einer neuen Domäne gewählt.
- Im dritten Fenster kann man definieren, ob eine neue Gesamtstruktur erstellt werden soll oder ob diese neue Domäne an einer bestehenden Gesamtstruktur angehängt werden soll, vorausgesetzt man hat im zweiten Fenster das Anlegen einer neuen Domäne gewählt.

In der aktuellen Version des AD können obige Entscheidungen nur in dieser Phase der Installation eines Domänencontrollers erfolgen.

Mit der Auswahl obiger Optionen werden auch die entsprechenden Vertrauensstellungen (trusts) implementiert, die im Gegensatz zu den expliziten Vertrauensstellungen aus den älteren NT-Versionen implizit und transitive sind. Dies hat den Vorteil, dass nicht mehr für alle Domänen, zwischen denen Zugriffe erfolgen sollen, explizite Vertrauensstellungen eingerichtet werden müssen. Betrachtet man z.B. Bild 6, so kann ein Benutzer aus der Domäne Teil1.FirmaA.Konzern.de auf Ressourcen der Domäne Teil3.FirmaB.Konzern.de zugreifen, vorausgesetzt, entsprechende Zugriffsrechte wurden konfiguriert, ohne dass eine explizite Vertrauensstellung zwischen den beiden Domänen besteht. Weiterhin können jedoch auch unter Windows 2000 explizite Vertrauensstellungen eingerichtet werden, deren Einsatz für verschiedene Migrationszenarien erforderlich ist, diese sind dann aber nicht transitiv und ersetzen keinesfalls die impliziten transitiven Vertrauensstellungen.

Die durch den Zeitpunkt der Implementierung von Domänen gegebene nicht vorhandenen Flexibilität muss im AD-Domänen-Design berücksichtigt werden und ist somit eine globale Anforderung an das AD-Domänen-Design und die Namensgebung. Grundsätzlich kann man zwei Ansätze definieren, einen Domänenbaum bzw. Tree und einen Domänenwald bzw. Forest, wobei man "eine" AD-Struktur immer als Gesamtstruktur bezeichnet, unabhängig davon ob es sich um einen Tree oder Forest handelt.

In einem Tree-Design gibt es die AD-Root-Domäne und eine äquivalente DNS-Domäne, von denen alle anderen Domänen im Namensraum abgeleitet werden, siehe Bild 6. Dieses Design besitzt folgende Eigenschaften:

- Nutzung der hierarchischen DNS-Strukur.
- Verwendung eines durchgängigen und zusammenhängenden Namensraums.
- Registrierung nur einer Domäne.
- Strukturen können nachgebildet werden, wobei eine unterschiedliche Anzahl von Stufen in den verschiedenen Ästen möglich ist.

Vorteilhaft scheint die Übernahmemöglichkeit bestehender DNS-Strukturen, wobei der Grad der Flexibilität immer in Abhängigkeit von der AD-Root-Domäne zu sehen ist. Natürlich kann die AD-Root-Domäne auch eine untergeordnete Domäne des DNS-Trees sein, beispielsweise AD.konzern.de. Die Alternative bzw. die Ergänzung zum Tree stellt die Implementierung eines Forests dar.

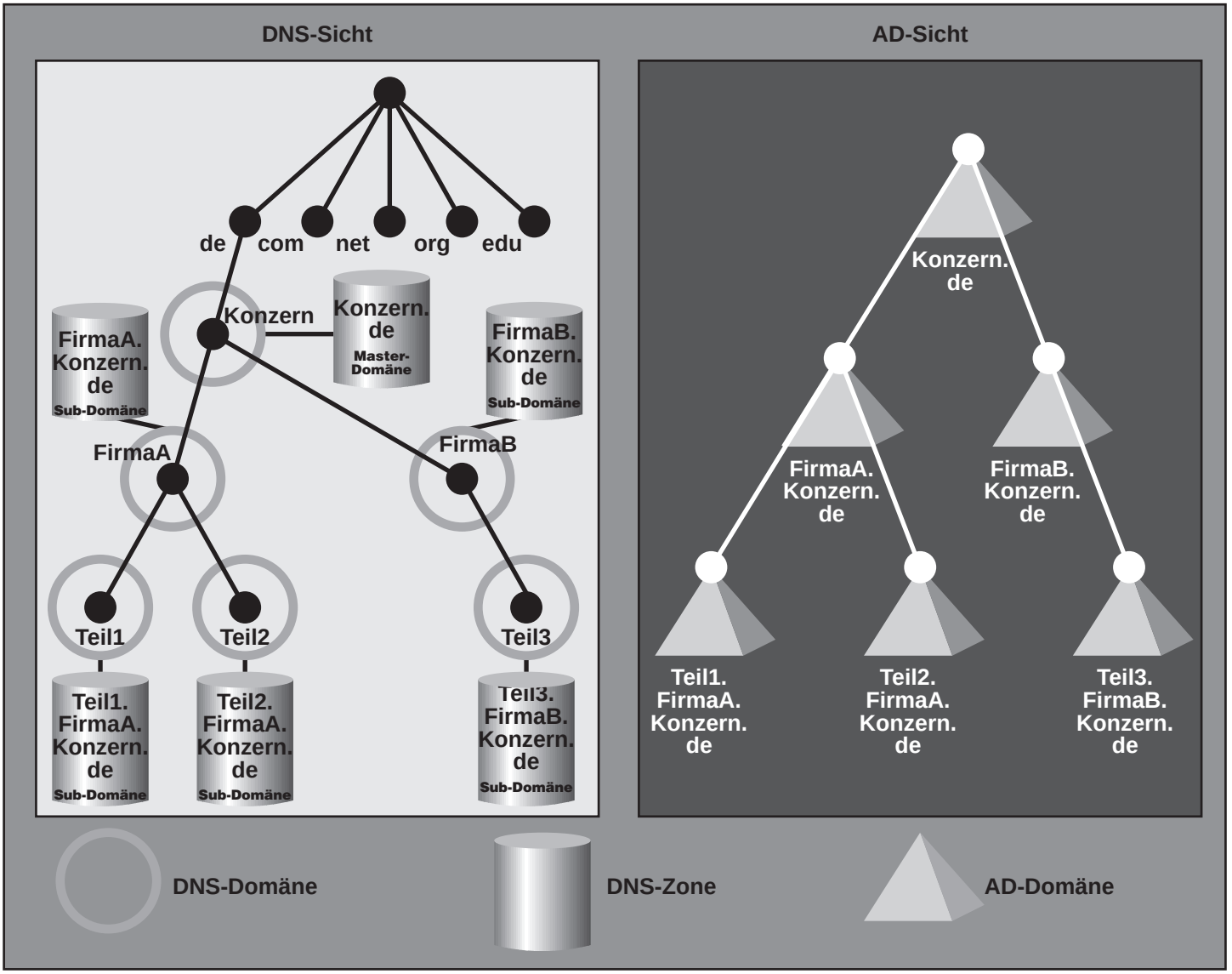


Bild 6 Tree bzw. Domänenbaum aus DNS- und AD-Sicht

Wie in Bild 7 zu sehen, gibt es bei einem AD-Forest-Design einen entscheidenden Unterschied zum DNS-Design. Im DNS hängen die Domänen der zweiten Ebene, also soche, die für eine Unternehmung registriert werden können, von den Top-Level-Domains (com, de, net ...) bzw. letztendlich von der DNS-Root dem Punkt ab. Da die DNS-Root bzw. auch die Top-Level-Domains nicht im Administrationsbereich eines Unternehmens liegen, kann die AD-Root-Domäne frühestens auf der zweiten Ebene installiert werden, im Bild FirmaA.com. Dieser Ansatz gilt prinzipiell auch wenn der Punkt "." für das Intranet intern verwaltet wird, siehe 2.2 "Verwendung eines internen DNS-Stamms". Um aber eine Forest-Struktur innerhalb des AD aufzubauen, können sogenannte Peer-Domänen, Domänen auf gleicher Ebene, in die Gesamtstruktur implementiert werden. Dies geschieht ebenfalls während des dcpromo und zwar im beschriebenen dritten Fenster (s.o.). Grundsätzlich besitzt dieses Design folgende Eigenschaften:

- Die Verbindung mehrer Trees ist möglich.
- Es wird aus DNS-Sicht kein durchgängiger und zusammenhängender Namensraum verwendet.
- Verschiedene Corporate Indentities können im AD-Design abgebildet werden.
- Registrierung mehrer Domänen ist erforderlich.
- Strukturen können nachgebildet werden, auch über Einzelunternehmensgrenzen hinaus.

Dieser Ansatz beinhaltet eine höhere Flexibilität, da verschiedenste Unternehmungen im Sinne eines zentralen Ansatzes miteinander verbunden werden können. Wie aus Bild 7 abzuleiten, besteht eine Abhängigkeit von der AD-Root-Domäne. Bevor auf die Besonderheiten der AD-Root-Domäne eingegangen wird, werden folgend einige globale Designkriterien für die Schaffung von Domänen vorgestellt.

- Das Domänendesign sollte sich an administrativen und sicherheitsrelevanten Bereichen orientieren. Die oft verwendete Anlehnung an das Organigramm eines Unternehmens oder eines Konzern wird nicht

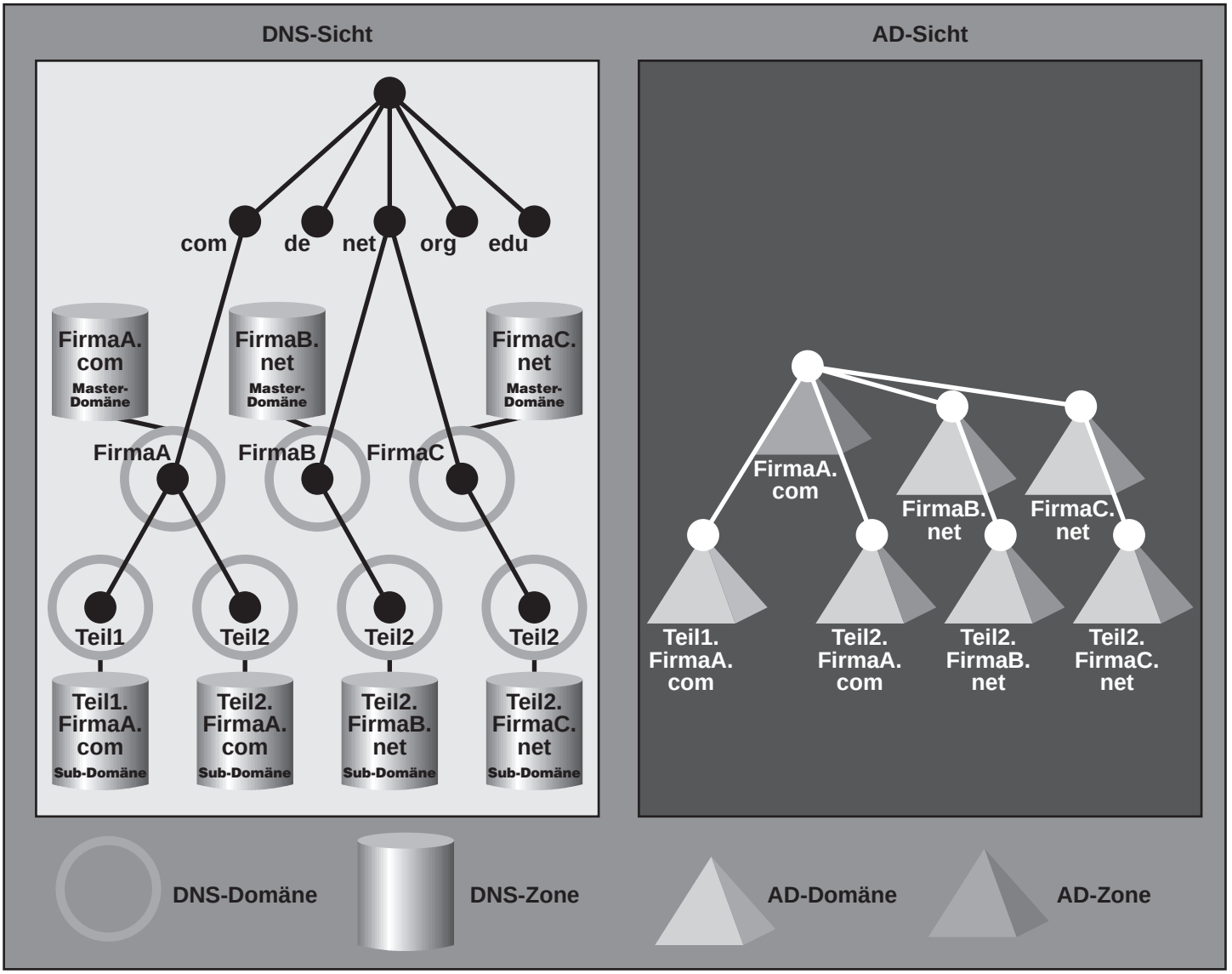


Bild 7 Forest bzw. Domänenwald aus DNS- und AD-Sicht

empfohlen, da diese oft einer zu großen Dynamik unterliegen. Die Orientierung an standortspezifische Gegebenheiten, sofern sie nicht mit administrativen Bereichen übereinstimmen, wird ebenfalls nicht empfohlen, da diese Parameter innerhalb des AD durch das Site(Standort)-Design abgebildet werden können.

- Sofern durchsetzbar, sollte ein möglichst flaches Design angestrebt werden, da innerhalb der Domänen - im Gegensatz zu älteren NT-Versionen - die Implementierung einer Struktur durch das Organisationeinheiten-Design möglich ist und Administrationsaufgaben entsprechend delegiert werden können. Je nach Unternehmen sollte die Planung mit der Prüfung beginnen, ob eine einzelne Domäne ausreicht.
- Aus sicherheitstechnischer Sicht besteht ebenfalls ein sehr entscheidendes Design-Kriterium. Kontorichtlinien (Kennwortrichtlinien, Kontosperrungsrichtlinien und Kerberos-Richtlinien) greifen nur auf Domänenebene! Dies ist z.B. ein Punkt, für den die eingangs beschriebene Anwesenheit der Sicherheitsleute erforderlich ist. Sollte auf dieser Ebene kein Konsens geschaffen werden können, so ist für jede unterschiedliche Kontorichtlinie mindestens eine Domäne erforderlich.
- Zur Minimierung der WAN-Belastung könnte es ggf. erforderlich sein, dass Domänen geschaffen werden, jedoch ist dieser Punkt bereits sehr projektspezifisch und ist in Kombination mit anderen Kriterien zu betrachten.
- Keinen Grund für die Schaffung einer neuen Domäne stellt wohl die Speicherkapazität einer AD-Domäne bzw. eines Domänencontrollers dar. War die Größe der Datenbank bei NT 4.0 mit 40 MB doch noch sehr beschränkt, so können beim AD Millionen von Objekten innerhalb einer Domäne verwaltet werden. Bevor die Speichergrenze zum Vorschein kommt, bestimmen vielmehr administrative Gründe die Grenze einer Domäne.

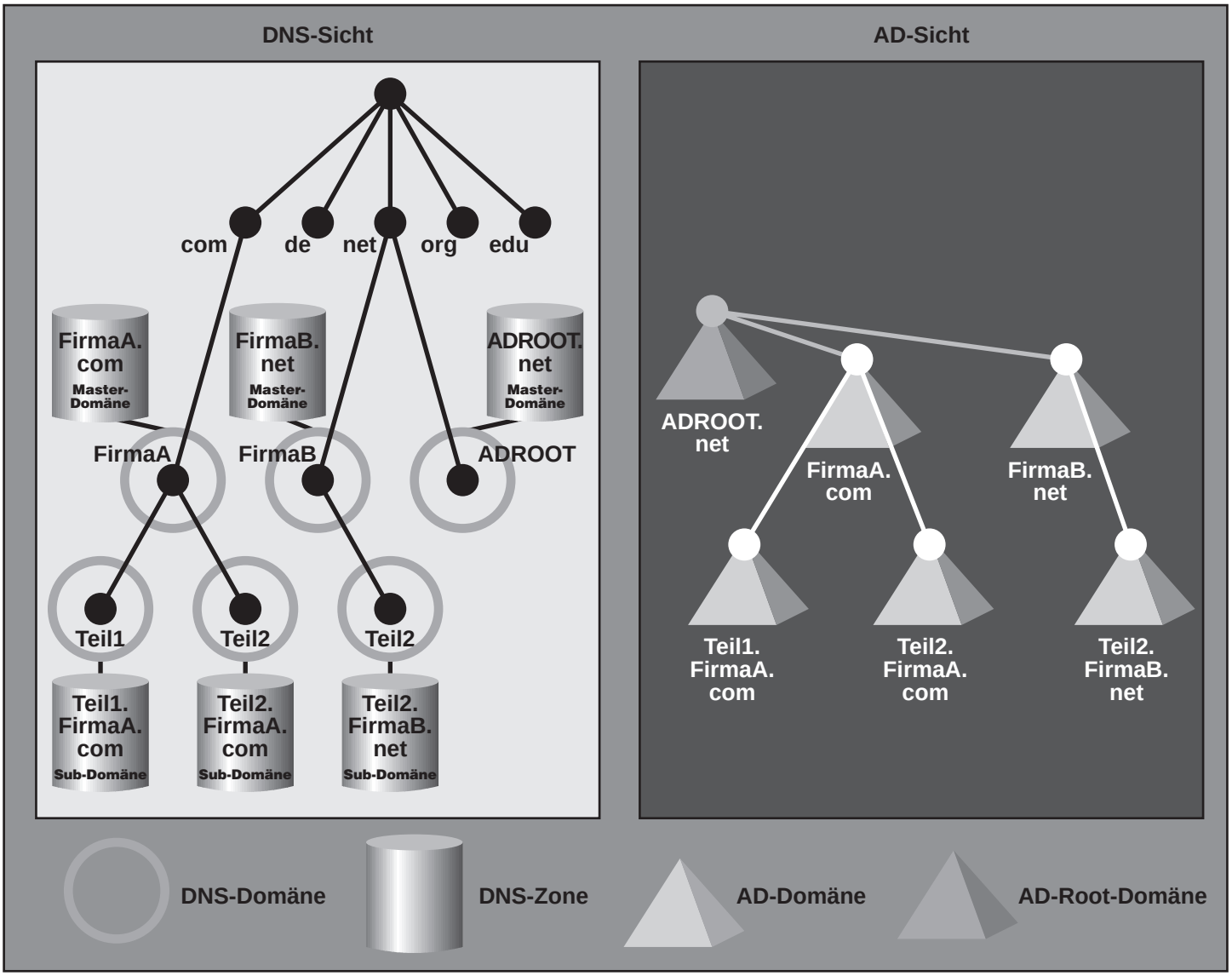
Bei den oben beschriebenen grundsätzlichen Design-Ansätzen Tree und Forest wurde bereits auf die Besonderheit der AD-Root-Domäne hingewiesen, die nun folgend näher betrachtet wird.

In der AD-Root-Domäne gibt es zwei besondere Gruppen: Die Organisations-Admins (Enterprise-Admins) und die Schema-Admins. Diese Gruppen sind sicherheitstechnisch sehr wichtig. Mitglieder der Enterprise-Admins besitzen domänentechnisch die größte Macht und nur diese sind in der Lage, neue Domänen der Gesamtstruktur hinzuzufügen bzw. auch bestehende Domänen zu entfernen. Mitglieder der Gruppe Schema-Admins besitzen insbesondere die Berechtigung, das AD-Schema zu erweitern.

Das Schema des AD, welches nur einmal in der Gesamtstruktur vorhanden ist, bildet die Basis für alle Objekte. Im Schema sind beispielweise alle Objekt- und Attributsklassen definiert, die das AD nutzt. Derzeit kann das Schema ergänzt werden, jedoch können keine Definitionen gelöscht sondern maximal deaktiviert werden. Eine Implementierung von Exchange 2000 beispielsweise verursacht ca. 1.200 Modifikationen am Schema, die dann natürlich auch entsprechend auf alle Domänencontroller repliziert werden müssen. Auf Grund dieser Tatsachen ist das Schema bzw. somit die Gruppe der Schema-Admins besonders schützenswert und sicherheitsrelevant.

Ebenfalls sehr wichtig ist, dass sich die Domänen-Admins der AD-Root-Domäne zu Mitgliedern beider Gruppen machen können, so dass sich die beschriebene Sicherheitsrelevanz auf die gesamte Domäne erstreckt. Um diese Domäne entsprechend zu schützen, sollte sie isoliert werden - man spricht dann von einer dedizierten AD-Root-Domäne. Die dedizierte AD-Root-Domäne zeichnet sich dadurch aus, dass nur die Standard-Benutzer- und Computer-Konten enthalten sind und keine weiteren Konten. Prinzipiell kann sie in eine Tree-Struktur und Forest-Struktur implementiert werden. Wird sie jedoch in einem Tree-Design verwendet, so kommt eine weitere Ebene hinzu und der Name wird länger, auch kann kein "Fantasiename" verwendet werden, da sie dann Vorgaben für den gesamten Namensraum schafft. Viel interessanter ist die Implementierung einer dedizierten AD-Root-Domäne in eine Forest-Struktur wie in Bild 8 dargestellt.

Bild 8 Forest bzw. Domänenwald mit dedizierter AD-Root-Domäne aus DNS- und AD-Sicht



Wie bereits aus Bild 8 abzuleiten, bringt eine dedizierte AD-Root-Domäne neben den sicherheitstechnischen Vorteilen auch den entscheidenden Flexibilitätsvorteil. Sollten neue Firmen zur Unternehmung hinzustossen und sollen diese in die Gesamtstruktur integriert werden, so kann dies geschehen, ohne die bestehende Gesamtstruktur zu verändern. Auch kann man die Coporate Indentity der hinzugekommenen Firma beibehalten, so dass auch politische Flexibilität gegeben ist.

Bei einem AD-Domänen-Design sollte immer die Implementierung einer dedizierten AD-Root-Domäne geprüft werden.

Derzeit scheint dies das Höchstmaß an Flexibilität zu sein, was beim AD-Domänen-Design möglich ist, auch wenn dazu zwei zusätzliche Domänencontroller erforderlich sind, was die Kosten in die Höhe treibt. Der Preis ist jedoch mehr als gerechtfertigt. Nicht vergessen sollte man in diesem Zusammenhang, dass diese Flexibilität "nur" bei der Implementierung neuer Domänen besteht. Fällt eine Firma aus dem Unternehmensverbund weg, so hat diese das Problem, dass sie mit der aktuellen Implementierung vom AD eine neue Struktur aufbauen muss, da ja wie beschrieben immer von der AD-Root-Domäne aus eine Struktur aufgebaut wird.

Prinzipiell bietet die im folgende Kapitel beschriebene "ungleiche Aufteilung" noch einen weiteren Ansatz zur Flexibilitätssteigerung, jedoch sollte von vorneherein geprüft werden, ob dieser Ansatz nicht zu umgehen ist.

4 Ungleiche Aufteilung

Standardmäßig müssen die Attribute DNS-Host-Name und SPN (Service Pricipal Name) eines Clients im Active Directory die folgende Syntax aufweisen:

<NetBIOS Name>.<Active Directory Domänenname>

Dabei entspricht der Active Directory Domänenname dem primären DNS-Suffix. Will man es ermöglichen, dass ein Client unter einem anderen FQDN im DNS registriert wird als unter <NetBIOS Name>.<Active Directory Domänenname>, so kann man das primäre DNS-Suffix ändern (dies kann statisch oder über eine Gruppenrichtlinie erfolgen). Damit aber die beiden oben beschriebenen Attribute im Active Directory auf den "neuen" FQDN registriert werden können, muss die ACL (Access Control List) der Domäne geändert werden. Diese Änderung der ACL hat zur Folge, dass sich jeder Client unter jedem Namen im Active Directory registrieren kann. Die Folge daraus könnte eine Denial of Service Attacke sein. Daher wird nicht empfohlen, das primäre Suffix ungleich dem Active Directory Domänennamen zu wählen. Die nachfolgend dargestellt Möglichkeit der Verwendung eines verbindungsspezifischen Suffixes stellt dazu eine Alternative dar.

Verwendung eines verbindungsspezifischen Suffix

In Windows 2000 kann jeder Netzwerkkarte ein eigenes DNS-Suffix zugeordnet werden. Dieses Suffix wird als verbindungsspezifisches Suffix bezeichnet. Dieses Suffix kann statisch am Client konfiguriert werden (siehe Bild 1) oder kann über einen DHCP-Server zugewiesen werden (Option 15 "DNS Domänename"). Je nach Konfiguration kann das verbindungsspezifische Suffix dazu verwendet werden, einen zweiten FQDN im DNS zu registrieren. Wie sich eine statische Konfiguration bzw. die Zuweisung über DHCP des verbindungsspezifischen Suffix auf die dynamische DNS-Aktualisierung auswirkt ist in der folgenden Aufstellung wiedergegeben. Dabei muss unterschieden werden, ob es sich um einen Windows 2000 Client handelt, ob die IP-Konfiguration über DHCP erfolgt und ob der Client oder der DHCP-Server die Aktualisierungen im DNS durchführen.

Windows 2000 Client

- Manuell konfigurierte IP-Adresse und verbindungsspezifisches Suffix; Client ist für die dynamische Aktualisierung des primären- und verbindungsspezifischen Suffix konfiguriert:

  2 A-Einträge (primäres- und verbindungsspezifisches Suffix)

  2 PTR-Einträge (primäres- und verbindungsspezifisches Suffix)

- Über DHCP konfigurierte IP-Adresse und verbindungsspezifisches Suffix; Client ist für die dynamische Aktualisierung des primären und verbindungsspezifischen Suffix konfiguriert:

  2 A-Einträge (primäres- und verbindungsspezifisches Suffix)

  2 PTR-Einträge (primäres- und verbindungsspezifisches Suffix)

- Über DHCP konfigurierte IP-Adresse und verbindungsspezifisches Suffix; Client ist nicht für die dynamische Aktualisierung konfiguriert:

  1 A-Eintrag (verbindungsspezifisches Suffix)

  1 PTR-Eintrag (verbindungsspezifisches Suffix)

Nicht Windows 2000 Client

Von nicht Windows 2000 Clients wird die dynamische DNS Aktualisierung nicht unterstützt und der DHCP-Server aktualisiert die A- und PTR-Einträge. Daher ist hier nur der Fall dargestellt, dass die IP-Konfiguration des Clients über DHCP erfolgt.

- Der DHCP-Server aktualisiert das DNS:

  1 A-Eintrag (verbindungsspezifisches Suffix)

  1 PTR-Eintrag (verbindungsspezifisches Suffix)

Prinzipiell könnte die Verwendung des verbindungsspezifischen Suffix dazu verleiten, die im Bild 9 dargestellte Struktur zu implementieren.

In diesem Design wird die erste OU-Ebene auch im DNS wiedergespiegelt. Dieser Ansatz ist in Kundengesprächen bereits diskutiert worden, hätte aber je nach DHCP-Ansatz (siehe oben) die Auswirkung, dass jeweils 2 Einträge pro Host im DNS vorkommen. Im Bild 9 wären dies z.B. die Einträge host.firmaA.com (primäres Suffix) und host.teil1.firmaA.com (verbindungsspezifisches Suffix).

Dies würde zwar zu einer Verflachung des AD-Domänendesigns führen, jedoch wäre der Preis die nicht eindeutige Identifizierbarkeit von Hosts innerhalb des DNS und doppelte - wenn auch dynamische -Pflege von DNS-Einträgen.

Unter Umständen können jedoch politische Gegebenheiten zu einem ähnlichen Modell führen, nämlich dann, wenn die vom AD betroffenen DNS-Domänen in die Hände der AD-Administration fallen und die nicht vom AD betroffenen DNS-Domänen z.B. von den Netzbetreibern weiter verwaltet werden. Ein Beispiel hierfür wäre der Ansatz, dass es noch DNS-Sub-Domänen unterhalb der AD-Domänen gibt. Diese Ansätze bergen ggf. noch weitere Kritikpunkte, die aber im Rahmen dieses Artikels nicht näher beleuchtet werden.

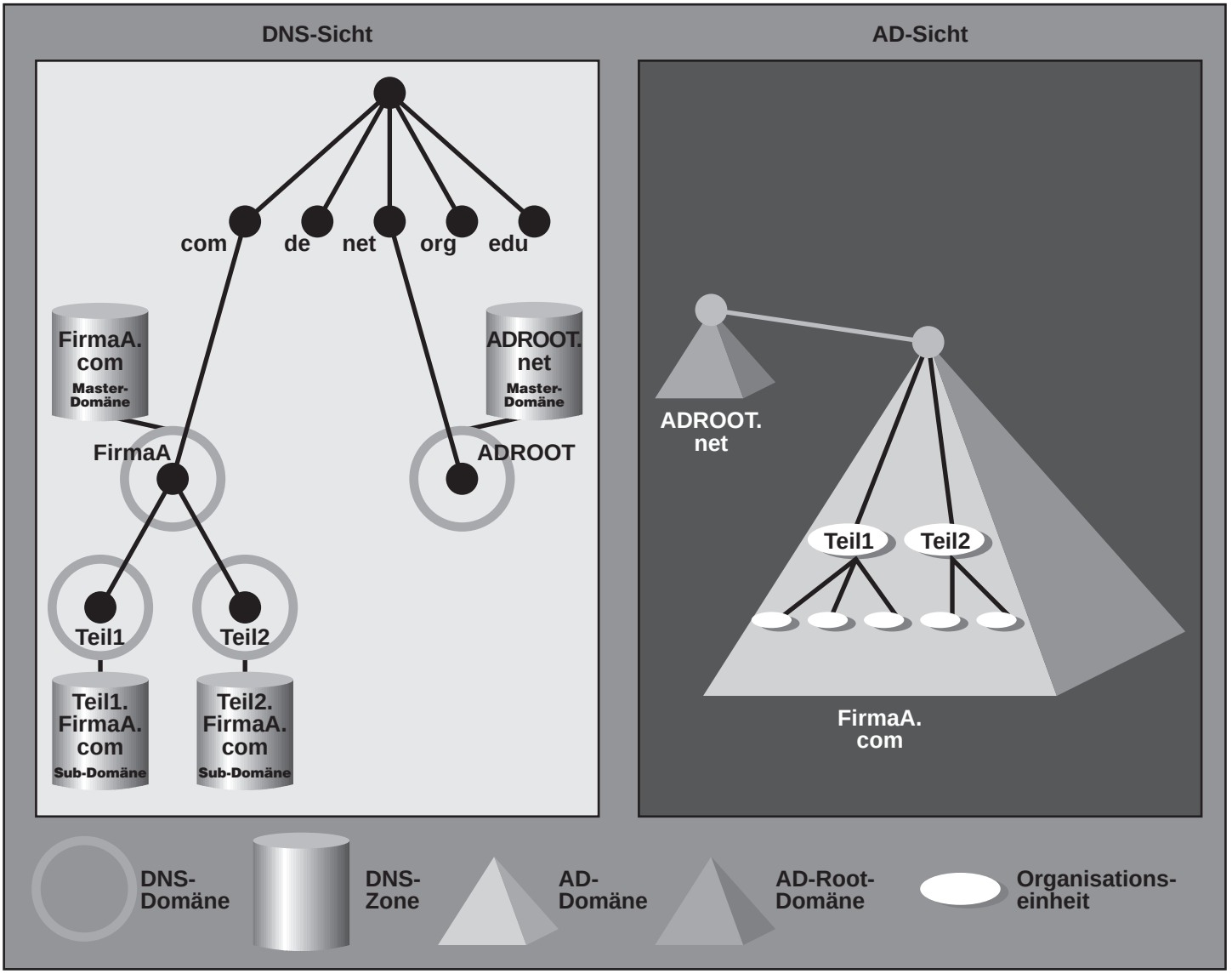


Bild 9 Verbindungsspezifisches Suffix zur Darstellung einer OU-Ebene

Vielmehr sollte in einem Projekt versucht werden solche Ansätze zu umgehen, ggf. auch auf Kosten zusätzlicher Domänen. Eine solche AD-DNS-Implementierung würde die Ausgangsfrage "Acitve Directory und DNS eine Welt?" jedoch anders beantworten, als bisher in diesem Artikel beschrieben, denn es sind dann eigentlich zwei Welten.

Nachdem in diesem Artikel bis jetzt hauptsächlich Design-Aspekte betrachtet wurden, stellt sich die Frage, wie man die beschriebenen Anforderungen und vor allem mit welcher DNS-Server-Implementierung erfüllt. Grundsätzlich kann gesagt werden, dass sämtliche Möglichkeiten offen stehen, also von einer DNS-Implementierung nur auf Windows 2000-Servern über die Implementierung einer Mischlandschaft bis hin zu einer ausschließlichen Implementierung auf Nicht-Windows 2000-Servern, vorausgesetzt die Anforderungen aus dem AD werden erfüllt (siehe 1 "Anforderungen aus dem Active Directory an das DNS"). Microsoft selber favorisiert entweder die völlige Integration des DNS in eine Windows 2000-Welt oder zumindest eine Integration der vom AD betroffenen DNS-Domänen. Zur Lösung dieser Frage kann wieder auf die eingangs beschriebene Runde verwiesen werden, deren Aufgabe es sein sollte eine Antwort zu finden, denn dies ist natürlich auch politisch ein ganz brisantes Thema.

Entscheidend für die Wahl der DNS-Server-Implementierung sollten folgende Fragestellungen sein:

- Welche Lösung ist derzeit implementiert und was ist zu tun, damit die Anforderungen aus dem AD erfüllt werden?
- Muss zusätzliches Know-How bzgl. der bestehenden oder einer neuen DNS-Lösung aufgebaut werden?
- Wenn man Richtung Windows 2000 DNS-Server wechselt, welche Funktionalitäten meiner aktuellen IP-Management-Lösung gehen verloren?
- Wenn man nicht Richtung Windows 2000 DNS-Server wechselt, welche Funktionalitäten aus dem AD bzw. auch aus dem Windows 2000 DNS kann man nicht nutzen?

In vielen Projekten stellt sich heraus, dass die Know-How-Frage ganz entscheidend ist! Hat man eine gut administrierte DNS-Umgebung und entsprechendes Know-How für diese, stellt sich eher die Frage, wie sich das AD darin implementieren lässt. Hat man eine heterogene DNS-Landschaft, stellt sich natürlich die Frage – auch im Sinne einer Know-How-Konzentration – mit welcher Lösung sich alle Anforderungen, auch die aus dem AD, am besten erfüllen lassen. Bei einer reinen NT 4.0-DNS-Server-Umgebung bietet sich wahrscheinlich an, direkt auf eine Windows 2000-DNS-Server-Umgebung zu migrieren, da dann ein Teil des Know-Hows genutzt werden kann. In diesem Zusammenhang stellt sich aber dann weiterhin die Frage, welche weiteren Anforderungen aus dem IP-Umfeld hat man. Nicht umsonst sind diverse andere IP-Management-Tools trotz hoher Kosten auf dem Markt so erfolgreich. Unter anderem werden zur Beantwortung dieser Frage im nächsten Abschnitt verschiedene DNS-Server-Implementierungen betrachtet. Im Sinne dieses Artikels liegt der Fokus jedoch auf der Windows 2000-DNS-Server-Implementierung. Nicht zuletzt können auch daraus Anforderungen an die DNS-Implementierung abgeleitet werden.

5
DNS Server Implementierungen

5.1
Windows 2000

DNS hat bei Windows 2000 eine fundamental andere Rolle als bei Windows NT. Bei Windows 2000 werden die meisten Funktionen, die bei Windows NT noch über NetBIOS durchgeführt wurden (Namensauflösung, Lokalisierung von Diensten, Lokalisierung von Domänencontrollern), über DNS abgewickelt. Nachfolgend werden einige neue Funktionen in Windows 2000 aus dem Bereich des DNS beschrieben:

Dynamisches DNS (DDNS)

Windows 2000 DNS ermöglicht eine dynamische Registrierung von Hostnamen zu IP-Adressen und umgekehrt gemäß RFC 2136. Die Aktualisierung der DNS-Einträge findet nach folgenden Ereignissen statt:

- Eine IP-Adresse wurde (manuell) hinzugefügt, erneuert oder verändert.
- Eine IP-Lease vom DHCP-Server wurde geändert oder erneuert.
- Der Befehl ipconfig /registerdns veranlasst die Erneuerung der Namensregistrierung beim DNS-Server (wurde unter Windows 2000 eingeführt).

Unabhängig von diesen Ereignissen werden die DNS-Einträge standardgemäß alle 12 Stunden aktualisiert.

Windows 2000 Clients können die Ressourceneinträge im DNS eigenständig aktualisieren oder die Aktualisierungen werden von einem geeigneten DHCP-Server vorgenommen (z.B. Windows 2000 DHCP). Von Windows 2000 Clients werden in der Standardeinstellung nur Aktualisierungen von A-Einträgen im DNS vorgenommen, vom DHCP-Server werden die entsprechenden PTR-Einträge aktualisiert. DHCP-Client und DHCP-Server können aber auch dahingehend konfiguriert werden, dass nur der DHCP-Server Aktualisierungen im DNS vornimmt.

Der DHCP-Server von Windows 2000 kann auch DNS-Aktualisierungen für Clients oder Server vornehmen, die Betriebssysteme vor Windows 2000 ausführen und die somit die dynamische Aktualisierung nicht unterstützen. Der DHCP-Server ist ebenfalls für das Entfernen aller DNS-Einträge verantwortlich, wenn eine Lease abgelaufen ist.

Subnetzpriorität

Für den Fall, dass der Auflösungsdienst eines DNS-Clients als Antwort auf eine DNS-Abfage mehrere A-Ressourceneinträge erhält und dass eine oder mehrere der IP-Adressen im Subnetz des Clients liegen, werden diese Einträge vom Auflösungsdienst an die erste Stelle sortiert. Somit wird sichergestellt, dass der Client versucht, zuerst eine Verbindung zu der nächst gelegenen IP-Adresse aufzubauen. Durch die Verwendung der Subnetzpriorität wird verhindert, dass das in RFC 1794 beschriebene Round-Robin-Verfahren verwendet wird. Die Verwendung der Subnetzpriorität ist in der Standardeinstellung eines Windows 2000 DNS-Clients aktiviert, kann aber über einen entsprechenden Registrierungsschlüssel deaktiviert werden (unter HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DnsCache\Parameters wird der Eintrag PrioritizeRecordData mit dem Wert 0 (REG_DWORD) hinzugefügt).

Inkrementelle Zonenübertragung

Vom Windows 2000 DNS-Server wird die inkrementelle Zonenübertragung (IXFR) für das Senden und Empfangen unterstützt. Dabei wird nicht die gesamte Zone repliziert sondern nur die Änderungen in der Zone, wodurch die Übertragungszeit und die erforderliche Bandbreite reduziert wird.

WINS-Lookup

Der DNS-Server von Windows 2000 kann - wie auch der DNS-Server von Windows NT 4.0 - pro Zone für das WINS-Lookup konfiguriert werden. Kann ein für eine Zone autorisierter DNS-Server einen Namen aufgrund der Zonen- und Cache-Informationen nicht auflösen, so schneidet ein für das WINS-Lookup konfigurierter DNS-Server den Hostnamen ab und gibt diesen an den konfigurierten WINS-Server weiter. Ist der Name im WINS registriert, so gibt der WINS-Server die zugehörige IP-Adresse an den DNS-Server zurück, und dieser antwortet dem anfragenden Client. Bei einer reversen Abfrage führt der DNS-Server eine Überprüfung des Status des NetBIOS-Knotenadapters durch. Um das WINS-Lookup zu nutzen, werden in die entsprechende Zone spezielle Ressourceneinträge (WINS, WINS-R) eingefügt, die eine proprietäre Entwicklung von Microsoft sind. Soll eine Zone, die für das WINS-Lookup konfiguriert ist auf einen nicht Microsoft DNS-Server repliziert werden, so kann die Replikation der WINS- und WINS-R-Einträge unterbunden werden.

Active Directory Integration

Active Directory ist der Verzeichnisdienst von Windows 2000 (basierend auf X.500). Das Active Directory kann genutzt werden, um die DNS-Zonen zu speichern. Die Zonen können nach drei verschiedenen Möglichkeiten geladen werden:

- von einer Zonen-Datei unter %SystemRoot%\System\dns
- von einem Master-Server, wenn es sich um eine sekundäre Zone handelt
- vom Active Directory

Die Integration von DNS in das Active Directory bietet eine Reihe von Vorteilen, die nachfolgend beschrieben werden.

Multi-Master-Replikation

Befinden sich die Zonen im Active Directory, so werden Änderungen auf jeden Domänencontroller der Domäne repliziert. Dies funktioniert nach dem Prinzip der Multi-Master-Replikation, was zur Folge hat, dass an jedem Domänencontroller Änderungen vorgenommen werden können, die dann gegenseitig repliziert werden.

Mehrere primäre DNS-Server

Die Multi-Master-Replikation von Zonen auf andere Domänencontroller bietet den Vorteil, dass mehrere primäre DNS-Server für dieselbe Zone existieren können. In Active Directory integrierte Zonen können nur auf DNS-Servern erstellt werden, die auf Domänencontrollern ausgeführt werden. Das bedeutet, dass sich genauso viele DNS-Server eine primäre Zone teilen können wie Domänencontroller in der Domäne vorhanden sind.

Sichere dynamische Aktualisierung

Active Directory-integrierte Zonen können für die sichere dynamische Aktualisierung konfiguriert werden. Dabei kann über eine Zugriffsliste angegeben werden, welche Benutzer oder Gruppen Änderungen in einer Zone durchführen dürfen. In der Standardeinstellung sind dies alle Mitglieder der Gruppe "Authentifizierte Benutzer".

DDNS-Clients versuchen zuerst eine nicht sichere dynamische Aktualisierung. Scheitert diese, müssen sie eine gesicherte Verbindung zur Aktualisierung aufbauen. Über diese Methode können nicht autorisierte Computer abgefangen werden.

Für nicht DDNS fähige Clients/Server kann der DHCP-Server die sicheren dynamischen Aktualisierungen durchführen.

Unterstützung der Alterung und des Aufräumvorgangs von Einträgen

Der DNS-Dienst kann die Alterung und den Aufräumvorgang von DNS-Einträgen verwalten. Falls aktiviert, kann diese Funktion verhindern, dass in DNS veraltete Einträge verbleiben. Dabei wird zu jedem Eintrag im DNS ein Zeitstempel gesetzt, der eine automatische Überprüfung ermöglicht, ob der Eintrag veraltet ist. Vom Administrator kann die Zeitspanne festgelegt werden, nach der ein Eintrag als veraltet gilt ist und der Löschvorgang erfolgen kann. Bei der Festlegung dieser Zeitspanne kann man sich an der Lease-Zeit des DHCP-Servers orientieren.

Unterstützung einer reinen DNS-Umgebung

In der Microsoft Literatur ist an vielen Stellen zu lesen, dass man keinen WINS-Server mehr benötigt, wenn alle Computer (Dienste und Applikationen) Windows 2000 verwenden. Da jedoch in vielen Firmennetzwerken auch auf längere Sicht aufgrund der vorhandenen Applikationen der WINS Dienst gebraucht wird, sollte neben der DNS- auch eine WINS-Konzipierung erfolgen.

Interoperabilität

Der DNS-Server von Windows 2000 ist RFC-konform und kann zusammen mit anderen DNS-Server-Implementierungen eingesetzt werden. Seitens Microsoft wurde die Interoperabilität mit den DNS-Server-Implementierungen von Windows NT 4.0, BIND 8.2, BIND 8.1.2 und BIND 4.9.7 getestet. Tabelle 1 vergleicht einige Features der unterschiedlichen DNS-Server-Implementierungen. Dabei kommt der Unterstützung der SRV-Einträge und der dynamischen Aktualisierung eine besondere Bedeutung zu.

Fazit

Der Windows 2000 DNS-Server ist selbstverständlich als DNS-Basis für das Active Directory geeignet. Die Möglichkeit der Integration der Zonen in das Active Directory und die damit verbundene Funktionalität mehrerer primärer DNS-Server und der sicheren dynamischen Aktualisierungen sind sicherlich interessante Neuerungen, die jedoch für ein korrektes Arbeiten des Active Directory nicht zwingend notwendig sind, aber als klare Vorteile der Lösung zu sehen sind.

5.2 BIND

BIND (Berkeley Internet Name Domain) ist die bekannteste und populärste Implementierung des DNS-Dienstes und wurde ursprünglich an der Universität von Kalifornien in Berkeley für das Betriebsystem BSD-UNIX entwickelt, um die bis dahin im Internet für die Auflösung von Hostnamen zu IP-Adresse verwendete HOSTS-Dateien abzulösen. BIND besteht aus zwei Teilen: Die Clientseite wird Resolver genannt und generiert die DNS-Abfragen und auf der Serverseite übernimmt diese der Daemon Named und beantwortet die Anfragen. Der BIND-DNS-Server kann kostenlos unter http://www.isc.org heruntergeladen werden. Ein BIND DNS-Server benötigt zum Start mehrere Dateien:
named.conf
(Startdatei, legt fest, welche Dateien aus welchem Verzeichnis geladen werden);
named.root
(Hinweise auf die Stammserver);
db.127.0.0.
(Loopback Adresse);
db.<Domänenname>
(Forward Lookupdatei für eine Domäne);
db.<Netzwerkkennung>
(Reverse Lookupdatei für ein Netzwerk).

Die BIND Dateien können mit einem Texteditor erstellt und konfiguriert werden, oder mit Hilfe von grafischen Benutzeroberflächen (z.B. Webmin).

Nachfolgend sind einige Funktionen aufgeführt, die von BIND 8.2.1 unterstützt werden:

Tabelle 1 Vergleich der DNS-Server-Implementierungen

Feature	Windows 2000	Windows NT 4.0	BIND 8.2	BIND 8.1.2	BIND 4.9.7
SRV-Einträge	Ja	Ja [SP4]	Ja	Ja	Ja
Dynamische Aktualisierung	Ja	Nein	Ja	Ja	Nein
Sichere dynamische Aktualisierung	Ja	Nein	Nein	Nein	Nein
WINS & WINS-R-Einträge	Ja	Ja	Nein	Nein	Nein
Schnelle Zonenübertragung	Ja	Ja	Ja	Ja	Ja
Inkrementelle Zonenübertragung	Ja	Nein	Ja	Nein	Nein
UTF-8-Zeichencodierung	Ja	Nein	Nein	Nein	Nein

- SRV-Einträge
  Die für das korrekte Arbeiten des Active Directory benötigten SRV-Einträge werden ab der BIND-Version 4.9.7 unterstützt.

- Dynamische Aktualisierung (gemäß RFC 2136)
  Die dynamische Aktualisierung kann für das automatische Hinzufügen der SRV-Einträge von Domänencontrollern und für die dynamische Clientregistrierung genutzt werden. Es kann vom Administrator definiert werden, welche Systeme das DNS aktualisieren dürfen.

- Überprüfung der Host-Namen
  BIND überprüft, ob die Hostnamen RFC 952-konform sind, nach dem folgende Zeichen verwendet werden dürfen: A bis Z; a bis z; 0 bis 9; Punkt "."; Bindestrich "-". Der Unterstrich "_" ist nicht erlaubt. Da die Active Directory-spezifischen DNS-Einträge den Unterstrich beinhalten, muss für eine einwandfreie Funktion die Syntaxüberprüfung deaktiviert werden.

- Inkrementelle Zonenübertragung

- DNS-Benachrichtigung

- Anhängen von Domänenamen

- @-Notation

- Nameserver-Adresssortierung

- Negative Zwischenspeicherung

- Round-Robin

- DNSSec

Fazit

BIND-Versionen, die SRV-Einträge unterstützen, können als DNS-Basis für das Active Directory genutzt werden. Eigenschaften wie die Integration der Zonen in das Active Directory, die damit verbundene sichere dynamische Aktualisierung, etc. werden jedoch nicht unterstützt.

5.3 Weitere IP-Management-Tools

Auf dem Markt gibt es noch eine ganze Reihe etablierter IP-Management-Tools. Bei der Bewertung dieser Tools muss herausgestellt werden, dass immer das gesamte Tool und sämtliche Funktionen zu bewerten sind. Aus diesem Grunde wird in diesem Artikel nur am Rande auf zwei Tools eingegangen, fokussiert auf DNS und speziell auf die AD-Implementierungsmöglichkeit.

Lucent Technologies – QIP 5.2

Erwähnenswert bei QIP ist, dass es eine datenbankbasierte Implementierung ist, die Oracle oder Sybase nutzt. Auch kann die Lösung auf verschiedenste Plattformen implementiert werden, wie HP-UX, Sun-Solaris oder IBM AIX für die UNIX-Seite oder Windows NT und Windows 2000 für die Microsoft-Seite. Die Version 5.2 ist BIND 8.1.2 kompatibel und unterstützt somit Features wie DDNS und SRV-Einträge. Für die SRV-Einträge muss jedoch in dieser Version beachtet werden, dass keine echte Dynamik unterstützt wird. Für die Aktualisierung der Einträge muss ein Zusatztool verwendet werden, welches nur manuell oder zeitgesteuert eingesetzt werden kann. Es ist jedoch angekündigt, dass mit der neuen Hauptversion QIP 6 dies dynamisch unterstützt wird. Ebenfalls sind eine Reihe weiterer AD-Integrationsmöglichkeiten, wie z.B. die Nutzung des sicheren DNS-Updates, in der neuen Version vorgesehen. Nicht unerwähnt sollten die hohen Kosten bleiben (Listenpreis bis 10.000 IP-Knoten, 4,55 ? (4 $) pro Knoten [Preisangaben ohne Gewähr]). Sicherlich muss auch erwähnt werden, dass QIP zahlreiche Features besitzt, die von Windows 2000 nicht unterstützt werden, so beinhaltet die Lösung z.B. redundantes DHCP auf Dienstebene, eine Programmierschnittstelle, eine gesonderte Auditfunktionalität, eine gesonderte Netzwerkmanagementkonnektivität, u.v.m.. Nicht zuletzt kann gesagt werden, dass im Gegensatz zu Microsoft, wo eine serverorientierte Sicht besteht, eine Sicht von der Netzwerkseite verwirklicht wurde.

Fazit

Unternehmen die QIP derzeit einsetzen, werden höchstwahrscheinlich nicht auf Windows 2000 DNS-Server migrieren, da das entsprechende Know-How auf Seiten von QIP liegt und sie eine Reihe QIP-Features nutzen, die nicht von Windows 2000 geliefert werden.

Check Point – Meta IP 4.1 (Enterprise)

Auch Meta IP kann auf verschiedensten Plattformen, wie HP-UX oder Sun Solaris bzw. Windows NT oder Windows 2000, implementiert werden, nutzt jedoch keine Datenbank. Die Version 4.1 ist BIND 8.2.2 kompatibel und unterstützt somit ebenfalls die erforderlichen Features für das AD. Dieses Tool zeichnet sich ebenfalls durch verschiedenste Funktionalitäten aus, dazu zählen beispielsweise das DHCP-Failover auf Dienstebene, der integrierte Radius-Server, ein sogenanntes User Authentification Trap bei dem eine Verknüpfung von IP-Adresse zum Benutzer erfolgt (interessant für Fälle bei denen eine Authentifizierung auf IP-Adressen-Basis erfolgt, jedoch eine Benutzerauthentifizerung gewünscht ist, die jedoch nicht implementiert werden kann), eine Firewall-1-Integrationsmöglichkeit, u.v.m.. Die Integrationsmöglichkeit in die Firewall spiegelt natürlich die Ausrichtung des Stammhauses wieder, bietet aber ggf. dem ein oder anderen Unternehmen gewünschte Funktionalität.

Die Kosten für das Produkt sind jedoch ebenfalls hoch (Listenpreis bis 10.000 IP-Knoten, 4,98 ? pro Knoten [Preisangaben ohne Gewähr]).

Fazit

Auch bei Meta IP gilt: Unternehmen die es derzeit einsetzen, werden höchstwahrscheinlich nicht auf Windows 2000 DNS-Server migrieren, da das entsprechende Know-How auf Seiten von Meta IP liegt und sie eine Reihe Meta IP-Features nutzen, die nicht von Windows 2000 geliefert werden. Auf die Betrachtung weiterer Tools, wie z.B. NetID von Nortel oder den Network Registrar von Cisco, wird verzichtet, da grundsätzlich die wesentlichen Anforderungen für das AD unterstützt werden, und andere Features der Produkte, sowie wie die Know-How-Frage, entscheidend für den Einsatz sind. Bei der Preisgestaltung scheinen sich die Hersteller jedoch weitestgehend einig, so dass auch die anderen Tools im Preisbereich von Meta IP und QIP liegen.

6 Active Directory und DNS – eine Welt?

Nach diesem Artikel kann die Ausgangsfrage, nur aus verschiedenen Sichten beantwortet werden, abhängig davon wie die Integration des AD erfolgt, wie bereits im ersten Teil des Artikels angedeutet wurde.

- Aus Sicht des DNS und einer BIND-Implementierung sowie BIND kompatibeler Implementierung kann definiert werden, dass das AD ein Teil der gesamten internen DNS-Welt ist.

- Aus Sicht des Active Directoy und einer DNS-Integration auf der Plattform Windows 2000 kann durchaus gesagt werden, dass es eine Welt ist, denn die Verknüpfungen sind sehr elementar.

7
Und was ändert sich mit "Whistler" (Windows XP, Windows 2002)?

Zum Abschluss des Artikels stellt sich noch die nicht unerhebliche Frage: "Was verändert sich mit dem Nachfolger von Windows 2000?". Mit dieser Frage verknüpfen noch einige Unternehmen die Frage, ob sie Windows 2000 einführen oder auf den Nachfolger warten.

Diese Frage muss aufgeteilt werden in folgende Punkte:

- Änderungen innerhalb des Active Directory.
- Änderung in der Client-Version.

Folgende Ausführungen beziehen sich auf von Microsoft gemachte Aussagen und auf die Beta Version 3 des Whistler Server bzw. auf den RC1 von Windows XP und wurden noch nicht vollständig im Testcenter des Competence Center Backoffice der ComConsult Beratung und Planung GmbH nachgestellt bzw. getestet. Sie geben jedoch Aufschluss darüber in welcher Richtung die Weiterentwicklung in diesem Umfeld erfolgt.

Änderungen innerhalb des Active Directory

Eine entscheidende Neuerung soll die Möglichkeit sein, transitive Beziehungen zwischen Forests anlegen zu können. Diese Möglichkeit, die den im Artikel beschriebenen Nachteil beim Verlust der Rootdomäne, z.B. beim Verlassen einer Gesamtstruktur, korrigiert, wird im AD-Umfeld als entscheidend angesehen. Im Kontext des Artikels gesehen führt dies zu einer erheblichen Steigerung der Flexibilität. Die Nutzung dieser Möglichkeit sollte nur mittelfristig gebraucht werden müssen, vorausgesetzt eine gute Konzipierung des AD ist erfolgt, und stellt somit keinen primären Grund dar, um auf die Einführung von Windows 2002 (Whistler Server) zu warten. Diese Funktionalität wurde noch nicht gestestet.

Auf Seiten der Schema-Verwaltung wird es ebenfalls eine entscheidende Neuerung geben. Mit dem neuen Feature "Schema Delete" können Objekte und Attribute gelöscht werden. Mit Hilfe dieses Features können somit vermeintliche Fehler rückgängig gemacht werden. Diese Möglichkeit erhöht jedoch auch das Sicherheitsbedürfnis für das Schema und ist somit ein weiterer Grund zur Nutzung einer dedizierten AD-Root-Domäne.

Dies sind zwei wichtige Ergänzungen zu der derzeitigen Version des AD und im Sinne des Artikels die wichtigsten, die bekannt sind. Folgend werden noch weitere Neuerungen vorgestellt:

- z.B. etwas beim DNS- bzw. Netzwerk-Client ändert.Benutzer sollen per Drag-and-Drop zwischen Organsisationeinheiten verschoben werden können.
- Authentifizierungsmöglichkeit an einen lokalen Domänencontroller ohne Kontaktierung des globalen Kataloges.
- Ein "Install Replica from Media" soll möglich sein. Dies bedeutet man kann bei der Erstinstallation (dcpromo) die Daten für die Anfangsreplikation eines neuen Domänencontroller vom Band, von CD-ROM oder von DVD importieren, so dass nicht alles über das Netzwerk repliziert werden muss. Dies ist besonders interessant, wenn WAN-Verbindungen mit geringer Bandbreite bestehen.
- Die MMC wird dahingehend verbessert, dass mehrere Objekte aus dem AD-Baum gleichzeitig ausgewählt werden können, um diese dann gemeinsam zu bearbeiten.
- Das Active Directory Migration Tool unterstützt jetzt auch bei der Migration von Benutzern die Möglichkeit Passwörter zwischen verschiedenen Forests zu migrieren.

Diese Aufzählung ist sicherlich nicht abschließend und bis zur endgültigen Version von Windows 2002 Server wird es sicherlich auch im AD-Umfeld noch weitere Neuerungen bzw. Ergänzungen geben.

Änderung in der Client-Version

Mit der Version Windows XP, die am 25.10.2001 erscheinen soll, möchte Microsoft eine einheitliche Clientbetriebssystemplattform implementieren, wobei es mit der

Bild 10 Netzwerkumgebung Windows XP (Beta 2)

"Home Edition" und der "Professional" Version auch wieder 2 Versionen geben wird. Auf die zahlreichen Neuerungen wird innerhalb dieses Artikels nicht eingegangen. Wichtig im Sinne dieses Artikels ist, ob sich z.B. etwas beim DNS- bzw. Netzwerk-Client ändert.

Wie in Bild 10 zu sehen, gibt es drei zusätzliche Features, die in Windows 2000 nur mit dem Kommandozeilentool ipconfig verfügbar sind.

- "DNS registrieren", entspricht ipconfig /registerdns und registriert den Client beim DNS-Server.
- "DNS leeren", entspricht ipconfig /flushdns und löscht den DNS Cache.
- "Erneuern", entspricht in etwa ipconfig /renew und erneuert die DHCP-Konfiguration. Durch die Auswahl der Checkbox "Aktuelle Einstellungen beim Erneuern freigeben" wird vor dem renew ipconfig /release ausgeführt und die IP-Adresse freigegeben.

Wie in Bild 11 zu sehen, kann auch eine benutzerdefinierte alternative IP-Konfiguration definiert werden oder es kann APIPA (Automatisch zugewiesene private IP-Adresse) genutzt werden. Dies ist sicherlich ein guter Ansatz, aber noch nicht ausreichend. Nachteilig ist, steht der DHCP-Server beim Start des Clients nicht zur Verfügung, erhält er entweder die manuell konfigurierte alternative IP-Konfiguration oder nutzt APIPA, aber nicht seine vom DHCP-Server zugewiesene Konfiguration. Da dieser Test sowie die Screenshots aus der Beta Release Version 2 von Windows XP stammen, besteht noch die Hoffnung, dass eine weitere Möglichkeit implementiert wird, die die Beibehaltung der DHCP-Konfiguration ermöglicht. Unter Windows 2000 Professional ist dies möglich, allerdings nur durch Editieren eines Registry-Schlüssels.

Bild 11 Alternative Konfiguration TCP/IP Windows XP (Beta 2)

ComConsult Certified Network Engineer

"Man hat keine Chance zum Einschlafen."

Ralf Bremer (39) kam von der AMMANN IMA GmbH um ComConsult Certified Network Engineer zu werden. Der Netzwerk Insider sprach mit ihm unmittelbar nach der bestandenen Prüfung.

Insider: Was macht die AMMANN IMA?

Ralf Bremer: Wir stellen Asphaltanlagen her für ganz Europa und auch für Asien und Afrika zum Teil. Die Firma sitzt in Arlfeld, an diesem Standort sind 300 Mitarbeiter, unternehmensweit sind es knapp 2000.

Insider: Wie ist Ihr beruflicher Werdegang?

Ralf Bremer: Ich bin seit 1991 bei der AMMANN IMA. Vorher war ich als Lehrer tätig in den Fächern Elektronik und Rechentechnik.

Insider: Wieso haben Sie Ihre Lehrertätigkeit aufgegeben?

Ralf Bremer: Das hatte mehr was mit der Wiedervereinigung zu tun. Lehrer ist auch nicht so mein Ding gewesen. Damals war ich auch noch viel zu jung um immer wieder dasselbe zu erzählen.

Insider: Was sind denn jetzt genau Ihre Aufgaben?

Ralf Bermer: Zur Zeit bin ich Abteilungsleiter für Elektroprojektierung und habe nebenbei auch mit Netzwerktechnik zu tun. Wir projektieren Elektroanlagen für Asphaltmischanlagen, das umfasst alles, was sich dreht, also Motoren und die komplette Steuerung dafür. Das sind Unix-Systeme über Ethernet. Und nebenbei bin ich auch noch als Admininstrator für unser Abteilungsnetz zuständig.

Insider: Wie groß ist Ihre Abteilung?

Ralf Bremer: Die Abteilung ist relativ klein. Da sind ungefähr 15 Clients und im ganzen Unternehmen sind es so in etwa 150 Clients und 4 oder 5 Server. Da wir ein relativ kleines Unternehmen sind, sind die Admininstratoren auf Abteilungsbereichsebene halt auch für das ganze Haus zuständig. Personaltechnisch ist das also relativ flach gehalten.

Insider: Was hat Sie dazu veranlasst die Ausbildung zum ComConsult Certified Network Engineer zu machen?

ComConsult Certified Network Engineer Ralf Bremer

Ralf Bremer: Eigentlich kam der Anstoß nach der Teilnahme an dem Seminar "Lokale Netze". Weil die Seminare doch sehr anspruchsvoll sind, möchte man sich doch selber mal testen, wie weit man kommt. Außerdem gibt es da noch den ganz normalen Wissensdrang, einfach mehr zu wissen.

Ließ den Teilnehmern keine Chance zum Einschlafen: Dr. Jürgen Suppan, hier bei der Unterzeichnung der Zertifikate

Ich habe relativ viel Einfluss darauf, zu welchen Lehrgängen ich gehen kann. Und die Lehrgänge von ComConsult sind im Gegensatz zu vielen anderen Schulungen eben nicht herstellerbehaftet und hier werden einem die Grundlagen eben auch sehr gut beigebracht.

Insider: Und wie haben Ihnen die Schulungen gefallen?

Ralf Bremer: Einprägend sind die "Lokalen Netze" bei Dr. Suppan. Man hat keine Chance zum Einschlafen. Rhetorisch ist das sehr gut und Dr. Suppan hat die sehr sehr gute Gabe etwas anschaulich zu erklären. Internetworking war für mich ein ganz neues Gebiet; das Seminar bei Frau Borowka war auch sehr interessant, die anderen Kurse aber auch. Durch die Bank weg haben alle vier Lehrgänge ihre Berechtigung und sind sehr vielseitig.

Insider: Wie ist die Ausbildung bei Ihnen abgelaufen?

Ralf Bremer: Vom Zeitraum her hat das viel zu lange gedauert. Ich habe die vier Seminare mit einem Abstand von je einem halben Jahr absolviert. Das liegt daran, dass bei uns so viel Arbeit anliegt, dass ich nicht zu oft weg sein konnte.

Insider: Haben Sie denn - gerade bei diesem langen Zeitraum - konkret gemerkt dass Sie Ihr erlerntes Wissen bei Ihrer täglichen Arbeit umsetzen konnten?

Ralf Bremer: Direkt gemerkt hab ich es bei der Entscheidungsfindung für irgendwelche Neuinvestitionen oder bei der Strukturplanung unseres Netzes. Wir haben zum Beispiel in diesem Zeitraum unser Netz auf strukturierte Verkabelung umgestellt. Vorher waren es halt mehrere kleinere Netze, ein Novell-Netz, NT-Netz, Unix-Netze, und die sind dann auf Fast Ethernet umgestellt worden. Und da gab es dann schon bei der Geräteauswahl oder bei der Planung der Kabelwege bestimmte Dinge, wo man jetzt die Hintergründe kannte.

Insider: Wie war die Prüfung für Sie?

Ralf Bremer: Im Vorfeld ganz schön hart, weil man alles lernen muss. Aber weil man ja schließlich so viel gelernt hatte, konnte man es dann etwas gelassener angehen, als man drin war.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Neue Ethernet-Technologien, 20. - 24.08.01 in der AGIT Aachen

Das Intensiv-Seminar beschäftigt sich mit dem Ausbau bzw. Umbau dieser Netze in Richtung Fast Ethernet und Frame Switching für alle Betreiber traditioneller Ethernet-Netzwerke. Referenten: Dipl.-Inform Oliver Flüs, Dipl.-Inform. Andreas Meder, Dipl.-Ing. Hartmut Kell, Dipl.-Ing. Harald Krause, Dr. Joachim Wetzlar, ComConsult Beratung und Planung Preis: EUR 1.990,--

Der Mainframe im IP-Netz, 27. - 28.08.01 im Holiday Inn Bonn

Das Seminar beschäftigt sich mit der Migration von klassischem SNA/Token Ring- zum IP/Ethernet-Umfeld und zeigt auf, wie der Mainframe erfolgreich an TCP/IP-Netzwerke angebunden wird.
Referenten: Ulrich Hamm, Dr. Behrooz Moayeri Preis: EUR 1.290,--

Betrieb von TCP/IP-Netzen, 27. - 29.08.01 im Holiday Inn Bonn

Das Seminar vermittelt praxisnah die für den erfolgreichen Betrieb von IP-Netzen notwendigen Basiskenntnisse der TCP/IP-Technologie und geht insbesondere auf die für den professionellen Betrieb notwendigen Hilfsmittel ein.
Referenten: Dipl.-Inform. Oliver Flüs, Dipl.-Inform. Andreas Meder Preis: EUR 1.990,--

xDSL – Technik und Nutzen, 30. - 31.08.01 im Holiday Inn Bonn

Dieses Seminar beschreibt die wesentlichen Möglichkeiten und Konzepte der xDSL-Technologiefamilie, die praktisch alle Kommunikationsanforderungen heutiger Anwendungen unter vergleichsweise minimalen Investitions- und Betriebsaufwänden abdeckt.
Referent: Dipl.-Ing. Ralf Boden Preis: EUR 1.290,--

IP-VPNs erfolgreich einsetzen, 03. - 05.09.01 im Holiday Inn Bonn

Das Seminar beschäftigt sich mit dem Home-Office-/Teleworker-Zugang, dem Unternehmens-WAN-Backbone, dem Filialnetzwerk und der Standort-Kopplung, denn VPNs stellen die wichtigste Weiterentwicklung im Bereich der Weitverkehrskommunikation dar.
Referenten: Dipl.-Inform. Andreas Meder, Dr. Behrooz Moayeri, ComConsult Beratung und Planung Preis: EUR 1.590,--

Fehlersuche in lokalen Netzen für Einsteiger, 03.09. - 05.09.01 in der AGIT Aachen

Das Praxis-Seminar stellt wesentliche Hilfsmittel für die Netzwerk-Überwachung und Fehlersuche über Vorträge und Übungen vor, typische Problemsituationen werden simuliert und systematisch deren Beseitigung erarbeeitet.
Referenten: 8 Mitarbeiter der ComConsult Beratung und Planung GmbH Preis: EUR 1.790,--

TCP/IP und SNMP, 03. - 07.09.01 im Holiday Inn Bonn

Das Intensiv-Seminar vermittelt einen praxis-orientierten Einblick in den Aufbau und den Betrieb von heterogenen Netzen, die den Kommunikationsstandard TCP/IP und den Netzmanagement-Standard SNMP benutzen.
Referenten: Dipl.-Phys. Frank Breitschaft, Dipl.-Inform. Detlef Weidenhammer (GAI NetConsult) Preis: EUR 1.990,--

DNS-/IP-Design für Windows 2000 Active Directory, 04. - 06.09.01 in Königswinter

Dieses Seminar behandelt in konzentrierter Form die Implementierungsgrundlagen aus dem IP-Bereich für Windows 2000 bzw. für das Active Directory. Dabei spielt DNS die Hauptrolle, wobei auch insbesondere die dynamische Verbindung zum DHCP betrachtet wird.
Referenten: Markus Holländer, Lars Kuhl, ComConsult Beratung und Planung Preis: EUR 1.590,--

Design Windows 2000 Active Directory, 10. - 12.09.01 im Holiday Inn Bonn

Das Seminar vermittelt, unterstützt durch den Praxisbezug zu Projekten in diesem Umfeld, wie das Active Directory zu strukturieren ist und legt dabei großen Wert auf den Entwurf der strategischen Komponenten (Domäne, Standort).
Referenten: Markus Holländer, Michael van Laak, Frank Neunzig, ComConsult Beratung und Planung Preis: EUR 1.590,--

ComConsult Akademie – Telefax: 02408/955-399

Anmeldung

Titel des Seminars _____ Name _____ Vorname _____

Termin _____ Firma, Abteilung _____ Position, Funktion _____

☐ Bitte buchen Sie für mich ein Zimmer im Veranstaltungshotel

Straße _____ PLZ, Ort _____

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **akademie@comconsult.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de**

Telefon _____ Fax _____

eMail _____ Unterschrift _____

Handelsplattform für gebrauchte Netzwerkkomponenten

Gebrauchte Netzwerk-Komponenten

Die Spielregeln

Gebrauchte Netzwerk-Komponenten, die im Rahmen eines Redesigns ausgemustert werden, könnten einige Betriebe sehr gut gebrauchen. Hier wollen wir helfen. Wir bauen für unsere Kunden eine Handelsplattform für gebrauchte Netzwerk-Komponenten auf. Die Spielregeln: Sie melden uns, welche Produkte/ Komponenten Sie anbieten/suchen mit Ihrer Preisvorstellung.

Ihr Angebot wird in anonymer Form auf dem Webserver der ComConsult Akademie unter www.comconsult-akademie.de und im Netzwerk Insider veröffentlicht.

Interessenten melden sich per Mail, mit dem Fax-Formular (unten) oder über den Web-Server bei uns. Wir stellen den Kontakt zwischen Anbieter und Nachfrager her.

Wir erhalten vom Verkäufer für diese Leistung 10% Provision auf den erzielten Kaufpreis. Davon stellen wir die Hälfte ausgewählten Schulen als Spende zum Aufbau ihres Internet-Zugangs oder ihres internen Netzwerks zur Verfügung. Der Kaufvertrag entsteht direkt zwischen Käufer und Verkäufer. Wir selber haften in keiner Form für die Qualität oder Nutzbarkeit der Komponenten.

Gebote

Adapter

Madge, TR-Karten ver. Typen (BM2, MK3, MK4, HSTR) alle PCI, 200 Stck., 60% d. Neupreises
B10322

Concentrator

Token Ring Rac 4001 Lan Optics 12 Slot, 5 Stck., DM 400,--
B10305

Hub

Token Ring Hub LANNET/LET 36, 6x LTR 104 Ports,1 Stck., DM 600,00
B10603

IBM, Hub 8250 mit Management, LWL u. Kupfer RI+RO 80 Ports, 1 Stck., VS
B10607

IBM, Hub 8250 mit Management, LWL u. Kupfer RI+RO, 100 Ports, 1 Stck., VS
B10608

IBM, Hub 8250 mit Management, LWL u. Kupfer RI+RO, 120 Ports, 1 Stck., VS
B10609

3Com, Superstack II Hub, LinkBuilder FMS TR, 24- port 4/16 Mbit/s Token Ring Hub, unmanaged, 1 Stck., DM 85,- zzgl. MwSt.
B10503

Repeater

AI 3008SL 10, Base 2 Ethernet 8 Port Allied, 1 Stck., DM 350,--
B10323

Router

RSP2- Board für Cisco 75xx, 8MB onboard Flash, 64MB Memory, 20 MB PCMIA Flash, 1 Stck., VS
B10324

Sternkoppler

Hirschmann ASGE mit diversen Interfacekarten wie: UYDE, CYDE, OYDE, BfOC, KTDE, TYDE, 35 Stck., DM 200,- bis 800,-
B10320

Steuereinheit

IBM Token Ring / SNA IBM 3174, 25 Stck., DM 280,-
B10303

Switch/Brücke

3Com, SuperStack Switch 3000, 1 Stck., DM 650,-
B10502

3Com SuperStack Switch 3000, SuperStack 3000, 8- port, 100 Base- TX, vollduplex, VLAN, SNMP, Spanning Tree, 1 Stck., DM 650,-
B10502

Bay Network, Switch Centillion 100 4x LWL, 12x Kupfer, 1 Stck., VS
B10605

Cabletron 8 Port Ethernet Module for ATX 3E02-08-ATX, 1 Stck., $ 300,-
B10310

Switch/Brücke

Cabletron Enhanced ATX Packet Processing Engine 3X00-ATX, 1 Stck., $ 500,--
B10311

Cabletron 3C05-ATX Chassis, inkl. 1 Power Supply 3CPSM-R-ATX, 1 Stck., $ 300,--
B10312

IBM, Switch 8272, 8x Kupfer , LWL RI + RO, 1 Stck., VS
B10606

Sonstiges

SDV 231 2-Draht, Standleitung, 18,2 KB, ca. 9KM, volldublex, Tischgerät V24, 1 Stck., DM 650,-
B10610

Perle Remote Access Server Mod. 400 RAS-2 Port Ethernet, 1 Stck., VS
B10604

Extendet Systems, ESI 2852 16/4 TR, 50 Stck., VB
B10611

Nortel Networks Printserver, 1 Stck. DM 250,--
B10702

Token Ring Einschübe für Rac 4001 12 port Lobemodul 4283 Lan Optics, 20 Stck., DM 400,- bis 700,-
B10304

TR LWL Karten BKM 4521 850 Nm 1300 Nm Lan Optics, 10 Stck., DM 400,- bis 700,-
B10308

Handelsplattform für gebrauchte Netzwerkkomponenten

Gesuche

Adapter

IBM Eth. USM Adapter für FDX BNC PT 8274-7100, 1 Stck., VS S10405

IBM, Olicom Token Ring Adapter PCI, 30 Stck., VS S10301

HP J2585B 100VG,160 Stck., DM 80,00 – Kaufen eventuell auch noch 100VG-Hubs wie J2415A sowie Switch 2000 J3100B S10504

Concentrator

IBM 8.230.013, 10 bis 50 Stck., DM 400,- S10321

IBM 8.230.013, 10 bis 50, VS S10401

Hub

IBM 8260-3010 Dual Fiber Repeater Module,1 bis 2 Stck.,VS S10404

IBM 8260-3018 18Port TR Media Mod.,1 bis 2 Stck., VS S10403

IBM 8260-1200 DMM Distributed Management Modul, 1 bis 2 Stck., VS S10402

IBM 8238 Token Ring,1 bis 2 Stck., VS S10703

Olicom OC-3626, neu oder gebraucht, 2 Stck., VS S10505

Prozessor

Intel 450 oder 500 MHZ II,1 Stck., DM 200,- S10306

Ringleitungsverteiler

Madge, Smart RAM Plus # Port Nr. 55-55, 1 Stck., VS S10601

Madge, Smart LAM Plus # Port Nr. 55-42, 1 Stck., VS S10602

Madge Smart Lam Plus UTP 55-50, 3 bis 6 Stck., DM 800,- S10307

Router

Cisco Router 2504, IP Feature 2500, ISDN/BRI, 5 Stck., 2000,-- DM S10501

Switch/Brücke

IBM 16 PT RJ 45 UTP/STP 4/16 MBIT TR Switching Modul 8274-0867, 1 Stck., VS S10408

IBM 8 PT 10 Base FL, MMF SC, 2k CAM Switching Modul 8274-0562, 1 Stck., VS S10406

IBM 32-PT 10/100 TX Switching Modul RJ 45 2k CAM 8274-3725, 1 Stck., VS S10407

Xylan/Alcatel/IBM, Omni Switch Serie (Switche und Module) mehrere Stck., VS S10701

Fax an 02408/955-399

☐ **Ich suche**
☐ **Ich biete**

Produkt/Komponente/Release/Software

_____

_____

_____

_____

Preisvorstellung_____

_____

Ansprechpartner

_____

Firma

_____

Ort

_____

Straße

_____

Telefon, Fax

_____

eMail

☐ **Antwort auf Gesuch**
☐ **Antwort auf Gebot**

☐ _____

Preisvorstellung_____

_____

Ansprechpartner

_____

Firma

_____

Ort

_____

Straße

_____

Telefon, Fax

_____

eMail

Weitere Gebote und Gesuche

finden Sie auf dem Web-Server der ComConsult Akademie unter

www.comconsult-akademie.de