Unterrichtseinheit 3:

Implementieren der Namensauflösung mit Hilfe von DNS

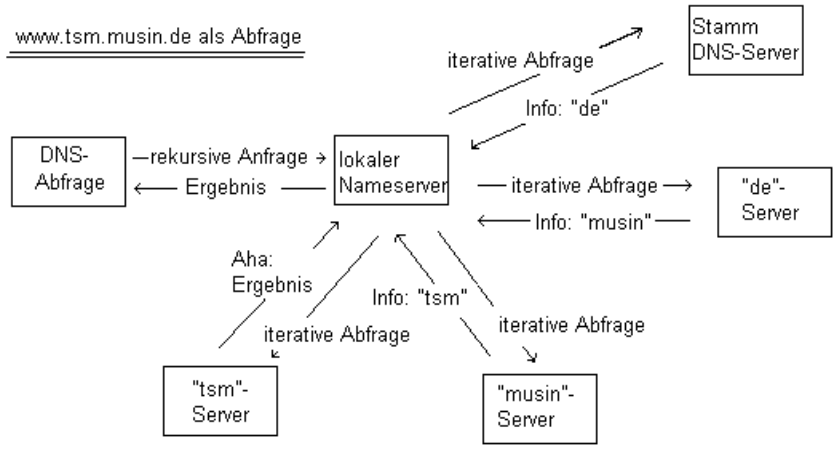
DNS (Domain Name System) ist ein integraler Bestandteil (verteilte Datenbank zum Übersetzen von Computernamen in IP-Adressen) der Client/Server-Kommunikation in IP-Netzwerken.

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)