Windows NT 4.0 im WAN

Optimierung und Kosteneinsparung

Betrachtung der Protokolle und Kommunikation zwischen Windows NT Systemen zur Reduzierung von Datenvolumen und Kosten der zur Steigerung der Geschwindigkeit und Zuverlässigkeit

Frank Carius EDV-Beratung

Zeiskamer Straße 28
76756 Bellheim

http://www.carius.de

Gedruckt: 27. August 2000
Autor: Frank Carius
eMail: frank@carius.de

Zuletzt gespeichert: 2. August 2000 / Version 2:

ZUR BENUTZUNG DIESER DOKUMENTATION

Diese Dokumentation hält sich an folgende Formatierungen

Kennzeichnungen durch unterschiedliche Schriften

Neben der Standardschrift für diese Dokumentation kennzeichnen weitere Formatierungen wichtige Passagen oder Informationen

```
Sourcecode, Batchfiles und Listings werden in der Schriftart COURIER ausgedruckt,
damit die Ausrichtung erhalten bleibt und 80 Zeichen in einer Zeile passen
12345678901234567890123456789012345678901234567890123456789012345678901234567890
```

Eingaben am Keyboard werden mit **`Courier FETT`** gekennzeichnet und optional durch Tastenzeichen gekennzeichnet. Sondertasten wie **`[ENTER]`** oder **`[ESC]`** sind in eckigen Klammern gesetzt

Kennzeichnung durch Symbole

Zeichen	Bedeutung
	**Information** Dieser Abschnitt enthält zusätzliche Informationen zum Thema, Verweise auf andere Dokumentationen und Quellen.
	**Hinweis** Bitte beachten Sie die Hinweise, da Sie wichtig für die Funktion sind.
	**Warnung** Dieser Abschnitt ist außerordentlich wichtig. Die Missachtung kann auch andere Dienste und Funktionen schwer beeinflussen.
	**Einschränkung** Sie erhalten Hinweise auf nur eingeschränkt mögliche Funktionen
	**Frage** Beantworten Sie sich die gestellte Frage bitte selbst und entscheiden dann, ob etwas zusätzlicher Aufwand gerechtfertigt ist, um einen Funktionsgewinn zu erhalten.
	**Diskettenlaufwerk** Sie benötigen Disketten um die Aktionen auszuführen.
	**CD-ROM** Sie benötigen eine CD-ROM um diese Aktionen auszuführen.
	**Maussteuerung** Die folgenden Aktionen beschreiben die Bedienung mit der Maus.
	**Tastatur** So können Sie die Funktion per Tastatur ausführen.
	**Multimedia** Um voll die Funktion nutzen zu können muss ihr PC Multimediadaten verarbeiten können, d.h. zumindest eine Soundkarte haben.

INHALTSVERZEICHNIS

1 Was sie wissen sollten

Sie sollten einige Eckpunkte beim Einsatz dieser Software oder Dokumentation wissen, um vor unliebsamen Überraschungen verschont zu bleiben.

1.1 Wer ist Frank Carius EDV-Beratung

Die Frank Carius EDV-Beratung, besteht im wesentlichen aus einer Person, mir. Wer etwas zu meiner Person, zur Familie und mehr zum Namen „Carius“ erfahren will, kann im Internet unter www.carius.de einige Informationen finden.

Geschäftlich gibt es diese Unternehmung seit Anfang 1993 mit Sitz in Bellheim. Als sogenannter „Freelancer“ bin ich mein eigener Herr und sehr unabhängig, was auch für meine Kunden von Vorteil ist. Es gibt keine strategischen Partnerschaften oder Bindungen mit besonderen Firmen, die die Unabhängigkeit beeinträchtigen könnten.

Damit ist aber auch klar, dass ich weder angestellt bin, noch in einer wissenschaftlichen Einrichtung arbeite und auch nicht als Student gelten kann. Sie müssen daher dafür Verständnis haben, dass ich von meiner Arbeit lebe und daher Leistungen meinerseits kostenpflichtig sind.

Alle Dokumentationen, Programme und andere Ergebnisse meiner Arbeit sind, soweit nicht explizit aufgeführt, geschützt und dürfen nicht ohne mein Einverständnis verteilt werden. Dies gilt insbesondere, wenn durch meine Arbeit andere Personen oder Firmen Gewinn erwirtschaften würden.

Aber auch ich profitiere von Informationen und Programmen, welche frei im Internet verfügbar sind, und trage meinen Teil damit bei, dass auch ich einen Teil meiner Ergebnisse kostenfrei zur Verfügung stelle. Zum einen sind dies Programme, die zwar einen hohen Nutzen haben, aber aufgrund der Trivialität nicht sonderlich schützenswert sind. Viele funktionieren sowieso nur im Rahmen einer Gesamtkonzeption wirkungsvoll.

Auch Dokumentationen und Ausarbeitungen sind meist nur einige Jahre haltbar und selten direkt auf eigene Projekte zu übertagen. Daher sind von mir bereitgestellt Dokumentationen sowohl als Nachweis meiner Tätigkeit und Kenntnisse mit dem entsprechenden Werbeeffekt zu verstehen. Allerdings sind wir uns alle bewusst, dass Veränderungen solche Informationen sehr schnell veraltet oder gar unrichtig werden lassen.

Wenn Sie Ergebnisse meiner Arbeit einsetzen, sind sie verpflichtet, die Quellen anzugeben und beim kommerziellen Einsatz vorab mit mir eine Vereinbarung über die finanzielle Regelung zu treffen.

Sie können natürlich jederzeit mit mir Kontakt aufnehmen, um Verbesserungen vorzuschlagen, Fehler zu melden oder eine Umsetzung in ihrem Umfeld zu diskutieren. Sie können mich natürlich auch direkt beauftragen, für Sie zu arbeiten oder Schulungen durchzuführen.

Bitte haben Sie Verständnis, dass ich keinen direkten Support kostenfrei bieten kann. Sie können allerdings in diversen Newsgroups kostenfrei Hilfe finden. Auch ich bin in einigen Newsgroups aktiv.

1.2 Versionen

Folgende Veränderungen hat diese Dokument durchlaufen:

Datum	Bearbeiter	Änderung
23.10.1997	FC	Erste Version
02.07.2000	FC	Umformatierung, Prüfung des Inhalts

2 Der WAN-Aspekt von Windows NT

Steigende Marktanteile von WindowsNT im Servermarkt und die Anforderungen zur Kopplung verschiedener Standorte eines Unternehmens münden im Aufbau von WAN-Verbindungen über ISDN-Wählleitungen mit WindowsNT-Servern. Dazu ist es notwendig, die verschiedenen Dienste und Kommunikationsbeziehungen zu kennen, um eine erfolgreiche Installation und einen kostengünstigen Betrieb zu erlauben.

2.1 Einbindung in die Domain

Die erste große Frage bei der Einbindung eines WindowsNT-Rechners in eine bestehende Domain ist die Frage: ”Wie findet das NT-Setup den PDC”, denn zu dieser frühen Phase funktioniert noch kein WINS. Wird der Rechner im gleichen Netzwerk installiert, dann kann Windows direkt den PDC finden, indem per Broadcast die richtige Information erfragt wird. Dies schlägt aber bei der Installation über Router hinweg fehl. Eine Möglichkeit hierbei ist der Eintrag eines bestehenden WINS-Servers im TCPIP-Steuerfeld. Dann versucht der NT-Server zukünftig seine Namen über den WINS-Server auf dem anderen Segment aufzulösen. Bei WAN-Verbindungen ist dies aber nicht sinnvoll, da hier besser ein lokaler WINS-Server arbeiten sollte, welche zyklisch die Daten des remote WINS-Servers repliziert. Der aktuelle NT-Server ist aber noch im Setup begriffen, so daß ein andere Option sinnvoll ist. Beim Setup des TCPIP-Protokolls kann schon zum Zeitpunkt der Installation eine LMHOSTS-Datei importiert werden. Diese sollte dann vorgefertigt auf einer Diskette vorliegen und enthält z.B.: einfach nur folgende Zeile

```
192.168.100.1 NTSERV01 #PRE #DOM:NETATWORK
```

Anhand dieser Information weiß der NT-Server, unter welcher Adresse ein Rechner mit dem Namen ”NTSERV01” zu erreichen ist, und daß dieser in der Domäne ”NETATWORK” ist. Wurde dann beim TCP/IP-Setup das richtige Default Gateway eingetragen, wird der NT-Server den PDC finden und das Setup problemlos fortfahren. Diese Technik funktioniert natürlich nicht, wenn erst später auf dem NT-Server ein Router installiert werden soll. Dann sollte der Server am gleichen Netzwerk wie der PDC installiert werden und erst danach an seinen endgültigen Platz transportiert werden. Dies bedeutet dann jedoch wieder Umstellungen der IP-Adressen und WINS-Daten.

2.2 Domainreplikation

Werden mehrere Server in der gleichen Domäne zusammengefaßt, so gleichen sich diese Server untereinander regelmäßig ab. Dabei werden z.B. Benutzer und Gruppendaten übertragen. Die Zeiten und Intervalle der Replikation sind einstellbar und müssen sowohl dem Gedanken der Kostenreduzierung als auch der Funktionssicherheit getroffen werden.

Die Replikation erfolgt immer vom Primary-Domain-Controller (PDC) aus. Der PDC prüft regelmäßig seine Datenbank (SAM) ab, ob Änderungen vorhanden sind. Dazu trägt jeder Datensatz eine Revisionsnummer, welche bei Änderungen erhöht wird. Wenn ja, dann werden die Backup-Domain-Controller (BDC) darüber informiert. Es liegt dann an den BDC’s, eine Kommunikation aufzunehmen, und sich die Daten zu holen. Der PDC versendet die Daten nicht von alleine. Nach einer einstellbaren Zeit fordert

der PDC die BDC's zu einer Synchronisation auf, auch wenn keine Änderungen aufgetreten sind.

Die Werte für die Domainreplikation werden in der Registry eingestellt. Da prinzipiell jeder BDC auch zum PDC umgestellt werden kann, sollten die Werte für alle Domaincontroller eingestellt werden.

```
HKEY_LOKAL_MACHINE\System\currentcontrolset\service\netlogon\parameter
```

"Pulse" regelt die Zeit zwischen zwei Überprüfungen auf Änderungen in der SAM (Security Datenbank) auf dem PDC und damit bei Änderungen den Versand der Benachrichtigung an die BDC, die noch nicht uptodate sind. (default: 5min, mögliche Werte liegen zwischen 60 und 3600 Sekunden)

"PulseMaximum" stellt die maximale Zeit nach der ein BDC eine Anfrage an den PDC stellt, auch wenn keine Änderungen vorliegen (default 2h, mögliche Werte liegen zwischen 60 und 86400 Sekunden. Dieser Wert darf nicht auf dem PDC eingestellt werden.
Hohe Werte reduzieren die Verbindungsaufbauten, aber verzögern Änderungen, d.h. wenn der Administrator einen Benutzer am PDC anlegt, kann es einige Zeit dauern, bis die BDCs die Informationen haben. Damit kann sich ein Anwender z.B. einer Außenstelle nicht sofort anmelden. Die Synchronisation kann im Gegensatz zur WINS-Replikation nicht forciert werden.

Der Parameter "ReplicationGovernor" (DWORD) mit werten Zwischen 0 und 100 bestimmt in Prozent, wieviel bei einem Durchlauf repliziert wird. Damit kann die WAN-Belastung reduziert werden (z.B. auf langsamen Strecken). Ein Wert von 0 führt aber dazu, daß NIE eine Replikation stattfindet. Der Wert ist auf jedem BDC dynamisch änderbar, so daß z.B. die Zeit der Replikation auf die Nachtstunden verlegt werden kann (REGINI mit WINAT gesteuert)

2.3 Browser

Der Browserdienst bei Microsoft Netzwerken verwaltet die Liste der Rechner, Arbeitsgruppen und Domains in einem Netzwerk. Der Domain-Master-Browser (DMB, der primäre Domain-Controller) tauscht sich dabei mit den Master-Browsers (MBR, meist die Backup-Domain-Controller) regelmäßig aus. Dazu gibt es noch je 32 Stationen einen Backup-Browser, welche ebenfalls die Liste mitführen. "Potentielle Browserserver" werden vom MBR zum Backup-Browser erhoben, wenn weitere 32 Stationen hinzugekommen sind Server ohne Browserserverfunktion brauchen nicht beachtet zu werden. (Siehe auch Microsoft Knowledge Base Artikel Q102878).

Da die meisten großen Netzwerke an jedem Standort einen BDC installiert haben, werden dadurch auch alle zwölf Minuten Daten des Browserdienst ausgetauscht. Dabei verbindet sich der MBR alle zwölf Minuten mit dem DMB und sendet seine lokale Liste zum DMB und erhält im Gegenzug die globale Liste. Diese Verbindung erfolgt über Remote procedure Calls (RPC) mittels Named-Pipes und kann auch länger dauern. Dadurch werden gerade bei ISDN-Wählverbindungen auch mehrere Gebühreneinheiten fällig. Auch nach Abschluß der Kommunikation bleibt die logische Verbindung bestehen und wird je nach Einstellung in der Regel nach zehn Minuten abgebaut, wodurch wieder eine WAN-Verbindung notwendig ist. Zwei Minuten später ist erneut die zwölf Minuten Frist verstrichen und das Spiel beginnt von vorne. Die Verkürzung der Einheiten und Reduzierung der Kosten von 23Pf auf 12Pf je Einheit haben hier schon viel Geld gespart. Optimierungen sind bei Windows NT4 und, Windows NT 3.51 (ab SP2, Siehe auch Microsoft Knowledgebase Artikel Q134985) durch Änderung einiger Parameter in der Registry möglich:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters
\
```

Der Schlüssel ”KeepConn” bestimmt die Zeit, wie lange eine logische Verbindung gehalten wird. Dieser Parameter sollte kurz gewählt werden, z.B. 5 Sekunden. Dadurch wird der ”Nachschlag” nach zehn Minuten zum Abbau der NamedPipe reduziert.

Ein weiterer Trick ist die Einschaltung einer zeitgesteuerten Filterung dieser Pakete auf dem Router. Wenn der Verlust der Browserliste zu arbeitsfreien Zeiten problemlos ist, können damit Kosten gespart werden.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser\Parameters
```

Der Schlüssel ”MasterPeriodicity: (DWORD) gibt an, alle wieviel Sekunden der MBR den DMB kontaktiert. Der Standardwert 720 (12 Min) kann auf Werte zwischen 300 (5 min) und 4294967 (49 Tage und 8 h) eingestellt werden. Der Wert kann dynamisch geändert werden und wird ohne Neustart gültig. Dieser Wert sollte auf jedem Computer gesetzt werden, welche zum Browserserver werden kann (also auch potentielle Browserserver). Die Änderung dieses Parameters auf dem DMB wirkt sich direkt auf die Abfragehäufigkeit des WINS-Servers aus.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser\Parameters\BackupPer
iodicity: (DOWRD)
```

Die BackupBrowser verbinden sich ebenfalls regelmäßig mit dem MBR. Dieser Zyklus kann mit dem Schlüssel ”BackupPeriodicity” (DWORD) eingestellt werden. Hier sind ebenfalls Der Standardwert von 720 Sekunden (12 Min) kann im Bereich zwischen 300 (5min) und 4,294,967 (0x418937 hex =49 Tage 8h) verändert werden. Der Parameter wird erst beim Neustart eingelesen. Dieser Verkehr ist jedoch immer auf dem gleichen Subnet und verursacht damit mit bei WAN-Bridges zusätzliche Kosten.

Wird die Einstellung ebenso auf dem DomainMasterBrowser eingestellt, so bestimmt dieser die Zeit zwischen den Anfragen an einen WINS-Server nach der Domainliste, was ebenso WAN-Verkehr verursachen kann.

Bestimmt, wie oft ein BackupBrowser den Masterbrowser anspricht.

2.4 Drucker

Wenn ihr PC einen Drucker freigegeben hat, aktiviert Windows einen eigenen Prozeß, um die Existenz dieses Druckers allen anderen Systemen bekanntzugeben. Diese Broadcasts belasten ein Netzwerk aber nicht die WAN-Verbindungen, da Router diese Pakete nicht weiterleiten. Nur WAN-Bridges und Router mit aktivierter NetBIOS-Weiterleitung produzieren hier Kosten. Dieser Thread kann deaktiveirt werden, mit der Folge, daß die Freigabe nicht mehr im Browser bekannt ist. Dazu muß in der Registry der Parameter

```
HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Print\DisableServerThread (DWORD)
```

auf ”1” gesetzt werden.

2.5 DHCP

Das DynamicHostConfigurationProtocol (DHCP) ersetzt und erweitert das bisherige BOOTP-Protokoll. Es erlaubt, daß Arbeitsstationen im Netzwerk dynamische Informationen über ihre IP-Adresse, Router, DomainName etc. erhalten. Auch zusätzliche Informationen wir der nächste WINS-Server, WINS-Typ und DNS-Server können so einfach verteilt werden. Änderungen sind nur zentral auf dem DHCP-Server notwendig und werden beim nächsten Neustart der Clients automatisch aktualisiert. Damit wird die Verwaltung eines IP-Netzwerkes stark vereinfacht und die individuelle

Einstellung der Daten auf den jeweiligen PCs und die Verwaltung in Listen reduziert.

Zur Ausfallsicherheit können mehrere DHCP-Server ein Netzwerk bedienen. Allerdings können nicht alle die gleichen Adreßbereiche verteilen, da eine Synchronisation untereinander aktuell nicht stattfindet, d.h. jeder Server muß einen eigenen Bereich verteilen. Netzwerksegmente, welche durch einen Router abgetrennt sind und keinen eigenen DHCP-Server besitzen, können über einen BOOTP-Relay bzw. DHCP-Proxy bedient werden. DHCP-Anfragen eines Clients werden als Broadcast abgesetzt und von Switches oder Bridges problemlos weitergeleitet. Bei Routern ist oftmals einstellbar, daß diese DHCP-Anfragen wie eine Bridge weiterleiten.

In der Regel haben abgesetzte und per ISDN-Router angebundene Filialnetzwerke einen eigenen DHCP-Server, so daß DHCP nicht zu unerwünschten Verbindungsaufbauten führt. Die Administration ist weiterhin auch über ISDN möglich. (Windows NT DHCP-Servermanager)

2.6 WINS

Der Windows Internet Name Service (WINS) von Microsoft sorgt für die Auflösung von Netzwerknamen und Adressen. Dieser ist nicht auf das Protokoll TCPIP beschränkt und funktioniert auch mit NetBEUI und IPX. In jedem größeren Netzwerk sollte mindestens ein WINS-Server installiert sein. Mehrere WINS-Server können sich untereinander synchronisieren und so die Last teilen bzw. Eine Ausfallsicherheit gewährleisten. Dazu muß man beim Setup der Clients diesen beide WINS-Server mitteilen.

Wird kein WINS-Server genutzt, dann schalten alle Clients auf ”Broadcast”-Node, d.h. alle Namensauflösungen werden mittels Broadcasts gelöst. Eine Funktion über Router hinweg ist dann nur mit Tricks, statischem DNS oder lokalen LMHOSTS-Dateien (hoher Pflegeaufwand) möglich. Ein WINS-Server reduziert daher die Anzahl der Broadcasts im Netzwerk und verbessert die Namensauflösung. WINS ersetzt nicht den Browserdienst, welche eine Liste der Computer der Domain vorhält, sondern hilft nur bei der Auflösung von gezielt angefragten Namen, z.B. beim Zugriff auf Dateien per UNC-Pfad (\\SERVER\SHARE\VERZEICHNIS\DATEI\} oder per TCPIP (ping hostname). Jeder WinsClient meldet registriert beim Start seinen Namen beim Server. Er erhält eine Bestätigung vom WINS-Server mit einem ”Time to Live” (TTL)-Wert. Nach 50% dieser Zeit sendet der Client ein ”Renew”. Im Hinblick auf WAN-Leitungen sollte daher ein lokaler WINS-Server benutzt werden. Ausfallsicherheit wird dann durch einen zweiten lokalen WINS-Server oder den Broadcastmode erreicht Ein Wins-Server kann meist über 1000 Registrierungen pro Minute verarbeiten und etwas weniger Anfragen beantworten. So kann ein WINS-Pärchen normal bis zu 10000 Stationen bedienen.

Bei räumlich getrennten Netzwerken bietet es sich an, jeweils mindestens einen WINS-Server vor Ort stehen zu haben, welche sich dann untereinander abgleichen. Damit wird zuverlässig verhindert, daß Clients über WAN-Verbindungen hinweg eine Namensauflösung versuchen. Die Anwender genießen eine höhere Geschwindigkeit und die WAN-Leitung wird effektiver genutzt bzw. die Kosten halten sich im Rahmen. Dies ist um so wichtiger, da auch DomainBrowser regelmäßig den WINS-Server nach einer Domainliste befragen und dadurch ebenso WAN-Verbindungen aufgebaut werden könnten.

Der WINS-Server sammelt die Daten, nach denen er zukünftig gefragt wird vom Netzwerk ein. Jeder Rechner oder Dienst, der neu startet oder sich verändert, teilt dies dem lokalen Netzwerk durch einen Broadcast in Abständen von 1,2,4,8 und dann alle weiteren 12 Minuten mit. Der WINS-

Server sammelt diese ein und verwaltet sie. Wenn Router die Fähigkeit besitzen, NetBios-Broadcasts wie eine Bridge weiterzuleiten, entstehen Kosten auf der WAN-Seite (IPX-Packet Typ20, bzw TCPIP-Port 137,138 und 139). Router sollten diese Pakete blockieren.

Informationen über andere Dienste und Rechner in anderen Netzwerken erhält der lokale WINS-Server über die Replikation zwischen WINS-Servern. Hierbei kann unterschieden werden, wer an wen Daten sendet. Es ist nicht notwendig, dass eine gegenseitige Replikation erfolgt. So ist z.B: denkbar, dass der WINS-Server einer Firmenzentrale seine Daten regelmäßig an die Vertriebsniederlassungen sendet. Da aber nur sehr wenig Dienste in den Niederlassungen aktiv sind, könnten diese in der Zentrale ”statisch” eingetragen werden. So ist keine Replikation zur Zentrale hin notwendig. Übertragungskapazität und Kosten werden gespart, aber in der Zentrale sind z.B. die Server der Niederlassung auch eingetragen, wenn diese nicht verfügbar sind.

Die Parameter für die Replikation sind in der Registry bzw. Mit dem WINS-Manager einstellbar. Der WINS-Server im Push-Betrieb prüft regelmäßig, ob Daten verändert worden sind. Wenn ja, dann wird der Gegenpartner benachrichtigt. Dieser holt sich dann die neuen Daten. (Pull). Die Zeiten sind einstellbar. Wichtig ist eine schnelle Replikation dann, wenn Dienste sehr oft ihren Status verändern, (z.B. Windows for Workgroups-Rechner als Fileserver, die mehrmals am Tag neu gestartet werden). Dienste, welche durchgehend laufen, können auch mit geringen Replikationszyklen ausreichend bekannt gemacht werden. Ein weiteres Argument für dedizierte Server im 24h Betrieb und gegen ”Workgroupnetzwerke”

Die Parameter des WINS-Service finden sich in der Registrierdatenbank unter

```
HKEY_LOCAL_MACHINE\CurrentControlSet\Services\wins
```

Alle für die WAN-Synchronisation wichtigen Parameter können und sollten mit dem WINS-Manager eingestellt werden.

2.7 Verzeichnisreplication

Windows NT 3.51 und 4.0 bieten beide die Möglichkeit, automatisch Verzeichnisse zu replizieren. Dabei wird regelmäßig geprüft, ob Veränderungen in einem Verzeichnis vorliegen, und diese dann replizieren. Die Replikation ist einem COPY gleichzusetzen. Bei der Replikation werden die kompletten Daten übertragen. Wird in einer Datei nur ein Teil geändert, wird trotzdem die komplette Datei neu übertragen. Dieser Replikationsdienst wird überwiegen dazu eingesetzt, Logonscripts einer Domain unter den verschiedenen DomainControllern zu synchronisieren. Die Synchronisation von Daten ist möglich, aber oftmals nicht sinnvoll.

Die Parameter der Verzeichnissynchronisation finden sich in der Registrierdatenbank unter

```
HKEY_LOCAL_MACHINE\CurrentControlSet\Services\Replicator
```

Eine elegante Möglichkeit, eine bessere und leistungsfähigere Replikation zu erreichen, ist einfach die Variante Dateien per XCOPY zu kopieren. Dies kann mit dem Zeitplandienst und dem Programm WINAT (Windows Resource Kit) elegant realisiert werden. Zumal hierbei auch mehrere Verzeichnisse unterschiedlicher Quellen repliziert werden können. Individuell zu Lösen ist dabei noch die Vergabe der Zugriffsrechte.

2.8 DNS

Mit dem Einsatz von TCPIP bietet sich an, die Namensauflösung um den hierarchische und replizierenden DomainNameService (DNS) zu erweitern. Im Gegensatz zu WINS sind die Einträge in der DNS statisch und dienen primär der Auflösung Hostname zu IP-Adresse. Wenngleich auch andere Dienste (Mail, HostInfo etc) damit verwaltet werden können. Eine DNS-Zone wird dabei zur Ausfallsicherheit und Lastverteilung gerne durch mehrere DNS-Server bedient. Damit können Namensanfragen schnell lokal aufgelöst werden. Zwischen den DNS-Servern findet ebenfalls eine Replikation statt. Die Daten für die Replikation werden bei der Definition der DNS-Zone vorgegeben. Je nach DNS-Server sind die Werte anders einzustellen. Beim BIND erfolgt die Steuerung per Textdatei. NetatWork benutzt aktuell folgende Konfiguration:

```
@        IN SOA    nts-nawpb.netatwork.de. admin.netatwork.de. (
              96090503 ; serial number
              43200    ; refresh every 12 hours
              7200     ; retry after 2 hours
              1209600  ; expire after 2 weeks
              172800)  ; default ttl is 2 days
```

Dabei bedeutet die ”serialNumber” eine fortlaufende Nummer, welche bei jeder Änderung im DNS hochgezählt werden muß. Alle nachgeschalteten DNS-Server prüfen alle 12 Stunden (nächste Parameter), ob die Seriennummer höher ist. Erst dann werden die Daten neu geladen. Sollte eine Verbindung nicht zustande kommen, wir dies alle 7200 Sekunden (2h) erneut versucht. Erst wenn 2 Wochen keine Antwort gekommen ist, wird angenommen, daß die Domain nicht mehr existiert.

Diese Replikation findet regelmäßig statt und beansprucht nur sehr wenig Bandbreite, aber führt speziell bei Wählverbindungen immer wieder zu Verbindungsaufbauten. Die baumartige Struktur der DNS im Internet und ”getaktete” Updates der DNS bewirken, daß Änderungen der DNS nicht sofort überall bekannt werden, sondern nach und nach ”verteilt” werden. Hohe Zeiten verursachen daher wenige Verbindungsaufbauten aber entsprechend lange Zeiten, bis die Daten auf allen DNS-Servern wieder konsistent sind. Ist abzusehen, daß Änderungen notwendig sind, so gibt es die Möglichkeit, die ”refresh”-Zeit z.B. auf 1 h runterzusetzen. Nach der alten eingestellten Zeit haben dann alle andere DNS-Server die neue Intervallzeit. Werden dann die Änderungen gemacht, kann danach wieder die alte lange Zeit eingestellt werden. Die nachgeschalteten DNS-Server werden noch mit der alten kurzen Zeit die neuen Daten sehr schnell übernehmen und dann wieder auf die lange Zeitspanne umschalten. Damit wird erreicht, daß die Daten sehr schnell bekannt werden. Der DNS-Server bei Windows NT4 folgt diesen Regeln. Die Parameter werden jedoch im DNS-Manager eingestellt.

2.9 Lizenzservice

Bei WindowsNT ist auch der Lizenzservice oftmals Grund für Verbindungsaufbauten, da ähnlich wie bei er Domaindatenbank auch die Lizenzeinträge synchronisiert werden müssen. Die Lizenzsynchronisation ist dabei innerhalb einer Domäne möglich. Dazu bestimmt man einen Hauptserver innerhalb der Domäne. Dies kann der PDC sein, aber auch jeder andere Server ist denkbar. Bei der Replikation überträgt jeder untergeordnete Server seine Lizenzdaten zum Hauptserver und bezieht von dort dann wieder eine aktualisierte Liste. Die Replikation kann in regelmäßigen Abständen oder zu bestimmten Zeiten erfolgen. Standardmäßig erfolgt die Replikation alle 24 Stunden, so daß eine neu eingespielte Lizenz auf einem Server bis zu 48 Stunden dauern kann, bis all

anderen Server davon wissen. Mit dem Lizenzmanager können diese Zeiten reduziert oder erhöht werden. Für eine gleichmäßige Lastverteilung ist es auch möglich, daß jeder Server zu einer anderen Zeit Kontakt zum Hauptserver aufnimmt.

2.10 Ein paar Worte zur Realisation

Die Veränderung von Daten in der Registry ist mit äußerster Vorsicht zu verwenden. Je nach betroffenen Dienst werden die Einstellungen sofort oder erst nach dem Neustart gültig. Mit dem Programm REGINI aus dem Resource Kit können Änderungen auch mittels Kommandozeile erfolgen. Damit können Änderungen automatisch erfolgen und mit dem Zeitplandienst auch regelmäßig ausgeführt werden.

Die Registry anderer WindowsNT-Rechner kann auch remote mit dem Registryeditor (REGEDT32.EXE) geändert werden. Falsche Einträge in der Registry können das komplette System unbrauchbar machen und eventuell erst durch Einsatz der Notfalldiskette wieder nutzbar werden. So habe ich selbst beim Verändern der Zeiten für die Domainreplikation (PulsMaximum) einen unabsichtlich PDC lahmgelegt. Für die Überprüfung der durchgeführten Werte ist ein Netzwerkanalysator (Sniffer®, NetMon, Lanalyser oder ähnliches sinnvoll. Einige Router können selbst einen Trace mitschneiden und die Datenpakete protokollieren. Eine reine Analyse der Verbindungsaufbauten und abbauten ist nur bedingt aussagekräftig.

2.11 Analyse des Netzwerkverkehrs

Zur Kontrolle und Analyse der Kosten wurde auf dem NT4-Server der mitgelieferte NETMON installiert und gestartet. Ich empfehle jedem Administrator, den Microsoft Netmon von Windows NT 4 Server mit zu installieren, auch wenn er in der Funktion beschnitten ist. Die voll funktionsfähige Version ist mit SMS verfügbar.

2.12 Verursacher von WAN-Verbindungen

Im Hinblick auf eine Kostenreduzierung im ISDN wurden diverse Tätigkeiten durchgeführt, um das Verkehrsaufkommen über ISDN zu bestimmen. Nicht jede Aktion verursacht einen Verbindungsaufbau. Teilweise gibt es zyklische Anforderungen, welche durch passende Konfiguration herabzusetzen oder ganz zu blockieren sind. Der Novell MPR besitzt noch keine Funktionen um NT-relevante Datenpakete zu spoofen, zu puffern oder bis zur nächsten regulären Verbindung zu verzögern.

In Ermangelung von Clients in dieser Domain beziehen sich die Anmeldungen nur auf den NT-Server selbst.

Ursachen für regelmäßige Verbindungen zwischen NT-Systemen sind:

- Domain browsing
- WINS replication
- Directory replication
- User accounts database (SAM) replication
- Printer browsing
- Other (DHCP, etc.)

Funktion	Auswirkung	Lösung
Anwender meldet	Verbindung wird aufgebaut,	Blockierung der Pakete

Funktion	Auswirkung	Lösung
sich an der Domäne an	Obwohl ein BDC vor Ort ist, wird der PDC gesucht. Wird die Verbindung zum PDC absichtlich blockiert, erfolgt die Anmeldung über den BDC..	zum PDC durch intelligente Filter der Router, um die Authorisierung über den PDC zu vermeiden.
”Browse” in der Netzwerk-verbindung innerhalb der Domain	kein Verbindungaufbau. Die Daten sind im lokalen Masterbrowser (BDC) verfügbar, Namensauflösung per Broadcast bleiben lokal. Der Masterbrowser im Segement übernimmt die Beantwortung der Anfragen	Konzeptionell sollte ein WINS-Server je Niederlassung zu bestimmten Zeiten mit der Zentrale synchronisieren. Die Clients sollten nur den lokalen WINS-Server kennen
”Browse” in anderen Domain	Verbindung wird aufgebaut, da der DomainMasterbrowser der anderen Domain angefragt werden muß	Nicht zu verhindern. Wenn der Browser nicht erwünscht ist, Filterung der Pakete. Dank WINS kann eine direkte Verbindung zum bekannten Hostnamen hergestellt werden.
Start des ”Benutzer-managers” unter NT	Verbindung wird aufgebaut. Dies ist besonders wichtig zu wissen, da z.B. bei der Neuanlage eines Benutzer aus einer Außenstelle eine Verbindung zum PDC der Zentrale notwendig ist.	Nicht zu verhindern. Hier ist z.B. das Konzept der NDS von NetWare leistungsfähiger
Start des Servermanagers	Verbindung wird aufgebaut	Nicht zu verhindern
SHUTDOWN des Servers	Es wird keine Verbindung aufgebaut, d.h. der BDC benachrichtigt den PDC nicht. Umgekehrt wird der PDC immer wieder versuchen, eine Verbindung zum BDC aufzubauen, wenn Synchronisationen anstehen.	keine Aktion notwendig Wird eine Außenstelle deaktiviert, so sollte zuerst der entsprechende Eintrag im Router deaktiviert werdenm, Damit Versuche des PDC zur Replikation keine Kosten verursachen.
Neustart des BDC	BDC kontaktiert PDC um Updates oder komplette Synchronisation zu empfangen Auch WINS-Server kann Anfangsreplikation ausführen	Anfangsreplikation kann in der Registry abgeschaltet werden, ist aber nicht sinnvoll.
PDC <-> BDC Synchronisation	PDC prüft regelmäßig auf Änderungen in der SAM. Sind diese eingetreten, werden die BDCs benachrichtigt. Diese holen dann aktiv die Änderungen ab.	Werte in der Registrierdatenbank anpassen

Funktion	Auswirkung	Lösung
Anwender ändert Paßwort	Verbindung wird aufgebaut Änderung wird im PDC abgelegt,	Blokade nicht sinnvoll
Im Ruhezustand sendet der Windows NT BDC unregelmäßig im Abstand von 3-12 Minuten jeweils zwei Anfragen ”Query PDC”.	Verbindung wird aufgebaut. Der BrowserService sucht den DomainMasterBrowser	DomainMasterBrowser und PDC aktiv halten. Bei längerem Ausfall des PDC einen BDC zum PDC hochstufen

Je mehr WindowsNT im WAN eingesetzt wird, desto eher wird die genaue Kenntnis der Kommunikation wichtig. Vom Novell-Umfeld her sind die üblichen Pakete (SAP, RIP) bekannt und die meisten Hersteller von Routersoftware haben sich Techniken zur Reduzierung von Datenpaketen einfallen lassen (Spoofing, Blockierung). Gerade auch im Bereich der NDS und Zeitsynchronisation haben die aktuellen Router (z.B. AVM) Forschritte erzielt. Wenn der Administrator die verschiedenen Verursacher von WAN-Verkehr eines WindowsNT-Netzwerkes kennt, kann es recht einfach und kontrolliert die Kosten im Zaum halten und die Funktion sicherstellen. Allerdings sind speziell bei Zugriffen auf Benutzerdaten die Nachteile der Domainkonzeption gegenüber der verteilen Novell NDS bemerkbar.

2.13 Einstellungsvorschlag

Beim PDC muß der Eintrag PulseMaximum entfernt werden, da sonst der PDC nicht mehr startet !

```
REGEDIT4

[HKEY_CURRENT_USER\System\Currentcontrolset\Services\netlogon]
"Pulse"="3600"
"PulseMaximum"="86400"
"ReplicationGovernor"="100"

[HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters
]
"KeepConn"="5"

[HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Services\Browser\Parameters]
"MasterPeriodicity"="28800"
```

2.14 Andere interessante Dokumente

Microsoft Knowledgebase:

Q120151 Browsing a Wide Area Network with WINS

Q133241 Browsing Domain Master Browsers w/ Multiple NICs and Protocols

Q136712 Common Questions About Browsing with Windows NT

Q117633 How Browsing a Wide Area Network Works

Q134304 Troubleshooting Browsing with Client for Microsoft Networks