Zusammenfassung aus den
Kursunterlagen

MOC 70-216
Implementieren einer Netzwerkinfrastruktur unter Windows 2000

Inhaltsverzeichnis

Unterrichtseinheit 1 *Seite*

Einführung die Netzwerkinfrastruktur 1

Übersicht über die Netzwerkinfrastruktur 1

Unterrichtseinheit 2 *Seite*

Automatisieren der IP-Adresszuweisung mit Hilfe von DHCP 1

Funktionsweise von DHCP 1

Erzeugungsvorgang für die DHCP 1

Erneuerungsvorgang für die DHCP-Lease 3

Anforderungen für DHCP-Server und -Clients 4

Aktivieren von DHCP-Clients 4

Installieren des DHCP-Dienstes 4

Autorisieren des DHCP-Dienstes 4

Erstellen und Konfigurieren eines Bereichs 5

Änder der Standardgültigkeitsdauer (8 Tage) einer Lease 5

Konfigurieren eines Bereichs mit Optionen 6

Reservieren von IP-Adressen für Clientcomputer 7

Anpassen der DHCP-Funktionalität 7

Verwenden von Optionsklassen 7

Ausgeben von Multicastadressen mit Hilfe von Multicastbereichen 8

Konfigurieren von DHCP in einem gerouteten Netzwerk 8

Unterrichtseinheit 3 *Seite*

Implementieren der Namensauflösung mit Hilfe von DNS 1

Übersicht über den DNS-Abfrageprozess 1

Installieren des DNS-Serverdienstes 2

Konfigurieren von Clientcomputern 2

Erstellen von Zonen 2

Identifizieren von Zonentypen 3

Konfigurieren von Standardzonen 3

Zonenübertragungsvorgang 3

Zonenübertragung 3

Inkrementelle Zonenübertragung 4

Konfigurieren von Zonenübertragungen 4

Änder des SOA-Ressourceneintrags 4

Konfigurieren von Zonenübertragungssicherheit 5

Konfigurieren der Benachrichtigung 5

Erstellen einer untergeordneten Domäne in einer vorhandenen Zone 5

Konfigurieren von Active Directory-integrierten Zonen 6

Umwandeln von vorhandenen Standardzonen 6

Migrieren von Zonen zum Windows 2000 DNS-Serverdienst 6

Umbenen von Zonendateien 7

Konfigurieren von DNS für die interne Verwendung 7

Integrieren von DNS und DHCP 7

Protokoll für die dynamische Aktualisierung 7

Konfigurieren des DHCP-Servers für dynamische Aktualisierungen 8

Konfigurieren W2000-basierter Clients für dynamische Aktualisierungen 8

Verwalten von DNS-Servern und Beheben von Problemen 9

Verwalten von DNS-Zonen 9

Überwachen von DNS-Servern 10

Überprüfen von Ressourceneinträgen mit Nslookup 10

Fehlerbehebung bei der Namensauflösung 10

Unterrichtseinheit 4 ***Seite***

Implementieren der Nemansauflösung mit Hilfe von WINS 1

NetBios-Namensschema 1

Namen bekannt geben und ermitteln 1

NetBios-Namensauflösung 1

NetBios über TCP/IP-Namensauflösungsknoten 2

LMHOSTS-Datei 2

WINS-Server Funktion 3

WINS und DNS 4

WINS-Proxy 5

WINS-Replikation 5

Überprüfen von Replikationspatnern 5

WINS-Datenbank 6

Sichern und Wiederherstellen der WINS-Datenbank 7

Unterrichtseinheit 5 *Seite*

Konfigurieren der Netzwerksicherheit mit Hilfe von PKI 1

Verschlüsselung mit öffentlichen Schlüsseln 1

Authentifizierung mit öffentlichen Schlüsseln 1

Digitale Signatur 1

Zertifizierung 2

Primäre Windows 2000 PKI-Komponenten 2

Bereitstellen der Zertifikatsdienste 2

Organisations-zertifizierungsstelle 2

Installieren der Zertifikatsdienste 3

Erstellen einer untergeordneten Zertifizierungsstelle 3

Zertifikatsanforderungs-Assistenten 4

Zertifikatsdienste-Webseiten 4

Anzeigen von Zertifikaten 4

Verwalten von Zertifikaten 5

Importieren und Exportieren von Zertifikaten 5

Konfigurieren von Active Directory für Zertifikate 5

Problembehandlung 5

Unterrichtseinheit 6 *Seite*

Netzwerksicherheit mit Hilfe von IPSec 1

Häufige Arten von Netzwerkangriffen 1

Untersuchen der Rolle von IPSec in einem Netzwerk 1

Erweitere Netzwerksicherheit (grober Ablauf) 2

Aktivieren IPSec 2

Verwalten von IP-Sicherheitsrichtlinien 2

Verwendung von vordefinierten IP-Sicherheitsrichtlinien 2

Aktivieren einer IP-Sicherheitsrichtlinie 3

Verwenden von IPSec im Übertragungsmodus 3

Konfigurieren von IPSec für Sicherheit zwischen Netzwerken 3

Verwenden von IPSec im Tunelmodus 3

Regelkomponenten 4

Standardantwortregel 4

Auswählen eines IPSec-Verschlüsselungsschemas 4

Überprüfung einer Zuweisung von IP-Sicherheitsrichtlinien 5

Verwenden der IP-Sicherheitsüberwachung zum Überprüfen der Zuweisung einer Richtlinie 5

Optimieren der IPSec-Leistung 5

Konfigurieren von TCP/IP für die Serversicherheit 5

Überprüfen der IP-Sicherheitsrichtlinie bei Auftreten von Problemen 5

Unterrichtseinheit 7 *Seite*

Konfigurieren von Remotezugriff 1

Aufbau einer RAS-Verbindung 1

Datentransportprotokoll 1

VPN-Protokoll 2

Konfigurieren eingehender Verbindungen 2

Konfigurieren von Benutzereinwähleinstellungen 3

Konfigurieren ausgehender Verbindungen (Client) 4

Erstellen einer DFÜ-Verbindung Kap 4

Herstellen einer Verbindung zu einem virtuellen privaten Netzwerk VPN 4

Konfigurieren von Authentifizierungsprotokollen 6

Standardmäßige Authentifizierungsprotokolle 6

Konfigurieren von Verschlüsselungsprotokollen (für Daten) 7

Konfigurieren von Routing und RAS für die DHCP-Integration 8

Unterrichtseinheit 8 *Seite*

Unterstützen des Remotezugriffs auf ein Netzwerk 1

Untersuchen von RAS-Richtlinien 1

Folgen der Auswertungslogik von Richtlinien 1

Untersuchen von Standardrichtlinien 2

Konfigurieren von RAS-Richtlinienbedingungen 3

Konfigurieren von RAS-Richtlinienbedingungen 3

Überwachen des Remotezugriffs 4

Verfolgen des Ablaufs von RAS-Verbindungen 4

Unterrichtseinheit 9 *Seite*

Erweitern der RAS-Fähigkeiten mit Hilfe von IAS 1

IAS und RADIUS in einem Windows 2000-Netzwerk 1

Zweck und Verwendung von IAS 1

Installation und Konfiguration von IAS 2

Konfiguration eines RAS-Server für die Verwendung der RADIUS-Authentifizierung 2

Konfiguration eines RAS-Server für die Verwendung der RADIUS-Kontoführung 2

Konfiguration der Protokolle für Kontoführungsinformationen 2

Unterrichtseinheit 10 *Seite*

Konfigurieren eines Windows 2000-basierten Servers als Router 1

Zweck des Routings und Routingtabelle 1

Konfiguration von Netzwerkverbindungen 2

Aktivieren von Routing mit Hilfe von Routing und RAS 2

Untersuchen einer statischen Routingtabelle 3

Hinzufügen einer statischen Route 3

Konfigurieren einer Routingschnittstelle 3

Paketfilterung 4

Konfigurieren von Filtern an einer IP-Routingschnittstelle 4

Routing für Wählen bei Bedarf 5

Konfigurieren von IP-Adressen für eingehende bei Bedarf herzustellende Wählverbindungen 6

Konfigurieren statischer Routen für eine Schnittstelle für Wählen bei Bedarf 6

RIP und OSPF 7

Konfigurieren des RIP-Betriebsmodus und dessen Protokolle 8

Konfigurieren von Routenfiltern 9

Konfigurieren von RIP für ein Nicht-Broadcastnetzwerk 9

Unterrichtseinheit 11 ***Seite***

Konfigurieren des Internetzugriffs für ein Netzwerk 1

Herstellen einer Verbindung mit dem Internet mit Hilfe eines Routers 1

Schützen von Internetverbindungen mit Hilfe einer Firewall 2

Herstellen einer Verbindung mit dem Internet mit Hilfe von NAT 2

Herstellen einer Verbindung mit dem Internet bei gemeinsamer Nutzung der Internetverbindung 4

Herstellen einer Verbindung mit dem Internet mit Hilfe eines Proxyservers 4

Unterrichtseinheit 12 *Seite*

Konfigurieren eines Webservers 1

Übersicht IIS 1

Vorbereitung einer ISS-Installation 1

Installieren von IIS (Version 5.0) 1

Konfigurieren einer Website 2

Konfigurieren des Basisverzeichnises 2

Identifizierung von Authentifizierungsmetoden 2

Auswählen einer Authentifizierungsmetode 3

Auswählen mehrerer Autentifizierungsmetoden 3

Konfigurieren der Authentifizierungsmetoden 4

Zuweisen eines Standarddokuments 4

Verwalten von IIS 4

Überwachen von Internet-Informationsdiensten 5

Testen einer Website im Intranet 5

Auflösen von IIS-Problemen 5

Unterrichtseinheit 13 *Seite*

Bereitstellen von Windows2000 Professional mit Hilfe von RIS 1

RIS-Übersicht 1

Identifizieren der RIS-Anforderungen 1

Installieren und Starten von RIS 2

Autorisieren des RIS-Servers 3

Zuweisen von Benutzerberechtigungen 3

Konfigurieren von Clientcomputernamen und Pfaden 4

Einrichten von Vorstufen-Clientcomputern 4

Ermitteln einer GUID 4

Bereitstellen von Abbildern mit Hilfe einer RIS 5

Erstellen eines RIPrep-Abbilds 5

Einrichten eines Quellcomputers 5

Ändern des Standardbenutzerprofils 6

Erstellen eines RIPrep-Abbilds 6

Vergleichen von CD-basierten Abbildern und RIPrep-Abbildern 6

Unterrichtseinheit 14 *Seite*

Verwalten eines Windows2000-Netzwerkes 1

Terminaldienste 1

SNMP-Betrieb 2

Unterrichtseinheit 15 *Seite*

Problembehandlung bei Windows 2000-Netzwerkdiensten 1

Lösen von TCP/IP-Problemen 1

Überprüfen der TCP/IP Konfiguration 1

Anzeigen von Details der TCP/IP-Konfiguration 1

Testen der IP-Konfiguration 2

Testen der Auflösung zwischen IP und MAC 2

Problembehandlung bei IP-Routing 3

Lösen von Problemen bei der Namensauflösung 3

Problembehandlung bei Netzwerkdiensten 4

Überwachen des Netzwerkes 4

Sammlungsfilter 4

Hilfe für Befehle mit -optionen 5

Unterrichtseinheit 16 *Seite*

Konfigurieren von Netzwerkverbindungen unter unterschiedlichen Betriebssystemen 1

Zugriff auf NetWare-Resourcen 1

Zugriff auf Windows2000-Ressourcen für Macintosh-Benutzer 2

Herstellen einer Verbindung zu SNA-Hosts mit Hilfe von MS Host Integration Server 2000 2

Herstellen von Verbindungen zu UNIX-Ressourcen 3

Unterrichtseinheit 1:

Einführung in die Netzwerkinfrastruktur

Windows 2000 wird während der Installation standardmäßig mit dem Netzwerkprotokoll TCP/IP installiert!

Übersicht über die Netzwerkinfrastruktur:

- **Intranet**
  Privates lokales Netzwerk (**L**ocal **A**rea **N**etwork, **LAN**) in einer Organisation, das für die Verteilung und Nutzung interner Informationen und Ressourcen vorgesehen ist.
  TCP/IP stellt die Grundlage für die Verbindungen im Netzwerk bereit.

- **Remotezugriff**
  Verbindung zu einem Netzwerk (Server) mittels RAS-Einwahl (**R**emote **A**ccess **S**ervice) eines Mitarbeiters, der sich nicht ihm LAN befindet.
  Es gibt zwei Arten von RAS-Verbindungen unter Windows 2000:
  - *DFÜ-Remotezugriff (**D**aten-**F**ern-**Ü**bertragung):*
    Zugriff über das öffentliche Telefonnetz, um eine Verbindung zum RAS-Server herzustellen (für Organisationen mit wenigen Remotebenutzern, oder bei Remotebenutzer innerhalb des Ortstarifbereiches)
  - *VPN-Remotezugriff (**v**irtuelles **p**rivates **N**etzwerk):*
    Zugriff über das Internet durch eine verschlüsselte Punkt-zu-Punkt-Verbindung mit einem VPN-Gateway (Kostenreduzierung für Ferngespräche und Schnelligkeit durch Breitbandunterstützung)

- **Remoteniederlassung**
  Teil einer Organisation der sich in einem geografisch getrennten Gebiet befindet. Das LAN der Remoteniederlassung kann mittels einer RAS-Verbindung mit der Organisation als dauerhafte Verbindung durch einen WAN (**W**ide **A**rea **N**etwork) verbunden werden.

- **Internet**
  Weltweites Netzwerk, welches mittels TCP/IP-Protokollen miteinander kommuniziert. Die Verbindungen werden entweder mit einer DFÜ-Verbindung zu einem **I**nternet **S**ervice **P**rovider (ISP) oder einer dedizierten T1-Trägerleitung (Standleitung) mit einem LAN hergestellt

- **Extranet**
  Ein Netzwerk, aufgebaut in Internet-Technologie, das die Zusammenarbeit zwischen verschiedenen Unternehmen (Lieferanten, Kunden, Geschäftspartner...) durch die gemeinsame Nutzung von Informationen (durch Erweiterung des Intranets) vereinfachen soll.

Unterrichtseinheit 2:

Automatisieren der IP-Adresszuweisung mit Hilfe von DHCP

Ein DHCP-Server verwendet einen Leaseerzeugungsvorgang um Clientcomputern für einen bestimmten Zeitraum IP-Adressen zuzuweisen.
Der Vorteil von DHCP gegenüber manueller TCP/IP-Vergabe besteht eindeutig in der Flexibilität und der Fehlervermeidung im Netzwerk!

Funktionsweise von DHCP:

Jedes Mal, wenn ein DHCP-Client gestartet wird, fordert er eine IP-Adresse von einem DHCP-Server (welcher einen Bereich von Adressen in seiner Datenbank bereithält) an.
Der Server weist daraufhin eine vom Client akzeptierte IP-Adresse für einen bestimmten Zeitraum (Standard: 8 Tage, jedoch konfigurierbar) zu.

Die vom DHCP-Server an den DHCP-Client gesendeten Informationen zur IP-Adressierung können mehrere Elemente enthalten, wie z.B.:

- IP-Adresse
- Subnetzmaske
- Optionale Werte:
    - Adresse eines Standardgateways (Router)
    - IP-Adressen von DNS-Servern (**D**omain **N**ame **S**ystem)
    - IP-Adressen von WINS-Servern (**W**indows **I**nternet **N**ame **S**ervice)

Anmerkung:
*Weitere Informationen zu BOOTP (Bootstrap Protocol) in Verbindung mit DHCP befinden sich in RFC 1542 unter **Weiterführen-de Literatur** auf der CD!*

Erzeugungsvorgang für die DHCP:

DHCP weist die Informationen zur IP-Adressierung in einem aus vier Schritten bestehenden Vorgang zu:

1. **IP-Leaseanforderung (DHCPDISCOVER)**

   Der Vorgang beginnt, wenn der Client eine limitierte Version von TCP/IP initialisiert (er verwendet 0.0.0.0 als Quelladresse und 255.255.255.255 als Zieladresse) und eine DCHPDISCOVER-Meldung für Informationen zur IP-Adressierung als Broadcast an das gesamte Teilnetz sendet. Die Anforderungsmeldung enthält darüber hinaus auch die MAC-Adresse (**M**edia **A**ccess **C**ontrol) und den Computernamen des Clients.

2. IP-Leaseangebot (DHCPOFFER)

Alle DHCP-Server, die über eine vom Client für das angeforderte Netzwerksegment gültige IP-Adresse verfügen, antworten mit einer DHCPOFFER-Meldung, welche die folgenden Informationen enthält:

- Hardwareadresse des Clients
- eine angebotene IP-Adresse
- eine Subnetzmaske
- Gültigkeitsdauer der Lease
- eine Serverkennung, die der IP-Adresse des anbietenden DHCP-Servers entspricht

Jeder antwortende DHCP-Server reserviert die angebotene IP-Adresse, sodass diese keinem anderen DHCP-Client angeboten wird, bevor der anfordernde Client die Adresse akzeptiert hat.
Der DHCP-Client wartet eine Sekunde lang auf ein Angebot. Erhält er keines, dann sendet er die Anforderung noch viermal als Broadcast in Abständen von 2, 4, 8 und 16 Sekunden, zusätzlich zu einer zufälligen Dauer zwischen 0 und 1000 Millisekunden!
Erhält der Client auch nach vier Anforderungen kein Angebot, so verwendet er eine IP-Adresse im reservierten Bereich (APIPA – private Class B Bereich) von 169.254.0.1 bis 169.254.255.254 und versucht weiterhin in Abständen von fünf Minuten einen DHCP-Server zu finden.

3. IP-Leaseauswahl (DHCPREQUEST)

Der DHCP-Client antwortet auf das erste Angebot das er erhält, indem er eine DHCPREQUEST-Meldung als Broadcast sendet, um dieses zu akzeptieren. Diese Meldung enthält die Serveridentifizierung des Servers, dessen Angebot er akzeptiert hat. Alle anderen DHCP-Server ziehen daraufhin ihre Angebote zurück und geben ihre reservierte IP-Adresse wieder frei.

4. IP-Leasebestätigung (DHCPACK)

Der DHCP-Server, welcher das akzeptierte Angebot ausgibt, sendet eine Bestätigungsmeldung (DHCPACK) als Broadcast, um die erfolgreiche Lease zu bestätigen. Diese Meldung enthält eine gültige Lease für die IP-Adresse und andere Konfigurationsinformationen.

Wichtig:
*Jede Kommunikation zwischen einem DHCP-Server und einem DHCP-Client findet mit Hilfe der UDP-Anschlüsse (**U**ser **D**atagram **P**rotocol) 67 und 68 statt.*

Erneuerungsvorgang für die DHCP-Lease:

In bestimmten Abständen versucht ein DHCP-Client, seine Lease zu erneuern, um sicherzustellen, dass die enthaltenen Konfiguartionsinformationen auf dem aktuellen Stand sind.

- **Automatische Leaserneuerung:**

  Ein DHCP-Client versucht automatisch mit einer DHCPREQUEST-Meldung seine Lease zu erneuern, wenn von dieser 50% der Gültigkeitsdauer abgelaufen sind.
  Ist der DHCP-Server verfügbar, so erneuert er die Lease und sendet eine DCHPACK-Meldung mit der neuen Lease-Gültigkeitsdauer und aktualisierten Konfigurationsparametern an den Client, welcher daraufhin seine Konfiguration erneuert.
  Sind hingegen schon 87,5% der gegenwärtigen Gültigkeitsdauer der Lease abgelaufen und der zuständige DHCP-Server antwortet nicht, so akzeptiert der DCHP-Client eine Lease, die von einem anderen beliebigen DHCP-Server ausgegeben wird.
  Läuft die Lease allerdings ab, ohne das sich ein DHCP-Server gemeldet hat, so muss der Client die Verwendung der gegenwärtigen IP-Adresse sofort beenden!

Anmerkung:
Startet ein DHCP-Client neu, so versucht er automatisch, die vor dem Herunterfahren gültige IP-Adresslease zu erneuern. Schlägt dies fehl, so versucht eine Verbindung mit dem konfigurierten Standardgateway herzustellen. Antwortet dieser und ist die Gültigkeitsdauer der Lease noch nicht abgelaufen, so verwendet der DHCP-Client bis zum nächsten Versuch der Leaseerneuerung die gleiche IP-Adresse. Schlägt allerdings die Verbindung zum Standardgateway fehl, so verwendet der Client eine IP-Adresse im reservierten Bereich (169.254.0.1 – 169.254.255.254) und versucht in Abständen von fünf Minuten eine Verbindung mit einem DHCP-Server herzustellen!

- **Manuelle Leaseerneuerung:**

  Um z.B. die Adresse eines neu installierten Routers dem DHCP-Client sofort mitzuteilen kann man die Lease auch manuell mit folgendem Befehl erneuern:

  ipconfig /renew

  Dies bewirkt, dass eine DHCPREQUEST-Meldung an den Server geschickt wird, der daraufhin die Lease erneuert und die Konfigurationsoptionen des Clients aktualisiert!

Anmerkung:
*Um eine Lease wieder freizugeben kann der Befehl **ipconfig /release** verwendet werden.*

Anforderungen für DHCP-Server und –Clients:

Serveranforderungen:

- DHCP-Dienst
- statische IP-Adresse, Subnetzmaske, Standardgateway
- Bereich gültiger IP-Adressen

Clientanforderungen:

- Windows für Workgroups 3.11 (mit TCP/IP-32)
- Windows 95, 98, 2000
- Windows NT (ab Version 3.51)
- MS Network Client 3.0 für MS-DOS
- LAN Manager 2.2c
- Viele Nicht-Microsoft-Betriebssysteme

Aktivieren von DHCP-Clients:

Um einen DHCP-Client unter Windows 2000 zu aktivieren müssen folgende Schritte unternommen werden:
Eigenschaftsdialogfeld für die Netzwerkverbindung öffnen → Internetprotokoll (TCP/IP) → Eigenschaften → Allgemein → IP-Adresse automatisch beziehen → DNS-Serveradresse automatisch beziehen → OK

Installieren des DHCP-Dienstes:

Wichtig:
Vor dem Installieren des DHCP-Dienstes auf dem DHCP-Server muss eine statische IP-Adresse, eine Subnetzmaske und eine Standardgatewayadresse für den an TCP/IP gebundenen Netzwerkadapter angegeben werden.

Systemsteuerung → Software → Windows-Komponenten hinzufügen/entfernen → Komponenten → Netzwerkdienste → Details → Unterkomponenten von „Netzwerkdienste“ → DHCP-Protokoll (Dynamic Host Configuration Protocol) aktivieren → OK → Weiter

Autorisieren des DHCP-Dienstes:

Bevor ein DHCP-Server Leases an DHCP-Clients ausgeben kann, muss er dafür autorisiert werden, um zu verhindern, dass nicht autorisierte DHCP-Server den Clients potenziell ungültige IP-Adressen anbieten.

Anmerkung:
Nur DHCP-Server unter Windows 2000 Server überprüfen die Autorisierung. Andere – auch nicht autorisierte - DHCP-Server werden weiterhin ordnungsgemäß ausgeführt.

Um eine ordnungsgemäße DHCP-Autorisierung zu gewährleisten, muss das Netzwerk so konfiguriert werden, dass es beim Starten des DHCP-Dienstes eine DHCP-Informationsmeldung (DHCPINFORM) an die lokale Broadcastadresse (255.255.255.255) sendet. Ist dies der Fall, so antworten andere DHCP-Server mit DHCP-Bestätigungsmeldungen (DHCPACK).

Autorisieren des DHCP-Dienstes:

Programme → Verwaltung → DHCP → mit rechter Maustaste auf DHCP → Autorisierte Server verwalten → Autorisieren → im Dialogfeld DHCP-Server autorisieren den Namen oder die IP-Adresse des DHCP-Servers eingeben → OK → Ja

Wichtig:
Um einen DCHP-Server zu autorisieren, muss man Mitglied der Gruppe Organisations-Admins sein!

Erstellen und Konfigurieren eines Bereichs

Um die dynamische IP-Adressierung zu aktivieren, muss ein Bereich von gültigen IP-Adressen eingegeben werden, die der DCHP-Server zum Ausgeben von Leases an Clientcomputern in einem bestimmten Teilnetz verwenden kann.
Ein Bereich wird mit Optionen konfiguriert, sodass der DHCP-Server mit einer IP-Adresslease zusätzliche Informationen – sog. Bereichsoptionen - bereitstellen kann.
Desweiteren kann ein Bereich auch so konfiguriert werden, dass der DHCP-Server einem bestimmten Computer (z.B. Printserver) immer die gleiche IP-Adresse bereitstellt (Clientreservierung).
Nachdem ein Bereich erstellt wurde, muss dieser erst aktiviert werden, damit dieser für Leasezuweisungen verfügbar ist.

Anmerkung:
Mit Hilfe des Befehls netsh kann DHCP von einer Eigabeaufforderung aus konfiguriert werden.

Ändern der Standardgültigkeitsdauer (8 Tage) einer Lease

- Wird die Gültigkeitsdauer einer Lease verringert, so erhalten Clients auch dann Leases, wenn nur wenige IP-Adressen zur Verfügung stehen – allerdings können Leases ablaufen, wenn ein DHCP-Server vorübergehend nicht verfügbar ist. Der Netzwerkverkehr wird durch diese Maßnahme erhöht!
- Wird die Gültigkeitsdauer der Lease erhöht, verringert sich der durch Leaserneuerungen verursachte Netzwerkverkehr. Die Clients behalten auch bei vorübergehender Nichtverfügbarkeit des DHCP-Servers ihre IP-Adressen, was allerdings zur Folge hat, dass bei nur wenig zur Verfügung stehenden IP-Adressen etliche Clientcomputer keine Lease erhalten.
- Bei einer unbegrenzten Gültigkeitsdauer der Lease stehen die IP-Adressen der aus dem Netzwerk entfernten Clientcomputern erst dann wieder für andere Clients zur Verfügung, wenn die Lease manuell entfernt wurde.

Konfigurieren eines Bereichs mit Optionen

Von DHCP unterstützte Bereichsoptionen enthalten:

- IP-Adresse eines Routers
  (Option **003 Router** mit der IP-Adresse eines Standardrouters [Standardgateway])
- IP-Adresse eines DNS-Servers
  (Option **006 DNS-Server** mit der IP-Adresse eines oder mehrerer DNS-Server)
- DNS-Domänenname
  (Option **015 DNS-Domänenname** mit dem richtigen DNS-Domänennamen)
- IP-Adresse eines WINS-Servers
  (Option **044 WINS/NBNS-Server** mit der IP-Adresse eines oder mehrerer WINS-Server)
- Namensaufläsungsart NetBIOS über TCP/IP
  (Option **046 WINS/NBT-Knotentyp** mit dem richtigen NetBIOS-Knotentyp [P,M,H-Knoten]. Die Namensauflösungsart bestimmt die Reihenfolge, in der ein Client NetBIOS-Namenserver und Broadcasts verwendet, um NetBIOS-Namen in IP-Adressen aufzulösen)

Programme → Verwaltung → DHCP → auf den Namen des zu konfigurierenden DHCP-Servers klicken → mit rechter Maustaste auf Bereichsoptionen → Optionen konfigurieren → Allgemein → im Dialogfeld Bereich-Optionen im Feld „Zur Verfügung stehende Optionen" das Kontrollkästchen der gewünschten Option aktivieren → im Feld Dateneingabe die entsprechenden Konfigurationsinformationen angeben

Bereichsoptionen können auf vier Ebenen konfiguriert werden:

- **Server**
  Optionen auf der Serverebene gelten für alle DHCP-Clients, die eine IP-Adresse vom DHCP-Server leasen
- **Bereich**
  Optionen auf der Bereichsebene haben Vorrang vor Optionen auf Serverebene und sind nur für Clients verfügbar, die eine Adresse aus diesem Bereich leasen
- **Klasse**
  Optionen auf der Klassenebene haben Vorrang vor Optionen auf Bereichs- oder Serverebene und sind nur für Clients verfügbar, die sich gegenüber dem DHCP-Server als Mitglied einer bestimmten Klasse identifizieren
- **Reservierter Client**
  Optionen auf dieser Ebene haben Vorrang vor Optionen anderer Ebenen und gelten nur für bestimmte vorher festgelegte Clients

Anmerkung:
Die auf dem Clientcomputer angegebenen TCP/IP-Eigenschaften haben Vorrang vor allen Informationen, die ein DHCP-Server bereitstellt.

Reservieren von IP-Adressen für Clientcomputer

Anmerkung:
Sind mehrere DHCP-Server in einem Netzwerk vorhanden, so muss auf allen die Clientreservierung vorgenommen werden, um zu verhindern, dass der Client verschiedene IP-Adressierungs-informationen erhält.

Programme → Verwaltung → DHCP → auf den Namen des zu konfigurierenden DHCP-Servers klicken → mit rechter Maustaste auf Reservierungen → Neue Reservierung → in den Feldern den Namen (wird der Hardwareadresse des Clients zugeordnet), die IP-Adresse, die MAC-Adresse und eine Beschreibung des zu reservierenden Clients eingeben → Unterstützte Typen → Hinzufügen → Beide

Anpassen der DHCP-Funktionalität

Durch das Erstellen von Optionsklassen kann ein DHCP-Server so angepasst werden, dass er entweder nur an einen bestimmten oder eine ganze Gruppe von Clientcomputern Konfigurationsinformationen ausgibt, was den Verwaltungsaufwand erheblich verringert.

Verwenden von Optionsklassen

Es werden zwei Typen von Optionsklassen unterstützt:

- **Herstellerdefinierte Klasse**
  Identifizieren den Herstellertyp und die Konfiguration des Betriebssystems eines DHCP-Clients (Eigenschaften nach Betriebssystem – z.B. Win95, WinNT...)
- **Benutzerdefinierte Klasse**
  Identifizieren einen DHCP-Client über den jeweiligen Typ (Eigenschaften nach Konfigurationsbedürfnissen - z.B.: DFÜ-Verbindung, Laptop...)

Konfigurieren von Clients für die Verwendung der Benutzerklasse:
Ausführen → ipconfig /setclassid [Klasse]
Ausführen → ipconfig /showclassid [Klasse]

Erstellen einer neuen Hersteller- oder Benutzerklasse:
Programme → Verwaltung → DHCP → mit rechter Maustaste auf DHCP-Server klicken → Herstellerklassen definieren → Benutzerklassen definieren → Hinzufügen → Kennungen eingeben

Werden zwei oder mehrere Bereiche miteinander kombiniert, sodass diese als einzelne Einheit verwaltet werden kann, werden sie zusammengeschlossen und als Bereichsgruppierung konfiguriert.

Ausgeben von Multicastadressen mit Hilfe von Multicastbereichen

Mit Hilfe eines Multicastbereichs kann an ausgewählten Computern in einem Netzwerk eine Multicastadresse (**von 224.0.0.0 bis 239.255.255.255**) ausgegeben werden. Wird DHCP verwendet, um Clientcomputer mit einer Multicastadresse zu konfigurieren, können diese Clients an gemeinschaftlichen Anwendungssitzungen teilnehmen. Normalerweise verwenden Audio- und Konferenzanwendungen (MS Windows Media) die Multicasttechnologie, um mehreren Computern von einem einzelnen Punkt aus gleichzeitig Informationen bereitzustellen.
Um die ordnungsgemäße Funktion von Multicasting sicherzustellen, müssen alle Router zwischen dem Server (sendet Pakete an die Multicastadresse) und den Clientcomputern (erhalten die Pakete) so konfiguriert sein, dass sie die Multicastadresse erkennen.

Programme → Verwaltung → DHCP → mit rechter Maustaste auf den Namen des zu konfigurierenden DHCP-Servers klicken → Neuer Multicastbereich → Multicastbereichs-Name eingeben → Weiter → IP-Adressbereich → Erste und letzte IP-Adresse eingeben → Weiter → Gültigkeitsdauer auswählen → Weiter → Ausschlüsse hinzufügen → alle ausgeschlossenen IP-Adressen angeben → Weiter → Leasdauer →Multicastbereich aktivieren → Ja → Weiter → Fertigstellen des Assistenten → Fertig stellen

Konfigurieren von DHCP in einem gerouteten Netzwerk

Router teilen große Netzwerkumgebungen in Teilnetze auf und sind so konfiguriert, dass sie Broadcastmeldungen nicht an andere Teilnetze weiterleiten.
Es gibt drei Möglichkeiten, die DHCP-Funktionaltät (welche ein broadcastbasierter Dienst ist) in einem geroutetem Netzwerk zu konfigurieren:

- **Mindestens ein DHCP-Server für jedes Teilnetz**
  Nachteil: hohe Kosten und Verwaltungsaufwand;
- **Konfigurieren eines RFC 1542-kompatiblen Routers zum Weiterleiten von DHCP-Meldungen zwischen Teilnetzen**
  Nachteil: Konfiguration kompliziert; DHCP-Kommunikation über mehrere Teilnetze ist langsam;
- **Konfigurieren eines DHCP-Relay-Agent in jedem Teilnetz zum Weiterleiten von DHCP-Meldungen zwischen Teilnetzen**
  Vorteil: einfache Konfiguration; Broadcasts werden auf das Teilnetz beschränkt, aus dem sie stammen; Bereitstellung von Fehlertoleranz; effizientes bereitstellen von IP-Adressen;

Unterrichtseinheit 3:

Implementieren der Namensauflösung mit Hilfe von DNS

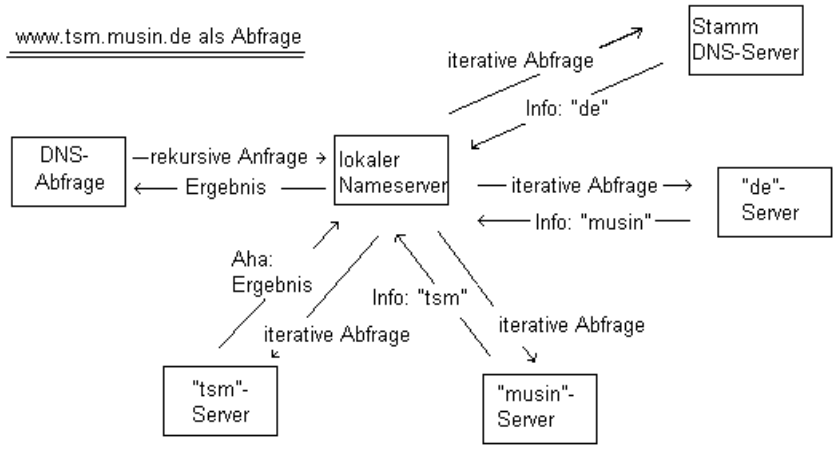
DNS (Domain Name System) ist ein integraler Bestandteil (verteilte Datenbank zum Übersetzen von Computernamen in IP-Adressen) der Client/Server-Kommunikation in IP-Netzwerken.

Übersicht über den DNS-Abfrageprozess:

Abfragetypen

Iterativ: Auflösung einer Ebene - Client sucht selbst (mit Hilfe von Serververweisen) nach der Antwort

Rekursiv: Server sucht selbst nach der Antwort des Clients und liefert das Ergebnis an diesen zurück



Der Lookuptype der Zone bestimmt die Aufgaben, die ein DNS-Server durchzuführen hat.

Lookuptypen:	gegeben	gesucht
Forward (standard)	DNS-Name	IP-Adresse
Reverse	IP-Adresse	DNS-Name

Installieren des DNS-Serverdienstes:

Konfigurieren von TCP/IP:
Es muss eine statische IP-Adresse (oder reservierte IP-Adresse im DHCP) im Dialogfeld **Eigenschaften von Internetprotokoll (TCP/IP)** auf dem Computer, auf welchem DNS-Serverdienst laufen soll, eintragen werden.

Domänennamen konfigurieren:
Netzwerkverbindung → Eigenschaften → Internetprotokoll (TCP/IP) → Eigenschaften → Erweitert → DNS → DNS-Serveradressen in Verwendungsreihenfolge überprüfen → Domänennamen im Feld „DNS-Suffix für diese Verbindung“ eingeben → OK

DNS-Serverdienst installieren:
Start → Systemsteuerung → Software → Windows-Komponenten hinzufügen/entfernen → Netzwerkdienste → Details → „DNS-Server (Domain Name System)“ aktivieren → OK → Weiter → Fertig stellen

Konfigurieren von Clientcomputern:

Der Clientcomputer kann auf folgende Arten für die Verwendung von DNS konfiguriert werden:

1. DNS-Serveradresse automatisch beziehen
2. Folgende DNS-Serveradressen verwenden / Bevorzugter DNS-Server

Anmerkung:
Windows 2000 verwendet den zweiten (oder alternativen) DNS-Server nur dann, wenn keine Verbindung zum primären DNS-Server hergestellt werden kann.

Windows 2000 kann Computernamen zu IP-Adressen sowohl über DHCP, als auch über lokale Hostdateien (die schnellere Antworten auf DNS-Abfragen bereitstellen und sich im Ordner **\Systemroot\System32\Driver\Etc** befinden) auflösen.

Erstellen von Zonen:

Eine Zone besteht aus einem zusammenhängenden Bereich des Domänennamespace, für den der DNS-Server über die Berechtigung zur Auflösung von DNS-Abfragen verfügt.

Wichtig:
Zum Erstellen von Zonen und Verwalten eines DNS-Servers, der nicht auf einem Domänencontroller ausgeführt wird, muss man Mitglied der Administratorengruppe für diesen Computer sein.
Zum Konfigurieren eines DNS-Servers, der auf einem Domänencontroller ausgeführt wird, muss man Mitglied der Gruppe DNS-Admins, Domänen-Admins oder Organisations-Admins sein.

Identifizieren von Zonentypen:

- Primär(Standard): Enthält eine Lese/-Schreibversion der Zonendatei
- Sekundär (Standard): Enthält eine schreibgeschützte Version der Zonen-Datei; Kopie einer vorhandenen Zone; dadurch kann die Arbeitslast der Namesauflösung auf mehrere DNS-Server verteilt werden
- Active Directory-integriert: Speichert die Zoneninformationen in Active Directory anstatt in einer Textdatei.

Zonendateien enthalten die notwendigen Informationen, auf die ein DNS-Server sich bezieht (für eine Zone), um zwei verschiedene Aufgaben durchzuführen: Auflösen von Hostnamen in IP-Adressen und umgekehrt

Die Domäne **in-addr.arpa** (für Reverse-Lookupzonen) stellt eine besondere DNS-Domäne der obersten Ebene dar, die für die Zuordnung von IP-Adressen in DNS-Hostnamen reserviert ist. Zum Erstellen des entgegengesetzten Namespace werden untergeordnete Domänen in der Domäne **in-addr.arpa** gebildet, indem die entgegengesetzte Reihenfolge der Zahlen in der dezimalen, durch Punkte unterteilten Notation von IP-Adressen verwendet wird.

Konfigurieren von Standardzonen:

Man kann einen oder mehrere DNS-Server so konfigurieren, dass eine beliebige Kombination von primären und sekundären Standardzonen gehostet werden kann.
Allerdings muss erst eine primäre Standardzone erstellt werden, bevor eine sekundäre Standardzone erstellt werden kann.
Wird eine sekundäre Standardzone hinzugefügt, so muss ein Master-DNS-Server bestimmt werden, von dem Zoneninformationen erhalten werden können.

Zonenübertragungsvorgang:

Die Zonendateien sollten auf mehreren DNS-Servern verfügbar sein, um bei der Auflösung von Namensabfragen Verfügbarkeit und Fehlertoleranz zu bieten.

Zonenübertragung

Die Zonenübertragung ist der Vorgang des Replizierens einer Zonendatei auf einem anderen DNS-Server. Bei diesem Vorgang werden die Änderungen an der Zone von einem Masterserver auf die sekundären Server kopiert.

Inkrementelle Zonenübertragung

Wird durch inkrementelle Zonenübertragung (IXFR) aktualisiert, werden nur die Änderungen an der Zonendatei, nicht die gesamte Zonendatei repliziert.

Bedingungen für den Start eines Zonenübertragungsvorgang:

- Masterserver sendet eine Benachrichtigung über die Änderung einer Zone an einen oder mehrere sekundäre Server
- Jeder sekundäre Server fragt einen Masterserver regelmäßig nach Änderungen an der Zonendatei ab. Dies geschieht, wenn der DNS-Serverdienst gestartet wird, oder wenn das Aktualisierungsintervall auf dem sekundären Server abläuft.

Konfigurieren von Zonenübertragungen

Die Häufigkeit und den Zeitpunkt der Zonenübertragungen kann gesteuert werden, indem man den SOA-Ressourceneintrag (Start of Authority, Autoritätsursprung) ändert.

Ändern des SOA-Ressourceneintrags

Zum Ändern des SOA-Ressourceneintraqgs auf der Registerkarte **Autoritätsursprung (SOA)** im Dialogfeld Eigenschaften sind folgende **Eigenschaften** vertreten:

Seriennummer	Diese verfolgt Aktualisierungen der Zonendatei. Bei jeder Änderung der Zonendatenbank wird die Seriennummer erhöht.
Primärer Server	Gibt den FQDN des primären Servers an
Verantwortliche Person	(wird mit Nslookup gesucht)
Aktualisierungsintervall	Steuert die Häufigkeit, mit der ein sekundärer Server seinen Masterserver nach neuen Daten abfragt. Wenn sich DNS-Daten permanent ändern, muss der Wert verringert werden, um sicherzustellen, dass die DNS-Daten rechtzeitig aktualisiert werden. (evtl. höherer Netzwerkverkehr)
Wiederholungsintervall	Steuert die Häufigkeit, mit der ein sekundärer Server versucht, seine Zonendatei zu aktualisieren. Bei einem sekundären Server, der keinen Kontakt zu seinem Masterserver herstellen kann, bestimmt das Wiederholungsintervall, wie lange der sekundäre Server wartet, bis er einen erneuten Versuch unternimmt, den Kontakt zu diesem herzustellen.
Läuft ab nach	Steuert die Zeitspanne, in der ein sekundärer Server seine aktuellen Zonendaten zum Beantworten von Abfragen verwendet, wenn er auf Grund von Netzwerkproblemen keinen Kontakt zu seinem Masterserver herstellen kann.

Minimum TTL	Gibt das TTL-Intervall (Time to live) oder die minimale Zeitdauer an, für die ein Server Informationen für eine Zone zwischenspeichern kann.
TTL für diesen Eintrag	Gibt die TTL des SOA-Ressourceneintrags an

Konfigurieren von Zonenübertragungssicherheit

Es können die zum Empfangen von Zonenübertragungen berechtigten Server für die Zone festgelegt werden, indem die folgenden Optionen auf der Registerkarte **Zonenübertragungen** des Dialogfeldes **Eigenschaften** für die Zone konfiguriert werden:

An jeden Server	Replizieren der Zoneninformation zu einem beliebigen Server
Nur an Server, die der Registerkarte „Namensserver“ aufgeführt sind	Die Registerkarte Namenserver enthält eine Liste der Server, die sich in derselben Domäne befinden wie die Zone
Nur an folgende Server	Replizieren der Zoneninformation zu einem durch die IP-Adresse festgelegten Server, welcher sich auch in anderen Domänen befinden kann

Konfigurieren der Benachrichtigung

Auf der Registerkarte **Namensserver** sollten die Master-DNS-Server so konfiguriert werden, dass Zonenübertragungen nur an designierten DNS-Server möglich sind.

Erstellen einer untergeordneten Domäne in einer vorhandenen Zone

Eine untergeordnete Domäne (wird erstellt, um eine Zone besser zu organisieren und um den Namespace eine Struktur zu verleihen) ist eine DNS-Domäne, die sich in der hierarchischen DNS-Struktur direkt unter einer anderen Domäne (übergeordnete Domäne) befindet.
Zum Erstellen einer untergeordneten Domäne wird die DNS-Konsole geöffnet und der Ordner Forward-Lookupzonen oder Reverse-Lookupzonen von der übergeordneten Domäne aus erweitert und anschließend auf Neue Domäne geklickt.
Die Zuständigkeiten für eine untergeordnete Domäne an einen DNS-Server, der diesen Bereich des DNS-Namespace verwalten soll, kann delegiert werden.
Zum Delegieren der Zuständigkeit für eine untergeordnete Domäne wird die DNS-Konsole geöffnet und der Ordner Forward-Lookupzonen oder Reverse-Lookupzonen von der übergeordneten Domäne aus erweitert und anschließend auf Neue Delegierung geklickt.

Konfigurieren von Active Directory-integrierten Zonen:

Active Directory-integrierte Zonen bieten folgende Vorteile:

Kein Einzelausfall	Änderungen, die durch das Protokoll für die dynamische Aktualisierung durchgeführt wurden, werden für alle Server vorgenommen
Fehlertoleranz	Jeder Domänencontroller verwaltet die Zoneninformationen
Einzelne Replikationstopologie	Replikation muss für DNS und Active Directory nicht separat konfiguriert werden
Sichere dynamische Aktualisierungen	Es können Berechtigungen für Zonen und Einträge in Zonen eingerichtet werden

Umwandeln von vorhandenen Standardzonen

Um eine vorhandene Standardzone in eine Active Directory-integrierte Zone umzuwandeln, muss der Server, der den DNS-Serverdienst ausführt, als Domänencontroller konfiguriert sein.
Wird eine Zone in Active Directory gespeichert, so wird die Zonendatei zuerst in Active Directory kopiert und anschließend auf dem primären Server (DNS-Server) für die Zone gelöscht.

Migrieren von Zonen zum Windows 2000 DNS-Serverdienst:

Der Installationsvorgang des DNS-Serverdienstes erstellt den Ordner ***Systemroot\System32\Dns***, welcher die DNS-Datenbankdateien enthält.

Dateityp	Beschreibung
domäne.dns	Forward-Lookupdatei
z.y.x.w.in-addr.arpa.dns	Reverse-Lookupdatei
Cache.dns	Die Cachedatei, die die erforderlichen Hostinformationen für das Auflösen von Namen außerhalb autorisierender Domänen enthält. Sie Enthält Einträge für alle Server, die die Stammzone im Internet hosten
Boot	Diese Datei ist optional, da die Starteinstellungen in der Registrierung gespeichert werden.

Umbenennen von Zonendateien

BIND-Zonendateien auf UNIX-basierten DNS-Servern müssen unter Windows 2000 kopiert (in den Ordner, der vom DNS-Serverdienst verwendet wird) und umbenannt werden:

Dateityp	UNIX-Dateiname	W2K-Dateiname
Startdatei	**named.boot**	**Boot**
Forward-Lookupzonendatei	**db**.*domäne*	*domäne*.**dns**
Reverse-Lookupzonendatei	**Db**.*w.x.y*	*y.x.w.***in-addr.arpa.dns**

Anmerkung:
Die Startdatei ist ein Teil der BIND (Berkeley Internet Name Domain)-spezifischen Implementierung von DNS. Wird eine Systemumstellung eines DNS-Servers (der BIND ausführt) ausgeführt, erlaubt das Kopieren der Startdatei eine einfache Migration der vorhandenen Konfiguration.

Konfigurieren von DNS für die interne Verwendung

Eine Stammzone wird auf einem DNS-Server konfiguriert, wenn

- das Intranet nicht mit dem Internet verbunden ist
- ein Proxyserver verwendet wird, um auf das Internet zuzugreifen

Wichtig:
*Damit der DNS-Server Lookups im Internet durchführen kann, muss sichergestellt sein, dass auf dem Server keine Stammzone konfiguriert ist und die Registrierkarte **Hinweise auf das Stammverzeichnis** im Dialogfeld **Eigenschaften** des Servers eine Liste der Server enthält, die für die Stammzone des Internet autorisierend sind.*

Integrieren von DNS und DHCP

Standardmäßig können Windows 2000-basierte Clients DNS mit ihren Informationen über die Zuordnung von Namen zu IP-Adressen immer dann aktualisieren, wenn ein DHCP-Server ihnen eine IP-Adresse zuweist.

Protokoll für die dynamische Aktualisierung

Windows2000-basierte Computer, die mit einer statischen IP-Adresse konfiguriert sind, sind zudem standardmäßig so konfiguriert, dass sie auf dem DNS-Server dynamisch Aktualisierungen (der Client aktualisiert sowohl die Forward- als auch die Reverse-Lookupeinträge) durchführen.

Vorgang der dynamischen Aktualisierung:

1. Der Client initiiert eine DCHP-Anforderungsmeldung (umfasst den FQDN) an den DCHP-Server, in der er eine IP-Adresse anfordert.
2. Der DHCP-Server gibt eine DHCP-Bestätigungsmeldung an den Client zurück, in der ein IP-Adresslease erteilt wird.

3. Ein DHCP-Client sendet eine DNS-Aktualisierungsanforderung für seinen eigenen Forward-Lookupeintrag, den Ressourceneintrag A, an den DNS-Server.
4. Der DHCP-Server sendet Aktualisierungen für den Reverse-Lookupeintrag des DHCP-Clients, den Ressourceneintrag PTR (Zeiger). Der DHCP-Server verwendet den FQDN, den er bei der Ausführung des ersten Schrittes erhalten hat, um diese Operation durchzuführen.

Clients, die frühere Versionen von Windows ausführen, unterstützen keine dynamischen Aktualisierungen und sind auch nicht in der Lage, dynamisch mit dem DNS-Server zusammenzuarbeiten. Daher muss man den DHCP-Server so konfigurieren, dass er für diese DNS-Clients immer die Ressourceneinträgeeinträge A und PTR aktualisiert.

Konfigurieren des DNS-Servers für dynamische Aktualisierungen

Optionen im Dialogfeld Eigenschaften für die Zone, Reiter dynamische Aktualisierung

Option	Beschreibung
Nein	Deaktiviert dynamische Aktualisierungen für die Zone
Ja	Aktiviert dynamische Aktualisierung für die Zone
Nur gesicherte Aktualisierung	Aktiviert gesicherte dynamische Aktualisierungen von autorisierten Clientcomputer für eine Active Directory-integrierte Zone

Konfigurieren des DHCP-Servers für dynamische Aktualisierungen

1. öffnen des DHCP-Dialogfeldes **Eigenschaften** → Registerkarte **DNS**
2. aktivieren des Kontrollkästchens **DHCP-Clientinformationen in der DNS automatisch aktualisieren**
3. Forward-Lookups Auswahl-Einstellungen vornehmen
4. für frühere Windowsversionen muss das Kontrollkästchen **Aktualisierung für DNS-Clients, die dynamisch Aktualisieren nicht unterstützen, aktivieren** aktiviert werden

Konfigurieren W2000-basierter Clients für dynamische Aktualisierungen

Eigenschaftsdialogfeld für die Netzwerk- und DFÜ-Verbindungen öffnen → Internetprotokoll (TCP/IP) → Eigenschaften → Erweitert → DNS → ***Erweiterte TCP/IP-Einstellungen*** *aktivieren und* ***Adressen dieser Verbindung in DNS registrieren*** *anklicken → 3x OK*

Verwalten von DNS-Servern und Beheben von Problemen:

In Windows2000 sind verschiedene Dienstprogramme zum Überwachen von DNS-Servern sowie zur Fehlerbehebung integriert:

• MMC (Microsoft Management Console)	Überwachung von DNS-Server-Leistung
• Befehlszeilenprogramm Nslookup	Überprüfung von Ressourceneinträgen; Beheben von DNS-Problemen
• DNS-Serverprotokoll	Anzeigen mit Ereignisprotokoll

Verringen des Netzwerkverkehrs durch Verwenden von Servern nur für Zwischenspeicherungen

Server nur für Zwischenspeicherung führen die Namensauflösung im Auftrag von Clients durch und speichern dann die Ergebnisse. Sie sind nicht Zonenautorisierend konfiguriert und speichern daher keine primären oder sekundären Standardzonen. Auch erzeugen solche Server keinen Zonenübertagungsverkehr.

Anwendung: Wenn eine Remoteniederlassung für die Verbindung mit einem Hauptbüro nur über eine begrenzte Bandbreite verfügt.

Konfigurieren von Weiterleitungen

Verwaltung → DNS → mit rechter Maustaste auf den zu bearbeitenden Server klicken → Eigenschaften → Weiterleitung → Kontrollkästchen ***Weiterleitung aktivieren*** *→ IP-Adresse des Servers eingeben → Hinzufügen → OK*

Verwalten von DNS-Zonen

Ressourceneinträge enthalten Daten, die zum Konfigurieren eines DNS-Servers verwendet werden. Es können folgende Einträge enthalten sein:

- A (Adresse)
- NS (Nameserver)
- CNAME (kanonischer Name – Aliaseintrag)
- MX (Mail-Exchanger)
- SOA (Autoritätsursprung)
- PTR (Zeiger)
- SRV (Dienst)

Wird ein DNS-Server aus dem Netzwerk entfernt, so müssen die DNS-Konfigurationen folgendermaßen aktualisiert werden:

- Entfernen des Ressourceneintrages A für den Server
- Löschen des Servernamens aus den NS-Ressourceneinträgen
- Überarbeiten des Besitzerfeldes des SOA-Ressourceneintrages (ist für Active Directory-integrierte Zonen nicht erforderlich)
- Überprüfen, ob alle für die Delegierung zur Zone verwendeten Einträge nicht mehr auf den entfernten Server verweisen

Überwachen von DNS-Servern

Um Sicherzustellen, dass der DNS-Serverdienst einwandfrei arbeitet, sollte die Konfiguration zuerst einmal getestet werden.
Verwaltung → DNS → mit rechter Maustaste auf den zu bearbeitenden Server klicken → Eigenschaften → Überwachen → entweder „Einfache Abfrage“ (lokaler Test) oder „Rekursive Abfrage“ (DNS-Servertest) oder beide auswählen → Jetzt testen → OK

Um die Debugprotokollierung des DNS-Servers zu aktivieren muss folgendermaßen vorgegangen werden:
Verwaltung → DNS → mit rechter Maustaste auf den zu bearbeitenden Server klicken → Eigenschaften → Protokollierung
Standardmäßig zeichnet nun der DNS-Server sine Protokollinformationen in der Datei **\%Systemroot%\System32\Dns\Dns.log** auf.

Wichtig:
Da die Protokollierung in hohem Maße Ressourcen beansprucht, was sich auf die gesamte Serverleistung auswirken und Festplattenspeicher belegen kann, sollte diese nur zur Behebung von Problemen aktiviert werden.

Überprüfen von Ressourceneinträgen mit Nslookup

Die Korrektheit von Ressourceneinträgen kann mit NSLOOKUP (es muss ein PTR-Ressourceneintrag für den Server vorhanden sein) überprüft werden.
Dieses Modul besitzt zwei verschiedene Modi:

- Interaktiv (um mehrere Datensätze zu bearbeiten)
  Start mit **nslookup**; Verlassen mit **exit**
- Nicht interaktiv (um einen einzelnen Datensatz zu bearbeiten)

Syntax von NSLOOKUP: **nslookup** *[-option] [gesuchter_computer* | *- [server]]*

-option	Nslookup-Befehle (kann mit ? abgefragt werden)
-gesuchter_computer	gibt je nach Eingabe entweder die IP-Adresse oder den Hostnamen zurück; um einen Computer außerhalb der aktuellen DNS-Domäne zu suchen, muss ein Punkt an den Namen angehängt werden
-server	DNS-Server

Fehlerbehebung bei der Namensauflösung

Wird die Namensauflösung für Clientcomputer nicht erkannt, so muss **ipconfig/flushdns** eingegeben werden, um den Cache auf dem Client zu leeren.
Um den Client zur Aktualisierung seiner Registrierung zu zwingen muss **ipconfig/registerdns** an der Eingabeaufforderung eingegeben werden.
Fehlerbehebung bei der Zonenübertragung (siehe Kapitel3 / Seite61)

Unterrichtseinheit 4:

Implementieren der Namensauflösung mit Hilfe von WINS

Mit Hilfe von WINS werden NetBIOS-Computernamen (welche von Windows 98 und Windows NT – Clients noch vereinzelt verwendet werden) in IP-Adressen aufgelöst.

NetBIOS-Namensschema:

NetBIOS-Namen werden dynamisch registriert (Arten: Computername, Gruppen-name), sind 16 Byte lang (15 Zeichen für Computernamen + 1 Zeichen als Dienstkennung, z.B. Serverdienst für Freigaben mit der Dienstkennung: 0x20) und verfügen - im Gegensatz zu DNS Namen - nur über eine Namespace-Ebene, was bedeutet, dass der Name nur einmal im ganzen Netzwerk vergeben werden kann und somit eindeutig ist.

Namen bekanntgeben und ermitteln:

NetBT-Host (NetBIOS über TCP/IP) sendet eine Registrierungsanforderung ins Netzwerk:

- Name nicht verwendet → Host darf Namen im Netzwerk verwenden
- Name schon registriert → Initialisierungsfehler, Host darf im Netzwerk nicht kommunizieren

Eine Namensfreigabe tritt automatisch immer dann auf, wenn eine NetBIOS-Anwendung oder ein NetBIOS-Dienst ordnungsgemäß heruntergefahren (beendet) wurde.

NetBIOS-Namensauflösung:

Zuerst wird der NetBIOS-Name im eigenen Namenscache, welcher die zuletzt aufgelösten Namen enthält, gesucht. (Der Namenszwischenspeicher kann mit **nbtstat –c** angezeigt werden). Wird er dort nicht fündig, wird eine Anfrage bei einem NetBIOS-Namenserver (in Windows200 ist ein WINS-Server ein NetBIOS-Namenserver und kann mit LMHOSTS-Datei vorbelegt werden) gestartet. Als letzte Möglichkeit bietet sich ein lokaler Broadcast an, um mit dem entsprechenden Host Verbindung aufzunehmen (liefert dann die IP-Adresse).

Anmerkung:
Das Konfigurieren der NetBIOS-Namensauflösung für lokale Broadcasts sollte vermieden werden, da dies übermäßigen Netzwerkverkehr erzeugen könnte und die meisten Router diese nicht in andere Netzbereiche weiterleiten.

NetBIOS über TCP/IP-Namensauflösungsknoten:

Die unterschiedlichen Methoden, mit denen ein Computer einen NetBIOS-Namen in ein IP-Adresse auflösen kann, bezeichnet man als Knoten.

Der **Knotentyp** des Clients bestimmt die Suchstrategie:		Registry-Wert:
B:	sendet Broadcast zur Namensregistrierung- und Auflösung	1
P:	(Peer-to-Peer) muß WINS-Server kennen, da er nur diesen fragen kann	2
M:	(gemischt) Kombination aus B- und P-Knoten; arbeitet standardmäßig als B-Knoten;	4
H:	(hybrid) Kombination aus P- und B-Knoten; arbeitet standardmäßgi als P-Knoten;	8

Wird kein WINS-Server konfiguriert, verwendet das System standardmäßig B-Knoten. Bei mindestens einem WINS-Server wird standardmäßig der H-Knoten verwendet.

Knotenwert in der Registry:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\NodeType

LMHOSTS-Datei

Eine LMHOSTS-Datei ist eine lokale Textdatei, die Zuordnungsinformationen von NetBIOS-Namen zu IP-Adressen enthält und wird sequentiell in den lokalen Namenscache des NetBT- Hosts gelesen.
Wird eine solche Datei manuell angelegt, so muss diese mit dem Namen **LMHOSTS** (ohne Dateiendung) im Ordner **%SYSTEMROOT%\SYSTEM32\DRIVERS\ETC** abgespeichert werden. (Musterdatei: **LMHOSTS.SAM**)
Vorkonfigurierte Einträge aus der LMHOSTS-Datei können in den NetBIOS-Namenszwischenspeicher geladen werden, wenn die TCP/IP-Eigenschaften initialisiert werden.

Folgende vordefinierte Schlüsselwörter können in dieser Datei enthalten sein:

#PRE	diese Einträge werden bei TCP/IP automatisch geladen; dauerhafte Einträge im Namenzwischenspeicher
#DOM:*[Domänenname]*	zeigt an, dass der Computer ein Domänencontroller ist
#INCLUDE	lädt und sucht NetBIOS-Einträge (weitere Liste) in einer von der Standard-LMHOSTS-Datei getrennten Datei
#BEGIN_ALTERNATE **#END_ALTERNATE**	definiert eine redundante Liste von alternativen Speicher-orten für LMHOSTS-Dateien
#MH	fügt mehrere Einträge zu einem mehrfach vernetzten Computer hinzu

Der typische Zeileneintrag lautet: **IP-Adresse NetBIOS-Name #Option**

Anmerkung:
Der wichtigste Server sollte zuerst eingetragen werden (der Domänencontroller wird mit #DOM gekennzeichnet); die #PRE–Einträge werden zuletzt eingetragen und bleiben dauerhaft im Namenscache erhalten.

Eine LMHOSTS-Datei wird folgendermaßen deaktiviert:
Eigenschaftsdialogfeld für die Netzwerkverbindung öffnen → Internetprotokoll (TCP/IP) → Eigenschaften → Erweitert → WINS → Häkchen von LMHOSTS-Abfrage aktivieren wegnehmen → OK

WINS-Server Funktion

Mit WINS wird der Broadcastverkehr erheblich verringert. Jedes Mal wenn ein WINS-Client gestartet wird, registriert dieser Client seinen NetBIOS-Namen und seine IP-Adresse bei einem konfigurierten WINS-Server (d.h. er muss die IP-Adresse mindestens eines WINS-Servers in seinen TCP/IP- Einstellungen konfiguriert haben).
Wenn dieser Client einen Befehl zur Kommunikation mit einem anderen Host initiiert, sendet er eine Namensabfrageanforderung direkt an den primären WINS-Server (für Arbeitsstations-, Server-, Nachrichtendienst, Arbeitsgruppe oder Domäne Namen des derzeit angemeldeten Benutzers), welcher nun in seiner Datenbank nach einer Registrierung von diesem Host sucht. Falls er eine aktive Registrierung findet und der Name noch nicht belegt ist, trägt er die Informationen in seine (dynamische) Datenbank ein und gibt WINS die IP-Adresse des Zielhosts an den WINS-Client mit der zugewiesenen Gültigkeitsdauer (TTL) zurück. Da diese Namensregistrierung nur temporär sind, müssen die Clients somit periodisch (Gültigkeit 6 Tage, nach 50% Aktualisierungsanforderung) ihre Registrierung erneuern.
Ist der Name bereits belegt, so prüft der WINS-Server, ob der andere Client mit dem selbem Namen noch aktiv ist und initialisiert ggf. eine Fehlermeldung mit einer Netzwerkdeaktivierung beim anfragenden Host .
Wird der primäre WINS-Server nicht gefunden, so geht die Anfrage an die weiteren WINS-Server in der Liste über; meldet sich allerdings kein WINS-Server, so bleibt dem Client nur noch die Anfrage über eine Broadcastmeldung übrig.

Wenn ein WINS-Client keinen Namen mehr benötigt (heruntergefahren wird), sendet er eine Meldung an den WINS-Server, damit dieser den Eintrag in seiner Datenbank löschen kann; dessen Bestätigung wird mit TTL=0 an den Client zurückgegeben
Wurden die Clientdienste *nicht* ordnungsgemäß beendet, so behält der WINS-Server zunächst den veralteten Eintrag und gibt fehlerhafte Auskunft (Zeitüberschreitung beim Netzwerkzugriff)

Installation und Anforderungen von WINS

Folgende Clients sind für die Installation von WINS Voraussetzung:

- Windows 2000
- Windows NT ab Version 3.5
- Windows 9x
- Windows for Workgroups 3.11 mit TPC/IP-32
- MS-DOS ab Netzwerk-Client 3.0
- LanManager ab 2.2c
- UNIX und Macintosh

Um einen WINS-Server konfigurieren zu können muss WINS darauf installiert sein und dieser über eine statische IP-Adresse, eine Subnetzmaske und ein Standardgateway verfügen. Auch die WINS-Clients müssen über die statische IP-Adresse eines WINS-Servers (normalerweise zwei Server) verfügen, wobei die Konfiguration entweder manuell über *TCP/IP-Eigenschaften → WINS → Serveradresse(n)* oder automatisch über *DHCP-Optionen 044 WINS-Server und 046 WINS/NBT-Knotentyp* eingetragen werden können (der manuelle Eintrag hat Vorrang!).

WINS wird folgendermaßen installiert:
Start → Einstellungen → Systemsteuerung → Software → Windows-Komponenten hinzufügen/entfernen → Komponenten → Netzwerkdienste → Details

Um Informationen zur Namensauflösung für NetBIOS-basierte Computer, die keine WINS-Clients sind, zur WINS-Serverdatenbank hinzuzufügen können statische Zuordnungen auf einem WINS-Server konfiguriert werden.
Start → Programme → Verwaltung → WINS → rechte Maustaste auf „Aktive Registrierungen" → Neue statische Zuordnung → Computername eingeben → Type eintragen → Eindeutig → IP-Adresse eingeben → OK

WINS und DNS

In einem gemischten DNS-Netzwerk (ab WIN NT 4.x und WIN 2000) kommuniziert der Client nur mit dem DNS-Server, auch wenn dieser die Clientanforderung an einen WINS-Server weiterleitet.
Nur DNS-Server unter Windows NT 4.0 und Windows 2000 sollten autorisierend für eine DNS-Zone sein, da nur diese die von Windows 2000 nicht standardmäßigen DNS-Ressourceneinträge und WINS-Lookup verwerten können.

Anmerkung:
*Wenn Windows-basierte Server zusammen mit anderen DNS-Servern als Host für eine Zone verwendet werden, sollten für alle primären Zonen, in denen der WINS-Lookup-Eintrag verwendet wird, das Kontrollkästchen „**Diesen Eintrag nicht replizieren"** aktiviert werden.*

Muss eine gesonderte Zone für WINS-Lookup erstellt werden, sollte folgendermaßen vorgegangen werden:

- erstellen einer DNS-Zone ohne Host-Einträge und aktivieren für WINS-Lookup
- jedem Clientcomputer die WINS-Zone hinzufügen (*Erweiterte TCP/IP-Einstellungen → DNS → Diese DNS-Suffixe anhängen*)

Wenn ein Client einen in WINS registrierten Computernamen anfordert, müssen folgende Schritte durchgeführt werden:

1. DNS-Client fragt seinen bevorzugten DNS-Server
2. DNS-Server fragt den für die Zone autorisierenden DNS-Server
3. autorisierenden DNS-Server leitet die Anforderung an WINS-Server weiter
4. WINS-Server löst den Namen auf und gibt die IP-Adresse dem autorisierenden DNS-Server zurück
5. autorisierter DNS-Server gibt die IP-Adresse an den bevorzugten DNS-Server zurück
6. DNS-Server gibt die IP-Adressinformation an den Client zurück

Konfigurieren einer DNS-Zone für das Verwenden von WINS-Lookup:
Start → Programme → Verwaltung → DNS → Forward-Lookupzonen → mit rechter Maustaste auf Eigenschaften → das Kontrollkästchen „WINS-Forward-Lookup verwenden" aktivieren → „Diesen Eintrag nicht replizieren" aktivieren → IP-Adresse des WINS-Servers eingeben → Hinzufügen → OK

WINS-Proxy

Ein WINS-Proxy ist ein Computer, der zum Weiterleiten von Broadcastanforderungen zur Namensauflösung an einen WINS-Server zum Zweck der Namensauflösung konfiguriert wurde (erforderlich, wenn Clients nicht für WINS konfiguriert sind: B-Knoten).
Der WINS-Proxy verarbeitet die NetBIOS-Broadcasts im Subnet zuerst mit dem eigenen NetBIOS-Namenscache. Wird er dort nicht fündig, so leitet er die Namensauflösungsanforderung an einen WINS-Server weiter, der im anderen Netzwerksegment steht.

Anmerkung:
In einem Teilnetz mit Nicht-WINS-Clients sollte man mindestens einen, aber nicht mehr als zwei WINS-Proxys konfigurieren, da es sonst zu übermäßigem Netzwerkverkehr und übermäßiger Arbeitsauslastung führen kann!

Um einen Computer als WINS-Proxy zu konfigurieren, muss in der Registry unter:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters
der Eintrag: **EnableProxy** auf **1** gesetzt werden.

WINS-Replikation

Obwohl ein einzelner WINS-Server mehr als 5000 Clients mit normaler Arbeitsauslastung unterstützen kann, sollte immer ein zweiter WINS-Server in einem Netzwerk installiert werden, um eine mögliche Fehlertoleranz für die NetBIOS-Namensauflösung bereitzustellen.
Durch die Replikation (nur Änderungen in ihrer Datenbank werden weitergegeben) von WINS-Datenbanken wird sichergestellt, dass ein Name, der bei einem WINS-Server registriert ist, auf allen anderen WINS-Server im Netzwerk repliziert wird.

Überprüfen von Replikationspartnern

Damit eine Replikation durchgeführt werden kann, muss für jeden WINS-Server mindestens einer der folgenden Replikationspartner konfiguriert werden.

PULL-Partner:

- fordert ein Replikat von neuen Datenbankeinträgen in bestimmten Intervallen (vom PUSH-Partnern) an
- für langsame Verbindungen

PUSH-Partner:

- informiert seine Replikationspartner (PULL-Partner), wenn die Anzahl von Änderungen einen bestimmten Schwellwert in der Datenbank übersteigt
- für schnelle Verbindungen

Wichtig:
Standardmäßig wird zwischen zwei WINS-Servern nur dann eine WINS-Replikation durchgeführt, wenn beide Server dafür konfiguriert wurden und einer der PULL- und der andere der PUSH-Partner ist. Primäre und sekundäre WINS-Server sollten gegenseitig als PUSH/PULL-Partner konfiguriert werden.

Hinzufügen eines Replikationspartners:
Start → Programme → Verwaltung → WINS → mit rechter Maustaste auf Replikationspartner → Neuer Replikationspartner → Computernamen und IP-Adresse des Partners eingeben → OK

Optionen für die WINS-Replikation:

- Replikationspartnertyp
- Bestehende Verbindung für Replikation verwenden
- Startzeit und Replikationsintervall
- Anzahl der Änderungen in der Versionskennung vor der Replikation
  (Mit dem Wert 0 deaktiviert die PUSH-Replikationen und kann dadurch die Replikationsanforderung auf die PULL- Partner verlagern)

WINS-Datenbank

Die WINS-Datenbank ist gespeichert in **%WINDIR%\SYSTEM32\WINS\WINS.MDB**
Der "Besitzer" eines Eintrags ist (bei Replikation) derjenige WINS-Server, der den Eintrag in seiner Datenbank, welche standardmäßig automatisch komprimiert wird, gespeichert hat.
Falls es notwendig ist, eine Datenbank manuell zu komprimieren, müssen folgende Schritte ausgeführt werden:

- WINS-Dienst beenden
- **Jetpack.exe** (aus dem Verzeichnis **%SystemRoot%\System32\Wins**) mit folgender Syntax ausführen:
  JETPACK WINS.MDB *temporärer_name*.**MDB** ausführen
- WINS-Dienst wieder starten

Um WINS so zu konfigurieren, dass zu löschende Einträge in automatischen Intervallen aus der Datenbank entfernt werden ist folgendes notwendig:
Start → Programme → Verwaltung → WINS → mit rechter Maustaste auf Servernamen → Eigenschaften → Intervalle → eingeben von ***Erneuerungsintervall*** *(Standard 6 Tage,* ***Alterungsintervall*** *(Standard 4 Tage),* ***Alterungszeitüberschreitung*** *und* ***Überprüfungsintervall****) → OK*

WINS-Server können die Verarbeitung von umfangreichen Serverlasten (Burstserverlasten) unterstützen. Mit der Option „**Burstverarbeitung aktivieren“** (in den erweiterten Eigenschaften von WINS-Server) wird ein WINS-Server so konfiguriert, dass er auch dann auf Clientanforderungen antwortet, wenn die Anzahl von diesen vorübergehend ansteigt. Wenn Burstverarbeitung aktiviert ist (dadurch werden Fehler auf WINS-Clients vermieden) und hoher Netzwerkverkehr vorherrscht, gibt der WINS-Server kurze Leases an Clients aus und zeichnet diese nicht in der Datenbank auf.

Sichern und Wiederherstellen der WINS-Datenbank

Um die Datenbank **automatisch** sichern zu lassen, muss ein Sichungsverzeichniss angegeben werden:
Start → Programme → Verwaltung → WINS → mit rechter Maustaste auf Servernamen → Eigenschaften → Allgemein → Standardpfad für die Sicherungskopie eingeben (\ für Sicherung auf der Systempartition – der Pfad muss lokal sein und darf sich nicht im Netzwerk befinden) → Kontrollkästchen ***„Datenbank beim Herunterfahren des Servers sichern“*** *aktivieren → OK*

Wenn WINS die Serverdatenbank alle 3 Stunden sichert, wird unter dem angegebenen Sicherungsordner (standardmäßig der Stammordner auf der Systempartition) ein Ordner namens **/Wins_bak/New** erstellt, indem die aktuellen Sicherungen der WINS-Datenbank (**WINS.mdb**) gespeichert werden.

Um die Datenbank **manuell** zu sichern, muss folgendermaßen vorgegangen werden:
Start → Programme → Verwaltung → WINS → mit rechter Maustaste auf Servernamen → Datenbank sichern → OK

Wichtig:
WINS speichert Informationen zur Konfiguration und zu Replikationspartnern in der Registrierung. Daher sollte immer eine aktuelle Sicherung der Registry verfügbar sein, um im Falle eines Fehlers die WINS-Datenbank wieder herstellen zu können!

Um die WINS-Datenbank wiederherzustellen sind folgende Schritte zu beachten:

- WINS-Dienst beenden (kann bis zu einigen Minuten dauern)
- alle Dateien im WINS-Verzeichnis löschen
- im WINS-Manager "aktualisieren", dann beim WINS-Server → "Datenbank wiederherstellen" aufrufen
- bei "Ordner suchen" den Pfad der Sicherungskopie angeben (der zur Wiederherstellung verwendete Sicherungspfad muss mit dem ursprünglichen als Standardpfad für die Sicherung angegebenen Pfad übereinstimmen)

Weitere Aktionen: Einträge entfernen, Datenbankkonsistenz prüfen (Netzlast, zeitgesteuert ausführen!)

Unterrichtseinheit 5:

Konfigurieren der Netzwerksicherheit mit Hilfe von PKI (Public Key Infrastructure)

Verschlüsselung mit öffentlichen Schlüsseln ist eine bedeutende Technologie für E-Commerce, Intranets, Extranets und Webanwendungen

Verschlüsselung mit öffentlichen Schlüsseln:

Die Verschlüsselung mit öffentlichen Schlüsseln stellt Datensicherheit bereit. Bei der Verwendung von öffentlichen Schlüsseln werden zwei Schlüssel verwendet, die einen mathematischen Bezug zueinander haben.

- Privater Schlüssel (bleibt geheim)
- Öffentlicher Schlüssel (wird an alle potenziellen Korrespondenten ausgegeben)

Das Ziel einer Verschlüsselung ist es, Daten auf eine Weise zu verändern dass sie nur vom Empfänger gelesen werden können, für denn sie bestimmt ist. Nur der Empfänger verfügt über den zugehörigen privaten Schlüssel.

Authentifizierung mit öffentlichen Schlüsseln:

Wie bei der Verschlüsselung mit öffentlichen Schlüsseln wird auch bei der Authentifizierung mit öffentlichen Schlüsseln ein Schlüsselpaar verwendet. Es wird eine Digitale Signatur erstellt. Bei einer digitalen Signatur sind die Funktionen des privaten und des öffentliches Schlüssels vertauscht.

Digitale Signatur

Eine digitale Signatur ist ein Mittel für den Absender einer Nachricht, einer Datei oder anderer codierter Informationen mit seiner Identität zu verbinden.

- Nur eine Person die über den privaten Schlüssel verfügt, kann die digitale Signatur erstellt haben.
- Jede Person mit Zugriff auf den öffentlichen Schlüssel kann die digitale Signatur überprüfen.

Zertifizierung

Zertifikate sind signierte Dokumente, mit denen öffentliche Schlüssel zu anderen Informationen, wie einem Namen oder einer E-Mail-Adresse, zugeordnet werden.
Die Signatur einer Zertifizierungsstelle (kann eine externe Ausstellungsfirma oder auch eine interne Abteilung einer Firma sein) garantiert, dass der öffentliche Schlüssel tatsächlich zu der Person oder Organisation gehört, die ihn angibt.

Nur *Stammzertifizierungsstellen* sind vertrauenswürdig, dagegen sind die *untergeordnete Zertifizierungsstellen* nicht vertrauenswürdig. Obwohl Stammzertifizierungsstellen verwendet werden können, um Zertifikate für Endbenutzer für Aufgaben wie das Senden von sicheren E-Mails auszustellen, werden sie in den meisten Organisationen nur verwendet, um Zertifikate für andere Zertifizierungsstellen, die sogenannten untergeordnete Zertifizierungsstellen, auszustellen.

Primäre Windows 2000 PKI-Komponenten

- *Zertifikatsdienste* (Hauptbetriebssystemdienst) ermöglichen als ihre eigenen Zertifizierungsstellen zu agieren und digitale Zertifikate auszustellen und zu verwalten
- *Active Directory* (Veröffentlichungsdienst) macht Zertifikate und Zertifikationssperrlisten innerhalb einer Organisation öffentlich verfügbar.

Es werden verschiedene Arten von Sicherheitsprotokollen verwendet
SSL (Secure Sockets Layer)
IPSec (Internet Protocol Security)
TSL (Transport Layer Security)

Bereitstellen der Zertifikatsdienste

In Windows 2000 Server gibt es zwei Typen von Zertifizierungsstellen: Organisationszertifizierungsstelle und eigene Zertifizierungsstellen.
Eine Organisationszertifizierungsstelle erfordert, dass alle Benutzer und Computer, die Zertifikate anfordern, über ein Konto in Active Directory verfügen.
Eine eigenständige Zertifizierungsstelle erfordert kein Active Directory.

Organisationszertifizierungsstelle

Eine **Organisationszertifizierungsstelle** (für Zertifikate nur für Benutzer und Computer innerhalb der Organisation) ist die Zertifizierungsstelle auf der höchsten Ebene in einer Zertifikatshierarchie. Für eine Organisationszertifizierungsstelle sind folgende Einstellungen nötig: Active Directory (um die Identität und die Sicherheitsberechtigungen des Anforderers zu bestimmen), DNS-Server-Dienste, Administratorberechtigung auf dem DNS-, Active Directory- und Zertifizierungsstellenserver, man muss Mitglied der Gruppe Organisations-Admins sein.

Wichtig:
Um Zertifikate in Active Directory zu veröffentlichen, muss der Server, auf dem die Zertifizierungsstelle installiert ist, ein Mitglied der Gruppe Zertifikatherausgeber sein.

Eine **untergeordnete Organisationszertifizierungsstelle** muss über eine übergeordnete Zertifizierungsstelle verfügen.
Eine **eigenständige Stammzertifizierungsstelle** (höchste Ebene in einer Zertifikatshierarchie) kann vom Netzwerk getrennt und in einem sicheren Bereich platziert werden. Für Einheiten außerhalb einer Organisation sollte eine eigenständige Stammzertifizierungsstelle installiert werden.
Eine Stammzertifizierungsstelle stellt üblicherweise nur Zertifikate für untergeordnete Zertifizierungsstellen aus. Für die Installation einer eigenen Zertifizierungsstelle benötigt man Administratorberechtigungen auf dem lokalen Server.
Eine eigenständige untergeordnete Zertifizierungsstelle fungiert als Einzelzertifikatsserver innerhalb einer Zertifizierungsstellenvertrauenshierarchie. Für die Installation dieser benötig man folgende Einstellungen: eine übergeordnete Zertifizierungsstelle, Administratorberechtigung auf dem lokalen Server.

Installieren der Zertifikatsdienste

Ein Computer kann nicht umbenannt oder mit einer Domäne verbunden, bzw. entfernt werden, nachdem die Zertifikatsdienste installiert wurden. Um eine dieser Aktionen durchzuführen, müssen die Zertifikatsdienste zunächst vom Computer entfernt werden.

Installieren der Zertifikatsdienste:

- Auswählen eines Zertifizierungsstellentyps
- Festlegen erweiterter Optionen
  Es gibt folgende Kryptografieeinstellungen: **Kryptografiedienstanbieter**, **Hashalgorithmus**, **Schlüssellänge** (Standard sind 512 Bit; für Stammzertifizierungsstellen sollten mindestens 2048 Bit verwendet werden) und **vorhandene Schlüssel verwenden**
- Eingeben von Identifikationsinformationen
- Angeben von Speicherorten für die Datenbank und die Protokolldateien
  Standardverzeichnis für Zertifikate „**%SystemRoot%\System32\CertLog**“

Erstellen einer untergeordneten Zertifizierungsstelle

Eine untergeordnete Zertifizierungsstelle muss einer Zertifizierungsstelle zugeordnet sein, welche die Zertifikatsanforderungen bearbeitet.

- Erhalten eines Zertifikats für eine untergeordneten Zertifizierungsstelle
  Anforderung eines Zertifikatsstellenzertifikats ⇒ Anforderung direkt an eine im Netzwerk vorhandene Zertifizierungsstelle senden ⇒ Computername ⇒ Übgeordnete Stelle
- Installieren eines Zertifikats aus einer Datei
  Verwaltung ⇒ Zertifizierungsstelle ⇒ Vorgang ⇒ alle Tasks ⇒ Zertifizierungsstellenzertifikat installieren ⇒ Öffnen
- Sichern der Zertifikatsdienste
  (nur durch Sicherungsoperatoren oder Administratoren)
  Verwaltung ⇒ Zertifizierungsstelle ⇒ alle Tasks ⇒ Zertifizierungsstelle sichern
- Wiederherstellen der Zertifikatsdienste
  (nur durch Sicherungsoperatoren oder Administratoren)
  Verwaltung ⇒ Zertifizierungsstelle ⇒ alle Tasks ⇒ Zertifizierungsstelle wiederherstellen

Zertifikatsanforderungs-Assistenten

Der Zertifikatsanforderungs-Assistent ist nur verfügbar, wenn ein Zertifikat von einer Organisationszertifizierungsstelle angefordert wird.

- Verwenden von Zertifikatsvorlagen
  Administrator, Domänencontroller, Computer, Basis-EFS, EFS-Wiederherstellungs-Agent, Benutzer, Webserver

- Anforderung eines Zertifikats
  MMC-Konsole öffnen ⇒ Snap-In hinzufügen/entfernen ⇒ Hinzufügen ⇒ Zertifikat auswählen ⇒ Hinzufügen ⇒ Eigenes Benutzerkonto, Dienstkonto oder Computerkonto auswählen ⇒ Fertig stellen ⇒ OK ⇒ Zertifikate - Aktueller Benutzer Zertifikate (Lokaler Computer) ⇒ mit rechter Maustaste auf Zertifikate klicken ⇒ Alle Task ⇒ Neues Zertifikat anfordern ⇒ Weiter ⇒ Zertifikatsvorlage ⇒ Erweiterte Optionen ⇒ Weiter ⇒ Zertifikat installieren

Zertifikatsdienste-Webseiten

- Senden einer Zertifikatsanforderung
  http://*<Servername auf dem sich die Zertifizierungsstelle befindet>*/Certsrv
  ⇒ Ein Zertifikat anfordern ⇒ Weiter ⇒ Anforderungstyp wählen ⇒ Weiter ⇒ Einsenden

- Senden einer erweiterten Zertifikatsanforderung (z.B. für IPSec)
  http://*<Servername auf dem sich die Zertifizierungsstelle befindet>*/Certsrv
  ⇒ Ein Zertifikat anfordern ⇒ Weiter ⇒ Anforderungstyp wählen ⇒ Erweiterte Anforderung ⇒ Weiter ⇒ Senden Sie ein Zertifikatsanforderungsformular an diese Zertifizierungsstelle ⇒ Einsenden

Wichtig:
Wird ein Zertifikat für einen Computer angefordert, so muss das Kontrollkästchen „Lokalen Speicherplatz verwenden“ aktiviert werden.

- Überprüfen einer ausstehenden Anforderung
  http://*<Servername auf dem sich die Zertifizierungsstelle befindet>*/Certsrv
  ⇒ auf ein ausstehendes Zertifikat überprüfen ⇒ Weiter ⇒ Weiter ⇒ Hier stehen drei Zertifikatsstatus zur Verfügung: 1) Noch ausstehend ⇒ Entfernen
  2) Ausgestellt ⇒ Dieses Zertifikat installieren
  3) Verweigert

Anzeigen von Zertifikaten

Windows2000 speichert Computerzertifikate lokal auf dem Computer, die diese angefordert hat.
Indem eine MMC-Konsole geöffnet wird, kann der Zertifikatsspeicher, der folgendermaßen strukturiert sein kann, angezeigt werden:
Eigene Zertifikate, Vertrauenswürdige Stammzertifizierungsstellen, Organisations-vertrauen, Zwischenzertifizierungsstellen, Active-Directory-Benutzerobjekt, Request, SPC

Verwalten von Zertifikaten

- Ausstellen von Zertifikaten
  *Öffnen der Konsole **Zertifizierungsstelle** ⇒ Ausstehende Anforderungen*

- Sperren von Zertifikaten
  *Öffnen der Konsole **Zertifizierungsstelle** ⇒ ausgestellte Zertifikate ⇒ mit rechter Maustaste auf das Zertifikat klicken ⇒ Alle Tasks ⇒ Zertifikat sperren ⇒ Grund auswählen ⇒ Ja*

- Veröffentlichen einer Zertifikatsperrliste
  - befindet sich im Ordner **%SystemRoot%\System32\CertSrv\CertEnroll**
  *Öffnen der Konsole **Zertifizierungsstelle** ⇒ mit rechter Maustaste auf **Gesperrte Zertifikate** klicken ⇒ Alle Tasks ⇒ Veröffentlichen ⇒ Ja*

Importieren und Exportieren von Zertifikaten

Folgende Formate können importiert und exportiert werden:

- Personal Information Exchange (PKCS #12)
- Cryptographic Message Syntax Standard (PKCS #7)
- DER Encoded Binary X.509
- Base64 Encoded X.509

- Importieren eines Zertifikats
  *Öffnen einer MMC-Konsole die das Snap-In **Zertifikat** enthält ⇒ Eigene Zertifikate ⇒ mit rechter Maustaste auf **Zertifikate** klicken ⇒ Alle Tasks ⇒ Importieren*

- Exportieren eines Zertifikats
  *Öffnen einer MMC-Konsole die das Snap-In **Zertifikat** enthält ⇒ Eigene Zertifikate ⇒ mit rechter Maustaste auf **Zertifikate** klicken ⇒ Alle Tasks ⇒ Exportieren*

Konfigurieren von Active Directory für Zertifikate

- Der externe Benutzer muss ein Zertifikat haben
- Der externe Benutzer muss ein Benutzerkonto haben
- Das Zertifikat des Externen Benutzers muss von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt werden
- Eine Namenszuordnung muss zwischen dem Zertifikat des externen Benutzers und dem Activ-Directory-Konto erstellt werden

Problembehandlung

- Überprüfen von Ereignisprotokollen
- Verwenden des Diagnosemodus
- Problembehandlung bei einer Zertifizierungsstelle
- Bestätigen der Gültigkeit eines Zertifikats

Unterrichtseinheit 6:

Netzwerksicherheit mit Hilfe von IPSec

Bei IPSec (Internet Protocol Security) handelt es sich um ein Gerüst offener Standards, um eine sichere, private Kommunikation über IP-Netzwerke (Internetprotokoll) mit Hilfe von kryptographischen Sicherheitsdiensten zu gewährleisten.
IPSec wird benötigt um Computer zu authentifizieren und die Daten zu verschlüsseln.

Anmerkung:
Bislang handelt es sich bei IPSec lediglich um einen Vorschlag und noch nicht um einen Standard.

Häufige Arten von Netzwerkangriffen:

- **Netzwerküberwachung:** durch Verwendung eines Netzwerkmonitors
- **Datenänderung:** während der Übertragung
- **Kennwörter:** stehlen und ändern
- **Adressenspoofing:** Ein Angreifer kann mit Hilfe von speziellen Programmen IP-Pakete erstellen, die scheinbar von gültigen Adressen innerhalb des vertrauten Netzwerkes stammen
- **Anwendungsschicht:** Schwächen im Betriebssystem werden ausgenutzt
- **Man-in-the-Middle:** eine Person erfasst und steuert zwischen den beiden kommunizierenden Computern die Daten aktiv und transparent
- **Denial-of-Service (DoS):** die normale Verwendung von Computern oder Netzwerkressourcen werden versucht zu verhindern

Das Netz muss auf alle Fälle geschützt werden vor:

- Änderungen während der Datenübertragung
- abfangen, anzeigen oder kopieren von Daten
- Zugriff durch unberechtigte Teilnehmer

Untersuchen der Rolle von IPSec in einem Netzwerk

Das Hauptziel von IPSec liegt im Schutz von IP-Paketen. Es basiert auf einem Ende-zu-Ende-Sicherheitsmodell, bei dem der Sender und der Empfänger die einzigen Hosts sind, die über den IPSec-Schutz informiert sein müssen.
Jeder Computer sorgt an seinem Ende für die Sicherheit, wobei davon ausgegangen wird, dass das Medium, über das die Kommunikation erfolgt, nicht sicher ist.
Computer, die Daten lediglich von der Quelle zum Ziel weiterleiten, müssen IPSec nicht unterstützen.

Erweitere Netzwerksicherheit (grober Ablauf):

- Gegenseitige Authentifizierung der Computer vor dem Datenaustausch
- Einrichten einer Sicherheitszone zwischen den beiden Computern
- Verschlüsseln der ausgetauschten Daten

Aktivieren von IPSec

IPSec wird mit Hilfe einer Richtlinienkonfiguration, die in der IP-Sicherheitsrichtlinienverwaltung verwaltet wird, gesteuert.

Anmerkung:
Zur Konfiguration dieser Sicherheitsrichtlinien sind Rechte der Gruppe Administratoren nötig.

Verwalten von IP-Sicherheitsrichtlinien

Durch hinzufügen einer Snap-In IP-Sicherheitsrichtlinienverwaltung zu der Microsoft-Management-Console (MMC) werden diese Richtlinien verwaltet.
Folgende Ebenen können damit verwaltet werden:

Ebenen:

- lokale Computer / Remotecomputer
- eigene Domäne
- fremde Domäne

Nötig sind Administratorrechte auf der betroffenen Ebene!

Verwendung von vordefinierten IP-Sicherheitsrichtlinien

Client: *(nur Antwort)*
(Für Computer, die nicht unbedingt eine sichere Kommunikation erfordern)
Diese Richtlinie ermöglicht es dem Computer, auf Anforderung für gesicherte Kommunikation entsprechend zu reagieren. Die Richtlinie enthält eine Standardantwortregel, die eine Verhandlung mit Computern ermöglicht, die IPSec anfordern.

Server: *(Sicherheit anfordern)*
(Für Computer, die meistens eine sichere Kommunikation benötigen)
Diese Richtlinie ermöglicht es dem Computer unsicheren Datenverkehr anzunehmen. Sie versucht jedoch, weitere Kommunikation zu sichern, indem Sicherheit vom ursprünglichen Sender angefordert wird.

Sicherer Server: *(Sicherheit erforderlich)*
(Für Computer, die immer eine sichere Kommunikation benötigen)
Diese Richtlinie weist unsichere eingehende Übertragungen ab. Der ausgehende Verkehr ist immer sicher.

Aktivieren einer IP-Sicherheitsrichtlinie

*In der IP-Sicherheitsrichtlinienverwaltung auf **IP-Sicherheitsrichtlinien auf lokalem Computer** klicken → im Detailfensterbereich mit der rechten Maustaste auf die zuzuweisende Richtlinie klicken → Zuweisen → OK*

Verwenden von IPSec im Übertragungsmodus

Der Übertragungsmodus (Standardmodus von IPSec) authentifiziert und verschlüsselt Daten, die zwischen zwei beliebigen Computern unter Windows2000 übertragen werden. Er wird folgendermaßen angegeben:
*Öffnen einer Komsole mit dem Snap-In **IP-Sicherheitsrichtlinienverwaltung** → im Detailfensterbereich mit der rechten Maustaste auf die zu ändernde Richtlinie klicken → Eigenschaften → Auf die zu ändernde Regel klicken → Bearbeiten → Tunneleinstellungen → Diese Regel spezifiziert keinen IPSec-Tunnel*

Es existieren zwei Übertragungsarten:

- Übertragungsmodus im gleichen Netzwerk (schlechter)
- Tunnelmodus über einen Router (besser)

Konfigurieren von IPSec für die Sicherheit zwischen Netzwerken

Um eine gesicherte Kommunikation zwischen Remotenetzwerken (über zwei Router) zu erstellen, kann IPSec für den Tunnelmodus konfiguriert werden. Daten zwischen den beiden Enden des Tunnels werden sicher und unabhängig von ihrem Ziel transportiert. Allerdings stellt der Tunnelmodus keine Sicherheit innerhalb der einzelnen Netzwerke bereit.

Verwenden von IPSec im Tunnelmodus

Windows2000 benötigt Routing und RAS, um den Tunnelmodus für IPSec zu implementieren. IPSec benötigt für den Tunnelmodus eine IP-Adresse für jedes Ende des Tunnels. Der IPSec-Tunnel wird folgendermaßen angegeben:
*Öffnen einer Komsole mit dem Snap-In **IP-Sicherheitsrichtlinienverwaltung** → im Detailfensterbereich mit der rechten Maustaste auf die zu ändernde Richtlinie klicken → Eigenschaften → Auf die zu ändernde Regel klicken → Bearbeiten → Tunneleinstellungen → Der Tunnelendpunkt wird durch diese IP-Adresse spezifiziert*

Windows2000 unterstützt zwar mehrere Verbindungen im Tunnelmodus, jedoch nicht mehrere Tunnel gleichzeitig. Jede Tunnelverbindung benötigt eine eigenständige Regel.

Regelkomponenten

Eine Regel besteht aus den folgenden Komponenten:

- Tunnelendpunkt
- Netzwerktyp
    - Alle Netzwerkverbindungen
    - LAN
    - RAS
- Authentifizierungsmethode
    - Windows2000-Standard (Kerberos V5-Protokoll)
    - Verwenden eines Zertifikats von dieser Zertifizierungsstelle
    - Diese Zeichenkette zum Schutz des Schlüsselaustauschs verwenden
- IP-Filterliste
    - All ICMP-Verkehr (ping...)
    - Gesamter IP-Verkehr
- Filteraktion

Standardantwortregel

Ein Computer verwendet diese Regel, um auf Anfragen für eine sichere Kommunikation zu antworten.

Die Standardrichtlinien wird folgendermaßen wieder hergestellt:
*Öffnen einer Komsole mit dem Snap-In **IP-Sicherheitsrichtlinienverwaltung** → im Detailfensterbereich mit der rechten Maustaste auf **IP-Sicherheitsrichtlinien auf lokalem Computer** klicken → Alle Tasks → Standardrichtlinien wiederherstellen → Ja*

Auswählen eines IPSec-Verschlüsselungsschemas

(**DES** – **D**ata **E**ncryption **S**tandard)

- **Authentifizierungsverschlüsselung**
  SHA (**S**ecure **H**ash **A**lgorithm) - 160-Bit-Schlüssel (höherwertig)
  MD5 (**M**essage **D**igest **5**) - 128-Bit-Schlüssel
- **Paketverschlüsselung (Datenverschlüsselung)**
  56-Bit DES - für die meisten exportierten Anwendungen
  40-Bit DES - nicht RFC-kompatibel
  3DES - sicherste Methode durch Verwendung von drei 56-Bit-Schlüssel

Überprüfung einer Zuweisung von IP-Sicherheitsrichtlinien

Mit dem Befehl „PING“ kann Gültigkeit einer Netzwerkverbindung überprüft werden. IPSec blockiert den Befehl PING nicht, wenn die Standardrichtlinien unverändert verwendet werden.

Wichtig:
Werden benutzerdefinierte Richtlinien erstellt, welche nicht ICMP (Internet Control Message Protocol) unterliegen, kann der Befehl PING falsche Ergebnisse anzeigen.

Verwenden der IP-Sicherheitsüberwachung zum Überprüfen der Zuweisung einer Richtlinie

Die IP-Sicherheitsüberwachung wird folgendermaßen gestartet:
Start → Ausführen → ipsecmon <Computername>
Um IPSec zu aktivieren muss eine Richtlinie zugewiesen werden.

Optimieren der IPSec-Leistung

Bevor IPSec im Netzwerk implementiert wird, sollten folgende Leistungsaspekte bedacht werden:

- **Erforderliche Sicherheitsebene:**
  Wird IPSec aktiviert, so erhöhen sich die Prozessorauslastung, der IP-Paketverkehr und die IP-Paketgröße.

Anmerkung:
Einige Hersteller bieten Netzwerkadapter an, welche die IPSec-Verschlüsselungstasks auf dem Netzwerkadapter durchführen. Das Durchführen der IPSec-Verschlüsselung mit Hilfe einer dediziert Hardware kann die Leistung erheblich steigern.

- **Sicherheitsanforderungen des Computers**
- **Anzahl der Einträge für IP-Sicherheitsrichtlinienfilter**

Konfigurieren von TCP/IP für die Serversicherheit

Die IP-Sicherheit für TCP/IP (Transmission Control Protocol) wird aktiviert, indem die Richtlinie **Sicherer Server** (standardmäßig deaktiviert) zugewiesen wird.

*Öffnen einer Komsole mit dem Snap-In **IP-Sicherheitsrichtlinienverwaltung** → im Detailfensterbereich mit der rechten Maustaste auf **IP-Sicherheitsrichtlinien auf lokalem Computer** klicken → Sicherer Server (Sicherheit erforderlich) → Zuweisen*

Überprüfen der IP-Sicherheitsrichtlinie bei Auftreten von Problemen

- Überprüfen der System- und Sicherheitsprotokolle auf Fehlermeldungen
- Überprüfen der IP-Sicherheitsüberwachung
- Überprüfen, ob die Richtlinien beiden Computern zugewiesen wurden
- die Richtlinien müssen miteinander kompatibel sein
- Neustart der IP-Sicherheitsüberwachung

Unterrichtseinheit 7:

Konfigurieren von Remotezugriff

Über Remotezugriff können Benutzer an einem Remotestandort eine Verbindung zu Ihrem Netzwerk herstellen.

Aufbau einer RAS-Verbindung (siehe Kapitel 7 / Seite 3)

Remotezugriffsvorgang
Der RAS-Server, ein Computer, auf dem Windows2000 Server und der Routing und RAS-Dienst ausgeführt werden, authentifiziert Benutzer und RAS-Sitzungen.
Der RAS-Server fungiert hierbei als ein Gateway, indem er Daten zwischen dem Client und dem LAN übertragt.

RAS-Verbindungsarten

- **DFÜ-Verbindungen:**
  Um über DFÜ-Remotezugriff eine Verbindung zum Netzwerk herzustellen, verwendet ein RAS-Client ein Kommunikationsnetzwerk, wie beispielsweise ein öffentlich geschaltetes Datennetzwerk (Public Switched Telephone Network PSTN) um eine physikalische Verbindung zu einen Anschluss an einem RAS-Server im privaten Netzwerk zu erstellen. Hierbei erfolgt das Einwählen beim RAS-Server normalerweise über ein Modem oder einen ISDN-Adapter (pro Verbindung).
  Es ergeben sich hierfür beträchtliche Kosten für Ferngespräche.

- **VPN-Verbindungen:**
  Sichere Remote-Verbindung über das Internet durch eine verschlüsselte virtuelle Punkt-zu-Punkt-Verbindung zu einem VPN-Gateway im privaten Netzwerk. Der Benutzer stellt die Verbindung zum Internet über einen Internetdienstanbieter (Internet Service Provider ISP) her.
  Die Kosten für Ferngespräche werden dadurch gesenkt und der Zugang ist für n Clients bereitgestellt.

Datentransportprotokoll

Routing und RAS in Windows2000 verwendet sowohl RAS- (für WAN-Verbindungen), als auch LAN-Protokolle (für Datenübertragung innerhalb des LANs), damit Clients die Verbindung zu RAS-Servern herstellen können.

Schicht 5	RAS Protokoll		PPP, SLIP		
Schicht 4 Schicht 3	Netzwerk Protokolle	Transport Vermittlung	IPX SPX	NetBEUI	TCP, UDP IP

RAS-Protokolle	LAN-Protokolle
PPP (Standard)	TCP/IP
SLIP (Serial Line Internetprotokoll) (alt, nur für Client)	NWLink
Microsoft RAS (alt)	NetBEUI
ARAP (nur Serverkomponente für Apple-Client)	AppleTalk

VPN-Protokoll

VPN-Protokolle kapseln Datenpakete in PPP-Datenpakete ein und können damit eine sichere verschlüsselte Übertragung über das Internet gewährleisten.

Der Weg der Daten kann folgendermaßen interpretiert werden:
Daten vom Sender → VPN → PPP → TCP/IP → WWW → TCP/IP → PPP → VPN → Übertragene Daten am Empfänger

VPNs verwenden entweder PPTP oder L2TP für den Verbindungsaufbau. Windows2000 aktiviert diese Protokolle automatisch, wenn während der Installation von Routing und RAS VPN-Anschlüsse erstellt werden.

PPTP (MS-spezialisiert)	L2TP (universell)
Netzwerk mus IP-basiert sein	Netzwerk kann IP-, Frame Relay-, x.25- oder ATM-basiert sein
Keine Headerkompression	Headerkompression
Keine Tunnelauthentifizierung	Tunnelauthentifizierung (dadurch werden sowohl die Kennwörter, als auch die Daten geschützt)
PPP-Verschlüsselung integriert	Verwendet IPSec-Verschlüsselung

Konfigurieren eingehender Verbindungen

Verbindungen werden folgendermaßen konfiguriert:
- In einer Domäne: Setup-Assistent für den Routing- und RAS-Server
- Bei einer Workstation oder Server ohne Domäne: mit Netzwerkverbindungsassistent

Konfigurieren eingehender DFÜ-Verbindungen (serverseitig)
Installieren und konfigurieren aller Protokolle, die von den DFÜ-Benutzer verwendet werden (TCP/IP, NWLink, NetBEUI, AppleTalk) → Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf den zu konfigurierenden Server klicken → Routing und RAS konfigurieren und aktivieren → Weiter → Allgemeine Konfigurationen → RAS-Server → Weiter → Remoteclientprotokolle → alle Transportprotokolle überprüfen → Weiter → Netzwerkauswahl → Weiter → IP-Adresszuweisung (eine Option auswählen) → Mehrere RAS-Server verwalten → Weiter → Fertig stellen

Konfiguration von VPN-Anschlüssen

Wird Routing und RAS zum ersten Mal gestartet, so erstellt Windows2000 automatisch fünf PPTP- und fünf L2TP-Anschlüsse (Ports). Die Anzahl der virtuellen Anschlüsse (kann auf eine Zahl erhöht oder verringert werden, die für die dem RAS-Server zur Verfügung stehende Bandbreite geeignet ist), die für jeden RAS-Server zur Verfügung stehen, wird nicht durch die Verfügbarkeit der Hardware beschränkt.

Anmerkung:
Wird im Setup-Assistenten für den Routing- und RAS-Server die Option VPN-Server ausgewählt, so erstellt Windows 2000 automatisch 128PPTP- und 128L2TP-Anschlüsse.

Programme → Verwaltung → Routing und RAS → Eigenschaften von Ports → Gerät auswählen → Konfigurieren → „RAS-Verbindungen (nur eingehend)" aktivieren → in den Dialogfeldern „Gerät konfigurieren" und „Eigenschaften von Ports" auf „OK" klicken

Konfigurieren von Modem- und Kabelanschlüssen

Wird Routing und RAS zum ersten Mal ausgeführt, erkennt Windows2000 automatisch alle installierten Modems und erstellt Modemanschlüsse für diese, sowie auch für alle erkannten parallelen oder seriellen Kabelverbindungen.

Programme → Verwaltung → Routing und RAS → Eigenschaften von Ports → Konfigurieren (Modem-, parallele und serielle Anschlüsse werden einzeln aufgeführt und können entweder einzeln oder gemeinsam konfiguriert werden) → Gerät konfigurieren → Kontrollkästchen „RAS-Verbindung (nur eingehend)" aktivieren → in den Dialogfeldern „Gerät konfigurieren" und „Eigenschaften von Ports" auf „OK" klicken

Konfigurieren von Benutzereinwähleinstellungen

Auf einen alleinstehenden Server werden die Einwähleinstellungen konfiguriert in:
→ Einwahl → Eigenschaften → Snap-In → Lokale Benutzer und Gruppen.
Bei Active Directory werden die Einwähleinstellungen konfiguriert in:
→ Einwahl → Eigenschaften → Active Directory-Benutzer und -Computer.

Aktivieren des Verifizierens der Anruferkennung

Wenn die Option Anruferkennung verifizieren ausgewählt ist, überprüft der Server die Rufnummer des Anrufers. Um die Verbindung herstellen zu können müssen alle Teile der Verbindung die Anruferkennung unterstützen

- ISDN-Rufnummer
- Hardware
- Netz
- Router

Konfigurieren ausgehender Verbindungen (Client)

Es gibt drei grundlegende Arten von ausgehenden Verbindungen:

- DFÜ-Verbindungen
  - Verbindungen zu einem privaten Netzwerk oder Server
  - Verbindung zu einem ISP
- Verbindungen zu einem VPN
- Direkte Verbindungen zu einem anderen Computer über Kabel

Es werden sämtliche ausgehende Verbindungen unter Windows 2000 mit Hilfe des Netzwerkverbindungs-Assistenten konfiguriert.

Tipp:
Der Assistent für das Microsoft Verbindungs-Manager-Verwaltungskit (Connection Manager Administration Kit, CMAK) vereinfacht den Anpassungsvorgang, da hiermit benutzerdefinierte Elemente für den Dienst angegeben werden können (z.B. DFÜ-Standort, Rufnummern, VPN-Einstellungen...). Auf dieser Basis wird anschließend ein benutzerdefiniertes Installationspaket erstellt.

Erstellen einer DFÜ-Verbindung Kap

Neue ausgehende Verbindungen werden folgendermaßen erstellt:
*Programme → Einstellungen → Netzwerk- und DFÜ-Verbindungen → Neue Verbindung erstellen → Weiter → Entweder „**In ein privates Netzwerk einwählen**“ (entweder ISP für eine Internetverbindung oder Modems eines privaten Netzwerkes) oder auf „**In das Internet einwählen**“ (Assistent für den Internetzugang) auswählen → „**für alle Benutzer verwenden**“ (Kontrollkästchen „**Gemeinsame Nutzung der Internetverbindung aktivieren**“ anklicken) oder „**nur selbst verwenden**“ auswählen → Weiter → Namen eingeben → Fertig stellen*

Herstellen einer Verbindung zu einem virtuellen privaten Netzwerk VPN

Erstellen einer Verbindung zu einem VPN (DFÜ zum ISP muss schon eingerichtet sein):
*Programme → Einstellungen → Netzwerk- und DFÜ-Verbindungen → Neue Verbindung erstellen → Verbindung mit einem privaten Netzwerk über das Internet herstellen → Weiter → Nachfolgende Schritte ausführen → Weiter → Namen und IP eingeben → Weiter → „**für alle Benutzer verwenden**“ (Kontrollkästchen „**Gemeinsame Nutzung der Internetverbindung aktivieren**“ anklicken) oder „**nur selbst verwenden**“ auswählen → Weiter → Namen eingeben → Fertig stellen*

Erstellen einer direkten Verbindung über ein Kabel:
(Ist der Computer Mitglied einer Domäne, sollte Routing und RAS verwendet werden)
*Programme → Einstellungen → Netzwerk- und DFÜ-Verbindungen → Neue Verbindung erstellen → Direkt mit anderem Computer verbinden → Weiter → Nachfolgende Schritte ausführen → Weiter → „**für alle Benutzer verwenden**“ (Kontrollkästchen „**Gemeinsame Nutzung der Internetverbindung aktivieren**“ anklicken) oder „**nur selbst verwenden**“ auswählen → Weiter → Namen eingeben → Fertig stellen*

Konfigurieren von Mehrfachverbindungen

Mehrfachverbindungen (arbeitet mit dem Protokoll PPP Multilink zusammen) versetzen den Computer in die Lage, zwei oder mehr Kommunikationsanschlüsse wie einen einzigen Anschluss mit größerer Bandbreite zu verwenden.

PPP Multilink
Das Protokoll PPP Multilink kombiniert die Bandbreite von zwei oder mehr Kommunikationsverbindungen, um eine einzige virtuelle Datenverbindung zu erstellen und so eine skalierbare Bandbreite basierend auf den Datenmengen bereitzustellen. Allerdings muss die Funktion Mehrfachverbindung sowohl auf dem Client als auch auf dem RAS-Server aktiviert sein.

BAP
Mit BAP wird die Funktion Mehrfachverbindung erweitert, indem Verbindungen bei Bedarf dynamisch hinzugefügt oder getrennt werden.

Konfigurieren von Mehrfachverbindungen und BAP auf dem RAS-Server

Durch das Aktivieren (auf der Registerkarte PPP im Dialogfeld Eigenschaften jedes RAS-Servers) von „Mehrfachverbindungen“ und „Dynamische Bandbreitensteuerung mit BAP oder BACP“ wird das Protokoll PPP Multilink, bzw. BAP aktiviert.

Konfigurieren von Mehrfachverbindungen und BAP auf dem RAS-Client

Programme → Einstellungen → Netzwerk- und DFÜ-Verbindungen → mit rechter Maustaste auf die zu aktivierende Verbindung klicken → Eigenschaften → Allgemein → Kontrollkästchen, die in Frage kommen auswählen → Optionen → Mehrere Geräte → Nachfolgende Schritte auswählen → Konfigurieren → OK

Konfigurieren von Authentifizierungsprotokollen

RAS-Server arbeiten mit Authentifizierung, um die Identität der Benutzer zu bestimmen.

Standardmäßige Authentifizierungsprotokolle

PAP (Password Authentication Protocol)	Niedrig	Verwendet unverschlüsselte Kennwörter
SPAP (Hardware) (Shiva Password Authentication Protocol)	Mittel	Bidirektional reversibler Verschlüsselungsmechanismus (Kennwortdaten werden verschlüsselt)
CHAP (auch MD5) (Challenge Authentication Protocol)	Mittel	Unidirektionales Verschlüsselungsschema MD5, um die Antwort zu verschlüsseln
MS-CHAP (auch MPPE) (Microsoft Challenge Handshake Authentication Protocol)	Hoch	Unidirektional verschlüsseltes Kennwort (auf einem Windows2000 RAS-Server ist dieses Protokoll standardmäßig aktiviert) (ab Win98/WinNT)
MS-CHAP v2 (neue Version von MS-CHAP) (Microsoft Challenge Handshake Authentication Protocol)	Hoch	Bidirektionale Authentifizierung, leistungsfähigere Schlüssel für die Verschlüsselung (nur für VPN bei Win98/WinNT)

Extensible Authentication-Protokoll (flexibel) EAP

EAP ermöglicht für RAS-Server die benutzerdefinierte Authentifizierung. Hierbei verhandeln Client und RAS-Server die exakte Authentifizierungsmethode, die verwendet werden soll.

EAP unterstützt folgende Protokolle:

- MD5-CHAP
- Transport Layer Security (TLS)
- Weitere Authentifizierungsmethoden von Drittanbietern

Unter Verwendung der EAP-Anwendungsprogrammierungsschnittstellen (Application Programming Interfaces, APIs) für Techniken wie beispielsweise Tokencards, Smartcards, biometrische Hardware (z.B.: Netzhaut- oder Fingerabdruckscanner) sowie für Authentifizierungstechniken entwickeln, die heute noch nicht bereitgestellt werden.

Konfigurieren von Verschlüsselungsprotokollen (für die Daten)

Die Datenverschlüsselung bietet Sicherheit durch das Verschlüsseln oder Codieren der Daten, die zwischen einem RAS-Client und einem RAS-Server übertragen werden. Die Verschlüsselungsprotokolle werden auf der Registerkarte **Verschlüsselung** im Dialogfeld **Einwählprofil bearbeiten** der RAS-Richtlinie aktiviert.

Wichtig:
Die Datenverschlüsselung steht nur zur Verfügung, wenn als Authentifizierungsprotokoll MS-CHAP (v1 oder v2) oder TLS (ein EAP-Protokoll) verwendet wird!

Es gibt zwei Methoden zum Verschlüsseln der Daten: MPPE und IPSec.

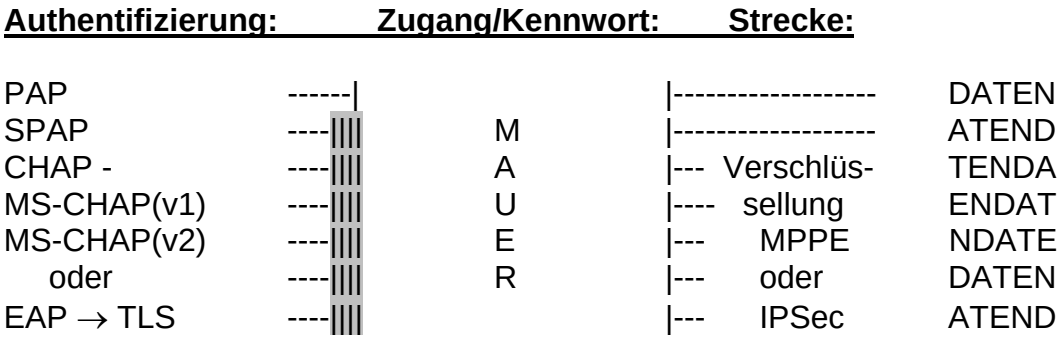
Verschlüsseln von Daten mit Hilfe von MPPE (Microsoftspezifische Lösung)

Mit MPPE werden Daten verschlüsselt, die zwischen einer PPTP-Verbindung und dem VPN-Server übertragen werden. Hierbei stehen drei Verschlüsselungsebenen zur Verfügung:

- stärkste Verschlüsselung (128 Bit)
- starke Verschlüsselung (56 Bit)
- Basisverschlüsselung (40 Bit)

Verschlüsseln von Daten mit Hilfe von IPSec (universelle Lösung)

IPSec bietet einen Rahmen für offene Standards, mit denen eine sichere private Kommunikation über IP-Netzwerke mit Hilfe von Verschlüsselung sichergestellt wird. Clients verhandeln eine Sicherheitszuordnung, die als privater Schlüssel zum Verschlüsseln des Datenflusses dient. Zum Konfigurieren der IPSec-Sicherheitsdienste (Schutz für die meisten Arten des Netzwerkverkehrs) werden IPSec-Richtlinien verwendet.

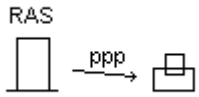


Konfiguration von Routing und RAS für die DHCP-Integration

Clients können vom RAS-Server auf drei verschiedene Arten ihre IP-Adresse erhalten:

1. Statische IP-Adresse

Die IP-Adresse wird auf dem Clientcomputer konfiguriert. (Nicht für DFÜ-Netzwerk geeignet)

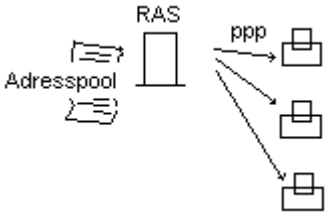


2. Aus einem Bereich von IP-Adressen

Ein RAS-Server kann eine IP-Adresse aus einem konfigurierten Adressbereich zuweisen. Es muss allerdings sichergestellt werden, dass er über eine ausreichende Anzahl von IP-Adressen verfügt, die ihm exklusiv für die Zuweisung zu Clientcomputern zugeordnet sind.

Positiv: Sicherheit durch getrennte Adressbereiche

Negativ: doppelte Verwaltung

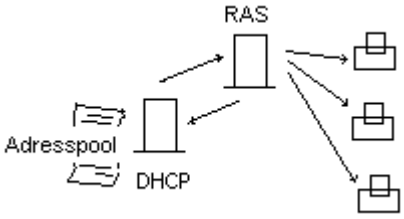


3. Vom DHCP-Server

Ein RAS-Server kann IP-Adressen von einem DHCP-Server (im 10er-Pack) erhalten und diese dann Clients zuweisen. Ein RAS-Server benötigt nur so viele IP-Adressen, wie gleichzeitig verbundene Clients vorhanden sind.

Positiv: gemeinsame Verwaltung

Negativ: Sicherheitslücke bei Ausfall des DHCP-Servers



Der RAS-Server wird zum Erhalt von IP-Adressen von einem DHCP-Server folgendermaßen konfiguriert :

Programme → Einstellungen → Systemsteuerung → Verwaltung → Routing und RAS → mit rechter Maustaste auf den entsprechenden Server klicken → Eigenschaften → IP - DHCP → Adapter → OK

Unterrichtseinheit 8:

Unterstützen des Remotezugriffs auf ein Netzwerk:

Der Routing und RAS-Dienst von Windows 2000 sowie der Internetauthentifizierungsdienst (IAS) von Windows 2000 verwenden beide RAS-Richtlinien (eine Gruppe von Bedingungen und Verbindungseinstellungen), um zu bestimmen, ob Verbindungsversuche angenommen oder verweigert werden.

Zugriffsversuch des Client

⇒ RAS-Richtlinie (Standard, Speziell) → *immer auf RAS-Server*

⇒ Einwahlberechtigung im Benutzerkonto → *z.B. Aktiv Directory*

⇒ Authentifizierungsvorgang

Untersuchen von RAS-Richtlienien

RAS-Richtlinien werden immer (auf der Serverseite) lokal und nicht im Aktiv Directory gespeichert. Eine RAS-Richtlinie besteht aus drei Komponenten, die mit dem Aktiv Directory zusammenarbeiten, um sicheren Zugriff auf RAS-Server bereit zu stellen:

- **Bedingungen**
  Die Bedingungen einer RAS-Richtlinie bilden eine Parameterliste, wie z.B. Tageszeit, Benutzergruppen, Anruferkennung oder IP-Adressen (Internetprotokoll), die mit den Parametern des Clients übereinstimmen müssen, der eine Verbindung zum Server herstellt.
- **Berechtigung**
  Kombination aus den Einwähleigenschaften eines Benutzerkontos und den RAS-Richtlinien. Die Berechtigungseinstellung einer RAS-Richtlinie arbeitet mit den Einwählrechten des Benutzers in Active Directory zusammen.
- **Profil**
  Jede Richtlinie schließt ein Profil mit Einstellungen ein, wie z.B. Authentifizierungs- und Verschlüsselungsprotokolle, die auf die Verbindung angewendet werden.

Folgen der Auswertungslogik von Richtlinien

⇒ siehe Graphik Kapitel 8 / Seite 5

RAS-Richtlinien werden folgendermaßen ausgewertet:

1. Routing und RAS vergleicht die Bedingungen der RAS-Richtlinie mit den Bedingungen des Verbindungsversuchs
2. Routing und RAS überprüft die Einwählrechte des Benutzerkontos
3. Routing und RAS wendet die Einstellungen im Richtlinienprofil auf die eingehende Verbindung an

Untersuchen von Standardrichtlinien

Die RAS-Standardrichtlinie hat keinen Einfluss auf eingehende Verbindungen, wenn sich die Domäne im gemischten Modus befindet. (Eine Domäne im gemischten Modus lässt Domänencontroller zu, die Windows 2000 oder NT 4.0 ausführen. Eine Domäne im einheitlichen Modus erfordert, dass alle Domänencontroller Windows 2000 ausführen.)

Die Standardrichtlinie lautet: ***Zugriff zulassen, wenn Einwählrechte erteilt worden sind***.

Einheitlicher Modus und eigenständige Server

Ist das Einwählrecht eines Benutzers auf **Zugriff gestatten** festgelegt, so werden alle Verbindungsversuche des jeweiligen Benutzers angenommen (im Benutzerkonto nachschauen)

Gemischter Modus

Die Standardrichtlinie wird in einer Domäne mit gemischten Modus immer außer Kraft gesetzt. Ist aber das Einwählrecht eines Benutzers auf **Zugriff gestatten** festgelegt, muss der Benutzer weiterhin die Bedingung einer Richtlinie (mindestens eine Richtlinie muss existieren) erfüllen um einen Zugriff zu erhalten.

Mehrere Richtlinien

Sind mehrere Richtlinien festgelegt, so wird immer die erste Richtlinie in der geordneten Liste der RAS-Richtlinien geprüft. Stimmen nicht alle Bedingungen der Richtlinie mit dem Verbindungsversuch überein, wird die nächste Richtlinie in der geordneten Liste überprüft, bis eine Richtlinie mit dem Verbindungsversuch übereinstimmt und anschließend mit Hinblick auf die Einstellungen des Profils und des Benutzerkontos ausgewertet. Treten hierbei Unstimmigkeiten auf, so wird der Verbindungsversuch zurückgewiesen – andere Richtlinien werden nicht überprüft.

⇒ RAS-Server
→ Benutzer
⇒ 1. Richtlinie → passt nicht; weiter
⇒ 2. Richtlinie → passt auf Benutzer ⇒ Profil widerspricht Benutzer
⇒ kein Zugriff
⇒ 3. Richtlinie → passt (wird nicht mehr angewendet)

Die 3. Richtlinie wird nicht mehr angewandt, da laut Auswertung die 2. Richtlinie passt und weitere Richtlinien nicht mehr abgefragt werden. Lösung des Problems: Richtlinienreihenfolge wechseln!

Wichtig:
Da Routing und RAS erfordert, dass mindestens die Bedingungen einer Richtlinie erfüllt sein müssen, werden alle Verbindungsversuche zurückgewiesen, wenn die Standardrichtlinie entfernt wird und keine andere Richtlinien vorhanden sind.

Konfigurieren von RAS-Richtlinienbedingungen

Eine RAS-Richtlinie besteht aus den Einwähleinstellungen des Benutzers, den RAS-Richtlinienbedingungen (Attribute, die mit den Einstellungen eines Verbindungsversuchs verglichen werden) und den RAS-Richtlinieneinstellungen.

Beispiel für Bedingungen von Verbindungsversuchen

- liegt zwischen 8.oo und 17.oo Uhr, Montag – Freitag
  und
- kommt von einer IP-Adresse, die 192.168.*.* entspricht
  und
- kommt von einem Benutzer der Gruppe „Sales“

Es können folgende RAS-Richtlinienbedingungen festgelegt werden:

- NAS-IP-Adress
- Service-Type
- Framed-Protocol
- Called-Station-ID
- Calling-Station-ID
- NAS-Identifier
- NAS-Port-Type
- Day-And-Time-Restrictions
- Client-IP-Adress
- Client-Vendor
- Client-Friendly-Name
- Windows-Groups
- Tunnel-Type

Um eine RAS-Richtlinie hinzuzufügen, muss folgendermaßen vorgegangen werden:
Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf RAS-Richtlinien → Neue RAS-Richtlinie → RAS-Richtlinie hinzufügen → Angezeigter Richtlinienname → Weiter → Hinzufügen → Attribut auswählen → Hinzufügen → Attributnamen eingeben *→ OK → Weiter → RAS-Berechtigungen erteilen* oder *RAS-Berechtigungen verweigern → Weiter → Fertig stellen*

Konfigurieren von RAS-Richtlinienbedingungen

Beispiel für Profileinstellungen

- 90 Minuten Verbindungszeit
  und
- vier Mehrfachverbindungsleitungen
  und
- erfordert IPSec-Verschlüsselung

Das RAS-Profil gibt an, welche Art Zugriff der Benutzer erhält, falls die Bedingungen erfüllt werden.

Ein Profil kann mit folgendenden Parametern konfiguriert werden:

- Einwähleinschränkungen
- IP
- Mehrfachverbindungen
- Authentifizierung
- Verschlüsselung
- Weitere Optionen

Überwachen des Remotezugriffs

Ereignisprotokolle
Das Windows 2000-Ereignisprotokoll enthält Informationen zu Systemkomponenten in Windows 2000 und sollte daher als erster überprüft werden, um Informationen zu einem Problem zu erhalten.
Arbeitsplatz → Verwalten → Computerverwaltung → Ereignisanzeige → System → RemoteAccess → Quelle

Modemprotokollierung
Windows 2000 Professional zeichnet während einer Verbindung automatisch ein Protokoll der Datenübertragung von Computer zu einem Modem auf. Bei Windows 2000 Server und Advanced Server muss die Protokolldatei manuell aktiviert werden.
Systemsteuerung → Telefon- und Modenoptionen → Modems → auf das zu konfigurierende Modem klicken → Eigenschaften → Diagnose → aktivieren von „Protokoll aufzeichnen", bzw. „An Protokoll anhängen" → OK
Um das Protokoll anzuzeigen muss man auf der Registerkarte *Diagnose* auf *Protokoll anzeigen* klicken.

Verfolgen des Ablaufs von RAS-Verbindungen

Windows 2000 verfügt über eine umfangreiche Ablaufverfolgungsmöglichkeit, mit der komplexe Netzwerkprobleme behandelt werden können. Die Ablaufverfolgungs-möglichkeiten müssen unter folgendem Registry-Schlüssel geändert werden: (siehe Kapitel 8/Seite25-26)

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing

Wert:	**Datentyp:**
EnableFileTracing	REG_DWORD (auf 1 festlegen) um Ablaufverfolgungsinformationen in einer Datei zu aktivieren (Standard 0)
FileDirectory	REG_EXPAND_SZ (Speicherortinformationen)
FileTracingMask	REG_DWORD (festlegen, wie viele Ablaufverfolgungsinformationen protokolliert werden)
MaxFileSize	REG_DWORD (Größe der Protokolldatei – Standard 64kB)

Da Ablaufverfolgungen sehr viel Systemressourcen benötigen, dürfen diese keinesfalls auf Computern mit mehreren Prozessoren aktiviert werden und sollten nur kurzzeitig zum Erkennen von Fehlern im Netzwerk verwendet werden.

Unterrichtseinheit 9:

Erweitern der RAS-Fähigkeiten mit Hilfe von IAS

Werden Outsourcingdienste (Internet, Remote) bereitgestellt, muss für eine nötige Authentifizierung der Benutzerkonten gesorgt werden. Windows 2000 stellt die Kombination von Routing und RAS, sowie der Internetauthentifizierungsdienst Unterstützung für RADIUS bereit.
Bei RADIUS (Remote Authentication Dial-in User Service) handelt es sich um ein Industriestandardprotokoll, das die Lösung dieser Authentifizierungs- und Kontoführungsanforderungen für Remotebenutzer bereitstellt.

IAS und RADIUS in einem Windows 2000-Netzwerk

IAS führt die folgenden Aufgaben durch:

- Zentrale Authentifizierung
- Autorisierung
- Überwachung von und Kontoführung für Einwählverbindungen
- VPN-Verbindungen
- Bei Bedarf herzustellende Wählverbindungen

Die folgenden Schritte beschreiben den grundlegenden Vorgang, den Remoteserver, ein RADIUS-Server und RADIUS-Clients verwenden, um Authentifizierung und Autorisierung durchzuführen:

1. Ein Benutzer stellt über eine Einwähl- oder VPN-Verbindung eine Verbindung zu einem Windows 2000-basierten Computer mit Routing und RAS her.
2. Der Windows 2000-basierte Computer mit Routing und RAS leitet die Authentifizierungsanforderungen an einen IAS-Server weiter und fungiert hierbei als RADIUS-Client.
3. Der IAS-Server, welcher hier die Funktionen eines RADIUS-Servers ausführt, greift auf die Benutzerkontoinformationen auf einem Domänencontroller zu und überprüft die RAS-Authentifizierungsinformationen.
4. Wenn die Anmeldeinformationen des Benutzers authentifiziert und der Verbindungsversuch autorisiert wurde, so autorisiert der IAS-Server den Benutzerzugriff und protokolliert die RAS-Verbindungen als Kontoführungsereignisse.

Zweck und Verwendung von IAS

- DFÜ-Zugriff für Firmen
- Extranet-Zugriff für Geschäftspartner
- Internet-Zugriff
- Geoutsourcter Firmen-Zugriff über Dienstanbieter

Installation und Konfiguration von IAS

Installation von IAS (wird zum Menü **Verwaltung** hinzugefügt):
Systemsteuerung → Software → Windows-Komponenten hinzufügen/entfernen → Komponenten → Netzwerkdienste → Details → Kontrollkästchen „Internetauthentifizierungsdienst“ aktivieren → OK → Weiter → Fertig stellen

Wenn ein IAS-Server auf Active Directory zugreifen muss, um Benutzer zu authentifizieren, muss dieser Server erst in der Microsoft Management Console (MMC) durch **Internetauthentifizierungsdienst** autorisiert werden. Nur Mitglieder der Gruppe **Organisations-Admins** können einen IAS-Server autorisieren!

Autorisieren eines IAS-Servers:
Programme → Verwaltung → Internetauthentifizierungsdienst → mit rechter Maustaste auf Internetauthentifizierungsdienst (lokal) → Dienst im Active Directory registrieren → Internetauthentifizierungsdienst im Active Directory registrieren → OK

Konfigurieren des IAS-Server für RADIUS-Clients:
Programme → Verwaltung → Internetauthentifizierungsdienst → mit rechter Maustaste auf Clients → Neuer Client → auf der Seite „Client hinzufügen“ im Feld „Angezeigter Name“ den RADIUS-Client-Namen angeben → Weiter → auf der Seite „Clientinformationen“ die Informationen eingeben (siehe Kapitel9 / Seite9) → Fertig stellen

Konfiguration eines RAS-Server für die Verwendung der RADIUS-Authentifizierung:

Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf Server → Eigenschaften → auf der Seite „Sicherheit“ im Feld „Authentifizierungsanbieter“ auf „RADIUS-Authentifizierung“ klicken → Konfigurieren → Hinzufügen → Servernamen eingeben → OK → Routing und RAS muss nun neu gestartet werden

Konfiguration eines RAS-Server für die Verwendung der RADIUS-Kontoführung:

Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf Server → Eigenschaften → auf der Seite „Sicherheit“ im Feld „Kontoführungsanbieter“ auf „RADIUS-Kontoführung“ klicken → Konfigurieren → Hinzufügen → Servernamen eingeben → Kontrollkästchen „RADIUS-Kontoführung EIN/AUS – Nachrichten senden“ aktivieren → OK → Routing und RAS muss nun neu gestartet werden

Konfiguration der Protokolle für Kontoführungsinformationen:

Programme → Verwaltung → Internetauthentifizierungsdienst → RAS-Protokollierung → mit rechter Maustaste auf „Lokale Datei“ klicken → Eigenschaften → Einstellungen → Ereignisse auswählen, die Protokolliert werden sollen → auf Registerkarte „Lokale Datei“ wechseln und Eingaben konfigurieren → OK

Unterrichtseinheit 10:

Konfigurieren eines Windows 2000-basierten Servers als Router

Router ermöglichen eine Skalierung des Netzwerkes und eine Verwaltung der Bandbreite durch Segmentieren des Netzwerkverkehrs.
Als Routing wird der Vorgang des Weiterleitens von Paketen (IP-Datagramm) zwischen verbundenen TCP/IP-Netzwerken bezeichnet.
Bei Windows 2000 Routing und RAS handelt es sich um einen Dienst, der Routing als einen von mehreren Prozessen durchführt.

Zweck des Routings und Routingtabellen:

- IP-Router stellen die Paketweiterleitung für andere TCP/IP-Hosts bereit.
- IP-Router sind mehrfach vernetzte Hosts. (Ein Netzwerkhost, der mindestens zwei Netzwerkverbindungs-Schnittstellen verwendet, um getrennte Netzwerksegmente zu verbinden)

Die Routingtabellen schließen IP-Informationen über alle Segmente ein, an die der Router angeschlossen ist. Die Daten schließen darüber hinaus Anweisungen ein, wie für andere Netzwerke bestimmte Pakete weitergeleitet werden, die nicht direkt mit dem Router verbunden sind.
Die IP-Routingtabelle kann durch den Befehl **route print** angezeigt werden.

Folgende Routingtabelleneinträgen werden unterschieden: (siehe Kapitel10 / Seite6)
- Netzwerkziel
- Netzwerkmaske (Subnetzmaske)
- Gateway
- Schnittstelle
- Anzahl: Anzahl der Abschnitte, Verzögerung, Durchsatz, Zuverlässigkeit

Standardmäßige Routingtabelleneinträge:

Netzwerkadresse	Beschreibung
0.0.0.0	Alle IP-Adressen, für die keine anderen Routen definiert wurden (Standardroute)
127.0.0.0	Lokale Loopbackadresse
224.0.0.0	Multicast-IP-Adresse
255.255.255.255	Broadcast-IP-Adresse

Konfiguration von Netzwerkverbindungen

Normalerweise sind in einem Computer, der Routing durchführt, mindestens zwei Netzwerkadapter (jeder besitzt eine fest vergebene IP-Adresse – kein DHCP) installiert. Um Verwechslungen unter Windows 2000 zu vermeiden, sollten für die **LAN-Verbindungen** (im Ordner **Netzwerk- und DFÜ-Verbindungen**) aussagekräftige Namen vergeben werden.
Die Schnittstellen des Windows 2000-basierten Routers, welcher mit dem Internet verbunden ist, werden manuell mit folgenden Eigenschaften konfiguriert:

- Manuell konfigurierte IP-Adresse
- Subnetzmaske
- Domänennamenserver (DNS)

Die Schnittstellen des Windows 2000-basierten Routers, welcher mit einem privaten Netzwerk und somit nur indirekt mit dem Internet verbunden ist, können beliebige Bereiche gültiger IP-Adressen verwendet werden.

Empfohlene private IP-Adressen sind:

Kennung des privaten Netzwerkes		Subnetzmaske	IP-Adressbereich
10.0.0.0	(Class A)	255.0.0.0	10.0.0.1 – 10.255.255.254
172.16.0.0	(Class B)	255.240.0.0	172.16.0.1 – 172.31.255.254
192.168.0.0	(Class C)	255.255.0.0	192.168.0.1 – 192.168.255.254

Wichtig:
Um spätere Adresskonflikte bei Einbindung des Internets zu vermeiden, sollten für private Netzwerke generell private Netzwerkadressen verwendet werden!

Um die Netzwerkkonfiguration zu überprüfen kann man das Dienstprogramm **ipconfig** (**ipconfig /all**) verwenden.

Aktivieren von Routing mit Hilfe von Routing und RAS

Handelt es sich bei dem Server um ein Mitglied einer Domäne des Windows 2000-Verzeichnisdienstes Active Directory und ist Routing für Wählen bei Bedarf aktiviert, so muss – um dieses Routing verwenden zu können - das Computerkonto des Servers zur Sicherheitsgruppe **RAS- und IAS-Server** hinzugefügt werden.

Um das Routing zu aktivieren, sind folgende Schritte notwendig:
*Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf den zu aktivierenden Server klicken → Routing und RAS konfigurieren und aktivieren → Weiter → Allgemeine Konfiguration → Netzwerkrouter → Weiter → auf der Seite **Geroutete Protokolle** die erforderlichen Netzwerkprotokolle (IP, IPX, AppleTalk) einstellen → Weiter → auf der Seite **Bei Bedarf herzustellende Wählverbindung** auf **Ja** klicken (die Schnittstelle wird nur dann aktiviert, wenn Daten an den Remotestandort gesendet werden) → Weiter → Fertig stellen*

Um einen RAS-Server für Routing zu aktivieren, sind folgende Schritte notwendig:
Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf den zu aktivierenden Server klicken → Eigenschaften → Allgemein → Router → Auswahl anklicken → OK

Untersuchen einer statischen Routingtabelle

Statische Routen, welche sich lediglich für kleine Internetzwerke eignen und nur schwer angepasst werden können, da sie manuell verwaltet werden müssen, werden folgendermaßen angezeigt:
*Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf den zu aktivierenden Server klicken → IP-Routing → mit rechter Maustaste auf **Statische Routen** klicken → IP-Routingtabelle anzeigen*

Die IP-Routingtabelle enthält folgende Informationen:

- Ziel
- Netzwerkmaske
- Gateway
- Schnittstelle
- Anzahl
- Protokoll (gibt an, wie die Route bestimmt wurde. Sind in dieser Spalte andere Werte als LOKAL aufgeführt, so wurde die Route manuell durch einen Administrator konfiguriert, oder der Router empfängt Routen von anderen Routern)

Hinzufügen einer statischen Route

Im Dialogfeld **Statische Route** (*Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf den zu aktivierenden Server klicken → IP-Routing → mit rechter Maustaste auf **Statische Routen** klicken → Neue Statische Route → OK)* können statische IP-Routen zur Routingtabelle hinzugefügt und mit den Befehlen **ping** und **tracert** überprüft werden.

Konfigurieren einer Routingschnittstelle

Bei einer Routingschnittstelle handelt es sich um eine physische oder logische Schnittstelle, über die IP-Pakete weitergeleitet werden.

Es gibt drei Typen von Routingschnittstellen:

1. LAN-Schnittstelle
   Diese Schnittstellen sind immer aktiv und erfordern zur Aktivierung normalerweise keinen Authentifizierungsvorgang

2.

Schnittstellen für Wählen bei Bedarf
Diese Schnittstellen erfordern normalerweise einen Authentifizierungsvorgang, um eine Punkt-zu-Punkt-Verbindung herzustellen, welche auf einer physischen Verbindung (z.B. zwei Router, die über Modems und eine analoge Telefonleitung verbunden sind), oder einer logische Verbindung (z.B. zwei Router, die mit Hilfe des Internet über ein VPN verbunden sind) basiert.

3. IP-in-IP-Tunnelschnittstellen
   Diese Schnittstellen erfordern zum Herstellen der Verbindung einen Authentifizierungsvorgang

Paketfilterung

Die IP-Paketfilterung (wichtig, wenn Firmenintranets mit MS-Produkten mit öffentlichen Netzwerken, wie z.B. dem Internet verbunden werden) ermöglicht es einem Netzwerkadministrator präzise zu definieren, welcher IP-Verkehr den Router durchlaufen darf und welcher nicht.

Beispiel: Wird ein Ping-Befehl aufgerufen, so wird automatisch ein ICMP-, oder SNMP-Verkehr erzeugt; um dies zu vermeiden, kann dieser allerdings ausgefiltert werden!

Das Blockieren des SNMP-Verkehrs verhindert ausserdem, dass ein Benutzer im betreffenden Netzwerk Verwaltungsfunktionen auf Computern durchführt, die mit dem restlichen Netzwerk verbunden sind.

Konfigurieren von Filtern an einer IP-Routingschnittstelle

Ein Netzwerkadministrator kann an jeder Schnittstelle Ein- und Ausgabefilter für Schlüsselfelder in den IP-, TCP-, UDP- und ICMP-Headern konfigurieren.

Eine Schnittstelle wird folgendermaßen ausgewählt:
Programme → Verwaltung → Routing und RAS → IP-Routing → Allgemein → mit rechter Maustaste auf die hinzuzufügende Schnittstelle klicken → Eigenschaften

Filter werden auf der Basis von Ausnahmen konfiguriert (entweder wird jeglicher Verkehr mit Ausnahme des angegebenen Verkehrs empfangen oder gesperrt).

Folgende Ein-, bzw. Ausgabefilter können ausgewählt werden:

- **Alle Pakete übertragen, mit Ausnahme derjenigen, die die unten aufgeführten Kriterien erfüllen** (wird verwendet, wenn kein hohes Maß an Sicherheit erforderlich ist)

ODER

- **Alle Pakete verwerfen, mit Ausnahme derjenigen, die die unten aufgeführten Kriterien erfüllen** (wird verwendet, wenn ein hohes Maß an Sicherheit erforderlich ist)

Um einen Filter hinzuzufügen müssen die Dialogfelder **IP-Filter hinzufügen**, bzw. **IP-Filter bearbeiten** mit folgenden Einstellungen bearbeitet werden:

1. Identifizieren des Quellnetzwerkes
   - IP-Adresse
   - Subnetzmaske

2. Identifizieren des Quellnetzwerkes
   - IP-Adresse
   - Subnetzmaske

3. Auswahl des Protokolles
   - **TCP** (ist kein Anschluss angegeben, nimmt die Einstellung den Standardwert 0 [alle Anschlüsse] an)
   - **TCP (eingerichtet)**
   - **UDP** (ist kein Anschluss angegeben, nimmt die Einstellung den Standardwert 0 [alle Anschlüsse] an)
   - **ICMP** (ist kein Anschluss angegeben, nimmt die Einstellung den Standardwert 255 [beliebiger Code oder jeder Typ] an)
   - **Beliebig**
   - **Weitere** (Die Datei ***systemroot*\system32\drivers\etc\protocol** enthält eine Liste der mit Windows 2000 kompatiblen Protokolle und die Nummer jedes Protokolls. Durch das Bearbeiten dieser Datei kann es Windows ermöglicht werden, weitere Protokolle zu erkennen)

Routing für Wählen bei Bedarf

Routing und RAS kann Pakete über andere Kommunikationsnetzwerke routen.
Windows 2000 schließt folgende Unterstützung mit ein:

- Filter für Wählen bei Bedarf (diese Filter sind unabhängig von IP-Paketfiltern)
- Hinauswählzeiten

Um einen Router für den Bedarf herzustellender Wählverbindungen zu konfigurieren muss folgendermaßen Vorgegangen werden:

- Konfigurieren der Verbindungseinstellungen zum Intranet der Zentrale
  (Einstellen der IP-Adresse, Subnetzmaske, DNS- und Wins-Server)
- Konfigurieren der Anschlüsse, sodass bei Bedarf herzustellende Wählverbindungen möglich sind
  *(Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf Ports klicken → Eigenschaften → erst auf ein Gerät, dann auf Konfigurieren klicken → Kontrollkästchen **Bei Bedarf herzustellende Routingverbindungen (ein- und ausgehend)** aktivieren → 2x OK)*
- Konfigurieren der Schnittstellen für Wählen bei Bedarf
  (Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf Routingschnittstellen klicken → Neue Schnittstelle für Wählen bei Bedarf → Informationen eingeben (siehe Kapitel10 / Seite35-36)

Konfigurieren von IP-Adressen für eingehende bei Bedarf herzustellende Wählverbindungen

Wird der RAS-Server für die Verwendung eines statischen Adresspools konfiguriert, so kann jeder IP-Adressbereich wie folgt eingegeben werden:

- Start-IP-Adresse und End-IP-Adresse für den Bereich

oder

- Start-IP-Adresse und die Gesamtzahl von IP-Adressen im Bereich

Programme → Verwaltung → Routing und RAS → mit rechter Maustaste erst auf Server, dann auf Eigenschaften klicken → IP → Statischen Adresspool → Hinzufügen → Adress-Informationen konfigurieren

Besteht der statische IP-Adresspool aus einem Bereich von Netzwerk-IP-Adressen, mit dem der RAS-Server verbunden ist, darf der IP-Adressbereich im RAS-IP-Adresspool weder statisch noch über DHCP anderen Hosts zugewiesen werden.

Um die ICMP-Verbindungsaktivitäten einzuschränken können diverse Filter gesetzt werden:
*Programme → Verwaltung → Routing und RAS → auf Routingschnittstellen klicken → mit rechter Maustaste auf die Schnittestelle klicken → Filter für Wählen bei Bedarf einrichten → Verbindung initiieren und Optionen auswählen → Hinzufügen → im Dialogfeld **IP-Filter hinzufügen** Daten eingeben → OK*

Wichtig:
Um zu verhindern, dass die bei Bedarf herzustellende Verbindung für Verkehr hergestellt wird, den die IP-Paketfilter blockieren, müssen die gleichen Filter für Wählen bei Bedarf, die für IP-Paketfilter konfiguriert wurden, konfiguriert werden.

Hinauswählzeiten werden folgendermaßen eingestellt:
Programme → Verwaltung → Routing und RAS → auf Routingschnittstellen klicken → mit rechter Maustaste auf die Schnittestelle klicken → Hinauswählzeiten → Zulassen, bzw. Verweigern → OK

Konfigurieren statischer Routen für eine Schnittstelle für Wählen bei Bedarf

Damit über eine Verbindung für Wählen bei Bedarf eine zweiseitige Kommunikation erfolgen kann, müssen auf beiden Seiten der Verbindung statische Routen für alle Netzwerke, zu denen eine Verbindung hergestellt werden soll, eingerichtet werden.

*Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf **Statische Routen** klicken → Neue statische Route → Informationen eingeben*

Um eine neukonfigurierte statische Route zu testen kann man entweder mit **ping –t *IP-Adresse*** oder **tracert *IP-Adresse*** eine Abfrage starten.

RIP und OSPF

Mit Hilfe von Routingprotokollen, wie beispielsweise RIP (Routing Information Protocol), kann eine Routingtabellenänderung, die aufgrund von Änderungen im Netzwerk erforderlich wird, automatisch verwaltet werden.
RIP erstellt Routingtabellen dynamisch, indem der Inhalt der betreffenden Routingtabelle den konfigurierten Schnittstellen angekündigt wird.
Die daran angebundenen Router teilen dann ihre empfangenen Tabellen allen anderen Routern im Netzwerk mit, damit diese ihre Routingtabellen erstellen, bzw. ergänzen können.

Die beiden gebräuchlichsten Routingprotokolle in Intranets sind RIP (RIP1 verwendet Broadcast- und RIP2 Multicast-IP-Pakete) und OSPF (Open shortest path first).

RIP	**OSPF**
Für kleine bis mittlere Internetzwerke (bis zu 50 Server)	Für große heterogene Internetzwerke
Verwaltet eine Routingtabelle	Verwendet eine Verbindungsstatus-datenbank
Einfach zu konfigurieren und bereitzu-stellen	Schwierig zu konfigurieren und zu verwalten
Schlecht skalierbar	Arbeitet effizient in großen Netzwerken

Anmerkung:
RIP wird auch als Name eines vergleichbaren, aber getrennten Routingprotokolls für IPX-Netzwerke verwendet.

OSPF wurde aufgrund der Unfähigkeit von RIP entworfen, große heterogene Internetzwerke zu bedienen. Der Vorteil von OSPF im Vergleich mit anderen Routingprotokollen besteht darin, dass es in großen Netzwerken effizient arbeitet, da durch die Berechnung der optimalen Route (ermöglicht einem Router die Berechnung des kürzesten Weges, um Pakete an die einzelnen Knoten zu senden) weniger Statusmeldungen erforderlich sind.
Die OSPF-Router verwalten eine „Karte“, die sogenannte „Verbindungsstatusdatenbank“ des Netzwerkes, die nach jeder Änderung der Netzwerktopologie aktualisiert wird.
Der Nachteil dieses Routingprotokolls liegt in seiner Komplexität, da es schwieriger zu konfigurieren ist und mehr Verwaltungszeit als RIP erfordert.

Ein Router, der RIP verwendet, nutzt Routingtabelleninformationen gemeinsam mit allen anderen Routern in einem Netzwerk.

Um RIP-für-IP und RIP-unterstützende-Schnittstellen hinzuzufügen muss folgender-maßen vorgegangen werden:

1. *Programme → Verwaltung → Routing und RAS → auf IP-Routing klicken → mit rechter Maustaste auf Allgemein klicken → Neues Routingprotokoll → folgende Eigenschaft auswählen:* ***RIP, Version 2, für das Internetprotokoll*** *→ OK*
2. *Programme → Verwaltung → Routing und RAS → auf IP-Routing klicken → mit rechter Maustaste auf RIP klicken → Neues Schnittstelle → Schnittstelle auswählen → OK*

Anschließend muss die Schnittstelle für RIP konfiguriert werden:
Programme → Verwaltung → Routing und RAS → auf IP-Routing klicken → RIP → mit rechter Maustaste auf die zu konfigurierende Schnittstelle klicken → Eigenschaften

Konfigurieren des RIP-Betriebsmodus und dessen Protokolle

Auf der Registerkarte **Allgemein** können im Feld **Betriebsmodus** die folgenden Einstellungen ausgewählt werden:

- **Modus für autostatische Aktualisierungen**
  RIP-Ankündigungen werden nur gesendet, wenn andere Router eine Aktualisierung anfordern. Dies ist die Standardeinstellung für eine Schnittstelle für Wählen bei Bedarf
- **Modus für regelmäßige Aktualisierungen**
  RIP-Ankündigungen werden regelmäßig gesendet. Dies ist die Standardeinstellung für eine LAN-Schnittstelle.

Auf der Registerkarte **Allgemein** können im Feld **Protokoll ausgehender Pakete** die folgenden Einstellungen ausgewählt werden:

- **RIP, Version 1-Broadcast**
  Sendet RIP-Ankündigungen der Version 1 als Broadcasts
- **RIP, Version 2-Broadcast**
  Sendet RIP-Ankündigungen der Version 2 als Broadcasts. Diese Einstellung wird in einer gemischten Umgebung, die RIP-Router der Version 1 und Version 2 enthält, verwendet.
- **RIP, Version 2-Multicast**
  Sendet RIP-Ankündigungen der Version 2 als Multicasts
- **Silent-RIP**
  Deaktiviert ausgehende RIP-Ankündigungen

Auf der Registerkarte **Allgemein** können im Feld **Protokoll eingehender Pakete** die folgenden Einstellungen ausgewählt werden:

- **RIP, Version 1 und 2**
  Standardauswahl; akzeptiert RIP-Ankündigungen der Version 1 und 2.
- **nur RIP, Version 1**
  akzeptiert nur RIP-Ankündigungen der Version 1.
- **nur RIP, Version 2**
  akzeptiert nur RIP-Ankündigungen der Version 2.

RIP kann durch das Einstellen von Schnittstellenkosten in der Routingtabelle so konfiguriert werden, dass es nur in Ausnahmefällen von seiner, vom Administrator festgelegten, vordefinierten Paket-Route abweicht.

Um eine Routerauthentifizierung zu erfordern, müssen alle eingehenden RIP-Pakete der Version 2 das gleiche Kennwort erhalten. Da RIP allerdings unverschlüsselte Kennwörter verwendet (nur minimale Sicherheit), wird diese Option hauptsächlich zur Identifikation verwendet.

Konfigurieren von Routenfiltern

Um die Sicherheit festzulegen (welcher Router nimmt welche Routen an), müssen die Sicherheitseinstellungen im RIP bearbeitet werden.

*Programme → Verwaltung → Routing und RAS → auf IP-Routing klicken → RIP → mit rechter Maustaste auf die zu konfigurierende Schnittstelle klicken → Eigenschaften → Sicherheit → in der Liste **Aktion** auf **Für eingehende Routen** oder **Für ausgehende Routen** klicken und Optionen auswählen → OK*

Konfigurieren von RIP für ein Nicht-Broadcastnetzwerk

Eine „Nachbarliste“ identifiziert eine Gruppe von Routern, die sich nicht in demselben Netzwerksegment wie der konfigurierte Router befinden, jedoch Ankündigungen empfangen können.

Programme → Verwaltung → Routing und RAS → auf IP-Routing klicken → RIP → mit rechter Maustaste auf die zu konfigurierende Schnittstelle klicken → Eigenschaften → Nachbarn → Optionen auswählen und anklicken→ OK

Folgende Optionen stehen hier zur Verfügung:

- **Nur Broadcast bzw. Multicast verwenden**
  Standardeinstellung
- **Nachbarn zusätzlich zu Broadcast bzw. Multicast verwenden**
  Sendet RIP-Ankündigungen mit Hilfe von Unicast zusätzlich zum Verwenden des Protokolls für ausgehende Pakete, das auf der Registerkarte **Allgemein** angegeben wurde
- **Nachbarn anstelle von Broadcast bzw. Multicast verwenden**
  Sendet RIP-Ankündigungen mit Hilfe von Unicast nur an die angegebenen Nachbarrouter. Diese Option sollte in Nicht-Broadcastnetzwerken, z.B. Frame-Relay, gewählt werden

Unterrichtseinheit 11:

Konfigurieren des Internetzugriffs für ein Netzwerk

Herstellen einer Verbindung mit dem Internet mit Hilfe eines Routers:

Ein Router ist ein Gerät, mit dessen Hilfe Datenpakete aus einem LAN oder WAN an ein anderes weitergeleitet werden. Er liest Paketheader und wählt (basierend auf den Routingtabellen) den jeweils günstigsten Pfad zum weiterleiten aus.
Obwohl die Verwendung eines Routers die einfachste Möglichkeit der Internetverbindung darstellt, bietet diese Methode keinen Schutz vor unerlaubtem Zugriff über das Internet und es muss sichergestellt werden, dass jeder Host im Netzwerk über eine öffentliche IP-Adresse verfügt.
Bei Bedarf wählendes Routing reduziert zwar die Verbindungskosten, allerdings ist diese Art der Internetverbindung sehr teuer.

Konfigurieren des Windows2000-basierten Routers:

1. Der Computer muss mit zwei Netzwerkverbindungen konfiguriert werden, wobei eine permanent mit dem internen Netzwerk und die zweite entweder permanent oder über eine DFÜ-Verbindung verbunden sein muss.
2. Beide Netzwerkkarten müssen konfiguriert werden
3. Routing und RAS installieren und aktivieren
4. Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf Server klicken → Eigenschaften → Kontrollkästchen „LAN und bei Bedarf wählendes Routing“ aktivieren → OK → mit rechter Maustaste auf Ports klicken → Eigenschaften → auf die zu aktivierende DFÜ-Verbindung klicken→ Konfigurieren → Gerät konfigurieren → Kontrollkästchen „Bei Bedarf herzustellende Routingverbindungen (ein- und ausgehend)“ aktivieren → OK → OK
5. Standardroute für die IP-Adresse des Internetdienstanbieters konfigurieren:
   Programme → Verwaltung → Routing und RAS → IP-Routing → mit rechter Maustaste auf Statische Routen klicken → Neue Statische Route → im Feld „Ziel“ und „Netzwerkmaske“ den Wert „0.0.0.0“ eingeben → im Feld „Gateway“ die Internet-IP-Adresse eingeben → Kontrollkästchen „Bei Bedarf herzustellende Wählverbindungen über diese Route initiieren“ aktivieren → OK
6. Besteht das interne Netzwerk aus mehreren Teilnetzen, müssen die Routen für alle Teilnetze hinzugefügt werden

Schützen von Internetverbindungen mit Hilfe einer Firewall:

Eine Firewall ist eine Kombination aus Hard- und Software, die ein Schutzsystem zur Verfügung stellt, das in der Regel nicht autorisierten Zugriff von aussen auf ein internes Netzwerk oder Intranet verhindert.

Erstellen von Sicherheitsregeln:

- Eine einfache Sicherheitsregel zum Weiterleiten von ausgewählten eingehenden Paketen ist zum Beispiel alle an den TCP-Anschluss 80 (standardmäßig von http verwendete Anschluss) gerichteten Pakete an einen Webserver innerhalb des Firewalls weiterleiten und alle anderen Pakete abweisen zu lassen.
- Eine weitere allgemeine Sicherheitsregel ist, die aus dem Internet eingehenden Pakete nur dann weiterzuleiten, wenn diese Teil einer Kommunikation sind, die von einem im internen Netzwerk befindlichen Computer initiiert wurden.

Herstellen einer Verbindung mit dem Internet mit Hilfe von NAT:

Netzwerkgeräte, denen private IP-Adressen zugewiesen sind, können nicht direkt auf Internetseiten zugreifen. Der Datenverkehr muss daher über ein NAT-Gerät (Netzwerkadressübersetzer) weitergeleitet werden, dem sowohl eine interne private IP-Adresse, als auch eine öffentliche IP-Adresse zugewiesen ist. NAT ist allerdings für Netzwerkverbindungen ohne Firewall nicht zu empfehlen.
Ein Netzwerkadressübersetzer ist ein IP-Router, der private IP-Adressen in externe, öffentliche IP-Adressen umwandelt. Somit ist die einzige IP-Adresse, die im Internet sichtbar ist, die IP-Adresse des Computers, auf dem NAT ausgeführt wird.

Funktionsweise von NAT:

Wenn ein Computer, auf dem NAT ausgeführt wird, ein Paket von einem internen Client erhält, wird der Paketheader ersetzt und die Anschlussnummer sowie die interne IP-Adresse des Clients in die NAT-Anschlussnummer und die externe IP-Adresse übersetzt. Anschließend sendet der Computer das Paket an den Zielhost im Internet und zeichnet die Zuordnungsinformationen in einer Tabelle auf, um die Antwort an den entsprechenden Clientcomputer weiterleiten zu können.
Wenn der Computer, auf dem NAT ausgeführt wird, eine Antwort vom Internethost erhält, ersetzt er wieder den Paketheader und sendet das Paket an den Client. Sowohl der Clientcomputer, als auch der Internethost erwecken somit den Anschein, direkt miteinander zu kommunizieren.

Vorteile von NAT:

- nur eine einzige Verbindung zum Internet erforderlich
- stellt DHCP-Dienste bereit
- ermöglicht allen über IP an das Intranet angeschlossenen Geräten die Kommunikation mit Computern im Internet ohne dass zusätzliche Clientsoftware erforderlich ist

Installieren von NAT:

Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf Server klicken → IP-Routing → mit rechter Maustaste auf Allgemein → Neues Routingprotokoll → Netzwerkadressübersetzung (NAT) → OK

Konfigurieren von NAT

Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf Server klicken → IP-Routing → mit rechter Maustaste auf Netzwerkadressübersetzung (NAT) → Eigenschaften

Im Eigenschaftendialogfeld können folgende Register ausgewählt werden:

Allgemein	Konfigurieren der Ereignisprotokollierung
Übersetzung	TCP-Zuordnung entfernen nach (Minuten) UDP-Zuordnung entfernen nach (Minuten) Standard zurücksetzen
Adresszuweisung	Konfigurieren des Computers mit NAT als DHCP-Server
Namensauflösung	Konfigurieren des Computers mit NAT als scheinbaren DNS-Server für Clients, der für diese Namen auflösen kann. (Wenn der Computer mit NAT eine DNS-Abfrage erhält, leitet er die Abfrage an einen DNS-Server und dann die von diesem DNS-Server erhaltene Antwort an den Client weiter)

Installieren der Routerschnittstelle für NAT:

Um NAT zu aktivieren, muss am Computer, der die Verbindung mit dem Internet herstellt, das NAT-Routingprotokoll hinzugefügt werden.

Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf Server klicken → IP-Routing → mit rechter Maustaste auf Netzwerkadressübersetzung (NAT) → Neue Schnittstelle → Neues Routingprotokoll für NAT → OK → Allgemein → im Dialogfeld „Eigenschaften von Eigenschaften der Netzwerkadressübersetzung“ eine Option auswählen → OK

Konfigurieren der Routerschnittstelle:

Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf Server klicken → IP-Routing → mit rechter Maustaste auf Netzwerkadressübersetzung (NAT) → Eigenschaften

Im Eigenschaftendialogfeld können folgende Register ausgewählt werden:

- Allgemein
- Adresspool
- Spezielle Ports

Herstellen einer Verbindung mit dem Internet bei gemeinsamer Nutzung der Internetverbindung:

Obwohl die gemeinsame Nutzung der Internetverbindung die gleiche Funktion wie NAT besitzt, bietet es jedoch nur äußerst geringen Konfigurationsspielraum. Auch ICS (Internet-Connection-Sharing) ist für Netzwerkverbindungen ohne Firewall nicht zu empfehlen. Diese Art der Verbindung eignet sich vor allem für kleine Netzwerke.

Herstellen einer Verbindung mit dem Internet mit Hilfe eines Proxyservers:

Ein Proxyserver (welcher in der Regel Zwischenspeicherung der Internet-informationen vornimmt) verwaltet den Verkehr zwischen dem Netzwerk und den Servern im Internet und bestimmt, ob Netzwerkpakete zum Netzwerk durchgelassen werden dürfen oder nicht. (Proxy=Cache+NAT+Firewall)

Vergleichen von Internetverbindungsoptionen:

- NAT bietet Netzwerksicherheit, die ein Router nicht bieten kann, andererseits ist NAT jedoch prozessorintensiver als Routing und unterstützt nicht alle Protokolle. Darüber hinaus übersetzt NAT in Windows2000 die IP-Adresse eines Computers nur im Paketheader, was die Verwendung von IPSec (Internet Protocol Security) verhindert.
- Ein Proxyserver muss alle Protokolle für Pakete, die er ins Internet weiterleitet, kennen. Dies ermöglicht es ihm Sicherheitsprüfungen durchzuführen. Die Clients müssen allerdings erst für die Verwendung eines Proxyservers (Browserkonfiguration) konfiguriert werden.
- Im Gegensatz zu NAT eignet sich die gemeinsame Verwendung der Internetverbindung aus folgenden nur für kleine Netzwerke, da:
    - sie einen festen IP-Adressbereich für interne Hosts erfordert
    - sie auf eine einzige öffentliche IP-Adresse für die Kommunikation mit externen Netzwerken begrenzt ist
    - sie nur eine einzige interne Netzwerkschnittstelle unterstützt

Unterrichtseinheit 12:

Konfigurieren eines Webservers

Erleichterung der Organisation und des Verwaltens von Webinhalten im Intranet und Internet.

Übersicht über IIS:

Der IIS-Dienst arbeitet mit folgenden Diensten zusammen:

- **WWW-Server (World Wide Web)**
- **FTP-Dienst (File Transfer Protocol)**
  Einrichten von FTP-Sites zum Up- und Download
- **NNTP-Dienst (Network News Transfer Protocol)**
  Unterstützung von elektronischen Diskussionsrunden oder Newsgroups
- **SMTP-Dienst (Simple Mail Transfer Protocol)**
  Empfang und Senden von E-Mail-Nachrichten über eine Clientanwendung

Vorbereitung einer IIS-Installation:

Folgende Netzwerkdienste müssen vor dem Installieren von IIS auf dem Windows2000 Server vorhanden sein:

1. **TCP/IP (Transmission Control Protocol / Internet Protocol)**
   Für das Übertragen von Daten notwendige Internetprotokoll
2. **Statische IP-Adresse (Internetprotokoll)**
   Für das Veröffentlichen von Inhalten im Internet muss eine statische IP-Adresse für den Server verwendet werden
3. **Domänenname**
   Für die Domänennamen müssen DNS-Server (Domain-Name-System) zur Verfügung stehen, um die Namen von Webservern aufzulösen
4. **NTFS**
   Zur Sicherheit wird empfohlen, alle Laufwerke, die Webinhalte enthalten mit NTFS zu formatieren

Installieren von IIS (Version 5.0):

Standardmäßig wird IIS bei der Installation von Windows 2000 automatisch installiert. Der Internetdienste-Manager wird zum Menü **Verwaltung** hinzugefügt .
Zum Testen der Installation ist es sinnvoll, den InternetExplorer zu verwenden.
Das *Basisverzeichnis* ist der zentrale Speicherort für die veröffentlichten Seiten. Das Standardbasisverzeichnis, welches IIS während er Installation erstellt, ist **C:\Inetpup\wwwroot.**

Um IIS von Hand zu installieren sind folgende Schritte notwendig:
Start → Einstellungen → Systemsteuerung → Software → Windows-Komponenten hinzufügen/entfernen → Internet-Informationsdienste (IIS) aktivieren

Konfigurieren einer Website:

Zum Konfigurieren der Standardwebsite müssen verschiedene Identifikationsparameter für die Website festgelegt werden; diese befinden sich im Internetdienste-Manager (mit der rechten Maustaste auf Eigenschaften klicken).

Beschreibung:	bestimmt den Namen der Website
IP-Adresse:	IP-Adresse der Website
TCP-Anschluss:	bestimmt den Anschluss auf dem der Webdienst ausgeführt wird → Standardmäßig Anschluss 80
SSL-Anschluss:	bestimmt den Anschluss für eine SSL-Verschlüsselung (Secure Socket Layer) → Standardmäßig Anschluss 443

Konfigurieren des Basisverzeichnisses

Das Basisverzeichnis (lokales Verzeichnis oder freigegebener Ordner) bestimmt den Speicherort des veröffentlichten Inhalts einer Site und kann im Dialogfeld **Eigenschaften** der Website auf der Registerkarte **Basisverzeichnis** zugewiesen werden.

Identifizierung von Authentifizierungsmetoden

Um unbefugten Zugriff auf die Website zu verhindern, muss die Identität von Benutzern durch eine Authentifizierung überprüft werden. IIS unterstützt vier Authentifizierungsmethoden zum Steuern des Zugriffs auf Inhalte auf dem Server:

- **Anonyme Anmeldung**
  Diese Standardeinstellung benötigt weder die Eingabe eines Benutzernamens, noch eines Kennwortes. Für die Verbindung ins WWW weist der Webserver den Benutzer dem Windows-Benutzerkonto namens IUSR_*Computername* (Benutzer der Gruppe **Gäste**) zu.

- **Standardauthentifizierung**
  Benötigt die Eingabe eines Benutzernamens und eines Kennwortes. Die Standardauthentifizierung kann auf Website-, Ordner- oder Dateiebene festgelegt werden. IIS kann so konfiguriert werden, dass eine bestimmte Domäne verwendet wird, wenn die Anmeldeinformationen eines Benutzers überprüft werden. Diese Art der Authentifizierung wird von den meisten Browsern unterstützt. Das Übertragen der Kennwörter erfolgt jedoch unverschlüsselt. Wenn die Übertragung der Benutzerkontoinformationen im Netzwerk gesichert werden soll, muss zusätzlich die SSL-Sicherheit verwenden werden.

- **Digestauthentifizierung**
  Steht nur Servern in einer Domäne mit Windows2000-Domänencontrollern zur Verfügung. Alle Benutzerkonten, die diese Authentifizierung verwenden, müssen im Active Directory Verzeichnisdienst mit der Kontooption **Kennwort mit reversibler Verschlüsselung speichern** konfiguriert werden.

- **Integrierte Windows-Authentifizierung**
  Statt der tatsächlichen Windows-Benutzerkonto- und Kennwortinformationen werden die Windows-Anmeldeinformationen des Clientcomputers verwendet.

Auswählen einer Authentifizierungsmethoden

Anonyme Anmeldung	Ermöglicht dem Benutzer den Zugriff auf den öffentliche Bereich einer Website
Standardauthentifizierung	Authentifizierung eines Benutzers, der über einen Browser oder Proxyserver zugreift
Digestauthentifizierung	sichere Authentifizierung einer Webseite; die Übertragung erfolgt über einen Proxyserver
Integrierte Windows-Authentifizierung	konfigurieren einer Internetseite, bei der sich die Benutzer und der Webserver in derselben Domäne, oder in Domänen mit gegenseitigen Vertrauensbeziehungen befinden

Auswählen mehrerer Authentifizierungsmethoden

Bei einer Kombination von anonymer Anmeldung und einer anderen Authentifizierungsmethode, hat die anonyme Anmeldung Vorrang. Die Vorrangreihenfolge lautet:

1. integrierte Windows-Authentifizierung
2. Digestauthentifizierung
3. Standardauthentifizierung.

Konfigurieren der Authentifizierungsmethoden

*Internetdienstemanager → mit rechter Maustaste auf **Eigenschaften** → Verzeichnissicherheit oder Datensicherheit → Steuerung des anonymen Zugriffs und der Authentifizierung → Bearbeiten → Authentifizierungsmethoden → **

Anonyme Anmeldung	Dem anonymen Konto muss das Benutzerrecht zum lokalen Anmelden erteilt werden. Standardmäßig wird den Konten **IUSR_*Computername*** dieses Recht erteilt. **→ *Anonyme Anmeldung → Bearbeiten → Anonymes Benutzerkonto → Durchsuchen → **Kennwortkontrolle durch IIS zulassen** deaktivieren, falls sich das Benutzerkonto auf einem anderen Rechner befindet*
Standardauthentifizierung	Zur Authentifizierung von Benutzern müssen die Windowsbenutzerkonten verwendet werden, die über das Benutzerrecht **Lokal anmelden** verfügen **→ **Integrierte Windows-Authentifizierung** deaktivieren → **Standardauthentifizierung** aktivieren → im **Internetdienste-Manger** auf **Ja** klicken → OK → OK*
Digestauthentifizierung	**→ **Digestauthentifizierung für Windows-Domänenserver** aktivieren → im **IIS-WWW-Konfiguration** auf **Ja** klicken → OK → OK*
Integrierten Windows-Authentifizierung	**→ **Integrierte Windows-Authentifizierung** aktivieren → OK → OK*

Zuweisen eines Standarddokuments

Es kann ein Standarddokument (index.htm) zugewiesen werden, sodass der Inhalt dieser Webseite auch dann dem Benutzer angezeigt wird, wenn eine Browseranforderung nicht einen bestimmten HTML-Dateinamen (Hypertext Markup Language) enthält.
Werden mehrere Standarddokumente zugewiesen, so durchsucht der Webserver die Liste der Standarddokumente in der Reihenfolge, in der die Namen angezeigt werden.

Verwalten von IIS

Um einen Webserver remote zu verwalten und die IIS-Leistung überwachen zu können wird folgende Datei benötigt: **adminpak.msi**. Diese befindet sich entweder auf der Windows2000 Server-CD im Verzeichnis **\i386**, oder auf einem Computer unter Windows2000 Server im Verzeichnis **%systemroot%\system32**. Die Installation kann auf einem beliebigen Windows 2000 Client erfolgen.

Überwachen von Internet-Informationsdienste

Um die IIS-Leistung zu überwachen, öffnet man im Menü **Verwaltung** den Systemmonitor, indem bei der Installation von IIS folgende Leistungsobjekte und Leistungsindikatoren hinzugefügt wurden:

- **Internet-Informationsdienste Global**
  enthält Leistungsindikatoren, die Bandbreitenbeschränkung und Verwendung des IIS-Objektcache (Größe, Inhalt und Effektivität) melden
- **WWW-Dienst**
  stellt Leistungsindikatoren bereit, die Daten über die Verbindungen zur HTTP-Dienstanwendung und HTTP-Anforderungen anzeigen
- **Active Server Pages**
  überwacht Anwendungen, die auf dem Webserver ausgeführt werden und Active Server Pages verwenden

Testen einer Website im Intranet

Die URL beginnt mit **http://** gefolgt vom Windows-Netzwerknamen des Servers und dem Pfad der Datei, die angezeigt werden soll.

Auflösen von IIS-Problemen

Wenn beim Testen einer Website diese nicht angezeigt werden kann, so muss die Fehlermeldung (ggf. mit Hilfe der Onlinedokumentation unter folgender Adresse **http://localhost/iishelp**) sorgfältig untersucht werden.

Unterrichtseinheit 13:

Bereitstellen von Windows 2000 Professional mit Hilfe von RIS

Die Remoteinstallationsdienste (Remote Installation Services, RIS) bilden die Grundlage der Windows2000-Remote-Betriebssysteminstallation. RIS vereinfacht die Bereitstellung von Windows2000 Professional innerhalb einer Organisation, ohne dass man hierzu physisch zu jedem Clientcomputer gehen muss.

RIS - Übersicht

RIS ermöglicht Clientcomputern, während der Anfangsstartphase eine Verbindung zu einem Server herzustellen um eine Remoteinstallation (nur von Windows2000 Professional) durchzuführen. Der Remoteinstallationsvorgang erhält drei Hauptkomponenten:

RIS-Server Auf diesen Servern befindet sich RIS, und man verteilt Windows2000 Professional an Clientcomputer, auf denen der Remotestart möglich ist. Bei RIS-Servern handelte es sich entweder um Domänencontroller oder Mitgliedsserver einer Windows2000-Domäne.

RIS-Clientcomputer Beim Start können RIS-Clientcomputer eine Verbindung zu einem RIS-Server herstellen um eine Wartung oder Remoteinstallation durchzuführen.

Abbilder Diese repräsentieren die Betriebssystemkonfiguration, die auf Clientcomputern installiert werden können. Es werden der CD-basierte- und der RIPrep-Abbilder unterstützt.

Identifizieren der RIS-Anforderungen

Für die Installation von RIS müssen verschiedene Bedingungen erfüllt sein:

Netzwerkanforderungen

- DHCP-Server-Dienst
- Active Directory
- DNS-Server-Dienst

Clientanforderungen

- Hardwareanforderungen für Windows2000 Professional
- Fähigkeit, vom Netzwerk zu starten
- PXE-Start-ROM Version .99c

Serveranforderungen

- Mindestens 2 GB Gesamtspeicherplatz (Festplatte muss über mindestens 2 Partitionen bei einer Basisfestplatte, oder 2 Datenträger bei einer dynamischen Festplatte verfügen)
- Abbilder gespeichert auf NTFS-Partition

Wichtig:
Um die Leistung beim Kopieren der Abbilddateien zu erhöhen, sollten diese auf einer Partition oder einem Datenträger auf einer gesonderten Festplatte oder einer Laufwerkgruppe platziert werden.

Installieren und Starten von RIS

Einstellungen ⇒ Systemsteuerung ⇒ Software ⇒ Windows-Komponenten hinzufügen/entfernen ⇒ das Kontrollkästchen „Remoteinstallationsdienste“ aktivieren ⇒ Weiter

Wichtig:
Der RIS-Server sollte im selben Teilnetz wie die Clientcomputer, für die er als Server fungieren soll, platziert werden, da hierdurch die Installationsleistung verbessert und der Umfang des RIS-bezogenen Netzwerkverkehrs begrenzt wird.

Nach der Installation von RIS muss der Assistent zur Installation der Remote-installationsdienste ausgeführt werden.
Start ⇒ Ausführen ⇒ ***risetup*** *⇒ OK*

Hier müssen eine Reihe von Informationen angegeben werden:

Remoteinstallationsordner	nicht verschlüsseltes NTFS-Dateisystem
Anfangseinstellungen	standardmäßig ist das Kontrollkästchen **Auf Dienstanfragen von Clients antworten** deaktiviert, somit antwortet der Server nicht auf Clientanforderungen
Pfad der Installationsquelldateien	auch wenn Benutzern nur RIPrep-Abbilder zur Verfügung gestellt werden sollen, muss ein erstes CD-basiertes Abbild erstellt werden, bevor RIS gestartet werden kann
Name des Windows-Installationsabbildordners	Ordner innerhalb des RIS-Installationsordners auf dem RIS-Server, indem das erste CD-basierte Abbild erstellt wird
Beschreibung und Hilfetext	wird angezeigt, wenn sich der Benutzer am RIS-Server anmeldet und dieses Abbild aus der Liste auswählt

Nachdem der Assistent zur Installation der Remoteinstallationsdienste abgeschlossen ist, führt Windows2000 automatisch folgende Tasks aus:

- Erstellen einer RIS-Ordnerstruktur
- Kopieren der Unterstützungsdateien auf den Server
- Erstellen des ersten CD-basierten Abbilds von Windows2000 Professional und der Standardantwortdatei
- Starten der erforderlichen Dienste auf dem RIS-Server

Autorisieren des RIS-Servers

Der RIS-Server muss im Active Directory (genau so wie ein DHCP-Server in der DHCP-Konsole) autorisiert werden.

Programme ⇒ Verwaltung ⇒ rechte Maustaste auf DHCP ⇒ Autorisierte Server verwalten ⇒ Autorisieren ⇒ OK

Wichtig:
Um einen DHCP- oder RIS-Server zu autorisieren, muss ein Benutzer Mitglied der Gruppe ***Organisations-Admins*** *sein, die in der Stammdomäne der Gesamtstruktur vorhanden ist.*

Zuweisen von Benutzerberechtigungen

Die Benutzerberechtigung zum Erstellen von Computerkonten im Active Directory wird folgendermaßen zugewiesen:

Programme ⇒ Verwaltung ⇒ Active Directory-Benutzer und -Computer ⇒ mit rechter Maustaste auf die entsprechende Domäne oder Organisationseinheit klicken ⇒ Objektverwaltung zuweisen ⇒ Weiter ⇒ Benutzer oder Gruppen ⇒ Hinzufügen ⇒ Benutzer, Computer oder ‚Gruppen auswählen ⇒ Benutzer auswählen ⇒ Hinzufügen ⇒ OK ⇒ Weiter ⇒ Zuzuweisende Aufgaben ⇒ Benutzerdefinierte Aufgaben zum Zuweisen erstellen ⇒ Weiter ⇒ Active Directory-Objekttyp ⇒ Zuweisen der Verwaltung von ⇒ Diesem Ordner, bestehenden Objekten in diesem Ordner und dem Erstellen neuer Objekte in diesem Ordner ⇒ Weiter ⇒ Berechtigungen ⇒ Diese Berechtigungen anzeigen ⇒ Kontrollkäschen „Erstellen/Löschen der Berechtigungen von bestimmten untergeordneten Objekten“ aktivieren ⇒ Kontrollkästchen „Computer-Objekte erstellen“ aktivieren ⇒ Weiter ⇒ Fertigstellen des Assistenten ⇒ Fertig stellen

Wichtig:
Standardmäßig verfügt jedes Benutzerkonto über das Recht, bis zu 10 Computerkonten in Active Directory zu erstellen. Benutzern müssen nur die Berechtigungen zum Erstellen von Benutzerkonten erteilt werden, wenn das standardmäßige Recht entfernt wurde, oder ein Benutzer mehr als 10 Computerkonten erstellen muss.

Konfigurieren von Clientcomputernamen und Pfaden

Namensformat für Clientcomputer

Programme ⇒ Verwaltung ⇒ Active Directory-Benutzer und -Computer ⇒ mit rechter Maustaste auf „Eigenschaften“ des entsprechenden RIS-Servers klicken ⇒ Remoteinstallation ⇒ Erweiterte Einstellungen ⇒ Eigenschaften von <Servername>-Remoteinstallationsdienste ⇒ Neue Clients ⇒ Anpassen

Standardmäßig benennt RIS Computer nach dem Benutzer, der die Remoteinstallation durchführt. Es kann ein beliebiger alphanumerischer Text (max 64 Zeichen) als Teil des Namensformat verwendet werden, außerdem kann man auch unter folgenden Variablen auswählen:
%Username (Benutzer)
%First (Vorname)
%Last (Nachname)
%# (Inkrementelle Nummer)
%MAC (MAC-Adresse des Netzwerkadapters)

Folgende Tabelle beschreibt die Optionen, die für das Einrichten von Speicherorten für Computerkonten verfügbar sind:

Standardstelle im Verzeichnis-dienst	erstellt neue Computerkonten im Container Computer
An derselben Stelle wie die Benutzereinstellungen des Computers	erstellt neue Computerkonten in derselben Organisationseinheit, in der sich auch das Benutzerkonto der Person befindet, die die Remoteinstallation durchführt
Folgende Verzeichnisdienststelle	erstellt neue Computerkonten in der Organisationseinheit die manuell angegeben werden

Einrichten von Vorstufen-Clientcomputern

Ermitteln einer GUID (Global Unique Identifier)

Bevor ein Vorstufen-Clientcomputer eingerichtet werden kann, muss die GUID (Teil der PXE-Spezifikation) des Computers bekannt sein.
Bei Computern, die von einer RIS-Startdiskette gestartet werden, ist die GUID (muss 32 Zeichen lang sein) die MAC-Adresse des Netzwerkadapters.

Um die Installationsoptionen zu konfigurieren, können Gruppenrichtlinien, welche aus einer Reihe von Benutzerumgebungseinstellungen bestehen verwendet werden.
Besteht ein Konflikt zwischen den Gruppenrichtlinieneinstellungen, setzt das Gruppenrichtlinienobjekt, das auf der Organisationseinheitsebene erstellt wurde, das Gruppenrichtlinienobjekt, das auf der Domänenebene erstellt wurde, außer Kraft.

Benutzer können Dienstprogramme zur Wartung und Problembehandlung verwenden, die von unabhängigen Softwareherstellern (Independet Software Vendors, ISVs) und OEMs (Original Equipment Manufacturers) bereitgestellt werden.

Bereitstellen von Abbildern mit Hilfe von RIS

Der Vorgang für das Bereitstellen von Abbildern beinhaltet folgende Verfahren:

- **Ändern der Installation eines CD-basierten Abbilds**
  Ein CD-basiertes Abbild ist ein Abbild des Betriebssystems und der zugehörigen Standardeinstellungen. Wird RIS installiert, so werden ein CD-basiertes Abbild und eine Standardantwortdatei (***Ristndrd.sif***), welche nach der Erstellung manuell konfiguriert werden kann, erstellt.
- **Zuordnen einer Antwortdatei zu einem Abbild**
  Eine Antwortdatei ist eine Textdatei (gleiche Format wie **Unattende.doc**), die Informationen enthält, welche der Benutzer normalerweise während der Installation eingeben müsste.
- **Beschränken von Abbildern**
  Standardmäßig stehen alle Abbilder allen Benutzern zur Verfügung, was allerdings durch Einschränkungen in der NTFS-Berechtigung geändert werden kann.
- **Erstellen einer RIS-Startdiskette**
  Die RIS-Startdiskette (erstellt mit dem Dienstprogramm ***Rbfg.exe***) simuliert den PXE-Startvorgang bei Computern mit Netzwerkadaptern, die PXE nicht unterstützen.
- **Installieren eines Abbilds auf einem RIS-Clientcomputer**
  Um eine Remoteinstallation auf einem Clientcomputer durchzuführen, müssen die Benutzer einen Netzwerkdienst-Start anfordern, indem Sie nach dem Einschalten des Computers ***F12*** drücken oder ihre Computer mit der RIS-Startdiskette starten.

Erstellen eines RIPrep-Abbilds

Werden Anwendungen zusammen mit dem Betriebssystem bereitgestellt, muss der RIPrep-Abbilder, welcher einen Quellcomputer und einen RIS-Server benötigt, verwendet werden.

Einrichten eines Quellcomputers

1. Installieren von Windows 2000 Professional
2. Konfigurieren von Komponenten und Einstellungen
3. Installieren und Konfigurieren von Anwendungen
4. Testen der Konfiguration von Betriebssystem und Anwendungen

Ändern des Standardbenutzerprofils

Wenn ein RIPrep-Abbild erstellt wird, werden alle vorgenommenen Änderungen im Administratorprofil aufgezeichnet. Somit erhalten nur die Benutzer, die sich als Administrator anmelden, Ihre angepasste Konfiguration, alle anderen erhalten das Standardbenutzerprofil.
Um aber alle angepassten Einstellungen für jeden Benutzer verfügbar zu machen, der sich an einem Computer anmeldet, welcher mit RIPrep-Abbild konfiguriert wurde, muss das Administratorprofil in das Standardbenutzerprofil auf dem Quellcomputer kopiert werden, bevor der Assistent zur Vorbereitung der Remoteinstallation ausgeführt wird.

mit rechter Maustaste auf „Arbeitsplatz" klicken ⇒ Eigenschaften ⇒ Systemeigenschaften ⇒ Benutzerprofile ⇒ Auf diesem Computer gespeicherte Profile ⇒ lokale Administratorprofil auswählen ⇒ Kopieren nach ⇒ im Textfeld „Pfad kopieren nach" den Pfad für den Standardbenutzerordner (C:\Dokumente und Einstellungen\Default User) eingeben ⇒ Ändern ⇒ Benutzer oder Gruppe auswählen ⇒ Suchen in ⇒ Jeder ⇒ OK ⇒ OK

Erstellen eines RIPrep-Abbilds

Nachdem die Konfiguration des Quellcomputers abgeschlossen ist, wird das Abbild mit Hilfe des Assistenten erstellt. Dieser Assistent führt folgende Aktionen aus:

- Entfernen aller eindeutigen Sicherheitskennungen (SID, Computernamen, Registrierungseinstellungen) vom Quellcomputer
- Erstellen des RIPrep-Abbildes auf der angegebenen RIS-Serverabbildpartition
- Erstellen und Zuordnen einer Antwortdatei für das neu erstellte RIPrep-Abbild

*Start ⇒ Ausführen ⇒ Feld Öffnen (**\\RIS-Server\reminst\admin\i386\riprep.exe**) ⇒ OK ⇒ Konfigurieren nachfolgender Optionen (Servername, Ordnername, Beschreibung und Hilfetext)*

Vergleichen von CD-basierten Abbildern und RIPrep-Abbildern

Merkmale CD-basierte Abbilder

- Bei der Installation von RIS-Servern wird automatisch ein Standardabbild erstellt
- Das Abbild kann nur das Betriebssystem enthalten
- Das Abbild basiert auf den Standardeinstellungen des Betriebssystems; eine Antwortdatei ist erforderlich, um das Abbild anzupassen
- Installation wir ausschließlich über das Netzwerk durchgeführt
- Abbild kann auf jedem Computer mit einer unterstützten Hardwareabstraktionsschicht (HAL) bereitgestellt werden

Merkmale RIPrep-Abbilder

- RIPrep-Abbilder müssen mit Hilfe eines Assistenten erstellt werden
- Das Abbild kann sowohl das Betriebssystem als auch Anwendungen enthalten
- Abbild basiert auf einen vorkonfigurierten Quellcomputer (zum Ändern muss das Abbild auf einen Clintcomputer bereitgestellt und konfiguriert werden)
- Kopiert nur die erforderlichen Dateien und Registrierungsschlüssel auf den Clientcomputer
- Abbild kann auf jedem Computer mit derselben HAL wie die des Quellcomputers bereitgestellt werden

Unterrichtseinheit 14:

Verwalten eines Windows2000-Netzwerkes

Windows2000 bietet bei der Verwaltung des Netzwerkes sehr große Flexibilität. Es stellt unter anderem die folgenden Tools und Methoden bereit:

- Terminaldienste
- SNMP
- SNMP-Dienst

Terminaldienste

Mit Hilfe der Terminaldienste kann man interaktive Sitzungen auf einem Remoteserver starten und den Server von einem Clientcomputer aus verwalten. Der Desktop des Servers wird in einem Fenster auf dem Desktop des lokalen Computers angezeigt. Der Terminaldiensteclient sendet Tastenanschläge und Mausbewegungen an den Terminalserver und empfängt Bildschirmaktualisierungen vom Server.

Um die Terminaldienste für Remoteverwaltung verwenden zu können, muss der Computer über folgende Systemanforderungen verfügen:

- Windows2000 Server-Betriebssystem
- Terminaldienste auf dem Server und dem Clientcomputer installieren
- genügend großer Arbeitsspeicher (jede aktive Sitzung erfordert ca. 16MB RAM auf dem Server zuzüglich Programmressourcen)

Remoteverwaltungsmodus

Die Merkmale dieses Modus sind folgende:

- die Terminaldienste sind auf zwei gleichzeitige Verbindungen beschränkt
- zwei Terminaldienstelizenzen sind enthalten
- die Leistung der Terminaldienste ist für eine geringe Anzahl an Verbindungen optimiert
- für die Terminaldienste sind strengere Sicherheitseinstellungen als im Anwendungsservermodus konfiguriert
- standardmäßig haben nur die Mitglieder der Gruppe **Administratoren** die Berechtigungen zum Verbinden mit dem Remotecomputer

Zum Installieren der Terminaldienste sind folgende Schritte notwendig:
*Systemsteuerung → Software → Windows-Komponenten hinzufügen/entfernen → Windows-Komponenten → aktivieren des Kontrollkästchens **Terminaldienste** → Setup der Terminaldienste → Remoteverwaltungsmodus → Weiter → Fertig stellen → Ja*

Leistungsparameter, um die Leistung der Terminaldienstesitzung zu verbessern können wie folgt konfiguriert werden:
Systemsteuerung → System → Erweitert → Systemeigenschaften → Systemleistungsoptionen → Systemleistung optimieren für → Hintergrunddienste

Zum Optimieren der Ressourcenverfügbarkeit sollten die maximale Leerlaufdauer auf 10 Minuten und das Zeitlimit zum Beenden einer getrennten Sitzung auf 5 Minuten festgelegt werden.
*Programme → Verwaltung → Terminaldienstekonfiguration → Sitzungen → Eigenschaften von RDP-Tcp → aktivieren von **Benutzereinstellungen überschreiben** → **Maximale Leerlaufdauer** auf **10 Minuten** und **Getrennte Sitzung beenden** auf **5 Minuten** einstellen*

Der Administratorzugriff (Sicherheitsparameter) kann wie folgt konfiguriert werden:
*Programme → Verwaltung → Terminaldienstekonfiguration → Verbindungen → mit rechter Maustaste auf **RDP-Tcp** klicken → Eigenschaften → Berechtigungen → nur Gruppen ausgewählter Administratoren die Berechtigung Vollzugriff zuweisen → alle anderen Benutzerkonten und –gruppen (ausgenommen **System**) aus dem Feld **Name** entfernen*

Terminaldienstedaten werden in 3 Stufen verschlüsselt (Voraussetzung ist die vorherige Installation des Windows2000-128Bit-Verschlüsselungs-Pack):
*Programme → Verwaltung → Terminaldienstekonfiguration → Verbindungen → mit rechter Maustaste auf **RDP-Tcp** klicken → Eigenschaften → Allgemein → Hoch*

SNMP-Betrieb

SNMP (Simple Network Management Protocol) ist ein Tool zur Netzwerkverwaltung nach Industriestandard, mit dem Netzwerkknoten (Server, Arbeitsstationen, Router, Brücken und Hubs) von einem zentralen Host verwaltet werden können.
Es ermöglicht die Überwachung von Netzwerkgeräten und das Kommunizieren von Statusinformationen zwischen diesen.
SNMP verwendet eine verteilte Architektur, welche aus den beiden Komponenten „Verwaltungssystemen“ und „Agents“ besteht.

Um Informationen eines SNMP-Verwaltungssystems anzufordern stehen vier Befehlsoptionen zur Verfügung:

get	fordert einen bestimmten Wert an
get-next	fordert den nächsten Wert an
get-bulk	fordert eine große Menge von Verwaltungsdaten an
set	ändert einen Wert

Beim Auftreten eines ungewöhnlichen Ereignisses werden vom Agent Verwaltungsoperationen (Trap-Nachrichten) an die Systeme gesandt. Diese Trap-Nachrichten sind die einzigen Verwaltungsoperationen, die ein Agent initiieren kann.

Windows2000-SNMP-Dienst

Für den Windows2000-SNMP-Dienst gilt Folgendes:

- er protokolliert bei Auftreten bestimmter Ereignisse Trap-Nachrichten, die er an einen oder mehrere Hosts sendet
- er behandelt Anforderungen für Statusinformationen von SNMP-Verwaltungssystemen
- er kann auf einem beliebigen Computer unter Windows2000 mit TCP/IP oder IPX/SPX installiert und verwendet werden
- er verwendet Hostnamen und IP-Adressen zum Identifizieren der Hosts, an die Informationen gesendet und von denen Anforderungen empfangen werden

Windows2000 erzeugt in folgenden Fällen Traps:

- ein Verwaltungssystem versucht, mit Hilfe eines ungültigen Communitynames eine Verbindung zu einem Agent herzustellen
- ein Verwaltungssystem versucht, von einem nicht autorisierten Host aus eine Verbindung zu einem Agent herzustellen

MIB

Eine MIB (Management Information Base) definiert, welche Daten ein Verwaltungssystem von einem Agent anfordern kann, wie das Verwaltungssystem die Daten anfordern muss und wie der Agent die Informationen formatiert, die er zurückgibt. SNMP-Verwaltungssysteme und –Agents können nur miteinander kommunizieren, wenn Sie das gleiche Wissen über MIB-Objekte (Internet-MIB II, Lan Manager-MIB II, DHCP-MIB, WINS-MIB) haben.

Hierarchische Namensstruktur

Der Namensraum für MIB-Objekte ist hierarchisch strukturiert; jedem verwaltbaren Objekt wird ein globaler eindeutiger Name zugewiesen.
Die Objektkennung wird in der Hierarchie als Sequenz von Bezeichnungen (welche durch Punkte voneinander getrennt werden – siehe Kapitel 15/Seite 17) dargestellt, die mit dem Stamm beginnen und beim Objekt enden.

Definieren von SNMP-Communities

SNMP-Agents und Verwaltungssysteme gehören Gruppen (Communities), welche eine einfache Sicherheits- und Kontextüberprüfung für diese bereitstellt, an.
Nur Agents (können auch Mitglied mehrerer Communities sein) und Verwaltungssysteme, die Mitglied derselben Community sind, können miteinander kommunizieren.
Die Standardcommunity ist **public**, welcher allerdings bei Verwendung in einen anderen Namen geändert werden sollte, um Sicherheitsprobleme zu vermeiden.

Installieren des SNMP-Dienstes

Einstellungen → Systemsteuerung → Software → Windows-Komponenten hinzufügen/entfernen → das Kontrollkästchen „Verwaltungs- und Überwachungsprogramme“ aktivieren → Details → das Kontrollkästchen „SNMP (Simple Network Management Protocol)“ aktivieren → OK → Windows-Komponenten → Weiter → Fertig stellen

Konfigurieren von Sicherheit für Agent-SNMP-Dienst

Programme → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → mit rechter Maustaste auf „SNMP-Dienst“ klicken → Eigenschaften → Sicherheit → Konfigurieren von „Authentifizierungstrap senden“, „Angenommene Communitynamen“, SNMP-Pakete von jedem Host annehmen“ und „SNMP-Pakete von diesem Host annehmen“

Konfigurieren von SNMP-Agent-Eigenschaften

Programme → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → mit rechter Maustaste auf „SNMP-Dienst“ klicken → Eigenschaften → Agent → Felder ausfüllen → Dienst → Kontrollkästchen für die Diensttypen aktivieren → OK

Um die Kommunikation des SNMP-Dienstes zu überprüfen, stellt Windows2000 im Server-Resource-Kit das Dienstprogramm **SNMPUTIL** bereit.

Syntax: **snmputil** *Befehl Community Objektkennung_(OID)*

Es gibt drei SNMPTUIL-Befehle: **get**, **get-next**, **walk**.

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
```

Unterrichtseinheit 16:

Konfigurieren von Netzwerkverbindungen unter unterschiedlichen Betriebssystemen

Windows2000 Server unterstützt die Interoperabilität mit Novell NetWare, Macintosh, IBM-Hosts und UNIX, da es die Migrationspfade von beliebig vielen vorhandenen Systemen, Geräten und Anwendungen bereitstellt.

Zugriff auf NetWare-Ressourcen:

Gateway Service für NetWare (abhängig von NWLink) fungiert als Gateway zwischen dem SMB (Server Message Block) bzw. dem CIFS (Common Internet File System) in Windows-Netzwerken und dem NCP (NetWare Core Protocol) in NetWare-Netzwerken.

Bevor das Gateway Service für NetWare auf einem Windows2000 basiertem Server installiert werden kann, müssen Benutzer- (gleicher Name und Kennwort wie unter Windows2000) und Gruppenkonten (mit dem Namen **NTGateway**) für das Gateway auf dem NetWare-Server erstellt werden.

Installation des Gatway-Service:

Netzwerk- und DFÜ-Verbindungen → mit rechter Maustaste auf die LAN-Verbindung für das Netzwerk klicken → Eigenschaften → Allgemein → Installieren → Typ der Netzwerkkomponente auswählen → Client → Hinzufügen → Netzwerkclient wählen → Gateway (und Client) Services für NetWare → OK

Anmerkung:
Um Gateway-Service für NetWare installieren zu können muss man Mitglied der Gruppe ***Administratoren*** *sein.*

Konfiguration des Gatway-Service:

Einstellungen → Systemsteuerung → GSNW → Gateway Service für NetWare → Gateway → Gateway konfigurieren → „Gateway aktivieren" anklicken → Namen und Kennwort (muss mit dem Kennwort des Benutzerkontos übereinstimmen) eingeben → OK

Services for NetWare ist ein eigenständiges Produkt, das Interoperabilitätsdienste und –tools enthält, mit denen eine vorhandene NetWare-Umgebung in ein Windows2000 Netzwerk integriert werden kann.
Folgende Dienstprogramme sind darin enthalten:

- Microsoft Directory Synchronization Services
- Microsoft File Migration Utility
- File and Print Services for NetWare

Zugriff auf Windows2000-Ressourcen für Macintosh-Benutzer:

Mit folgenden Diensten der AppleTalk-Netzwerkintegration kann ein zugreifbarer Datenträger auf einem Windows2000-Server (Vorraussetzung: NTFS-Partition) erstellt werden:

- Dateidienste für Macintosh (gemeinsame Dateinutzung)
- Druckdienste für Macintosh (gemeinsame Druckerspoolnutzung)
- AppleTalk-Protokoll (Netzwerkprotokolle unter Windows2000)

Installation der Datei- und Druckdienste für Macintosh:
Einstellungen → Systemsteuerung → Software → Windows-Komponenten hinzufügen/entfernen → Windows-Komponenten → Weitere Datei- und Druckdienste für das Netzwerk → Details → Weitere Datei- und Druckdienste für das Netzwerk → „Druckdienste für Macintosh“ oder „Dateidienste für Macintosh“ (oder beide) aktivieren → OK → Weiter → Fertig stellen

Konfiguration der Dateidienste für Macintosh:
Programme → Verwaltung → Computerverwaltung → Freigegebene Ordner → mit rechter Maustaste auf „Freigaben“ klicken → Neue Dateifreigabe → Freigabe erstellen → die nachfolgenden Felder bearbeiten → Folgende Clients haben Zugriff → Kontrollkästchen „Microsoft Windows“ und „Apple Macintosh“ aktivieren → „Macintosh-Freigabenamen“ eingeben → Weiter → Fertig stellen

Konfiguration der Druckdienste für Macintosh:
Programme → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → SFM-Druck-Server → Eigenschaften von SFM-Druck-Server → Anmelden → Dieses Konto → Namen und Kennwort eingeben → OK

Herstellen einer Verbindung zu SNA-Hosts mit Hilfe von MS Host Integration Server2000:

Host Integration Server2000 (früher SNA Server) ist ein eigenständiges Produkt von Microsoft BackOffice, das Windows2000-Clients und –Server das Herstellen einer Verbindung zu IBM-Hostsystemen (SNA-Hosts) über Standard-Netzwerkprotokolle ermöglicht.
Es stehen zwei Verbindungstypen zur Verfügung:

- die Physischen und logischen Verbindungen zur Host Integration Server2000-Umgebung
- die Client/Server-Netzwerkverbindungen zu den Nicht-SNA-Systemen im LAN oder WAN, wie PC`s oder Serveranwendungen, die Zugriff auf Anwendungen unter Host Integration Server2000 benötigen

Herstellen von Verbindungen zu UNIX-Ressourcen

Da UNIX NFS (Network File System) und Windows2000 CIFS verwendet, muss das Dienstprogramm Windows-Services-for-UNIX 2.0 auf den Windows2000 Rechner aufgespielt werden, um diesen mit UNIX zu integrieren.
Dieses Dienstprogramm bietet folgende Vorteile:

- es ermöglicht das gemeinsame Nutzen von Netzwerkressourcen durch Systeme unter WindowsNT, Windows2000 und UNIX
- es bietet eine Zusammenstellung von UNIX-Dienstprogrammen, sodass UNIX-Benutzer und – Administratoren mit ihren gewohnten Tools arbeiten können
- es vereinfacht die Netzwerkadministration sowohl lokal, als auch remote und unterstützt die Verwaltung genauso über die Befehlszeile, wie auch die grafische Oberfläche
- es kann UNIX- und Windows-Konten unter Windows2000 konsolidieren und die Kontenverwaltung zentralisieren und synchronisieren