## *Unterrichtseinheit 15:*

# Problembehandlung bei Windows2000-Netzwerkdiensten

Die Windows2000-Netzwerkinfrastruktur besteht aus vielen verschiedenen Komponenten und Verbindungen, in denen Netzwerkprobleme auftreten können.
Eine effektive Problembehandlung in Netzwerken besteht aus drei Phasen:

1. Untersuchen der Symptome von Netzwerkproblemen
2. Identifizieren der Ursachen von Netzwerkproblemen
   (evtl. mit Hilfe des Befehles **net helpmsg** ***Zahl*** und dem Ereignisprotokoll)
3. Lösen von Netzwerkproblemen

## Lösen von TCP/IP-Problemen

Der TCP/IP-Prozess, der Computern das Übertragen von Daten über ein Netzwerk ermöglicht, kann in vier verschiedene Schritte unterteilt werden:

1. Auflösen des Hostnamens oder NetBIOS-Names in eine IP-Adresse
2. Bestimmen der zu verwendenden Schnittstelle und der weiterleitenden IP-Adresse anhand der Ziel-IP-Adresse und der IP-Routingtabelle
3. Auflösen der weiterleitenden IP-Adresse in eine MAC-Adresse mit Hilfe von ARP (bei Broadcast-Verkehr auf gemeinsamen genutzten Zugriffstechnologien wird die MAC-Adresse 0xFF-FF-FF-FF-FF-FF zugeordnet)
4. Senden des Pakets an die MAC-Adresse

## Überprüfen der TCP/IP Konfiguration

Bei dem Dienstprogramm **ipconfig** handelt es sich um ein Befehlszeilentool, welches folgende Werte ausliest: IP-Adresse, Subnetzmaske, Standardgateway.

*Anmerkung:*
*Wenn als lokale Adresse 169.254.x.x zurückgegeben wird, wurde die IP-Adresse von der automatischen Zuweisung von privaten IP-Adressen von Windows 2000 zugewiesen. Die lokale Adresse 169.254.x.x zeigt an, dass der lokale DHCP-Server nicht ordnungsgemäß konfiguriert ist.*

## Anzeigen von Details der TCP/IP-Konfiguration

Die Ausgabe des Befehls **ipconfig** ***/all*** schließt zusätzliche Konfigurations-informationen ein, wie z.B. die Adressen von DNS- und WINS-Servern, die konfiguriert wurden oder die ein DHCP-Server zugewiesen hat. Wenn ein Computer beispielsweise mit einer doppelten IP-Adresse konfiguriert wurde, wird die Subnetmask als 0.0.0.0 angezeigt.

## Testen der IP-Konfiguration

Beim Dienstprogramm **ping** handelt es sich um ein Diagnosetool, mit dem die TCP/IP-Konfiguration überprüft und Verbindungsfehler diagnostiziert werden können. Um die Netzwerkkommunikation zu testen sollte man folgendermaßen vorgehen:

1. ping 127.0.0.1 (Loopbackadresse - verläst nicht die Netzwerkkarte)
2. ping *IP-Adresse des Computers*
3. ping *IP-Adresse des Standardgateways*
4. ping *IP-Adresse des Remotehosts*
5. ping *Hostname des Remotehosts*

Wenn der Befehl **ping** zu der Fehlermeldung „Zielhost nicht erreichbar“ führt, kann der andere Computer überhaupt nicht erreicht werden. Bei der Fehlermeldung „Zeitüberschreitung der Anforderung“ kann der Computer zwar erreicht werden, eine IPSec-Richtlinie blockiert jedoch unter Umständen die Kommunikation.

## Testen der Auflösung zwischen IP und MAC

**ARP**
Bei ARP (Address Resolution Protocol) handelt es sich um ein Protokoll der TCP/IP-Suite, das IP-Adressen in MAC-Adressen auflöst. Es ermöglicht einem Host, die MAC-Adresse eines Knotens anhand einer IP-Adresse im selben physikalischen Netzwerk zu finden.

**ARP-CACHE**
Wenn eine ARP-Anforderung beantwortet wird, zeichnen der Sender der ARP-Antwort **und** der ursprüngliche ARP-Antragsteller die jeweilige IP-Adresse und MAC-Adresse des anderen in einer lokalen Tabelle, dem ARP-CACHE, auf, die dynamische und statische Einträge enthält.
Anzeigen und ändern der Einträge mit dem Dienstprogramm **arp** (zur Anzeige der lokalen ARP-Cacheeinträge: **arp –a**).

*Anmerkung:*
*Jeder Netzwerkadapter verfügt auf einem Computer unter Windows2000 über einen eigenständigen ARP-Cache.*

**Dynamische Einträge (Standard)**
Dynamische Einträge unterliegen einer Alterung und werden aus dem Cache gelöscht, wenn sie innerhalb von zwei Minuten nicht wieder verwendet werden.

**Statische Einträge (z.B. DNS-Rootserver)**
Statische Einträge werden bis zum Neustart des Computers im Cache beibehalten und können helfen, den ARP-Broadcastverkehr im Netzwerk zu minimieren. Um einen statischen Eintrag hinzuzufügen muss an der Eingabeaufforderung **arp –s** *IP-Adresse MAC- Adresse* eingegeben werden.

**Löschen ungültiger Einträge im ARP-Cache**
Ungültige statische Einträge werden mit **arp –d** *IP-Adresse* aus dem ARP-Cache gelöscht.

## Problembehandlung bei IP-Routing

Der erste Schritt bei der Problembehandlung von IP-Routing besteht darin, zu überprüfen, ob ein Standardgateway konfiguriert ist und dieses eine Verbindung zum Host herstellen kann.
Ist das Standardgateway ordnungsgemäß konfiguriert, so wird die Kommunikation zwischen den Netzwerken mittels folgender Dienstprogramme überprüft:

**ping**
- Gültigkeitsdauer wurde bei der Übertragung überschritten
- Zielhost nicht erreichbar
- Zeitüberschreitung der Anforderung
- Unbekannter Host

**tracert** - ermittelt den Pfad zur Ziel-IP-Adresse

**pathping** - sendet Pakete an jeden Router in der Route bis zu einem Endziel und berechnet die Ergebnisse anhand der Pakete, die von jedem Abschnitt zurückgegeben werden. Das Programm kann das Ausmaß des Paketverlusts bei einem bestimmten Router oder Verbindung feststellen und bestimmen, ob ein bestimmter Router oder Verbindung Netzwerkprobleme verursacht

## Lösen von Problemen bei der Namensauflösung

Es muss zuerst bestimmt werden, ob die fehlerhafte Anwendung NetBIOS- oder Hostnamen verwendet.

### Hostnamensprobleme

Probleme bei der Hostnamensauflösung können an einer fehlerhaften Konfiguration der Datei **HOSTS** (%SystemRoot%\System32\Drivers\Etc) oder des DNS-Servers liegen.

Um DNS-Abfragen durchzuführen, sowie die DNS-Installation testen und DNS-Probleme behandeln zu können, wird das Dienstprogramm **nslookup** (siehe Kapitel 15 / Seite 18 Tabelle) verwendet.

Bei der Isolierung von Netzwerk- und Verbindungsproblemen hilft zu Diagnosezwecken das Dienstprogramm **NetDiag**. Es diagnostiziert Netzwerkprobleme, indem alle Aspekte der Netzwerkkonfiguration und Verbindungen eines Hostcomputers überprüft werden.

**NetBIOS-Namensprobleme**

Mit den Befehlen **nbtstat** und **net view** können Probleme bei NetBIOS-Namensauflösungen diagnostiziert werden.

| | |
|---|---|
| **nbstat –n** | - identifizieren von NetBIOS-Namen, die ein Computer mit Hilfe von NetBT registriert hat |
| **nbstat –R** | - erneutes registrieren beim Namensserver, nachdem ein Computer bereits gestartet wurde |
| **net view** | - anzeigen von Listen der Domänen, Computern, Ressourcen |

## Problembehandlung bei Netzwerkdiensten

Zur Problembehandlung und zum Lösen von Problemen mit Netzwerkdiensten wird die Konsole **Dienste**, auf die im Menü **Verwaltung** oder der Konsole **Computerverwaltung** aus zugegriffen werden kann verwendet.

## Überwachen des Netzwerkes

Mit einem Dienstprogramm zur Analyse von Netzwerkpaketen können Informationen zur Netzwerkfunktionalität zusammengestellt werden. Es ermöglicht:

- Überwachen der Netzwerkauslastung oder –bandbreite in Echtzeit
- Problembehandlung von Netzwerkfehlern durch Diagnostizieren von Kabelverbindungen, Bandbreiten- oder Protokollproblemen und defekten Netzwerkkarten
- Bestimmen anhand von Überwachungsinformationen, wie das Netzwerk durch Aufteilen in Teilnetze optimiert werden kann
- Planen des Erwerbs zusätzlicher Geräte für das Netzwerk anhand von Überwachungsfunktionen

Der **Microsoft Netzwerkmonitor** (softwarebasiertes Dienstprogramm)

- sammelt Pakete direkt aus dem Netzwerk
- filtert und zeigt Pakete unmittelbar nach einer Sammlung an, oder speichert die gesammelten Daten in einer CAP-Datei
  (Speicherort: WINNT\System32\netmon\Captures)
- für eine spätere Analyse
- Möglichkeit der Bearbeitung gesammelter Pakete und Übertragen der Pakete zurück in das Netzwerk
- Sammeln von Paketen von einem Remotecomputer

***Wichtig:***
*Um den Netzwerkmonitor installieren oder verwenden zu können, muss man Mitglied der Gruppe Administratoren sein.*

## Sammlungsfilter

Ein Sammlungsfilter beschreibt die Rahmen, die gesammelt, gepuffert, angezeigt und gespeichert werden sollen. Dazu müssen erst die Excludefilter vor den Includefiltern und anschließend der **Sammlungsauslöser** definiert werden.

# Hilfe für Befehle mit –optionen

## ARP

```
ändert und zeigt die Übersetzungstabellen für IP-Adressen/physikalische
Adressen an, die von ARP (Address Resolution Protocol) verwendet werden.

ARP -s IP_Adr Eth_Adr [Schnittst]
ARP -d IP_Adr [Schnittst]
ARP -a [IP_Adr] [-N Schnittst]

   -a            Zeigt aktuelle ARP-Einträge durch Abfrage der Protokoll-
                 daten an. Falls IP_Adr angegeben wurde, werden die IP- und
                 physikalische Adresse für den angegebenen Computer ange-
                 zeigt. Wenn mehr als eine Netzwerkschnittstelle ARP
                 verwendet, werden die Einträge für jede ARP-Tabelle
                 angezeigt.
   -g            Gleiche Funktion wie -a.
   IP_Adr        Gibt eine Internet-Adresse an.
   -N Schnittst  Zeigt die ARP-Einträge für die angegebene Netzwerk-
                 schnittstelle an.
   -d            Löscht den durch IP_Adr angegebenen Hosteintrag. Die IP-Adr
                 kann mit dem '*'-Platzhalter versehen werden, um alle Hosts
                 zu löschen.
   -s            Fügt einen Hosteintrag hinzu und ordnet die Internetadresse
                 der physikalischen Adresse zu. Die physikalische Adresse wird
                 durch 6 hexadezimale, durch Bindestrich getrennte Bytes
                 angegeben. Der Eintrag ist permanent.
   Eth_Adr       Gibt eine physikalische Adresse (Ethernetadresse) an.
   Schnittst     Gibt, falls vorhanden, die Internetadresse der Schnittstelle
                 an, deren Übersetzungstabelle geändert werden soll.
                 Sonst wird die erste geeignete Schnittstelle verwendet.
Beispiel:
  > arp -s 157.55.85.212  00-aa-00-62-c6-09 ... Fügt statischen Eintrag hinzu.
  > arp -a                                  ... Zeigt die ARP-Tabelle an.
```

## IPCONFIG

```
Syntax:
   ipconfig [/? ¦ /all ¦ /release [Adapter] ¦ /renew [Adapter]
            ¦ /flushdns ¦ /registerdns
            ¦ /showclassid Adapter
            ¦ /setclassid Adapter [Klassenkennung] ]

   Adapter    Ganzer Name oder Zeichen mit "*" und "?", wobei
              "*" für beliebig viele und "?" für ein Zeichen steht.
   Optionen
       /?           Zeigt diesen Hilfetext an.
       /all         Zeigt die vollständigen Konfigurationsinformationen an.
       /release     Gibt die IP-Adresse für den angegebenen Adapter frei.
       /renew       Erneuert die IP-Adresse für den angegebenen Adapter.
       /flushdns    Leert den DNS-Auflösungscache.
       /registerdns Aktualisiert alle DHCP-Leases und registriert DNS-Namen.
       /displaydns  Zeigt den Inhalt des DNS-Auflösungscaches an.
       /showclassid Zeigt alle DHCP-Klassenkennungen an, die für diesen Adapter
                    zugelassen sind.
       /setclassid  ändert die DHCP-Klassenkennung.

Standardmäßig wird nur die IP-Adresse, die Subnetzmaske und das Standard-
gateway für jeden an TCP/IP gebundenen Adapter angezeigt.

Wird bei /RELEASE oder /RENEW kein Adaptername angegeben, so werden
die IP-Adressen von allen an TCP/IP gebundenen Adapter freigegeben
oder erneuert.

Wird bei /SETCLASSID keine Klassenkennung angegeben, dann wird die Klassen-
kennung gelöscht.

Beispiele:
    > ipconfig                    ... Zeigt Informationen an.
    > ipconfig /all               ... Zeigt detaillierte Informationen an.
    > ipconfig /renew             ... Erneuert IP-Adressen für alle
                                      Adapter.
    > ipconfig /renew EL*         ... Erneuert IP-Adressen für Adapter
                                      mit Namen EL....
    > ipconfig /release *ELINK?21*... Gibt alle entsprechenden Adapter
                                      frei, z.B. ELINK-21, ELINKi21karte usw.
```

## NTBSTAT

```
Zeigt Protokollstatistik und aktuelle TCP/IP-Verbindungen an, die
NBT (NetBIOS über TCP/IP) verwenden.

NBTSTAT [-a Remotename] [-A IP-Adresse] [-c] [-n]
        [-r] [-R] [-RR] [-s] [Intervall] ]

  -a          Zeigt die Namentabelle des mit Namen angegebenen
              Remotecomputers an.
  -A          Zeigt die Namentabelle des mit IP-Adressen angegebenen
              Remotecomputers an.
  -c          Zeigt Inhalt des Remotenamencache mit IP-Adressen an.
  -n          Zeigt lokale NetBIOS-Namen an.
  -r          Zeigt mit Broadcast und WINS aufgelöste Namen an.
  -R          Lädt Remotecache-Namentabelle neu.
  -S          Zeigt Sitzungstabelle mit den Ziel-IP-Adressen an.
  -s          Zeigt Sitzungstabelle mit Computer NetBIOS-Namen an, die aus
              den Ziel-IP-Adressen bestimmt wurden.
  -RR         (ReleaseRefresh) Sendet Namensfreigabe-Pakete an WINS und
              startet die Aktualisierung.

  Remotename  Name des Remotehosts
  IP-Adresse  Punktierte Dezimalschreibweise einer IP-Adresse
  Intervall   Zeigt die ausgewählte Statistik nach der angegebenen
              Anzahl Sekunden erneut an. Drücken Sie STRG+C zum Beenden
              der Intervallanzeige.
```

## NSLOOKUP

```
Befehle:  (Kennungen werden in Großbuchstaben angezeigt, [] steht für optional)
NAME                        - Info über Host/Domäne NAME
                              (verwendet Standardserver)
NAME1 NAME2                 - Wie oben; verwendet NAME2 als Server
help oder ?                 - Info über allgemeine Befehle; siehe auch
                              nslookup(1)
set OPTION                  - Legt eine Option fest
    all                     - Zeigt alle Optionen, aktuelle Server und
                              Hosts an
    [no]debug               - Zeigt Debuginformationen an
    [no]d2                  - Zeigt ausführliche Debuginformationen an
    [no]defname             - Fügt jeder Abfrage den Domänenname an
    [no]recurse             - Rekursive Antwort auf Anfrage
    [no]search              - Verwendet die Domänensuchliste
    [no]vc                  - Verwendet immer einen "virtual circuit"
    domain=NAME             - Legt den Standarddomänennamen mit NAME fest
    srchlist=N1[/N2/.../N6]  - Legt Domäne mit N1 und Suchliste mit
                              N1,N2.. fest
    root=NAME               - Legt den Stammserver mit NAME fest
    retry=X                 - Legt die Anzahl der Neuversuche mit X fest
    timeout=X               - Legt das erste Zeitüberschreitungsintervall
                              mit X Sekunden fest
    querytype=X             - Legt den Abfragetyp fest, z.B.
                              A,ANY,CNAME,HINFO,NS,SOA,WKS
    type=X                  - Synonym mit "querytype"
    class=X                 - Legt die Abfrageklasse mit IN, CHAOS,
                              HESIOD oder ANY fest
server NAME                 - Legt mit dem akt. Server den Standardserver
                              mit NAME fest
lserver NAME                - Legt mit dem 1. Server den Standardserver
                              mit NAME fest
finger [USER]               - Führt den Befehl "finger" für NAME aus
root                        - Legt den aktuellen Standardserver mit
                              "root" fest
ls [opt] DOMÄNE [> DATEI]   - Zeigt Adressen in DOMÄNE an
                              (Ausgabe in DATEI)
    -a                      - Führt kanonische Namen und Aliase auf
    -d                      - Führt alle Einträge auf
    -t TYP                  - Führt die Einträge des Typs auf
                              (z.B. A, CNAME, MX, usw.)
view DATEI                  - Sortiert eine "ls"-Outputdatei und zeigt
                              sie mit "pg" an
exit                        - Beendet das Programm, auch EOF (z.B. ^D)
                              möglich
```

## PATHPING

```
Syntax: pathping [-n] [-h max. Abschnitte] [-g Hostliste] [-p Zeitraum]
                 [-q Abfrageanzahl] [-w Zeitlimit] [-t] [-R] [-r] Zielname

Optionen:
    -n                  Adressen nicht in Hostnamen auflösen.
    -h max. Abschnitte  Max. Anzahl an Abschnitten bei Zielsuche.
    -g Hostliste        "Loose Source Route" gemäß Hostliste.
    -p Zeitraum         Wartezeit in Millisekunden zwischen Pings.
    -q Abfrageanzahl    Anzahl der Abfragen pro Abschnitt.
    -w Zeitlimit        Zeitlimit in Millisekunden für eine Antwort.
    -T                  Überprüft Verbindung zu jedem Abschnitt mit
                        Layer-2-Prioritätskennungen.
    -R                  überprüft, ob jeder Abschnitt RSVP unterstützt.
```

## PING

```
Syntax: ping [-t] [-a] [-n Anzahl] [-l Größe] [-f] [-i Gültigkeitsdauer]
             [-v Diensttyp] [-r Anzahl] [-s Anzahl] [[-j Hostliste] |
             [-k Hostliste]] [-w Zeitlimit] Zielliste

Optionen:
    -t              Sendet fortlaufend Ping-Signale zum angegebenen Host.
                    Geben Sie STRG-UNTRBR ein, um die Statistik anzuzeigen.
                    Geben Sie STRG-C ein, um den Vorgang abzubrechen.
    -a              Löst Adressen in Hostnamen auf.
    -n n Anzahl     Anzahl zu sendender Echoanforderungen
    -l Länge        Pufferlänge senden
    -f              Setzt Flag für "Don't Fragment".
    -i TTL          Gültigkeitsdauer (Time To Live)
    -v TOS          Diensttyp (Type Of Service)
    -r Anzahl       Route für Anzahl der Abschnitte aufzeichnen
    -s Anzahl       Zeiteintrag für Anzahl Abschnitte
    -j Hostliste    "Loose Source Route" gemäß Hostliste
    -k Hostliste    "Strict Source Route" gemäß Hostliste
    -w Zeitlimit    Zeitlimit in Millisekunden für eine Rückmeldung
```

## TRACERT

```
Syntax: tracert [-d] [-h Abschnitte max] [-j Hostliste] [-w Zeitlimit]
                Zielname

Optionen:
    -d                  Adressen nicht in Hostnamen auflösen
    -h Abschnitte max   Max. Anzahl an Abschnitten bei Zielsuche
    -j Hostliste        "Loose Source Route" gemäß Hostliste
    -w Zeitlimit        Zeitlimit in Millisekunden für eine Antwort
```