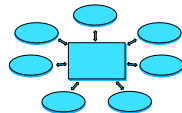


NetBIOS und SMB



F. Hodel
A-Net GmbH
www.anetgmbh.ch



NetBios und SMB Grundlagen

- ▶ Das **NetBios API** ist nach wie vor beliebt für Netzwerkprogramme. Der Programmierer kann mit wenigen Befehlen Daten über das Netzwerk austauschen, ohne sich um Kommunikationsdetails zu kümmern.
- ▶ Das NetBios (=Network Basic Input/Output System) wurde Anfangs der 80er Jahre von IBM entwickelt, um einigen 10 PCs eine einfache Kommunikationsmöglichkeit im LAN zu geben.
- ▶ Die Stationen finden sich per **NetBios Namen**
 - Jeder Computer hat einen Netbios-Namen im Netz, der nur einmal im ganzen Netz existieren darf. Jeder Computer sendet seinen Namen beim Starten an alle Stationen im erreichbaren Netzwerk (=Broadcast). Dies wird dreimal wiederholt. Wenn innert 12 Sekunden niemand reklamiert, benutzt dieser Computer den Namen.
 - Arbeitet schon ein anderer Computer mit dem gewünschten Namen, reklamiert er, sobald ein anderer ebenfalls diesen benutzen will (=Verteidigung des Namens). Nur der zuerst gestartete Computer kann den Namen benutzen.
 - Ein zentraler NetBios - Namensserver ist nicht notwendig.



SMB Grundlagen

- ▶ 3Com und Microsoft entwickelten auf dem NetBios-API basierend erste Server und Client Lösungen für DOS (PC LAN Programm). Die dazu benötigten Befehle sind als SMB (Server Message Block) Protokoll bekannt.
- ▶ SMB Server stellen Ressourcen im Netzwerk zur Verfügung. Diese werden mit dem Namen des Servers (z.B. "server01") und dem Namen der Ressource (z.B. Freigabe "daten") gefunden:
`\\server01\daten`. Dies ist der **UNC** - Name (Universal Naming Convention)
- ▶ Die Freigaben des Servers erscheinen beim Client als Laufwerksbuchstaben. Die Zuordnung erfolgt mit :
`net use x: \\server01\daten` lässt die Daten unter dem Laufwerk x: erscheinen.
- ▶ Der Freigaben eines Servers oder Clients mit Freigabedienst lassen sich via Netzwerk anzeigen:
`net view \\server01`



Anmelden - Wo?

- ▶ Anmelden an einer **Domäne**
 - OS/2: logon hans /V:D /P:
 - Win9x: Netzwerkumgebung --> Eigenschaften --> Client für Microsoft-Netzwerke --> An Windows NT Domäne Anmelden
 - Win NT, 2000, XP: Netzwerkumgebung --> Eigenschaften --> Identifikation --> Ändern --> Domäne (Domänen Admin-Passwort notwendig!)
- ▶ Anmelden an der **Arbeitsstation**
 - OS/2: logon hans /V:L /P:
 - Win9x: Netzwerkumgebung --> Eigenschaften --> Client für Microsoft-Netzwerke --> Windows-Anmeldung
 - Win NT, 2000, XP: Netzwerkumgebung --> Eigenschaften --> Identifikation --> Ändern --> Arbeitsgruppe



Welche Rechte habe ich nun?

- ▶ Bei Anmeldung an der Domäne:
 - Die Rechte, die ich in der Domäne habe. d.h. wenn ich in der Domäne Administrator bin, bin ich es auch lokal. Wenn ich in der Domäne User bin, bin ich es auch lokal, auch wenn ich sonst auf der Arbeitsstation Administrator bin!
- ▶ Bei lokaler Anmeldung:
 - Es gelten die lokal definierten Rechte auf dieser Arbeitsstation, egal was in der Domäne definiert ist.

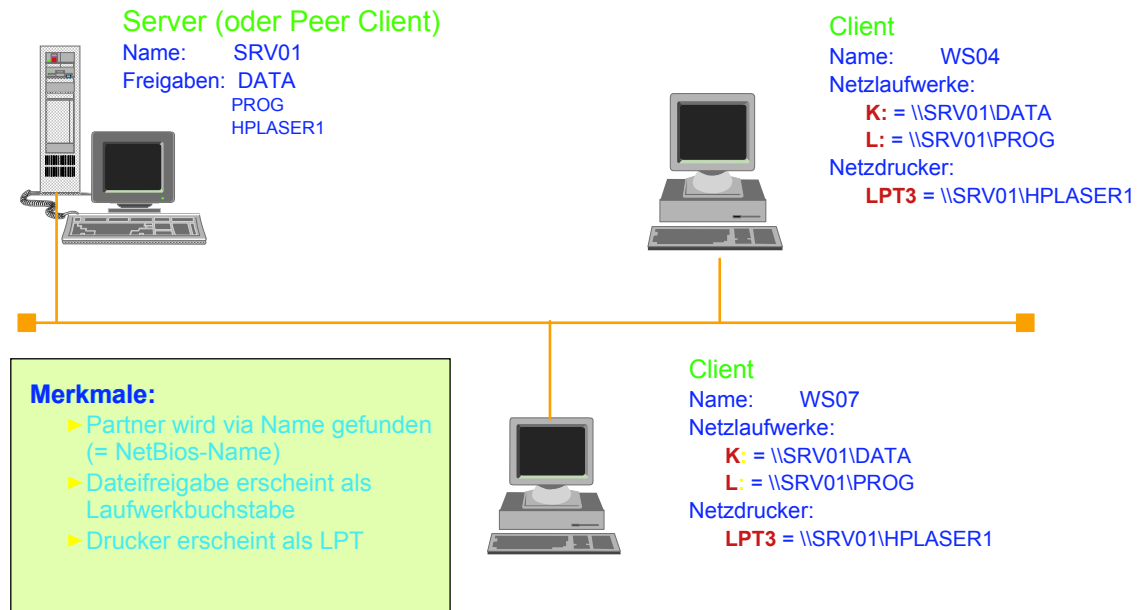


Rechte auf den Freigaben

- ▶ Server (OS/2, NT, Win2000):
 - User Level Security:
 - ▶ *immer abhängig vom Benutzer*
 - ▶ *unbekannte Benutzer erhalten gar nichts*
- ▶ Peer-Dienst (Datei- und Druckfreigabe)
 - Share Level Security
 - ▶ *ein Passwort pro Freigabe*
 - ▶ *alle Benutzer, die das Passwort kennen, erhalten Zugriff, auch wenn sie auf der Peer-Station nicht definiert sind*
 - User Level Security
 - ▶ *Benutzer werden auch auf der Arbeitsstation erfasst*
 - ▶ *individuelle Berechtigung pro Benutzer möglich*



SMB: Freigaben (=Shares)



einige NET-Befehle

- ▶ NET SHARE zeigt die eigenen Freigaben an
- ▶ NET USE zeigt an, welche Freigaben diese Station momentan von anderen Stationen benutzt
- ▶ NET USE X: \\SRV01\DATA (oder) hängt die Freigabe DATA vom Server SRV01 als X: an
- ▶ NET USE X: \\192.168.112.23\DATA (nur Windows Systeme ab 98SE)
- ▶ NET USE X: /D hängt X: wieder ab
- ▶ NET VIEW \\SRV01 zeigt die Freigaben von SRV01 an (ohne mit \$-endende)
- ▶ NET USER zeigt die Benutzer dieser Station an
- ▶ NET USER FHO zeigt Details von Benutzer FHO an
- ▶ NET START SERVER Startet den SMB Serverdienst
- ▶ NET STOP SERVER Stoppt den Serverdienst
- ▶ NET TIME \\SRV01 /SET /Y übernimmt die Zeit von Server SRV01

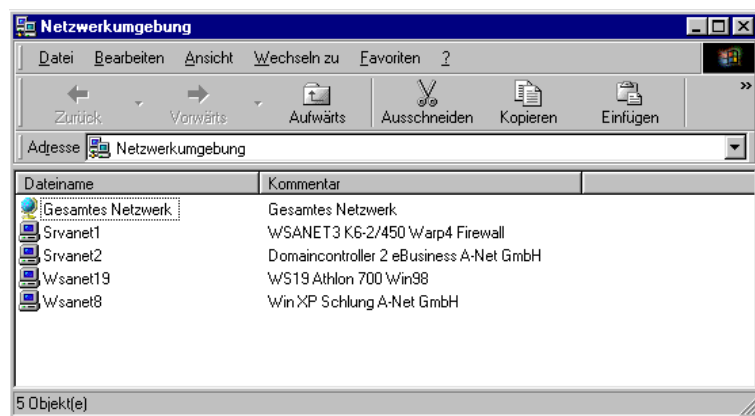


Wo sehe ich die anderen Stationen?

- ▶ OS/2:
 - einige Stationen erscheinen in Ordner "File und Print Client Ressource Browser"
 - bei Windows9x mache Sie folgendes:
Netzwerkumgebung --> Eigenschaften --> Datei- und Druckfreigabe Dienst --> LM-Dienst [Ja]
 - bei Windows NT, 2000 und XP:
Regedit --> HKEY_Local_Machine\System\CurrentControlSet\Services\LanmanServer\Parameters
Lmannounce 1 (statt 0)
- ▶ Windows Stationen
 - einige Stationen erscheinen automatisch
 - ... kann aber sehr lange dauern (bis zu 52 Minuten!)
 - Windows ME zeigt bis maximal 10 Stationen an
- ▶ Fazit: Verwenden Sie: **net view \\server01**
Das geht immer und schnell !!



Beispiel: Netzwerkumgebung Win9x

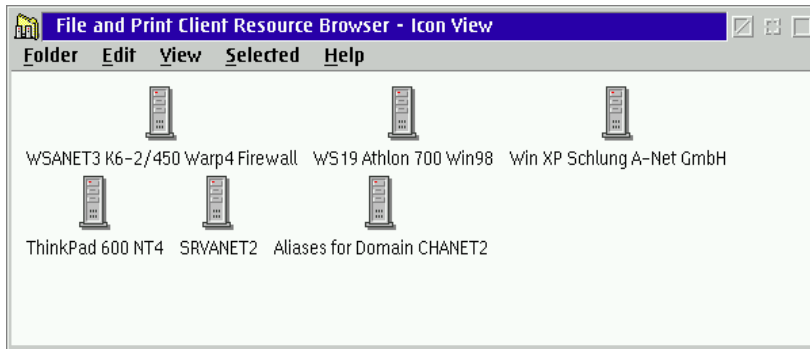


Windows Netzwerkumgebung. Hier erscheinen einige Systeme,
andere erst viel später oder gar nie!

Zu früh nach dem Starten erscheint die Meldung:
"Netzwerk kann nicht durchsucht werden".

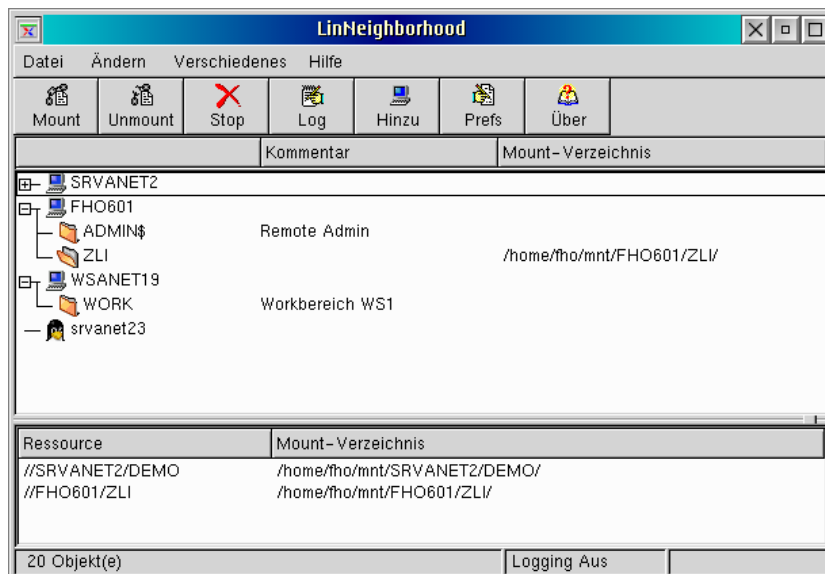
Dann einfach 10 oder mehr Minuten warten und nochmals probieren.

Beispiel: Ressourcenbrowser OS/2



Der OS/2 File und Print Ressourcen Browser behält einmal gefundene Systeme. Deshalb gelegentlich auf [View] und dann [Refresh now] drücken. Nicht mehr aktuelle Systeme löschen.

Beispiel: LinNeighborhood Linux 8.0



Zum Hinzufügen von Stationen drücken Sie auf [Hinzu] und browsen mit einer bei den anderen Stationen gültigen UserId und Passwort. Hier können auch direkt Freigaben "gemountet" werden.

wichtige Net-Befehle

► NET VIEW

- Zeigt die Freigaben eines Servers oder Clients mit Freigabedienst (Peerdienst) an. Bei Servern muss der angemeldete Benutzer berechtigt sein. Angezeigt werden freigegebene Verzeichnisse, Drucker und Modem (diese nur im OS/2).
- Freigaben mit einem \$ am Schluss des Namens werden nicht angezeigt.
- Beispiel: **net view \\server01**

► NET USE

- Startet oder beendet die Benutzung von Netzwerkressourcen.
- Beispiele:
 - **net use** zeigt die momentan benutzten Ressourcen an.
 - **net use x: \\server01\daten** macht die Freigabe "daten" als Laufwerk x: nutzbar.
 - **net use x: \\server01\daten *** macht dasselbe, fragt aber nach dem **Passwort** (notwendig, falls auf dem Server ein anderes Passwort definiert ist, als auf dem Client)
 - **net use x: \\server01\daten /user:peter *** (notwendig, wenn ein anderer Benutzer auf dem Server (z.B. Peter) benutzt wird, möglich unter NT, Win2000 und XP)



Befehle zum Ansehen der NetBIOS Namen

► Windows Plattformen

- NBTSTAT -n zeigt die eigenen Netbiosnamen an
- NBTSTAT -A 192.168.112.12 zeigt Netbiosnamen dieser Station
- NBTSTAT -r zeigt Resultate von Rundsendungen
- IPCONFIG /all zeigt Knotentyp an (e.g. Hybrid)

► OS/2 (Programme in den Server Utilities)

- NBJDSTAT 0 out.dat schreibt Netbios-Details von LAN Adapter 0 in File out.dat
- NETPING SRVANET12 sucht das System SRVANET12 im LAN



Beispiel von NetBios Namen

NBTSTAT -n unter WindowsXP:

LAN-Verbindung:

Knoten-IP-Adresse: [192.168.112.8] Bereichskennung: []

Lokale NetBIOS-Namentabelle

Name	Typ	Status
WSANET8	<00> EINDEUTIG	Registriert
CHANET2	<00> GRUPPE	Registriert
WSANET8	<03> EINDEUTIG	Registriert
WSANET8	<20> EINDEUTIG	Registriert
CHANET2	<1E> GRUPPE	Registriert
CHANET2	<1D> EINDEUTIG	Registriert
..__MSBROWSE__.	<01> GRUPPE	Registriert

NBJDSTAT 0 out.dat unter OS/2 (Teil):

```
Local address.....400090909002
Number of Free NCBs.....244
Configured NCB maximum.....254
Maximum NCBs.....254
Local station busy count.....0
Maximum datagram packet.....512
Number of pending sessions.....5
Configured session maximum.....254
Maximum sessions.....254
Maximum session packet.....4352
Number of names in table.....4
Name...SRVANET2      ..Name number..002..status..04..Unique name..A registered name
Name...SRVANET2      ..Name number..003..status..04..Unique name..A registered name
Name...CHANET2       ..Name number..004..status..84..Group name...A registered name
Name...SRVANET2      ..Name number..005..status..04..Unique name..A registered name
```

SMB Server

- ▶ Die meisten heutigen Server benutzen das SMB-Protokoll (und damit das NetBios API).
 - PC LAN Program (DOS)
 - Windows for Workgroups 3.1
 - Windows 95, 98, ME
 - Windows NT, 2000 und XP
 - OS/2 ab 1.1 und 2.0 und folgende
 - OS/2 Warp 3 und folgende
 - eComStation
 - eBusiness Server
 - Linux und andere Unixe mit Samba



NetBIOS über TCP/IP - Knotentypen

- ▶ Da bei TPC/IP der Namensbroadcast fehlt, muss eine andere Lösung zum Auffinden von NetBios Namen benutzt werden.
 - b-node
 - ▶ *Benutzt nur IP-Broadcasts für Registrierung und Namensauflösung (= nur im gleichen Subnet möglich)*
 - p-node
 - ▶ *Benutzt nur Point-to-Point Registrierung und Namensauflösung*
 - m-node
 - ▶ *benutzt Broadcast zur Registrierung, informiert dann den NBNS(NetBIOS Name Server). Benutzt Broadcast zur Namensauflösung, falls dies nicht geht, fragt er den NBNS*
 - h-node (hybrid Node)
 - ▶ *Benutzt den NBNS für Registrierung und Namensauflösung, Broadcast wenn dies nicht erfolgreich war*



NetBIOS-Namen

- ▶ Ein Unique NetBIOS-Name muss **einzig** sein im ganzen Netzwerk, Group Names können von mehreren Systemen genutzt werden (z.B. Workgroup- oder Domänen-Name)
- ▶ Für NetBIOS-Namen stehen **15 Bytes** frei zur Verfügung
 - Möglich sind **a-z, A-Z, 0-9** und die Spezialzeichen **!@#\$\$%^&()-'{}~***
 - dabei darf der * nicht am Anfang stehen und der \$ hat eine spezielle Funktion
- ▶ ein 16-tes Byte wird ergänzt und steuert die Bedeutung des Namens:
 - Einzelnamen (Unique im ganzen Netzwerk)
 - ▶ 00 Standard Arbeitstationsdienst
 - ▶ 03 Messenger Service (NET SEND und WINPOPOP)
 - ▶ 06 RAS Service (Remote Access Server)
 - ▶ 1B Domain Masterbrowser (vom Primary Domain Controller)
 - ▶ 1D Master Browser Name
 - ▶ 1F NetDDE Service
 - ▶ 20 File und Print Server
 - ▶ 21 RAS Client Service
 - ▶ BENetwork Monitor Agent
 - ▶ BF Network Monitor Utility
 - Gruppennamen (gemeinsam für mehrer Systeme)
 - ▶ 00 Domänen-Name oder Workgroup-Name
 - ▶ 1C Domänenname auf einem PDC oder BDC
 - ▶ 1E für Browserauswahl in Domäne/Workgroup



Wieweit sind die Namen sichtbar?

- ▶ Native NetBIOS (NetBEUI) ist sichtbar
 - soweit, wie NetBIOS Broadcasts durchgelassen werden:
 - ▶ durch Hubs
 - ▶ durch Switches
 - ▶ durch Bridges
 - ▶ durch Router nur, falls diese NetBIOS durchlassen (z.B. Data Link Switching), sonst sperrt ein Router die Broadcasts !
- ▶ NetBIOS over TCP/IP (NBT- NetBIOS Transport, TCPBEUI)
 - mit Broadcasts
 - ▶ nur im gleichen IP-Subnet, endet beim ersten Router
 - mit WINS-Server
 - ▶ alle Stationen, die den gleichen WINS-Server benutzen
 - mit DNS
 - ▶ alle Stationen, die diesen DNS-Server benutzen
 - mit Hilfstabelle auf jedem PC: LMHOSTS



Funktionen und Protokolle der SMB-Server

Plattform	File Sharing	Printer Sharing	Modem Sharing	NetBeui (native)	NetBios over TCP/IP	NetBios over IPX
DOS PC LAN Program	X	X	-	S	-	-
Windows 3.1	X	X	-	S	X	X
Windows 9x, ME	X	X	-	X	S	X
Windows NT4	X	X	-	X	S	X
Windows 2000	X	X	-	X	S	X
Windows XP	X	X	-	X*	S	X
OS2 Warp, eCS	X	X	X	S	X	X
Linux mit Samba	X	X	-	-	S	-

* bei Windows XP auf CD im Verzeichnis \VALUEADD\MSFT\NET\NETBEUI
 S=Standard, X=vorhanden, - =nicht vorhanden