Allgemeines zum Praktikum Computernetze im WS 2001/02

Insgesamt werden 6 Versuche mit jeweils 90 Min. Dauer angeboten, Ersatztermine werden nicht angeboten. Die Versuche dienen dazu, den in der Vorlesung vermittelten Stoff durch praktische Beispiele zu vertiefen und zu ergänzen. Die Inhalte der Versuche sind damit auch relevant für die Prüfung, die Anwesenheit ist insofern auch nicht Pflicht, sondern schlicht und einfach sinnvoll.

Vorbereitung:

Die Vorbereitung der Versuche ist unterschiedlich zeitaufwendig. Einige erfordern nur ein generelles Verständnis des Stoffes, andere erfordern, daß Sie sich vorher genaue Gedanken zum Inhalt machen, damit der Versuch in der angegebenen Zeit überhaupt durchführbar ist. Wenn Sie bei diesen Versuchen nicht vorbereitet sind, haben Sie weniger vom Versuch selbst.
Zu manchen Versuchen werden Ihnen Handbücher bzw. Auszüge aus der On-Line Dokumenation der Produkte zur Verfügung gestellt. Diese Handbücher/Online Dokumentation müssen natürlich NICHT von vorne bis hinten durchgelesen werden, sie dienen als Nachschlagemöglichkeit auch während des Versuchs. Lesen Sie die entsprechenden Kapitel soweit, daß Sie den generellen Ablauf nachvollziehen können, und daß Sie wissen, wo Sie evtl nachschauen können.

Durchführung:

Für manche Versuche wird der Zugriff auf den Laborserver des Labors Betriebssysteme benötigt. Dies ist ein NetWare Server mit Namen LABSERVER mit folgender Organisation der NDS:

[Root]
O=LBS
OU=Labor

Der Server Kontext ist OU=Labor, dort sind jeweils Sie als Benutzerteams definiert. Die Gruppen heißen:

- Team1 bis Team12

Dieselbe Nummerierung wird auch in manchen Versuchen für NDS Objekte oder Verzeichnisse verwendet, z.B. für den Versuch 1 als Organisationsname XYZ#, d.h. die Gruppe Team3 würde dann die Organisation XYZ3 erstellen usw. Dieselben Bezeichnungen sollen auch für von Ihnen anzulegenden Objekte, Dateien usw. in den Versuchen verwendet werden.

Novell Serverkonsole

Sie verwenden die oben angegebenen Benutzerkennungen, teilweise werden auch andere verwendet, diese finden Sie in der jeweiligen Praktikumsanleitung. Grundsätzlich gilt: **Sie loggen sich an einem Client ein um eine Verbindung zu einem Fileserver aufzubauen.** Windows 2000 erlaubt das einloggen an einem Server direkt, da hier ein Clientprozeß mit auf dem Server läuft. Nachdem Novell NetWare 4.x keine graphische Benutzeroberfläche auf dem Server selbst zur Verfügung stellt, läuft der Client Prozeß grundsätzlich nur auf einer anderen Station, nicht aber auf dem Server. Einen Novell Serverbildschirm erkennen Sie am Prompt mit " : ", also z.B. "Asterix: ". An dieser Station können Sie also kein "Login" eintippen!!!
NetWare 5 stellt eine graphische Benutzeroberfläche unter Java auf der Konsole zur Verfügung, hier ist ein einloggen gar nicht erst nötig. Im Praktikum wird diese Java-Konsole nicht verwendet.

Aufbau Novell Client

Der Novell Client unter Windows ist in die Windows Oberfläche integriert. Sie finden in der Windows Taskleiste ein großen rotes „N“. Hier können Sie den Client konfigurieren und auch aufrufen. Bei einem zweiten Login können Sie im Anmeldefenster auswählen, ob dabei die ursprüngliche Verbindung beibehalten oder gekappt werden soll. Letzteres ist der Defaulteintrag.
Der Novell Client unter Windows ist in die Windows Oberfläche integriert. Sie finden in der Windows Taskleiste ein großen rotes „N“. Hier können Sie den Client konfigurieren und auch aufrufen. Bei einem zweiten Login können Sie im Anmeldefenster auswählen, ob dabei die ursprüngliche Verbindung beibehalten oder gekappt werden soll. Letzteres ist der Defaulteintrag.
Nachdem Windows NT bzw. 2000 seine eigene lokale Sicherheitstruktur mitbringt, müssen Sie sich beim Login zweimal einloggen, einmal in das lokale Windows und dann zusätzlich in die NDS. Wenn Sie die Passworte für Windows und Novell nicht übereinstimmen, werden Sie nach dem ersten Login in die NDS gleich noch nach dem Passwort nach dem lokal verwendten Benutzerkonto gefragt. Sie können das Anmeldefenster so umschalten, daß sie sich nur lokal in Windows anmelden (und evtl zu einem späteren Zeitpunkt in die NDS).

Login in eine Novell NDS:

NDS erlaubt eine hierarchische Verwaltung von Benutzern, d.h. die Benutzer werden in organisatorischen Einheiten zusammengefaßt, diese wiederum in darüberliegenden organisatorischen Einheiten oder Organisationen. Der höchste Punkt ist die Wurzel [Root] des NDS Baums. Der Standort des Benutzers innerhalb dieser Hierarchie wird als “Kontext” bezeichnet.
Zum Login in eine NDS muß grundsätzlich der Name eines Benutzers inklusive seines Kontexts angegeben werden. Der Kontext wird dabei üblicherweise relativ zur [Root] des NDS Baums gebildet, dies wird durch einen führenden Punkt im Login Kommando festgelegt.
Wenn Sie sich vom Client aus in einen Baum als User “Fluglotsa” in eine Organisational Unit “Leuchtturm” in der Organisation “Orient” einwählen möchten, sind beim Login folgende Angaben nötig:
Entweder:

- Login Name: Fluglotsa
- Kontext: .Leuchturm.Orient (mit führendem Punkt!)

Oder:

- Login Name: .Fluglotsa.Leuchturm.Orient (mit führendem Punkt!)
- Kontext: keine Angabe

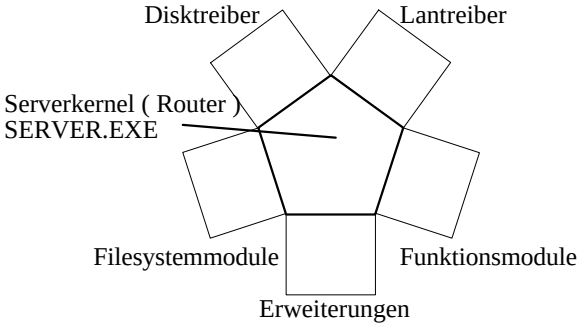
Zudem müssen Sie im Anmeldefenster entweder den Namen des NDS Baumes angeben oder über welchen Server Sie sich in den NDS Baum einwählen.

Mehrfachkonfiguration der Praktikumsrechner

Im Praktikum werden die Rechner für verschiedene parallele Praktikas mit eigenen Konfigurationen verwendet. Auf manchen Rechnern sind Windows (98, NT, 2000 oder 2000 Server) und Novell NetWare Server parallel installiert. Zum Start des Novell Servers wählen Sie beim Systemstart die „DOS/NetWare Partition“ und dann beim nachfolgenden DOS-Auswahlmenü den Menüpunkt „NetWare Server“.

Aufbau NetWare

NetWare besteht aus einem Betriebssystemkern, zu dem im laufenden Betrieb Module, sog. NLMs, dazugeladen werden können.



Lantreiber xxx.LAN
- Herstellerbezogen

Disktreiber xxx.DSK
- AT - Bus
- IDE - Bus
- SCSI - Bus

Funktionsmodule xxx.NLM
- INSTALL.NLM (Installation)
- MONITOR.NLM (Serverüberwachung)

Erweiterungsmodule xxx.NLM
- Gateways
- Printserver
- Faxserver
- Unixkopplung
- Netzwerkmanagement
- Routing (fremde Protokolle)

Filesystemmodule xxx.NAM
- intern: Proprietäres Filesystem (flach)
- emuliert:

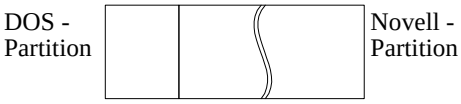
FAT	DOS	File Allocation Table
HPFS	OS/2	High Performance File System
NFS	UNIX	Netware File System
FTAM	OSI	File Transfer, Access and Management
MacOS	MAC	Macintosh Operating System

<u>Start des NetWare Servers</u>

Zum Start des NetWare Servers geben Sie am Dos-Prompt “Server” ein, die NLMs werden mit “Load <Name des NLMs>” dazugeladen. Um das Hochfahren zu automatisieren, gibt es zwei Konfigurationsdateien, die Autoexec.ncf und die Startup.ncf, in denen die entsprechenden Load Kommandos zusammengefaßt werden. Beide erreichen Sie, wenn Sie am Serverprompt “Load NWCONFIG” eingeben, und den Menüpunkt “NCF Fileoptionen” auswählen.

Server- Konfigurationsdateien

- STARTUP.NCF(NCF = Netware Control File)
  liest Disktreiber Info von DOS - Partition



- AUTOEXEC.NCF
  liest alle anderen Module von Novell - Partition

Einige Novell Befehle

Start des Servers:

- Server

Server Konsole:

- Load Nwconfig: Installation und Konfiguration (Netware 5)
- Load Install Installation und Konfiguration (Netware 4)
- Load Monitor: Überwachung des Servers
- Load Inetcfg: Konfiguration der LAN Treiber und Protokolle
- Load Tcpcon: Überwachen des TCP/IP Datenverkehrs sowie der Protokollkonfiguration
- Down: Herunterfahren des Servers
- Restart Server: Neustart
- Exit: Verlassen und Rückkehr zu DOS nach dem Herunterfahhren

Windows Client:

- Login: unter Windows erfolgt über die Windows Anmeldung unter zusätzlicher Angabe des Novell Servers (erweitertes Login Fenster).
- Netzwerkverwaltung: Die Netzwerkverwaltung erfolgt über das Tool NWAdmin.

Nützliche Client Kommandos im DOS Fenster:

- Whoami: Wer bin ich?
- NLIST: Abfragen von Daten aus der NDS
- CX: Feststellen des momentanen Kontextes
- CX /T /R /A Darstellung der kompletten NDS (auch bereits vor dem Login!)

Grundsätzlich können die verschiedenen Optionen für die DOS basierenden Kommandos am Bildschirm abgefragt werden, in dem nach dem Befehl ein “/?” eingegeben wird, z.B. “NLIST /?”.

Versuche:

Folgende Versuche werden durchgeführt:

Versuch 1: NetWare 5 Directory Services (NDS) Management

Unterlagen: Grundlagen der NetWare Verzeichnis Services unter
www.novell.com/documentation/german/index.html

Versuch 2: Desktopmanagement mit Z.E.N.Works 2

Unterlagen: On-Line Dokumentation von Z.E.N.Works und NetWare unter
www.novell.com/documentation/german/index.html

Versuch 3: TCP/IP Routing

Unterlagen: Online Dokumentation (TCP/IP Supervisorhandbuch) im Web unter
http://www.novell.com/documentation/lg/nw312/docui/index.html

Versuch 4: Internet Security

Unterlagen: On-Line Dokumentation der Novell Border Manager Enterprise Edition 3.6 unter
www.novell.com/documentation/german/index.html

Versuch 5: Windows NT 4 Vertrauensstellungen (Trusts)

Unterlagen: Ausdruck der On-Line Dokumentation zu Windows NT

Versuch 6: Netzwerkmanagement mit ManageWise 2.7

Unterlagen: Novell Network Management Guide (als pdf unter
http://www.novell.com/documentation/lg/mwise27/docui/index.html verfügbar)

Versuch 1: NetWare 5 Directory Services (NDS) Management

Vorbereitung:

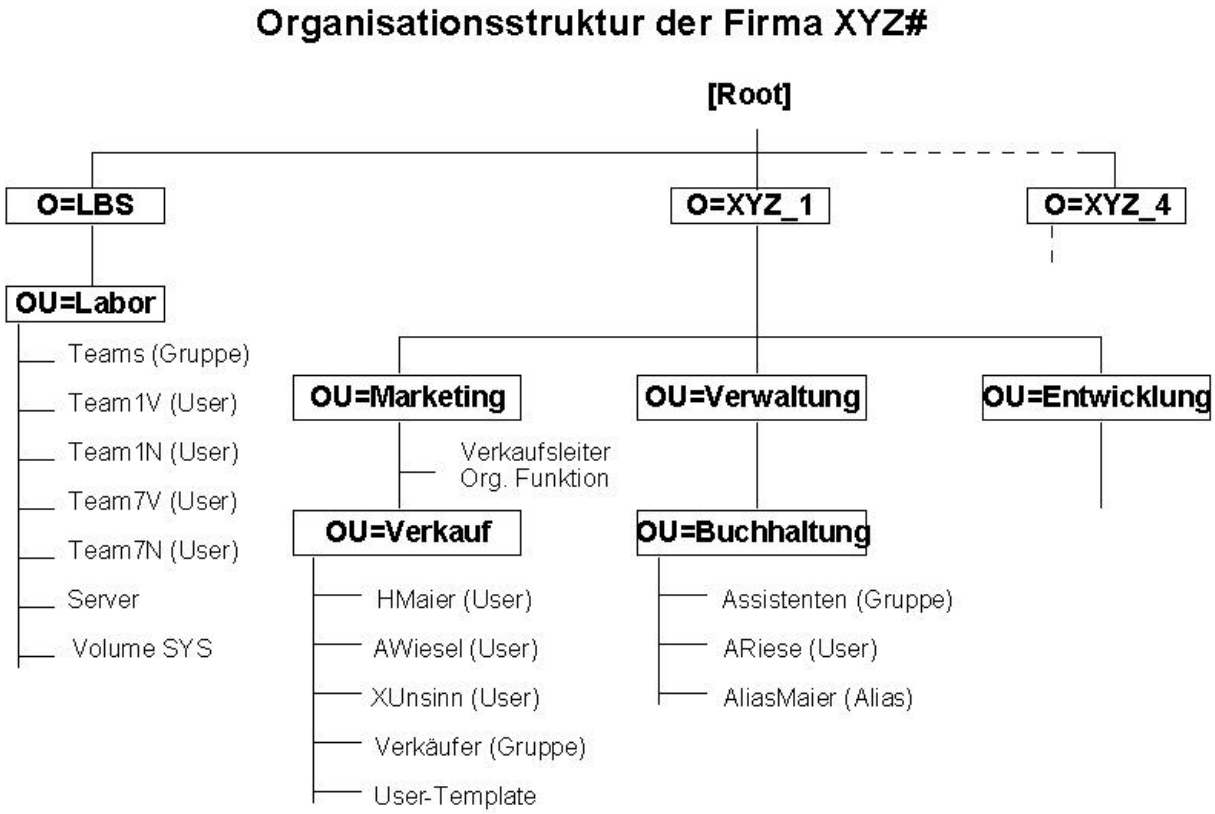
Die Vorbereitung dieses Versuchs ist zugegebenermaßen etwas zeitaufwendig, allerdings führen Sie hierzu doch weitgehend nur eine lesende Tätigkeit aus.
Lesen Sie die Online Dokumentation zu NetWare 4.2 im Internet unter
www.novell.com/documentation/german/index.html → NetWare → NetWare 4.2 die Abschnitte
→ Inhalt → Kurzanleitungen → NDS Baum erstellen und Verwalten sowie
→ Inhalt → Netzwerk-Management-Services → Supervisor-Handbuch → Verwalten von Novell Directory Services

Machen Sie sich mit den Begriffen *Benutzerobjekt* und *Benutzerschablone (Template)* und mit Filesystemrechten vertraut.
Nach Ihren Bemühungen sollten Sie wissen, was eine NDS ist, welche Objekte es gibt, was deren Eigenschaften sind, was Benutzer und Benutzerschablonen sind. Sie sollten darüberhinaus eine ungefähre Vorstellung des Utilities *NWAdmin (Netware Administrator)* und dessen Möglichkeiten für die Durchführung des Praktikums mitbringen. Ebenfalls sollten Ihnen die Begriffe *Trustee* und *effektives Recht* klar sein.

Wenn Sie Fragen haben, kommen Sie bitte VORHER in die Sprechstunde!

Durchführung:

Für die nachfolgend gegebene Organisationsstruktur der Firma "XYZ#" soll ein NetWare Verzeichnisbaum mit Userobjekten, Gruppenobjekten, Benutzerprofilen (Schablonen) erstellt werden und die Eigenschaften der Objekte verwaltet werden. Verwendet wird dazu das Windows Utility NWAdmin (NetWare Administrator).


Organisationsstruktur der Firma XYZ#
[Root]
O=LBS
O=XYZ_1
O=XYZ_4
OU=Labor
Teams (Gruppe)
Team1V (User)
Team1N (User)
Team7V (User)
Team7N (User)
Server
Volume SYS
OU=Marketing
Verkaufsleiter
Org. Funktion
OU=Verkauf
HMaier (User)
AWiesel (User)
XUnsinn (User)
Verkäufer (Gruppe)
User-Template
OU=Verwaltung
OU=Buchhaltung
Assistenten (Gruppe)
ARiese (User)
AliasMaier (Alias)
OU=Entwicklung

Für diesen Versuch besitzen Sie unter Ihrem Benutzernamen alle nötigen Rechte, um neue Organisationen unter der [Root] anzulegen (C-Recht auf [Root]). Für diese selbsterstellten Objekte erhält dann der Ersteller automatisch alle Rechte.
Jede Praktikumsgruppe kann also unterhalb der [Root] den bestehenden NDS-Baum um einen Zweig erweitern. Dieser soll jeweils mit der Organisation O=XYZ# bzw XYZ# beginnen, wobei # der Nummer Ihres Teams entspricht.

Teil I: Erstellen von Container und Blattobjekten

1. Loggen Sie sich als Labserver/Team# ein. Erstellen mit dem Windows Utility NWadmin (Programmgruppe NetWare Tools) die Organisation O=XYZ# und legen Sie eine Beschreibung und einen Standort fest.

2. Erstellen Sie die organisatorischen Einheiten OU=Marketing, OU=Entwicklung und OU=Verkauf. Legen Sie für OU=Verkauf RF (Read und Filescan) Rechte im Dateisystem auf das Public Directory fest. (Vorgehensweise hierzu: Suchen Sie das Volume Objekt LABSERVER_SYS im Serverkontext, wählen Sie das darunter liegende Verzeichnis "Public" aus. Über Details (rechte Maustaste) öffnen Sie das entsprechnde Menü. Legen Sie über "Trustees dieses Verzeichnisses" den Behälter fest, der die entsprechenden Zugriffsrechte haben soll. Wozu könnte irgendjemand diese Rechte brauchen?

   Antwort: _____

3. Nun zu den Benutzern des Netzes. Erstellen Sie einen Benutzer HMaier unter Verkauf und legen Sie Objekteigenschaften fest:
   - Standort, Telefonnr. , Abteilung, Kennwort (Legen Sie fest, daß es eindeutig sein muß), Adresse.

   Welche Rechte hat der Benutzer auf das Filesystem des Servers? Schauen sie dazu unter den Details des Benutzers seine effektiven Rechte im Filesystem an.
   Loggen Sie sich testweise als Benutzer HMaier ins Netz ein. Und? Klappt's? Na Also.

4. Genauso funktioniert das Anlegen von Gruppen. Erstellen Sie eine Gruppe CN=Verkäufer in OU=Verkauf. Legen Sie folgende Informationen fest:
   - Gruppenmitglied: HMaier
   - Abteilung

Teil II: Administration mehrerer Benutzer mit Benutzerschablonen

Das einzelne Anlegen von Benutzern auf diese Weise ist beim Anlegen mehrerer Benutzer doch etwas ermüdend. Hier eine elegantere Art und Weise:

1. Erstellen Sie eine Benutzerschablone (User-Template) im Behälterobjekt (Container) Verkauf an. Damit legen wir fest, wie ein "Standardbenutzer" in dieser Abteilung auszusehen hat, um mit dieser Information später mehrere Benutzer gleichzeitig erstellen zu können. Legen Sie folgende Informationen fest:
   - Standort, Abteilung, Fax-Nummer,
   - Begrenzen Sie die gleichzeitig möglichen Verbindungen auf 2
   - Legen Sie eine Login Time von Montag bis Freitag 8:00 bis 18:00 Uhr fest

2. Erstellen Sie zwei weitere Benutzer AWiesel und XUnsinn mit Hilfe der Benutzerschablone. Welche Eigenschaften besitzen die beiden neuen Benutzerobjekte?

   Antwort:_____

Teil III: Ausbau des Baumes und Sonderfunktionen

1. Erstellen Sie die Behälterobjekte für die restlichen Abteilungen. Damit ist die Firmenstruktur komplett. Damit auch die Abteilung Buchhaltung nicht leer bleibt, erstellen Sie ein Objekt Gruppe mit dem Namen "Assistenten" und geben Sie wiederum Rechte auf das Filesystem für das Verzeichnis Public. Erstellen Sie einen Benutzer ARiese und fügen Ihn der Gruppe zu. Hier haben wir ja nun schon etwas Übung.

2. Nun wollen wir's aber genau wissen. Erstellen Sie in ein Alias-Objekt "AliasMaier" und zeigen Sie damit auf den Benutzer HMaier in der Abteilung Verkauf. Fügen Sie das Objekt ebenfalls in die Gruppe Assistenten ein. Tragen Sie als aktuellen Kontext im Anmeldefenster *.OU=Buchhaltung.OU=Verwaltung.O=XYZ#* ein. Loggen Sie sich ein als AliasMaier.
   Wie heißt nun der komplette Benutzername (im Login Fenster wird es Ihnen angezeigt, ansonsten hilft auch der Befehl WHOAMI (im DOS Fenster), wörtlich übersetzt wäre das WERBINICH, hier weiter)?
   Was also bewirkt ein Alias?
   Haben Sie Ideen (natürlich haben Sie, Sie sind jung und dynamisch), wie sonst ein Alias einsetzbar wäre?

   Antwort:_____

3. Aus irgendwelchen Gründen (und auch weil es hier steht) denken Sie, daß der Benutzer AWiesel in der Abteilung Engineering besser aufgehoben wäre. Verschieben Sie Ihn also in die Abteilung Entwicklung (Drücken Sie die Taste STRG und verschieben Sie den Benutzer mit der Maus, wir hätten auch sagen können draggen Sie ihn und droppen sie ihn in der Abteilung Entwicklung). Was hat AWiesel nun für effektive Rechte auf das Filesystem?

   Antwort:_____

4. Erstellen Sie in der Abteilung Verkauf ein Objekt "Organisatorische Funktion" mit der Bezeichnung "CN=Verkaufsleiter". Machen Sie sich bei XUnsinn beliebt und "befördern" Ihn zum Verkaufsleiter.

Spätestens nun sollten Ihnen folgende Punkte klar geworden sein:

- Der ungefähre Organsationsstruktur von Objekten innerhalb einer NDS
- Die Bedeutung eines Kontexts
- Die Bedeutung gängier Behälterobjekte
- Die Bedeutung gängier Blattobjekte
- Die Bedeutung von Rechten im Filesystem
- Wenn etwas unklar geblieben ist, fragen Sie.

Versuch 2: Desktopmanagement mit Z.E.N.Works

In diesem Versuch werden folgende Komponenten des Desktopmanagements von Netzen untersucht:
- Management des Zugriffs auf Anwendungssoftware
- Softwareverteilung
- Zentrales Management von Benutzer-Richtlinien
- Inventarisierung
- Remote Control

Hierzu stehen ein NetWare 5 Server mit Z.E.N.Works sowie zwei Windows 2000 Arbeitsstationen zur Verfügung.

Vorbereitung:

Die Online Dokumentation zu Z.E.N.Works finden Sie im Internet unter http://www.novell.com/documentation/german/index.html.
Suchen Sie sie die entsprechende Information anhand der Praktikumsbeschreibung zusammen, damit Sie sie bei der Praktikumsdurchführung gegebenenfalls auf die Hilfe zurückgreifen können.
Machen Sie sich insbesondere mit der Erstellung von Anwendungsobjekten in der NDS mit und ohne AOT File (Application Management) sowie mit dem Erstellen von Richtlinienpaketen (Workstation Management) vertraut. Sie können dabei voraussetzen, daß die zu überwachenden Workstations bereits in der NDS registriert sind (dies ist eine Voraussetzung für das Management von Richtlinienpaketen).
Zudem lesen Sie bitte den Abschnitt über Remote Management.

Durchführung:

Sie arbeiten am Server Majestix als .zenadmin#.zenteam#.lbs. Sie besitzen im Container zenteam# Administratorberechtigung.

Teil I: Management von Anwendungen und Softwareverteilung

1. Starten Sie den NWAdmin und schreiben Sie auf der Eigenschaftsseite Login Script Ihres Containers die Zeile “#nalexpld” in das Login Script für den Container. Damit wird bei jedem Einloggen eines Benutzers in diesem Kontext das Login Script mit diesem Befehl ausgeführt und damit die Client-Komponente für das Anwendungsmanagement (der sog. NAL Explorer) automatisch gestartet.

1. Erstellen Sie ein einfache Anwendungsobjekte (ohne AOT File) für die Datei Kaffee.exe im Verzeichnis \\Majestix\sys\public und für badday.mpg im Verzeichnis \\Majestix\datanss\fun des Servers und weisen sie diese dem Container zur Benutzung zu (Nutzung über NAL, Startleiste und Taskleiste in Windows). Damit erhalten automatisch alle Benutzer in diesem Container durch Vererbung das Recht, diese Anwendungen zu verwenden.

2. Erstellen Sie ein Anwendungsobjekt (mit AOT File) für die Software “Netscape”. Das entsprechende AOT File wurde bereits generiert und liegt im Verzeichnis sys:public\shots\netscape des Servers (dieses AOT File enthält die Installationsinformation, Erklärung siehe unten). Loggen Sie sich als .zenuser#.zenteam#.lbs ein. Starten Sie die Softwareverteilung durch Start der Anwendung im NAL Explorer.

3. Löschen Sie die Dateien des lokalen Netscape und starten Sie die Anwendung erneut im NAL Explorer. Was geschieht?

Teil II: Benutzerrichtlinien

2. Erzeugen Sie ein Richtlinienpaket (Policy package) und wählen Sie hierbei die Erstellung eines kompletten Benutzerrichtlinienpakets (User Policy Package) aus. Nach Erstellung des kompletten Pakets konfigurieren Sie über die Eigenschaft “Details” NT Desktop Preferences und NT User System Policies. Geben Sie hier das Aussehen des Desktops für die Benutzer in Ihrem Container vor und weisen Sie dann das Richtlinienpaket nur dem User zenuser#v,n zu (über die Eigenschaft Associations des Richtlinienpakets). Ein entsprechendes BMP File für den Hintergrund finden sie unter \\majesix\datanss\fun\bitmaps.

3. Loggen Sie sich als zenadmin# und danach als zenuser# ins System ein und vergleichen Sie das Aussehen Ihres Desktops

Teil III: Workstationrichtlinien

Um Workstations über die NDS managen zu können, müssen Sie sich zunächst bei der NDS registrieren und dann in die NDS importiert werden. Die Workstation WINNTPC12 ist bereits registriert, jedoch noch nicht importiert. Zum Import wählen Sie im NWAdmin den Menüpunkt Tools → Import Workstations.

1. Importieren Sie die Workstation in den Container zen.lbs. Bewegen Sie das Workstationobjekt danach in Ihren Container zenteam# (mit NWAdmin → Object → Move).

2. Erzeugen Sie in Ihrem Container ein Workstation-Richtlinienpaket (Workstation policy package). In diesem aktivieren Sie Remote Control Policy sowie Workstation Inventory. Editieren Sie den “Default Package schedule” so, daß alle Aktionen event-gesteuert beim User Login stattfinden.

3. Starten Sie die NT Workstation neu und loggen Sie sich erneut als zenuser# ins System ein.

4. Greifen Sie von der Administrationsworkstation aus dem NetWare Administrator auf die Benutzerworkstation zu (Remote Control). Sehen Sie sich dann die Inventarisierungsinformation über diese Workstation an.

Spätestens jetzt sollte Ihnen klar geworden sein, wie man dutzende, hunderte, oder sogar tausende von Workstations zentral administrieren kann.

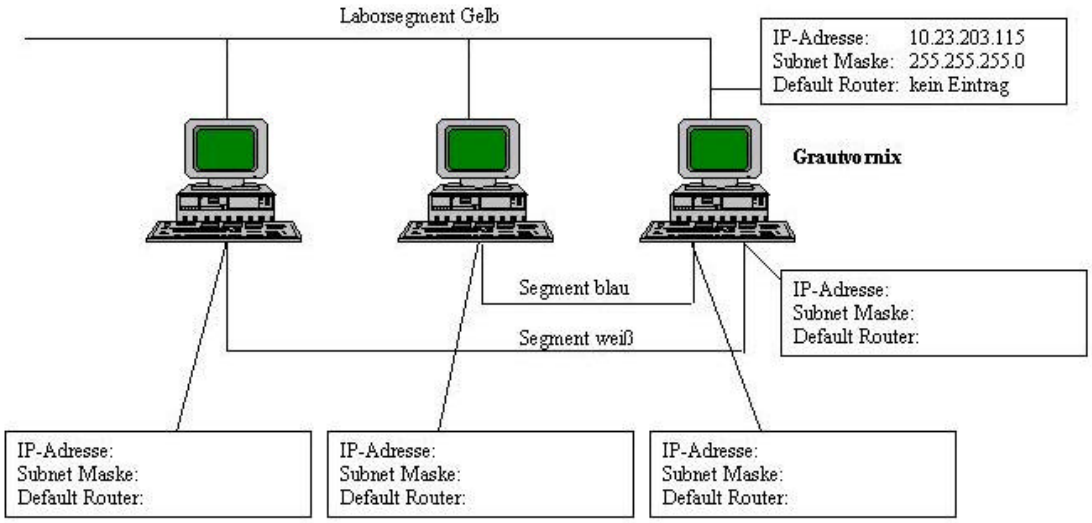
Versuch 3: TCP/IP Routing

Vorbereitung:
Lesen Sie zur Vorbereitung unbedingt das entsprechende Kapitel des Vorlesungsscripts. In diesem ist ein Beispiel für einen Router mit mehren Subnetzen mit unterschiedlichen Subnetzen gezeigt. Dieses Beispiel entspricht in etwa dem vorliegenden Versuch. Lesen Sie darüberhinaus die ausgeteilten Handbuchausdrucke mit Konfigurationsanweisungen für TCP/IP. Machen Sie sich insbesondere mit

- dem INETCFG Utility für den Server
- dem Ping.nlm für den Server und Ping.exe für den Client
- dem TCPCON Utility
- der Konfiguration eines IP-Tunnels (Wie in der Dokumentation von NetWare 4 beschrieben) vertraut.

Laboraufbau TCP/IP-Versuch

Bitte ergänzen Sie als Teil der Vorbereitung die von Ihnen geplanten Adressen und Netzwerkmasken



Planen Sie vor Versuchsbeginn (!) ein TCP/IP Adreß-Schema für ein TCP/IP Netz entsprechend der nachfolgenden Fragen und obigem Netzwerkplan. Tragen Sie alle Netzwerkadressen der Stationen sowie der Anschlüsse des Routers ein. Die für das Labor vorhandene Netzadresse ist das Class-C Subnetz 10.23.203.0 (d.h. Subnet Mask 255.255.255.0). Der Router selbst besitzt im Laborsegment die Adresse 10.23.203.115. Es sollen nun zwei weitere Subnetze gebildet werden, in denen jeweils bis zu 14 PCs verwendet werden könnten. Alle anderen Adressen sollen für alle anderen Rechner im Labor zur Verfügung stehen. Das bedeutet, daß die beiden Segmente als sog. Stub-Subnets eine andere Netzwerkmaske erhalten als die Stationen im Hauptsegment.
Wie muß die Subnet-Maske für die Stationen in den Subnetzen gewählt werden, damit jeweils 14 PCs pro Subnet adressierbar sind?

Welche Adressbereiche währen mögliche Adessbereiche für die Subnetze? Wieviele Subnetze könnten insgesamt gebildet werden?

Welche Ethernet Frames unterstützen TCP/IP?

Lassen Sie Ihr Adresskonzept vor Versuchsbeginn vom Betreuer überprüfen!

Durchführung:

Sie haben einen NetWare 5 Fileserver/Router und zwei Windows 2000 Workstations zur Verfügung. Die Workstations verfügen über zwei Netzwerkkarten. Über eine (Intel) erreichen Sie das Laborsegement, über die zweite (3Com) erreichen Sie das jeweilige eigene Netzwerksegment (Subnetz).

Konfiguration des Novell TCP/IP Routers

1. Starten Sie den Novell Server "Grautvornix". Nach dem Hochfahren konfigurieren Sie ihn dann als TCP/IP Router. Starten Sie dazu das entsprechende Konfigurationsutility mit "LOAD INETCFG" an der Konsole des Fileservers. Legen Sie folgende Parameter fest:
   - Protocols: Enable TCP/IP → IP Packet Forwarding = Router
   - Bindings: Binden Sie das TCP/IP Protokoll unter Angabe der entsprechenden IP-Adressen und Netzwerkmasken an die entsprechenden Karten. Dabei gilt:
     - 3C905_1: blaues Segment
     - 3C905_2: weisses Segment
     - CE100B: gelbes Segment (Hauptsegment des Labors)
2. Starten Sie den Fileserver erneut (Down → Restart Server). Dies ist nötig, damit die Parameter für die TCPIP Konfiguration übernommen werden. Der Befehl "Reinitialize System" würde nicht ausreichen

Konfiguration der Clients in den Segmenten:

3. Konfigurieren Sie Ihre TCP/IP Adressen (Adresse, Maske und Gateway!) auf den Win 2000 Arbeitsstationen. Die Konfiguration kann mittels Ausführen: ipconfig /all zunächst überprüft werden.

Verifizieren Sie die Funktion des Routers

4. Starten Sie das Ping-Utility auf den Workstations oder auch am Server. Überprüfen Sie mittels Ping:
   - Die Verbindungen zwischen den Workstations im jeweiligen Subnetz und dem Router.
   - Von der Workstation eines Subnetzes an die anderen Routerports und zur Workstation im anderen Subnetz zur Verifizierung des Routings
   - an den Fileserver Labserver (10.23.203.200).
   - an den DNS Server im Labornetz mit der Numer 10.23.61.1

5. Sie werden feststellen, daß es dabei keine Probleme gibt. Allerdings sollten Sie eigentlich welche erwartet haben. Welche sind das und warum funktioniert das Routing in diesem Fall trotzdem (ein zugegebenermaßen verzwicktes Problem, aber wenn Sie draufkommen, haben Sie Subnetting wirklich verstanden)?

Ursache:

Überprüfen der Routing Tabellen und des ARP Cache des Routers

6. Starten Sie auf der Server Console “Load TCPCON”
    - Suchen Sie Routing Tabelle sowie die Tabelle zur Zuordnung von IP und Hardwareadressen (ARP Tabelle, ARP Cache).
    - Greifen Sie aus dem TCPCON Utility durch Änderung der Adresse auf den Fileserver LABSERVER zu und überprüfen Sie seine Routing Tabellen auf einen Eintrag für Ihre beiden Subnetze. Sind Einträge vorhanden?

Konfiguration eines IP-Tunnels

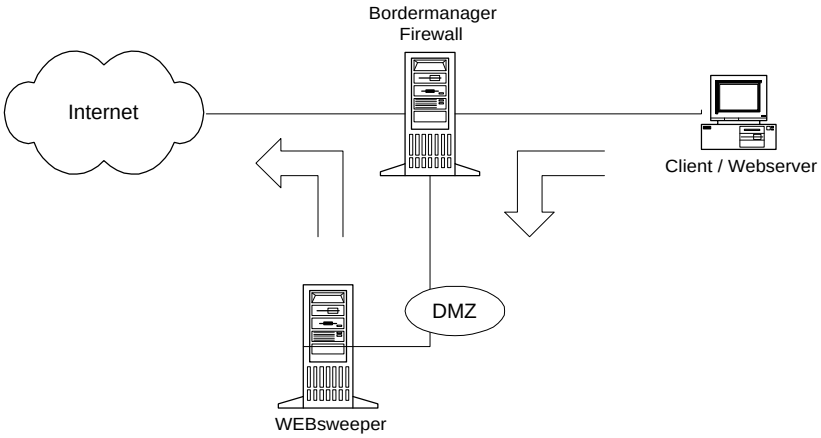
7. Konfigurieren Sie einen IP-Tunnel vom Server Grautvornix zum Server Majestix (Server zum Versuch ZENWorks). Vorgehensweise dazu wie folgt.
    - Laden Sie am Server Grautvornix den entsprechenden Treiber für den IP-Tunnel mit dem Befehl “Load IPTUNNEL peer= <IP-Adresse 10.23.203.200> und verifizieren Sie, das dasselbe am Server Majestix bereits geschehen ist (Bitte Adressen überprüfen)
    - Binden Sie das IPX Protokoll an den IP-Tunnel mit “Bind IPX IPTUNNEL net=A0008888”
8. Versuchen Sie aus einem der Subnetze heraus durch den IP-Tunnel hindurch den Server LABSERVER zu erreichen. Starten sie dazu den Client und schauen Sie, daß dieser eine Verbindung zum LABSERVER erhält. Wenn das geschehen ist, schreiben Sie in Ihr Login Fenster <Team#> und als Kontext <labor.lbs>, senden den Login Befehl aber noch nicht ab.
9. Gehen Sie zur Gruppe, die den Netzwerkmanagementversuch macht, und lassen Sie den Lanalyzer des Netzwerkmanagementsystems starten. Setzen Sie dazu einen Capture-Filter auf die gesamte Kommunikation mit dem Server Majestix. Danach loggen Sie sich von Ihrer Workstation über den IP-Tunnel in den LABSERVER als Team# ein und protokollieren Sie diesen Vorgang über den Lanalyzer mit. Wie ist das IP-Tunnel Paket aufgebaut? Holen Sie den Betreuer für weitere Erläuterungen.

Nun sollten Sie folgendes verstanden haben:
Die Funktionsweise von Routern
Die Rolle einer Netzwerkadressierung bzw. eines Routingfähigen Protokolls wie IP
Die Adressvergabe in IP-Subnetzen
Die Konfiguration von Netzwerkadressen auf einem Novell Server
Den Aufbau eines Pakets zur Kommunikation zwischen Client und Server

Versuch 4: Internet Security

In diesem Versuch sollen die verschiedenen Komponenten einer Firewall am Beispiel des Bordermanagers von Novell sowie des Websweepers von Content Technologies demonstriert werden. Zur Verfügung stehen hier drei Netze:

- ein öffentliches
- ein Zwischennetz (DMZ) mit einem Content Filtering Proxy Server (WEBsweeper)
- ein privates Netz mit einer Workstation Den prinzipiellen Versuchsaufbau zeigt die folgende Abbildung:



Es werden folgende Netzwerkadressen verwendet:
Privates Netz:

Workstation/Webserver: 192.168.1.1
Border Manager: 192.168.1.111

DMZ:

WEBsweeper: 10.23.201.112
Border Manager: 10.23.201.111

Öffentliches Netz:

WebServer: www-lbs.e-technik.fh-muenchen.de
DNS Server: 10.23.61.1
Gateway: 10.23.64.1
Border Manager: 10.23.200.111

Der Versuch besteht aus drei Teilen:

- Einrichten und Test von Paketfiltern und Zugriff ins Internet via Proxy
- Einrichten und Testen von NAT (statisch und dynamisch)
- Verwenden des Bordermanagers als HTTP Reverse Proxy Cache

Eingesetzte Produkte

Novell Bordermanager:
Der Novell Bordermanger ist Firewall und Proxy Server in einem. Da er kaum über Content Filtering Mechanismen verfügt, wird jedoch ein anderer Proxy Server eingesetzt. Er kann aber insbesondere als Reverse Proxy (für Zugriffe aus dem Internet) eingesetzt werden, und hierfür wird er im Praktikum auch eingesetzt.

Content Technologies WEBsweeper:
Der WEBsweeper ist ein Proxy Server mit Content Filtering Technologie, d.h. es können Virenscanner eingebunden werden, zudem lassen sich Internetseiteninhaltlich untersuchen und ggf. sperren. Damit auf verschiedene Benutzer unterschiedliche Regeln angewandt werden können, bringt er eine eigene Benutzerverwaltung mit. Der Websweeper ist im wesentlichen vorkonfiguriert, es müssen lediglich Zuweisungen bestimmter Filterszenarien auf bestimmte Benutzer vorgenommen werden.

Vorbereitung:

Lesen Sie vorab die Kapitel über Network Layer, Transportprotokolle sowie Firewalls der Vorlesung. Zudem machen Sie sich bitte mit dem Handbuch des Bordermanagers (als Online Dokumentation auf CD) vertraut. Blättern Sie durch die Dokumentation und gehen Sie parallel nachfolgende Praktikumsbeschreibung durch. Suchen Sie die Stellen, auf die Sie während des Praktikums zur Versuchsdurchführung gegebenenfalls zugreifen müssen
Die zu verwendenden Konfigurationstools heißen:

- BRDCFG: Konfiguration des Bordermanagers, ermöglich automatische Anfangskonfiguration. Greift im weiteren Verlauf dann auf die beiden folgenden Utilities zu
- INETCFG: Ermöglicht Konfiguration von Netzwerkkarten und Protokollen, sowie Protokollumsetzung über NAT. Die Konfigurationsänderungen werden dabei in ein Konfigurationsfile auf dem Server geschrieben und durch den Befehl “Reinitialize System” aus dem INETCFG heraus implementiert.
- FILTCFG: Ermöglicht die Konfiguration von Paketfiltern. Damit die Filter gesetzt werden können, muß Filtering grundsätzlich für jedes Protokoll getrennt enabled werden. Eine Alternative steht mit BRDCFG zur Verfügung (s.o.) Hier wird bei Aufruf der automatischen Konfiguration die Filterunterstützung für alle am Server gebundenen Protokolle eingeschaltet.

Überlegen Sie sich vorab, welche Filterregeln notwendig sind, damit die nachfolgend beschriebene Sicherheitspolice umgesetzt wird:0

- http/https und ftp Zugriff der Clients aus dem internen Netz nur zum Websweeper. Direkter Zugriff ins Internet soll nicht erfolgen können, da so ja der Viren und Content Filter umgangen werden könnte).
- http/https und ftp Zugriff des WEBsweepers ins Internet (dazu ist dns ebenfalls erforderlich)
- Zugriff aus dem öffentlichen Netz auf den Bordermanager Reverse Proxy
- Einsatz von NAT (Network Adress Translation) zur DMZ und zum internen Netzwerk. (Überlegen Sie sich, ob Sie statisches oder dynamisches NAT brauchen) .

Hinweis: Zunächst werden alle Wege blockiert und danach ausnahmeregeln konfiguriert. Der Bordermanger unterstützt sog. Stateful filtering. Damit muß nur jeweils eine Regel von innen nach außen konfiguriert werden, die entsprechenden Antwortpakete lässt der Bordermanger dynamisch hindurch.

Versuchs-Durchführung:

Teil I: Einrichten von Paketfiltern, Internetzugriff via Proxy

1. Schalten Sie zunächst alle Filter auf dem öffentlichen Interface (Intel-Netzwerkkarte) ein. (Automatische Konfiguration). Prinzipielle Vorgehensweise hierzu:
   - Laden Sie am Server "Gartenzaun" mit Load BRDCFG das Konfigurationsutility des Bordermanagers. Auf die Frage, ob Sie ein sicheres System aufsetzen wollen, antworten Sie mit "yes".
   - Starten Sie INETCFG → Protocols →IPX und disablen Sie die Filter für IPX Zugriff. (Es soll nur IP Protokoll gefiltert werden, das erlaubt es uns, jederzeit auf alle Komponenten via IPX zuzugreifen. Beenden Sie INETCFG.
   - Starten Sie FILTCFG und setzen Sie am public interface (Intel-Netzwerkkarte) alle Filter
   - Gehen sie zum Menüpunkt configure filters

2. Setzen Sie nun die Filter entsprechend obiger Sicherheitspolice (zunächst ohne NAT) für den Zugriff von innen ins Internet.
   - Der Grundzustand ist bereits, daß keine Pakete die Firewall passieren dürfen
   - Konfigurieren Sie danach obige Sicherheitspolice über entsprechende Ausnahmen (Exceptions). Hierbei konfigurieren Sie Filter zwischen dem privaten Interface und der DMZ sowie zwischen der DMZ und dem öffentlichen (Intel-) Interface.

3. Konfigurieren Sie auf Clientseite den Netscape Browser auf Verwendung des WEBsweepers als Proxy Server (edit → preferences → advanced → proxies)

4. Testen Sie Ihre Konfiguration von innen über Ping und HTTP Requests.

5. Rufen Sie eine beliebige Seite aus dem Internet auf, die noch nicht im Proxy Server gecached ist. Merken Sie sich, wie lange der Bildaufbau dauert. Löschen Sie nun den lokalen Cache im Browser. Rufen Sie nun die Seite (die nun im WEBsweeper gecached ist) erneut auf. Ist ein Geschwindigkeitsunterschied feststellbar?

6. Rufen Sie nun eine Seite auf, die laut WEBsweeper Policy nicht aufrufbar sein soll und testen Sie ob der WEBsweeper richtig filtert.

Teil II: Einrichten von NAT

1. Konfigurieren Sie dynamisches NAT am Bordermanager (öffentliche Seite)
   - Schalten Sie im Modul INETCFG die Verwendung von dynamischem NAT ein. Load INETCFG → Bindings → TCP/IP an INTELBRD → Expert TCP/IP Bind Options
   - Starten Sie den Server neu durch Eingabe von "Restart". Überprüfen Sie beim Laden der Module, ob NAT geladen ist (INETCFG → View Configuration → Console Messages
   - Überprüfen Sie mit Ping aus dem internen Netz, ob Sie die Firewall erreichen können (beide Netzwerkkarten!)

2. Greifen Sie via HTTP aus dem privaten Netz auf den Webserver www-lbs im öffentlichen Netz zu. Überprüfen Sie im Log File dieses Webservers (http://www-lbs.e-technik.fh-muenchen.de/logs) , von welcher Adresse der Zugriff erfolgt ist.

Adresse: _____

Können Sie nun von außen auf Ihren privaten Webserver zugreifen oder ihn anpingen?

3. Konfigurieren Sie nun zusätzlich statisches NAT, in dem Sie folgende Netzwerkadresse zusätzlich auf die öffentliche Netzwerkkarte des Bordermangers binden (add secondary ipadress 10.23.200.211).

   Konfigurieren Sie in INETCFG (unter Bindings → TCPIP → Expert TCP/IP Bind Options →NAT → NAT Table) eine Umsetzung dieser Adresse auf die Adresse Ihres Webservers im privaten Netz.

4. Starten Sie den Server erneut mit "restart"
5. Überprüfen Sie nun den Zugriff auf Ihren privaten Webserver von der Workstation aus dem öffentlichen Netz. Unter welcher Adresse finden Sie nun den Webserver?
6. Gehen Sie nun wieder zurück auf dynamisches NAT zur DMZ hin und starten Sie den Server neu (restart).

Teil III: Einrichten eines HTTP Reverse Proxy Servers

1. Konfigurieren Sie den Bordermanager als HTTP Reverse Proxy.
   Prinzipielle Vorgehensweise hierzu:

   - Loggen Sie sich von der Workstation in den Bordermanager ein Servername: Gartenzaun (Login als .Team#.security.lbs)
   - Starten Sie den NetWare Administrator (NWAdmin in Sys:public\win32)
   - Sehen Sie sich die Details des Serverobjekts des Servers "Gartenzaun" an, setzen Sie HTTP Reverse Proxy auf "Enable"

2. Konfigurieren Sie den Reverse Proxy so, daß er die Seiten Ihres auf Ihren internen Webservers zwischenspeichert.
3. Greifen Sie nun von einer Workstation aus dem öffentlichen Netz auf Ihren Webserver zu. (http://<Adresse>. Welche Adresse müssen Sie nun eingeben?
4. Löschen Sie den Cacheinhalt und machen Sie die Proxy Konfiguration für den nächsten Versuchstermin wieder rückgängig.

Sie sollten nun einen Überblick über die Wirkung von dynamischen Paketfiltern, von statischem und dynamischem NAT sowie die Funktionsweise eines Application Layer Proxies erhalten haben.

Versuch 5: Windows NT Vertrauensstellungen (Trusts)

In diesem Übung geht um die praktische Realisierung des Master Domänen Konzeptes von Microsoft. Aufbauend auf dem folgenden Szenario werden Sie zuerst eine einfache Vertrauensstellung zwischen den zwei Domänen (**One-Way Trust Relationship**) aufbauen, sich dann über diese Vertrauenstellung einloggen. Dieses Konzept wird als Master Domain Modell bezeichnet und ist eine häufig angewandte Methode zur Verwaltung von Windows NT Netzen. Hierbei wird es den Benutzern der einen Domäne (**Account Domain/Master Domain**) ermöglicht, auf die Ressourcen der anderen Domäne (**Resource Domain**) zuzugreifen. Die dazu nötigen Benutzerkonten befinden sich nicht auf der Ressourcendomäne, sondern auf einer Benutzerkontendomäne (**Account Domain/Master Domain**).
Weiteres Ziel der Übung ist, beide Domänen über die Vertrauensbeziehung zu verwalten.

Vorbereitung:

Zur Versuchsdurchführung werden Informationen zu folgenden Punkten benötigt.

- Hinzufügen eines Computer Kontos zu einer Domäne
- Globale und lokale Gruppen
- Vertrauensstellungen zwischen Domänen

Lesen Sie hierzu die Ausdrucke der ON-Line Hilfe. Im Praktikum sind zwei Domänenkontroller (Domänen Kleinbonum und Lutetia) installiert. Zudem ist eine Windows NT Workstation vorhanden.

Szenario

Das Windows NT Netzwerk der "HinkelSteinbruch Manufacturing Company" in Kleinbonum besitzt eine Windows NT Domäne **Kleinbonum** mit einem Primärkontroller (**Primary Domain Controller / PDC**), zwei Sicherungskontrollern (**Backup Domain Controller / BDC**) und 50 Windows NT Arbeitsstationen. Alle Benutzerkonten (**User Accounts**) wurden in dieser Domäne definiert.
Nun soll die Firma um eine Forschungsabteilung in Lutetia zur Entwicklung neuer bahnbrechender Technologien im Hinkelsteinabbau erweitert werden. Es werden 20 Arbeitsstationen benötigt, die Benutzerkonten sollen zentral verwaltet werden, die Ressourcen der Forschungsabteilung sollen von der Abteilung eigenständig verwaltet werden. Der Zugriff auf die Ressourcen der Forschungsabteilung soll aus dem gesamten Netz möglich sein.

Um diese Struktur zu verwirklichen wird eine zweite Domäne für die neue Forschungsabteilung installliert. Diese Domäne soll **Lutetia** heißen und der Domäne **Kleinbonum** vertrauen. Alle neuen Benutzerkonten der Forschungsabteilung befinden sich in der Benutzerdomäne **Kleinbonum**, während die neuen Arbeitsstationen der Forschungsabteilung Mitglieder der Domäne **Lutetia** sind.
Zur Verwaltung der Benutzer sollen zwei globale Gruppen für die Forschungsabteilung in der Domäne **Kleinbonum** gebildet werden:

- "Alle" enthält alle Konten der Mitarbeiter, die für die Forschungsabteilung arbeiten
- "Manager" enthält die Manager-Konten der Forschungsabteilung. Diese Manager sind zusätzlich für die Administrierung der Ressourcen Domäne verantwortlich.

Da alle Mitarbeiter der Forschungsabteilung auf die Ressourcen zugreifen müssen, soll eine lokale Gruppe mit Namen "Forscher" mit Rechte auf die Ressourcen auf **Lutetia** angelegt werden. Die erste Ressource ist ein freigegebenes Verzeichnis "Steinbruch", die zweite Ressource ein Drucker "HP-PapyrosJet".

Namensbezeichnungen für Versuche:

Zur Unterscheidbarkeit der Usernamen, Gruppennamen und Ressourcenbezeichnungen verwenden Sie bitte folgende Bezeichnungen: #Name wobei # für Ihre Teamnummer steht. Team1 verwendet also Bezeichnungen wie 1Alle, 1Manager, 1Forscher usw. Sie arbeiten als User "Praktikum".

Teil I: Arbeitsstation in Ressourcendomäne einbinden

In dieser Übung soll eine NT Workstation in die Ressourcendomäne **Lutetia** der Forschungsabteilung eingebunden werden.

1. Richten Sie ein Computerkonto für die Workstation "PC12" auf dem **Lutetia** PDC ein. Gehen Sie dazu auf der Station PC12 zum Menpunkt Systemsteuerung Netzwerk und fügen Sie den PC in die Domäne Lutetia ein. Starten Sie die Workstation neu. (Alternative: Fügen Sie die Station im Servermanager auf dem Domänenkontroller ein, hier dauert es unter Umständen erfahrungsgemäß deutlich länger, bis der PC im Netz gefunden und als aktiv angezeigt wird).

2. Melden Sie sich dazu als User "Praktikum" für Lutetia auf der Arbeitsstation an.

Teil II: Implementierung einer Vertrauesbeziehung (One-Way Trust Relationship)

In dieser Übung soll folgende Vertrauensbeziehung aufgebaut werden: **Kleinbonum** ist die Benutzerkontendomäne („***trusted domain***"), der vertraut wird, und **Lutetia** die vertrauende Ressourcen Domäne („***trusting domain***"). Nach dem die Vertrauensbeziehung aufgebaut wurde, sollen die Domänennamen in der Domain Box der Logon Dialog Box erscheinen.

1. Konfigurieren Sie Lutetia als "vertrauende" Domäne. Tragen Sie dazu auf dem **Kleinbonum** PDC mit Hilfe des Benutzermanagers für Domänen (**User Manger for Domains**) über das Richtlinienmenü (**Policies Menu**) die Vertrauensbeziehung (**Trust Relationship**) ein, und zwar so, daß **Lutetia** als „***trusting domain (berechtigt, dieser Domäne zu vertrauen)***" erscheint. Melden Sie sich wieder ab (Alt-Ctrl-Del).

2. Bauen Sie eine One-Way Trust Beziehung auf. Richten Sie dazu auf dem **Lutetia** PDC mit Hilfe des Benutzermanagers für Domänen (**User Manger for Domains**) über das Richtlinienmenü (**Policies Menu**) die Vertrauensbeziehung (**Trust Relationship**) zu **Kleinbonum** ein („***trusted domain***", „***Vertraute Domäne***").

Teil III: Überprüfen der Vertrauensbeziehung

In dieser Übung sollen die Benutzer, wie im Szenario beschrieben, eingerichtet werden. Dann soll die Vertrauensbeziehung überprüft werden

1. Legen Sie neue Benutzer in der Domäne **Kleinbonum** an.
   Melden Sie sich hierzu am PDC der Domäne **Kleinbonum** als User Praktikum an und erzeugen Sie die folgenden drei Benutzer: #Troubadix; #Miraculix; #Majestix Ordnen Sie #Majestix der Manager-Gruppe zu. (Erkärung der Namen siehe oben). Keiner der Benutzer darf ein Konto in der Domäne **Lutetia** besitzen. Melden Sie sich wieder ab.

2. Domänenbeziehung über **Kleinbonum**
   Melden Sie sich als User "Praktikum" auf dem PDC von **Kleinbonum** an. In der Domain Box der Logon Information werden die verfügbaren Domänen angezeigt.
   Frage: Welche Namen erscheinen in der Domain Box der vertrauten (trusted) Domain?

   _____

3. Domänenbeziehung über **Lutetia**
   Melden Sie sich als User "Praktikum" auf dem PDC von **Lutetia** an. In der Domain Box der Logon Information werden die verfügbaren Domänen angezeigt.
   Frage: Welche Namen erscheinen in der Domain Box der vertrauten (trusted) Domain?

   _____

4. Vervollständigen Sie den Logon Prozeß
   Versuchen Sie sich auf dem PDC von **Lutetia** mit einem der angelegten Benutzernamen anzumelden. **Lutetia** sollte in der Domain Box erscheinen.
   Frage: Können Sie sich einloggen? Warum oder warum nicht?

   _____

   Versuchen Sie sich auf dem PDC von **Kleinbonum** mit einem der angelegten Benutzernamen anzumelden.
   Kleinbonum sollte in der Domain Box erscheinen.
   Frage: Können Sie sich einloggen? Warum oder warum nicht?

   _____

   Versuchen Sie sich von der Arbeitsstation aus
   1.) auf dem PDC von **Kleinbonum**
   2.) auf dem PDC von **Lutetia**
   3.) auf der lokalen Arbeitsstation mit einem der angelegten Benutzernamen anzumelden.
   Frage: Wo ist eine Anmeldung möglich? Warum oder warum nicht?

   _____

   _____

Teil IV: Domänen über „Trustbeziehung" administrieren

In dieser Übung werden die globalen Gruppen erzeugt. Anschließend sollen die Administratoren und die Ressourcen der Ressourcen Domäne über die Vertrauensbeziehung (**Trust**) konfiguriert werden.

1. Erzeugen Sie die globalen Gruppen #Alle und #Manager.
   Loggen Sie sich dazu als User "Praktikum" in **Kleinbonum** ein, starten sie den Benutzermanager für Domänen (**User Manager for Domains**) und erzeugen sie die beiden globalen Gruppen.
   - #Alle: Machen Sie ihren angelegten Benutzer zu Mitgliedern dieser Gruppe. Entfernen sie alle sonstigen Mitglieder dieser Gruppe.
   - #Manager: Machen sie ihren #MajestixV,N zum alleinigen Mitglied dieser Gruppe.

2. Konfigurieren Sie eine vertrauende („*trusting*") Domäne über Vertrauensbeziehungen.
   Melden sie sich dazu auf dem PDC von **Lutetia** in der Domäne **Lutetia** an. In der Domain Box der Logon Information werden die verfügbaren Domänen angezeigt.
   Starten sie den Benutzermanager für Domänen (**User Manager for Domains**) und fügen sie die globale Administratorgruppe #Manager der „***trusted domain***" der lokalen von Windows NT vordefinierten Administratorgruppe "Administratoren" der „***trusting domain***" hinzu. (Wählen Sie dazu die Gruppe aus und fügen Sie sie in die globale Gruppe "#Manager".
   Frage: Welche Benutzer können nun die Ressourcen der **Lutetia** administrieren?

   _____

3. Nun lassen wir unseren neugebackenen Manager die vertrauende (trusting) Domäne administrieren.
   Melden sie sich als #Majestix in **Kleinbonum** über **Lutetia** an. Starten sie den Benutzer Manager für Domänen und wählen sie die Domäne **Lutetia** aus. Erzeugen sie für die Domäne **Lutetia** die lokale Gruppe #ForscherV,N und fügen sie die Gruppe **Kleinbonum\#AlleV,N** als Mitglied hinzu. Entfernen sie alle sonstigen Mitglieder dieser Gruppe!

   Installieren sie einen Drucker "#HP-PapyrosJetV,N" (Über Systemsteuerung → Drucker → Neuer Drucker → Druckertreiber IBM-Proprinter III) am lokalen Printerport Lpt1.
   Erzeugen sie ein Verzeichnis "C:\LAN-Praktikum\#Steinbruch", das sie unter dem gleichem Namen freigeben.
   Weisen sie beiden Ressourcen die lokale Gruppe #Forscher als Mitglied zu und entfernen sie alle sonstigen Mitglieder. Die Gruppe #Forscher erhält auf beiden Ressourcen das Recht "Vollzugriff".

Teil V: Zugriff auf die Ressourcen über Vertrauensbeziehungen

1. Zugriff auf Verzeichnis
   Melden sich sich auf **Kleinbonum** als #Miraculix an. Ordnen sie dem freigegeben Verzeichnis #Steinbruch der Domäne **Lutetia** einen Laufwerksbuchstaben zu (Explorer). Wechseln sie zu diesem Laufwerk und überprüfen sie ihre Rechte (Vollzugriff) wie folgt: Kopieren Sie das File "Rezept Zaubertrank" in das Veerzeichnis "#Steinbruch".
   Legen Sie einen neuen Drucker an und verbinden Sie diesen mit dem obigen Drucker "#HP-PapyrosJet "(Konfiguration: Druckserver im Netzwerk). Drucken Sie obiges File aus.

Teil VI: Ausgangszustand wieder herstellen

1. Vertrauensbeziehung auflösen:
   Melden sie sich sowohl bei **Kleinbonum** als auch bei **Lutetia** als Adminsitrator an und lösen mit Hilfe des Benutzer Managers für Domänen, die Vertrauensbeziehung zwischen **Kleinbonum** und **Lutetia** auf. Versuchen sie sich anschließend über **Kleinbonum** auf **Lutetia** anzumelden. In der Domain Box dürfte **Kleinbonum** nicht mehr erscheinen.

2. Workstation aus Domäne entfernen:
   Entfernen sie mir Hilfe des Server Manager die Workstation aus der Domäne. Loggen sie sich als Administrator in die Workstation ein und fügen sie die Arbeitsstation einer Arbeitsgruppe (**Workgroup**) ihrer Wahl zu.

3. Benutzerkonten und lokale bzw. globale Gruppen löschen:
   Löschen sie mit Hilfe des Benutzermanagers die von Ihnen definierten lokalen und globalen Gruppen, sowie die von ihnen angelegten Benutzer auf **Kleinbonum** und **Lutetia**. Löschen Sie die Einträge für den Drucker "#HP-PapyrosJet".

Was Sie jetzt verstanden haben sollten:

- Was Domänen und Vertrauensstellungen sind
- Was genau eine Vertrauensstellung bewirkt (wer vertraut wem und warum!)
- Was eine globale Gruppe und eine lokale Gruppe ist,
- Wie die Benutzer durch Gruppenzugehörigkeiten Zugriff auf Resourcen erhalten können.

Versuch 6: Netzwerkmanagement

Vorbereitung:

Dieser Versuch erfordert ein allgemeines Protokollverständnis sowie ein allgemeines Verständnis des Themas Netzwerkmanagement entsprechend der beiligenden Beschreibung. Lesen Sie ebenfalls den unter http://www.novell.com/documentation/lg/mwise27/docui/index.html als pdf verfügbaren Network Management Guide, um Ihnen einen Überblick über das Produkt ManageWise zu geben. Auch hier sei gesagt, daß es sich um ein Handbuch handelt, das Sie soweit verstehen sollen, daß Sie bei Bedarf auf im Versuch benötigte Information zugreifen können.

Durchführung:

Ziel des Versuchs ist es, verschiedene Aspekte des Managements von Netzen kennenzulernen. Als Managementsystem steht Novell ManageWise zur Verfügung, überwacht werden ein Novell Server („LABSERVER“) mit entsprechendem Management Agent sowie ein managebarer Ethernet Switch. Der Einsatz von SNMP und HTTP als Managementprotokolle sollen demonstriert werden. Zur Performancemessung und Paketanalyse steht ein PC mit Lanalyzer Software zur Verfügung.

Teil I: Configuration und Performance Management

1. Starten Sie den Fileserver Asterix und die Management-Station
   Starten Sie ManageWise und sehen Sie sich das Netz der FH München an (Über die Menüleiste > File > Open > Internet Map). Wechseln Sie in das Labor-Segment durch Doppelklick. Überwacht werden soll das Netzwerksegment im Labor. Dies hat die Netzwerknummern: IPX: 08000206 bzw. IP 141.39.253.0. Überwachen Sie den Server LABSERVER im Hinblick auf einige Eckwerte. Hierzu wählen Sie die Server aus, es öffnet sich dann jeweils ein Fenster mit dem Netzwerkmanagement Agent (NMA). Sehen Sie sich insbesondere auch die historischen Daten an.
   Überprüfen Sie:
   - Speicherbenutzung: Wieviele Cache Buffers stehen zur Verfügung?
   - Prozessorauslastung
   - Geladene NLMs (Wie groß sind die NLMs, die die Netzwerkmanagement Agents darstellen, welche das sind, solten Sie aus der Vorbereitung wissen).
   - Volume Information
   - Festplatten Information. Welche Typ von Festplatte wird im LABSERVER verwendet, wie ist sie konfiguriert?

   _____

2. Machen Sie eine Performance-Grafik, die die vom LABSERVER gelesenen und die auf den Server geschriebenen Pakete anzeigt. Vorgehensweise hierzu: Wählen Sie den entsprecheden Server aus (kein Doppelklick!), wählen Sie dann über die Menüleiste: Performance > NetWare Server Trends > Configure General Trends > File System Reads und Filesystem Writes (beide auswählen, Maustaste hierzu gedrückt halten). Nach der erfolgten Auswahl wird Ihnen eine Performance Grafik angezeigt. Ist hier jeweils eine schreib- oder leseintensive Umgebung vorhanden (Diese Information kann z.B. zum Fileserver Tuning verwendet werden)?

   _____

3. Markieren Sie den Fileserver LABSERVER, wählen Sie auf der Menüleiste Configure und sehen Sie sich die SET Parameter des Servers an. Hierüber könnte man den Server konfigurieren.

Teil II: Managebarer Ethernet-Switch

Der Switch der Firma Allied Telesyn ist u.A. per http-Protokoll aus einem Standardbrowser heraus managebar. Seine Adresse ist http://sw1-lbs. Zudem unterstützt er das SNMP Protokoll und die Adresse der Management Station ist als Zieladresse für Fehlermeldungen (Traps) eingetragen.

1. Starten Sie an der Managementstation einen Browser und gehen Sie auf die Adresse http://sw1-lbs. Holen Sie den Betreuer zum Einloggen. Nach dem Einloggen sehen Sie den Switch bildlich vor sich. Wechseln Sie auf das Hauptmenü. Sehen Sie sich den Port Status und die allgemeinen Konfigurationsdaten an, ändern Sie jedoch bitte nichts.

2. Unter System Configuration → IP Parameters finden Sie auch die sogenannten SNMP Community Strings. Bitte notieren Sie sich diese für später. Überprüfen Sie auch, ob als Management Station die korrekte IP-Adresse eingetragen ist (Die Ip-Adresse der Management Station finden Sie unter → Ausführen → Winipcfg heraus.

3. Sehen Sie sich die Konfigurationsmöglichkeiten für Spanning Tree an, machen Sie aber keine Konfigurationsänderungen. Das Spanning Tree Protokoll wird in der Vorlesung besprochen.

Nachdem ein Switch den Datenverkehr auf jeweils zwei Ports (Quell- und Zielport) beschränkt und der Datenverkehr nicht wie bei einem Hub an allen Ports gleichzeitig sichtbar wird, ist es zunächst schwierig, den Datenverkehr wie in einem shared LAN mit Hilfe eines LAN-Analysetools zu überwachen. Grundsätzlich gibt es zwei Möglichkeiten zur Überwachung des Datenverkehrs im Switch.

- Remote Monitoring über das RMON Protokoll bzw. eine RMON Anwendung innerhalb des Switches
- Port Mirroring, wobei der gesamte Datenverkehr eines bestimmten Ports auf einen zweiten gespiegelt werden kann, mit dem dann ein LAN Analysetool verbunden ist.

4. Wechseln Sie auf die Ethernet Statistics. Hier können Sie sich einen groben Überblick über den Datenverkehr auf den einzelnen Ports verschaffen. Eine Anwendung zur Online Performance Messung oder Paketanalyse ist hier jedoch nicht vorgesehen.

5. Wechseln Sie auf den Menüpunkt Port Mirroring und spiegeln Sie den Port 19 (das ist der Port, der mit der Management Station verbunden ist) auf den Port 23 (mit Lanalyzer Tool verbunden). Starten Sie nun den Lanalyzer auf der benachbarten Station, um den Datenverkehr mitprotokollieren zu können. Drücken Sie dazu auf „Capture Packets“. Greifen Sie von der Management Konsole auf irgendeine Komponente im Netz zu um Datenverkehr zu erzeugen, stoppen Sie „Capture Packets“ und sehen Sie sich den Datenverkehr an.

Teil III: Alarm Management:

Ziel des Management ist es, genau festzulegen, welche Meldungen (Traps) vom jeweiligen Agent auf den überwachten Geräten im Netz angezeigt werden sollen und wie mit Ihnen umgegangen werden soll. Z.B. könnte bei bestimmten Fehlern auch noch Notprogramme gestartet werden z.B. ein Not-Backup.

1. Wir konfigurieren nun, daß bei einem Serverausfall angezeigt wird, daß das TTS (Transaction Tracking System) des Servers ausgefallen ist und das Notprogramm “Calc (=Taschenrechner)” gestartet wird (Damit kann sich der Netzwerküberwacher im Notfall zumindest ausrechnen, wie lange es dauert, bis der erste Benutzer genervt anruft. Vielleicht rechnet er sich aber auch nur aus wie er ohne die nächste Gehaltserhöhung, die er nun in den Wind schreiben kann, auskommt). Die Konfiguration erfolgt über den Menüpunkt Fault > Fault Disposition. Wählen Sie die Meldung

TTS Disabled by Server aus der Liste und geben Sie an, daß das Programm Calc.exe im Verzeichnis C:\Windows gestartet werden soll, falls diese Meldung auftritt.

2. Gehen Sie nun in Ihre Segment Map, quittieren Sie alle noch angezeigten Alarmmeldungen (Glocken auf den Server-Symbolen) duch Markieren der Server und Menüleiste > Fault > Ack. Alarms.

3. Starten Sie nun den Lanalyzer auf der benachbarten Station, um den Fehler mitprotokollieren zu können. Drücken Sie auf „Capture Packets“.
   Produzieren Sie nun einen Fehler, indem Sie an der Serverkonsole „dismount sys“ eingeben. Ist der Calculator da?
   Nachdem der Rechner auf dem Bildschirm erscheint, beenden Sie den Capture Vorgang ("Stop") und sehen sich mit "View" den Inhalt des Paketpuffers an. Sie müßten jetzt zwei SNMP Trapmeldungen (Fehlermeldungen des Novell Servers Asterix) erhalten haben, und zwar eine über das IPX Protokoll, die andere über IP. Suchen Sie nach den Traps und sehen sich die Pakete an. Hier finden sich z.B. die Agent Adresse und entsprechende Fehlermeldung nach der Enterprise MIB der Firma Novell. Holen Sie den Betreuer für weitere Erläuterungen zum Inhalt dieser Pakete.
   Geben Sie nun am Server wieder „mount sys“ ein. Sehen Sie sich die Alarmmeldung an über Menüleiste > Fault > Alarms und bestätigen Sie den Alarm.

4. Um spezielle Traps vom Switch „verstehen“ zu können, muß die Management Konsole Kenntnis über den Aufbau der Enterprise MIB von Allied Telesyn besitzen. Dazu muss ein entsprechendes MIB File vom Hersteller vorhanden sein. Sie finden dieses im Verzeichnis c:\atmib auf Ihrer Festplatte. Kopieren Sie dieses in das Verzeichnis c:\mw\nms\snmpmibs\current und starten Sie an der ManageWise Konsole über die Menüleiste den sog. MIB Compiler.

5. Sehen Sie sich nun die Konfigurationsmöglichkeiten unter Menüpunkt Fault > Fault Disposition an. Hier können Sie nun Aktionen definieren, die ausgeführt werden sollen, sollte ein bestimmter Trap vom Switch kommen. Unglücklicherweise sind diese Fehler im Praktikum nicht reproduzierbar, das Prinzip sollte jedoch im vorangegangenen Menüpunkt deutlich geworden sein.

6. Die Grundproblematik dieser Vorgehensweise ist, daß Sie daon ausgehen müssen, daß der ausgefallene Server noch Zeit für eine Trap Meldung vor seinem Absturz hatte. Wenn Sie hier nicht sicher sein können, gibt es noch eine Alternative: Senden Sie einen dauernden Ping an ein zu überwachendes Gerät (connectivity test) und konfigurieren Sie das Alarmmanagement so, daß an der Konsole eine Aktion geschieht, wenn der Ping nicht mehr beantwortet werden kann. Testen Sie diese Vorgehensweise mit dem Server Asterix, indem Sie den Server bei Laufendem Connectivity Test einfach abschalten.

<u>Was Sie nach Durchführung des Versuchs verstanden haben sollten:</u>
- Die Bedeutung von Configuration, Performance und Alarm-Management
- Die Möglichkeiten des Configuration Managements über SNMP und/oder http
- Die Möglichkeiten des Performance Managements in Netzen mit Switches
- Die Bedeutung einer MIB, sowie der Unterschied zwischen Standard und Enterprise MIBs
- Die Möglichkeiten zum Alarm-Management

Allgemeines zum Thema Netzwerkmanagement

Kommunikation:

Im Allgemeinen besteht ein Netzwerkmanagementsystem aus zwei Komponenten, einer Managementstation und einem überwachten Rechner. Der Rechner wird durch eine spezielle Schnittstelle, dem sogenannten Management-Agent, managebar. Der Agent ist als Software auf dem zu überwachenden Rechner installiert. Bei managebare Hardware Komponenten ist der Management Agent als Software in einem E-Prom oder auf einer im Gerät integrierten Festplatte gespeichert.

Management Agents:

Die Agents haben unterschiedliche Funktionalität, z.B.:

Serverüberwachung:
- Netzwerkmanagement-Agent: Überwachung der Server Hardware allgemein
- Server-Agent: z.B. Überwachung bestimmter Server-Hardware (z.B. Compaq)
- andere Agents zur Überwachung von Zusatzfunktionen wie z.. USV (Unterbrechungsfreie Stromversorgung)

Netzwerküberwachung:
- LANalyzer Agent: LanaLyzer Funktion als NLM auf dem Fileserver zur Überwachung der angeschlossenen Netzwerke
- Agents zur Überwachung von Hubs, Bridges, Routern

Die folgenden Produkte werden im Versuch Netzwerkmanagement eingesetzt:
- NMA (NetWare Management Agent)
- ein Switch der Firma Allied Telesyn
- Novell Lanalyzer

SNMP:

Jeder Agent stellt eine Datenbank (MIB=Management Information Base) zur Verfügung, in der spezifische Daten des überwachten Gerätes festgehalten sind. Die Kommunikation zwischen Netzwerkmanagementstation und den Agents (genauer mit der MIB der Agents) erfolgt im Allgemeine über das Protokoll SNMP (Simple Network Management Protocol).

SNMP erlaubt die Fernsteuerung der überwachten Geräte (Veränderung der Werte in der MIB) sowie das Versenden von Fehlermeldungen (sogenannte Traps) vom Agent zur Managementstation. SNMP kann, auch wenn es aus der IP Welt kommt, in verschiedenen Protokollwelten verwendet werden, es kann insbesondere auch auf das Novell IPX Protokoll aufsetzen.

Konfiguration:

Als Managementsoftware auf der Management Station wird Novell ManageWise eingesetzt.

<u>ManageWise in Novell IPX Netzen:</u>
ManageWise bietet seine Dienste zunächst über das Novell SAP Protokoll (Service Advertising Protocol) im Netz an, hierbei werden SAP Pakete alle 60 Sek. geschickt. Die Agents finden also normalerweise die Netzwerkmanagementstation aufgrund diese Protokolls. Dieses Verfahren kann aber unter Umständen zu einer hohen Belastung des Netzes speziell bei WAN Verbindungen führen. Ersatzweise kann dann SAP abgeschaltet werden und jeder Agent so konfiguriert werden, daß die Adresse der Netzwerkmanagementstation (Netzwerk und Stationsadresse) expizit angeben wird.

ManageWise in IP-Netzen:
Hier muß grundsätzlich jeder Agent so konfiguriert werden, daß die Managementstation explizit angegeben wird.
Novell Agents werden so konfiguriert, daß die IPX oder IP Adresse der ManageWise Station im File Traptarg.cfg im Verzeichnis SYS:ETC spezifiziert wird. Damit werden Traps automatisch zu dieser Adresse geschickt. In anderen Betriebssystemen heißen die Files ähnlich, Netzwerk-Hardware muss üblicherweise ebenfalls entsprechend konfiguriert werden.

Aufbau der MIB

Als MIB wird die Gesamtheit aller managebaren Einheiten (CPUs, Prozesse, Netzwerkkarten, Ports in Hubs etc.) in Netzwerkkomponenten mit allen Attributen (Konfigurationsmöglichkeiten, Fehlerzuständen etc.) bezeichnet. Die MIB ist hierarchisch aufgebaut und enthält zwei Bereich, die Standard MIB und die Enterprise MIB.

- Standard MIB: standardisierter Aufbau von Objekten innerhalb der MIB sowie zugehöriger managebarer Attribute. Typische Fehlermeldungen (Traps) der Standard MIB sind z.B. Cold Start, Warm Start, Link Up, Link Down, EGP Neighbour Loss etc.
- Enterprise MIBs: Hier kann jeder Hersteller für sein Gerät (z.B. ein Routerhersteller für seine Router) genau festlegen, welche Parameter des Geräts überwacht werden sollen, und welche Traps (Fehlermeldungen) in welchen Fällen an eine Management Station geschickt werden.

Die Agent Software enthält Information über das zu überwachende Gerät in Form sogenannter MIB Files. Generell muß natürlich auch die Managementstation über die Informationen der einzelnen Parameter der MIBs aller Agents verfügen, sonst könnten unter Umständen Traps, die ankommen, nicht richtig interpretiert werden. Speziell bei nicht standardisierten MIBs z.B. bestimmten Enterprise MIBs muß eventuell die MIB an der Managementstation entsprechend compiliert werden, damit die entsprechende Information hier vorliegen kann. Bei NMS erfolgt dies über einen speziellen MIB Compiler,der innerhalb der Management Konsole gestartet werden kann.

Allgemeines zum Thema ManageWise

Die Novell Management Konsole ist eine Windows basierende Anwendung. Die Konsole enthält eine auf Btrieve basierende Topologiedatenbank mit Angaben über alle Komponenten im Netz. Die Komponenten können von Hand eingetragen werden, sie können aber auch mit Hilfe der sog. Explorer Software im Netz gesucht werden. Diese NetExplorer Software (Netxplor.nlm) wertet Routing Tabellen von Routern aus und hört auf RIP und SAP Pakete aus dem Netz, um alle Komponenten zu erkennen.

Managewise erlaubt den Zugriff auf spezielle Novell Agents über entsprechende Front End Komponenten mit graphischer Benutzeroberfläche, die in ManageWise integriert sind. Zusätzlich steht ein sogenannter MIB Browser (textbasierend) zur Verfügung, mit dem beliebige Daten von managebaren Komponenten konfiguriert werden können, gute Kenntnis der entsprechenden MIB vorausgesetzt.

Tools von Drittanbietern für das Configuration Management können entweder auf der Management Station neben Managewise betrieben werden, oder mit ManageWise verknüpft werden.

ManageWise kann als zentrale Konsole für das Alarmmanagement dienen. Wenn Traps von Geräten kommen, die der Managementstation bekannt sind, wird eine entsprechende Alarmmeldung angezeigt. Diese ist umso detaillierter, je mehr über das überwachte Gerät (in Form von Enterprise MIB Files) bekannt ist. Über eine sogenannte Alarm Dispositionstabelle können dann Aktionen (Start externer Programme) definiert werden, die bei Eintreffen eines bestimmten Alarms ausgelöst werden sollen. Als externe Programme können hier z.B. Programme zum Weiterleiten von Alarmmeldungen an Pager, Handys, Fax , e-Mauil oder ähnliches dienen.