Version 7

# DB2-Konnektivität - Ergänzung

*Version 7*

SDB2-CONN-SU

# DB2-Konnektivität - Ergänzung

*Version 7*

SDB2-CONN-SU

**Hinweis**

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die allgemeinen Informationen unter „Anhang B. Bemerkungen” auf Seite 203 gelesen werden.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
*IBM DB2 Connectivity Supplement*,
IBM Form CONN-SUPP,

herausgegeben von International Business Machines Corporation, USA



Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW NLS Center
Kst. 2877
April 2000

# Inhaltsverzeichnis

# Willkommen bei ″Konnektivität - Ergänzung″!

Dieses Handbuch enthält zusätzliche Informationen zur Installation und Konfiguration verschiedener DB2-Verwaltungssystemprodukte für relationale Datenbanken für DRDA-Anwendungs-Requester oder Anwendungs-Server. Diese Informationen sollen Ihnen die Konfiguration folgender Systeme erleichtern:

- Server unter IBM DB2 Universal Database (UDB) Version 7, die als DRDA-Anwendungs-Server (AS) ausgeführt werden
- Anwendungs-Requester (AR) unter IBM DB2 Connect Version 7
- Andere DRDA-konforme Produkte

Die in diesem Handbuch enthaltenen Informationen dienen als Ergänzung zu den Informationen in den folgenden Handbüchern:

- *Einstieg* für DB2 Universal Database Enterprise Edition Version 7
- *Einstieg* für DB2 Universal Database Enterprise - Extended Edition Version 7
- *Einstieg* für DB2 Connect Enterprise Edition Version 7
- *Einstieg* für DB2 Connect Personal Edition Version 7.

Die neuesten Informationen zu den Host-Produkten (DB2 Universal Database für OS/390, DB2 Universal Database für AS/400 und DB2 für VSE & VM) finden Sie in der mit diesen Produkten ausgelieferten Dokumentation.

Informationen zum Konfigurieren des Synchronisationspunktmanagers (SPM) für Aktualisierungen auf mehreren Systemen finden Sie im Handbuch *Installation und Konfiguration: Ergänzung*.

## Aufbau dieses Handbuchs

Dieses Handbuch ist wie folgt strukturiert:

- „Kapitel 6. Verbinden von DB2 für VSE & VM in einem DRDA-Netzwerk” auf Seite 133
- „Anhang A. Häufige Verbindungsprobleme” auf Seite 191
- „Anhang B. Bemerkungen” auf Seite 203

## Zielgruppe

Dieses Handbuch richtet sich an alle Personen, die DB2 Universal Database oder DB2 Connect installiert haben und mehr über Konnektivität bezüglich der im vorigen Abschnitt aufgelisteten Themen wissen möchten.

## Weitere Informationsquellen

In diesem Abschnitt werden weitere nützliche Informationsquellen aufgeführt.

### World Wide Web

Sie können die aktuellsten Informationen zu DB2 Connect, DB2 Universal Database und anderen IBM Softwareprodukten im World Wide Web abrufen. Hierzu gehören die neuesten Veröffentlichungen sowie technische Tips und Anweisungen in der Form von technischen Hinweisen. Führen Sie folgende Schritte aus, um diese Informationen im World Wide Web zu finden:

1. Zeigen Sie in Ihrem Web-Browser die folgende URL-Adresse an:

   `http://www.ibm.com/software/data/db2/library/`

2. Wählen Sie “DB2 Universal Database” aus.
3. Sie können z. B. mit dem Schlüsselwort “DDCS”, “DRDA” oder “Connect” nach “Technotes” (technischen Hinweisen) suchen.

### Zugehörige DRDA-Veröffentlichungen

Die folgenden Veröffentlichungen enthalten Referenzinformationen und werden möglicherweise im vorliegenden Handbuch erwähnt.

| IBM Form | Buchtitel |
|---|---|
| SC26-4783 | *Distributed Relational Database Architecture Connectivity Guide* |
| SC26-4773 | *Distributed Relational Database Architecture Application Programming Guide* |
| SC26-4782 | *Distributed Relational Database Architecture Problem Determination Guide* |
| SC26-4650 | *Planning for Distributed Relational Database Architecture* |
| GC26-3195 | *Distributed Relational Database Architecture Every Manager’s Guide* |

| IBM Form | Buchtitel |
|---|---|
| G321-5482 | *IBM Distributed Data Management Architecture Level 3: Reference* |

## Veröffentlichungen über DRDA-Server

Zu den Veröffentlichungen über DRDA-Server zählen folgende Handbücher aus den Bibliotheken für DB2 Universal Database für AS/400, DB2 für OS/390 und DB2 für VSE & VM.

| IBM Form | Buchtitel |
|---|---|
| SC41-5702 | *AS/400 Distributed Database Programming* |
| SC41-9609 | *AS/400 SAA Structured Query Language/400 Programmer's Guide* |
| SC41-9608 | *AS/400 SAA Structured Query Language/400 Reference* |
| GC21-8180 | *AS/400 Communications Configuration Reference* |
| SC26-8958 | *DB2 for OS/390 Application Programming and SQL Reference* |
| SC26-8960 | *DB2 for OS/390 Command Reference* |
| GC26-8970 | *DB2 for OS/390 Installation Reference* |
| SC26-8964 | *DB2 for OS/390 Reference for Remote DRDA Requesters and Servers* |
| SC26-8966 | *DB2 for OS/390 SQL Reference* |
| SC26-8957 | *DB2 for OS/390 Administration Guide* |
| SC26-8967 | *DB2 for OS/390 Utility Guide and Reference* |
| SH09-8087 | *DB2 for VSE & VM SQL Reference* |
| SC26-3255 | *IBM SQL Reference* |

## Weitere Referenzliteratur

| IBM Form | Buchtitel |
|---|---|
| SG24-2006 | *Migrating to DB2 Universal Database Version 5* |
| SG24-2213 | *DB2 for OS/390 Version 5 Performance Topics* |
| SG24-4893 | *DB2 Meets NT* |
| SG24-4894 | *The Universal Connectivity Guide to DB2* |
| SG24-4693 | *Getting Started with DB2 Stored Procedures* |

| IBM Form | Buchtitel |
|---|---|
| SG24-2212 | *DRDA Support for TCP/IP in DB2 for OS/390 V5.1 and DB2 Universal Database V5.0* |
| SC33-0814 | *CICS for AIX Application Programming Guide* |
| SC33-0931 | *CICS for AIX Customization and Operation Guide* |
| GC12-2862-00 | *DB2 Connect Enterprise Edition für UNIX Einstieg* |
| GC12-2863-00 | *DB2 Connect Enterprise Edition für OS/2 und Windows Einstieg* |
| GC12-2869-00 | *DB2 Connect Personal Edition Einstieg* |
| GG24-4155 | *Distributed Relational Database Architecture: Using DDCS for AIX DRDA support with DB2 for MVS/ESA and DB2 Universal Database für AS/400* |
| GG24-4311 | *Distributed Relational Database Architecture Cross Platform Connectivity and Application* |
| SC23-2443 | *Encina for AIX Product Family Overview* |

# Kapitel 1. Verbinden von DB2 für MVS/ESA in einem DRDA-Netzwerk

DB2 für MVS/ESA ist das Verwaltungssystem für relationale Datenbanken von IBM für MVS/XA- und MVS/ESA-Systeme. DB2 für MVS/ESA Version 2 Release 3 war das erste Release von DB2 für MVS/ESA, das relationale Daten mit anderen Datenbankverwaltungssystemen, die DRDA-Protokolle unterstützen, gemeinsam benutzen konnte. In diesem Kapitel wird beschrieben, wie DB2 für MVS/ESA verteilte relationale Datenbanksysteme unterstützt. Wenn Sie mit DB2 Universal Database für OS/390 arbeiten, *übergehen Sie dieses Kapitel*. Lesen Sie anstelle dessen „Kapitel 2. Verbinden von DB2 Universal Database für OS/390 in einem DRDA-Netzwerk" auf Seite 47.

Der Schwerpunkt der Informationen in diesem Kapitel liegt auf dem Konfigurieren von DB2 für MVS/ESA für Konnektivität zwischen:

1. DB2 Connect (siehe „Konfigurieren des Anwendungs-Servers" auf Seite 30) und
2. Servern mit DB2 Universal Database (siehe „Konfigurieren des Anwendungs-Requesters" auf Seite 8)

Weitere Informationen zur Herstellung von Verbindungen zwischen zwei Systemen mit DB2 für MVS/ESA und zur Definition von DRDA-Verbindungen für DB2 für MVS/ESA finden Sie im Abschnitt zum Verbinden verteilter Datenbanksysteme des Handbuchs *IBM Database 2 Systemverwaltung*.

Die AnyNet-Funktion von VTAM Version 4 Release 2 ermöglicht das Ausführen von APPC über ein TCP/IP-Netzwerk. Die AnyNet-Funktion umfaßt AnyNet/MVS (auf einem Host ausgeführt) und AnyNet/2 (auf einer Workstation ausgeführt und vom Host heruntergeladen). Endbenutzer in einem TCP/IP-Netzwerk können auf eine APPC-Anwendung zugreifen, ohne zur Anwendung wechseln zu müssen. Mit APPC über TCP/IP kann ein Anwendungsprogramm unter MVS/ESA Daten an ein anderes APPC-Anwendungsprogramm übertragen, das mit Hilfe von AnyNet APPC über TCP/IP unter MVS/ESA, OS/2, AIX/6000, OS/400 oder Windows ausführt. Weitere Informationen finden Sie im Handbuch *VTAM AnyNet Feature for V4R2 Guide to SNA over TCP/IP*.

## DB2 für MVS/ESA

Abb. 1 zeigt ein MVS-System, auf dem eine einzelne Kopie von DB2 für MVS/ESA ausgeführt wird. Auf einem MVS-System können aber auch mehrere Kopien von DB2 für MVS/ESA ausgeführt werden. Zur Identifikation von Kopien von DB2 für MVS/ESA auf einem bestimmten MVS-System (bzw. von Kopien von DB2 für MVS/ESA innerhalb eines MVS/JES-Komplexes) wird jedem DB2-System ein *Subsystemname* gegeben, der eine 1 bis 4 Zeichen lange eindeutige Folge innerhalb eines MVS/JES-Komplexes ist. In Abb. 1 ist der Subsystemname von DB2 für MVS/ESA *xxxx*. Vier der MVS-Adreßraumnamen wird der Subsystemname von DB2 für MVS/ESA vorangestellt. Jeder dieser vier Adreßräume hat Anteil an der ordnungsgemäßen Funktionsweise von DB2 für MVS/ESA.

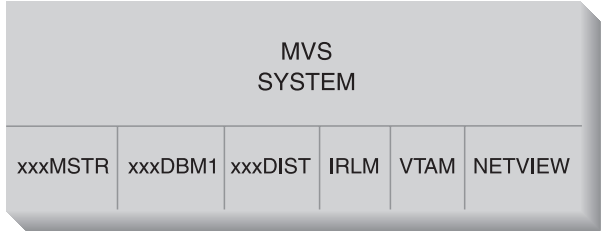


*Abbildung 1. Von DB2 für MVS/ESA verwendete Adreßräume*

Abb. 1 zeigt die MVS-Adreßräume, die an der Verarbeitung für verteilte Datenbanken durch DB2 für MVS/ESA beteiligt sind. Diese Adreßräume arbeiten zusammen, um Benutzern von DB2 für MVS/ESA den Zugriff auf lokale relationale Datenbanken und die Kommunikation mit fernen DRDA-Systemen zu ermöglichen. Die einzelnen Adreßräume werden im folgenden erklärt:

**xxxxMSTR**
Der Adreßraum des Systemservice von DB2 für MVS/ESA, der für das Starten und Stoppen von DB2 für MVS/ESA sowie das Steuern des lokalen Zugriffs auf DB2 für MVS/ESA zuständig ist.

**xxxxDBM1**
Der Adreßraum des Datenbankservice, der für den Zugriff auf von DB2 für MVS/ESA gesteuerte relationale Datenbanken zuständig ist. Hier wird im Auftrag von SQL-Anwendungsprogrammen die Eingabe in und Ausgabe von Datenbankressourcen ausgeführt.

**xxxxDIST**

Die Komponente von DB2 für MVS/ESA, die Funktionen für verteilte Datenbanken bereitstellt; auch als DDF (*Distributed Data Facility*) bekannt. Wenn eine Anforderung für verteilte Datenbanken empfangen wird, übergibt DDF die Anforderung an *xxxx*DBM1, damit die erforderlichen Datenbank-E/A-Operationen ausgeführt werden können. In diesem Handbuch wird DDF ausführlich behandelt.

**IRLM** Der von DB2 für MVS/ESA verwendete Sperrenmanager (Lock Manager) zum Steuern des Zugriffs auf Datenbankressourcen.

**VTAM**

Der SNA-Kommunikationsmanager für das MVS-System; DDF verwendet VTAM im Auftrag von DB2 für MVS/ESA zum Ausführen von Kommunikation für verteilte Datenbanken.

**NETVIEW**

Das zentrale Alert-Verarbeitungssystem der Netzwerkverwaltung auf MVS-Systemen; wenn während der Verarbeitung für verteilte Datenbanken Fehler auftreten, zeichnet DDF Fehlerinformationen (auch als *Alerts* bekannt) in der NetView-Datenbank für Hardwareüberwachung auf. Systemadministratoren können mit NetView die in der Datenbank für Hardwareüberwachung gespeicherten Fehler überprüfen oder den automatischen Aufruf von Befehlsprozeduren beim Aufzeichnen der Alert-Bedingungen einrichten.

Mit NetView können Sie auch eine Diagnose der VTAM-Übertragungsfehler erstellen. Weitere Informationen finden Sie im Handbuch *Distributed Relational Database Architecture Problem Determination Guide*.

Abb. 1 auf Seite 2 zeigt keine SQL-Anwendungsprogramme. Wenn ein Anwendungsprogramm mit DB2 SQL-Anweisungen absetzt, muß es auf eine der folgenden Arten eine Verbindung zu DB2 für MVS/ESA herstellen:

**TSO** Für Stapeljobs und an TSO angemeldete Endbenutzer wird über die TSO-Verbindungseinrichtung eine Verbindung zu DB2 für MVS/ESA hergestellt. Mit diesem Verfahren wird die Verbindung von SPUFI-Anwendungen und den meisten QMF-Anwendungen zu DB2 für MVS/ESA hergestellt.

**CICS/ESA**

Wenn eine CICS/ESA-Anwendung SQL-Aufrufe absetzt, verwendet das CICS/ESA-Produkt die CICS-Verbindungsschnittstelle, um SQL-Anforderungen an DB2 für MVS/ESA weiterzuleiten.

**IMS/ESA**
Transaktionen, die unter der Steuerung von IMS/ESA ausgeführt werden, verwenden die IMS-Verbindungsschnittstelle, um SQL-Anweisungen zur Verarbeitung an DB2 für MVS/ESA zu übergeben.

**DDF** DDF (Distributed Data Facility) ist für die Herstellung der Verbindung verteilter Anwendungen zu DB2 für MVS/ESA zuständig.

**CAF** CAF (Call Attachment Facility) ermöglicht benutzerdefinierten Subsystemen die Herstellung einer direkten Verbindung zu DB2 für MVS/ESA.

## Implementierung von DB2 für MVS/ESA

DRDA definiert die Funktionsarten des Verwaltungssystems für verteilte Datenbanken. DB2 für MVS/ESA Version 2 Release 3 unterstützt ferne Arbeitseinheiten. Durch ferne Arbeitseinheiten kann ein auf einem System ausgeführtes Anwendungsprogramm eines fernen Datenbankverwaltungssystems zugreifen (mit Hilfe der vom fernen Datenbankverwaltungssystem bereitgestellten SQL-Anweisungen). DB2 für MVS/ESA Version 3 Release 1 unterstützt verteilte Arbeitseinheiten. Durch verteilte Arbeitseinheiten kann ein auf einem System ausgeführtes Anwendungsprogramm auf Daten mehrerer ferner Datenbankverwaltungssysteme zugreifen (mit Hilfe der von den fernen Datenbankverwaltungssystemen bereitgestellten SQL-Anweisungen). Weitere Informationen zu von DRDA definierten Verteilungsarten finden Sie im Handbuch *DRDA Connectivity Guide*.

Wie in Abb. 2 auf Seite 6 gezeigt, unterstützt DB2 für MVS/ESA drei Konfigurationen von Verbindungen für verteilte Datenbanken unter Verwendung von zwei Zugriffsmethoden:

**[1]** *Systemgesteuerter Zugriff* ermöglicht einem Requester unter DB2 für MVS/ESA die Verbindung zu mindestens einem Server unter DB2 für MVS/ESA. Die zwischen dem Requester und Server unter DB2 für MVS/ESA hergestellte Verbindung hält sich nicht an die in DRDA definierten Protokolle und kann nicht zur Herstellung einer Verbindung zwischen anderen Produkten als DB2 für MVS/ESA und DB2 für MVS/ESA verwendet werden. Diese Art der Verbindung wird durch die Codierung von dreiteiligen Namen oder Aliasnamen in der Anwendung hergestellt.

**[2]** *Anwendungsgesteuerter Zugriff* ermöglicht einem Requester unter DB2 für MVS/ESA oder unter einem anderen Produkt als DB2 für MVS/ESA wie DB2 Connect die Verbindung zu mindestens einem Anwendungs-Server unter DB2 für MVS/ESA oder einem anderen Produkt als DB2 für MVS/ESA wie DB2 Universal Database und DB2 Universal Database für AS/400 über DRDA-Protokolle. Die Anzahl Anwendungs-Server, für die jeweils eine Verbindung zum Anwendungs-Requester bestehen kann, hängt von der Version von DB2 für MVS/ESA für den Anwendungs-Requester ab. Wenn der Anwendungs-Requester unter DB2 für MVS/ESA Version 2 Release 3 läuft, kann nur zu jeweils einem einzigen Anwendungs-Server eine Verbindung hergestellt werden. Diese Art der Verbindung wird durch die Codierung von SQL-Anweisungen CONNECT in der Anwendung hergestellt. Wenn der Anwendungs-Requester unter DB2 für MVS/ESA Version 3 Release 1 läuft, kann die Verbindung zu mehreren Anwendungs-Servern gleichzeitig hergestellt werden.

**[3]** Anwendungsgesteuerter und systemgesteuerter Zugriff können zur Verbindungsherstellung gemeinsam verwendet werden.

Der Begriff *sekundärer Server* beschreibt Systeme,die für den Anwendungs-Server als Server fungieren.

Wenn alle Systeme in einer Konfiguration zweiphasige Festschreibung unterstützen, werden verteilte Arbeitseinheiten (Lesen und Aktualisieren von auf mehrere Standorte verteilten Daten) unterstützt. Wenn nicht alle Systeme zweiphasige Festschreibung unterstützen, sind Aktualisierungen innerhalb einer Arbeitseinheit auf einen einzelnen Standort beschränkt, der zweiphasige Festschreibung nicht unterstützt, oder auf die Untergruppe der Standorte, die zweiphasige Festschreibung unterstützen.

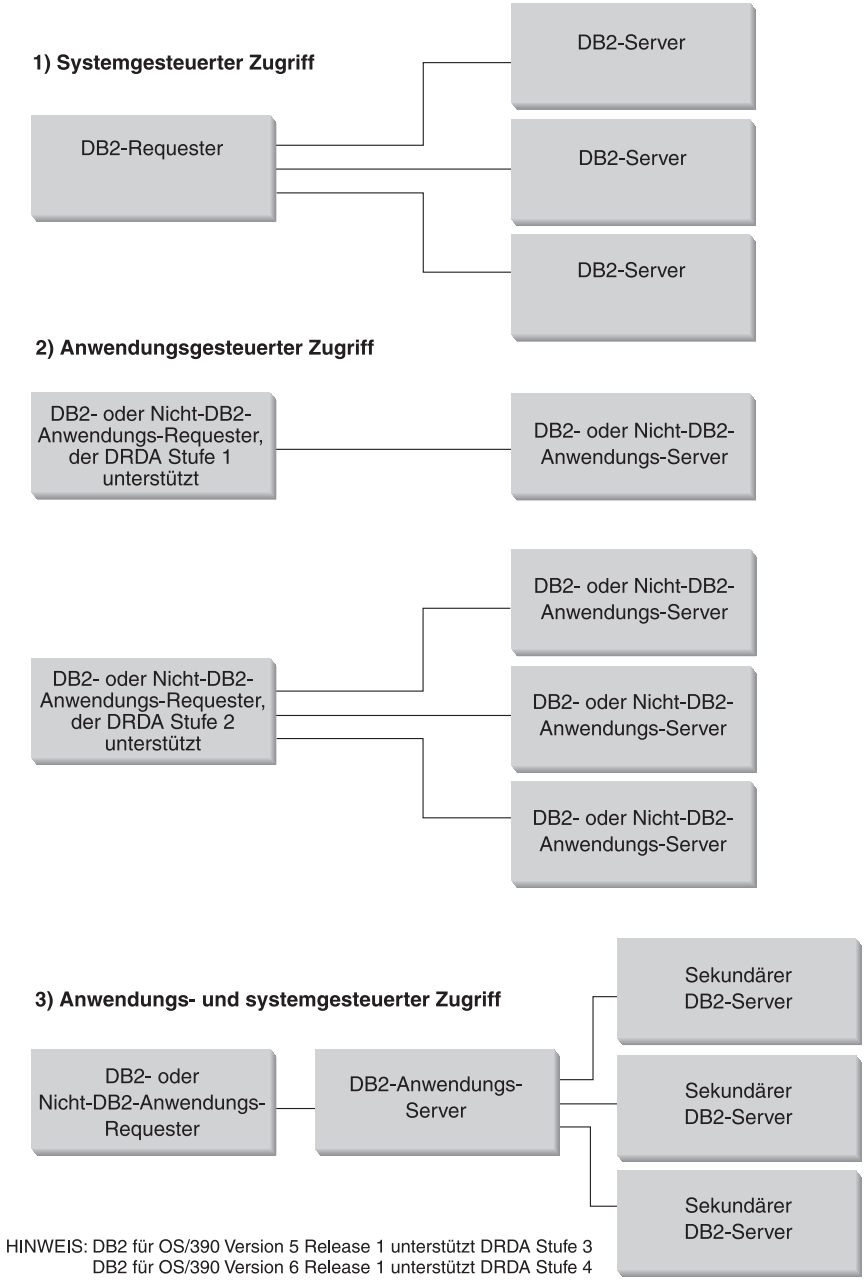


*Abbildung 2. Verteilte Verbindungen von DB2 für MVS/ESA*

Tabelle 1 vergleicht die Verbindungsarten verteilter Datenbanken von DB2 für MVS/ESA.

*Tabelle 1. Vergleich der Verbindungen verteilter Datenbanken von DB2 für MVS/ESA*

| **[1] Systemgesteuerter Zugriff** | **[2] Anwendungsgesteuerter Zugriff (alle Systeme unterstützen zweiphasige Festschreibung)** | **[3] Anwendungsgesteuerter und systemgesteuerter Zugriff** |
|---|---|---|
| Alle Partner müssen Systeme mit DB2 für MVS/ESA sein. | Kann Verbindung zwischen zwei DRDA-Systemen herstellen. | Der Anwendungs-Requester kann ein beliebiges DRDA-System sein. Server müssen Systeme mit DB2 für MVS/ESA sein. |
| Kann direkte Verbindung zu vielen Partnern herstellen. | Kann direkte Verbindung zu vielen Partnern herstellen. | Der Anwendungs-Requester stellt direkte Verbindungen zu Anwendungs-Servern her. Anwendungs-Server können Verbindungen zu vielen sekundären Servern unter DB2 für MVS/ESA herstellen. |
| Jede SQL-Anwendung kann für jeden Server mehrere APPC-Dialoge einrichten. | Jede SQL-Anwendung richtet für jeden Server einen einzigen APPC-Dialog ein. | Die SQL-Anwendung richtet für jeden Server einen einzigen APPC-Dialog ein. Anwendungs-Server unter DB2 für MVS/ESA können für die Anwendung viele APPC-Dialoge mit jedem Server herstellen. |
| Kann sowohl auf lokale als auch auf ferne Ressourcen in einem COMMIT-Bereich zugreifen. | Kann sowohl auf lokale als auch auf ferne Ressourcen in einem COMMIT-Bereich zugreifen. | Anwendungs-Requester und Anwendungs-Server können auf lokale und ferne Daten zugreifen. |
| Effektiver bei großen Abfragen und mehreren gleichzeitig ablaufenden Abfragen | Effektiver bei SQL-Anweisungen, die in einem COMMIT-Bereich nicht häufig ausgeführt werden | Verbindungen zwischen Anwendungs-Requester und Anwendungs-Server verhalten sich wie **[2]**. Verbindungen zu sekundären Servern verhalten sich wie **[1]**. |
| Kann statisches oder dynamisches SQL unterstützen, der Server bindet statisches SQL bei der Erstausführung in einem COMMIT-Bereich jedoch dynamisch. | Kann statisches oder dynamisches SQL absetzen. | Anwendungs-Requester und Anwendungs-Server können statisches oder dynamisches SQL absetzen. Sekundäre Server unterstützen statisches oder dynamisches SQL, binden statisches SQL bei der Erstausführung in einem COMMIT-Bereich jedoch dynamisch. |

*Tabelle 1. Vergleich der Verbindungen verteilter Datenbanken von DB2 für MVS/ESA (Forts.)*

| [1] Systemgesteuerter Zugriff | [2] Anwendungsgesteuerter Zugriff (alle Systeme unterstützen zweiphasige Festschreibung) | [3] Anwendungsgesteuerter und systemgesteuerter Zugriff |
|---|---|---|
| Auf die SQL-Anweisungen INSERT, DELETE und UPDATE und auf Anweisungen beschränkt, die SELECT unterstützen. | Kann eine Anweisung verwenden, die vom die Anweisung ausführenden System unterstützt wird. | Anwendungs-Server unterstützen beliebiges SQL, sekundäre Server unterstützen nur DML-SQL (z. B. CREATE oder ALTER). |

## Konfigurieren des Anwendungs-Requesters

DB2 für MVS/ESA implementiert die Unterstützung für den DRDA-Anwendungs-Requester als integralen Bestandteil von DB2 für MVS/ESA DDF (Distributed Data Facility). DDF kann unabhängig von den lokalen Funktionen für die Verwaltung von Datenbanken unter DB2 für MVS/ESA gestoppt werden, DDF kann jedoch nicht ohne lokale Unterstützung für die Verwaltung von Datenbanken unter DB2 für MVS/ESA ausgeführt werden.

Wenn DB2 für MVS/ESA als Anwendungs-Requester fungiert, kann die Verbindung zwischen auf dem System ausgeführten Anwendungen und fernen Datenbank-Servern unter DB2 Universal Database, DB2 für MVS/ESA, DB2 Universal Database für OS/390, DB2 Universal Database für AS/400 und DB2 für VSE & VM hergestellt werden, die die DRDA-Anwendungs-Server-Funktion implementieren.

Sie müssen folgende Schritte ausführen, damit der Anwendungs-Requester unter DB2 für MVS/ESA Zugriff auf verteilte Datenbanken bereitstellen kann:

- „Bereitstellen von Netzwerkinformationen” auf Seite 9—Der Anwendungs-Requester muß in der Lage sein, RDB_NAME-Werte entgegenzunehmen und in SNA-NETID.LUNAME-Werte umzuwandeln. DB2 für MVS/ESA verwendet die *Kommunikationsdatenbank von DB2 für MVS/ESA* zum Registrieren der RDB_NAME-Werte und ihrer entsprechenden Netzwerkparameter. Mit der Kommunikationsdatenbank kann der Anwendungs-Requester unter DB2 für MVS/ESA die erforderlichen SNA-Informationen an VTAM übergeben, wenn Anforderungen für verteilte Datenbanken abgesetzt werden.

- „Gewährleisten der Sicherheit” auf Seite 22— Damit der Anwendungs-Server Anforderungen für ferne Datenbanken entgegennehmen kann, muß der Anwendungs-Requester die vom Server benötigten Sicherheitsinformationen bereitstellen. DB2 für MVS/ESA verwendet die Kommunikationsdatenbank und RACF, um die erforderlichen Netzwerksicherheitsinformationen zur Verfügung zu stellen.
- „Darstellen von Daten” auf Seite 29—Sie müssen sicherstellen, daß die CCSID (Coded Character Set Identifier - ID des codierten Zeichensatzes) des Anwendungs-Requesters mit der des Anwendungs-Servers kompatibel ist.

## Bereitstellen von Netzwerkinformationen

Viele Verarbeitungsprozesse in einer verteilten Datenbankumgebung machen den Austausch von Nachrichten mit anderen Netzwerkstandorten erforderlich. Damit diese Verarbeitungsprozesse korrekt ausgeführt werden können, sind Ihrerseits folgende Schritte notwendig:

1. Definieren des lokalen Systems
2. Definieren der fernen Systeme
3. Definieren der Kommunikation
4. Einstellen von RU-Größe und Nachrichtendosierung

### Definieren des lokalen Systems

Jedem Programm im Netzwerk werden eine Netzwerk-ID (NETID) und ein LU-Name zugeordnet, d. h. der Anwendungs-Requester unter DB2 für MVS/ESA muß einen NETID.LUNAME-Wert aufweisen, wenn die Verbindung zum Netzwerk hergestellt wird. Da der Anwendungs-Requester unter DB2 für MVS/ESA in das Verwaltungssystem lokaler Datenbanken von DB2 für MVS/ESA integriert ist, muß der Anwendungs-Requester auch einen RDB_NAME-Wert aufweisen. In den Veröffentlichungen zu DB2 für MVS/ESA wird der RDB_NAME als *Location Name* (Standortname) bezeichnet.

Definieren Sie den Anwendungs-Requester unter DB2 für MVS/ESA wie folgt für das SNA-Netzwerk:

1. Wählen Sie einen LU-Namen für das System mit DB2 für MVS/ESA aus. Die NETID des Systems mit DB2 für MVS/ESA wird beim Starten von DDF von VTAM automatisch abgerufen.
2. Definieren Sie den LU-Namen und Standortnamen im BSDS (*Bootstrap Data Set*) von DB2 für MVS/ESA (DB2 für MVS/ESA beschränkt die Länge des Standortnamens auf 16 Zeichen).
3. Erstellen Sie eine VTAM-APPL-Definition zum Registrieren des ausgewählten LU-Namens für VTAM.

**Konfigurieren des DDF-BSDS:** DB2 für MVS/ESA liest den BSDS während des Startvorgangs, um Parameter zur Systeminstallation abzurufen. Einer der im BSDS gespeicherten Datensätze ist der sogenannte *DDF-Datensatz*, weil er die von DDF verwendeten Informationen zur Verbindungsherstellung zu VTAM enthält. Dabei handelt es sich um folgende Informationen:

- Der Standortname für das System mit DB2 für MVS/ESA
- Der LU-Name für das System mit DB2 für MVS/ESA
- Das bei der Verbindungsherstellung vom System mit DB2 für MVS/ESA zu VTAM verwendete Kennwort

Sie können DB2 für MVS/ESA die DDF-BSDS-Informationen auf zwei Arten bereitstellen:

- Stellen Sie die erforderlichen DDF-BSDS-Informationen bei der Erstinstallation von DB2 für MVS/ESA mit Hilfe der DDF-Installationsanzeige DSNTIPR bereit. Viele der Installationsparameter werden hier nicht erläutert, weil es wichtiger ist, das Verfahren zur Herstellung einer Verbindung zwischen DB2 für MVS/ESA und VTAM zu kennen. Abb. 3 zeigt, wie Sie mit Hilfe der Installationsanzeige den Standortnamen SYDNEY, den LU-Namen LUDBD1 und das Kennwort PSWDBD1 im BSDS von DB2 für MVS/ESA eintragen können.

```
    1 DDF STARTUP OPTION   ===> AUTO      NO (DDF not startable),
                                        AUTO (automatic start up), or
                                        COMMAND (start by command)
  2 DB2 LOCATION NAME    ===> SYDNEY    The name other DB2s use to
                                               refer to this DB2
  3 DB2 NETWORK LUNAME   ===> LUDBD1    The name VTAM uses to refer to this DB2
  4 DB2 NETWORK PASSWORD ===> PSWDBD1   Password for connecting to other DB2s
  5 RLST ACCESS ERROR    ===> NOLIMIT   Action on non-local RLST access error
                                        NOLIMIT   - Run without limit
                                        NORUN     - Do not run at all
                                        1-5000000 - Limit in CPU service units
 PRESS:  ENTER to continue   END to exit   HELP for more information
```

*Abbildung 3. Installationsanzeige DSNTIPR von DB2 für MVS/ESA*

- Wenn DB2 für MVS/ESA bereits installiert ist, können Sie die Informationen im BSDS mit dem Dienstprogramm zum Ändern des Protokollinventars (DSNJU003) aktualisieren.

  Abb. 4 zeigt, wie Sie den BSDS mit dem Standortnamen SYDNEY, dem LU-Namen LUDBD1 und dem Kennwort PSWDBD1 aktualisieren können.

```
//SYSADMB JOB ,'DB2 2.3 JOB',CLASS=A
//*
//*        CHANGE LOG INVENTORY:
//*        UPDATE BSDS WITH
//*             - DB2 LOCATION NAME FOR SYDNEY
//*             - VTAM LUNAME (LUDBD1)
//*             - DB2/VTAM PASSWORD
//*
//DSNBSDS EXEC PGM=DSNJU003
//STEPLIB  DD  DISP=SHR,DSN=DSN230.DSNLOAD
//SYSUT1   DD  DISP=OLD,DSN=DSNC230.BSDS01
//SYSUT2   DD  DISP=OLD,DSN=DSNC230.BSDS02
//SYSPRINT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
//SYSIN    DD  *
 DDF    LOCATION=SYDNEY,LUNAME=LUDBD1,PASSWORD=PSWDBD1
//*
```

*Abbildung 4. Beispiel für BSDS-DDF-Definition*

Beim Starten von DDF (entweder automatisch beim Starten von DB2 für MVS/ESA oder durch den Befehl START DDF von DB2 für MVS/ESA) wird die Verbindung zu VTAM hergestellt, wobei der LU-Name und das Kennwort an VTAM übergeben werden. VTAM erkennt das System mit DB2 für MVS/ESA, indem es den LU-Namen und das Kennwort (sofern ein VTAM-Kennwort erforderlich ist) anhand der in der VTAM-Anweisung APPL von DB2 für MVS/ESA definierten Werte überprüft. Mit dem VTAM-Kennwort wird geprüft, ob DB2 für MVS/ESA dazu berechtigt ist, den angegebenen LU-Namen auf dem VTAM-System zu verwenden. Das VTAM-Kennwort wird nicht über das Netzwerk übertragen, und es wird nicht zur Herstellung einer Verbindung zwischen anderen Systemen im Netzwerk und DB2 für MVS/ESA verwendet.

Wenn für VTAM kein Kennwort erforderlich ist, übergehen Sie das Schlüsselwort PASSWORD= im Dienstprogramm zum Ändern des Protokollinventars. Das Fehlen des Schlüsselworts gibt an, daß kein VTAM-Kennwort erforderlich ist.

**Erstellen einer VTAM-APPL-Definition:** Nach dem Definieren des LU-Namens und Kennworts von VTAM für DB2 für MVS/ESA müssen Sie diese Werte in VTAM registrieren. VTAM definiert lokale LU-Namen mit der Anweisung APPL. Abb. 5 zeigt die Definition des LU-Namens LUDBD1 für VTAM.

```
DB2APPLS VBUILD TYPE=APPL
*
*--------------------------------------------------------------------*
*                                                                    *
*           APPL-DEFINITION FÜR DAS DB2-SYSTEM SYDNEY                *
*                                                                    *
*--------------------------------------------------------------------*
*
LUDBD1   APPL  APPC=YES,                                            X
               AUTH=(ACQ),                                          X
               AUTOSES=1,                                          X
               DMINWNL=10,                                         X
               DMINWNR=10,                                         X
               DSESLIM=20,                                         X
               EAS=9999,                                           X
               MODETAB=RDBMODES,                                   X
               PRTCT=PSWDBD1,                                       X
               SECACPT=ALREADYV,                                   X
               SRBEXIT=YES,                                         X
               VERIFY=NONE,                                         X
               VPACING=2,                                           X
               SYNCLVL=SYNCPT,                                     X
               ATNLOSS=ALL                                          X
```

*Abbildung 5. APPL-Beispieldefinition von DB2 für MVS/ESA*

Die VTAM-Anweisung APPL weist viele Schlüsselwörter auf. Die Bedeutung dieser Schlüsselwörter wird im Handbuch *DB2 Systemverwaltung* genauer erläutert. Hier werden lediglich die Schlüsselwörter erläutert, die für dieses Handbuch relevant sind. Es folgt eine Beschreibung der relevanten Schlüsselwörter in Abb. 5:

**LUDBD1**
: VTAM verwendet den Kennsatz der Anweisung APPL als LU-Namen. In diesem Fall ist der LU-Name LUDBD1. Die APPL-Syntax läßt keinen vollständigen NETID.LUNAME-Wert zu. Der NETID-Wert wird in der VTAM-Anweisung APPL nicht angegeben, weil allen VTAM-Anwendungen automatisch die NETID für das VTAM-System zugeordnet wird.

**AUTOSES=1**

Die Anzahl SNA-Konfliktgewinnersitzungen, die automatisch gestartet werden, wenn eine Anforderung zum Ändern der Sitzungsanzahl (CNOS - Change Number of Sessions) abgesetzt wird; Sie müssen für AUTOSES einen Wert ungleich Null angeben, damit DB2 für MVS/ESA in jedem Fall darauf hingewiesen wird, wenn die VTAM-CNOS-Verarbeitung fehlschlägt.

Sie brauchen nicht alle APPC-Sitzungen zwischen zwei beliebigen Partnerpaaren der verteilten Datenbankumgebung automatisch zu starten. Wenn der Wert für AUTOSES unter der Konfliktgewinnerbegrenzung (DMINWNL) liegt, verzögert VTAM das Starten der übrigen SNA-Sitzungen, bis sie von einer Anwendung für verteilte Datenbanken benötigt werden.

**DMINWNL=10**

Die Anzahl Sitzungen, in denen dieses System mit DB2 für MVS/ESA der Konfliktgewinner ist; die CNOS-Verarbeitung verwendet den Parameter DMINWNL als Standardwert. Er kann jedoch für jeden Partner durch Hinzufügen einer Zeile zur Tabelle SYSIBM.SYSLUMODES in der Kommunikationsdatenbank von DB2 für MVS/ESA außer Kraft gesetzt werden.

**DMINWNR=10**

Die Anzahl Sitzungen, in denen das Partnersystem der Konfliktgewinner ist; die CNOS-Verarbeitung verwendet den Parameter DMINWNR als Standardwert. Er kann jedoch für jeden Partner durch Hinzufügen einer Zeile zur Tabelle SYSIBM.SYSLUMODES in der Kommunikationsdatenbank von DB2 für MVS/ESA außer Kraft gesetzt werden.

**DSESLIM=20**

Die Gesamtzahl zulässiger Sitzungen (Konfliktgewinner und Konfliktverlierer), die zwischen DB2 für MVS/ESA und einem anderen verteilten System für einen bestimmten Modusgruppennamen hergestellt werden können; die CNOS-Verarbeitung verwendet den Parameter DSESLIM als Standardwert. Er kann jedoch für jeden Partner durch Hinzufügen einer Zeile zur Tabelle SYSIBM.SYSLUMODES in der Kommunikationsdatenbank von DB2 für MVS/ESA außer Kraft gesetzt werden.

Wenn der Partner die im Parameter DSESLIM, DMINWNL oder DMINWNR angeforderte Anzahl Sitzungen nicht unterstützen kann, vereinbart der CNOS-Prozeß für diese Parameter neue Werte, die für den Partner akzeptabel sind.

**EAS=9999**

Ein Schätzwert für die Gesamtzahl Sitzungen, die von dieser VTAM-LU benötigt werden.

**MODETAB=RDBMODES**

Gibt die VTAM-MODE-Tabelle mit den einzelnen Modusnamen von DB2 für MVS/ESA an.

**PRTCT=PSWDBD1**

Gibt das VTAM-Kennwort an, das benutzt werden muß, wenn DB2 für MVS/ESA versucht, eine Verbindung zu VTAM herzustellen. Wenn das Schlüsselwort PRTCT übergangen wird, ist kein Kennwort erforderlich, und Sie müssen das Schlüsselwort PASSWORD= im Dienstprogramm zum Ändern des Protokollinventars von DB2 für MVS/ESA übergehen.

**SECACPT=ALREADYV**

Gibt den höchsten Sicherheitswert auf SNA-Dialogebene an, der von diesem System mit DB2 für MVS/ESA beim Empfangen einer Anforderung für verteilte Datenbanken von einem fernen System akzeptiert wird. Das Schlüsselwort ALREADYV gibt an, daß dieses System mit DB2 für MVS/ESA drei Sicherheitsoptionen für SNA-Sitzungen von anderen DRDA-Systemen akzeptieren kann, die Daten von diesem System mit DB2 für MVS/ESA anfordern:

- SECURITY=SAME (eine bereits überprüfte Anforderung, die nur die Benutzer-ID des Requesters enthält)
- SECURITY=PGM (eine Anforderung, in der die Benutzer-ID und das Kennwort des Requesters enthalten sind)
- SECURITY=NONE (eine Anforderung, die keine Sicherheitsinformationen enthält); DB2 für MVS/ESA weist DRDA-Anforderungen mit SECURITY=NONE zurück.

Es wird empfohlen, immer SECACPT=ALREADYV anzugeben, weil die Stufe der SNA-Dialogsicherheit für jeden Partner von DB2 für MVS/ESA aus der Kommunikationsdatenbank von DB2 für MVS/ESA (Spalte USERSECURITY der Tabelle SYSIBM.SYSLUNAMES) kommt. SECACPT=ALREADYV verleiht Ihnen die größte Flexibilität bei der Auswahl der Werte für USERSECURITY.

**VERIFY=NONE**

Gibt die Sicherheitsstufe für SNA-Sitzungen (Partner-LU-Prüfung) an, die für dieses System mit DB2 für MVS/ESA erforderlich ist. Der Wert NONE gibt an, daß keine Partner-LU-Prüfung erforderlich ist.

DB2 für MVS/ESA schränkt Ihre Auswahl für das Schlüsselwort VERIFY nicht ein. In einem nicht gesicherten Netzwerk wird die Einstellung VERIFY=REQUIRED empfohlen. VERIFY=REQUIRED bewirkt, daß VTAM diejenigen Partner zurückweist, die keine Partner-

LU-Prüfung ausführen können. Wenn Sie VERIFY=OPTIONAL angeben, führt VTAM die Partner-LU-Prüfung nur für solche Partner durch, die diese Unterstützung bereitstellen.

**VPACING=2**
Stellt den VTAM-Nachrichtendosierungszähler auf 2 ein.

**SYNCLVL=SYNCPT**
Gibt an, daß DB2 für MVS/ESA in der Lage ist, zweiphasige Festschreibung zu unterstützen. VTAM informiert den Partner mit Hilfe dieser Informationen darüber, daß zweiphasige Festschreibung verfügbar ist. Wenn dieses Schlüsselwort vorhanden ist, verwendet DB2 für MVS/ESA automatisch zweiphasige Festschreibung, sofern der Partner sie unterstützen kann.

**ATNLOSS=ALL**
Gibt an, daß DB2 für MVS/ESA bei jeder Beendigung einer VTAM-Sitzung informiert werden muß. Dadurch wird sichergestellt, daß DB2 für MVS/ESA eine SNA-Resynchronisation ausführt, wenn sie erforderlich ist.

Mit DSESLIM, DMINWNL und DMINWNR können Sie VTAM-Standardsitzungsbegrenzungen für alle Partner festlegen. Für Partner mit speziellen Sitzungsbegrenzungsanforderungen können Sie die Standardsitzungsbegrenzungen mit Hilfe der Tabelle SYSIBM.SYSLUMODES überschreiben. Ein Beispiel dafür ist die Angabe der für Ihre OS/2-Systeme geeigneten VTAM-Standardsitzungsbegrenzungen. Für andere Partner können Sie Zeilen in der Tabelle SYSIBM.SYSLUMODES erstellen, um die gewünschten Sitzungsbegrenzungen zu definieren. Beispielwerte:

```
DSESLIM=4,DMINWNL=0,DMINWNR=4
```

Diese Parameter ermöglichen jedem Partner die Erstellung von maximal vier Sitzungen mit DB2 für MVS/ESA, wobei der Partner in allen Sitzungen der Konfliktgewinner ist. Da OS/2 die LU 6.2-Dialoge mit DB2 für MVS/ESA erstellt und OS/2 zum Konfliktgewinner in den Sitzungen macht, wird der Durchsatz etwas verbessert. Wenn OS/2 eine Konfliktgewinnersitzung zur Verfügung steht, braucht es nicht um die Berechtigung zum Starten eines neuen LU 6.2-Dialogs zu bitten.

### Definieren der fernen Systeme

Wenn eine Anwendung unter DB2 für MVS/ESA Daten von einem fernen System anfordert, sucht DB2 für MVS/ESA in den Tabellen der Kommunikationsdatenbank unter anderem nach folgenden Informationen zum fernen System:

- LU-Name und TPN
- Vom fernen Standort benötigte Netzwerksicherheitsinformationen
- Zum Übertragen von Daten an ferne Standorte verwendete Sitzungsbegrenzungen und Modusnamen

Die Kommunikationsdatenbank ist eine Gruppe von SQL-Tabellen, die vom Systemadministrator von DB2 für MVS/ESA verwaltet wird. Der Systemadministrator von DB2 für MVS/ESA muß mit Hilfe von SQL Zeilen mit einer Beschreibung aller potentiellen DRDA-Partner in die Kommunikationsdatenbank einfügen. Die Kommunikationsdatenbank besteht aus fünf Tabellen:

1. **SYSIBM.SYSLOCATIONS**

   Anhand dieser Tabelle ermittelt DB2 für MVS/ESA den LU-Namen und den TPN-Wert für jeden von einer Anwendung unter DB2 für MVS/ESA ausgewählten RDB_NAME-Wert. Es gibt folgende Spalten:

   **LOCATION**
   Der RDB_NAME des fernen Systems; DB2 für MVS/ESA beschränkt den Wert für RDB_NAME auf 16 Byte, was zwei Byte kürzer als die in DRDA definierte 18-Byte-Begrenzung ist.

   **LOCTYPE**
   Momentan nicht verwendet; diese Spalte muß leer sein.

   **LINKNAME**
   Der LU-Name des fernen Systems.

   **LINKATTR**
   Der TPN (Transaktionsprogrammname) des fernen Systems; wenn das ferne System ein System mit DB2 für MVS/ESA ist oder das ferne System den DRDA-TPN-Standardwert verwendet (X'07F6C4C2'[1]), kann für den TPN eine leere Zeichenfolge angegeben werden, weil DB2 für MVS/ESA automatisch den korrekten Wert wählt.

   Wenn für das ferne System ein anderer TPN-Wert als der TPN-Standardwert erforderlich ist, muß er hier angegeben werden.

1. Dieser TPN-Wert gilt *momentan* für DB2 für VM.

2. **SYSIBM.SYSLUNAMES**

   Mit dieser Tabelle werden die Netzwerkattribute der fernen Systeme definiert. Es gibt folgende Spalten:

   **LUNAME**
   Der LU-Name des fernen Systems.

   **SYSMODENAME**
   Der VTAM-Anmeldemodusname, mit dem Dialoge zwischen Systemen mit DB2 für MVS/ESA für die Unterstützung sekundärer Server unter DB2 für MVS/ESA erstellt werden (systemgesteuerter Zugriff); wird in dieser Spalte kein Wert angegeben, wird IBMDB2LM für Dialoge bei Systemen mit DB2 für MVS/ESA verwendet.

   **USERSECURITY**
   Die vom fernen System benötigten Netzwerksicherheitsoptionen, wenn dieses System mit DB2 für MVS/ESA als Server für das ferne System fungiert (Voraussetzungen für die *Sicherheit bei eingehenden Anforderungen*).

   **ENCRYPTPSWDS**
   Gibt an, ob mit dem Partner ausgetauschte Kennwörter verschlüsselt sind. Verschlüsselte Kennwörter werden nur von Requestern und Servern unter DB2 für MVS/ESA unterstützt.

   **MODESELECT**
   Legt fest, ob die Tabelle SYSIBM.SYSMODESELECT verwendet wird, um einen VTAM-Anmeldemoduseintrag (Modusname) auf Grundlage des Endbenutzers und der Anwendung auszuwählen, die die Anforderung absetzen. Wenn diese Spalte ein 'Y' enthält, wird der Modusname für alle abgehenden Anforderungen für verteilte Datenbanken aus der Tabelle SYSIBM.SYSMODESELECT abgerufen.

   Wenn in der Spalte MODESELECT ein anderer Wert als ein 'Y' enthalten ist, wird der Modusname IBMDB2LM für systemgesteuerte Zugriffsanforderungen und der Modusname IBMRDB für DRDA-Anforderungen verwendet.

   In der Spalte MODESELECT können Sie Prioritäten für Anforderungen für verteilte Datenbanken vergeben, indem Sie eine dem Modusnamen zugeordnete VTAM-Serviceklasse (Class of Service, COS) angeben.

   **USERNAMES**
   Die erforderliche Stufe für die Herkunftsüberprüfung und Umsetzung der Benutzer-ID; In dieser Spalte werden auch die Sicherheitsparameter angegeben, die dieses DB2 für MVS/ESA-Subsystem bei der Anforderung von Daten vom fernen Partner

verwendet (Voraussetzungen für die *Sicherheit bei abgehenden Anforderungen*). Gültige Werte für USERNAMES sind I, O und B.

3. **SYSIBM.SYSLUMODES**

   Mit dieser Tabelle werden die LU 6.2-Sitzungsbegrenzungen (CNOS-Begrenzungen) für alle Partnersysteme definiert. Es gibt folgende Spalten:

   **LUNAME**
   Der LU-Name des fernen Systems.

   **MODENAME**
   Der Name des VTAM-Anmeldemodus, dessen Begrenzungen angegeben werden; wird in der Spalte MODENAME kein Wert angegeben, wird standardmäßig IBMDB2LM verwendet.

   **CONVLIMIT**
   Die maximale Anzahl der in diesem Anmeldemodus aktiven Dialoge zwischen dem lokalen System mit DB2 für MVS/ESA und dem fernen System; mit diesem Wert wird der Parameter DSESLIM in der VTAM-Definitionsanweisung APPL für diesen Anmeldemodus außer Kraft gesetzt. Dieser Parameter stellt die VTAM-Standardsitzungsbegrenzungen für DB2 für MVS/ESA bereit.

   Mit dem in der Spalte CONVLIMIT ausgewählten Wert werden die Werte für DMINWNR und DMINWNL während der Änderung der Sitzungsanzahl (CNOS) auf CONVLIMIT/2 gesetzt.

   **AUTO**
   Gibt an, ob CNOS-Verarbeitung und Vorabzuordnung von Sitzungen beim DDF-Start automatisch eingeleitet oder bis zum ersten Verweis auf den LU-Namen über diesen Anmeldemodus verzögert werden.

4. **SYSIBM.SYSMODESELECT**

   Mit dieser Tabelle können Sie die verschiedenen Modusnamen für einzelne Endbenutzer und Anwendungen unter DB2 für MVS/ESA angeben. Da jedem VTAM-Modusnamen eine Serviceklasse (Class of Service, COS) zugeordnet werden kann, können Sie diese Tabelle verwenden, um Anwendungen für verteilte Datenbanken mit Hilfe einer Kombination aus AUTHID, PLANNAME und LUNAME Netzwerkübertragungsprioritäten zuzuordnen.

Es gibt folgende Spalten:

**AUTHID**
Die Berechtigungs-ID des Benutzers (Benutzer-ID) von DB2 für MVS/ESA; in dieser Spalte werden standardmäßig keine Angaben gemacht. Dadurch wird festgelegt, daß der angegebene Anmeldemodusname für alle Berechtigungs-IDs gilt.

**PLANNAME**
Der Planname für die Anwendung, die Zugriff auf ein fernes Datenbanksystem anfordert; in dieser Spalte werden standardmäßig keine Angaben gemacht. Dadurch wird festgelegt, daß der angegebene Anmeldemodusname für alle Plannamen gilt. Der für den Befehl BIND PACKAGE verwendete Planname ist DSNBIND.

**LUNAME**
Der LU-Name für das ferne Datenbanksystem.

**MODENAME**
Der beim Weiterleiten einer Anforderung für verteilte Datenbanken an das angegebene ferne System zu verwendende Name des VTAM-Anmeldemodus; in dieser Spalte werden standardmäßig keine Angaben gemacht. Dadurch wird angegeben, daß IBMDB2LM für Dialoge mit systemgesteuertem Zugriff und IBMRDB für DRDA-Dialoge verwendet werden soll.

5. **SYSIBM.SYSUSERNAMES**

Mit dieser Tabelle werden Endbenutzernamen durch Bereitstellen von Kennwörtern, Umsetzungen für Namen und Herkunftsüberprüfungen verwaltet. DB2 für MVS/ESA bezeichnet den Endbenutzernamen als Berechtigungs-ID. Die meisten anderen Produkte bezeichnen diesen Namen als Benutzer-ID.

In dieser Tabelle können Sie mit Hilfe der Umsetzung für Namen die Verwendung verschiedener Werte für die SNA-Benutzer-ID und die Berechtigungs-ID von DB2 für MVS/ESA erzwingen. Der Umsetzungsprozeß für Namen ist für Anforderungen an ein fernes System (*abgehende Anforderungen*) und für Anforderungen von einem fernen System (*eingehende Anforderungen*) zulässig. Werden Kennwörter nicht verschlüsselt, ist diese Tabelle die Quelle des Kennworts für den Endbenutzer, wenn sowohl Benutzer-ID als auch Kennwort an den fernen Standort gesendet werden. Es gibt folgende Spalten:

**TYPE** Beschreibung für den Verwendungszweck der Zeile (Umsetzung von Namen für abgehende oder eingehende Überprüfungsanforderungen, wobei letztere auch als Herkunftsüberprüfungsanforderungen bezeichnet werden.)

**AUTHID**
Bei der Namensumsetzung für abgehende Anforderungen wird die

Berechtigungs-ID von DB2 für MVS/ESA umgesetzt. Bei der Namensumsetzung für eingehende Anforderungen wird die SNA-Benutzer-ID umgesetzt. In beiden Fällen werden, wenn für AUTHID kein Wert angegeben ist, alle Berechtigungs-IDs oder Benutzer-IDs umgesetzt.

**LUNAME**
Der LU-Name des fernen Systems, auf das sich diese Zeile bezieht; wenn in dieser Spalte keine Angaben gemacht werden, gilt der Wert für NEWAUTHID für alle Systeme.

**NEWAUTHID**
Der neue Endbenutzername (SNA-Benutzer-ID oder Berechtigungs-ID von DB2 für MVS/ESA); wenn in dieser Spalte keine Angaben gemacht werden, braucht die ID nicht umgesetzt zu werden.

**PASSWORD**
Das im Zuordnungsdialog verwendete Kennwort, wenn Kennwörter nicht verschlüsselt werden (ENCRYPTPSWDS = 'N' in SYSIBM.SYSLUNAMES); wenn Kennwörter verschlüsselt werden, wird diese Spalte ignoriert.

### Definieren der Kommunikation

VTAM ist der Kommunikationsmanager für MVS-Systeme. VTAM nimmt LU 6.2-Verben von DB2 für MVS/ESA entgegen und wandelt diese Verben in LU 6.2-Datenströme um, die über das Netzwerk übertragen werden können. Damit VTAM mit den in der Kommunikationsdatenbank von DB2 für MVS/ESA angegebenen Partneranwendungen kommunizieren kann, müssen Sie folgende Informationen für VTAM bereitstellen:

- Die LU-Namen für alle Server.

  Wenn DB2 für MVS/ESA mit VTAM kommuniziert, darf DB2 für MVS/ESA nur einen LU-Namen (nicht NETID.LUNAME) an VTAM übergeben, um den gewünschten Standort anzugeben. Dieser LU-Name muß innerhalb der auf dem lokalen VTAM-System bekannten LU-Namengruppe eindeutig sein, damit VTAM die NETID und den LU-Namen aus dem von DB2 für MVS/ESA übergebenen LU-Namenwert ermitteln kann. Wenn LU-Namen im SNA-Netzwerk eines Unternehmens eindeutig sind, vereinfacht dies den VTAM-Ressourcendefinitionsprozeß enorm. Dies ist jedoch nicht immer möglich. Wenn LU-Namen innerhalb Ihres SNA-Netzwerks nicht eindeutig sind, müssen Sie die VTAM-LU-Umsetzung für Namen verwenden, um die korrekte NETID.LUNAME-Kombination für einen nicht eindeutigen LU-Namen zu erstellen. Dieser Prozeß wird im Abschnitt „Resource Name Translation” des Handbuchs *VTAM Network Implementation Guide* beschrieben.

Plazierung und Syntax dieser VTAM-Definitionen zum Definieren der fernen LU-Namen hängen stark davon ab, wie das ferne System logisch und physisch mit dem lokalen VTAM-System verbunden ist.

- RU-Größe, Größe des Nachrichtendosierungsfensters und Serviceklasse für jeden Modusnamen; erstellen Sie in der VTAM-Modustabelle für jeden in der Kommunikationsdatenbank angegebenen Modusnamen einen Eintrag. Sie müssen auch IBMRDB und IBMDB2LM definieren.
- Die VTAM- und RACF-Profile für den LU-Prüfungsalgorithmus, wenn Sie die Partner-LU-Prüfung verwenden wollen.

### Einstellen von RU-Größe und Nachrichtendosierung

Die in der VTAM-Modustabelle von Ihnen definierten Einträge geben die RU-Größe und die Nachrichtendosierungszähler an. Fehlende oder fehlerhafte Definitionen für diese Werte können sich nachteilig auf alle VTAM-Anwendungen auswirken.

Bedenken Sie bei der Wahl der RU-Größe, Sitzungsbegrenzungen und Nachrichtendosierungszähler, welche Auswirkungen diese Werte auf das vorhandene VTAM-Netzwerk haben können. Überprüfen Sie beim Installieren eines neuen verteilten Datenbanksystems die folgenden Punkte:

- Stellen Sie für VTAM-CTC-Verbindungen sicher, daß der Parameterwert für MAXBFRU groß genug ist, um Ihre RU-Größe plus der 29 Byte, die VTAM als SNA-Anforderungs- und Übertragungskopf hinzufügt, zu verarbeiten. MAXBFRU wird in Einheiten von 4 KB gemessen, d. h. der Wert für MAXBFRU muß mindestens 2 betragen, um eine RU-Größe von 4 KB zu unterstützen.
- Stellen Sie für NCP-Verbindungen sicher, daß der Wert für MAXDATA groß genug ist, um Ihre RU-Größe plus 29 Byte zu verarbeiten. Wenn Sie als RU-Größe 4 KB angegeben haben, muß der Wert für MAXDATA mindestens 4125 betragen.

  Wenn Sie den NCP-Parameter MAXBFRU angeben, wählen Sie einen Wert aus, der für Ihre RU-Größe plus 29 Byte ausreicht. Bei NCP definiert der Parameter MAXBFRU die Anzahl der VTAM-E/A-Puffer für die PIU. Wenn Sie für IOBUF eine Puffergröße von 441 angeben, verarbeitet MAXBFRU=10 die RU-Größe 4 KB korrekt, weil 10*441 größer ist als 4096+29.
- Im Handbuch *DRDA Connectivity Guide* wird beschrieben, wie Sie die Auswirkung der verteilten Datenbank auf den VTAM-IOBUF-Pool einschätzen können. Wenn ein zu großer Anteil der IOBUF-Poolressource belegt ist, hat dies nachteilige Auswirkungen auf die Leistung aller VTAM-Anwendungen.

## Gewährleisten der Sicherheit

Wenn ein fernes System die Verarbeitung für verteilte Datenbanken im Auftrag einer SQL-Anwendung ausführt, muß es in der Lage sein, die Sicherheitsanforderungen des Anwendungs-Requesters, des Anwendungs-Servers und des verwendeten Netzwerks zu erfüllen. Diese Anforderungen betreffen mindestens einen der folgenden Bereiche:

- Auswählen von Endbenutzernamen
- Sicherheitsparameter des Netzwerks
- Sicherheit des Datenbankmanagers
- Von einem externen Sicherheitssubsystem implementierte Sicherheit
- Datendarstellung

### Auswählen von Endbenutzernamen

Auf MVS-Systemen wird jedem Endbenutzer eine *Benutzer-ID* aus 1 bis 8 Zeichen zugeordnet. Der Wert dieser Benutzer-ID muß zwar innerhalb eines bestimmten MVS-Systems, jedoch nicht unbedingt im gesamten SNA-Netzwerk eindeutig sein. Beispielsweise kann es im System NEWYORK einen Benutzer mit dem Namen JONES und im System DALLAS einen weiteren Benutzer dieses Namens geben. Wenn diese beiden Benutzer dieselbe Person sind, entsteht dadurch kein Konflikt. Ist jedoch der Benutzer JONES in DALLAS nicht identisch mit dem Benutzer JONES in NEWYORK, kann das SNA-Netzwerk (und können folglich auch die verteilten Datenbanksysteme innerhalb dieses Netzwerks) den Benutzer JONES in NEWYORK nicht von dem Benutzer JONES in DALLAS unterscheiden. Wird diese Situation nicht durch geeignete Maßnahmen verhindert, können diese beiden Benutzer die Berechtigungen des jeweils anderen benutzen.

Zur Vermeidung solcher Namenskonflikte unterstützt DB2 für MVS/ESA die Umsetzung für Endbenutzernamen. Wenn eine Anwendung auf dem Anwendungs-Requester unter DB2 für MVS/ESA eine verteilte Datenbank anfordert, führt DB2 für MVS/ESA die Umsetzung für Namen aus, wenn in der Kommunikationsdatenbank die *Namensumsetzung für abgehende Anforderungen* als erforderlich angegeben ist. Wenn die Namensumsetzung für abgehende Anforderungen ausgewählt ist, erzwingt DB2 für MVS/ESA immer das Senden eines Kennworts bei jeder abgehenden Anforderung für verteilte Datenbanken.

Die Namensumsetzung für abgehende Anforderungen in DB2 für MVS/ESA wird durch das Setzen der Spalte USERNAMES in der Tabelle SYSIBM.SYSLUNAMES auf 'O' oder 'B' aktiviert. Wenn USERNAMES auf 'O' gesetzt ist, wird die Umsetzung von Endbenutzernamen für abgehende Anforderungen ausgeführt. Wenn USERNAMES auf 'B' gesetzt ist, wird die Umsetzung von Endbenutzernamen für eingehende und abgehende Anforderungen ausgeführt.

Da Berechtigungen in DB2 für MVS/ESA sowohl von der Benutzer-ID des Endbenutzers als auch von der Benutzer-ID des Plan- bzw. Paketeigners von DB2 für MVS/ESA abhängen, wird der Umsetzungsprozeß des Endbenutzernamens für die Benutzer-ID des Endbenutzers, die Benutzer-ID des Planeigners und die Benutzer-ID des Paketeigners ausgeführt. [2]Der Umsetzungsprozeß für Namen durchsucht die Tabelle SYSIBM.SYSUSERNAMES in der folgenden Reihenfolge nach einer Zeile, die einem der folgenden Muster (TYPE.AUTHID.LUNAME) entspricht:

1. O.AUTHID.LUNAME — eine Umsetzungsregel für einen bestimmten Endbenutzer eines bestimmten Partnersystems
2. O.AUTHID.leer — eine Umsetzungsregel für einen bestimmten Endbenutzer eines beliebigen Partnersystems
3. O.leer.LUNAME — eine Umsetzungsregel für einen beliebigen Benutzer eines bestimmten Partnersystems

Wenn keine übereinstimmende Zeile gefunden wird, wird die Anforderung für verteilte Datenbanken von DB2 für MVS/ESA zurückgewiesen. Wenn eine Zeile gefunden wird, wird der Wert in der Spalte NEWAUTHID als Berechtigungs-ID verwendet. (Ein leerer Wert für NEWAUTHID gibt an, daß der Originalname ohne Umsetzung verwendet wird.)

2. Wird die Anforderung an einen DB2 für MVS/ESA-Server geschickt, wird die Namenumsetzung auch für den Planeigner und den Paketeigner ausgeführt. Paket- und Planeignernamen werden nie Kennwörter zugeordnet.

Das weiter oben angeführte Beispiel soll erneut der Verdeutlichung dieser Sachverhalte dienen. Sie wollen dem Benutzer JONES im System NEWYORK einen anderen Namen geben (NYJONES), wenn JONES Anforderungen für verteilte Datenbanken an das System DALLAS absetzt. Angenommen, der Eigner der vom Benutzer JONES verwendeten Anwendung ist DSNPLAN (der Planeigner in DB2 für MVS/ESA), und Sie brauchen diese Benutzer-ID beim Senden an das System DALLAS nicht umzusetzen. Die SQL-Anweisungen, die zum Bereitstellen der Regeln für die Umsetzung für Namen in der Kommunikationsdatenbank erforderlich sind, werden in Abb. 6 gezeigt.

```
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', 'O');
INSERT INTO SYSIBM.SYSLOCATIONS
     (LOCATION, LOCTYPE, LINKNAME, LINKATTR)
  VALUES ('DALLAS', ' ', 'LUDALLAS', '');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('O', 'JONES', 'LUDALLAS', 'NYJONES', 'JONESPWD');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('O', 'DSNPLAN', 'LUDALLAS', ' ', 'PLANPWD');
```

*Abbildung 6. SQL für die Namensumsetzung für abgehende Anforderungen*

Die daraus resultierenden Kommunikationsdatenbanktabellen werden in Abb. 7 auf Seite 25 gezeigt:

NEWYORK.SYSIBM.SYSLOCATIONS

| LOCATION | LOCTYPE | LINKNAME | LINKATTR |
|---|---|---|---|
| DALLAS | | LUDALLAS | |

NEWYORK.SYSIBM.SYSLUNAMES

| LUNAME | SYSMODENAME | USERSECURITY | ENCRYPTPSWDS | MODESELECT | USERNAMES |
|---|---|---|---|---|---|
| LUDALLAS | | A | N | N | O |

NEWYORK.SYSIBM.SYSUSERNAMES

| TYPE | AUTHID | LUNAME | NEWAUTHID | PASSWORD |
|---|---|---|---|---|
| 0<br>0 | JONES<br>DSNPLAN | LUDALLAS<br>LUDALLAS | NYJONES | JONESPWD<br>PLANPWD |

*Abbildung 7. Namensumsetzung für abgehende Anforderungen*

### Netzwerksicherheit

Nachdem der Anwendungs-Requester die Endbenutzernamen für die ferne Anwendung ausgewählt hat, muß er die erforderlichen LU 6.2-Sicherheitsinformationen für das Netzwerk bereitstellen. LU 6.2 stellt die folgenden drei Hauptsicherheitseinrichtungen für das Netzwerk zur Verfügung:

- Sicherheit auf Sitzungsebene, die durch das Schlüsselwort VERIFY in der VTAM-Anweisung APPL gesteuert wird; weitere Informationen zur Angabe der Sicherheitsoptionen auf Sitzungsebene finden Sie in den sich an Abb. 5 auf Seite 12 anschließenden Erläuterungen.

- Sicherheit auf Dialogebene, die durch den Inhalt der Tabelle SYSIBM.SYSLUNAMES gesteuert wird.
- Datenverschlüsselung, die nur für VTAM 3.4 und spätere Releases von VTAM unterstützt wird.

Da der Anwendungs-Server für die Verwaltung der Datenbankressourcen zuständig ist, legt er fest, welche Netzwerksicherheitseinrichtungen vom Anwendungs-Requester bereitgestellt werden müssen. Sie müssen die Sicherheitsanforderungen auf Dialogebene der einzelnen Anwendungs-Server in der Tabelle SYSIBM.SYSLUNAMES eintragen, indem Sie die Anforderung des Anwendungs-Servers in der Spalte USERNAMES der Tabelle SYSIBM.SYSLUNAMES aufnehmen.

Die folgenden Optionen für SNA-Dialogsicherheit sind möglich:

**SECURITY=SAME**

Diese Option wird auch als bereits geprüfte Sicherheit bezeichnet, weil nur die Benutzer-ID des Endbenutzers zum fernen System gesendet wird (es wird kein Kennwort übertragen). Verwenden Sie diese Stufe von Dialogsicherheit, wenn in der Spalte USERNAMES in der Tabelle SYSIBM.SYSLUNAMES kein 'O' oder 'B' enthalten ist.

Da DB2 für MVS/ESA die Umsetzung für Endbenutzernamen mit Ausgangsdialogsicherheit koppelt, kann SECURITY=SAME nicht verwendet werden, wenn die Umsetzung von Endbenutzernamen für abgehende Anforderungen aktiviert ist.

**SECURITY=PGM**

Benutzer-ID und Kennwort des Endbenutzers werden zur Gültigkeitsprüfung an das ferne System gesendet. Verwenden Sie diese Sicherheitsoption, wenn in der Spalte USERNAMES der Tabelle SYSIBM.SYSLUNAMES ein 'O' oder 'B' enthalten ist.

In Abhängigkeit von den in der Tabelle SYSIBM.SYSLUNAMES angegebenen Optionen ruft DB2 für MVS/ESA das Kennwort des Endbenutzers aus zwei verschiedenen Quellen ab:

- Nicht verschlüsselte Kennwörter werden aus der Spalte PASSWORD in der Tabelle SYSIBM.SYSUSERNAMES abgerufen. DB2 für MVS/ESA extrahiert Kennwörter aus der Tabelle SYSIBM.SYSUSERNAMES, wenn die Spalte ENCRYPTPSWDS in der Tabelle SYSIBM.SYSLUNAMES nicht auf 'Y' gesetzt ist. Aus dieser Quelle abgerufene Kennwörter können an beliebige DRDA-Anwendungs-Server übertragen werden.

Abb. 8 definiert Kennwörter für die Benutzer SMITH und JONES. In der Spalte LUNAME im Beispiel sind Leerzeichen enthalten, d. h. diese Kennwörter werden für alle fernen Systeme verwendet, auf die der Benutzer SMITH bzw. JONES zuzugreifen versucht.

```
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('O', 'JONES', ' ', ' ', 'JONESPWD');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('O', 'SMITH', ' ', ' ', 'SMITHPWD');
```

*Abbildung 8. Senden von Kennwörtern an ferne Standorte*

- Verschlüsselte Kennwörter werden an den fernen Standort gesendet, wenn in der Spalte ENCRYPTPSWDS der Tabelle SYSIBM.SYSLUNAMES 'Y' enthalten ist. Verschlüsselte Kennwörter werden von RACF (oder einem äquivalenten Produkt) extrahiert und können nur von einem anderen System mit DB2 für MVS/ESA interpretiert werden. Setzen Sie ENCRYPTPSWDS bei der Kommunikation mit einem System über ein anderes Produkt als DB2 für MVS/ESA nicht auf 'Y'.

  DB2 für MVS/ESA sucht in der Tabelle SYSIBM.SYSUSERNAMES nach der an das ferne System zu übertragenden Benutzer-ID (Wert für NEWAUTHID). Dieser umgesetzte Name wird für die RACF-Kennwortextraktion verwendet. Wenn Sie die Namen nicht umsetzen wollen, müssen Sie die Zeilen in der Tabelle SYSIBM.SYSUSERNAMES erstellen, durch die Namen ohne Umsetzung gesendet werden. Die Anweisungen in Abb. 9 ermöglichen das Senden von Anforderungen an LUDALLAS und LUNYC, ohne daß der Name (die Benutzer-ID) des Endbenutzers umgesetzt wird.

```
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('O', ' ', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('O', ' ', 'LUDALLAS', ' ', ' ');
```

*Abbildung 9. Senden verschlüsselter Kennwörter an ferne Standorte*

**SECURITY=NONE**

Diese Option wird von DRDA nicht unterstützt, d. h. DB2 für MVS/ESA kann diese Sicherheitsoption nicht bereitstellen.

### Sicherheit des Datenbankmanagers

Wie im Abschnitt „Auswählen von Endbenutzernamen" auf Seite 22 beschrieben, kann der Anwendungs-Requester durch die Namensumsetzung für abgehende Anforderungen an den Sicherheitsfunktionen für verteilte Datenbanken beteiligt sein. Mit der Namensumsetzung für abgehende Anforderungen können Sie den Zugriff auf einen bestimmten Anwendungs-Server anhand der Identität des Endbenutzers und der Anwendung einschränken, von denen die Anforderung ausgeht. Der Anwendungs-Requester unter DB2 für MVS/ESA kann auf folgende andere Arten an den Systemsicherheitsfunktionen beteiligt sein:

**Binden ferner Anwendungen**

Endbenutzer binden ferne Anwendungen auf dem Anwendungs-Server mit dem Befehl BIND PACKAGE von DB2 für MVS/ESA. DB2 für MVS/ESA *schränkt* die Verwendung des Befehls BIND PACKAGE auf dem Requester *nicht ein*. Ein Endbenutzer kann ein fernes Paket jedoch erst dann verwenden, nachdem es in einen Plan in DB2 für MVS/ESA aufgenommen wurde. DB2 für MVS/ESA *schränkt* die Verwendung des Befehls BIND PLAN hingegen *ein*. Ein Endbenutzer kann einem Plan das ferne Paket nur dann hinzufügen, wenn dem Endbenutzer mit der Anweisung GRANT von DB2 für MVS/ESA das Zugriffsrecht BIND bzw. BINDADD erteilt wurde.

Geben Sie beim Binden eines Pakets mit der Option ENABLE/DISABLE an, ob das Paket von einem TSO-, CICS/ESA-, IMS/ESA- oder einem fernen Subsystem mit DB2 für MVS/ESA verwendet werden soll.

**Ausführen ferner Anwendungen**

Damit ein Endbenutzer von DB2 für MVS/ESA eine ferne Anwendung ausführen kann, muß er über die Berechtigung zum Ausführen des Plans von DB2 für MVS/ESA verfügen, der dieser Anwendung zugeordnet ist. Der Planeigner in DB2 für MVS/ESA verfügt automatisch über die Berechtigung zum Ausführen des Plans. Anderen Endbenutzern kann die Berechtigung zum Ausführen des Plans durch die Anweisung GRANT EXECUTE von DB2 für MVS/ESA erteilt werden. Auf diese Weise kann der Eigner einer Anwendung für verteilte Datenbanken individuell steuern, welche Benutzer die Anwendung verwenden dürfen.

### Sicherheitssubsystem

Das externe Sicherheitssubsystem auf MVS-Systemen wird entweder durch RACF oder durch gleichwertige Produkte bereitgestellt, die über eine mit RACF kompatible Schnittstelle verfügen. Der Anwendungs-Requester unter DB2 für MVS/ESA kann das externe Sicherheitssubsystem nicht direkt aufrufen, abgesehen von der im Abschnitt „Netzwerksicherheit" auf Seite 25 beschriebenen Unterstützung für verschlüsselte Kennwörter. Das externe Sicherheitssubsystem wird jedoch in den folgenden Situationen indirekt auf dem Anwendungs-Requester verwendet:

- Das für die Verbindungsherstellung zwischen Endbenutzer und DB2 für MVS/ESA zuständige Produkt verwendet das externe Sicherheitssubsystem zur Überprüfung der Identität des Endbenutzers (Benutzer-ID und Kennwort). Dies geschieht vor der Verbindungsherstellung zwischen Endbenutzer und DB2 für MVS/ESA. Wie bereits erwähnt, sind CICS/ESA, TSO und IMS/ESA Beispiele für Produkte, die die Verbindung zwischen Endbenutzern und DB2 für MVS/ESA herstellen.
- Wenn Sie Sicherheit auf SNA-Sitzungsebene (über das Schlüsselwort VERIFY in der VTAM-Anweisung APPL von DB2 für MVS/ESA) verwenden, wird das externe Sicherheitssubsystem von VTAM aufgerufen, um die Identität des fernen Systems zu überprüfen.

## Darstellen von Daten

DB2 für MVS/ESA wird mit einer Standardinstallations-CCSID (Coded Character Set Identifier - ID für codierten Zeichensatz) von 500 ausgeliefert. Diese Standardeinstellung ist für Ihre Installation wahrscheinlich *nicht* korrekt. Bei der Installation von DB2 für MVS/ESA müssen Sie die Installations-CCSID auf die CCSID der Zeichen setzen, die von den Eingabeeinheiten an Ihrem Standort generiert und an DB2 für MVS/ESA gesendet werden. Diese CCSID wird in der Regel durch die verwendete Landessprache festgelegt. Wenn die Installations-CCSID falsch ist, werden durch die Zeichenumsetzung inkorrekte Ergebnisse erzeugt. Eine Liste der in den einzelnen Ländern bzw. Landessprachen unterstützten CCSIDs finden Sie im *DB2 Connect Benutzerhandbuch.*

Sie müssen sicherstellen, daß Ihr Subsystem mit DB2 für MVS/ESA die CCSIDs der einzelnen Anwendungs-Server in die Installations-CCSID des Subsystems mit DB2 für MVS/ESA umsetzen kann. DB2 für MVS/ESA stellt Umsetzungstabellen für die gängigsten Kombinationen aus Quellen- und Ziel-CCSIDs, jedoch nicht für jede mögliche Kombination bereit. Falls erforderlich, können Sie der Gruppe verfügbarer Umsetzungstabellen und Umsetzungsroutinen Angaben hinzufügen. Weitere Informationen zur Zeichenumsetzung unter DB2 für MVS/ESA finden Sie im Handbuch *DB2 Systemverwaltung.*

## Konfigurieren des Anwendungs-Servers

Die Anwendungs-Server-Unterstützung unter DB2 für MVS/ESA ermöglicht die Verwendung des Systems mit DB2 für MVS/ESA als Server für DRDA-Anwendungs-Requester. Folgende Anwendungs-Requester können mit einem Anwendungs-Server unter DB2 für MVS/ESA verbunden sein:

- Requester unter DB2 für MVS/ESA
- DB2 Connect Version 7, das unter AIX, HP-UX, OS/2, SCO, Solaris, Linux, Windows 9x oder Windows NT ausgeführt werden kann
- DB2 Universal Database Enterprise Edition Version 7 oder DB2 Universal Database Enterprise - Extended Edition mit aktivierter DB2 Connect-Unterstützung
- Requester mit Distributed Database Connection Services (DDCS) Version 2, der unter AIX, HP-UX, OS/2, Solaris, Windows 3.1, Windows 3.11 für Workgroups, Windows 95 oder Windows NT sowie SCO, SGI oder SINIX ausgeführt werden kann
- Requester unter OS/400
- Requester unter DB2 für VM
- Jedes andere Produkt, das die Protokolle für DRDA-Anwendungs-Requester unterstützt

Für jeden mit einem Anwendungs-Server unter DB2 für MVS/ESA verbundenen Anwendungs-Requester unterstützt der Anwendungs-Server unter DB2 für MVS/ESA folgenden Datenbankzugriff:

- Der Anwendungs-Requester kann auf Tabellen zugreifen, die auf dem Anwendungs-Server unter DB2 für MVS/ESA gespeichert sind. Der Anwendungs-Requester muß auf dem Anwendungs-Server unter DB2 für MVS/ESA ein Paket erstellen, bevor die Anwendung ausgeführt werden kann. Der Anwendungs-Server unter DB2 für MVS/ESA verwendet dieses Paket, um die SQL-Anweisungen der Anwendung während der Ausführung zu lokalisieren.
- Der Anwendungs-Requester kann den Anwendungs-Server unter DB2 für MVS/ESA anweisen, den Zugriff auf Lesevorgänge einzuschränken, wenn die DRDA-Verbindung zwischen Requester und Server den zweiphasigen Festschreibeprozeß nicht unterstützt. Beispielsweise würde ein Requester unter DB2 für MVS/ESA Version 2 Release 3 mit einer CICS-Front-End-Anwendung den Anwendungs-Server unter DB2 für MVS/ESA darüber informieren, daß Aktualisierungen nicht zulässig sind.
- Der Anwendungs-Requester kann durch systemgesteuerten Zugriff auch über die Berechtigung zum Zugriff auf Tabellen verfügen, die auf anderen Systemen mit DB2 für MVS/ESA im Netzwerk gespeichert sind. Systemgesteuerter Zugriff ermöglicht dem Anwendungs-Requester die Herstellung von Verbindungen zu mehreren Datenbanksystemen in einer einzelnen Arbeitseinheit.

## Bereitstellen von Netzwerkinformationen

Damit der Anwendungs-Server unter DB2 für MVS/ESA Anforderungen für verteilte Datenbanken ordnungsgemäß verarbeiten kann, müssen Sie folgende Schritte ausführen:

1. Definieren des Anwendungs-Servers für den lokalen Kommunikationsmanager
2. Definieren aller potentiellen Bestimmungsorte für sekundäre Server, damit der Anwendungs-Server unter DB2 für MVS/ESA die SQL-Anforderungen an ihre Zielorte weiterleiten kann
3. Gewährleisten der erforderlichen Sicherheit
4. Gewährleisten von Datendarstellung

### Definieren des Anwendungs-Servers

Damit der Anwendungs-Server Anforderungen für verteilte Datenbanken empfangen kann, muß er für den lokalen Kommunikationsmanager definiert sein und über einen eindeutigen RDB_NAME-Wert verfügen. Sie müssen folgende Schritte ausführen, um den Anwendungs-Server ordnungsgemäß zu definieren:

1. Wählen Sie den vom Anwendungs-Server unter DB2 für MVS/ESA zu verwendenden LU-Namen und RDB_NAME-Wert aus. Der Aufzeichnungsprozeß dieser Namen in DB2 für MVS/ESA und VTAM entspricht dem im Abschnitt „Definieren des lokalen Systems” auf Seite 9 beschriebenen Prozeß. Der für DB2 für MVS/ESA gewählte RDB_NAME-Wert muß allen Endbenutzern und Anwendungs-Requestern bereitgestellt werden, für die eine Verbindung zum Anwendungs-Server erforderlich ist.
2. Registrieren Sie den Wert für NETID.LUNAME für den Anwendungs-Server unter DB2 für MVS/ESA auf allen Anwendungs-Requestern, die Zugriff erfordern, damit der Anwendungs-Requester SNA-Anforderungen an den Server unter DB2 für MVS/ESA weiterleiten kann. Dies gilt auch für Fälle, in denen der Anwendungs-Requester dynamische Netzwerkweiterleitung ausführen kann, weil der Anwendungs-Requester den Wert für NETID.LUNAME kennen muß, bevor dynamische Netzwerkweiterleitung verwendet werden kann.
3. Stellen Sie den Standard-DRDA-TPN (X'07F6C4C2') für die einzelnen Anwendungs-Requester bereit, weil DB2 für MVS/ESA diesen Wert automatisch verwendet.
4. Erstellen Sie für jeden von einem Anwendungs-Requester angeforderten Modusnamen einen Eintrag in der VTAM-Modustabelle. Diese Einträge beschreiben die RU-Größe, die Größe des Nachrichtendosierungsfensters und die Serviceklasse für die einzelnen Modusnamen.

5. Definieren Sie Sitzungsbegrenzungen für die Anwendungs-Requester, die eine Verbindung zu dem Anwendungs-Server unter DB2 für MVS/ESA herstellen. Die VTAM-Anweisung APPL definiert Standardwerte für die Sitzungsbegrenzungen aller Partnersysteme. Verwenden Sie zum Definieren eindeutiger Standardwerte für einen bestimmten Partner die Tabelle SYSIBM.SYSLUMODES der Kommunikationsdatenbank.

   Informationen zum Überprüfen des VTAM-Netzwerks finden Sie in „Einstellen von RU-Größe und Nachrichtendosierung" auf Seite 21.

6. Erstellen Sie in der Kommunikationsdatenbank von DB2 für MVS/ESA Einträge, mit denen Sie angeben, welche Anwendungs-Requester zur Herstellung einer Verbindung zum Anwendungs-Server unter DB2 für MVS/ESA berechtigt sind. Es gibt zwei grundlegende Vorgehensweisen beim Definieren der Kommunikationsdatenbankeinträge für die Anwendungs-Requester im Netzwerk:

   a. Sie können eine Zeile in die Tabelle SYSIBM.SYSLUNAMES einfügen, die die Standardwerte für eine in der Kommunikationsdatenbank nicht spezifisch beschriebene LU bereitstellt (die Standardzeile enthält in der Spalte LUNAME Leerzeichen). Diese Vorgehensweise ermöglicht das Definieren spezifischer Attribute für einige der LUs in Ihrem Netzwerk und gleichzeitig das Bereitstellen von Standardwerten für alle anderen LUs.

      Beispielsweise können Sie dem System DALLAS (ein weiteres System mit DB2 für MVS/ESA) die Berechtigung erteilen, bereits überprüfte Anforderungen für verteilte Datenbanken (LU 6.2 SECURITY=SAME) zu senden, von Systemen mit Datenbankmanagern hingegen das Senden von Kennwörtern fordern. Zudem wollen Sie unter Umständen in der Kommunikationsdatenbank nicht für alle Systeme mit Datenbankmanager Einträge vornehmen, vor allem wenn es sich um viele Systeme handelt. Abb. 10 zeigt, wie die Kommunikationsdatenbank zur Angabe von SECURITY=SAME für das System DALLAS und von SECURITY=PGM für alle anderen Requester verwendet werden kann.

```
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', ' ');
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES (' ', ' ', 'C', 'N', 'N', ' ');
```

*Abbildung 10. Bereitstellen von Standardwerten für Anwendungs-Requester-Verbindungen*

b. Mit der Kommunikationsdatenbank können Sie Berechtigungen für die einzelnen Anwendungs-Requester im Netzwerk individuell erteilen. Konfigurieren Sie dazu die Kommunikationsdatenbank auf eine der folgenden Arten:

   - Stellen Sie sicher, daß die Tabelle SYSIBM.SYSLUNAMES keine Standardzeile enthält. Wenn die Standardzeile (die Zeile mit einem leeren LU-Namen) fehlt, muß für jeden Anwendungs-Requester, der eine Verbindungsherstellung versucht, in der Tabelle SYSIBM.SYSLUNAMES eine Zeile mit dem LU-Namen aufgenommen werden. Wenn in der Kommunikationsdatenbank keine übereinstimmende Zeile gefunden wird, wird dem Anwendungs-Requester der Zugriff verweigert.
   - Tragen Sie in der Tabelle SYSIBM.SYSLUNAMES eine Standardzeile ein, die angibt, daß eine Herkunftsüberprüfung erforderlich ist (Spalte USERNAMES auf 'I' oder 'B' gesetzt). Dadurch beschränkt DB2 für MVS/ESA den Zugriff auf Anwendungs-Requester und Endbenutzer, die in der Tabelle SYSIBM.SYSUSERNAMES angegeben sind (wie im Abschnitt „Herkunftsüberprüfung” auf Seite 38 beschrieben). Diese Vorgehensweise empfiehlt sich, wenn Ihre Regeln für die Umsetzung für Namen eine Zeile mit einem leeren LU-Namen in der Tabelle SYSIBM.SYSLUNAMES erfordern, DB2 für MVS/ESA diese Zeile jedoch nicht zum Erteilen eines unbeschränkten Zugriffs auf den Anwendungs-Server unter DB2 für MVS/ESA verwenden soll.

   In Abb. 11 enthält keine Zeile in der Spalte LUNAME Leerzeichen, d. h. DB2 für MVS/ESA verweigert allen LUs außer LUDALLAS bzw. LUNYC den Zugriff.

```
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', ' ');
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', ' ');
```

*Abbildung 11. Angeben individueller Anwendungs-Requester-Verbindungen*

### Definieren von sekundären Servern

DB2 für MVS/ESA implementiert definierte Datenbank-Server nicht gemäß der DRDA-Definition. Statt dessen stellt DB2 für MVS/ESA sekundäre Server bereit, die durch systemgesteuerten Zugriff den Zugriff auf mehrere Systeme mit DB2 für MVS/ESA in einer einzelnen Arbeitseinheit bereitstellen.

**SQL-Unterschiede:** Das von systemgesteuertem Zugriff unterstützte SQL unterscheidet sich wesentlich von der fernen DRDA-Arbeitseinheit:

- Die SQL-Anweisung CONNECT wird nicht zur Herstellung einer Verbindung zu einem sekundären Server verwendet. Statt dessen wird durch die Angabe von dreiteiligen SQL-Objektnamen auf den Server zugegriffen. Beispielsweise wird die folgende SQL-Anweisung an den Server CHICAGO mit systemgesteuertem Zugriff weitergeleitet:

  ```
  SELECT * FROM CHICAGO.USER.TABLE;
  ```

- SQL-DDL-Anweisungen (z. B. CREATE) sind nicht zulässig.
- Fernes Binden (z. B. BIND PACKAGE) wird vom systemgesteuerten Zugriff nicht unterstützt, d. h. Sie brauchen Ihre Anwendung auf dem Server mit systemgesteuertem Zugriff vor der Ausführung der Anwendung nicht erst zu binden.
- Die an einen sekundären Server gesendeten SQL-Anweisungen können statisch oder dynamisch sein, alle Anweisungen werden jedoch dynamisch abgesetzt. Dazu kommt es, weil der sekundäre Server nicht über einen Plan bzw. ein Paket mit den SQL-Anweisungen der Anwendung verfügt, d. h. der Server kann die Datenbankzugriffspfade nicht im voraus auswählen.
- Eine einzelne SQL-Anwendung kann auf mehrere sekundäre Server gleichzeitig zugreifen.
- Mehrere Systeme mit DB2 für MVS/ESA (nicht nur eines) können das Ziel von SQL-Aktualisierungen in einem bestimmten COMMIT-Bereich sein.
- Eine Anwendung kann mehrere LU 6.2-Dialoge mit einem sekundären Server in einem einzelnen COMMIT-Bereich verwenden. Der Anwendungs-Server unter DB2 für MVS/ESA erstellt in der Regel für jede SQL-Abfrage mit Lesezugriff einen LU 6.2-Dialog. Dadurch kann der sekundäre Server die Abrufanforderungen (FETCH) voraussehen und die Antwortgruppe senden, bevor sie von der Anwendung angefordert wird.

**SQL-Objektnamen:** Wenn der Anwendungs-Server unter DB2 für MVS/ESA eine SQL-Anforderung empfängt, wird der SQL-Objektname überprüft, um zu ermitteln, wo sich das Objekt im Netzwerk befindet. DB2 für MVS/ESA akzeptiert ein-, zwei- und dreiteilige SQL-Objektnamen. Ein Name kann eines der folgenden Formate annehmen:

**objectname** gibt den Namen einer Tabelle, einer Sicht oder eines Synonyms oder einen Aliasnamen in DB2 für MVS/ESA an.

**authid.objectname** gibt den Objekteigner und den Objektnamen an.

**location.authid.objectname** gibt das Eignersystem, den Eigner und den Objektnamen an.

Wenn der Standortname (der erste Teil des dreiteiligen Objektnamens) mit dem RDB_NAME-Wert des lokalen Systems mit DB2 für MVS/ESA übereinstimmt, identifiziert die Anforderung ein lokales Objekt von DB2 für MVS/ESA.

Wenn der Standortname nicht mit dem RDB_NAME-Wert des lokalen Systems mit DB2 für MVS/ESA übereinstimmt, leitet der Anwendungs-Server unter DB2 für MVS/ESA die Anforderung über systemgesteuerten Zugriff an das System weiter, das durch den Standortnamen identifiziert wurde. Das Zielsystem muß ein weiteres System mit DB2 für MVS/ESA sein, weil systemgesteuerter Zugriff nur zwischen Systemen mit DB2 für MVS/ESA unterstützt wird. Funktionen für fernes Binden werden vom systemgesteuerten Zugriff nicht unterstützt, d. h. Sie brauchen Ihre Anwendung auf dem Server vor der Ausführung der Anwendung nicht erst zu binden. Abb. 12 auf Seite 36 faßt den von DB2 für MVS/ESA angewandten Prozeß zum Auflösen der SQL-Objektnamen zusammen.

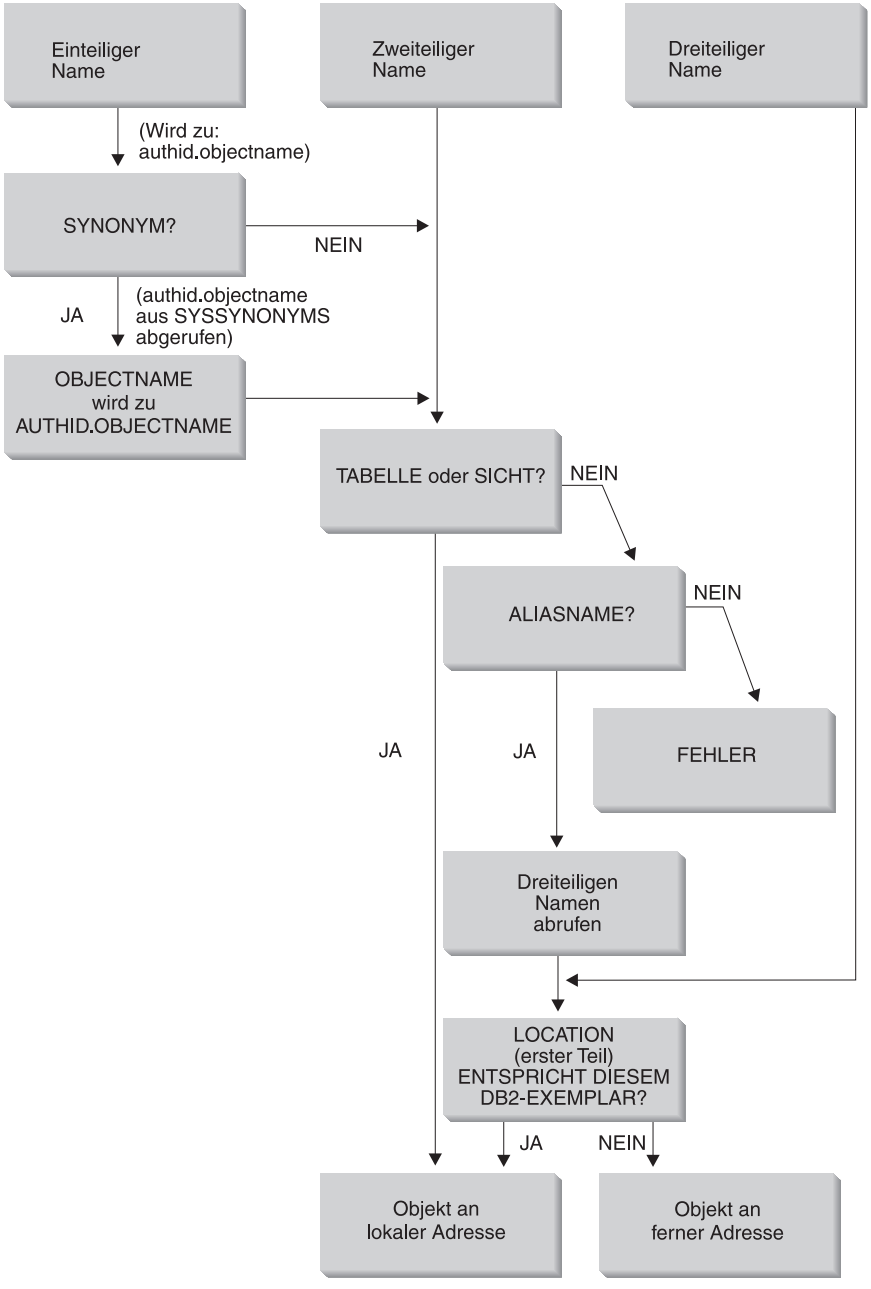


*Abbildung 12. SQL-Objektnamenauflösung unter DB2 für MVS/ESA*

**Server-Definition:** Wenn der Anwendungs-Server unter DB2 für MVS/ESA SQL-Anforderungen weiterleiten soll, müssen Sie alle sekundären Server in der Kommunikationsdatenbank und in VTAM definieren. Der Großteil des Definitionsprozesses ähnelt dem im Abschnitt „Definieren der fernen Systeme" auf Seite 16 beschriebenen Prozeß. Gehen Sie wie folgt vor, um sekundäre Server zu verbinden:

1. Tragen Sie die Werte für RDB_NAME und LU-Name für alle Server in der Kommunikationsdatenbank und in VTAM ein. Der vom systemgesteuerten Zugriff verwendete TPN-Wert weicht vom DRDA-Standardwert ab. Dieser Unterschied ist jedoch nicht wichtig, weil DB2 für MVS/ESA automatisch den korrekten Wert wählt.
2. Definieren Sie die Sicherheitsanforderungen für alle sekundären Server in der Tabelle SYSIBM.SYSLUNAMES. Dieser Prozeß wird in „Gewährleisten der Sicherheit" auf Seite 22 beschrieben.
3. Definieren Sie die zwischen dem Anwendungs-Server unter DB2 für MVS/ESA und den sekundären Servern verwendeten Modusnamen, und nehmen Sie diese Modusnamen in die VTAM-Modustabelle auf. Der Standardmodusname ist IBMDB2LM.
4. Definieren Sie die Sitzungsbegrenzungen für alle sekundären Server. Der Prozeß zum Definieren der Sitzungsbegrenzung entspricht dem im Abschnitt „Definieren des lokalen Systems" auf Seite 9 beschriebenen Prozeß. Systemgesteuerter Zugriff kann jedoch mehrere Dialoge für jede SQL-Anwendung definieren. Für Verbindungen mit systemgesteuertem Zugriff müssen Sie unter Umständen höhere Sitzungsbegrenzungen definieren als für DRDA-Verbindungen.Einzelheiten zur Berechnung der von Anwendungen mit systemgesteuertem Zugriff erforderlichen Anzahl LU 6.2-Sitzungen finden Sie im Abschnitt zum Verbinden verteilter Datenbanksysteme des Handbuchs *DB2 Systemverwaltung*.

Als Eigner der Datenbankressourcen steuert der sekundäre Server die Datenbanksicherheitsfunktionen für SQL-Objekte, die sich auf dem Server befinden. Diese Zuständigkeit teilt sich der sekundäre Server jedoch mit dem Anwendungs-Server unter DB2 für MVS/ESA, der die Anforderung absetzt. Der Zugriff auf SQL-Objekte wird wie folgt vom Server gesteuert:

- Der sekundäre Server verfügt nicht über eine Kopie des Plans von DB2 für MVS/ESA, d. h. der die Anforderung stellende Anwendungs-Server unter DB2 für MVS/ESA muß prüfen, ob der Endbenutzer auf dem die Anforderung stellenden System (dem Anwendungs-Server) über die Berechtigung zum Ausführen des Pakets verfügt.
- Statische SQL-Anweisungen werden auf dem sekundären Server dynamisch ausgeführt. Dazu werden die Zugriffsrechte herangezogen, die dem Eigner des Pakets von DB2 für MVS/ESA auf dem die Anforderung stellenden Anwendungs-Server unter DB2 für MVS/ESA erteilt wurden.

- Bei der Ausführung dynamischer SQL-Anweisungen werden die Zugriffsrechte herangezogen, die dem Endbenutzer auf dem Anwendungs-Requester erteilt wurden.

## Gewährleisten der Sicherheit

Wenn ein Anwendungs-Requester eine Anforderung für verteilte Datenbanken an den Anwendungs-Server unter DB2 für MVS/ESA weiterleitet, kann die Sicherheit in folgenden Bereichen eine Rolle spielen:

- Herkunftsüberprüfung
- Auswählen von Endbenutzernamen
- Sicherheitsparameter des Netzwerks
- Sicherheit des Datenbankmanagers
- Von einem externen Sicherheitssubsystem implementierte Sicherheit

### Herkunftsüberprüfung

Der Anwendungs-Server unter DB2 für MVS/ESA kann Einschränkungen für den Empfang von Endbenutzernamen von einem Anwendungs-Requester festlegen. Dazu wird die *Herkunftsüberprüfung* verwendet. Durch die Herkunftsüberprüfung kann der Anwendungs-Server angeben, daß eine bestimmte Benutzer-ID nur von bestimmten Partnern verwendet werden darf. Beispielsweise kann der Anwendungs-Server die Herkunft von JONES auf das System DALLAS beschränken. Wenn ein anderer Anwendungs-Requester (als DALLAS) versucht, den Namen JONES an den Anwendungs-Server zu senden, kann der Anwendungs-Server die Anforderung zurückweisen, weil der Name nicht vom korrekten Netzwerkstandort kommt.

DB2 für MVS/ESA implementiert die Herkunftsüberprüfung als Teil der Umsetzung von Endbenutzernamen für eingehende Anforderungen, die im nächsten Abschnitt beschrieben wird.

### Auswählen von Endbenutzernamen

Die vom Anwendungs-Requester übergebene Benutzer-ID ist möglicherweise nicht im gesamten SNA-Netzwerk eindeutig. Der Anwendungs-Server unter DB2 für MVS/ESA muß unter Umständen die Namensumsetzung für eingehende Anforderungen ausführen, um im gesamten SNA-Netzwerk eindeutige Endbenutzernamen erstellen zu können. Gleichermaßen muß der Anwendungs-Server unter DB2 für MVS/ESA unter Umständen die Namensumsetzung für abgehende Anforderungen ausführen, um den an der Anwendung beteiligten sekundären Servern einen eindeutigen Endbenutzernamen bereitzustellen. (Weitere Informationen zur Umsetzung von Endbenutzernamen für abgehende Anforderungen finden Sie in „Gewährleisten der Sicherheit” auf Seite 22.)

Die Namensumsetzung für eingehende Anforderungen wird durch das Setzen der Spalte USERNAMES in der Tabelle SYSIBM.SYSLUNAMES auf 'I'

(Namensumsetzung für eingehende Anforderungen) oder 'B' (Namensumsetzung für eingehende und abgehende Anforderungen) aktiviert. Wenn die Namensumsetzung für eingehende Anforderungen aktiviert ist, setzt DB2 für MVS/ESA die vom Anwendungs-Requester gesendete Benutzer-ID und den Eignernamen des Plans von DB2 für MVS/ESA um (wenn der Anwendungs-Requester ein weiteres System mit DB2 für MVS/ESA ist).

Wenn der Anwendungs-Requester eine Benutzer-ID und ein Kennwort an das APPC-Verb ALLOCATE sendet, werden die Benutzer-ID und das Kennwort vor der Umsetzung der Benutzer-ID auf Gültigkeit überprüft. Die Spalte PASSWORD in der Tabelle SYSIBM.SYSUSERNAMES wird nicht für die Gültigkeitsprüfung des Kennworts verwendet. Statt dessen werden die Benutzer-ID und das Kennwort dem externen Sicherheitssystem (RACF oder ein äquivalentes Produkt) zur Gültigkeitsprüfung übergeben.

Bei der Prüfung der ankommenden Benutzer-ID im Verb ALLOCATE kann DB2 für MVS/ESA mit Hilfe der Benutzerausgänge für Berechtigungsüberprüfungen eine Liste der sekundären Berechtigungs-IDs (AUTHIDs) bereitstellen und zusätzliche Sicherheitsprüfungen ausführen. Weitere Informationen finden Sie im Handbuch *DB2 Systemverwaltung*.

Der Prozeß zur Namensumsetzung für eingehende Anforderungen sucht in der Tabelle SYSIBM.SYSUSERNAMES nach einer Zeile, die einem der in der folgenden Liste gezeigten Muster entsprechen muß (TYPE.AUTHID.LUNAME):

1. I.AUTHID.LUNAME — ein bestimmter Endbenutzer von einem bestimmten Anwendungs-Requester
2. I.AUTHID.leer — ein bestimmter Endbenutzer von einem beliebigen Anwendungs-Requester
3. I.leer.LUNAME — ein beliebiger Endbenutzer von einem bestimmten Anwendungs-Requester

Wenn keine Zeile gefunden wird, wird der Fernzugriff verweigert. Wenn eine Zeile gefunden wird, wird der Fernzugriff erteilt, und der Endbenutzername wird in den von der Spalte NEWAUTHID bereitgestellten Wert geändert. Dabei gibt ein leerer NEWAUTHID-Wert an, daß der Name nicht geändert wird. Alle von DB2 für MVS/ESA ausgeführten Ressourcenberechtigungsprüfungen (z. B. SQL-Tabellenzugriffsrechte) werden an den umgesetzten Endbenutzernamen und nicht an den Originalbenutzernamen vorgenommen.

Beim Empfangen eines Endbenutzernamens vom Anwendungs-Requester durch den Anwendungs-Server unter DB2 für MVS/ESA können durch die Funktion zur Namensumsetzung für eingehende Anforderungen mehrere Ziele erreicht werden:

- Sie können einen Endbenutzernamen so ändern, daß er eindeutig ist. Beispielsweise setzen die folgenden SQL-Anweisungen den Endbenutzernamen JONES vom Anwendungs-Requester NEWYORK (LUNAME LUNYC) in einen anderen Namen (NYJONES) um.

```
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS,
              MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('I', 'JONES', 'LUNYC', 'NYJONES', ' ');
```

- Sie können den Endbenutzernamen ändern, um eine Gruppe von Endbenutzern durch einen einzelnen Namen zu repräsentieren. Beispielsweise könnten Sie alle Benutzer vom Anwendungs-Requester NEWYORK (LUNAME LUNYC) durch den Benutzernamen NYUSER repräsentieren. Dadurch können Sie dem Namen NYUSER SQL-Zugriffsrechte erteilen und den SQL-Zugriff steuern, der den Benutzern des Systems NEWYORK erteilt wird.

```
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS,
              MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
  VALUES ('I', ' ', 'LUNYC', 'NYUSER', ' ');
```

- Sie können die durch einen bestimmten Anwendungs-Requester übertragenen Endbenutzernamen einschränken. Durch diese Verwendung der Umsetzung für Endbenutzernamen wird die im Abschnitt „Herkunftsüberprüfung” auf Seite 38 beschriebene Herkunftsüberprüfung erzielt. Beispielsweise lassen die folgenden SQL-Anweisungen nur SMITH und JONES als Endbenutzernamen vom Anwendungs-Requester NEWYORK zu. Allen anderen Namen wird der Zugriff verweigert, weil sie nicht in der Tabelle SYSIBM.SYSUSERNAMES aufgelistet sind.

```
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS,
              MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('I', 'SMITH', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('I', 'JONES', 'LUNYC', ' ', ' ');
```

- Sie können die Anwendungs-Requester einschränken, denen die Verbindung zum Anwendungs-Server unter DB2 für MVS/ESA erlaubt wird. Dies ist eine weitere Funktion der Herkunftsüberprüfung. Im folgenden Beispiel werden alle an den Anwendungs-Requester NEWYORK (LUNYC) und den Anwendungs-Requester CHICAGO (LUCHI) gesendeten Endbenutzernamen akzeptiert. Anderen Anwendungs-Requestern wird der Zugriff verwei-

gert, weil in der Standardzeile der Tabelle SYSIBM.SYSLUNAMES die Namensumsetzung für alle eingehenden Anforderungen angegeben ist.

```
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS,
              MODESELECT, USERNAMES)
VALUES (' ', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('I', ' ', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('I', ' ', 'LUCHI', ' ', ' ');
```

### Gewährleisten der Netzwerksicherheit

LU 6.2 stellt die folgenden drei Hauptsicherheitseinrichtungen für das Netzwerk zur Verfügung:

- Sicherheit auf Sitzungsebene
- Sicherheit auf Dialogebene
- Verschlüsselung

Im Abschnitt „Netzwerksicherheit” auf Seite 25 wird die Angabe der Sicherheit auf Sitzungsebene und der Verschlüsselung unter DB2 für MVS/ESA erläutert. Die Verwendung von Sicherheit auf Sitzungsebene und von Verschlüsselung seitens des Anwendungs-Servers unter DB2 für MVS/ESA entspricht genau der seitens des Anwendungs-Requesters unter DB2 für MVS/ESA.

In punkto Netzwerksicherheit muß nun nur noch die SNA-Dialogsicherheitsstufe behandelt werden. Einige der Aspekte der Dialolgsicherheitsstufe gelten nur für einen Anwendungs-Server unter DB2 für MVS/ESA. Der Anwendungs-Server unter DB2 für MVS/ESA spielt in der Netzwerksicherheit zwei unterschiedliche Rollen:

- Zum einen ist der Anwendungs-Server unter DB2 für MVS/ESA als Requester für sekundäre Server für das Absetzen von APPC-Anforderungen zuständig, die die für sekundäre Server erforderlichen Parameter der SNA-Dialogsicherheitsstufe enthalten. Der Anwendungs-Server unter DB2 für MVS/ESA definiert die Anforderungen der SNA-Dialogsicherheitsstufe für alle sekundären Server unter Verwendung der Spalte USERNAMES in der Tabelle SYSIBM.SYSLUNAMES und der Tabelle SYSIBM.SYSUSERNAMES. Die Einzelangaben dieser Definitionen entsprechen denen im Abschnitt „Netzwerksicherheit” auf Seite 25.
- Zum anderen diktiert der Anwendungs-Server unter DB2 für MVS/ESA als Server für den Anwendungs-Requester die Anforderungen der SNA-Dialogsicherheitsstufe für den Anwendungs-Requester. DB2 für MVS/ESA ermittelt die für jeden Anwendungs-Requester im Netzwerk erforderliche

Dialogsicherheit unter Verwendung der Spalte USERSECURITY in der Tabelle SYSIBM.SYSLUNAMES. Folgende Werte werden in der Spalte USERSECURITY verwendet:

**C** Hiermit wird angegeben, daß DB2 für MVS/ESA vom Anwendungs-Requester das Senden einer Benutzer-ID und eines Kennworts (LU 6.2 SECURITY=PGM) bei jeder Anforderung für verteilte Datenbanken erfordert. Wenn in der Spalte ENCRYPTPSWDS der Tabelle SYSIBM.SYSLUNAMES ein 'Y' enthalten ist, geht DB2 für MVS/ESA davon aus, daß das Kennwort bereits in verschlüsseltem RACF-Format vorliegt (dies ist nur für einen Anwendungs-Requester unter DB2 für MVS/ESA möglich). Wenn in der Spalte ENCRYPTPSWDS kein 'Y' enthalten ist, erwartet DB2 für MVS/ESA das Kennwort im LU 6.2-Standardformat (EBCDIC-Zeichendarstellung). In beiden Fällen übergibt DB2 für MVS/ESA die Werte für Benutzer-ID und Kennwort zur Gültigkeitsprüfung an das Sicherheitssubsystem. Ihr Sicherheitssubsystem muß eine Prüfung von APPC-Benutzer-ID und APPC-Kennwort bereitstellen, wie z. B. RACF. Wenn das Sicherheitssubsystem das Paar aus Benutzer-ID und Kennwort zurückweist, wird der Zugriff auf verteilte Datenbanken verweigert.

**Jeder andere Wert**
Hiermit wird angegeben, daß der Anwendungs-Requester eine bereits überprüfte Benutzer-ID (LU 6.2 SECURITY=SAME) oder eine Benutzer-ID und ein Kennwort (LU 6.2 SECURITY=PGM) senden kann. Wenn eine Benutzer-ID und ein Kennwort gesendet werden, verarbeitet DB2 für MVS/ESA sie wie für 'C' oben beschrieben. Wenn in der Anforderung nur eine Benutzer-ID enthalten ist, wird das Sicherheitssubsystem aufgerufen, um den Benutzer zu überprüfen, sofern nicht die Tabelle SYSUSERNAMES zum Verwalten der eingehenden Benutzer-IDs verwendet wird.

Wenn eine Sicherheitsverletzung festgestellt wird, fordert LU 6.2 den Anwendungs-Server unter DB2 für MVS/ESA auf, dem Anwendungs-Requester den Prüfcode der SNA-Sicherheitsstörung ('080F6051'X) zu liefern. Da dieser Prüfcode die Fehlerursache nicht beschreibt, werden von DB2 für MVS/ESA zwei Methoden zum Aufzeichnen der Ursache der Sicherheitsverletzung in einer verteilten Umgebung bereitgestellt:

- Eine Nachricht DSNL030I mit der LUWID des Requesters und einem DB2-Ursachencode, der den Fehler beschreibt, wird angezeigt. DSNL030I enthält auch (sofern bekannt) die zurückgewiesene AUTHID, die von der Anwendungsanforderung gesendet wurde.
- In der NetView-Datenbank für Hardwareüberwachung wird ein Alert eingetragen, der die gleichen Informationen wie die Nachricht DSNL030I enthält.

### Sicherheit des Datenbankmanagers

Als Eigner der Datenbankressourcen steuert der Anwendungs-Server unter DB2 für MVS/ESA die Datenbanksicherheitsfunktionen für SQL-Objekte, die sich auf dem Anwendungs-Server unter DB2 für MVS/ESA befinden. Der Zugriff auf von DB2 für MVS/ESA verwaltete Objekte wird durch Zugriffsrechte gesteuert, die Benutzern durch den Administrator von DB2 für MVS/ESA oder durch die Eigner der einzelnen Objekte erteilt werden. Der Anwendungs-Server unter DB2 für MVS/ESA steuert die folgenden beiden grundlegenden Objektklassen:

- **Pakete**— Einzelne Endbenutzer erhalten mit Hilfe der DB2 für MVS/ESA.Anweisung GRANT die Berechtigung zum Erstellen, Ersetzen und Ausführen von Paketen. Wenn ein Endbenutzer der Eigner eines Pakets ist, kann er das Paket automatisch ausführen und ersetzen. Anderen Endbenutzern muß mit der Anweisung GRANT ausdrücklich die Berechtigung zum Ausführen eines Pakets auf dem Anwendungs-Server unter DB2 für MVS/ESA erteilt werden. Die Berechtigung USE kann für einzelne Endbenutzer erteilt werden oder für PUBLIC, d. h. alle Endbenutzer dürfen das Paket ausführen.

  Nach dem Binden einer Anwendung an DB2 für MVS/ESA enthält das Paket die im Anwendungsprogramm enthaltenen SQL-Anweisungen. Diese SQL-Anweisungen werden wie folgt klassifiziert:

  **Statisches SQL**

  Statisches SQL bedeutet, daß die SQL-Anweisung und die SQL-Objekte, auf die in der Anweisung verwiesen wird, zum Zeitpunkt des Bindens der Anwendung an DB2 für MVS/ESA bekannt sind. Der Ersteller des Pakets muß über die Berechtigung zum Ausführen für jede der statischen SQL-Anweisungen in dem Paket verfügen.

  Wenn Endbenutzer die Berechtigung zum Ausführen eines Pakets erhalten, verfügen sie damit automatisch über die Berechtigung zum Ausführen aller statischen SQL-Anweisungen in dem Paket. Dies bedeutet, daß Endbenutzer keine Tabellenzugriffsrechte von DB2 für MVS/ESA benötigen, wenn das Paket ausschließlich statische SQL-Anweisungen enthält.

  **Dynamisches SQL**

  Dynamisches SQL bezeichnet eine SQL-Anweisung, die vor der Ausführung des Pakets nicht bekannt ist. Mit anderen Worten, die SQL-Anweisung wird von dem betreffenden Programm erstellt und durch die SQL-Anweisung PREPARE dynamisch an DB2 für MVS/ESA gebunden. Wenn ein Endbenutzer eine dynamische SQL-Anweisung ausführt, muß er über die erforderlichen Tabellenzugriffsrechte zum Ausführen der SQL-Anweisung verfügen. Da die SQL-Anweisung bei der Erstellung des Plans bzw. Pakets noch nicht bekannt ist, wird dem Endbenutzer die erforderliche Berechtigung vom Paketeigner nicht automatisch erteilt.

- **SQL-Objekte:** Hierbei handelt es sich um Tabellen, Sichten, Synonyme oder Aliasnamen. Benutzern von DB2 für MVS/ESA können verschiedene Berechtigungsstufen zum Erstellen, Löschen, Ändern oder Lesen einzelner SQL-Objekte erteilt werden. Diese Berechtigung ist für das Binden statischer SQL-Anweisungen und zum Ausführen dynamischer SQL-Anweisungen erforderlich.

Beim Erstellen eines Pakets können Sie mit der Option DISABLE/ENABLE steuern, welche Verbindungsarten von DB2 für MVS/ESA das Paket ausführen können. Sie können mit RACF und Sicherheitsausgangsroutinen von DB2 für MVS/ESA Endbenutzern selektiv die Verwendung von DDF erlauben. Sie können mit RLF Angaben zur Begrenzung der Verarbeitungszeit für ferne Bindevorgänge und für die Ausführung dynamischer SQL-Anweisungen vornehmen.

Beispiel: Der Eigner eines Pakets von DB2 für MVS/ESA namens MYPKG heißt JOE. JOE kann SAL die Berechtigung zum Ausführen des Pakets durch Absetzen der Anweisung GRANT USE von DB2 für MVS/ESA erteilen. Wenn SAL das Paket ausführt, geschieht folgendes:

- DB2 für MVS/ESA prüft, ob SAL die Berechtigung USE für das Paket erteilt wurde.
- SAL kann alle statischen SQL-Anweisungen im Paket absetzen, weil JOE über die erforderlichen SQL-Objektzugriffsrechte zum Erstellen des Pakets verfügt.
- Wenn das Paket dynamische SQL-Anweisungen enthält, muß SAL über eigene SQL-Tabellenzugriffsrechte verfügen. Beispielsweise kann SAL SELECT * FROM JOE.TABLE5 erst absetzen, nachdem SAL der Lesezugriff auf JOE.TABLE5 erteilt wurde.

### Sicherheitssubsystem

Die Verwendung des Sicherheitssubsystems (RACF oder ein äquivalentes Produkt) durch den Anwendungs-Server unter DB2 für MVS/ESA hängt davon ab, wie Sie die Funktion zur Namensumsetzung für eingehende Anforderungen für Namen in der Tabelle SYSIBM.SYSLUNAMES definieren:

- Wenn Sie 'I' oder 'B' für die Spalte USERNAMES angeben, ist die Namensumsetzung für eingehende Anforderungen aktiv, und DB2 für MVS/ESA nimmt an, daß der Administrator von DB2 für MVS/ESA die Namensumsetzung für eingehende Anforderungen als Teil der Systemsicherheitsimplementierung ausführt. Das externe Sicherheitssubsystem wird nur aufgerufen, wenn der Anwendungs-Requester eine Anforderung mit Benutzer-ID und Kennwort (SECURITY=PGM) sendet. Ihr Sicherheitssubsystem muß eine Prüfung von APPC-Benutzer-ID und APPC-Kennwort bereitstellen, wie z. B. RACF.

Wenn die Anforderung des Anwendungs-Requesters nur eine Benutzer-ID enthält (SECURITY=SAME), wird das externe Sicherheitssystem nicht aufgerufen, weil die Regeln der Namensumsetzung für eingehende Anforderungen definieren, welche Benutzer eine Verbindung zum Anwendungs-Server unter DB2 für MVS/ESA herstellen dürfen.

- Wenn Sie eine andere Angabe als 'I' oder 'B' für die Spalte USERNAMES vornehmen, werden die folgenden Sicherheitssubsystemüberprüfungen ausgeführt:
  - Wenn eine Anforderung für verteilte Datenbanken des Anwendungs-Requesters empfangen wird, ruft DB2 für MVS/ESA das externe Sicherheitssystem auf, um die Gültigkeit der Benutzer-ID (und des Kennworts, sofern bereitgestellt) des Endbenutzers zu überprüfen.
  - Das externe Sicherheitssystem wird aufgerufen, um zu prüfen, ob der Endbenutzer über die Berechtigung zur Verbindungsherstellung zum Subsystem mit DB2 für MVS/ESA verfügt.
- In jedem Fall wird ein Benutzerausgang für Berechtigungsüberprüfungen implementiert, um eine Liste der sekundären Berechtigungs-IDs bereitzustellen. Weitere Informationen finden Sie im Handbuch *DB2 Systemverwaltung*.

## Darstellen von Daten

Sie müssen sicherstellen, daß Ihr Subsystem mit DB2 für MVS/ESA die CCSIDs der einzelnen Anwendungs-Requester in die Installations-CCSID des Subsystems mit DB2 für MVS/ESA umsetzen kann. Weitere Informationen finden Sie in „Darstellen von Daten” auf Seite 29.

# Kapitel 2. Verbinden von DB2 Universal Database für OS/390 in einem DRDA-Netzwerk

DB2 Universal Database für OS/390 ist das Verwaltungssystem für relationale Datenbanken von IBM für OS/390-Systeme. In diesem Kapitel werden frühere Releases nicht behandelt. Weitere Informationen finden Sie in „Kapitel 1. Verbinden von DB2 für MVS/ESA in einem DRDA-Netzwerk" auf Seite 1.

In diesem Kapitel wird beschrieben, wie Sie DRDA-Anwendungs-Requester (z. B. DB2 Connect) mit einem Anwendungs-Server unter DB2 Universal Database für OS/390 verbinden und wie Sie Anwendungs-Requester unter DB2 Universal Database für OS/390 für die Kommunikation mit DRDA-Anwendungs-Servern wie DB2 Universal Database auf anderen Systemen definieren.

Der Schwerpunkt der Informationen in diesem Kapitel liegt auf dem Verbinden von ungleichen DRDA-Systemen mit DB2 Universal Database für OS/390 über SNA-Netzwerkverbindungen. Für DB2 Universal Database für OS/390 Version 5 wurde jedoch Unterstützung für die Kommunikation von Datenbanken über eigenständige TCP/IP-Verbindungen (nicht über AnyNet) entwickelt. Daher wird auch die Verwendung von TCP/IP-Verbindungen bis zu einem gewissen Grad erläutert. Ausführliche Informationen zum Definieren und Verwenden von TCP/IP-Verbindungen finden Sie in den Handbüchern *DB2 Universal Database für OS/390 Installation* und *DRDA Support for TCPIP with DB2 Universal Database für OS/390 and DB2 Universal Database*.

Weitere Informationen zur Herstellung von Verbindungen zwischen zwei Systemen mit DB2 Universal Database für OS/390 und zur Definition von DRDA-Verbindungen zu Systemen mit DB2 Universal Database für OS/390 finden Sie im Abschnitt zum Verbinden von Systemen mit verteilten Datenbanken im Handbuch *DB2 Universal Database for OS/390 Administration Guide*.

**Anmerkungen:**

1. Die AnyNet-Funktion von VTAM Version 4 Release 2 ermöglicht das Ausführen von APPC über ein TCP/IP-Netzwerk. Benutzern von DB2 Universal Database für OS/390 Version 5.1 wird empfohlen, Unterstützung für eigenständige TCP/IP-Verbindungen anstelle von AnyNet-APPC über die TCP/IP-Funktion zu verwenden.
2. Dieses Kapitel enthält keine Informationen zur Verwendung von DCE (Distributed Computing Environment - Umgebung für verteilte Datenverarbeitung).

## DB2 Universal Database für OS/390

Abb. 13 zeigt ein OS/390-System, auf dem eine einzelne Kopie von DB2 Universal Database für OS/390 ausgeführt wird. Auf einem einzelnen System können aber auch mehrere Kopien von DB2 Universal Database für OS/390 ausgeführt werden. Zur Identifikation von Kopien von DB2 Universal Database für OS/390 auf einem bestimmten System (bzw. von Kopien von DB2 Universal Database für OS/390 innerhalb eines JES-Komplexes) wird jedem DB2-System ein *Subsystemname* gegeben, der eine 1 bis 4 Zeichen lange eindeutige Folge innerhalb eines JES-Komplexes ist. In Abb. 13 ist der Name des DB2 Universal Database für OS/390-Subsystems *xxxx*. Vier der OS/390-Adreßraumnamen wird der Subsystemname von DB2 Universal Database für OS/390 vorangestellt. Jeder dieser vier Adreßräume hat Anteil an der ordnungsgemäßen Funktionsweise von DB2 Universal Database für OS/390.

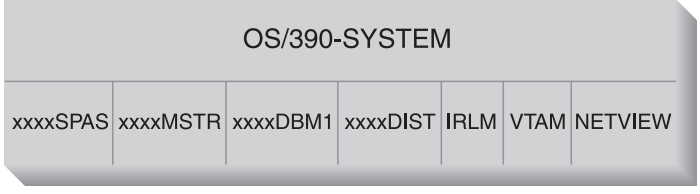


*Abbildung 13. Von OS/390 verwendete Adreßräume*

Abb. 13 zeigt die OS/390-Adreßräume, die an der Verarbeitung für verteilte Datenbanken durch DB2 Universal Database für OS/390 beteiligt sind. Diese Adreßräume arbeiten zusammen, um Benutzern von DB2 Universal Database für OS/390 den Zugriff auf lokale relationale Datenbanken und Kommunikation mit fernen DRDA-Systemen zu ermöglichen. Die einzelnen Adreßräume werden im folgenden erklärt:

**xxxxSPAS**
: Der Adreßraum für gespeicherte DB2-Prozeduren

**xxxxMSTR**
: Der Adreßraum des Systemservice von DB2 Universal Database für OS/390, der für das Starten und Stoppen von DB2 Universal Database für OS/390 sowie das Steuern des lokalen Zugriffs auf DB2 Universal Database für OS/390 zuständig ist.

**xxxxDBM1**
Der Adreßraum des Datenbankservice, der für den Zugriff auf von DB2 Universal Database für OS/390 gesteuerte relationale Datenbanken zuständig ist. Hier wird im Auftrag von SQL-Anwendungsprogrammen die Eingabe in und Ausgabe von Datenbankressourcen ausgeführt.

**xxxxDIST**
Die Komponente von DB2 Universal Database für OS/390, die Funktionen für verteilte Datenbanken bereitstellt; auch als DDF (*Distributed Data Facility*) bekannt. Wenn eine Anforderung für verteilte Datenbanken empfangen wird, übergibt DDF die Anforderung an *xxxx*DBM1, damit die erforderlichen Datenbank-E/A-Operationen ausgeführt werden können.

**IRLM** Der von DB2 Universal Database für OS/390 verwendete Sperrenmanager (Lock Manager) zum Steuern des Zugriffs auf Datenbankressourcen.

**VTAM**
SNA-Funktionen (VTAM) von IBM Communications Server für OS/390; DDF verwendet SNA bzw. TCP/IP im Auftrag von DB2 Universal Database für OS/390 zum Ausführen von Kommunikation für verteilte Datenbanken. In dieses Diagramm wurde kein Adreßraum für TCP/IP aufgenommen.

**NETVIEW**
Das zentrale Alert-Verarbeitungssystem der Netzwerkverwaltung auf OS/390-Systemen; wenn während der Verarbeitung für verteilte Datenbanken Fehler auftreten, zeichnet DDF Fehlerinformationen (auch als *Alerts* bekannt) in der NetView-Datenbank für Hardwareüberwachung auf. Systemadministratoren können mit NetView die in der Datenbank für Hardwareüberwachung gespeicherten Fehler überprüfen oder den automatischen Aufruf von Befehlsprozeduren beim Aufzeichnen der Alert-Bedingungen einrichten.

Mit NetView können Sie auch eine Diagnose der VTAM-Übertragungsfehler erstellen. Weitere Informationen finden Sie im Handbuch *Distributed Relational Database Architecture Problem Determination Guide*.

Abb. 13 auf Seite 48 zeigt keine SQL-Anwendungsprogramme. Wenn ein Anwendungsprogramm mit DB2 SQL-Anweisungen absetzt, muß es auf eine der folgenden Arten eine Verbindung zu DB2 Universal Database für OS/390 herstellen:

**TSO** Für Stapeljobs und an TSO angemeldete Endbenutzer wird über die TSO-Verbindungseinrichtung eine Verbindung zu DB2 Universal Database für OS/390 hergestellt. Mit diesem Verfahren wird die Verbindung von SPUFI-Anwendungen und den meisten QMF-Anwendungen zu DB2 Universal Database für OS/390 hergestellt.

**CICS/ESA**
Wenn eine CICS/ESA-Anwendung SQL-Aufrufe absetzt, verwendet das CICS/ESA-Produkt die CICS-Verbindungsschnittstelle, um SQL-Anforderungen an DB2 Universal Database für OS/390 weiterzuleiten.

**IMS/ESA**
Transaktionen, die unter der Steuerung von IMS/ESA ausgeführt werden, verwenden die IMS-Verbindungsschnittstelle, um SQL-Anweisungen zur Verarbeitung an DB2 Universal Database für OS/390 zu übergeben.

**DDF** DDF (Distributed Data Facility) ist für die Herstellung der Verbindung verteilter Anwendungen zu DB2 Universal Database für OS/390 zuständig.

**CAF** CAF (Call Attachment Facility) ermöglicht benutzerdefinierten Subsystemen die Herstellung einer direkten Verbindung zu DB2 Universal Database für OS/390.

## Implementierung von DB2 Universal Database für OS/390

DRDA definiert die Funktionsarten des Verwaltungssystems für verteilte Datenbanken. DB2 Universal Database für OS/390 unterstützt ferne Arbeitseinheiten. Durch ferne Arbeitseinheiten kann ein auf einem System ausgeführtes Anwendungsprogramm eines fernen Datenbankverwaltungssystems zugreifen (mit Hilfe der vom fernen Datenbankverwaltungssystem bereitgestellten SQL-Anweisungen).

DB2 Universal Database für OS/390 unterstützt auch verteilte Arbeitseinheiten. Durch verteilte Arbeitseinheiten kann ein auf einem System ausgeführtes Anwendungsprogramm auf Daten mehrerer ferner Datenbankverwaltungssysteme zugreifen (mit Hilfe der von den fernen Datenbankverwaltungssystemen bereitgestellten SQL-Anweisungen). Weitere Informationen zu von DRDA definierten Verteilungsarten finden Sie im Handbuch *DRDA Connectivity Guide*.

Wie in Abb. 14 auf Seite 52 gezeigt, unterstützt DB2 Universal Database für OS/390 drei Konfigurationen von Verbindungen für verteilte Datenbanken unter Verwendung von zwei Zugriffsmethoden:

**[1]** *Systemgesteuerter Zugriff* (auch als die Verwendung des *privaten Protokolls von DB2 Universal Database für OS/390* bekannt) ermöglicht einem Requester unter DB2 Universal Database für OS/390 die Verbindung zu

mindestens einem Server unter DB2 Universal Database für OS/390. Die zwischen dem Requester und Server unter DB2 Universal Database für OS/390 hergestellte Verbindung hält sich nicht an die in DRDA definierten Protokolle und kann nicht zur Herstellung einer Verbindung zwischen anderen Produkten als DB2 Universal Database für OS/390 und DB2 Universal Database für OS/390 verwendet werden. Diese Art der Verbindung wird durch die Codierung von dreiteiligen Namen oder Aliasnamen in der Anwendung hergestellt.

**[2]** *Anwendungsgesteuerter Zugriff* ermöglicht einem Requester unter DB2 Universal Database für OS/390 oder unter einem anderen Produkt als DB2 Universal Database für OS/390 wie DB2 Connect die Verbindung zu mindestens einem Anwendungs-Server unter DB2 Universal Database für OS/390 oder einem anderen Produkt als DB2 Universal Database für OS/390 wie DB2 Universal Database und DB2 Universal Database für AS/400 über DRDA-Protokolle. Die Anzahl Anwendungs-Server, für die jeweils eine Verbindung zum Anwendungs-Requester bestehen kann, hängt von der Version von DB2 Universal Database für OS/390 für den Anwendungs-Requester ab. Wenn der Anwendungs-Requester unter DB2 für MVS/ESA Version 2 Release 3 läuft, kann nur zu jeweils einem einzigen Anwendungs-Server eine Verbindung hergestellt werden. Diese Art der Verbindung wird durch die Codierung von SQL-Anweisungen CONNECT in der Anwendung hergestellt. Wenn der Anwendungs-Requester unter DB2 für MVS/ESA Version 3 Release 1 oder höher läuft, kann die Verbindung zu mehreren Anwendungs-Servern gleichzeitig hergestellt werden.

**[3]** Anwendungsgesteuerter und systemgesteuerter Zugriff können zur Verbindungsherstellung gemeinsam verwendet werden. Sie können eine Verbindung nicht über DRDA und systemgesteuerte Speicherung im gleichen Thread herstellen.

Der Begriff *sekundärer Server* beschreibt Systeme, die für den Anwendungs-Server als Server fungieren.

Wenn alle Systeme in einer Konfiguration zweiphasige Festschreibung unterstützen, werden verteilte Arbeitseinheiten (Lesen und Aktualisieren von auf mehrere Standorte verteilten Daten) unterstützt. Wenn nicht alle Systeme zweiphasige Festschreibung unterstützen, sind Aktualisierungen innerhalb einer Arbeitseinheit auf einen einzelnen Standort beschränkt, der zweiphasige Festschreibung nicht unterstützt, oder auf die Untergruppe der Standorte, die zweiphasige Festschreibung unterstützen.

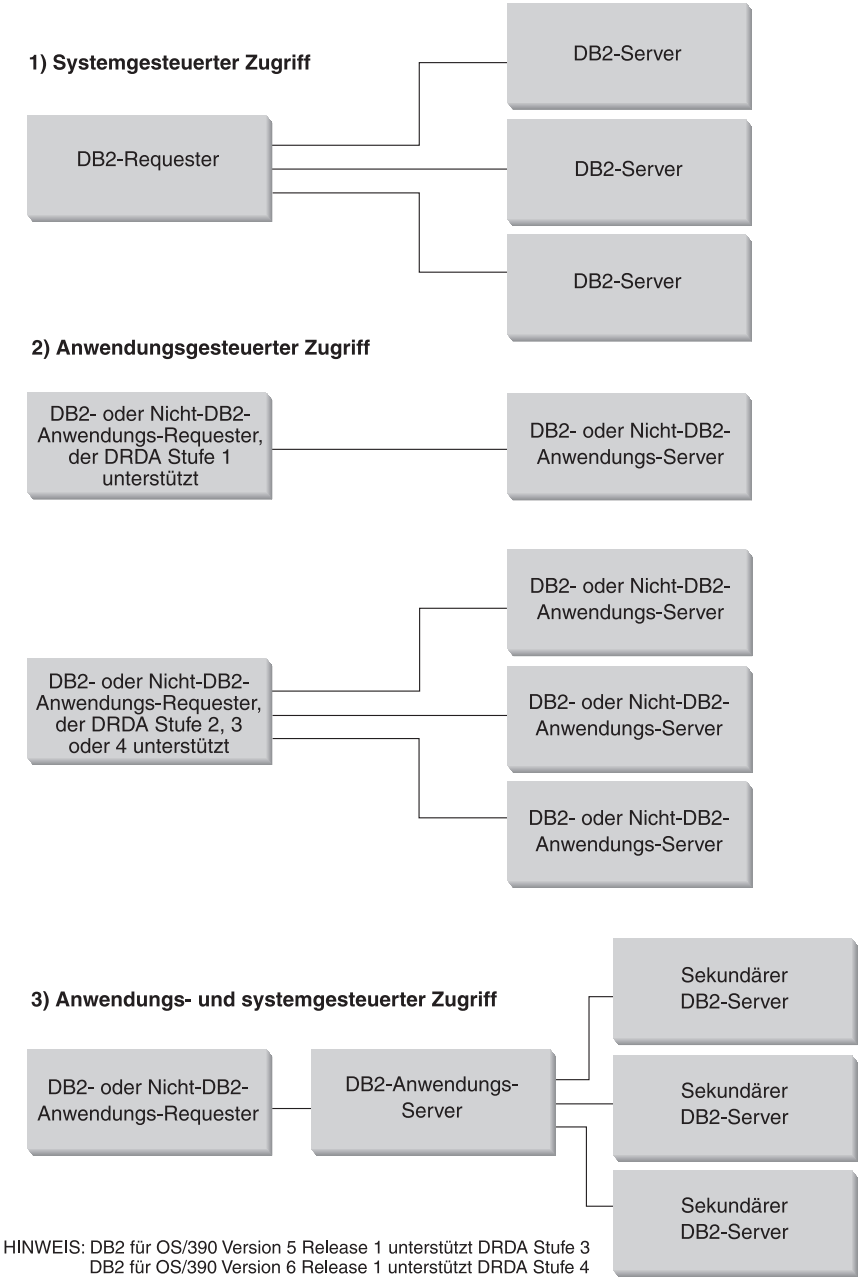


*Abbildung 14. Verteilte Verbindungen von DB2 Universal Database für OS/390*

Tabelle 2 vergleicht die Verbindungsarten verteilter Datenbanken von DB2 Universal Database für OS/390.

*Tabelle 2. Vergleich der Verbindungen verteilter Datenbanken von DB2 Universal Database für OS/390*

| **[1] Systemgesteuerter Zugriff** | **[2] Anwendungsgesteuerter Zugriff (alle Systeme unterstützen zweiphasige Festschreibung)** | **[3] Anwendungsgesteuerter und systemgesteuerter Zugriff** |
|---|---|---|
| Alle Partner müssen Systeme mit DB2 Universal Database für OS/390 sein. | Kann Verbindung zwischen zwei DRDA-Systemen herstellen. | Der Anwendungs-Requester kann ein beliebiges DRDA-System sein. Server müssen Systeme mit DB2 Universal Database für OS/390 sein. |
| Kann direkte Verbindung zu vielen Partnern herstellen. | Kann direkte Verbindung zu vielen Partnern herstellen. | Der Anwendungs-Requester stellt direkte Verbindungen zu Anwendungs-Servern her. Anwendungs-Server können Verbindungen zu vielen sekundären Servern unter DB2 Universal Database für OS/390 herstellen. |
| Jede SQL-Anwendung kann für jeden Server mehrere Dialoge einrichten. | Jede SQL-Anwendung richtet für jeden Server einen Dialog ein. | Die SQL-Anwendung richtet für jeden Server einen Dialog ein. Anwendungs-Server unter DB2 Universal Database für OS/390 können für die Anwendung viele Dialoge mit jedem Server herstellen. |
| Kann sowohl auf lokale als auch auf ferne Ressourcen in einem COMMIT-Bereich zugreifen. | Kann sowohl auf lokale als auch auf ferne Ressourcen in einem COMMIT-Bereich zugreifen. | Anwendungs-Requester und Anwendungs-Server können auf lokale und ferne Daten zugreifen. |
| Effektiver bei großen Abfragen und mehreren gleichzeitig ablaufenden Abfragen | Effektiver bei SQL-Anweisungen, die in einem COMMIT-Bereich nicht häufig ausgeführt werden | Verbindungen zwischen Anwendungs-Requester und Anwendungs-Server verhalten sich wie **[2]**. Verbindungen zu sekundären Servern verhalten sich wie **[1]**. |
| Kann statisches oder dynamisches SQL unterstützen, der Server bindet statisches SQL bei der Erstausführung in einem COMMIT-Bereich jedoch dynamisch. | Kann statisches oder dynamisches SQL absetzen. | Anwendungs-Requester und Anwendungs-Server können statisches oder dynamisches SQL absetzen. Sekundäre Server unterstützen statisches oder dynamisches SQL, binden statisches SQL bei der Erstausführung in einem COMMIT-Bereich jedoch dynamisch. |

*Tabelle 2. Vergleich der Verbindungen verteilter Datenbanken von DB2 Universal Database für OS/390 (Forts.)*

| [1] Systemgesteuerter Zugriff | [2] Anwendungsgesteuerter Zugriff (alle Systeme unterstützen zweiphasige Festschreibung) | [3] Anwendungsgesteuerter und systemgesteuerter Zugriff |
|---|---|---|
| Auf die SQL-Anweisungen INSERT, DELETE und UPDATE und auf Anweisungen beschränkt, die SELECT unterstützen. | Kann eine Anweisung verwenden, die vom die Anweisung ausführenden System unterstützt wird. | Anwendungs-Server unterstützen beliebiges SQL, sekundäre Server unterstützen nur DML-SQL (z. B. CREATE oder ALTER). |

## Zusätzliche Sicherheitsverbesserungen

### Erweiterte Sicherheitscodes

Bis DB2 Universal Database für OS/390 Version 5.1 konnte es vorkommen, daß Verbindungsanforderungen, die Benutzer-IDs oder Kennwörter angaben, mit SQL30082 Ursachencode 0 fehlschlugen, aber keine andere Nachricht mit Angaben zur Fehlerursache ausgegeben wurde.

In DB2 Universal Database für OS/390 Version 5.1 wurde eine Erweiterung eingeführt, die Unterstützung für erweiterte Sicherheitscodes zur Verfügung stellt. Durch das Angeben erweiterter Sicherheitscodes werden zusätzliche Diagnoseinformationen, beispielsweise Informationen zu einem abgelaufenen Kennwort zusätzlich zum Ursachencode geliefert.

Um diese Möglichkeiten nutzen zu können, muß der DB2 Universal Database für OS/390-Installationsparameter ZPARM für erweiterte Sicherheit auf YES eingestellt werden. Mit der Installationsanzeige DSN6SYSP von DB2 Universal Database für OS/390 kann EXTSEC=YES eingestellt werden. Sie können dafür auch DDF-Anzeige 1 (DSNTIPR) verwenden. Der Standardwert ist EXTSEC=NO. Falls das Kennwort nicht mehr gültig ist, wird von Anwendungen für Personal Computer, UNIX, Apple Macintosh und das Web, die mit DB2 Connect arbeiten, die Fehlernachricht SQL01404 empfangen.

### Bereits überprüfte TCP/IP-Sicherheit

Wenn Sie Unterstützung für die Sicherheitsoption AUTHENTICATION=CLIENT von DB2 Universal Database wünschen, geben Sie in der Installationsanzeige DSNTIP4 von DB2 Universal Database für OS/390 (DDF-Anzeige 2) mit YES an, daß die TCP/IP-Sicherheit bereits überprüft ist.

### Sicherheit für ODBC- und Java-Anwendungen auf Workstations

ODBC- und Java-Anwendungen auf Workstations verwenden dynamisches SQL. Dies kann bei einigen Installationen Sicherheitsfragen aufwerfen. DB2 Universal Database für OS/390 führt eine neue Bindeoption, DYNAMICRULES-(BIND), ein, die die Ausführung von dynamischem SQL unter der Berechti-

gung des Eigners oder des Binders zuläßt. Informationen zur Angabe von DYNAMICRULES über DB2 Connect finden Sie im Handbuch *Command Reference*.

DB2 Universal Database und DB2 Connect bieten einen neuen CLI/ODBC-Konfigurationsparameter, CURRENTPACKAGESET, in der Konfigurationsdatei DB2CLI.INI. Dieser sollte auf einen Schemennamen eingestellt werden, der die geeigneten Zugriffsrechte hat. Eine SQL-Anweisung SET CURRENT PACKAGESET schema wird automatisch nach jeder Verbindungsherstellung für die Anwendung abgesetzt.

Mit dem ODBC-Manager können Sie DB2CLI.INI aktualisieren. Weitere Informationen finden Sie im Handbuch *Installation und Konfiguration Ergänzung*.

### Unterstützung für Kennwortänderung

Wenn eine SQL-Anweisung CONNECT eine Nachricht zurückgibt, die besagt, daß das Kennwort der Benutzer-ID nicht mehr gültig ist, können Sie mit DB2 Connect ab Version 5.2 das Kennwort ändern, ohne sich an TSO anzumelden. Mit Hilfe von DRDA kann DB2 Universal Database für OS/390 das Kennwort für Sie ändern.

Der Benutzer muß das alte Kennwort zusammen mit dem neuen Kennwort und dem Prüfkennwort angeben. Wenn die am DB2 Connect Enterprise Edition-Server angegebene Sicherheitseinstufung DCS ist, wird eine Anforderung zum Ändern des Kennworts an den Datenbank-Server unter DB2 Universal Database für OS/390 gesendet. Wenn die angegebene Sicherheitseinstufung SERVER ist, wird das Kennwort auf dem DB2 Connect-Server geändert.

Ein weiterer Vorteil ist, daß eine separate LU Definition nicht erforderlich ist. Weitere Informationen hierzu finden Sie im Handbuch *Einstieg* für DB2 Connect Enterprise Edition.

## Konfigurieren des Anwendungs-Requesters

DB2 Universal Database für OS/390 implementiert die Unterstützung für den DRDA-Anwendungs-Requester als integralen Bestandteil von DB2 Universal Database für OS/390 DDF (Distributed Data Facility). DDF kann unabhängig von den lokalen Funktionen für die Verwaltung von Datenbanken unter DB2 Universal Database für OS/390 gestoppt werden, DDF kann jedoch nicht ohne Unterstützung für die lokale Verwaltung von Datenbanken unter DB2 Universal Database für OS/390 ausgeführt werden.

Wenn DB2 Universal Database für OS/390 als Anwendungs-Requester fungiert, kann die Verbindung zwischen auf dem System ausgeführten Anwendungen und fernen Datenbank-Servern unter DB2 Universal Database, DB2 für MVS/ESA, DB2 Universal Database für OS/390, DB2 Universal Database

für AS/400 und DB2 für VSE & VM hergestellt werden, die die DRDA-Anwendungs-Server-Funktion implementieren.

Sie müssen folgende Schritte ausführen, damit der Anwendungs-Requester unter DB2 Universal Database für OS/390 Zugriff auf verteilte Datenbanken bereitstellen kann:

- „Bereitstellen von Netzwerkinformationen": Der Anwendungs-Requester muß in der Lage sein, RDB_NAME-Werte entgegenzunehmen und in SNA-NETID.LUNAME-Werte oder TCP/IP-Adreßwerte umzuwandeln. DB2 Universal Database für OS/390 verwendet die *Kommunikationsdatenbank (CDB - Communications Database) von DB2 Universal Database für OS/390* zum Registrieren der RDB_NAME-Werte und ihrer entsprechenden Netzwerkparameter. Mit der Kommunikationsdatenbank kann der Anwendungs-Requester unter DB2 Universal Database für OS/390 die erforderlichen Informationen an den Communications Server übergeben, wenn Anforderungen für verteilte Datenbanken über SNA- bzw. TCP/IP-Verbindungen abgesetzt werden.
- „Gewährleisten der Sicherheit" auf Seite 76— Damit der Anwendungs-Server Anforderungen für ferne Datenbanken entgegennehmen kann, muß der Anwendungs-Requester die vom Server benötigten Sicherheitsinformationen bereitstellen. DB2 Universal Database für OS/390 stellt die erforderlichen Netzwerksicherheitsinformationen mit Hilfe der Kommunikationsdatenbank und DCE, RACF und anderen Sicherheitssubsystemen bereit.
- „Darstellen von Daten" auf Seite 86—Sie müssen sicherstellen, daß die CCSID (Coded Character Set Identifier - ID des codierten Zeichensatzes) des Anwendungs-Requesters mit der des Anwendungs-Servers kompatibel ist.

### Bereitstellen von Netzwerkinformationen

Viele Verarbeitungsprozesse in einer verteilten Datenbankumgebung machen den Austausch von Nachrichten mit anderen Netzwerkstandorten erforderlich. Damit diese Verarbeitungsprozesse korrekt ausgeführt werden können, sind Ihrerseits folgende Schritte notwendig:

1. Definieren des lokalen Systems
2. Definieren der fernen Systeme
3. Definieren der Kommunikation (für SNA- bzw. TCP/IP-Verbindungen)
4. Einstellen von RU-Größe und Nachrichtendosierung (nur für SNA-Verbindungen)

Weitere Informationen finden Sie in den Abschnitten „Definieren des lokalen Systems (SNA)" auf Seite 57 und „Definieren des lokalen Systems (TCP/IP)" auf Seite 64.

### Definieren des lokalen Systems (SNA)

Jedem Programm im SNA-Netzwerk werden eine Netzwerk-ID (NETID) und ein LU-Name zugeordnet, d. h. der Anwendungs-Requester unter DB2 Universal Database für OS/390 muß einen NETID.LUNAME-Wert aufweisen (durch VTAM zugeordnet), wenn die Verbindung zum Netzwerk hergestellt wird. Da der Anwendungs-Requester unter DB2 Universal Database für OS/390 in das Verwaltungssystem lokaler Datenbanken von DB2 Universal Database für OS/390 integriert ist, muß der Anwendungs-Requester auch einen RDB_NAME-Wert aufweisen. In den Veröffentlichungen zu DB2 Universal Database für OS/390 wird der RDB_NAME als *Location Name* (Standordname) bezeichnet.

Definieren Sie den Anwendungs-Requester unter DB2 Universal Database für OS/390 wie folgt für das SNA-Netzwerk:

1. Wählen Sie einen LU-Namen für das System mit DB2 Universal Database für OS/390 aus. Die NETID des Systems mit DB2 Universal Database für OS/390 wird beim Starten von DDF von VTAM automatisch abgerufen.
2. Definieren Sie den LU-Namen und Standortnamen im BSDS (*Bootstrap Data Set*) von DB2 Universal Database für OS/390 (DB2 Universal Database für OS/390 beschränkt die Länge des Standortnamens auf 16 Zeichen).
3. Erstellen Sie eine VTAM-APPL-Definition zum Registrieren des ausgewählten LU-Namens für VTAM.
4. Stellen Sie sicher, daß die Option für erweiterte Sicherheit (Extended Security) auf YES gesetzt ist. Weitere Informationen finden Sie in „Zusätzliche Sicherheitsverbesserungen” auf Seite 54.

**Konfigurieren des DDF-BSDS:** DB2 Universal Database für OS/390 liest den BSDS während des Startvorgangs, um Parameter zur Systeminstallation abzurufen. Einer der im BSDS gespeicherten Datensätze ist der sogenannte *DDF-Datensatz*, weil er die von DDF verwendeten Informationen zur Verbindungsherstellung zu VTAM enthält. Dabei handelt es sich um folgende Informationen:

- Der Standortname für das System mit DB2 Universal Database für OS/390
- Der LU-Name für das System mit DB2 Universal Database für OS/390
- Das bei der Verbindungsherstellung vom System mit DB2 Universal Database für OS/390 zu VTAM verwendete Kennwort

Sie können DB2 Universal Database für OS/390 die DDF-BSDS-Informationen auf zwei Arten bereitstellen:

- Stellen Sie die erforderlichen DDF-BSDS-Informationen bei der Erstinstallation von DB2 Universal Database für OS/390 mit Hilfe der DDF-Installationsanzeige DSNTIPR bereit. Viele der Installationsparameter werden hier nicht erläutert, weil es wichtiger ist, das Verfahren zur Herstellung einer Verbindung zwischen DB2 Universal Database für OS/390 und VTAM zu kennen. Abb. 15 zeigt, wie Sie mit Hilfe der Installationsanzeige den Standortnamen NEW_YORK3, den LU-Namen NYM2DB2 und das Kennwort PSWDBD1 im BSDS von DB2 Universal Database für OS/390 eintragen können.

```
                          DISTRIBUTED DATA FACILITY                      =
==> _

 Enter data below:

  1 DDF STARTUP OPTION   ===> AUTO      NO, AUTO, or COMMAND
  2 DB2 LOCATION NAME    ===> NEW_YORK3         The name other DB2s use to
                                                refer to this DB2
  3 DB2 NETWORK LUNAME   ===> NYM2DB2   The name VTAM uses to refer to this DB2
  4 DB2 NETWORK PASSWORD ===> PSWDBD1   Password for DB2's VTAM application
  5 RLST ACCESS ERROR    ===> NOLIMIT   NOLIMIT, NORUN, or 1-5000000
  6 RESYNC INTERVAL      ===> 3         Minutes between resynchronization period
  7 DDF THREADS          ===> ACTIVE    (ACTIVE or INACTIVE) Status of a
                                        database access thread that commits or
                                        rolls back and holds no database locks
                                        or cursors
  8 DB2 GENERIC LUNAME   ===>           Generic VTAM LU name for this DB2
                                        subsystem or data sharing group
  9 IDLE THREAD TIMEOUT  ===> 120       0 or seconds until dormant server ACTIVE
                                        thread will be terminated (0-9999)
 10 EXTENDED SECURITY    ===> YES       Allow change password and descriptive
                                        security error codes.  YES or NO.
 PRESS:  ENTER to continue   RETURN to exit   HELP for more information
```

*Abbildung 15. Installationsanzeige DSNTIPR von DB2 Universal Database für OS/390*

- Wenn DB2 Universal Database für OS/390 bereits installiert ist, können Sie die Informationen im BSDS mit dem Dienstprogramm zum Ändern des Protokollinventars (DSNJU003) aktualisieren.

  Abb. 16 zeigt, wie Sie den BSDS mit dem Standortnamen NEW_YORK3, dem LU-Namen NYM2DB2 und dem Kennwort PSWDBD1 aktualisieren können.

```
//SYSADMB JOB ,'DB2 5.1 JOB',CLASS=A
//*
//*        CHANGE LOG INVENTORY:
//*        UPDATE BSDS WITH
//*             - DB2 LOCATION NAME FOR NEW_YORK3
//*             - VTAM LUNAME (NYM2DB2)
//*             - DB2/VTAM PASSWORD
//*
//DSNBSDS EXEC PGM=DSNJU003
//STEPLIB  DD  DISP=SHR,DSN=DSN510.DSNLOAD
//SYSUT1   DD  DISP=OLD,DSN=DSNC510.BSDS01
//SYSUT2   DD  DISP=OLD,DSN=DSNC510.BSDS02
//SYSPRINT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
//SYSIN    DD  *
 DDF    LOCATION=NEW_YORK3,LUNAME=NYM2DB2,PASSWORD=PSWDBD1
//*
```

*Abbildung 16. Beispiel für BSDS-DDF-Definition (für VTAM)*

Beim Starten von DDF (entweder automatisch beim Starten von DB2 Universal Database für OS/390 oder durch den Befehl START DDF von DB2 Universal Database für OS/390) wird die Verbindung zu VTAM hergestellt, wobei der LU-Name und das Kennwort an VTAM übergeben werden. VTAM erkennt das System mit DB2 Universal Database für OS/390, indem es den LU-Namen und das Kennwort (sofern ein VTAM-Kennwort erforderlich ist) anhand der in der VTAM-Anweisung APPL von DB2 Universal Database für OS/390 definierten Werte überprüft. Mit dem VTAM-Kennwort wird geprüft, ob DB2 Universal Database für OS/390 dazu berechtigt ist, den angegebenen LU-Namen auf dem VTAM-System zu verwenden. Das VTAM-Kennwort wird nicht über das Netzwerk übertragen, und es wird nicht zur Herstellung einer Verbindung zwischen anderen Systemen im Netzwerk und DB2 Universal Database für OS/390 verwendet.

Wenn für VTAM kein Kennwort erforderlich ist, übergehen Sie das Schlüsselwort PASSWORD= im Dienstprogramm zum Ändern des Protokollinventars. Das Fehlen des Schlüsselworts gibt an, daß kein VTAM-Kennwort erforderlich ist.

**Erstellen einer VTAM-APPL-Definition:** Nach dem Definieren des LU-Namens und Kennworts von VTAM für DB2 Universal Database für OS/390 müssen Sie diese Werte in VTAM registrieren. VTAM definiert lokale LU-Namen mit der Anweisung APPL. Abb. 17 zeigt die Definition des LU-Namens NYM2DB2 für VTAM.

```
 DB2APPLS VBUILD TYPE=APPL
 *
 *--------------------------------------------------------------------*
 *                                                                    *
 *           APPL-DEFINITION FÜR DAS DB2-SYSTEM NEW_YORK3             *
 *                                                                    *
 *--------------------------------------------------------------------*
 *
NYM2DB2  APPL  APPC=YES,                                            X
               AUTH=(ACQ),                                          X
               AUTOSES=1,                                  X
               DMINWNL=10,                                 X
               DMINWNR=10,                                 X
               DSESLIM=20,                                 X
               EAS=9999,                                   X
               MODETAB=RDBMODES,                           X
               PRTCT=PSWDBD1,                                       X
               SECACPT=ALREADYV,                           X
               SRBEXIT=YES,                                         X
               VERIFY=NONE,                                         X
               VPACING=2,                                           X
               SYNCLVL=SYNCPT,                             X
               ATNLOSS=ALL                                          X
```

*Abbildung 17. VTAM-APPL-Beispieldefinition für DB2 Universal Database für OS/390*

Die VTAM-Anweisung APPL weist viele Schlüsselwörter auf. Die Bedeutung dieser Schlüsselwörter wird genauer im Handbuch *DB2 Universal Database for OS/390 Administration Guide* erläutert. Hier werden lediglich die Schlüsselwörter erläutert, die für dieses Handbuch relevant sind. Es folgt eine Beschreibung der relevanten Schlüsselwörter in Abb. 17:

**NYM2DB2**
: VTAM verwendet den Kennsatz der Anweisung APPL als LU-Namen. In diesem Fall ist der LU-Name NYM2DB2. Die APPL-Syntax läßt keinen vollständigen NETID.LUNAME-Wert zu. Der NETID-Wert wird in der VTAM-Anweisung APPL nicht angegeben, weil allen VTAM-Anwendungen automatisch die NETID für das VTAM-System zugeordnet wird.

**AUTOSES=1**

Die Anzahl SNA-Konfliktgewinnersitzungen, die automatisch gestartet werden, wenn eine Anforderung zum Ändern der Sitzungsanzahl (CNOS - Change Number of Sessions) abgesetzt wird; Sie müssen für AUTOSES einen Wert ungleich Null angeben, damit DB2 Universal Database für OS/390 in jedem Fall darauf hingewiesen wird, wenn die VTAM-CNOS-Verarbeitung fehlschlägt.

Sie brauchen nicht alle APPC-Sitzungen zwischen zwei beliebigen Partnerpaaren der verteilten Datenbankumgebung automatisch zu starten. Wenn der Wert für AUTOSES unter der Konfliktgewinnerbegrenzung (DMINWNL) liegt, verzögert VTAM das Starten der übrigen SNA-Sitzungen, bis sie von einer Anwendung für verteilte Datenbanken benötigt werden.

**DMINWNL=10**

Die Anzahl Sitzungen, in denen dieses System mit DB2 Universal Database für OS/390 der Konfliktgewinner ist; die CNOS-Verarbeitung verwendet den Parameter DMINWNL als Standardwert. Er kann jedoch für jeden Partner durch Hinzufügen einer Zeile zur Tabelle SYSIBM.LUMODES in der Kommunikationsdatenbank von DB2 Universal Database für OS/390 außer Kraft gesetzt werden.

**DMINWNR=10**

Die Anzahl Sitzungen, in denen das Partnersystem der Konfliktgewinner ist; die CNOS-Verarbeitung verwendet den Parameter DMINWNR als Standardwert. Er kann jedoch für jeden Partner durch Hinzufügen einer Zeile zur Tabelle SYSIBM.LUMODES in der Kommunikationsdatenbank von DB2 Universal Database für OS/390 außer Kraft gesetzt werden.

**DSESLIM=20**

Die Gesamtzahl zulässiger Sitzungen (Konfliktgewinner und Konfliktverlierer), die zwischen DB2 Universal Database für OS/390 und einem anderen verteilten System für einen bestimmten Modusgruppennamen hergestellt werden können; die CNOS-Verarbeitung verwendet den Parameter DSESLIM als Standardwert. Er kann jedoch für jeden Partner durch Hinzufügen einer Zeile zur Tabelle SYSIBM.LUMODES in der Kommunikationsdatenbank von DB2 Universal Database für OS/390 außer Kraft gesetzt werden.

Wenn der Partner die im Parameter DSESLIM, DMINWNL oder DMINWNR angeforderte Anzahl Sitzungen nicht unterstützen kann, vereinbart der CNOS-Prozeß für diese Parameter neue Werte, die für den Partner akzeptabel sind.

**EAS=9999**

Ein Schätzwert für die Gesamtzahl Sitzungen, die von dieser VTAM-LU benötigt werden.

**MODETAB=RDBMODES**

Gibt die VTAM-MODE-Tabelle mit den einzelnen Modusnamen von DB2 Universal Database für OS/390 an.

**PRTCT=PSWDBD1**

Gibt das VTAM-Kennwort an, das benutzt werden muß, wenn DB2 Universal Database für OS/390 versucht, eine Verbindung in VTAM herzustellen. Wenn das Schlüsselwort PRTCT übergangen wird, ist kein Kennwort erforderlich, und Sie müssen das Schlüsselwort PASSWORD= im Dienstprogramm zum Ändern des Protokollinventars von DB2 Universal Database für OS/390 übergehen.

**SECACPT=ALREADYV**

Gibt den höchsten Sicherheitswert auf SNA-Dialogebene an, der von diesem System mit DB2 Universal Database für OS/390 beim Empfangen einer Anforderung für verteilte Datenbanken von einem fernen System akzeptiert wird. Das Schlüsselwort ALREADYV gibt an, daß dieses System mit DB2 Universal Database für OS/390 drei SNA-Sitzungssicherheitsoptionen von anderen DRDA-Systemen akzeptieren kann, die Daten von diesem System mit DB2 Universal Database für OS/390 anfordern:

- SECURITY=SAME (eine bereits überprüfte Anforderung, die nur die Benutzer-ID des Requesters enthält)
- SECURITY=PGM (eine Anforderung, in der das Kennwort des Requesters, d. h. ein PassTicket, enthalten ist)
- SECURITY=NONE (eine Anforderung, die keine Sicherheitsinformationen enthält); DB2 Universal Database für OS/390 weist DRDA-Anforderungen mit SECURITY=NONE zurück.

Es wird empfohlen, immer SECACPT=ALREADYV anzugeben, weil die Stufe der SNA-Dialogsicherheit für jeden Partner von DB2 Universal Database für OS/390 aus der Kommunikationsdatenbank von DB2 Universal Database für OS/390 (Spalte USERSECURITY der Tabelle SYSIBM.LUNAMES) kommt. SECACPT=ALREADYV verleiht Ihnen die größte Flexibilität bei der Auswahl der Werte für USERSECURITY.

**VERIFY=NONE**

Gibt die Sicherheitsstufe für SNA-Sitzungen (Partner-LU-Prüfung) an, die für dieses System mit DB2 Universal Database für OS/390 erforderlich ist. Der Wert NONE gibt an, daß keine Partner-LU-Prüfung erforderlich ist.

DB2 Universal Database für OS/390 schränkt Ihre Auswahl für das Schlüsselwort VERIFY nicht ein. In einem nicht gesicherten Netzwerk wird die Einstellung VERIFY=REQUIRED empfohlen.
VERIFY=REQUIRED bewirkt, daß VTAM diejenigen Partner zurückweist, die keine Partner-LU-Prüfung ausführen können. Wenn Sie

VERIFY=OPTIONAL angeben, führt VTAM die Partner-LU-Prüfung nur für solche Partner durch, die diese Unterstützung bereitstellen.

**VPACING=2**
Stellt den VTAM-Nachrichtendosierungszähler auf 2 ein.

**SYNCLVL=SYNCPT**
Gibt an, daß DB2 Universal Database für OS/390 in der Lage ist, zweiphasige Festschreibung zu unterstützen. VTAM informiert den Partner mit Hilfe dieser Informationen darüber, daß zweiphasige Festschreibung verfügbar ist. Wenn dieses Schlüsselwort vorhanden ist, verwendet DB2 Universal Database für OS/390 automatisch zweiphasige Festschreibung, sofern der Partner sie unterstützen kann.

**ATNLOSS=ALL**
Gibt an, daß DB2 Universal Database für OS/390 bei jeder Beendigung einer VTAM-Sitzung informiert werden muß. Dadurch wird sichergestellt, daß DB2 Universal Database für OS/390 eine SNA-Resynchronisation ausführt, wenn sie erforderlich ist.

Mit DSESLIM, DMINWNL und DMINWNR können Sie VTAM-Standardsitzungsbegrenzungen für alle Partner festlegen. Für Partner mit speziellen Sitzungsbegrenzungsanforderungen können Sie die Standardsitzungsbegrenzungen mit Hilfe der Tabelle SYSIBM.LUMODES überschreiben. Ein Beispiel dafür ist die Angabe der für Ihre OS/2-Systeme geeigneten VTAM-Standardsitzungsbegrenzungen. Für andere Partner können Sie Zeilen in der Tabelle SYSIBM.LUMODES erstellen, um die gewünschten Sitzungsbegrenzungen zu definieren. Beispielwerte:

```
DSESLIM=4,DMINWNL=0,DMINWNR=4
```

Diese Parameter ermöglichen jedem Partner die Erstellung von maximal vier Sitzungen mit DB2 Universal Database für OS/390, wobei der Partner in allen Sitzungen der Konfliktgewinner ist. Da OS/2 die LU 6.2-Dialoge mit DB2 Universal Database für OS/390 erstellt und OS/2 zum Konfliktgewinner in den Sitzungen macht, wird der Durchsatz etwas verbessert. Wenn OS/2 eine Konfliktgewinnersitzung zur Verfügung steht, braucht es nicht um die Berechtigung zum Starten eines neuen LU 6.2-Dialogs zu bitten.

### Definieren des lokalen Systems (TCP/IP)

Die Informationen in diesem Abschnitt wurden aus dem Handbuch *DB2 Connect Enterprise Edition für OS/2 und Windows Einstieg* zusammengestellt. Ausführlichere Informationen hierzu finden Sie in den Handbüchern *DB2 Universal Database für OS/390 Installation Reference* und *DRDA Support for TCP/IP with DB2 Universal Database für OS/390 and DB2 Universal Database*.

Folgende Schritte sind zum Definieren der TCP/IP-Kommunikation mit DB2 Universal Database für OS/390 erforderlich:

1. TCP/IP-Kommunikation muß für das System mit DB2 Universal Database für OS/390 und auf dem Partnersystem aktiviert sein.
2. Der Netzwerkadministrator muß zwei geeignete TCP/IP-Anschlußnummern zuordnen. DB2 Universal Database für OS/390 verwendet standardmäßig die Anschlußnummer 446 für Datenbankverbindungen und die Anschlußnummer 5001 für Resynchronisationsanforderungen (zweiphasige Festschreibung).
3. Der ferne Anwendungs-Server bzw. Anwendungs-Requester muß die gleichen Anschlußnummern (bzw. Servicenamen) wie DB2 Universal Database für OS/390 verwenden.
4. Stellen Sie sicher, daß die Option für bereits überprüfte TCP/IP-Sicherheit auf YES gesetzt ist. Weitere Informationen finden Sie in „Zusätzliche Sicherheitsverbesserungen” auf Seite 54.
5. Der BSDS von DB2 Universal Database für OS/390 muß zusätzliche Parameter enthalten. Abb. 18 auf Seite 65 verdeutlicht die für die Aktivierung der TCP/IP-Kommunikation erforderlichen zusätzlichen Parameter.

```
//SYSADMB JOB ,'DB2 5.1 JOB',CLASS=A
//*
//*        CHANGE LOG INVENTORY:
//*        UPDATE BSDS WITH
//*             - DB2 LOCATION NAME FOR NEW_YORK3
//*             - VTAM LUNAME (NYM2DB2)
//*             - DB2/VTAM PASSWORD
//*
//*             - GENERIC LU NAME
//*             - TCP/IP PORT FOR DATABASE CONNECTIONS
//*             - TCP/IP PORT FOR RESYNCH OPERATIONS
//*
//DSNBSDS EXEC PGM=DSNJU003
//STEPLIB  DD  DISP=SHR,DSN=DSN510.DSNLOAD
//SYSUT1   DD  DISP=OLD,DSN=DSNC510.BSDS01
//SYSUT2   DD  DISP=OLD,DSN=DSNC510.BSDS02
//SYSPRINT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
//SYSIN    DD  *
 DDF    LOCATION=NEW_YORK3,LUNAME=NTYM2DB2,PASSWORD=PSWDBD1,
        GENERICLU=name,PORT=446,RESPORT=5001
/*
//*
```

*Abbildung 18. Beispiel für BSDS-DDF-Definition (für TCP/IP)*

### Definieren der fernen Systeme

Wenn eine Anwendung unter DB2 Universal Database für OS/390 Daten von einem fernen System anfordert, sucht DB2 Universal Database für OS/390 in den Tabellen der Kommunikationsdatenbank nach Informationen zum fernen System. Die Kommunikationsdatenbank ist eine Gruppe von SQL-Tabellen, die vom Systemadministrator von DB2 Universal Database für OS/390 verwaltet wird. Der Systemadministrator von DB2 Universal Database für OS/390 kann mit Hilfe von SQL Zeilen mit einer Beschreibung aller potentiellen DRDA-Partner in die Kommunikationsdatenbank einfügen. Eine vollständige Beschreibung der Kommunikationsdatenbank und ihrer Verwendungsweise finden Sie in den Handbüchern *DB2 Universal Database für OS/390 SQL Reference* und *DB2 Universal Database für OS/390 Installation*.

Verweise auf die Kommunikationsdatenbank suchen unter anderem nach folgenden Informationen:

- LU-Name und TPN (für SNA-Verbindungen)
- TCP/IP-Adreßinformationen (nur für abgehende TCP/IP-SNA-Verbindungen erforderlich)
- Vom fernen Standort benötigte Netzwerksicherheitsinformationen
- Zum Übertragen von Daten an ferne Standorte verwendete Sitzungsbegrenzungen und Modusnamen (für SNA-Verbindungen)

**Eintragen von Werten in die Kommunikationsdatenbank:** Aktualisierungen der Kommunikationsdatenbank sind nicht erforderlich, wenn Sie nur TCP/IP-Datenbankverbindungen für eingehende Anforderungen verwenden. Wenn DB2 Universal Database für OS/390 nur als TCP/IP-Server verwendet werden soll, müssen Sie daher keine Werte in die Kommunikationsdatenbank eintragen. Anstelle dessen können die Standardwerte verwendet werden. Wenn jedoch SNA-Verbindungen für eingehende Anforderungen verwendet werden, müssen Sie mindestens eine leere Zeile in der Tabelle SYSIBM.LUNAMES bereitstellen. Beispielsweise werden Anforderungen für SNA-Datenbankverbindungen von einer beliebigen ankommenden LU von DB2 Connect akzeptiert, wenn Sie einen SQL-Befehl wie den folgenden verwenden:

```
INSERT INTO SYSIBM.LUNAMES (LUNAME) VALUES ('        ')
```

Wenn Sie DB2 Universal Database für OS/390 als Requester verwenden, müssen Sie die Kommunikationsdatenbank immer aktualisieren. Sie müssen in die Tabelle SYSIBM.LOCATIONS und entweder in die Tabelle SYSIBM.LUNAMES (für SNA-Verbindungen) oder die Tabelle SYSIBM.IPNAMES (für TCP/IP-Verbindungen) Zeilen einfügen.

Wenn Sie bei SNA-Verbindungen die Sicherheitsvoraussetzungen oder Namensumsetzung für eingehende Anforderungen steuern wollen, sind unter Umständen zusätzliche Kommunikationsdatenbankaktualisierungen erforderlich. In den folgenden Abschnitten werden zusätzliche Beispiele gegeben: „Gewährleisten der Sicherheit" auf Seite 76 beschreibt das Definieren der Benutzersicherheit beim Konfigurieren eines Anwendungs-Requesters, und „Gewährleisten der Sicherheit" auf Seite 91 beschreibt das Konfigurieren eines Anwendungs-Servers.

Ausführlichere Informationen zu den Voraussetzungen für das Aktualisieren von Kommunikationsdatenbanktabellen finden Sie im Handbuch *DB2 Universal Database for OS/390 Administration Guide*. Nach dem Eintragen der Werte in die Kommunikationsdatenbank können Sie Abfragen schreiben, die auf Daten ferner Systeme zugreifen. Weitere Informationen zum Aktualisieren der Kommunikationsdatenbank finden Sie zudem im Handbuch *DB2 Universal Database for OS/390 Installation Reference*.

**Handhaben von Anforderungen seitens der Kommunikationsdatenbank:** Wenn DB2 Universal Database für OS/390 eine Anforderung sendet, ermittelt es mit Hilfe der Spalte LINKNAME in der Katalogtabelle SYSIBM.LOCATIONS das für Datenbankverbindungen für abgehende Verbindungen zu verwendende Netzwerkprotokoll. Sie müssen einen LUNAME-Wert in der Installationsanzeige DSNTIPR von DB2 Universal Database für OS/390 auswählen, um VTAM-Anforderungen empfangen zu können. Sie müssen einen DRDA-Anschluß und einen Resynchronisationsanschluß in der Installationsanzeige DSNTIP5 von DB2 Universal Database für OS/390 auswählen, um TCP/IP-

Anforderungen empfangen zu können. TCP/IP verwendet die Anschlußnummer des Servers, um Netzwerkanforderungen an das korrekte DB2-Subsystem zu übergeben.

Wenn der Wert in der Spalte LINKNAME der Tabelle SYSIBM.IPNAMES gefunden wird, wird TCP/IP für DRDA-Verbindungen verwendet. Wenn der Wert in der Tabelle SYSIBM.LUNAMES gefunden wird, wird SNA verwendet. Wenn der gleiche Name in beiden Tabellen (SYSIBM.LUNAMES und SYSIBM.IPNAMES) gefunden wird, wird TCP/IP zur Herstellung der Verbindung zum Standort verwendet.

**Anmerkung:** Ein Requester kann die Verbindung zu einem bestimmten Standort nicht unter Verwendung beider Protokolle, SNA und TCP/IP, herstellen. Wenn beispielsweise in der Tabelle SYSIBM-.LOCATIONS für LINKNAME der Wert LU1 angegeben ist und LU1 in den Tabellen SYSIBM.IPNAMES und SYSIBM.LUNAMES definiert ist, wird nur das Protokoll TCP/IP zur Verbindung zu LU1 von diesem Requester verwendet.

**Kommunikationsdatenbanktabellen:** Die Kommunikationsdatenbank besteht aus folgenden Tabellen:

1. **SYSIBM.LOCATIONS**

   Anhand dieser Tabelle ermittelt DB2 Universal Database für OS/390 die SNA- bzw. TCP/IP-Adreßinformationen, die beim Zugriff auf die durch eine Anwendung von DB2 Universal Database für OS/390 *für abgehende Anforderungen* ausgewählten RDB_NAME-Werte erforderlich sind. Es gibt folgende Spalten:

   **LOCATION**
   Der RDB_NAME des fernen Systems; DB2 Universal Database für OS/390 beschränkt den Wert für RDB_NAME auf 16 Byte, was zwei Byte kürzer als die in DRDA definierte 18-Byte-Begrenzung ist.

   **LINKNAME**
   Der LU-Name bzw. die TCP/IP-Attribute des fernen Systems.

   **PORT** Der TCP/IP-Anschlußname bzw. Servicename (der Standardanschlußname für DRDA ist 446).

   **TPN** Der APPC-Transaktionsprogrammname (TPN) des fernen Systems; wenn das ferne System ein System mit DB2 Universal Database für OS/390 ist oder das ferne System den DRDA-TPN-Standardwert verwendet (X'07F6C4C2'), kann für TPN eine leere Zeichenfolge angegeben werden, weil DB2 Universal Database für OS/390 automatisch den korrekten Wert wählt.

Wenn für das ferne System ein anderer TPN-Wert als der TPN-Standardwert erforderlich ist, muß er hier angegeben werden.

2. **SYSIBM.LUNAMES**

   Mit dieser Tabelle werden die Netzwerkattribute der fernen Systeme definiert, auf die über SNA-Verbindungen zugegriffen wird. Es gibt folgende Spalten:

   **LUNAME**
   Der LU-Name des fernen Systems.

   **SYSMODENAME**
   Der VTAM-Anmeldemodusname, mit dem Dialoge zwischen Systemen mit DB2 Universal Database für OS/390 für die *Unterstützung sekundärer Server* unter DB2 Universal Database für OS/390 erstellt werden (systemgesteuerter Zugriff); wird in dieser Spalte kein Wert angegeben, wird IBMDB2LM für Dialoge bei Systemen mit DB2 Universal Database für OS/390 verwendet.

   **SECURITY_IN**
   Die vom fernen System benötigten Netzwerksicherheitsoptionen, wenn dieses System mit DB2 Universal Database für OS/390 als Server für das ferne System fungiert (Voraussetzungen für die *Sicherheit bei eingehenden Anforderungen*); folgende Werte sind möglich:

   - **V** steht für „verify" (überprüfen). Eine eingehende Verbindungsanforderung muß eine der drei folgenden Angaben enthalten: Benutzer-ID und Kennwort, Benutzer-ID und RACF-PassTicket oder DCE-Sicherheitszugriffsberechtigung.
   - **A** steht für „already verified" (bereits überprüft). Für eine Anforderung ist kein Kennwort erforderlich, aber wenn ein Kennwort gesendet wird, wird es überprüft. Bei dieser Option wird eine eingehende Verbindungsanforderung akzeptiert, wenn sie eine der folgenden vier Angaben enthält: Benutzer-ID, Benutzer-ID und Kennwort, Benutzer-ID und RACF-PassTicket oder DCE-Sicherheitszugriffsberechtigung.

     Wenn die Spalte USERNAMES 'I' oder 'B' enthält, wird RACF nicht aufgerufen, um eingehende Verbindungsanforderungen zu überprüfen, die nur eine Benutzer-ID enthalten.

   **SECURITY_OUT**
   Die vom fernen System benötigten Netzwerksicherheitsoptionen, wenn dieses System mit DB2 Universal Database für OS/390 als Requester fungiert (Voraussetzungen für die *Sicherheit bei abgehenden Anforderungen*); folgende Werte sind möglich:

   - **A** steht für „already verified" (bereits überprüft). Abgehende Verbindungsanforderungen enthalten eine Berechtigungs-ID und

kein Kennwort. Die für eine abgehende Anforderung verwendete Berechtigungs-ID ist in Abhängigkeit vom Wert in der Spalte USERNAMES die DB2-Benutzerberechtigungs-ID oder eine umgesetzte ID.

- **R** steht für „RACF-PassTicket". Abgehende Verbindungsanforderungen enthalten eine Benutzer-ID und ein RACF-PassTicket. Der LU-Name des Servers dient als RACF-PassTicket-Anwendungsname.

  Die für eine abgehende Anforderung verwendete Berechtigungs-ID ist in Abhängigkeit vom Wert in der Spalte USERNAMES die DB2-Benutzerberechtigungs-ID oder eine umgesetzte ID.

- **P** steht für „password" (Kennwort). Abgehende Verbindungsanforderungen enthalten eine Berechtigungs-ID und ein Kennwort. Das Kennwort kommt in Abhängigkeit vom in der Spalte ENCRYPTPWDS angegebenen Wert aus der Tabelle SYSIBM.USERNAMES oder aus RACF.

  In der Spalte USERNAMES muß 'B' oder 'O' angegeben sein.

**ENCRYPTPSWDS**
Gibt an, ob mit dem Partner ausgetauschte Kennwörter verschlüsselt sind. Verschlüsselte Kennwörter werden nur von Requestern und Servern unter DB2 Universal Database für OS/390 unterstützt.

**MODESELECT**
Legt fest, ob die Tabelle SYSIBM.MODESELECT verwendet wird, um einen VTAM-Anmeldemoduseintrag (Modusname) auf Grundlage des Endbenutzers und der Anwendung auszuwählen, die die Anforderung absetzen. Wenn diese Spalte ein 'Y' enthält, wird der Modusname für alle abgehende Anforderungen für verteilte Datenbanken aus der Tabelle SYSIBM.MODESELECT abgerufen.

Wenn in der Spalte MODESELECT ein anderer Wert als ein 'Y' enthalten ist, wird der Modusname IBMDB2LM für systemgesteuerte Zugriffsanforderungen und der Modusname IBMRDB für DRDA-Anforderungen verwendet.

In der Spalte MODESELECT können Sie Prioritäten für Anforderungen für verteilte Datenbanken vergeben, indem Sie eine dem Modusnamen zugeordnete VTAM-Serviceklasse (Class of Service, COS) angeben.

**USERNAMES**
Die erforderliche Stufe für die Herkunftsüberprüfung und Umsetzung der Benutzer-ID; in dieser Spalte werden auch die Sicherheitsparameter dieses Subsystems mit DB2 Universal Database für OS/390 bei der Anforderung von Daten vom fernen

Partner angegeben (Voraussetzungen für die *Sicherheit bei abgehenden Anforderungen*). Gültige Werte für USERNAMES sind I (Inbound, d. h. eingehende Anforderungen), O (Outbound, d. h. abgehende Anforderungen) und B (Both, d. h. beide Arten von Anforderungen).

**GENERIC**
Gibt an, ob DB2 Universal Database für OS/390 seinen echten oder den generischen LU-Namen verwenden soll.

3. **SYSIBM.LUMODES**

Mit dieser Tabelle werden für VTAM die LU 6.2-Sitzungsbegrenzungen (CNOS-Begrenzungen) für alle Partnersysteme definiert, die APPC-SNA-Verbindungen verwenden. Es gibt folgende Spalten:

**LUNAME**
Der LU-Name des fernen Systems.

**MODENAME**
Der Name des VTAM-Anmeldemodus, dessen Begrenzungen angegeben werden; wird in der Spalte MODENAME kein Wert angegeben, wird standardmäßig IBMDB2LM verwendet.

**CONVLIMIT**
Die maximale Anzahl der in diesen Anmeldemodus aktiven Dialoge zwischen dem lokalen System mit DB2 Universal Database für OS/390 und dem fernen System; mit diesem Wert wird der Parameter DSESLIM in der VTAM-Definitionsanweisung APPL für diesen Anmeldemodus außer Kraft gesetzt. Dieser Parameter stellt die VTAM-Standardsitzungsbegrenzungen für DB2 Universal Database für OS/390 bereit.

Mit dem in der Spalte CONVLIMIT ausgewählten Wert werden die Werte für DMINWNR und DMINWNL während der Änderung der Sitzungsanzahl (CNOS) auf CONVLIMIT/2 gesetzt.

4. **SYSIBM.MODESELECT**

Mit dieser Tabelle können Sie die verschiedenen Modusnamen für einzelne Endbenutzer und Anwendungen unter DB2 Universal Database für OS/390 angeben. Diese Tabelle wird nur für SNA-Verbindungen verwendet. Da jedem VTAM-Modusnamen eine Serviceklasse (Class of Service, COS) zugeordnet werden kann, können Sie diese Tabelle verwenden, um Anwendungen für verteilte Datenbanken mit Hilfe einer Kombination aus AUTHID, PLANNAME und LUNAME Netzwerkübertragungsprioritäten zuzuordnen. Es gibt folgende Spalten:

**AUTHID**
Die Berechtigungs-ID des Benutzers (Benutzer-ID) von DB2 Universal Database für OS/390; in dieser Spalte werden standard-

mäßig keine Angaben gemacht. Dadurch wird festgelegt, daß der angegebene Anmeldemodusname für alle Berechtigungs-IDs gilt.

**PLANNAME**
Der Planname für die Anwendung, die Zugriff auf ein fernes Datenbanksystem anfordert; in dieser Spalte werden standardmäßig keine Angaben gemacht. Dadurch wird festgelegt, daß der angegebene Anmeldemodusname für alle Plannamen gilt. Der für den Befehl BIND PACKAGE verwendete Planname ist DSNBIND.

**LUNAME**
Der LU-Name für das ferne Datenbanksystem.

**MODENAME**
Der beim Weiterleiten einer Anforderung für verteilte Datenbanken an das angegebene ferne System zu verwendende Name des VTAM-Anmeldemodus; in dieser Spalte werden standardmäßig keine Angaben gemacht. Dadurch wird angegeben, daß IBMDB2LM für Dialoge mit systemgesteuertem Zugriff und IBMRDB für DRDA-Dialoge verwendet werden soll.

5. **SYSIBM.USERNAMES**

Mit dieser Tabelle werden Endbenutzernamen durch Bereitstellen von Kennwörtern, Umsetzungen für Namen und Herkunftsüberprüfungen verwaltet. DB2 Universal Database für OS/390 bezeichnet den Endbenutzernamen als Berechtigungs-ID. Die meisten anderen Produkte bezeichnen diesen Namen als Benutzer-ID.

In dieser Tabelle können Sie mit Hilfe der Umsetzung für Namen die Verwendung verschiedener Werte für Benutzer-ID-Verbindungen und die Berechtigungs-ID von DB2 Universal Database für OS/390 erzwingen. Der Umsetzungsprozeß für Namen ist für Anforderungen an ein fernes System (*abgehende Anforderungen*) und für Anforderungen von einem fernen System (*eingehende Anforderungen*) zulässig. Werden Kennwörter nicht verschlüsselt, ist diese Tabelle die Quelle des Kennworts für den Endbenutzer, wenn sowohl Benutzer-ID als auch Kennwort an den fernen Standort gesendet werden. Es gibt folgende Spalten:

**TYPE** Beschreibung für den Verwendungszweck der Zeile (Umsetzung von Namen für abgehende oder eingehende Überprüfungsanforderungen, wobei letztere auch als Herkunftsüberprüfungsanforderungen bezeichnet werden.)

**I** steht für eingehende Verbindungen, **O** für abgehende Verbindungen.

Verwenden Sie „O" für TCP/IP-Verbindungen (Die Namensumsetzung für eingehende Anforderungen und die Herkunftsüberprüfung werden für TCP/IP-Anforderungen nicht ausgeführt).

**AUTHID**

Bei der Namensumsetzung für abgehende Anforderungen wird die Berechtigungs-ID von DB2 Universal Database für OS/390 umgesetzt. Bei der Namensumsetzung für eingehende Anforderungen wird die SNA-Benutzer-ID umgesetzt. In beiden Fällen werden, wenn für AUTHID kein Wert angegeben ist, alle Berechtigungs-IDs oder Benutzer-IDs umgesetzt.

**LINKNAME**

Gibt die VTAM- bzw. TCP/IP-Netzwerkstandorte für die Zeile an. Wird in dieser Spalte kein Wert angegeben, wird diese Regel für die Namensumsetzung auf alle TCP/IP- bzw. SNA-Partner angewandt.

Wenn in dieser Spalte ein Wert angegeben wird, muß mindestens eine der folgenden Aussagen wahr sein:

- In der Tabelle SYSIBM.LUNAMES gibt es eine Zeile, deren LUNAME-Wert mit dem in der Spalte LINKNAME der Tabelle SYSIBM.USERNAMES angegebenen Wert übereinstimmt. Diese Zeile gibt den VTAM-Standort an, der dieser Regel für die Namensumsetzung zugeordnet ist.
- In der Tabelle SYSIBM.IPNAMES gibt es eine Zeile, deren LINKNAME-Wert mit dem in der Spalte LINKNAME der Tabelle SYSIBM.USERNAMES angegebenen Wert übereinstimmt. Diese Zeile gibt den TCP/IP-Host an, der dieser Regel für die Namensumsetzung zugeordnet ist.

  Die Namensumsetzung für eingehende Anforderungen und die Herkunftsüberprüfung werden für TCP/IP-Clients nicht ausgeführt.

**NEWAUTHID**

Der neue Endbenutzername (SNA-Benutzer-ID oder Berechtigungs-ID von DB2 Universal Database für OS/390); wenn in dieser Spalte keine Angaben gemacht werden, braucht die ID nicht umgesetzt zu werden.

**PASSWORD**

Das im Zuordnungsdialog verwendete Kennwort, wenn Kennwörter nicht verschlüsselt werden (ENCRYPTPSWDS = 'N' in SYSIBM.LUNAMES); wenn Kennwörter verschlüsselt werden, wird diese Spalte ignoriert.

6. **SYSIBM.IPNAMES**

Diese Tabelle wird für TCP/IP-Knoten verwendet.

**LINKNAME**

Der in dieser Spalte angegebene Wert muß mit dem in der Spalte LINKNAME der Tabelle SYSIBM.LOCATIONS angegebenen Wert übereinstimmen.

**SECURITY_OUT**

Diese Spalte definiert die DRDA-Sicherheitsoption, die verwendet wird, wenn lokale DB2-SQL-Anwendungen eine Verbindung zu einem fernen Server herstellen, der diesem TCP/IP-Host zugeordnet ist:

- **A** steht für „already verified" (bereits überprüft). Abgehende Verbindungsanforderungen enthalten eine Berechtigungs-ID und kein Kennwort. Die für eine abgehende Anforderung verwendete Berechtigungs-ID ist in Abhängigkeit vom Wert in der Spalte USERNAMES die DB2-Benutzerberechtigungs-ID oder eine umgesetzte ID.
- **R** steht für „RACF-PassTicket". Abgehende Verbindungsanforderungen enthalten eine Benutzer-ID und ein RACF-PassTicket. Der in der Spalte LINKNAME angegebene Wert wird als RACF-PassTicket-Anwendungsname für den fernen Server verwendet.

  Die für eine abgehende Anforderung verwendete Berechtigungs-ID ist in Abhängigkeit vom Wert in der Spalte USERNAMES die DB2-Benutzerberechtigungs-ID oder eine umgesetzte ID.
- **P** steht für „password" (Kennwort). Abgehende Verbindungsanforderungen enthalten eine Berechtigungs-ID und ein Kennwort. Das Kennwort kommt aus der Tabelle SYSIBM.USERNAMES.

  In der Spalte USERNAMES muß „O" angegeben sein.

**USERNAMES**

Diese Spalte steuert die Umsetzung von Berechtigungs-IDs für abgehende Anforderungen. Namensumsetzung für abgehende Anforderungen wird ausgeführt, wenn eine Berechtigungs-ID von DB2 an einen fernen Server gesendet wird.

- **O** gibt an, daß die ID einer abgehenden Anforderung umgesetzt werden soll. Die Umsetzung der ID wird mit Hilfe von Zeilen in der Tabelle SYSIBM.USERNAMES ausgeführt.

  Für IDs einer eingehenden Anforderung wird keine Umsetzung oder Herkunftsüberprüfung ausgeführt.
- Wenn keine Angaben gemacht werden, wird keine Umsetzung ausgeführt.

**IPADDR**

Diese Spalte enthält die IP-Adresse bzw. den Domänennamen eines fernen TCP/IP-Hosts. Die Spalte IPADDR muß wie folgt angegeben werden:

- Wenn in der Spalte IPADDR eine linksbündige Zeichenfolge mit vier durch Dezimalzeichen voneinander getrennten numerischen Werten enthalten ist, geht DB2 davon aus, daß der Wert eine IP-Adresse in Schreibweise mit Trennzeichen ist. Beispielsweise würde '123.456.78.91' als IP-Adresse in Schreibweise mit Trennzeichen interpretiert.
- Alle anderen Werte werden als TCP/IP-Domänennamen interpretiert, die durch den TCP/IP-Socket-Aufruf `gethostbyname` aufgelöst werden können. TCP/IP-Domänennamen unterliegen nicht der Groß-/Kleinschreibung.

### Definieren der Kommunikation (SNA)

VTAM ist der Kommunikationsmanager für OS/390-Systeme. VTAM nimmt LU 6.2-Verben von DB2 Universal Database für OS/390 entgegen und wandelt diese Verben in LU 6.2-Datenströme um, die über das Netzwerk übertragen werden können. Damit VTAM mit den in der Kommunikationsdatenbank von DB2 Universal Database für OS/390 angegebenen Partneranwendungen kommunizieren kann, müssen Sie folgende Informationen für VTAM bereitstellen:

- Die LU-Namen für alle Server.

  Wenn DB2 Universal Database für OS/390 mit VTAM kommuniziert, darf DB2 Universal Database für OS/390 nur einen LU-Namen (nicht NETID-.LUNAME) an VTAM übergeben, um den gewünschten Standort anzugeben. Dieser LU-Name muß innerhalb der auf dem lokalen VTAM-System bekannten LU-Namengruppe eindeutig sein, damit VTAM die NETID und den LU-Namen aus dem von DB2 Universal Database für OS/390 übergebenen LU-Namenwert ermitteln kann. Wenn LU-Namen im SNA-Netzwerk eines Unternehmens eindeutig sind, vereinfacht dies den VTAM-Ressourcendefinitionsprozeß enorm. Dies ist jedoch nicht immer möglich. Wenn LU-Namen innerhalb Ihres SNA-Netzwerks nicht eindeutig sind, müssen Sie die VTAM-LU-Umsetzung für Namen verwenden, um die korrekte NETID.LUNAME-Kombination für einen nicht eindeutigen LU-Namen zu erstellen. Dieser Prozeß wird im Abschnitt „Resource Name Translation" des Handbuchs *VTAM Network Implementation Guide* beschrieben.

  Plazierung und Syntax dieser VTAM-Definitionen zum Definieren der fernen LU-Namen hängen stark davon ab, wie das ferne System logisch und physisch mit dem lokalen VTAM-System verbunden ist.

- RU-Größe, Größe des Nachrichtendosierungsfensters und Serviceklasse für jeden Modusnamen; erstellen Sie in der VTAM-Modustabelle für jeden in

der Kommunikationsdatenbank angegebenen Modusnamen einen Eintrag. Sie müssen auch IBMRDB und IBMDB2LM definieren.

- Die VTAM- und RACF-Profile für den LU-Prüfungsalgorithmus, wenn Sie die Partner-LU-Prüfung verwenden wollen.

**Einstellen von RU-Größe und Nachrichtendosierung:** Die in der VTAM-Modustabelle von Ihnen definierten Einträge geben die RU-Größe und die Nachrichtendosierungszähler an. Fehlende oder fehlerhafte Definitionen für diese Werte können sich nachteilig auf alle VTAM-Anwendungen auswirken.

Bedenken Sie bei der Wahl der RU-Größe, Sitzungsbegrenzungen und Nachrichtendosierungszähler, welche Auswirkungen diese Werte auf das vorhandene VTAM-Netzwerk haben können. Überprüfen Sie beim Installieren eines neuen verteilten Datenbanksystems die folgenden Punkte:

- Stellen Sie für VTAM-CTC-Verbindungen sicher, daß der Parameterwert für MAXBFRU groß genug ist, um Ihre RU-Größe plus der 29 Byte, die VTAM als SNA-Anforderungs- und Übertragungskopf hinzufügt, zu verarbeiten. MAXBFRU wird in Einheiten von 4 KB gemessen, d. h. der Wert für MAXBFRU muß mindestens 2 betragen, um eine RU-Größe von 4 KB zu unterstützen.
- Stellen Sie für NCP-Verbindungen sicher, daß der Wert für MAXDATA groß genug ist, um Ihre RU-Größe plus 29 Byte zu verarbeiten. Wenn Sie als RU-Größe 4 KB angegeben haben, muß der Wert für MAXDATA mindestens 4125 betragen.

  Wenn Sie den NCP-Parameter MAXBFRU angeben, wählen Sie einen Wert aus, der für Ihre RU-Größe plus 29 Byte ausreicht. Bei NCP definiert der Parameter MAXBFRU die Anzahl der VTAM-E/A-Puffer für die PIU. Wenn Sie für IOBUF eine Puffergröße von 441 angeben, verarbeitet MAXBFRU=10 die RU-Größe 4 KB korrekt, weil 10*441 größer ist als 4096+29.
- Im Handbuch *DRDA Connectivity Guide* wird beschrieben, wie Sie die Auswirkung der verteilten Datenbank auf den VTAM-IOBUF-Pool einschätzen können. Wenn ein zu großer Anteil der IOBUF-Poolressource belegt ist, hat dies nachteilige Auswirkungen auf die Leistung aller VTAM-Anwendungen.

### Definieren der Kommunikation (TCP/IP)

Die Überlegungen stimmen mit den weiter oben angestellten Überlegungen überein (siehe „Definieren des lokalen Systems (TCP/IP)” auf Seite 64).

## Gewährleisten der Sicherheit

Wenn ein fernes System die Verarbeitung für verteilte Datenbanken im Auftrag einer SQL-Anwendung ausführt, muß es in der Lage sein, die Sicherheitsanforderungen des Anwendungs-Requesters, des Anwendungs-Servers und des verwendeten Netzwerks zu erfüllen. Diese Anforderungen betreffen mindestens einen der folgenden Bereiche:

- Auswählen von Endbenutzernamen
- Sicherheitsparameter des Netzwerks
- Sicherheit des Datenbankmanagers
- Von einem externen Sicherheitssubsystem implementierte Sicherheit
- Datendarstellung

### Auswählen von Endbenutzernamen

Auf OS/390-Systemen wird jedem Endbenutzer eine *Benutzer-ID* aus 1 bis 8 Zeichen zugeordnet. Der Wert dieser Benutzer-ID muß zwar innerhalb eines bestimmten OS/390-Systems, jedoch nicht unbedingt im gesamten SNA-Netzwerk eindeutig sein. Beispielsweise kann es im System NEWYORK einen Benutzer mit dem Namen JONES und im System DALLAS einen weiteren Benutzer dieses Namens geben. Wenn diese beiden Benutzer dieselbe Person sind, entsteht dadurch kein Konflikt. Ist jedoch der Benutzer JONES in DALLAS nicht identisch mit dem Benutzer JONES in NEWYORK, kann das SNA-Netzwerk (und können folglich auch die verteilten Datenbanksysteme innerhalb dieses Netzwerks) den Benutzer JONES in NEWYORK nicht von dem Benutzer JONES in DALLAS unterscheiden. Wird diese Situation nicht durch geeignete Maßnahmen verhindert, können diese beiden Benutzer die Berechtigungen des jeweils anderen benutzen.

Zur Vermeidung solcher Namenskonflikte unterstützt DB2 Universal Database für OS/390 die Umsetzung für Endbenutzernamen. Wenn eine Anwendung auf dem Anwendungs-Requester unter DB2 Universal Database für OS/390 eine verteilte Datenbank anfordert, führt DB2 Universal Database für OS/390 die Umsetzung für Namen aus, wenn in der Kommunikationsdatenbank die *Namensumsetzung für abgehende Anforderungen* als erforderlich angegeben ist. Wenn die Namensumsetzung für abgehende Anforderungen ausgewählt ist, erzwingt DB2 Universal Database für OS/390 immer das Senden eines Kennworts bei jeder abgehenden Anforderung für verteilte Datenbanken.

Die Namensumsetzung für abgehende Anforderungen in DB2 Universal Database für OS/390 wird durch das Setzen der Spalte USERNAMES in der Tabelle SYSIBM.LUNAMES bzw. SYSIBM.IPNAMES auf 'O' oder 'B' aktiviert. Wenn USERNAMES auf 'O' gesetzt ist, wird die Umsetzung von Endbenutzernamen für abgehende Anforderungen ausgeführt. Wenn USERNAMES auf 'B' gesetzt ist, wird die Umsetzung von Endbenutzernamen für eingehende und abgehende Anforderungen ausgeführt.

Da Berechtigungen in DB2 Universal Database für OS/390 sowohl von der Benutzer-ID des Endbenutzers als auch von der Benutzer-ID des Plan- bzw. Paketeigners von DB2 Universal Database für OS/390 abhängen, wird der Umsetzungsprozeß des Endbenutzernamens für die Benutzer-ID des Endbenutzers, die Benutzer-ID des Planeigners und die Benutzer-ID des Paketeigners ausgeführt. [3]Der Umsetzungsprozeß für Namen durchsucht die Tabelle SYSIBM.USERNAMES in der folgenden Reihenfolge nach einer Zeile, die einem der folgenden Muster (TYPE.AUTHID.LINKNAME) entspricht:

1. O.AUTHID.LINKNAME — eine Umsetzungsregel für einen bestimmten Endbenutzer eines bestimmten Partnersystems
2. O.AUTHID.leer — eine Umsetzungsregel für einen bestimmten Endbenutzer eines beliebigen Partnersystems
3. O.leer.LINKNAME — eine Umsetzungsregel für einen beliebigen Benutzer eines bestimmten Partnersystems

Wenn keine übereinstimmende Zeile gefunden wird, wird die Anforderung für verteilte Datenbanken von DB2 Universal Database für OS/390 zurückgewiesen. Wenn eine Zeile gefunden wird, wird der Wert in der Spalte NEWAUTHID als Berechtigungs-ID verwendet. (Ein leerer Wert für NEWAUTHID gibt an, daß der Originalname ohne Umsetzung verwendet wird.)

Das weiter oben angeführte Beispiel soll erneut der Verdeutlichung dieser Sachverhalte dienen. Sie wollen dem Benutzer JONES im System NEWYORK einen anderen Namen geben (NYJONES), wenn JONES Anforderungen für verteilte Datenbanken an das System DALLAS absetzt. Angenommen, der Eigner der vom Benutzer JONES verwendeten Anwendung ist DSNPLAN (der Planeigner in DB2 Universal Database für OS/390), und Sie brauchen diese Benutzer-ID beim Senden an das System DALLAS nicht umzusetzen.

3. Wird die Anforderung an einen DB2 Universal Database für OS/390-Server geschickt, wird die Namenumsetzung auch für den Planeigner und den Paketeigner ausgeführt. Paket- und Planeignernamen werden nie Kennwörter zugeordnet.

Die SQL-Anweisungen, die zum Bereitstellen der Regeln für die Umsetzung für Namen in der Kommunikationsdatenbank erforderlich sind, werden in Abb. 19 gezeigt.

```
INSERT INTO SYSIBM.LUNAMES
     (LUNAME, SYSMODENAME, SECURITY_OUT, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', 'O');
INSERT INTO SYSIBM.LOCATIONS
     (LOCATION, LINKNAME, LINKATTR)
  VALUES ('DALLAS', 'LUDALLAS', '');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('O', 'JONES', 'LUDALLAS', 'NYJONES', 'JONESPWD');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('O', 'DSNPLAN', 'LUDALLAS', ' ', 'PLANPWD');
```

*Abbildung 19. SQL für die Namensumsetzung für abgehende Anforderungen (SNA)*

Die daraus resultierenden Kommunikationsdatenbanktabellen werden in Abb. 20 gezeigt:

NEWYORK.SYSIBM.LOCATIONS

| LOCATION | LINKNAME | PORT | TPN |
|---|---|---|---|
| DALLAS | LUDALLAS | | |

NEWYORK.SYSIBM.LUNAMES

| LUNAME | SYSMODENAME | SECURITY-IN | SECURITY-OUT | ENCRYPTPSWDS | MODESELECT | USERNAMES |
|---|---|---|---|---|---|---|
| LUDALLAS | | | A | N | N | O |

NEWYORK.SYSIBM.USERNAMES

| TYPE | AUTHID | LINKNAME | NEWAUTHID | PASSWORD |
|---|---|---|---|---|
| 0<br>0 | JONES<br>DSNPLAN | LUDALLAS<br>LUDALLAS | NYJONES | JONESPWD<br>PLANPWD |

*Abbildung 20. Namensumsetzung für abgehende Anforderungen*

Abb. 21 zeigt ein einfacheres Beispiel für das Herstellen einer Verbindung zu einem DRDA-Anwendungs-Server unter DB2 Universal Database über eine SNA-Verbindung.

```
   INSERT INTO SYSIBM.LUNAMES (LUNAME,
                               SECURITY_OUT,
                               ENCRYPTPSWDS,
                               USERNAMES)
                         VALUES ('NYX1GW01','P','N','O');
 INSERT INTO SYSIBM.LOCATIONS (LOCATION,LINKNAME,TPN)
                              VALUES('TASG6',
                                     'NYX1GW01','NYSERVER');
 INSERT INTO SYSIBM.USERNAMES (TYPE,AUTHID,LINKNAME,NEWAUTHID,PASSWORD)
        VALUES ('O','      ','NYX1GW01','SVTDBM6','SG6JOHN');
```

*Abbildung 21. SQL für die Namensumsetzung für abgehende Anforderungen (einfaches Beispiel für SNA)*

Abb. 22 auf Seite 81 zeigt ein einfaches Beispiel für das Herstellen einer Verbindung zu einem DRDA-Anwendungs-Server unter DB2 Universal Database über eine TCP/IP-Verbindung.

```
-- DB2 für Solaris1 - UNIX
   DELETE FROM SYSIBM.IPNAMES WHERE LINKNAME = 'SOLARIS1' ;
   INSERT INTO SYSIBM.IPNAMES ( LINKNAME
                              , SECURITY_OUT
                              , USERNAMES
                                , IBMREQD
                              , IPADDR)
                        VALUES ( 'SOLARIS1'
                              , 'P'
                              , 'O'
                                , 'N'
                              , '9.21.45.4')
                              ;
   INSERT INTO SYSIBM.LOCATIONS ( LOCATION
                                , LINKNAME
                                , IBMREQD
                                , PORT
                                , TPN)
                          VALUES ( 'TCPDB1'
                                , 'SOLARIS1'
                                , 'N'
                                , '30088'
                                , '')
                                ;
   INSERT INTO SYSIBM.USERNAMES ( TYPE
                                , AUTHID
                                , LINKNAME
                                , NEWAUTHID
                                , PASSWORD
                                , IBMREQD)
                          VALUES ( 'O'
                                , ''
                                , 'SOLARIS1'
                                , 'svtdbm5'
                                , 'svt5dbm'
                                , 'N')
                                ;
```

*Abbildung 22. SQL für die Namensumsetzung für abgehende Anforderungen (einfaches Beispiel für TCP/IP)*

### Netzwerksicherheit

Nachdem der Anwendungs-Requester die Endbenutzernamen für die ferne Anwendung ausgewählt hat, muß er die erforderlichen Netzwerksicherheitsinformationen bereitstellen.

LU 6.2 stellt bei SNA-Verbindungen die folgenden drei Hauptsicherheitseinrichtungen für das Netzwerk zur Verfügung:

- Sicherheit auf Sitzungsebene, die durch das Schlüsselwort VERIFY in der VTAM-Anweisung APPL gesteuert wird; weitere Informationen zur Angabe der Sicherheitsoptionen auf Sitzungsebene finden Sie in den sich an Abb. 17 auf Seite 60 anschließenden Erläuterungen.

- Sicherheit auf Dialogebene, die durch den Inhalt der Tabelle SYSIBM.LUNAMES gesteuert wird.
- Datenverschlüsselung, die nur für VTAM 3.4 und spätere Releases von VTAM unterstützt wird.

Da der Anwendungs-Server für die Verwaltung der Datenbankressourcen zuständig ist, legt er fest, welche Netzwerksicherheitseinrichtungen vom Anwendungs-Requester bereitgestellt werden müssen. Sie müssen die Sicherheitsanforderungen auf Dialogebene der einzelnen Anwendungs-Server in die Tabelle SYSIBM.LUNAMES bzw. SYSIBM.IPNAMES eintragen, indem Sie die Anforderung des Anwendungs-Servers in der Spalte USERNAMES aufnehmen.

Die folgenden Optionen für SNA-Dialogsicherheit sind möglich:

**SECURITY=SAME**

Diese Option wird auch als bereits geprüfte Sicherheit bezeichnet, weil nur die Benutzer-ID des Endbenutzers zum fernen System gesendet wird (es wird kein Kennwort übertragen). Verwenden Sie diese Stufe von Dialogsicherheit, wenn in der Spalte USERNAMES in der Tabelle SYSIBM.LUNAMES kein 'O' oder 'B' enthalten ist.

Da DB2 Universal Database für OS/390 die Umsetzung für Endbenutzernamen mit Ausgangsdialogsicherheit koppelt, kann SECURITY=SAME nicht verwendet werden, wenn die Umsetzung von Endbenutzernamen für abgehende Anforderungen aktiviert ist.

**SECURITY=PGM**

Benutzer-ID und Kennwort des Endbenutzers werden zur Gültigkeitsprüfung an das ferne System gesendet. Verwenden Sie diese Sicherheitsoption, wenn in der Spalte USERNAMES der Tabelle SYSIBM.LUNAMES ein 'O' oder 'B' enthalten ist.

In Abhängigkeit von den in der Tabelle SYSIBM.LUNAMES angegebenen Optionen ruft DB2 Universal Database für OS/390 das Kennwort des Endbenutzers aus zwei verschiedenen Quellen ab:

- Nicht verschlüsselte Kennwörter werden aus der Spalte PASSWORD in der Tabelle SYSIBM.USERNAMES abgerufen. DB2 Universal Database für OS/390 extrahiert Kennwörter aus der Tabelle SYSIBM.USERNAMES, wenn die Spalte ENCRYPTPSWDS in der Tabelle SYSIBM.LUNAMES nicht auf 'Y' gesetzt ist. Aus dieser Quelle abgerufene Kennwörter können an beliebige DRDA-Anwendungs-Server übertragen werden.

  Abb. 23 definiert Kennwörter für die Benutzer SMITH und JONES. In der Spalte LUNAME im Beispiel sind Leerzeichen enthalten, d. h. diese Kennwörter werden für alle fernen Systeme verwendet, auf die der Benutzer SMITH bzw. JONES zuzugreifen versucht.

```
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('O', 'JONES', ' ', ' ', 'JONESPWD');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('O', 'SMITH', ' ', ' ', 'SMITHPWD');
```

*Abbildung 23. Senden von Kennwörtern an ferne Standorte (SNA)*

- Verschlüsselte Kennwörter werden an den fernen Standort gesendet, wenn in der Spalte ENCRYPTPSWDS der Tabelle SYSIBM.LUNAMES 'Y' enthalten ist. Verschlüsselte Kennwörter werden von RACF (oder einem äquivalenten Produkt) extrahiert und können nur von einem anderen System mit DB2 Universal Database für OS/390 interpretiert werden. Setzen Sie ENCRYPTPSWDS bei der Kommunikation mit einem System über ein anderes Produkt als DB2 Universal Database für OS/390 nicht auf 'Y'.

  DB2 Universal Database für OS/390 sucht in der Tabelle SYSIBM.USERNAMES nach der an das ferne System zu übertragenden Benutzer-ID (Wert für NEWAUTHID). Dieser umgesetzte Name wird für die RACF-Kennwortextraktion verwendet. Wenn Sie die Namen nicht umsetzen wollen, müssen Sie die Zeilen in der Tabelle SYSIBM.USERNAMES erstellen, durch die Namen ohne Umsetzung gesendet werden. Die Anweisungen in Abb. 24 auf Seite 84 ermöglichen das Senden von Anforderungen an LUDALLAS und LUNYC, ohne daß der Name (die Benutzer-ID) des Endbenutzers umgesetzt wird.

```
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('O', ' ', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('O', ' ', 'LUDALLAS', ' ', ' ');
```

*Abbildung 24. Senden verschlüsselter Kennwörter an ferne Standorte (SNA)*

**SECURITY=NONE**

Diese Option wird von DRDA nicht unterstützt, d. h. DB2 Universal Database für OS/390 kann diese Sicherheitsoption nicht bereitstellen.

### Sicherheit des Datenbankmanagers

Wie im Abschnitt „Auswählen von Endbenutzernamen" auf Seite 76 beschrieben, kann der Anwendungs-Requester durch die Namensumsetzung für abgehende Anforderungen an den Sicherheitsfunktionen für verteilte Datenbanken beteiligt sein. Mit der Namensumsetzung für abgehende Anforderungen können Sie den Zugriff auf einen bestimmten Anwendungs-Server anhand der Identität des Endbenutzers und der Anwendung einschränken, von denen die Anforderung ausgeht. Der Anwendungs-Requester unter DB2 Universal Database für OS/390 kann auf folgende andere Arten an den Systemsicherheitsfunktionen beteiligt sein:

**Binden ferner Anwendungen**

Endbenutzer binden ferne Anwendungen auf dem Anwendungs-Server mit dem Befehl BIND PACKAGE von DB2 Universal Database für OS/390. DB2 Universal Database für OS/390 *schränkt* die Verwendung des Befehls BIND PACKAGE auf dem Requester *nicht ein*. Ein Endbenutzer kann ein fernes Paket jedoch erst dann verwenden, nachdem es in einen Plan in DB2 Universal Database für OS/390 aufgenommen wurde. DB2 Universal Database für OS/390 *schränkt* die Verwendung des Befehls BIND PLAN hingegen *ein*. Ein Endbenutzer kann einem Plan das ferne Paket nur dann hinzufügen, wenn dem Endbenutzer mit der Anweisung GRANT von DB2 Universal Database für OS/390 das Zugriffsrecht BIND bzw. BINDADD erteilt wurde.

Geben Sie beim Binden eines Pakets mit der Option ENABLE/DISABLE an, ob das Paket von einem TSO-, CICS/ESA-, IMS/ESA- oder einem fernen Subsystem mit DB2 Universal Database für OS/390 verwendet werden soll.

**Ausführen ferner Anwendungen**

Damit ein Endbenutzer von DB2 Universal Database für OS/390 eine ferne Anwendung ausführen kann, muß er über die Berechtigung zum Ausführen des Plans von DB2 Universal Database für OS/390 verfügen, der dieser Anwendung zugeordnet ist. Der Planeigner in DB2 Universal Database für OS/390 verfügt automatisch über die Berechtigung zum Ausführen des Plans. Anderen Endbenutzern kann die Berechtigung zum Ausführen des Plans durch die Anweisung GRANT EXECUTE von DB2 Universal Database für OS/390 erteilt werden. Auf diese Weise kann der Eigner einer Anwendung für verteilte Datenbanken individuell steuern, welche Benutzer die Anwendung verwenden dürfen.

### Sicherheitssubsystem

Das externe Sicherheitssubsystem auf OS/390-Systemen wird entweder durch RACF oder durch gleichwertige Produkte bereitgestellt, die über eine mit RACF kompatible Schnittstelle verfügen. Der Anwendungs-Requester unter DB2 Universal Database für OS/390 kann das externe Sicherheitssubsystem nicht direkt aufrufen, abgesehen von der im Abschnitt „Netzwerksicherheit” auf Seite 81 beschriebenen Unterstützung für verschlüsselte Kennwörter. Das externe Sicherheitssubsystem wird jedoch in den folgenden Situationen indirekt auf dem Anwendungs-Requester verwendet:

- Das für die Verbindungsherstellung zwischen Endbenutzer und DB2 Universal Database für OS/390 zuständige Produkt verwendet das externe Sicherheitssubsystem zur Überprüfung der Identität des Endbenutzers (Benutzer-ID und Kennwort). Dies geschieht vor der Verbindungsherstellung zwischen Endbenutzer und DB2 Universal Database für OS/390. Wie bereits erwähnt, sind CICS/ESA, TSO und IMS/ESA Beispiele für Produkte, die die Verbindung zwischen Endbenutzern und DB2 Universal Database für OS/390 herstellen.
- Wenn Sie Sicherheit auf SNA-Sitzungsebene (über das Schlüsselwort VERIFY in der VTAM-Anweisung APPL von DB2 Universal Database für OS/390) verwenden, wird das externe Sicherheitssubsystem von VTAM aufgerufen, um die Identität des fernen Systems zu überprüfen.

### Darstellen von Daten

DB2 Universal Database für OS/390 wird mit einer Standardinstallations-CCSID (Coded Character Set Identifier - ID für codierten Zeichensatz) von 500 ausgeliefert. Diese Standardeinstellung ist für Ihre Installation wahrscheinlich *nicht* korrekt.

Bei der Installation von DB2 Universal Database für OS/390 müssen Sie die Installations-CCSID auf die CCSID der Zeichen setzen, die von den Eingabeeinheiten an Ihrem Standort an DB2 Universal Database für OS/390 gesendet werden. Diese CCSID wird in der Regel durch die verwendete Landessprache festgelegt. Wenn die Installations-CCSID falsch ist, werden durch die Zeichenumsetzung inkorrekte Ergebnisse erzeugt. Eine Liste der in den einzelnen Ländern bzw. Landessprachen unterstützten CCSIDs finden Sie im *DB2 Connect Benutzerhandbuch*.

Sie müssen sicherstellen, daß Ihr Subsystem mit DB2 Universal Database für OS/390 die CCSIDs der einzelnen Anwendungs-Server in die Installations-CCSID des Subsystems mit DB2 Universal Database für OS/390 umsetzen kann. DB2 Universal Database für OS/390 stellt Umsetzungstabellen für die gängigsten Kombinationen aus Quellen- und Ziel-CCSIDs, jedoch nicht für jede mögliche Kombination bereit. Falls erforderlich, können Sie der Gruppe verfügbarer Umsetzungstabellen und Umsetzungsroutinen Angaben hinzufügen. Weitere Informationen zur Zeichenumsetzung unter DB2 Universal Database für OS/390 finden Sie im Handbuch *DB2 Universal Database for OS/390 Administration Guide*.

## Konfigurieren des Anwendungs-Servers

Die Anwendungs-Server-Unterstützung unter DB2 Universal Database für OS/390 ermöglicht die Verwendung des Systems mit DB2 Universal Database für OS/390 als Server für DRDA-Anwendungs-Requester. Folgende Anwendungs-Requester können mit einem Anwendungs-Server unter DB2 Universal Database für OS/390 verbunden sein:

- Requester unter DB2 Universal Database für OS/390
- DB2 Connect
- DB2 Universal Database Enterprise Edition oder DB2 Universal Database Enterprise - Extended Edition mit aktivierter DB2 Connect-Unterstützung
- Requester mit DB2 Version 2, der unter AIX, HP-UX, OS/2, Solaris, Windows 3.1, Windows 3.11 für Workgroups, Windows 95 oder Windows NT sowie Macintosh, SCO, SGI oder SINIX ausgeführt werden kann; Distributed Database Connection Services (DDCS) Mehrbenutzer-Gateway Version 2.3, DDCS Einzelplatz-System Version 2.3 und DDCS für Windows Version 2.4 stellen diese Funktion bereit
- Requester unter OS/400

- Requester unter DB2 für VM
- Jedes andere Produkt, das die Protokolle für DRDA-Anwendungs-Requester unterstützt

Für jeden mit einem Anwendungs-Server unter DB2 Universal Database für OS/390 verbundenen Anwendungs-Requester unterstützt der Anwendungs-Server unter DB2 Universal Database für OS/390 folgenden Datenbankzugriff:

- Der Anwendungs-Requester kann auf Tabellen zugreifen, die auf dem Anwendungs-Server unter DB2 Universal Database für OS/390 gespeichert sind. Der Anwendungs-Requester muß auf dem Anwendungs-Server unter DB2 Universal Database für OS/390 ein Paket erstellen, bevor die Anwendung ausgeführt werden kann. Der Anwendungs-Server unter DB2 Universal Database für OS/390 verwendet dieses Paket, um die SQL-Anweisungen der Anwendung während der Ausführung zu lokalisieren.
- Der Anwendungs-Requester kann den Anwendungs-Server unter DB2 Universal Database für OS/390 anweisen, den Zugriff auf Lesevorgänge einzuschränken, wenn die DRDA-Verbindung zwischen Requester und Server den zweiphasigen Festschreibeprozeß nicht unterstützt. Beispielsweise würde ein Requester unter DDCS Version 2 Release 3 mit einer CICS-Front-End-Anwendung den Anwendungs-Server unter DB2 Universal Database für OS/390 darüber informieren, daß Aktualisierungen nicht zulässig sind.
- Der Anwendungs-Requester kann durch systemgesteuerten Zugriff auch über die Berechtigung zum Zugriff auf Tabellen verfügen, die auf anderen Systemen mit DB2 Universal Database für OS/390 im Netzwerk gespeichert sind. Systemgesteuerter Zugriff ermöglicht dem Anwendungs-Requester die Herstellung von Verbindungen zu mehreren Datenbanksystemen in einer einzelnen Arbeitseinheit.

## Bereitstellen von Netzwerkinformationen

Damit der Anwendungs-Server unter DB2 Universal Database für OS/390 Anforderungen für verteilte Datenbanken ordnungsgemäß verarbeiten kann, müssen Sie folgende Schritte ausführen:

1. Definieren des Anwendungs-Servers für den lokalen Kommunikationsmanager
2. Definieren aller potentiellen Bestimmungsorte für sekundäre Server, damit der Anwendungs-Server unter DB2 Universal Database für OS/390 die SQL-Anforderungen an ihre Zielorte weiterleiten kann
3. Gewährleisten der erforderlichen Sicherheit
4. Gewährleisten der Datendarstellung

### Definieren des Anwendungs-Servers (SNA)

Damit der Anwendungs-Server Anforderungen für verteilte Datenbanken empfangen kann, muß er für den lokalen Kommunikationsmanager definiert sein und über einen eindeutigen RDB_NAME-Wert verfügen. Die folgenden Erläuterungen beziehen sich auf SNA-Verbindungen. Sie müssen folgende Schritte ausführen, um den Anwendungs-Server ordnungsgemäß zu definieren:

1. Wählen Sie den vom Anwendungs-Server unter DB2 Universal Database für OS/390 zu verwendenden LU-Namen und RDB_NAME-Wert aus. Der Aufzeichnungsprozeß dieser Namen in DB2 Universal Database für OS/390 und VTAM entspricht dem im Abschnitt „Definieren des lokalen Systems (SNA)" auf Seite 57 beschriebenen Prozeß. Der für DB2 Universal Database für OS/390 gewählte RDB_NAME-Wert muß allen Endbenutzern und Anwendungs-Requestern bereitgestellt werden, für die eine Verbindung zum Anwendungs-Server erforderlich ist.
2. Registrieren Sie den Wert für NETID.LUNAME für den Anwendungs-Server unter DB2 Universal Database für OS/390 auf allen Anwendungs-Requestern, die Zugriff erfordern, damit der Anwendungs-Requester SNA-Anforderungen an den Server unter DB2 Universal Database für OS/390 weiterleiten kann. Dies gilt auch für Fälle, in denen der Anwendungs-Requester dynamische Netzwerkweiterleitung ausführen kann, weil der Anwendungs-Requester den Wert für NETID.LUNAME kennen muß, bevor dynamische Netzwerkweiterleitung verwendet werden kann.
3. Stellen Sie den Standard-DRDA-TPN (X'07F6C4C2') für die einzelnen Anwendungs-Requester bereit, weil DB2 Universal Database für OS/390 diesen Wert automatisch verwendet.
4. Erstellen Sie für jeden von einem Anwendungs-Requester angeforderten Modusnamen einen Eintrag in der VTAM-Modustabelle. Diese Einträge beschreiben die RU-Größe, die Größe des Nachrichtendosierungsfensters und die Serviceklasse für die einzelnen Modusnamen.
5. Definieren Sie Sitzungsbegrenzungen für die Anwendungs-Requester, die eine Verbindung zu dem Anwendungs-Server unter DB2 Universal Database für OS/390 herstellen. Die VTAM-Anweisung APPL definiert Standardwerte für die Sitzungsbegrenzungen aller Partnersysteme. Verwenden Sie zum Definieren eindeutiger Standardwerte für einen bestimmten Partner die Tabelle SYSIBM.LUMODES der Kommunikationsdatenbank.

   Informationen zum Überprüfen des VTAM-Netzwerks finden Sie in „Einstellen von RU-Größe und Nachrichtendosierung" auf Seite 75.
6. Erstellen Sie in der Kommunikationsdatenbank von DB2 Universal Database für OS/390 Einträge, mit denen Sie angeben, welche Anwendungs-Requester zur Herstellung einer Verbindung zum Anwendungs-Server unter DB2 Universal Database für OS/390 berechtigt sind. Es gibt zwei

grundlegende Vorgehensweisen beim Definieren der Kommunikationsdatenbankeinträge für die Anwendungs-Requester im Netzwerk:

a. Sie können eine Zeile in die Tabelle SYSIBM.LUNAMES einfügen, die die Standardwerte für eine in der Kommunikationsdatenbank nicht spezifisch beschriebene LU bereitstellt (die Standardzeile enthält in der Spalte LUNAME Leerzeichen). Diese Vorgehensweise ermöglicht das Definieren spezifischer Attribute für einige der LUs in Ihrem Netzwerk und gleichzeitig das Bereitstellen von Standardwerten für alle anderen LUs.

   Beispielsweise können Sie dem System DALLAS (ein weiteres System mit DB2 Universal Database für OS/390) die Berechtigung erteilen, bereits überprüfte Anforderungen für verteilte Datenbanken (LU 6.2 SECURITY=SAME) zu senden, von Systemen mit Datenbankmanagern hingegen das Senden von Kennwörtern fordern. Zudem wollen Sie unter Umständen in der Kommunikationsdatenbank nicht für alle Systeme mit Datenbankmanager Einträge vornehmen, vor allem wenn es sich um viele Systeme handelt. Abb. 25 zeigt, wie die Kommunikationsdatenbank zur Angabe von SECURITY=SAME für das System DALLAS und von SECURITY=PGM für alle anderen Requester verwendet werden kann.

```
INSERT INTO SYSIBM.LUNAMES
     (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', ' ');
INSERT INTO SYSIBM.LUNAMES
     (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES (' ', ' ', 'C', 'N', 'N', ' ');
```

*Abbildung 25. Bereitstellen von Standardwerten für Anwendungs-Requester-Verbindungen (SNA)*

b. Mit der Kommunikationsdatenbank können Sie Berechtigungen für die einzelnen Anwendungs-Requester im Netzwerk individuell erteilen. Konfigurieren Sie dazu die Kommunikationsdatenbank auf eine der folgenden Arten:

   - Stellen Sie sicher, daß die Tabelle SYSIBM.LUNAMES keine Standardzeile enthält. Wenn die Standardzeile (die Zeile mit einem leeren LU-Namen) fehlt, muß für jeden Anwendungs-Requester, der eine Verbindungsherstellung versucht, in der Tabelle SYSIBM.LUNAMES eine Zeile mit dem LU-Namen aufgenommen werden. Wenn in der Kommunikationsdatenbank keine übereinstimmende Zeile gefunden wird, wird dem Anwendungs-Requester der Zugriff verweigert.
   - Tragen Sie in der Tabelle SYSIBM.LUNAMES eine Standardzeile ein, die angibt, daß eine Herkunftsüberprüfung erforderlich ist (Spalte USERNAMES auf 'I' oder 'B' gesetzt). Dadurch beschränkt DB2 Universal Database für OS/390 den Zugriff auf Anwendungs-

Requester und Endbenutzer, die in der Tabelle SYSIBM.USERNAMES angegeben sind (wie im Abschnitt „Herkunftsüberprüfung" auf Seite 91 beschrieben). Diese Vorgehensweise empfiehlt sich, wenn Ihre Regeln für die Umsetzung für Namen eine Zeile mit einem leeren LU-Namen in der Tabelle SYSIBM.LUNAMES erfordern, DB2 Universal Database für OS/390 diese Zeile jedoch nicht zum Erteilen eines unbeschränkten Zugriffs auf den Anwendungs-Server unter DB2 Universal Database für OS/390 verwenden soll.

In Abb. 26 enthält keine Zeile in der Spalte LUNAME Leerzeichen, d. h. DB2 Universal Database für OS/390 verweigert allen LUs außer LUDALLAS bzw. LUNYC den Zugriff.

```
INSERT INTO SYSIBM.LUNAMES
     (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', ' ');
INSERT INTO SYSIBM.LUNAMES
     (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', ' ');
```

*Abbildung 26. Angeben individueller Anwendungs-Requester-Verbindungen (SNA)*

### Definieren des Anwendungs-Servers (TCP/IP)

Damit der Anwendungs-Server Anforderungen für verteilte Datenbanken über TCP/IP-Verbindungen empfangen kann, muß er für das lokale TCP/IP-Subsystem definiert sein und über einen eindeutigen RDB_NAME-Wert verfügen. Zudem muß der BSDS von DB2 Universal Database für OS/390 die notwendigen Parameter enthalten, und Sie müssen unter Umständen die Kommunikationsdatenbank von DB2 Universal Database für OS/390 aktualisieren.

1. Informationen zum Konfigurieren von TCP/IP auf dem Anwendungs-Server finden Sie im Handbuch *DB2 Universal Database for OS/390 Installation Reference*. Das Konfigurieren des Anwendungs-Requesters wird in den Handbüchern *DB2 Connect Enterprise Edition für OS/2 und Windows Einstieg* und *DB2 Connect Personal Edition Einstieg* beschrieben.
2. Ein Beispiel für eine BSDS-Definition wird in Abb. 18 auf Seite 65 gezeigt.

3. Aktualisierungen der Kommunikationsdatenbank sind nicht erforderlich, wenn Sie nur TCP/IP-Datenbankverbindungen für eingehende Anforderungen verwenden, d. h. wenn DB2 Universal Database für OS/390 nur als TCP/IP-Server verwendet werden soll, müssen Sie in der Kommunikationsdatenbank keine Werte eintragen. Anstelle dessen können die Standardwerte verwendet werden. Es folgt ein einfaches Beispiel für die Aktualisierung der Tabelle SYSIBM.IPNAMES.

   Wenn Sie Anforderungen für Datenbankverbindungen für eingehende Anforderungen für TCP/IP-Knoten zulassen wollen, können Sie einen SQL-Befehl wie den folgenden verwenden, um diese Tabelle zu aktualisieren:

   ```
   INSERT INTO SYSIBM.IPNAMES (LINKNAME) VALUES('        ')
   ```

## Gewährleisten der Sicherheit

Wenn ein Anwendungs-Requester eine Anforderung für verteilte Datenbanken an den Anwendungs-Server unter DB2 Universal Database für OS/390 weiterleitet, kann die Sicherheit in folgenden Bereichen eine Rolle spielen:

- Herkunftsüberprüfung
- Auswählen von Endbenutzernamen
- Sicherheitsparameter des Netzwerks
- Sicherheit des Datenbankmanagers
- Von einem externen Sicherheitssubsystem implementierte Sicherheit

### Herkunftsüberprüfung

Der Anwendungs-Server unter DB2 Universal Database für OS/390 kann Einschränkungen für den Empfang von Endbenutzernamen von einem Anwendungs-Requester festlegen. Dazu wird die *Herkunftsüberprüfung* verwendet. Durch die Herkunftsüberprüfung kann der Anwendungs-Server angeben, daß eine bestimmte Benutzer-ID nur von bestimmten Partnern verwendet werden darf. Beispielsweise kann der Anwendungs-Server die Herkunft von JONES auf das System DALLAS beschränken. Wenn ein anderer Anwendungs-Requester (als DALLAS) versucht, den Namen JONES an den Anwendungs-Server zu senden, kann der Anwendungs-Server die Anforderung zurückweisen, weil der Name nicht vom korrekten Netzwerkstandort kommt.

DB2 Universal Database für OS/390 implementiert die Herkunftsüberprüfung als Teil der Umsetzung von Endbenutzernamen für eingehende Anforderungen, die im nächsten Abschnitt beschrieben wird.

**Anmerkung:** Eingangs- und Herkunftsüberprüfungen werden für eingehende TCP/IP-Anforderungen nicht ausgeführt.

### Auswählen von Endbenutzernamen

Die vom Anwendungs-Requester übergebene Benutzer-ID ist möglicherweise nicht im gesamten SNA-Netzwerk eindeutig. Der Anwendungs-Server unter DB2 Universal Database für OS/390 muß unter Umständen die Namensumsetzung für eingehende Anforderungen ausführen, um im gesamten SNA-Netzwerk eindeutige Endbenutzernamen erstellen zu können. Gleichermaßen muß der Anwendungs-Server unter DB2 Universal Database für OS/390 unter Umständen die Namensumsetzung für abgehende Anforderungen ausführen, um den an der Anwendung beteiligten sekundären Servern einen eindeutigen Endbenutzernamen bereitzustellen. (Weitere Informationen zur Umsetzung von Endbenutzernamen für abgehende Anforderungen finden Sie in „Gewährleisten der Sicherheit" auf Seite 76.)

Die Namensumsetzung für eingehende Anforderungen wird durch das Setzen der Spalte USERNAMES in der Tabelle SYSIBM.LUNAMES bzw. SYSIBM.IPNAMES auf 'I' (Namensumsetzung für eingehende Anforderungen) oder 'B' (Namensumsetzung für eingehende und abgehende Anforderungne) aktiviert. Wenn Namensumsetzung für eingehende Anforderungen aktiviert ist, setzt DB2 Universal Database für OS/390 die vom Anwendungs-Requester gesendete Benutzer-ID und den Eignernamen des Plans von DB2 Universal Database für OS/390 um (wenn der Anwendungs-Requester ein weiteres System mit DB2 Universal Database für OS/390 ist).

Wenn der Anwendungs-Requester eine Benutzer-ID und ein Kennwort an das APPC-Verb ALLOCATE sendet, werden die Benutzer-ID und das Kennwort vor der Umsetzung der Benutzer-ID auf Gültigkeit überprüft. Die Spalte PASSWORD in der Tabelle SYSIBM.USERNAMES wird nicht für die Gültigkeitsprüfung des Kennworts verwendet. Statt dessen werden die Benutzer-ID und das Kennwort dem externen Sicherheitssystem (RACF oder ein äquivalentes Produkt) zur Gültigkeitsprüfung übergeben.

Bei der Prüfung der ankommenden Benutzer-ID im Verb ALLOCATE kann DB2 Universal Database für OS/390 mit Hilfe der Benutzerausgänge für Berechtigungsüberprüfungen eine Liste der sekundären Berechtigungs-IDs (AUTHIDs) bereitstellen und zusätzliche Sicherheitsprüfungen ausführen. Ausführlichere Informationen hierzu finden Sie im Handbuch *DB2 Universal Database für OS/390 Systemverwaltung*.

Der Prozeß zur Namensumsetzung für eingehende Anforderungen sucht in der Tabelle SYSIBM.USERNAMES nach einer Zeile, die einem der in der folgenden Liste gezeigten Muster entsprechen muß (TYPE.AUTHID.LINKNAME):

1. I.AUTHID.LINKNAME — ein bestimmter Endbenutzer von einem bestimmten Anwendungs-Requester
2. I.AUTHID.leer — ein bestimmter Endbenutzer von einem beliebigen Anwendungs-Requester

3. I.leer.LINKNAME — ein beliebiger Endbenutzer von einem bestimmten Anwendungs-Requester

Wenn keine Zeile gefunden wird, wird der Fernzugriff verweigert. Wenn eine Zeile gefunden wird, wird der Fernzugriff erteilt, und der Endbenutzername wird in den von der Spalte NEWAUTHID bereitgestellten Wert geändert. Dabei gibt ein leerer NEWAUTHID-Wert an, daß der Name nicht geändert wird. Alle von DB2 Universal Database für OS/390 ausgeführten Ressourcenberechtigungsprüfungen (z. B. SQL-Tabellenzugriffsrechte) werden an den umgesetzten Endbenutzernamen und nicht an den Originalbenutzernamen vorgenommen.

Beim Empfangen eines Endbenutzernamens vom Anwendungs-Requester durch den Anwendungs-Server unter DB2 Universal Database für OS/390 können durch die Funktion zur Namensumsetzung für eingehende Anforderungen mehrere Ziele erreicht werden:

- Sie können einen Endbenutzernamen so ändern, daß er eindeutig ist. Beispielsweise setzen die folgenden SQL-Anweisungen den Endbenutzernamen JONES vom Anwendungs-Requester NEWYORK (LUNAME LUNYC) in einen anderen Namen (NYJONES) um.

```
INSERT INTO SYSIBM.LUNAMES
     (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS,
              MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('I', 'JONES', 'LUNYC', 'NYJONES', ' ');
```

- Sie können den Endbenutzernamen ändern, um eine Gruppe von Endbenutzern durch einen einzelnen Namen zu repräsentieren. Beispielsweise könnten Sie alle Benutzer vom Anwendungs-Requester NEWYORK (LUNAME LUNYC) durch den Benutzernamen NYUSER repräsentieren. Dadurch können Sie dem Namen NYUSER SQL-Zugriffsrechte erteilen und den SQL-Zugriff steuern, der den Benutzern des Systems NEWYORK erteilt wird.

```
INSERT INTO SYSIBM.LUNAMES
     (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS,
              MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
  VALUES ('I', ' ', 'LUNYC', 'NYUSER', ' ');
```

- Sie können die durch einen bestimmten Anwendungs-Requester übertragenen Endbenutzernamen einschränken. Durch diese Verwendung der Umsetzung für Endbenutzernamen wird die im Abschnitt „Herkunftsüberprüfung” auf Seite 91 beschriebene Herkunftsüberprüfung erzielt. Beispielsweise lassen die folgenden SQL-Anweisungen nur SMITH und JONES als Endbenutzernamen vom Anwendungs-Requester

NEWYORK zu. Allen anderen Namen wird der Zugriff verweigert, weil sie nicht in der Tabelle SYSIBM.USERNAMES aufgelistet sind.

```
INSERT INTO SYSIBM.LUNAMES
     (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS,
              MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('I', 'SMITH', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('I', 'JONES', 'LUNYC', ' ', ' ');
```

- Sie können die Anwendungs-Requester einschränken, denen die Verbindung zum Anwendungs-Server unter DB2 Universal Database für OS/390 erlaubt wird. Dies ist eine weitere Funktion der Herkunftsüberprüfung. Im folgenden Beispiel werden alle an den Anwendungs-Requester NEWYORK (LUNYC) und den Anwendungs-Requester CHICAGO (LUCHI) gesendeten Endbenutzernamen akzeptiert. Anderen Anwendungs-Requestern wird der Zugriff verweigert, weil in der Standardzeile der Tabelle SYSIBM.LUNAMES die Namensumsetzung für alle eingehenden Anforderungen angegeben ist.

  ```
  INSERT INTO SYSIBM.LUNAMES
       (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS,
                MODESELECT, USERNAMES)
  VALUES (' ', ' ', 'A', 'N', 'N', 'I');
  INSERT INTO SYSIBM.USERNAMES
       (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
  VALUES ('I', ' ', 'LUNYC', ' ', ' ');
  INSERT INTO SYSIBM.USERNAMES
       (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
  VALUES ('I', ' ', 'LUCHI', ' ', ' ');
  ```

### Gewährleisten der Netzwerksicherheit

LU 6.2 stellt bei SNA-Verbindungen die folgenden drei Hauptsicherheitseinrichtungen für das Netzwerk zur Verfügung:

- Sicherheit auf Sitzungsebene
- Sicherheit auf Dialogebene
- Verschlüsselung

Im Abschnitt „Netzwerksicherheit” auf Seite 81 wird die Angabe der Sicherheit auf Sitzungsebene und der Verschlüsselung unter DB2 Universal Database für OS/390 erläutert. Die Verwendung von Sicherheit auf Sitzungsebene und von Verschlüsselung seitens des Anwendungs-Servers unter DB2 Universal Database für OS/390 entspricht genau der seitens des Anwendungs-Requesters unter DB2 Universal Database für OS/390.

In punkto Netzwerksicherheit muß nun nur noch die SNA-Dialogsicherheitsstufe behandelt werden. Einige der Aspekte der Dialog-

sicherheitsstufe gelten nur für einen Anwendungs-Server unter DB2 Universal Database für OS/390. Der Anwendungs-Server unter DB2 Universal Database für OS/390 spielt in der Netzwerksicherheit zwei unterschiedliche Rollen:

- Zum einen ist der Anwendungs-Server unter DB2 Universal Database für OS/390 als Requester für sekundäre Server für das Absetzen von APPC-Anforderungen zuständig, die die für sekundäre Server erforderlichen Parameter der SNA-Dialogsicherheitsstufe enthalten. Der Anwendungs-Server unter DB2 Universal Database für OS/390 definiert die Anforderungen der SNA-Dialogsicherheitsstufe für alle sekundären Server unter Verwendung der Spalte USERNAMES in der Tabelle SYSIBM.LUNAMES und der Tabelle SYSIBM.USERNAMES. Die Einzelangaben dieser Definitionen entsprechen denen im Abschnitt „Netzwerksicherheit" auf Seite 81.
- Zum anderen diktiert der Anwendungs-Server unter DB2 Universal Database für OS/390 als Server für den Anwendungs-Requester die Anforderungen der SNA-Dialogsicherheitsstufe für den Anwendungs-Requester. DB2 Universal Database für OS/390 ermittelt die für jeden Anwendungs-Requester im Netzwerk erforderliche Dialogsicherheit unter Verwendung der Spalte USERSECURITY in der Tabelle SYSIBM.LUNAMES. Folgende Werte werden in der Spalte USERSECURITY verwendet:

  **C** Hiermit wird angegeben, daß DB2 Universal Database für OS/390 vom Anwendungs-Requester das Senden einer Benutzer-ID und eines Kennworts (LU 6.2 SECURITY=PGM) bei jeder Anforderung für verteilte Datenbanken erfordert. Wenn in der Spalte ENCRYPTPSWDS der Tabelle SYSIBM.LUNAMES ein 'Y' enthalten ist, geht DB2 Universal Database für OS/390 davon aus, daß das Kennwort bereits in verschlüsseltem RACF-Format vorliegt (dies ist nur für einen Anwendungs-Requester unter DB2 Universal Database für OS/390 möglich). Wenn in der Spalte ENCRYPTPSWDS kein 'Y' enthalten ist, erwartet DB2 Universal Database für OS/390 das Kennwort im LU 6.2-Standardformat (EBCDIC-Zeichendarstellung). In beiden Fällen übergibt DB2 Universal Database für OS/390 die Werte für Benutzer-ID und Kennwort zur Gültigkeitsprüfung an das Sicherheitssubsystem. Ihr Sicherheitssubsystem muß eine Prüfung von APPC-Benutzer-ID und APPC-Kennwort bereitstellen, wie z. B. RACF. Wenn das Sicherheitssubsystem das Paar aus Benutzer-ID und Kennwort zurückweist, wird der Zugriff auf verteilte Datenbanken verweigert.

  **Jeder andere Wert**
  Hiermit wird angegeben, daß der Anwendungs-Requester eine bereits überprüfte Benutzer-ID (LU 6.2 SECURITY=SAME) oder eine Benutzer-ID und ein Kennwort (LU 6.2 SECURITY=PGM) senden kann. Wenn eine Benutzer-ID und ein Kennwort gesendet werden, verarbeitet DB2 Universal Database für OS/390 sie wie für 'C' oben beschrieben. Wenn in der Anforderung nur eine

Benutzer-ID enthalten ist, wird das Sicherheitssubsystem aufgerufen, um den Benutzer zu überprüfen, sofern nicht die Tabelle SYSUSERNAMES zum Verwalten der eingehenden Benutzer-IDs verwendet wird.

Wenn eine Sicherheitsverletzung festgestellt wird, fordert LU 6.2 den Anwendungs-Server unter DB2 Universal Database für OS/390 auf, dem Anwendungs-Requester den Prüfcode der SNA-Sicherheitsstörung ('080F6051'X) zu liefern. Da dieser Prüfcode die Fehlerursache nicht beschreibt, werden von DB2 Universal Database für OS/390 zwei Methoden zum Aufzeichnen der Sicherheitsverletzungsursache bei verteilten Datenbanken bereitgestellt:

- Eine Nachricht DSNL030I mit der LUWID des Requesters und einem DB2-Ursachencode, der den Fehler beschreibt, wird angezeigt. DSNL030I enthält auch (sofern bekannt) die zurückgewiesene AUTHID, die von der Anwendungsanforderung gesendet wurde.
- In der NetView-Datenbank für Hardwareüberwachung wird ein Alert eingetragen, der die gleichen Informationen wie die Nachricht DSNL030I enthält.

## Sicherheit des Datenbankmanagers

Als Eigner der Datenbankressourcen steuert der Anwendungs-Server unter DB2 Universal Database für OS/390 die Datenbanksicherheitsfunktionen für SQL-Objekte, die sich auf dem Anwendungs-Server unter DB2 Universal Database für OS/390 befinden. Der Zugriff auf von DB2 Universal Database für OS/390 verwaltete Objekte wird durch Zugriffsrechte gesteuert, die Benutzern durch den Administrator von DB2 Universal Database für OS/390 oder durch die Eigner der einzelnen Objekte erteilt werden. Der Anwendungs-Server unter DB2 Universal Database für OS/390 steuert die folgenden beiden grundlegenden Objektklassen:

- **Pakete**— Einzelne Endbenutzer erhalten die Berechtigung zum Erstellen, Ersetzen und Ausführen von Paketen mit Hilfe der Anweisung GRANT in DB2 Universal Database für OS/390. Wenn ein Endbenutzer der Eigner eines Pakets ist, kann er das Paket automatisch ausführen und ersetzen. Anderen Endbenutzern muß mit der Anweisung GRANT ausdrücklich die Berechtigung zum Ausführen eines Pakets auf dem Anwendungs-Server unter DB2 Universal Database für OS/390 erteilt werden. Die Berechtigung USE kann für einzelne Endbenutzer erteilt werden oder für PUBLIC, d. h. alle Endbenutzer dürfen das Paket ausführen.

  Nach dem Binden einer Anwendung an DB2 Universal Database für OS/390 enthält das Paket die im Anwendungsprogramm enthaltenen SQL-Anweisungen. Diese SQL-Anweisungen werden wie folgt klassifiziert:

  **Statisches SQL**
  Statisches SQL bedeutet, daß die SQL-Anweisung und die SQL-Objekte, auf die in der Anweisung verwiesen wird, zum Zeitpunkt

des Bindens der Anwendung an DB2 Universal Database für OS/390 bekannt sind. Der Ersteller des Pakets muß über die Berechtigung zum Ausführen für jede der statischen SQL-Anweisungen in dem Paket verfügen.

Wenn Endbenutzer die Berechtigung zum Ausführen eines Pakets erhalten, verfügen sie damit automatisch über die Berechtigung zum Ausführen aller statischen SQL-Anweisungen in dem Paket. Dies bedeutet, daß Endbenutzer keine Tabellenzugriffsrechte von DB2 Universal Database für OS/390 benötigen, wenn das Paket ausschließlich statische SQL-Anweisungen enthält.

**Dynamisches SQL**

Dynamisches SQL bezeichnet eine SQL-Anweisung, die vor der Ausführung des Pakets nicht bekannt ist. Mit anderen Worten, die SQL-Anweisung wird von dem betreffenden Programm erstellt und durch die SQL-Anweisung PREPARE dynamisch an DB2 Universal Database für OS/390 gebunden. Wenn ein Endbenutzer eine dynamische SQL-Anweisung ausführt, muß er über die erforderlichen Tabellenzugriffsrechte zum Ausführen der SQL-Anweisung verfügen. Da die SQL-Anweisung bei der Erstellung des Plans bzw. Pakets noch nicht bekannt ist, wird dem Endbenutzer die erforderliche Berechtigung vom Paketeigner nicht automatisch erteilt.

- **SQL-Objekte:** Hierbei handelt es sich um Tabellen, Sichten, Synonyme oder Aliasnamen. Benutzern von DB2 Universal Database für OS/390 können verschiedene Berechtigungsstufen zum Erstellen, Löschen, Ändern oder Lesen einzelner SQL-Objekte erteilt werden. Diese Berechtigung ist für das Binden statischer SQL-Anweisungen und zum Ausführen dynamischer SQL-Anweisungen erforderlich.

Beim Erstellen eines Pakets können Sie mit der Option DISABLE/ENABLE steuern, welche Verbindungsarten von DB2 Universal Database für OS/390 das Paket ausführen können. Sie können mit RACF und Sicherheitsausgangsroutinen von DB2 Universal Database für OS/390 Endbenutzern selektiv die Verwendung von DDF erlauben. Sie können mit RLF Angaben zur Begrenzung der Verarbeitungszeit für ferne Bindevorgänge und für die Ausführung dynamischer SQL-Anweisungen vornehmen.

Beispiel: Der Eigner eines Pakets von DB2 Universal Database für OS/390 namens MYPKG heißt JOE. JOE kann SAL die Berechtigung zum Ausführen des Pakets durch Absetzen der Anweisung GRANT USE von DB2 Universal Database für OS/390 erteilen. Wenn SAL das Paket ausführt, geschieht folgendes:

- DB2 Universal Database für OS/390 prüft, ob SAL die Berechtigung USE für das Paket erteilt wurde.

- SAL kann alle statischen SQL-Anweisungen im Paket absetzen, weil JOE über die erforderlichen SQL-Objektzugriffsrechte zum Erstellen des Pakets verfügt.
- Wenn das Paket dynamische SQL-Anweisungen enthält, muß SAL über eigene SQL-Tabellenzugriffsrechte verfügen. Beispielsweise kann SAL SELECT * FROM JOE.TABLE5 erst absetzen, nachdem SAL der Lesezugriff auf JOE.TABLE5 erteilt wurde.

### Sicherheitssubsystem

Die Verwendung des Sicherheitssubsystems (RACF oder ein äquivalentes Produkt) vom Anwendungs-Server unter DB2 Universal Database für OS/390 hängt davon ab, wie Sie die Funktion zur Namensumsetzung für eingehende Anforderungen in der Tabelle SYSIBM.LUNAMES definieren:

- Wenn Sie 'I' oder 'B' für die Spalte USERNAMES angeben, ist die Namensumsetzung für eingehende Anforderungen aktiv, und DB2 Universal Database für OS/390 nimmt an, daß der Administrator von DB2 Universal Database für OS/390 die Namensumsetzung für eingehende Anforderungen als Teil der Systemsicherheitsimplementierung ausführt. Das externe Sicherheitssubsystem wird nur aufgerufen, wenn der Anwendungs-Requester eine Anforderung mit Benutzer-ID und Kennwort (SECURITY=PGM) sendet. Ihr Sicherheitssubsystem muß eine Prüfung von APPC-Benutzer-ID und APPC-Kennwort bereitstellen, wie z. B. RACF.

  Wenn die Anforderung vom Anwendungs-Requester nur eine Benutzer-ID enthält (SECURITY=SAME), wird das externe Sicherheitssystem nicht aufgerufen, weil die Regeln für die Namensumsetzung für eingehende Anforderungne definieren, welche Benutzer eine Verbindung zum Anwendungs-Server unter DB2 Universal Database für OS/390 herstellen dürfen.
- Wenn Sie eine andere Angabe als 'I' oder 'B' für die Spalte USERNAMES vornehmen, werden die folgenden Sicherheitssubsystemüberprüfungen ausgeführt:
  - Wenn eine Anforderung für verteilte Datenbanken des Anwendungs-Requesters empfangen wird, ruft DB2 Universal Database für OS/390 das externe Sicherheitssystem auf, um die Gültigkeit der Benutzer-ID (und des Kennworts, sofern bereitgestellt) des Endbenutzers zu überprüfen.
  - Das externe Sicherheitssystem wird aufgerufen, um zu prüfen, ob der Endbenutzer über die Berechtigung zur Verbindungsherstellung zum Subsystem mit DB2 Universal Database für OS/390 verfügt.
- In jedem Fall wird ein Benutzerausgang für Berechtigungsüberprüfungen implementiert, um eine Liste der sekundären Berechtigungs-IDs bereitzustellen. Weitere Informationen finden Sie im Handbuch *DB2 Universal Database für OS/390 Administration Guide*.

### Darstellen von Daten

Sie müssen sicherstellen, daß Ihr Subsystem mit DB2 Universal Database für OS/390 die CCSIDs der einzelnen Anwendungs-Requester in die Installations-CCSID des Subsystems mit DB2 Universal Database für OS/390 umsetzen kann. Weitere Informationen finden Sie in „Darstellen von Daten” auf Seite 86.

# Kapitel 3. Verbinden von DB2 Universal Database für AS/400 in einem DRDA-Netzwerk über SNA

OS/400 umfaßt DB2 Universal Database für AS/400, das Verwaltungssystem für relationale Datenbanken von IBM für Systeme IBM AS/400.

In diesem Kapitel wird erklärt, wie Sie ein System IBM AS/400 konfigurieren können, um Konnektivität zu unterstützen zwischen:

1. Workstations mit DB2 Connect (siehe „Konfigurieren des Anwendungs-Servers" auf Seite 113) und
2. einem Server mit DB2 Universal Database (siehe „Konfigurieren des Anwendungs-Requesters" auf Seite 102)

Informationen zur Herstellung von Verbindungen zwischen zwei Systemen IBM AS/400 finden Sie im Handbuch *AS/400 Distributed Database Programming*.

DB2 Universal Database für AS/400 Version 4.2 führt Unterstützung für DRDA-Kommunikation über TCP/IP ein. Die Mehrzahl der Informationen zu diesem Thema finden Sie ebenfalls im Handbuch *AS/400 Distributed Database Programming*, und die erforderlichen Schritte aus diesem Handbuch sind in „Kapitel 4. Verbinden von DB2 Universal Database für AS/400 in einem DRDA-Netzwerk über TCP/IP" auf Seite 121 zusammengefaßt. Die Prinzipien entsprechen denjenigen, die auch in diesem Kapitel dargestellt sind. Die Netzwerkkonfigurationsaufgaben sind jedoch viel einfacher.

## Implementierung von DB2 Universal Database für AS/400

Dieses Kapitel beschreibt, wie DB2 Universal Database für AS/400 Systeme für verteilte Datenbanken unterstützt. Ab Version 2 Release 1 Modifikation 1 des Lizenzprogramms OS/400 werden ferne DRDA-Arbeitseinheiten unterstützt, und ab OS/400 Version 3 Release 1 werden verteilte DRDA-Arbeitseinheiten (DUOW) unterstützt. Diese Unterstützung ist Bestandteil des Betriebssystems OS/400. Die Lizenzprogramme Query Manager und SQL Development Kit von DB2 Universal Database für AS/400 sind also für die Verwendung der DRDA-Unterstützung oder zum Ausführen von Programmen mit eingebetteten SQL-Anweisungen nicht erforderlich.

## Konfigurieren des Anwendungs-Requesters

Das System IBM AS/400 implementiert die Unterstützung für den DRDA-Anwendungs-Requester als integralen Bestandteil des Betriebssystems OS/400. Daher ist die Unterstützung für Anwendungs-Requester immer aktiv, wenn das Betriebssystem aktiv ist. Dies gilt auch für die Unterstützung des Anwendungs-Servers unter DB2 Universal Database für AS/400.

Wenn DB2 Universal Database für AS/400 als Anwendungs-Requester fungiert, kann es eine Verbindung zu jedem Anwendungs-Server herstellen, der DRDA unterstützt. Sie müssen folgende Punkte beachten, damit der Anwendungs-Requester unter DB2 Universal Database für AS/400 Zugriff auf verteilte Datenbanken bereitstellen kann:

- Bereitstellen von Netzwerkinformationen
- Gewährleisten der Sicherheit
- Darstellen von Daten

### Bereitstellen von Netzwerkinformationen

Der Anwendungs-Requester muß in der Lage sein, den Namen einer relationalen Datenbank entgegenzunehmen und in Netzwerkparameter umzusetzen. Das System IBM AS/400 verwendet das Verzeichnis für relationale Datenbanken zum Registrieren der Namen relationaler Datenbanken und der dazugehörigen Netzwerkparameter. Dieses Verzeichnis ermöglicht dem Anwendungs-Requester auf dem System IBM AS/400 das Übergeben der erforderlichen Netzwerkinformationen, um Fernverbindungen in einem Netzwerk mit verteilten Datenbanken herzustellen.

Viele Verarbeitungsprozesse in einer verteilten Datenbankumgebung machen den Austausch von Nachrichten mit anderen Netzwerkstandorten erforderlich. Damit diese Verarbeitungsprozesse korrekt in der SNA-Umgebung ausgeführt werden können, sind Ihrerseits folgende Schritte notwendig:

- Definieren des lokalen Systems für DB2 Universal Database für AS/400
- Definieren des fernen Systems für DB2 Universal Database für AS/400
- Definieren der Kommunikation für DB2 Universal Database für AS/400

#### Definieren des lokalen Systems für DB2 Universal Database für AS/400

Jeder Anwendungs-Requester im Netzwerk mit verteilten Datenbanken muß in seinem Verzeichnis relationaler Datenbanken einen Eintrag für die eigene lokale relationale Datenbank und je einen Eintrag für jede ferne relationale Datenbank haben, auf die der Anwendungs-Requester zugreift. Jedes System IBM AS/400 im Netzwerk mit verteilten Datenbanken, das nur als Anwendungs-Server fungiert, muß im eigenen Verzeichnis relationaler Datenbanken einen Eintrag für die lokale relationale Datenbank haben. Weitere Informationen zum Verzeichnis relationaler Datenbanken finden Sie im Handbuch *AS/400 Distributed Database Programming*.

Benennen sie zum Definieren des lokalen Systems die lokale Datenbank, indem Sie einen Eintrag mit dem Namen der fernen Station als *LOCAL zum relationalen Datenbankverzeichnis hinzufügen. Verwenden Sie dazu den Befehl zum Hinzufügen eines Eintrags im Verzeichnis relationaler Datenbanken (ADDRDBDIRE). Das folgende Beispiel zeigt den Befehl ADDRDBDIRE, in dem als Datenbankname des Anwendungs-Requesters ROCHESTERDB angegeben wird:

```
ADDRDBDIRE RDB(ROCHESTERDB) RMTLOCNAME(*LOCAL)
```

Ausführlichere Informationen zu Befehlen für das Verzeichnis relationaler Datenbanken finden Sie im Handbuch *AS/400 Distributed Database Programming*.

**Anmerkung:** In den neusten Versionen von OS/400 wird der lokale RDB-Namenseintrag bei Bedarf automatisch erstellt, wenn er nicht bereits vorhanden ist. Als lokaler RDB-Name wird der Systemname in den Netzwerkattributen verwendet.

### Definieren des fernen Systems für DB2 Universal Database für AS/400

Für jeden Anwendungs-Server im Netzwerk mit verteilten Datenbanken muß auch ein lokaler Eintrag im RDB-Verzeichnis vorhanden sein. Zudem muß im RDB-Verzeichnis der einzelnen Anwendungs-Requester ein Eintrag für jede ferne Datenbank bestehen. Erstellen Sie diese Einträge wie folgt:

- Definieren Sie mit dem Befehl ADDRDBDIRE bzw. WRKRDBDIRE die fernen Datenbanken für die lokale Datenbank, indem Sie dem Verzeichnis relationaler Datenbanken einen Eintrag für jede ferne Datenbank hinzufügen. Bei SNA-Kommunikation können Sie folgende Informationen angeben:
  - Name der fernen Datenbank
  - Name des fernen Standorts der Datenbank
  - Name des lokalen Standorts
  - Modusname zur Herstellung der Fernverbindungen
  - Ferne Netzwerk-ID
  - Name der Einheit für die Fernverbindungen
  - Name des Transaktionsprogramms der fernen Datenbank

  In den meisten Fällen sind nur der Name der fernen Datenbank und der Name des fernen Standorts[4] der Datenbank erforderlich. Wenn nur der Name des fernen Standorts angegeben wird, werden für die übrigen Parameter Standardwerte verwendet. Das System wählt eine Einheitenbeschreibung aus, die den Namen der fernen Datenbank enthält.

4. „Standortname" in OS/400 ist gleichbedeutend mit „LU-Name" in VTAM. „Name des fernen Standorts" bedeutet „Name der Partner-LU oder der fernen LU".

Wenn derselbe Name für einen fernen Standort in mehreren Einheitenbeschreibungen vorkommt und eine bestimmte Beschreibung erforderlich ist, sollten die Werte für den lokalen Standort und die ferne Netzwerk-ID in dem Eintrag im Verzeichnis relationaler Datenbanken mit den Werten in der Einheitenbeschreibung übereinstimmen. Das Auswählen von Einheitenbeschreibungen kann kompliziert werden, wenn derselbe Name für einen fernen Standort in mehreren Einheitenbeschreibungen verwendet wird. Verwenden Sie in jeder Einheitenbeschreibung eindeutige Namen für ferne Standorte, um Verwechslungen zu vermeiden. Als Transaktionsprogrammname der fernen Datenbank wird standardmäßig der DRDA-Standard-Transaktionsprogrammname X'07F6C4C2' verwendet.

Die Informationen zur Fernverbindung im Verzeichnis relationaler Datenbanken werden zum Einrichten eines Dialogs mit dem fernen System verwendet.

Bei TCP/IP-Verbindungen (in DB2 Universal Database für AS/400 Version 4.2 unterstützt) sind nur der Name der fernen Datenbank sowie die zugehörige IP-Adresse und der zugehörige Anschluß erforderlich. Weitere Informationen finden Sie in „Kapitel 4. Verbinden von DB2 Universal Database für AS/400 in einem DRDA-Netzwerk über TCP/IP” auf Seite 121.

### Definieren der SNA-Kommunikation

Dieser Abschnitt beschreibt das Konfigurieren der Kommunikation auf dem System IBM AS/400 über APPN (Advanced Peer-to-Peer Networking). Das System IBM AS/400 ermöglicht außerdem Konfigurationen für APPC (Advanced Program-to-Program Communications), die keine Unterstützung für die Weiterleitung im Netzwerk bereitstellen. Eine verteilte AS/400-Datenbank kann mit jeder der beiden Konfigurationen betrieben werden. Weitere Informationen zu APPC-Konfigurationen finden Sie im Handbuch *OS/400 Communications Configuration*.

Die AnyNet-Unterstützung auf dem System IBM AS/400 ermöglicht das Ausführen von APPC-Anwendungen über TCP/IP-Netzwerke (TCP/IP - Transmission Control Protocol/Internet Protocol). Die Beispiele in den nachfolgenden Abschnitten umfassen DDM, SNA-Verteilungsservices (Systems Network Architecture Distribution Services), Alerts und 5250 Datensichtgerätsdurchgriff. Diese Anwendungen können zusammen mit DRDA nach einigen zusätzlichen Konfigurationsschritten unverändert über TCP/IP-Netzwerke ausgeführt werden. Geben Sie für die AnyNet-Unterstützung den Wert *ANYNW im Parameter LINKTYPE des Befehls CRTCTLAPPC ein.

Weitere Informationen zu APPC über TCP/IP finden Sie in den Handbüchern *OS/400 Communications Configuration* und *OS/400 TCP/IP Configuration and Reference*. (Unterstützung für eigenständige TCP/IP-Verbindungen bei DRDA-Kommunikation wird in DB2 Universal Database für AS/400 Version 4.2

bereitgestellt. Weitere Informationen finden Sie in „Kapitel 4. Verbinden von DB2 Universal Database für AS/400 in einem DRDA-Netzwerk über TCP/IP" auf Seite 121.)

APPN stellt eine Unterstützung für den Netzwerkbetrieb zur Verfügung, mit deren Hilfe das System IBM AS/400 an einem Netzwerk mit Systemen teilnehmen und dieses steuern kann, ohne die Netzwerkunterstützung zu benötigen, die normalerweise von einem Großrechnersystem implementiert wird. Die folgenden Schritte beschreiben das Konfigurieren eines Systems IBM AS/400 für APPN-Unterstützung.

1. Definieren Sie die Netzwerkattribute mit dem Befehl CHGNETA (Netzwerkattributänderung).

   Zu den Netzwerkattributen gehören:

   - Der Name des lokalen Systems
   - Der Name des Systems im APPN-Netzwerk
   - Die Kennung (ID) des lokalen Netzwerks
   - Die Netzwerkknotenart
   - Die Namen der vom System IBM AS/400 verwendeten Netzwerk-Server, wenn die Maschine ein Endknoten ist
   - Die Netzwerksteuerpunkte, wenn das System IBM AS/400 ein Endknoten ist

2. Erstellen Sie die Leitungsbeschreibung.

   Die Leitungsbeschreibung beschreibt die physische Verbindungsleitung und das Datenübertragungsprotokoll, die zwischen dem System IBM AS/400 und dem Netzwerk verwendet werden sollen. Verwenden Sie die folgenden Befehle zum Erstellen von Leitungsbeschreibungen:

   - Leitungsbeschreibung erstellen (Ethernet) (CRTLINETH)
   - Leitungsbeschreibung erstellen (SDLC) (CRTLINSDLC)
   - Leitungsbeschreibung erstellen (Token-Ring) (CRTLINTRN)
   - Leitungsbeschreibung erstellen (X.25) (CRTLINX25)

3. Erstellen Sie Steuereinheitenbeschreibungen.

   Die Steuereinheitenbeschreibung beschreibt die benachbarten Systeme im Netzwerk. Weisen Sie auf die Verwendung der APPN-Unterstützung durch Angeben von APPN(*YES) beim Erstellen der Steuereinheitenbeschreibung hin. Verwenden Sie die folgenden Befehle zum Erstellen von Steuereinheitenbeschreibungen:

   - Steuereinheitenbeschreibung erstellen (APPC) (CRTCTLAPPC)
   - Steuereinheitenbeschreibung erstellen (SNA-HOST) (CRTCTLHOST)

   Wird der Parameter AUTOCRTCTL einer Token-Ring- oder Ethernet-Leitungsbeschreibung auf *YES gesetzt, wird automatisch eine Steuer-

einheitenbeschreibung erstellt, wenn das System über die Token-Ring- oder Ethernet-Leitung eine Sitzungsstartanforderung empfängt.

4. Erstellen Sie eine Serviceklassenbeschreibung.

   Verwenden Sie die Serviceklassenbeschreibung zum Auswählen der Kommunikationsverbindungswege (Verbindungsgruppen) und zur Vergabe von Übertragungsprioritäten. Das System stellt folgende fünf Serviceklassenbeschreibungen zur Verfügung:

   **#CONNECT**
   Die Standardserviceklasse.

   **#BATCH**
   Eine Serviceklasse für Stapeljobs.

   **#BATCHSC**
   Entspricht #BATCH, jedoch ist mindestens die Datenübertragungssicherheit eines Netzwerks mit Paketvermittlung erforderlich; in paketvermittelten Netzwerken nehmen Daten nicht immer denselben Weg durch das Netzwerk.

   **#INTER**
   Eine Serviceklasse, die auf interaktive Kommunikation abgestimmt ist.

   **#INTERSC**
   Entspricht #INTER, jedoch ist mindestens die Datenübertragungssicherheit eines Netzwerks mit Paketvermittlung erforderlich.

   Erstellen Sie weitere Serviceklassenbeschreibungen mit dem Befehl zum Erstellen von Serviceklassen (CRTCOSD).

5. Erstellen Sie eine Modusbeschreibung.

   Die Modusbeschreibung gibt die Kenndaten der Sitzung an sowie die Anzahl Sitzungen, die zum Vereinbaren der zulässigen Werte zwischen dem lokalen und dem fernen Standort verwendet werden können. Die Modusbeschreibung verweist außerdem auf die Serviceklasse, die für den Datenaustausch verwendet wird. Im Lieferumfang des Systems sind mehrere vordefinierte Modi enthalten:

   **BLANK**
   Der werkseitig in den Netzwerkattributen angegebene Standardmodusname

   **#BATCH**
   Ein auf Stapeljobs abgestimmter Modus

   **#BATCHSC**
   Entspricht #BATCH, jedoch erfordert die zugeordnete Serviceklassenbeschreibung mindestens die Datenübertragungssicherheit eines Netzwerks mit Paketvermittlung

**#INTER**
Ein auf interaktive Kommunikation abgestimmter Modus

**#INTERSC**
Entspricht #INTER, jedoch erfordert die zugeordnete Serviceklassenbeschreibung mindestens die Datenübertragungssicherheit eines Netzwerks mit Paketvermittlung

**IBMRDB**
Ein auf DRDA-Kommunikation abgestimmter Modus

Weitere Modusbeschreibungen können mit dem Befehl zum Erstellen von Modusbeschreibungen (CRTMODD) erstellt werden.

6. Erstellen Sie Einheitenbeschreibungen.

   Die Einheitenbeschreibung gibt die Kenndaten der logischen Verbindung zwischen dem lokalen und dem fernen System an. Sie müssen Einheitenbeschreibungen nicht manuell erstellen, wenn das System IBM AS/400 in Verbindung mit einem Host-System mit APPN und als unabhängige logische Einheit (LU) ausgeführt wird. Das System IBM AS/400 erstellt automatisch die Einheitenbeschreibung und ordnet sie der entsprechenden Steuereinheitenbeschreibung zu, wenn die Sitzung eingerichtet wird. Wenn das System IBM AS/400 eine abhängige LU ist, müssen Sie die Einheitenbeschreibungen mit dem Befehl zum Erstellen von Einheitenbeschreibungen (CRTDEVAPPC) manuell erstellen. Geben Sie in der Einheitenbeschreibung `APPN(*YES)` an, um anzuzeigen, daß APPN verwendet wird.

7. Erstellen Sie APPN-Standortlisten.

   Wenn zusätzliche lokale Standorte (in anderen Systemen als *LUs* bezeichnet) oder spezielle Kenndaten für ferne Standorte für APPN erforderlich sind, müssen Sie APPN-Standortlisten erstellen. Der Name des lokalen Standorts ist der in den Netzwerkattributen angegebene Steuerpunktname. Wenn Sie zusätzliche Standorte für das System IBM AS/400 benötigen, ist eine Liste lokaler APPN-Standorte erforderlich. Ein Beispiel für einen fernen Standort mit speziellen Kenndaten liegt vor, wenn der ferne Standort sich in einem anderen Netzwerk befindet als der lokale Standort. Unter diesen Bedingungen ist eine Liste ferner APPN-Standorte erforderlich. Erstellen Sie APPN-Standortlisten mit dem Befehl zum Erstellen von Konfigurationslisten (CRTCFGL).

8. Aktivieren Sie die Kommunikation (vary on).

   Zum Aktivieren der Beschreibungen für die Kommunikation können Sie den Befehl zum An-/Abhängen der Konfiguration (VRYCFG) oder den Befehl zum Arbeiten mit dem Konfigurationsstatus (WRKCFGSTS) verwenden. Wenn die Leitungsbeschreibungen aktiviert sind, sind die mit

dieser Leitung verbundenen Steuereinheiten und Einheiten ebenfalls aktiviert. Mit dem Befehl WRKCFGSTS kann außerdem der Status jeder Verbindung angezeigt werden.

9. RU-Größe und Nachrichtendosierung.

   RU-Größe und Nachrichtendosierung werden durch Werte gesteuert, die in der Modusbeschreibung angegeben sind. Wenn Sie die Modusbeschreibung erstellen, werden Standardwerte für die RU-Größe und Nachrichtendosierung bereitgestellt. Die Standardwerte sind ein AS/400-Schätzwert für die meisten Umgebungen (einschließlich einer verteilten Datenbank). Wenn für die RU-Größe der Standardwert übernommen wird, schätzt das System IBM AS/400 den besten Wert ab. Wenn das System IBM AS/400 mit einem anderen System kommuniziert, das angepaßte Nachrichtendosierung unterstützt, sind die angegebenen Nachrichtendosierungswerte nur vorläufige Anfangswerte. Die Nachrichtendosierung wird von jedem System entsprechend seiner Fähigkeiten zum Verarbeiten der empfangenen Daten angepaßt. Für Systeme, die keine angepaßte Nachrichtendosierung unterstützen, werden die Nachrichtendosierungswerte zu Beginn der Sitzung festgelegt und bleiben für die Dauer der Sitzung unverändert. Weitere Informationen finden Sie in *OS/400 Communications Configuration*.

**Anmerkungen:**

1. Die Steuereinheitenbeschreibung entspricht den NCP/VTAM-PU-Makros (IBM Network Control Program/Virtual Telecommunications Access Method Physical Unit Macros).
2. Die Einheitenbeschreibung entspricht dem NCP/VTAM-LU-Makro. Die Einheitenbeschreibung enthält ähnliche Informationen wie die, die im Partner-LU-Profil von Communications Manager Version 2 1.1 gespeichert sind.
3. Die Modusbeschreibung entspricht den NCP/VTAM-Modustabellen und dem Übertragungsservice-Modusprofil von Communications Manager.

Weitere Informationen zum Konfigurieren der Netzwerkunterstützung und zum Arbeiten mit Standortlisten finden Sie in den Handbüchern *OS/400 Communications Configuration* und *APPN Support*. Beispiele zur Verwendung von CL-Befehlen zum Definieren von Systemkonfigurationen finden Sie im Handbuch *AS/400 Distributed Database Programming*.

## Gewährleisten der Sicherheit

Wenn ein fernes System die Verarbeitung verteilter Datenbanken im Auftrag einer SQL-Anwendung ausführt, muß es in der Lage sein, die Sicherheitsanforderungen des Anwendungs-Requesters, des Anwendungs-Servers und des verwendeten Netzwerks zu erfüllen. Diese Anforderungen betreffen mindestens einen der folgenden Bereiche:

- Auswählen von Endbenutzernamen
- Sicherheitsparameter des Netzwerks

- Sicherheit des Datenbankmanagers
- Vom AS/400-Sicherheitssystem implementierte Sicherheit

### Auswählen von Endbenutzernamen

Auf Systemen IBM AS/400 wird Endbenutzern eine Benutzer-ID mit 1 bis 10 Zeichen zugeordnet, die zwar im betreffenden System, jedoch nicht unbedingt im gesamten Netzwerk eindeutig ist. Diese Benutzer-ID wird an das ferne System übermittelt, wenn die Verbindung zwischen zwei Datenbanken hergestellt wird. Zur Vermeidung von Konflikten zwischen Benutzer-IDs auf Systemen im Netzwerk wird häufig eine Namensumsetzung für abgehende Anforderungen zum Ändern der Benutzer-ID durchgeführt. Dadurch werden Konflikte gelöst, bevor die Benutzer-IDs über das Netzwerk gesendet werden. Das System IBM AS/400 stellt jedoch keine Namensumsetzung für abgehende Anforderungen zur Behebung potentieller Konflikte auf dem Server zur Verfügung. Diese Konflikte müssen auf dem Anwendungs-Server behoben werden, sofern Sie nicht die zusätzlichen Klauseln USER und USING in der AS/400-SQL-Anweisung CONNECT verwenden. USER gibt eine gültige ID auf dem Anwendungs-Server und USING das entsprechende Kennwort für den Benutzer an.

### Netzwerksicherheit

Nachdem der Anwendungs-Requester die Endbenutzernamen für die ferne Anwendung ausgewählt hat, muß er die erforderlichen LU 6.2-Sicherheitsinformationen für das Netzwerk bereitstellen. LU 6.2 stellt die folgenden drei Hauptsicherheitseinrichtungen für das Netzwerk zur Verfügung:

- Sicherheit auf Sitzungsebene, gesteuert durch das Schlüsselwort LOCPWD im Befehl CRTDEVAPPC
- Sicherheit auf Dialogebene, gesteuert durch das Betriebssystem OS/400
- Verschlüsselung (vom Betriebssystem OS/400 nicht unterstützt)

Sicherheit auf Sitzungsebene wird durch die LU-LU-Prüfung bereitgestellt. Jede LU verfügt über einen Schlüssel, der mit dem Schlüssel der fernen LU übereinstimmen muß. Den Schlüssel legen Sie mit dem Schlüsselwort LOCPWD im Befehl CRTDEVAPPC fest.

Der Anwendungs-Server ist zuständig für die Verwaltung der Datenbankressourcen und legt deshalb auch fest, welche Netzwerksicherheitseinrichtungen seitens des Anwendungs-Requesters erforderlich sind. Der AS/400-Sicherheitsadministrator muß sicherstellen, daß kein Anwendungs-Server höhere Sicherheitsanforderungen stellt als vom AS/400-Anwendungs-Requester unterstützt werden.

Die folgenden Optionen für SNA-Dialogsicherheit sind möglich:

**SECURITY=SAME**

Auch als bereits geprüfte Sicherheit bezeichnet. Nur die Benutzer-ID eines Anwendungsbenutzers wird zum fernen System gesendet. Es wird kein Kennwort übermittelt. Vor AS/400 Version 2 Release 2 Modifikationsstufe 0 wurde nur diese Stufe der Dialogsicherheit von AS/400-Anwendungs-Requestern unterstützt.

**SECURITY=PGM**

Benutzer-ID und Kennwort des Anwendungsbenutzers werden zur Gültigkeitsprüfung an das ferne System gesendet. Vor AS/400 Version 2 Release 2 Modifikationsstufe 0 wurde diese Sicherheitsoption von AS/400-Anwendungs-Requestern nicht unterstützt.

**SECURITY=NONE**

Wird nicht unterstützt, wenn das System IBM AS/400 als Anwendungs-Requester fungiert.

### Sicherheit des Datenbankmanagers

Das System IBM AS/400 verfügt nicht über ein externes Sicherheitssubsystem. Alle Sicherheitseinrichtungen werden vom Betriebssystem OS/400 implementiert, wie es im folgenden Abschnitt „Systemsicherheit" beschrieben wird.

### Systemsicherheit

Das Betriebssystem OS/400 steuert die Vergabe von Berechtigungen für alle Objekte im System, einschließlich Programmen, Paketen, Tabellen, Sichten und Objektgruppen.

Der Anwendungs-Requester steuert die Vergabe von Berechtigungen für Objekte, die sich auf dem Anwendungs-Requester befinden. Die Sicherheit für Objekte auf dem Anwendungs-Server wird vom Anwendungs-Server gemäß der vom Anwendungs-Requester übermittelten Benutzer-ID gesteuert. Die an den Anwendungs-Server übermittelte Benutzer-ID wird dem Benutzer des AS/400-Anwendungs-Requesters oder der in der Klausel USER der AS/400-SQL-Anweisung CONNECT angegebenen Benutzer-ID zugeordnet. Beispiel: CONNECT TO rdbname USER benutzer-ID USING kennwort

Die Objektsicherheit kann mit Hilfe der CL-Befehle für Objektberechtigung oder mit den SQL-Anweisungen GRANT und REVOKE verwaltet werden. Zu den CL-Befehlen für Objektberechtigungen gehören der Befehl zum Erteilen von Objektberechtigungen (GRTOBJAUT) und der Befehl zum Entziehen von Objektberechtigungen (RVKOBJAUT). Diese Befehle gelten für jedes Objekt auf dem System. Die Anweisungen GRANT und REVOKE gelten nur für SQL-Objekte (Tabellen, Sichten und Pakete). Verwenden Sie zum Ändern der Berechtigungen für andere Objekte (z. B. Programme und Objektgruppen) die Befehle GRTOBJAUT und RVKOBJAUT.

**Erteilen und Entziehen von Berechtigungen:** Geben Sie auf einem System IBM AS/400 den folgenden Befehl ein, um dem Benutzer USER1 die Berechtigung *USE für das Programm PGMA zu erteilen:

```
GRTOBJAUT OBJ(PGMA) OBJTYPE(*PGM) USER(USER1) AUT(*USE)
```

Der Befehl zum Entziehen dieser Berechtigung lautet:

```
RVKOBJAUT OBJ(PGMA) OBJTYPE(*PGM) USER(USER1) AUT(*USE)
```

*PGM gibt in diesem Beispiel die Objektart Programm an. *SQLPKG steht für ein Paket, *LIB für eine Objektgruppe und *FILE für eine Tabelle.

Darüber hinaus können GRTOBJAUT und RVKOBJAUT verwendet werden, um zu verhindern, daß Benutzer Programme und Pakete erstellen. Wenn die Berechtigung für einen der Befehle CRTSQLxxx (mit xxx = RPG, C, CBL, FTN oder PLI) entzogen wird, kann der Benutzer keine Programme erstellen. Wird die Berechtigung für den Befehl CRTSQLPKG entzogen, kann der Benutzer weder vom Anwendungs-Requester aus noch auf dem Anwendungs-Server Pakete erstellen.

Geben Sie beispielsweise den folgenden Befehl ein, um auf einem System IBM AS/400 dem Benutzer USER1 die Berechtigung *USE für den Befehl CRTSQLPKG zu erteilen:

```
GRTOBJAUT OBJ(CRTSQLPKG) OBJTYPE(*CMD) USER(USER1) AUT(*USE)
```

Dies betrifft die Ausführung des Befehls CRTSQLPKG auf dem Anwendungs-Requester. Auf dem Anwendungs-Server ermöglicht dieser Befehl das Erstellen von Paketen.

Der Befehl zum Entziehen dieser Berechtigung lautet:

```
RVKOBJAUT OBJ(CRTSQLPKG) OBJTYPE(*CMD) USER(USER1) AUT(*USE)
```

**Vergeben der Standardberechtigung:** Bei der Erstellung von Objekten wird eine Standardberechtigung vergeben. Der Ersteller einer Tabelle, einer Sicht oder eines Programms erhält standardmäßig sämtliche Berechtigungen für die von ihm erstellten Objekte. Außerdem erhält PUBLIC für diese Objekte dieselbe Berechtigung, die PUBLIC für die Bibliothek oder Objektgruppe dieser Objekte hat.

Weitere Informationen zur Systemsicherheit finden Sie im Handbuch *AS/400 Security - Reference*.

## Darstellen von Daten

Produkte mit Unterstützung für DRDA führen alle erforderlichen Umwandlungen auf dem empfangenden System automatisch aus. Damit dies möglich ist, muß der CCSID-Wert des Anwendungs-Requesters ein Wert sein, der vom Empfangssystem für die Umwandlung unterstützt wird.

Auf einem Anwendungs-Requester sollten Sie besonders auf die CCSID (Coded Character Set ID - ID für codierten Zeichensatz) achten, die folgenden Objekten zugeordnet ist:

- Anfordernder Job

  Die OS/400-Arbeitsverwaltungsunterstützung (Work Management Support) initialisiert die Job-CCSID mit dem CCSID-Wert im Benutzerprofil. Wenn der CCSID-Wert im Benutzerprofil *SYSVAL ist, fragt die Arbeitsverwaltungsunterstützung die CCSID aus dem Systemwert QCCSID ab. Der Systemwert QCCSID ist anfangs auf CCSID 65535 eingestellt. Wenn 65535 für die CCSID von Jobs verwendet wird, über die von DB2 Universal Database Verbindungen hergestellt werden sollen, scheitern diese Verbindungsversuche. Da die Änderung des Systemwerts QCCSID Auswirkungen auf das gesamte System hat, wird empfohlen, die CCSID des Benutzerprofils für den Job zu ändern, mit dem der Server-Job ausgeführt wird. Legen Sie die CCSID des Benutzerprofils für den Job auf einen geeigneten Wert fest. Verwenden Sie beispielsweise CCSID 37 für amerikanisches Englisch. In der Regel sollte die Standard-CCSID für das System IBM AS/400 gewählt werden, zu dem Verbindung hergestellt werden soll.

  Die Job-CCSID kann mit dem Befehl zum Ändern des Jobs (CHGJOB) geändert werden. Oder verwenden Sie für nachfolgende Jobs den Befehl zum Ändern des Benutzerprofils (CHGUSRPRF), um den CCSID-Wert des Benutzerprofils zu ändern. Mit dem Befehl zum Abrufen der Jobattribute (RTVJOBA) können Sie feststellen, welche CCSID für einen Job in einem CL-Programm gilt. Verwenden Sie bei der interaktiven Verarbeitung den Befehl zum Arbeiten mit einem Job (WRKJOB), und wählen Sie in der dazugehörigen Anzeige MIT JOB ARBEITEN die Option 2 (Jobdefinitionsattribute anzeigen) aus.

- Physische Datenbankdateien

  Physische Datenbankdateien verwenden bei der Dateierstellung standardmäßig die Standard-Job-CCSID (die von der Job-CCSID abweichen kann), wenn im Befehl zum Erstellen einer physischen Datei (CRTPF) oder im Befehl zum Erstellen einer physischen Quellendatei (CRTSRCPF) keine CCSID explizit angegeben ist. Vor DB2 für AS/400 Version 3 Release 1 war der Standardwert die Job-CCSID, die häufig 65535 und für DRDA-Verwendung ungeeignet war. Die Standard-Job-CCSID ist nie 65535 und eignet sich daher besser für die CCSID physischer Dateien, auf die über DRDA zugegriffen wird.

  Mit dem Befehl zum Anzeigen der Dateibeschreibung (DSPFD) können Sie die CCSID einer Datei und mit dem Befehl zum Anzeigen der Dateifeldbeschreibung (DSPFFD) die CCSID der Felder einer Datei abrufen.

  Ändern Sie die CCSID einer physischen Datei mit dem Befehl zum Ändern der physischen Datei (CHGPF). Eine physische Datei kann nicht in jedem Fall geändert werden, wenn mindestens eine der folgenden Bedingungen zutrifft:

- Logische Dateien wurden über die physische Datei definiert. In diesem Fall müssen Sie eventuell folgende Schritte ausführen:
  1. Sichern Sie die logischen und die physischen Dateien zusammen mit ihren Zugriffspfaden.
  2. Drucken Sie eine Liste der Berechtigungen für logische Dateien (DSPOBJAUT).
  3. Löschen Sie die logischen Dateien.
  4. Ändern Sie die physischen Dateien.
  5. Stellen Sie die physischen und die logischen Dateien mit ihren Zugriffspfaden mit Hilfe der geänderten physischen Dateien wieder her.
  6. Erteilen Sie die persönliche Berechtigung für die logischen Dateien (siehe hierzu die gedruckte Liste).
- Dateien oder Feldern wurde explizit ein CCSID-Wert zugeordnet. Erstellen Sie zum Ändern einer physischen Datei mit auf Feldebene zugeordneter CCSID die physische Datei erneut, und kopieren Sie die Daten mit dem Parameter FMTOPT(*MAP) des Befehls zum Kopieren einer Datei (CPYF) in die neue Datei.
- Satzformate werden in einer älteren Version von OS/400 als Version 3 Release 1 gemeinsam benutzt.

## Konfigurieren des Anwendungs-Servers

Die Anwendungs-Server-Unterstützung des Systems IBM AS/400 ermöglicht die Verwendung des Systems IBM AS/400 als Server für DRDA-Anwendungs-Requester. Der Anwendungs-Requester, der mit einem Anwendungs-Server unter DB2 Universal Database für AS/400 verbunden ist, kann ein beliebiger Client sein, der DRDA-Protokolle unterstützt.

Der Anwendungs-Requester kann auf Tabellen zugreifen, die lokal auf dem Anwendungs-Requester unter DB2 Universal Database für AS/400 gespeichert sind. Damit SQL-Anweisungen ausgeführt werden können, muß der Anwendungs-Requester zuvor ein Paket auf dem Anwendungs-Server unter DB2 Universal Database für AS/400 erstellen. Der Anwendungs-Server unter DB2 Universal Database für AS/400 verwendet das Paket mit den SQL-Anweisungen der Anwendung bei der Programmausführung.

### Bereitstellen von Netzwerkinformationen

Zur Verarbeitung von Anforderungen für verteilte Datenbanken auf dem AS/400-Anwendungs-Server müssen Sie die Anwendungs-Server-Datenbank im Verzeichnis RDB benennen. Für SNA-Kommunikation müssen Sie das Anwendungs-Server-System definieren und die Größe und Nachrichtendosierung für Anforderungs- und Antworteinheiten einstellen. Informationen zu TCP/IP-Kommunikation, die von DB2 Universal Database für AS/400 Version

4.2 unterstützt wird, finden Sie in „Kapitel 4. Verbinden von DB2 Universal Database für AS/400 in einem DRDA-Netzwerk über TCP/IP” auf Seite 121.

#### Benennen der Anwendungs-Server-Datenbank

Das Benennen der Anwendungs-Server-Datenbank (am Standort des Anwendungs-Servers) erfolgt auf die gleiche Weise wie das Identifizieren der Anwendungs-Requester-Datenbank (am Standort des Anwendungs-Requesters). Verwenden Sie dazu den Befehl zum Hinzufügen eines Eintrags im Verzeichnis relationaler Datenbanken (ADDRDBDIRE), und geben Sie als fernen Standort *LOCAL an.

#### Definieren des Anwendungs-Servers im Netzwerk

Beim Zugriff über SNA ist das Definieren des Anwendungs-Servers im Netzwerk identisch mit dem Definieren des Anwendungs-Requesters im Netzwerk. Sie müssen Leitungs-, Steuereinheiten-, Einheiten- und Modusbeschreibungen erstellen, um sowohl den Anwendungs-Server als auch den Anwendungs-Requester, der die Anforderungen sendet, zu definieren. Informationen zum Definieren des Anwendungs-Servers im Netzwerk finden Sie in den Abschnitten „Definieren des lokalen Systems für DB2 Universal Database für AS/400” auf Seite 102 und „Definieren des fernen Systems für DB2 Universal Database für AS/400” auf Seite 103. Siehe auch das Handbuch *AS/400 Distributed Database Programming*.

Als Transaktionsprogrammname zum Starten einer AS/400-Anwendungs-Server-Datenbank wird der DRDA-Standardwert X'07F6C4C2' verwendet. Dieser Transaktionsprogrammname ist innerhalb des Systems IBM AS/400 zum Starten des Anwendungs-Servers definiert. Wenn TCP/IP von DB2/400 unterstützt wird, ist der entsprechende Parameter für TCP/IP-Verbindungen der Anschluß. DB2/400 verwendet immer den herkömmlichen DRDA-Anschluß 446 als Server.

#### Einstellen von RU-Größe und Nachrichtendosierung

Die Netzwerkdefinitionen müssen überprüft werden, um festzustellen, ob das Netzwerk mit verteilten Datenbanken Auswirkungen auf das vorhandene Netzwerk hat. Dabei gelten für Anwendungs-Server und Anwendungs-Requester dieselben Überlegungen.

### Gewährleisten der Sicherheit

Wenn ein Anwendungs-Requester eine Anforderung für verteilte Datenbanken an den AS/400-Anwendungs-Server weiterleitet, kann die Sicherheit in folgenden Bereichen eine Rolle spielen:

- Auswählen von Endbenutzernamen
- Sicherheitsparameter des Netzwerks
- Sicherheit des Datenbankmanagers
- Sicherheit des Systems IBM AS/400

### Auswählen von Endbenutzernamen

Der Anwendungs-Requester sendet eine Benutzer-ID zur Sicherheitsüberprüfung an den Anwendungs-Server. Der auf dem AS/400-Anwendungs-Server ausgeführte Job verwendet diese Benutzer-ID oder in einigen Fällen eine Standard-Benutzer-ID.

Der AS/400-Anwendungs-Server stellt keine Umsetzung von Benutzer-IDs für eingehende Anforderungen zur Behebung von Konflikten zwischen Benutzer-IDs zur Verfügung, die nicht eindeutig sind, und gruppiert auch nicht mehrere Benutzer unter einer einzigen Benutzer-ID. Jede von einem Anwendungs-Requester gesendete Benutzer-ID muß auf dem Anwendungs-Server vorhanden sein. Ein Verfahren zur Gruppierung eingehender Anforderungen unter einer einzigen Benutzer-ID (mit gewissen Sicherheitseinbußen) ist das Angeben einer Standard-Benutzer-ID in einem Kommunikationseintrag des Subsystems, das die Startanforderungen für ferne Jobs verarbeitet. Informationen hierzu finden Sie in den Beschreibungen der Befehle ADDCMNE und CHGCMNE im Handbuch *AS/400 CL Reference*.

### SNA-Netzwerksicherheit

LU 6.2 stellt die folgenden drei Hauptsicherheitseinrichtungen für das Netzwerk zur Verfügung:

- Sicherheit auf Sitzungsebene
- Sicherheit auf Dialogebene
- Verschlüsselung (vom System IBM AS/400 nicht unterstützt)

Der Anwendungs-Server unter DB2 Universal Database für AS/400 verwendet die Sicherheit auf Sitzungsebene in derselben Weise wie der Anwendungs-Requester unter DB2 Universal Database für AS/400.

Der Anwendungs-Server steuert die für den Datenaustausch verwendeten SNA-Dialogebenen. Der Parameter SECURELOC in der APPC-Einheitenbeschreibung und der Standortschutzwert in der Liste ferner APPN-Standorte legen fest, was vom Anwendungs-Requester für den Datenaustausch akzeptiert wird.

Die folgenden Optionen für SNA-Dialogsicherheit sind möglich:

**SECURITY=SAME**

Auch als bereits geprüfte Sicherheit bezeichnet. Nur die Benutzer-ID des Anwendungsbenutzers ist für den Anwendungs-Server erforderlich. Es wird kein Kennwort übermittelt. Aktivieren Sie diese Stufe der Dialogsicherheit auf dem Anwendungs-Server durch Einstellen des Parameters SECURELOC in der APPC-Einheitenbeschreibung auf *YES oder durch Einstellen des Standortschutzwerts in der Liste ferner APPN-Standorte auf *YES.

**SECURITY=PGM**

Bewirkt, daß sowohl Benutzer-ID als auch Kennwort für den Anwendungs-Server zur Gültigkeitsprüfung erforderlich sind. Aktivieren Sie diese Stufe der Dialogsicherheit auf dem Anwendungs-Server, indem Sie die standardmäßige Benutzer-ID im Kommunikationseintrag des AS/400-Subsystems auf *NONE (keine standardmäßige Benutzer-ID) und den Parameter SECURELOC oder den Wert für den Standortschutz auf *NO einstellen.

**SECURITY=NONE**

Ein Anwendungs-Server erwartet keine Benutzer-ID und kein Kennwort. Der Datenaustausch wird durch ein Standardbenutzerprofil auf dem Anwendungs-Server zugelassen. Aktivieren Sie diese Option durch Angeben eines Standardbenutzerprofils im Kommunikationsverzeichnis des Subsystems und durch Angeben von *NO für den Parameter SECURELOC oder den Standortschutzwert.

Für SNA/DS (SNA Distribution Services) ist eine Standardbenutzer-ID erforderlich. Deshalb sollte SNA/DS für den Normalfall (d. h. wenn keine Standardbenutzer-ID für DRDA-Anwendungen erwünscht ist) über ein eigenes Subsystem verfügen.

Auf eine Methode zur Gruppierung eingehender Jobstartanforderungen unter einer einzigen Benutzer-ID wurde bereits im Abschnitt „Auswählen von Endbenutzernamen" auf Seite 115 hingewiesen. Bei dieser Methode wird die vom Anwendungs-Requester gesendete Benutzer-ID nicht überprüft. Der Job auf dem Anwendungs-Server wird mit einer Standardbenutzer-ID gestartet, und der Benutzer, der die Verbindung vom Anwendungs-Server eingeleitet hat, erhält auch dann eine Zugriffsberechtigung für den Anwendungs-Server, wenn die übermittelte Benutzer-ID nur über eingeschränkte Berechtigungen verfügt. Dies erfolgt, indem der Anwendungs-Server als nicht geschützter Standort definiert, im Kommunikationseintrag des AS/400-Subsystems eine Standardbenutzer-ID angegeben und der Anwendungs-Requester so konfiguriert wird, daß bei der Herstellung der Verbindung nur eine Benutzer-ID gesendet wird. Wird ein Kennwort gesendet, wird die dazugehörige Benutzer-ID anstelle der Standardbenutzer-ID verwendet.

Die Kommunikationseinträge des AS/400-Subsystems unterscheiden sich durch die zum Starten des Datenaustauschs verwendeten Einheiten- und Modusnamen. Durch Zuordnen unterschiedlicher Standardbenutzer-IDs zu verschiedenen Einheit/Modus-Paaren können Benutzer nach der Art ihrer Kommunikation mit dem Anwendungs-Server gruppiert werden.

Das System IBM AS/400 stellt außerdem eine Netzwerksicherheitseinrichtung zur Verfügung, die nur für die Verwaltung verteilter Datenbanken und verteilter Dateien verwendet wird. Ein Netzwerkattribut für diese Arten von

Systemzugriff weist entweder alle Zugriffsversuche zurück oder bewirkt, daß die Sicherheit vom System auf der Grundlage einzelner Objekte gesteuert wird.

### TCP/IP-Netzwerksicherheit

In DB2 Universal Database für AS/400 Version 4.2 gibt es einen neuen Befehl namens CRTDDMTCPA. Damit können Sie angeben, daß ein Server TCP/IP-Verbindungsanforderungen ohne Kennwort akzeptieren soll.

### Sicherheit des Datenbankmanagers

Alle Sicherheitseinrichtungen werden von der OS/400-Sicherheitsfunktion gesteuert.

### Systemsicherheit

Das System IBM AS/400 verfügt nicht über ein externes Sicherheitssubsystem. Alle Sicherheitseinrichtungen werden von der OS/400-Sicherheitsfunktion gesteuert, die integraler Bestandteil des Betriebssystems ist. Das Betriebssystem steuert die Vergabe von Berechtigungen für alle Objekte im System, einschließlich Programmen, Paketen, Tabellen, Sichten und Objektgruppen.

Der Anwendungs-Server steuert die Vergabe von Berechtigungen für die Objekte, die sich auf dem Anwendungs-Server befinden. Die Sicherheitssteuerung für diese Objekte richtet sich danach, von welcher Benutzer-ID der Anwendungs-Server-Job gestartet wird. Diese Benutzer-ID wird wie im Abschnitt „Auswählen von Endbenutzernamen” auf Seite 115 beschrieben ermittelt.

Die Objektsicherheit kann mit Hilfe der CL-Befehle für Objektberechtigung oder mit den SQL-Anweisungen GRANT und REVOKE verwaltet werden. Zu den CL-Befehlen für Objektberechtigungen gehören der Befehl zum Erteilen von Objektberechtigungen (GRTOBJAUT) und der Befehl zum Entziehen von Objektberechtigungen (RVKOBJAUT). Diese CL-Befehle gelten für jedes Objekt auf dem System. Die Anweisungen GRANT und REVOKE gelten nur für SQL-Objekte (Tabellen, Sichten und Pakete). Verwenden Sie zum Ändern der Berechtigungen für andere Objekte (z. B. Programme und Objektgruppen) die Befehle GRTOBJAUT und RVKOBJAUT.

Bei der Erstellung von Objekten im System wird eine Standardberechtigung vergeben. Die Benutzer-ID, von der Tabellen, Sichten und Pakete erstellt werden, erhält sämtliche Berechtigungen. Alle anderen Benutzer-IDs (die Öffentlichkeit (PUBLIC)) erhalten dieselben Berechtigungen, die sie auch für die Objektgruppe oder Bibliothek haben, in der das betreffende Objekt erstellt wird.

Die Berechtigungen für Objekte, auf die innerhalb des Pakets durch statische oder dynamische Anweisungen verwiesen wird, werden zur Laufzeit des

Pakets überprüft. Wenn der Ersteller des Pakets keine Berechtigung für das Objekt hat, auf das verwiesen wird, werden bei der Erstellung des Pakets entsprechende Warnungen zurückgegeben. Zur Ausführungszeit erhält der Benutzer, von dem das Paket ausgeführt wird, die Berechtigung des Paketerstellers. Wenn der Ersteller des Pakets Zugriffsberechtigung für eine Tabelle hat, der ausführende Benutzer jedoch nicht über diese Berechtigung verfügt, erhält der Benutzer automatisch die Berechtigungen des Paketerstellers, d. h. er kann nun ebenfalls auf die Tabelle zugreifen.

Weitere Informationen zur Systemsicherheit finden Sie im Handbuch *AS/400 Security - Reference*.

## Darstellen von Daten

Produkte mit DRDA-Unterstützung führen alle erforderlichen Umwandlungen auf dem Anwendungs-Server automatisch aus. Damit dies möglich wird, muß der CCSID-Wert (Coded Character Set ID - ID für codierten Zeichensatz) des Anwendungs-Servers ein Wert sein, der vom Anwendungs-Requester für die Umwandlung unterstützt wird.

Auf einem Anwendungs-Server sollten Sie besonders auf die CCSID achten, die folgenden Bereichen zugeordnet ist:

- Service-Job im Kommunikationssubsystem

  Die CCSID Ihres Service-Jobs muß mit dem Anwendungs-Requester kompatibel sein. Diese CCSID wird durch das Benutzerprofil der Benutzer-ID festgelegt, von der die Verbindung angefordert wird. Die OS/400-Arbeitsverwaltungsunterstützung (Work Management Support) initialisiert die Job-CCSID für die CCSID im Benutzerprofil. Wenn im Benutzerprofil keine CCSID vorhanden ist, fragt die Arbeitsverwaltungsunterstützung die CCSID (QCCSID) aus dem Systemwert ab. Der Systemwert QCCSID ist anfangs auf CCSID 65535 eingestellt.

  Bevor Sie eine Anforderung an DB2 Universal Database für AS/400 einleiten, sollten Sie sich anmelden und mit dem Befehl zum Ändern des Benutzerprofils (CHGUSRPRF) dem Benutzerprofil des Jobs, der die DRDA-Anforderungen verwaltet, einen zulässigen CCSID-Wert zuordnen.

- SQL-Objektgruppen

  Eine SQL-Objektgruppe besteht aus einem OS/400-Bibliotheksobjekt, einem Journal, einem Journalempfänger und (wahlfrei) einem IDDU-Datenverzeichnis (IDDU Data Dictionary), wenn in der Anweisung CREATE COLLECTION die Klausel WITH DATA DICTIONARY angegeben wurde. Den physischen und logischen Dateien, die für einige dieser Objekte verwendet werden, wird standardmäßig die zur Zeit der Erstellung gültige Job-CCSID zugeordnet. Beim Abfragen des Datenverzeichnisses oder des Katalogs über einen Anwendungs-Requester, der den CCSID-Wert dieser Dateien nicht unterstützt, werden möglicherweise nicht darstellbare oder verzerrte Daten angezeigt. Oder der Anwendungs-Requester weist in einer

Nachricht darauf hin, daß der CCSID-Wert nicht unterstützt wird. Zur Behebung dieses Fehlers müssen Sie eine neue SQL-Objektgruppe mit einem CCSID-Wert erstellen, der für das andere System akzeptabel ist.

Die Job-CCSID kann mit dem Befehl zum Ändern des Jobs (CHGJOB) geändert werden. Oder verwenden Sie für nachfolgende Jobs den Befehl zum Ändern des Benutzerprofils (CHGUSRPRF), um den CCSID-Wert des Benutzerprofils zu ändern. Verwenden Sie in einem CL-Programm den Befehl zum Abrufen der Jobattribute (RTVJOBA), um die CCSID des aktuellen Jobs abzurufen. Verwenden Sie bei der interaktiven Verarbeitung den Befehl zum Arbeiten mit einem Job (WRKJOB), und wählen Sie in der dazugehörigen Anzeige MIT JOB ARBEITEN die Option 2 (Jobdefinitionsattribute anzeigen) aus.

- SQL-Tabellen und andere Dateien von DB2 Universal Database für AS/400, auf die über DRDA zugegriffen wird

  Eine SQL-Tabelle entspricht einer physischen Datei von DB2 Universal Database für AS/400 innerhalb einer Bibliothek mit demselben Namen wie Ihre Objektgruppe. Die Spalten einer Tabelle entsprechen ebenfalls den Felddefinitionen einer physischen Datei. Die CCSID-Werte für die Tabelle oder die Spalten der Tabelle sind möglicherweise nicht mit dem Anwendungs-Requester kompatibel. Informationen zum Ändern dieses Werts finden Sie in „Darstellen von Daten" auf Seite 111, wo das Ändern von physischen Datenbankdateien beschrieben wird. Eine Hauptursache für CCSID-Inkompatibilitäten in älteren OS/400-Versionen als Version 3 Release 1 lag darin, daß viele Dateien oder SQL-Tabellen standardmäßig mit der CCSID 65535 gekennzeichnet wurden. In Version 3 Release 1 und nachfolgenden Releases werden die CCSIDs dieser Dateien automatisch auf einen anderen, besser geeigneten Wert gesetzt.

# Kapitel 4. Verbinden von DB2 Universal Database für AS/400 in einem DRDA-Netzwerk über TCP/IP

In diesem Kapitel sind die im Handbuch *AS/400 Distributed Database Programming* enthaltenen Informationen zum Konfigurieren des Systems IBM AS/400 zusammengefaßt:

- Als DRDA-Anwendungs-Requester, der abgehende TCP/IP-Kommunikation verwendet
- Als DRDA-Anwendungs-Server, der eingehende TCP/IP-Kommunikation verwendet

Die Prinzipien entsprechen denjenigen, die in „Kapitel 3. Verbinden von DB2 Universal Database für AS/400 in einem DRDA-Netzwerk über SNA" auf Seite 101, beschrieben sind. Die Schritte zur Konfiguration der Kommunikation sind jedoch viel einfacher.

**Anmerkungen:**

1. Bei DRDA-Kommunikation über TCP/IP ist die Standardanschlußnummer für Datenbankverbindungen 446.
2. Die Implementierung von DB2 Universal Database für AS/400 Version 4 Release 2 unterstützt die zweiphasige Festschreibung (verteilte Arbeitseinheit) über TCP/IP-Kommunikation nicht.

## Zusammenfassung der Informationen zu DB2 Universal Database für AS/400

*AS/400 Distributed Database Programming* enthält die folgenden Abschnitte, die Sie lesen und als Referenzmaterial verwenden sollten:

- Chapter 1. Distributed Relational Database and the AS/400 System:
  - Distributed Relational Database Processing
  - DRDA and CDRA Support
- Chapter 3. Communications for an AS/400 Distributed Relational Database:
  - Configuring a Communications Network using TCP/IP
- Chapter 4. Security for an AS/400 Distributed Relational Database:
  - DRDA Security using TCP/IP
- Chapter 5. Setting Up an AS/400 Distributed Relational Database:
  - Work Management for DRDA Use with TCP/IP
  - Setting up the TCP/IP Server
- Chapter 6. Distributed Relational Database Administration and Operation Tasks:

  - Managing a TCP/IP Server
- Chapter 8. Distributed Relational Database Performance:
  - Factors that Affect Blocking for DRDA
- Chapter 9. Handling Distributed Relational Database Problems:
  - Handling Connection Request Failures for TCP/IP
  - Starting a Service Job for a TCP/IP Server
- Appendix B. Cross-Platform Access Using DRDA

Außerdem müssen Sie folgende Angaben kennen:

- TCP/IP-Anschlußnummer und Host-Name für den Server und den Requester
- ID für codierten Zeichensatz (CCSID) und Codepage für den Server und den Requester
- Beim Herstellen von Datenbankverbindungen die erforderliche Benutzer-ID und das erforderliche Kennwort

## Überlegungen zur Einrichtung und Verwendung des DRDA-TCP/IP-Servers unter DB2 Universal Database für AS/400

Beim Einrichten des DRDA-TCP/IP-Servers unter DB2 Universal Database für AS/400 müssen Sie sicherstellen, daß der Server gestartet wurde. Der CL-Befehl zum Starten des DRDA-Servers (auch als DDM-Server bekannt) lautet:

```
STRTCPSVR SERVER(*DDM)
```

Beim Starten des DRDA-Servers können Sie den Befehl zum Starten des TCP/IP-Servers (STRTCPSVR) auch ohne Parameter angeben oder *ALL für den Parameter SERVER angeben. Der DRDA-Server wird nach dem Absetzen des folgenden CL-Befehls beim Start von TCP/IP automatisch gestartet:

```
CHGDDMTCPA AUTOSTART(*YES)
```

Sie können prüfen, ob der Server gestartet wurde, indem Sie den folgenden CL-Befehl absetzen:

```
WRKUSRJOB USER(QUSER) STATUS(*ACTIVE)
```

Durch diesen Befehl wird eine Jobliste mit Blätterfunktion angezeigt. Wenn Sie ungefähr eine Seite vorblättern, werden zwei Zeilen mit den folgenden Informationen angezeigt:

```
__   QRWTLSTN    QUSER       BATCH    ACTIVE
__   QRWTSRVR    QUSER       PJ        ACTIVE
```

(Die Zeile QRWTSRVR kommt eventuell mehrfach vor, je nachdem, wie viele vorab gestartete Server-Jobs aktiv sind.)

Das Vorkommen der Zeile QRWTLSTN gibt an, daß der Job, der auf DRDA- und DDM-Verbindungsanforderungen wartet, aktiv ist. Dieser Job teilt dem bzw. den QRWTSRVR-Job(s) Arbeit zu, wenn Verbindungsanforderungen empfangen werden.

Sie können auch prüfen, ob der DRDA-Server gestartet wurde, indem Sie den Befehl STRTCPSVR SERVER(*DDM) absetzen und auf die Nachricht 'DDM TCP/IP Server ist bereits aktiv' warten.

Sie können den Namen des vorab gestarteten Jobs für eine bestimmte Verbindung durch Absetzen eines DSPLOG-Befehls abrufen, z. B.:

```
DSPLOG PERIOD(('15:55'))
```

Dabei muß die angegebene Zeit vor der Verbindungsherstellung liegen. Durch diesen Befehl wird eine Liste der Systemprotokolleinträge mit Blätterfunktion angezeigt. Suchen Sie nach einem Eintrag, der den Namen des Server-Jobs enthält, z. B.:

```
DDM Server-Job 039554/QUSER/QRWTSRVR wird für Benutzer SRR am 30.03.98
um 15:57:38 ausgeführt.
```

Mit diesem Jobnamen können Sie das Jobprotokoll weiterhin aktiver Jobs aufrufen. Damit können Sie zudem einen Wartungsjob für noch aktive Jobs zum Zweck der Fehlerbestimmung starten oder Nachrichten des Abfrageoptimierungsprogramms aufrufen. Beispiel eines CL-Befehls zum Starten eines Wartungsjobs unter Verwendung der obigen Informationen:

```
STRSRVJOB 039554/QUSER/QRWTSRVR
```

Führen Sie den Befehl STRDBG aus, um für den gewarteten Job den Fehlerbehebungsmodus zu aktivieren:

```
STRDBG UPDPROD(*YES)
```

In bestimmten Situationen sichert der DRDA-Server das Jobprotokoll des vorab gestarteten Jobs vor dem Neustart des Jobs und dem Löschen des Jobprotokolls. Dazu kommt es, wenn ein schwerwiegender Fehler entdeckt wurde oder wenn das Jobende während der Wartung (mit dem Befehl STRSRVJOB) erreicht wurde.

Setzen Sie den folgenden Befehl ab, um das gesicherte Jobprotokoll nach dem Jobende zu suchen:

```
WRKJOB benutzer-ID/QPRTJOB
```

Dabei ist benutzer-ID der Name der Benutzer-ID, unter der die Verbindung hergestellt wurde (im obigen Beispiel SRR).

Hierdurch wird eine Liste mit Jobs, aus der Sie einen Job auswählen können, oder ein Auswahlmenü für einen einzelnen Job angezeigt. Wählen Sie Option 4, 'Mit Spool-Dateien arbeiten', um das gesicherte Jobprotokoll zu suchen. Falls mehrere gespoolte Dateien vorhanden sind, handelt es sich um das Protokoll mit dem Dateinamen QPJOBLOG. Mit Option 5 können Sie die Jobprotokolldatei anzeigen.

Beispiel für die Art von Nachrichten des Abfrageoptimierungsprogramms in einem Server-Jobprotokoll beim Ausführen des Jobs während der Fehlerbehebung:

```
 CPI4329    Information   00    03/30/98   16:14:57   QQQIMPLE
          QSYS        3911     QSQOPEN      QSYS         09C4
Nachricht . . . :   Zugriff nach Eingangsfolge für Datei TBL2 verwendet.
Ursache . . . . :   Der Zugriffspfad nach Eingangsfolge wurde verwendet,
um Sätze aus Teildatei TBL2 der Datei TBL2 in Bibliothek SR auszuwählen.
Handelt es sich bei Datei TBL2 in Bibliothek SR um eine logische Datei,
ist Teildatei TBL2 der physischen Datei TBL2 in Bibliothek SR die tatsäch
liche Datei, aus der Sätze ausgewählt werden. Der Dateiname *N für die
Datei zeigt an, daß es sich um eine temporäte Datei handelt.
Fehlerbeseitigung . . . :   Die Verwendung eines Zugriffspfads kann die
Leistung der Abfrage verbessern, wenn Satzauswahl angegeben ist. Besteht
kein Zugriffspfad, empfiehlt es sich, einen Zugriffspfad zu erstellen,
dessen links angeordneten Schlüsselfelder mit einem der Felder in der
Satzauswahl übereinstimmen. Die Übereinstimmung weiterer Schlüsselfelder
im Zugriffspfad mit Feldern in der Satzauswahl führt zu einer höheren
Leistung. Normalerweise kann die erzwungene Verwendung eines bestehenden
Zugriffspfads erreicht werden, indem eine Sortierung nach Feldern angegeben
wird, die mit den links angeordneten Schlüsselfeldern dieses Zugriffspfads
übereinstimmen. Weitere Informationen enthält das Handbuch "DB2 for AS/400
SQL Programming", IBM form SC41-4612.
```

## Überlegungen zur Einrichtung des DRDA-TCP/IP-Clients unter DB2 Universal Database für AS/400

Als Hauptgrund für den Einsatz von DB2 Universal Database für AS/400 als DRDA-Anwendungs-Requester über TCP/IP spricht neben den im folgenden Abschnitt dargestellten Sicherheitsüberlegungen das Hinzufügen eines RDB-Verzeichniseintrags für den fernen Anwendungs-Server. Dies geschieht auf ähnliche Weise wie im vorherigen Kapitel zur Verwendung der SNA-Kommunikation beschrieben. Anstelle von APPC-Parametern wie dem fernen LU-Namen und dem Transaktionsprogrammnamen gibt es zwei TCP/IP-Parameter, und zwar der Name des fernen Hosts bzw. die IP-Adresse und die Anschlußnummer bzw. der Servicename. Das zweite Element des Parameters für den fernen Standort kann als *SNA (Standardwert) oder als *IP (Verbindung verwendet TCP/IP) angegeben werden.

## Sicherheitsüberlegungen zur Verwendung von DRDA über TCP/IP

DRDA über eigenständige TCP/IP-Verbindungen verwendet keine OS/400-Kommunikationssicherheitsservices und -konzepte wie Datenübertragungseinheiten, Modi, Standortschutzattribute und Dialogsicherheitsstufen, die der APPC-Kommunikation zugeordnet sind. Daher wird die Sicherheit für TCP/IP anders eingerichtet.

Von der aktuellen DB2/400-Implementierung von DRDA über TCP/IP werden zwei Typen von Sicherheitsmechanismen unterstützt:

1. nur Benutzer-ID
2. Benutzer-ID mit Kennwort

Bei einem Anwendungs-Server (AS) unter DB2 Universal Database für AS/400 wird als Standardsicherheitsmodus die Benutzer-ID mit Kennwort verwendet. Dies bedeutet, daß ankommende TCP/IP-Verbindungsanforderungen nach der Installation des Systems über ein Kennwort verfügen müssen, das zu der Benutzer-ID gehört, unter der der Server-Job ausgeführt werden soll. Mit dem Befehl CHGDDMTCPA können Sie angeben, daß das Kennwort nicht erforderlich ist. Nehmen Sie diese Änderung durch Eingabe von CHGDDMTCPA PWDRQD(*NO) vor. Sie müssen über die Sonderberechtigung *IOSYSCFG verfügen, um diesen Befehl verwenden zu können.

Bei einem Anwendungs-Requester (AR bzw. Client) unter DB2 Universal Database für AS/400 können Sie bei TCP/IP-Verbindungsanforderungen anhand von zwei Methoden ein Kennwort zusammen mit der Benutzer-ID senden. Wenn beide fehlen, wird nur die Benutzer-ID verwendet.

Die erste Methode ist das Senden eines Kennworts unter Verwendung des Formats USER/USING der SQL-Anweisung CONNECT. Die Syntax lautet wie folgt:

```
CONNECT TO rdbname USER benutzer-ID USING 'kennwort'
```

Dabei stellen die Wörter in Kleinbuchstaben die entsprechenden Verbindungsparameter dar. In einem Programm, das eingebettetes SQL verwendet, können die Werte für die Benutzer-ID und das Kennwort in Host-Variablen enthalten sein.

Die andere Methode zum Bereitstellen eines zu sendenden Kennworts bei einer Verbindungsanforderung über TCP/IP ist die Verwendung eines Server-Berechtigungseintrags. Jedem Benutzerprofil auf dem System ist eine Server-Berechtigungsliste zugeordnet. Die Liste ist standardmäßig leer, mit dem Befehl ADDSVRAUTE können jedoch Einträge hinzugefügt werden. Beim Versuch einer DRDA-Verbindung über TCP/IP überprüft DB2 Universal Database für AS/400 die Server-Berechtigungsliste auf das Benutzerprofil, unter dem der Client-Job ausgeführt wird.

Wenn eine Übereinstimmung zwischen dem RDB-Namen in der Anweisung CONNECT und dem SERVER-Namen in einem Berechtigungseintrag gefunden wird, wird der zugehörige Parameter USRID im Eintrag für die Verbindungsbenutzer-ID verwendet. Falls ein Parameter PASSWORD im Eintrag gespeichert ist, wird dieses Kennwort bei der Verbindungsanforderung ebenfalls gesendet.

Sie müssen den Systemwert QRETSVRSEC auf '1' setzen, um ein Kennwort mit dem Befehl ADDSVRAUTE speichern zu können. Der Standardwert ist '0'. Geben Sie den folgenden Befehl ein, um die Änderung auszuführen:

```
CHGSYSVAL QRETSVRSEC VALUE('1')
```

Die Syntax des Befehls ADDSVRAUTE lautet wie folgt:

```
ADDSVRAUTE USRPRF(benutzerprofil) SERVER(rdbname) USRID(benutzer-ID)
PASSWORD(kennwort)
```

Der Parameter USRPRF gibt das Benutzerprofil an, unter dem der Anwendungs-Requester-Job ausgeführt wird. Der Parameter SERVER gibt den Namen der fernen relationalen Datenbank an, und der Parameter USRID gibt das Benutzerprofil an, unter dem der Server-Job ausgeführt wird. Der Parameter PASSWORD gibt das Kennwort für das Benutzerprofil auf dem Server an.

**Anmerkung:** Es ist sehr wichtig, daß der RDB-Name im Parameter SERVER in Großbuchstaben angegeben wird.

Wenn der Parameter USRPRF ausgelassen wird, wird er standardmäßig auf das Benutzerprofil gesetzt, unter dem der Befehl ADDSVRAUTE ausgeführt wird. Wenn der Parameter USRID ausgelassen wird, nimmt er standardmäßig den Wert des Parameters USRPRF an. Wenn der Parameter PASSWORD ausgelassen wird bzw. wenn der Wert für QRETSVRSEC 0 ist, wird im Eintrag kein Kennwort gespeichert. In diesem Fall wird bei einem Verbindungsversuch mit Hilfe des Eintrags als Sicherheitsmechanismus nur die Benutzer-ID verwendet.

Ein Server-Berechtigungseintrag kann mit dem Befehl RMVSVRAUTE entfernt und mit dem Befehl CHGSVRAUTE geändert werden. Eine vollständige Beschreibung dieser Befehle finden Sie im Handbuch *AS/400 Command Reference.*

Wenn ein Server-Berechtigungseintrag für eine relationale Datenbank (RDB) vorhanden ist und zudem das Format USER/USING der Anweisung CONNECT verwendet wird, hat letzteres Vorrang.

# Kapitel 5. Zusätzliche Überlegungen zu DB2 Universal Database für AS/400 und DB2 Universal Database

In diesem Kapitel werden einige zusätzliche Überlegungen angestellt, die sich auf SQL-Operationen zwischen DB2 Universal Database für AS/400 und DB2 Server-Plattform Version 2 bzw. DB2 Universal Database beziehen. Außerdem werden Erläuterungen zu DB2 für OS/2 gegeben. In der Mehrzahl der Fälle gelten jedoch folgende ähnliche Überlegungen für DB2 Server-Plattform Version 2 und DB2 Universal Database auf anderen Plattformen:

1. Auf dem System IBM AS/400 werden Tabellennamen durch eine Objektgruppe (einen Bibliotheksnamen) qualifiziert und befinden sich in der Datenbank von DB2 Universal Database für AS/400 (eine Datenbank pro System IBM AS/400). Auf dem Personal Computer hingegen werden Tabellen durch eine Benutzer-ID (Ersteller der Tabelle) qualifiziert und befinden sich in einer bestimmten Datenbank (auf einem Personal Computer mit DB2 für OS/2 sind mehrere Datenbanken möglich).
   a. Eine Abfrage von DB2 für OS/2 (über DB2 Connect) an DB2 Universal Database für AS/400 verwendet also die Benutzer-ID des Jobs auf der Zielseite (auf dem System IBM AS/400) als (Standard-)Objektgruppennamen, wenn der Name der abgefragten Tabelle keine Objektgruppe enthält. Bedenken Sie diese Zuordnungen, ansonsten wird die Tabelle unter Umständen nicht gefunden.
   b. Dies bedeutet auch, daß eine Abfrage von DB2 Universal Database für AS/400 an DB2 für OS/2 ein impliziertes Abfragequalifikationsmerkmal hat, wenn es nicht in der Abfrage (in der Form 'qualifikationsmerkmal.tabellenname') angegeben ist. Das Tabellenqualifikationsmerkmal von DB2 für OS/2 (vom AS/400-Anwendungs-Requester als Objektgruppe oder Bibliothek angegeben) wird standardmäßig auf die Benutzer-ID des Benutzers gesetzt, der die Abfrage vornimmt. Bedenken Sie auch diese Zuordnungen, ansonsten findet die Abfrage unter Umständen die Tabelle nicht.
   c. Es wird empfohlen, die Datenbanken und Tabellen in DB2 für OS/2 mit einer allgemeinen Benutzer-ID zu erstellen. Für DB2 für OS/2 gibt es im Gegensatz zu DB2 Universal Database für AS/400 keine physischen Objektgruppen, sondern lediglich ein Tabellenqualifikationsmerkmal, das die Benutzer-ID des Erstellers ist.
2. DB2 Connect (oder DDCS) wird benötigt, wenn DB2 für OS/2 ein Client ist, der das DRDA-Protokoll verwendet. Es wird nicht benötigt, wenn DB2 für OS/2 nur als Server verwendet wird.

3. Es ist sehr wichtig, DB2 Connect ordnungsgemäß zu konfigurieren:
   a. Stellen Sie sicher, daß Sie über die aktuelle Version von DB2 für OS/2 und DB2 Connect verfügen. Ist dies nicht der Fall, wenden Sie verfügbare FixPaks an.
   b. Befolgen Sie die in den Handbüchern aufgeführten Installations- und Konfigurationsanweisungen.
4. Wenn Sie APPC verwenden, muß die Kommunikation ordnungsgemäß konfiguriert werden, d. h. für den Personal Computer müssen ein Controller und eine Einheit erstellt werden, wenn DB2 für OS/2 als Anwendungs-Requester oder als Anwendungs-Server eingesetzt wird. Zudem muß unabhängig vom verwendeten Kommunikationsprotokoll für jede Datenbank von DB2 für OS/2, zu der ein System IBM AS/400 eine Verbindung herstellen will, ein Eintrag im Verzeichnis RDB vorhanden sein.

   Gehen Sie wie folgt vor, um die APPC-Kommunikation zu definieren:
   a. Sie können die Einheiten- und Steuereinheitenbeschreibungen manuell erstellen. Sie können sie auch vom System erstellen lassen, wenn Sie über eine Token-Ring-Leitung verfügen und der Parameter AUTOCRTCLT der Leitungsbeschreibung auf *YES gesetzt ist. Sie können die Leitungsbeschreibung mit dem Befehl WRKLIND aufrufen. Verwenden Sie dazu die Option 2 (Ändern). Wechseln Sie zum Parameter 'Steuereinheit automatisch erstellen', und lesen Sie den Wert für AUTOCRTCLT ab.

      Wenn das System automatisch Steuereinheiten erstellt, können Sie das Erstellen der notwendigen Steuereinheitenbeschreibungen einleiten. Starten Sie im Ordner **CM/2** unter OS/2 die Kommunikationsverbindung, und führen Sie **Subsystem Management** aus. Schauen Sie sich in **Subsystem Management** die Einzelangaben des SNA-Subsystems an. Hier können Sie logische Links (Logical Links) aufrufen. Aktivieren Sie nach der Auswahl dieser Option die Verbindung zum gewünschten System, um dort die Steuereinheit automatisch zu erstellen. Die Einheitenbeschreibung wird später automatisch erstellt.
   b. Die Einheit und die Steuereinheit für den Personal Computer auf dem System IBM AS/400 müssen für eine korrekte Funktionsweise der Netzwerkverbindung zwischen Systemen aktiv sein (ACTIVE). Sie können den Parameter SWTDSC in der Steuereinheitenbeschreibung auf *NO setzen, um die Aktivierung von Steuereinheiten beizubehalten. Sie können außerdem den Parameter ONLINE auf *YES setzen, damit die Steuereinheit bei IPL aktiviert wird. (Der Parameter ONLINE in der Einheitenbeschreibung muß unter Umständen auch auf *YES gesetzt werden). Sollen Parameter in einer Steuereinheitenbeschreibung geändert werden, muß die Steuereinheitenbeschreibung abgehängt und der Eigner der Steuereinheit (Parameter CTLOWN) auf *USER gesetzt werden.

c. Verwenden Sie den Befehl ADDRDBDIRE, um für jede DB2 für OS/2-Datenbank, zu der ein System IBM AS/400 eine Verbindung herstellt, einen Eintrag zum RDB-Verzeichnis hinzuzufügen. Dabei ist der RDB-Name der Datenbankname von DB2 für OS/2, und der Name des fernen Standorts ist der Name der Workstation.

5. Für Tabellen (physische Dateien) auf dem System IBM AS/400, die von DB2 für OS/2 verwendet werden, wird der korrekte CCSID-Wert (für den deutschen Kunden in der Regel 273) benötigt. Sie können den CCSID-Wert mit DSPFD ansehen und den CCSID-Wert für physische Dateien mit CHGPF ändern. Für eine erfolgreiche Verbindungsherstellung müssen Sie zudem unter Umständen einen der folgenden Werte ändern: die CCSID des Jobs, die CCSID des verwendeten Benutzerprofils oder die CCSID aus dem Systemwert (QCCSID), wenn sie dem Standardwert 65535 entspricht. In der Regel wird diese Änderung am besten in dem Benutzerprofil vorgenommen, unter dem der Server-Job ausgeführt wird.
6. Vor der Verwendung von DB2 Connect zur Zusammenarbeit mit einem AS/400-Server müssen Sie auf dem System IBM AS/400 SQL-Pakete für Anwendungsprogramme und für Dienstprogramme von DB2 Connect erstellen.
   a. Mit dem DB2-Befehl PREP können Sie die Quellendatei eines Anwendungsprogramms mit eingebettetem SQL verarbeiten. Durch diese Verarbeitung wird eine geänderte Quellendatei erstellt, die Aufrufe der Host-Programmiersprache für SQL-Anweisungen enthält. Außerdem wird standardmäßig in der Datenbank, zu der momentan eine Verbindung besteht, ein SQL-Paket erstellt.
   b. Gehen Sie wie folgt vor, um die Dienstprogramme von DB2 Connect an einen AS/400-Server mit DB2 zu binden:
      1)
      ```
      CONNECT TO rdb-name
      ```
      2)
      ```
      BIND pfad@DDCS400.LST BLOCKING ALL SQLERROR CONTINUE
               MESSAGES DDCS400.MGS GRANT PUBLIC
      ```
      Ersetzen Sie pfad in pfad@DDCS400.LST oben durch den Standardpfad C:\SQLLIB\BND\ oder durch den lokalen Wert, wenn die Installation nicht an der Standardposition vorgenommen wurde.

      **Anmerkung:** Für OS/400 Version 3 Release 1 wird PTF SF23624 benötigt, um zu vermeiden, daß die Datenbank von DB2 Universal Database für AS/400 in der dritten Bindedatei der Liste den SQL-Code -901 absetzt.
      3)
      ```
      CONNECT RESET
      ```

7. Gehen Sie für interaktives SQL zwischen DB2 Universal Database für AS/400 und DB2 für OS/2 wie folgt vor:
   a. Verwenden Sie die Sitzungsattribute NAMING(*SQL), DATFMT(*ISO) und TIMFMT(*ISO). Andere Formate außer *ISO funktionieren nicht notwendigerweise. Die Angaben für das Datumsformat (DATFMT) müssen auch für das Zeitformat (TIMFMT) verwendet werden.
   b. Beachten Sie die Übereinstimmung zwischen Objektgruppen (COLLECTION) auf dem System IBM AS/400 und dem Tabellenqualifikationsmerkmal (Benutzer-ID des Erstellers) für DB2 für OS/2. Informationen zu SQL-Operationen finden Sie in Punkt 1 dieser Liste von Überlegungen.
   c. Für die allererste interaktive Sitzung MÜSSEN Sie COMMIT(*CS) für die COMMIT-Steuerung und anschließend (1) RELEASE ALL, (2) COMMIT und (3) CONNECT TO rdb-name (dabei wird 'rdb-name' durch eine bestimmte Datenbank ersetzt) angeben. Sie können gleichzeitig GRANT EXECUTE ON PACKAGE QSQL400.QSQL0200 TO PUBLIC (PUBLIC kann durch bestimmte Benutzer ersetzt werden) absetzen, um anderen Benutzern die Verwendung des SQL-Pakets zu ermöglichen, das für interaktives SQL auf dem Personal Computer erstellt wurde.
8. Für Programme, die auf einem System IBM AS/400 erstellt wurden und auf eine Datenbank von DB2 für OS/2 zugreifen, müssen die folgenden Befehle von DB2 für OS/2 verwendet werden:
   a.
   ```
   GRANT ALL PRIVILEGES ON TABLE tabellenname TO benutzer
   ```
   b.
   ```
   GRANT EXECUTE ON PACKAGE paketname (in der Regel AS/400-
     Programmname) TO benutzer
   ```

   Für „benutzer" können Sie PUBLIC angeben.
9. Bei der Entwicklung von AS/400-Anwendungen für den Zugriff auf DB2 für OS/2 (Version 2.1.1 oder früher) wurde als Antwort auf den Befehl CRTSQLxxx die Nachricht SQL5057 abgesetzt, die besagt, daß auf dem Personal Computer ein SQL-Paket erstellt wurde, selbst wenn dies noch nicht der Fall war. Dies wurde in der letzten Version von DB2 für OS/2 behoben.

   In älteren Versionen von DB2 für OS/2 wurden zudem keine SQL-Pakete für OS/400-Programme erstellt, deren Textfelder für die Quellen-Member-Beschreibung ausgefüllt waren.

10. Gespeicherte Prozeduren der Programmiersprache C in DB2 für OS/2 können argc und argv nicht als Parameter verwenden (sie können nicht vom Typ main() sein). Dies unterscheidet sie von gespeicherten Prozeduren für AS/400, die argc und argv verwenden müssen. Informationen zu gespeicherten Prozeduren für DB2 für OS/2 finden Sie in den Beispielen im Unterverzeichnis \SQLLIB\SAMPLES. Sehen Sie sich OUTSRV.SQC und OUTCLI.SQC im Unterverzeichnis C an.
11. Verwenden Sie bei gespeicherten Prozeduren in DB2 für OS/2, die von einem System IBM AS/400 aufgerufen werden, für den Prozedurnamen Großschreibung. Das System IBM AS/400 setzt Prozedurnamen momentan in Großbuchstaben um. Dies bedeutet jedoch, daß eine Prozedur auf dem Personal Computer mit dem gleichen Prozedurnamen (allerdings in Kleinbuchstaben) nicht gefunden wird. Die Prozedurnamen gespeicherter Prozeduren für AS/400 müssen also groß geschrieben werden.
12. Ohne die entsprechende vorläufige Programmkorrektur (PTF) für eingebettetes SQL funktioniert die Anweisung CALL von einem System IBM AS/400 an DB2 für OS/2 nur dann, wenn der Prozedurname in eine Host-Variable aufgenommen wird (CALL :host-prozedurname(...)). Die vorläufige Programmkorrektur für Version 3 Release 7 zur Vermeidung dieses Umgehungsverfahrens ist SF35932. Die vorläufige Programmkorrektur für Version 3 Release 2 ist SF36535.
13. Gespeicherte Prozeduren für AS/400 können keine Anweisung COMMIT enthalten, wenn sie zur Ausführung in der gleichen Aktivierungsgruppe wie das aufrufende Programm erstellt werden (die korrekte Art der Erstellung). Eine gespeicherte Prozedur für DB2 für OS/2 darf eine Anweisung COMMIT enthalten, der Anwendungsentwickler sollte aber nicht vergessen, daß DB2 Universal Database für AS/400 über die Ausführung dieser Anweisung COMMIT nicht informiert wird.

# Kapitel 6. Verbinden von DB2 für VSE & VM in einem DRDA-Netzwerk

SQL/DS (DB2 für VM) Version 3 Release 5 unterstützt bei VM-Systemen DRDA-Anwendungs-Server für ferne Arbeitseinheiten und Anwendungs-Requester. SQL/DS (DB2 für VSE) Version 3 Release 5 stellt bei VSE-Systemen DRDA-Anwendungs-Server-Unterstützung für ferne Arbeitseinheiten bereit.

Zudem unterstützt DB2 für VSE &VM Version 5 Release 1 sowohl bei VM- als auch VSE-Systemen DRDA-Anwendungs-Server für verteilte Arbeitseinheiten. Dieses Kapitel enthält hauptsächlich Informationen zur Verbindung von Systemen mit DB2 für VSE &VM mit andersartigen fernen DRDA-Systemen. Weitere Informationen zum Verbinden zweier Systeme mit DB2 für VSE &VM enthalten die folgenden Handbücher:

- *VM/ESA Connectivity Planning, Administration and Operation*
- *DB2 for VM System Administration*
- *DB2 for VSE System Administration*

## DB2 für VM - Übersicht

Jeder Datenbankmanager von DB2 für VM kann mehrere Datenbanken (allerdings immer nur eine einzige Datenbank gleichzeitig) verwalten und wird normalerweise mit dem Namen der Datenbank bezeichnet, die momentan verwaltet wird. Der Name dieser relationalen Datenbank ist innerhalb einer Gruppe miteinander verbundener SNA-Netzwerke eindeutig.

Die verschiedenen DRDA- und VM-Komponenten für dir Verarbeitung verteilter Datenbanken werden im folgenden beschrieben. Über diese Komponenten können die Datenbankmanager von DB2 für VM auf lokale relationale Datenbanken zugreifen und mit fernen DRDA-Systemen im SNA-Netzwerk kommunizieren.

**AVS** APPC/VTAM-Unterstützung (AVS) ist eine VM-Komponente, über die VM-Anwendungen auf das SNA-Netzwerk zugreifen können. Sie stellt die Funktionalität für die logische Einheit (Logical Unit, LU) bereit, wie sie durch SNA definiert ist. Eine LU wird in der VM-Umgebung als *Gateway* bezeichnet. AVS wird in einem Gruppensteuerungssystem als eine VTAM-Anwendung ausgeführt. AVS setzt APPC/VM-Makroaufrufe in APPC/VTAM-Makroaufrufe um und umgekehrt. APPC/VM verwendet AVS zur Weiterleitung und Umsetzung von Datenströmen. Mit AVS können Anforderungen von DB2 für VM zwischen dem lokalen VM-System und fernen SNA-

Standorten übertragen werden. AVS muß verwendet werden, wenn Anwendungen oder Datenbanken unter DB2 für VM mit Datenbanken oder Anwendungen kommunizieren, die nicht unter DB2 für VM ausgeführt werden.

Auf der Seite des Anwendungs-Requesters muß der Benutzer die Berechtigung zur Herstellung einer Verbindung über einen AVS-Gateway erhalten, bevor die Anforderungen gesendet werden können. Außerdem muß der empfangende AVS-Gateway auf der Seite des Anwendungs-Servers die entsprechende Berechtigung zur Herstellung einer Verbindung zur Server-Maschine unter DB2 für VM erhalten, bevor AVS die Anforderungen des Benutzers weiterleiten kann. Die Berechtigung erfolgt durch Bereitstellen der entsprechenden Anweisung für die IUCV-Verzeichnissteuerung in der Benutzermaschine, der Datenbankmaschine sowie der sendenden und empfangenden AVS-Maschinen. Ausführliche Informationen hierzu enthält das Handbuch *VM/ESA Connectivity Planning, Administration, and Operation*.

**APPC/VM**
APPC/VM ist die VM-API auf Assemblerebene, die eine Untermenge der LU 6.2-Funktionen bereitstellt, wie sie durch SNA definiert werden. Praktisch bedeutet dies, daß APPC/VM die LU 6.2-Verben bereitstellt, die Anwendungen unter DB2 für VM die Verbindungsherstellung zu lokalen und fernen Datenbankmanagern und die Verarbeitung in diesen Systemen ermöglichen. Die von APPC/VM unterstützten LU 6.2-Verben sind im Handbuch *VM/ESA CP Programming Services* aufgelistet.

**Kommunikationsverzeichnis (Communications Directory)**
Das Kommunikationsverzeichnis ist eine CMS-Datei mit dem Dateityp NAMES, die beim Einrichten von APPC-Dialogen zwischen einem lokalen VM-Anwendungs-Requester und einem Anwendungs-Server eine bestimmte Aufgabe erfüllt. Dieses Verzeichnis stellt die erforderlichen Informationen zur Weiterleitung und Einrichtung eines APPC-Dialogs mit dem Ziel-Server bereit. Zu diesen Informationen gehören Angaben wie LU-Name, TPN, Sicherheit, Modusname, Benutzer-ID, Kennwort und Datenbankname.

DB2 für VM verwendet das COMDIR-Kennzeichen :dbname zum Auflösen von RDB_NAME in die entsprechenden Leitwegdaten.

Diese Sonderdatei und ihre Funktion bei der Datenübertragung werden im Handbuch *VM/ESA Connectivity Planning, Administration, and Operation* beschrieben.

**CRR** CRR (Coordinated Resource Recovery) ist eine VM-Einrichtung, die das Festschreiben bzw. Zurücksetzen von Aktualisierungen geschützter Ressourcen koordiniert. Verteilte Anwendungsprogramme stellen

in Zusammenarbeit mit CRR anhand geschützter Dialoge die Integrität der verteilten Transaktionsressourcen sicher.

**CRR Recovery Server**
Der CRR Recovery Server ist eine Komponente von CRR und wird auf der eigenen virtuellen Maschine ausgeführt. Dieser Server ist für die Ausführung von Funktionen für Synchronisationspunktprotokollierung und Resynchronisation zuständig.

**GCS** Das Gruppensteuerungssystem (GCS, Group Control System) ist eine VM-Komponente mit folgenden Bestandteilen:

- Ein gemeinsam benutztes Segment, das auf einer virtuellen Maschine ausgeführt wird
- Ein Supervisor für virtuelle Maschinen, der mehrere virtuelle Maschinen in einer Gruppe zusammenfaßt und ihre Operationen überwacht
- Eine Schnittstelle zwischen folgenden Programmprodukten:
  - Virtual Telecommunications Access Method (VTAM)
  - APPC/VTAM-Unterstützung (AVS)
  - Remote Spooling Communications Subsystem (RSCS)
  - Steuerprogramm (Control Program, CP)

  GCS überwacht die Ausführung von VTAM-Anwendungen wie z. B. AVS in einer VM-Umgebung. Virtuelle Maschinen, die unter der Überwachung von GCS ausgeführt werden, verwenden kein CMS.

**Ressourcenadapter**
Der Ressourcenadapter ist der Teil der Logik von DB2 für VM, der sich in Ihrer virtuellen Maschine befindet und Ihrer Anwendung ermöglicht, Zugriff auf einen Server unter DB2 für VM anzufordern. Die Funktion für DRDA-Anwendungs-Requester ist in den Ressourcenadapter integriert.

**TSAF** TSAF (Transparent Services Access Facility) ist eine VM-Komponente, die Kommunikationsunterstützung zwischen miteinander verbundenen VM-Systemen zur Verfügung stellt. Bis zu acht VM-Systeme können zu einem TSAF-Verbund zusammengeschlossen werden, der mit einem VM-LAN (oder einem Weitverkehrsnetz) verglichen werden kann. Auf jedem teilnehmendem VM-System muß eine virtuelle TSAF-Maschine betrieben werden. Innerhalb eines TSAF-Verbunds sind alle Benutzer-IDs und Ressourcen-IDs eindeutig.

DB2 für VM verwendet TSAF zum Weiterleiten von Anforderungen für verteilte Datenbanken an andere Maschinen mit DB2 für VM innerhalb des TSAF-Verbunds. Wenn das lokale VM-System nicht über eine virtuelle AVS-Maschine verfügt, verwendet DB2 für VM TSAF

zum Weiterleiten von DRDA-Anforderungen an ein VM-System, das über eine virtuelle AVS-Maschine verfügt. Über AVS kann die Anforderung an andere TSAF-Verbunde sowie an Systeme ohne DB2 für VM weitergeleitet werden.

Ein TSAF-Verbund wird im SNA-Netzwerk als mindestens eine logische Einheit angesehen. Auf Ressourcen, die innerhalb eines TSAF-Verbunds als global definiert sind, können ferne APPC-Programme zugreifen, die sich an einer beliebigen Stelle im Verbund befinden können.

Normalerweise arbeitet ein TSAF-Verbund als eigenständige Komponente, unabhängig von VTAM und vom SNA-Netzwerk. Er kann jedoch mit AVS und VTAM zusammenarbeiten, um seine globalen Ressourcen für ferne APPC-Programme zugänglich zu machen, die sich an einer beliebigen Stelle im SNA-Netzwerk befinden. Dazu ist es erforderlich, daß eine AVS-Maschine und eine VTAM-Maschine auf mindestens einem Mitglied des TSAF-Verbunds ausgeführt werden. TSAF wird im Handbuch *VM/ESA Connectivity Planning, Administration, and Operation* beschrieben.

**VTAM**

VTAM (Virtual Telecommunications Access Method) stellt die Netzwerkkommunikationsunterstützung für Konnektivität zur Verfügung. DB2 für VM verwendet die VTAM-Services über AVS, um Verbindungen und Anforderungen an ferne DRDA-Systeme weiterzuleiten. VTAM wird *ausschließlich* für ferne Anforderungen verwendet, die auf das SNA-Netzwerk zugreifen.

***IDENT**

AVS und TSAF verwenden den Transaktionsprogrammnamen (TPN) zum Weiterleiten von Anforderungen zwischen VM-Systemen, die über TSAF und AVS verbunden sind. Der TPN kann ein in SNA registrierter Transaktionsprogrammname oder ein gültiger alphanumerischer Name sein. In VM wird der TPN-Wert als Ressourcen-ID angesehen. Damit ferne DRDA-Systeme auf einen Server unter DB2 für VM zugreifen können, verwendet der Server unter DB2 für VM den VM-Systemservice IDENTIFY (*IDENT), um sich selbst als Manager einer globalen Ressourcen-ID (TPN) zu definieren. Sobald der Server als globale Ressource identifiziert ist, können TSAF und AVS DRDA-Anforderungen an den Server unter DB2 für VM weiterleiten, sofern der empfangene TPN mit der Ressourcen-ID übereinstimmt.

## Anwendungs-Requester - Beispiel für Kommunikationsdatenfluß

Das folgende Beispiel zeigt, welche Rolle die einzelnen Komponenten beim Einrichten der Verbindung zwischen einem VM-Anwendungs-Requester und einem fernen DRDA-Server spielen. Abb. 27 zeigt, wie der Anwendungs-Requester die Verbindung zu AVS herstellt und über VTAM auf das SNA-Netzwerk zugreift. Der Zugriff auf ferne Ressourcen erfolgt nicht über den lokalen Anwendungs-Server unter DB2 für VM.

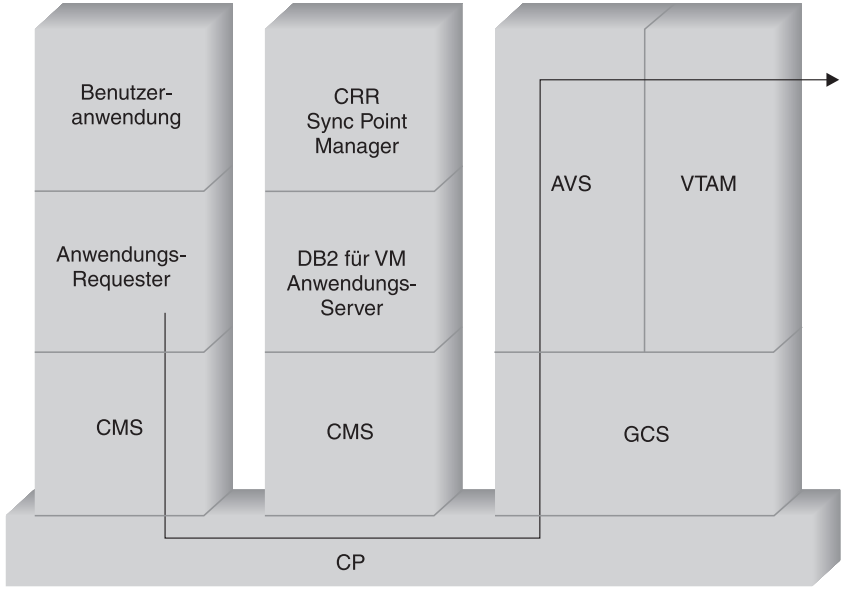


*Abbildung 27. Anfordern des Zugriffs auf eine ferne Ressource*

Angenommen, ein Anwendungs-Requester unter DB2 für VM, der in einem TSAF-Verbund betrieben wird, soll auf ferne Daten zugreifen, die von einem DRDA-Anwendungs-Server verwaltet werden. Per Definition heißt dies, daß auf dem lokalen VM-Host, auf dem sich der Anwendungs-Requester befindet, eine TSAF-Maschine betrieben wird. Außerdem werden eine AVS-Komponente und eine VTAM-Maschine auf einem VM-System im TSAF-Verbund betrieben. AVS und VTAM könnten sich auch auf dem gleichen System wie der Anwendungs-Requester und der Anwendungs-Server befinden.

Nach dem Start definiert die VTAM-Maschine den lokalen AVS-Gateway gegenüber dem SNA-Netzwerk und definiert eine oder mehrere Sitzungen, die später zur Einrichtung von Dialogen verwendet werden können.

Die AVS-Maschine vereinbart nach dem Starten Sitzungsbegrenzungen zwischen dem lokalen AVS-Gateway und den potentiellen Partner-LUs.

Der Anwendungs-Server kann aktiv oder inaktiv sein. Der Bediener muß den Anwendungs-Server starten, damit Anforderungen von gleichartigen oder andersartigen Anwendungs-Requestern verarbeitet werden können.

Der Anwendungs-Requester setzt eine APPC/VM-Anweisung CONNECT ab, um einen LU 6.2-Dialog mit dem Anwendungs-Server einzurichten. Die Funktion CONNECT verwendet das CMS-Kommunikationsverzeichnis zum Auflösen des Namens der relationalen Datenbank in den zugehörigen LU-Namen und den TPN, aus denen die Adresse des Anwendungs-Servers im SNA-Netzwerk besteht. Das CMS-Kommunikationsverzeichnis legt außerdem die Stufe der Dialogsicherheit und die Sicherheits-Token (z. B. Benutzer-ID und Kennwort) fest, die zum Zweck der Berechtigungsüberprüfung an den fernen Standort übermittelt werden. Wenn SECURITY=PGM verwendet wird, muß der Anwendungs-Requester eine Benutzer-ID und ein Kennwort an den Anwendungs-Server übermitteln. Sie können die Benutzer-ID und das Kennwort im CMS-Kommunikationsverzeichnis oder im APPCPASS-Datensatz angeben, der im Benutzerverzeichnis des Anwendungs-Requesters definiert ist. Bei der Verwendung von SECURITY=SAME wird nur die VM-Anmelde-ID des Benutzers des Anwendungs-Requesters an den Anwendungs-Server übermittelt, und es ist kein zusätzliches Kennwort erforderlich.

Beispiel: Wenn Sie SECURITY=SAME verwenden, überprüft der Host, ob eine AVS-Maschine lokal ausgeführt wird. Ist dies nicht der Fall, stellt der Host eine Verbindung zwischen dem Anwendungs-Requester und der lokalen TSAF-Maschine her. Die lokale TSAF-Maschine fragt die AVS-Maschine unter den anderen TSAF-Maschinen im TSAF-Verbund ab und stellt eine Verbindung zur AVS-Maschine her.

Die AVS-Komponente im TSAF-Verbund wandelt die APPC/VM-Verbindungsanforderung in den äquivalenten APPC/VTAM-Funktionsaufruf um. Anschließend verwendet AVS eine vorhandene Sitzung oder richtet eine neue Sitzung zwischen dem Gateway (LU) und der fernen LU ein. Danach richtet AVS einen Dialog mit der fernen LU ein und übermittelt den LU-Namen, den TPN, die Sicherheitsstufe und die Benutzer-ID. Wenn die ferne LU ebenfalls ein VM-System ist, werden Sitzung und Dialog von der AVS-Komponente verwaltet, die auf diesem System ausgeführt wird.

## Anwendungs-Server - Beispiel für Kommunikationsdatenfluß

Das folgende Beispiel zeigt, welche Rolle die einzelnen Komponenten beim Einrichten der Verbindung zwischen einem fernen Anwendungs-Requester und einem lokalen DRDA-Server unter DB2 für VM spielen. Abb. 28 zeigt, daß VTAM die eingehende Verbindung zu dem spezifischen AVS-Gateway und anschließend zum Anwendungs-Server weiterleitet.

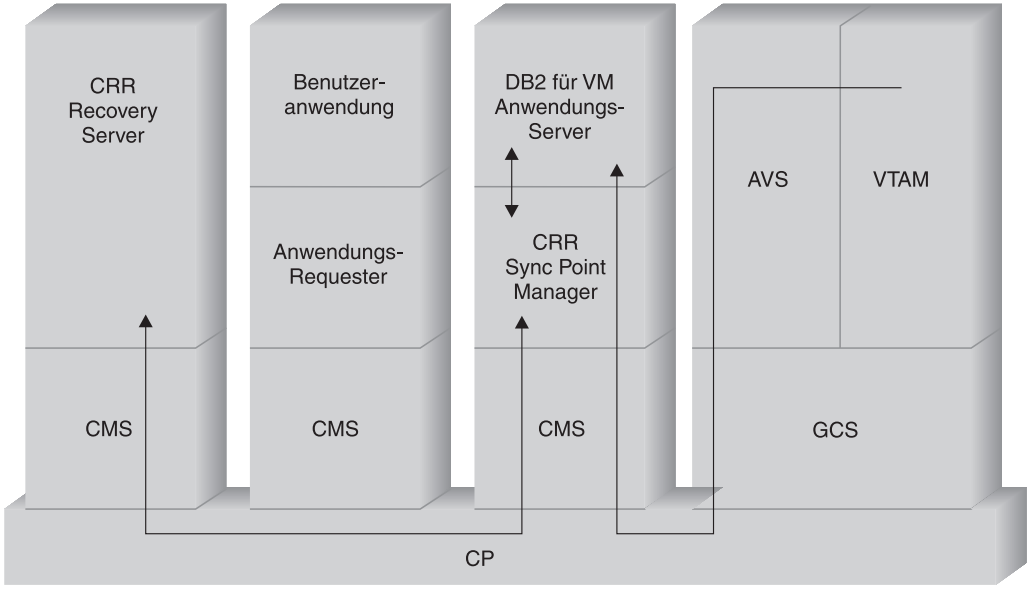


*Abbildung 28. Einrichten des Zugriffs auf eine ferne Ressource*

Angenommen, ein Anwendungs-Server unter DB2 für VM wird in einem TSAF-Verbund betrieben. Per Definition heißt dies, daß auf dem lokalen VM-Host, auf dem sich der Anwendungs-Server befindet, eine TSAF-Maschine betrieben wird. Außerdem werden eine AVS-Komponente und eine VTAM-Maschine auf einem VM-System im TSAF-Verbund betrieben. AVS und VTAM könnten sich auch auf dem gleichen System wie der Anwendungs-Requester und der Anwendungs-Server befinden.

Nach dem Start definiert die VTAM-Maschine den lokalen AVS-Gateway gegenüber dem SNA-Netzwerk und definiert eine oder mehrere Sitzungen, die später zur Einrichtung von Dialogen verwendet werden können.

Die AVS-Maschine vereinbart nach dem Starten Sitzungsbegrenzungen zwischen dem lokalen AVS-Gateway und den potentiellen Partner-LUs.

Der Anwendungs-Server kann aktiv oder inaktiv sein. Der Bediener muß den Anwendungs-Server starten, damit Anforderungen von gleichartigen oder andersartigen Anwendungs-Requestern verarbeitet werden können. Nach dem Starten verwendet der Anwendungs-Server den Service *IDENT, um die Ressourcen-ID, die er verwaltet, auf dem VM-Host-System zu registrieren. Durch jede Registrierung wird in einer internen Ressourcentabelle, die durch das VM-System verwaltet wird, ein Eintrag erstellt.

Nachdem die lokale AVS-Komponente die Sitzung mit ihrer Partner-LU eingerichtet hat, akzeptiert sie den Dialog und leitet den TPN, die Benutzer-ID und das Kennwort zur Gültigkeitsprüfung an den VM-Host weiter. Das VM-System sucht in der eigenen internen Ressourcentabelle nach dem TPN. Diese Tabelle enthält für jede Ressourcen-ID, die durch den Systemservice *IDENT registriert wurde, einen Eintrag. Wenn der TPN gefunden wird, prüft das VM-System die Gültigkeit von Benutzer-ID und Kennwort anhand des eigenen Verzeichnisses oder mit Hilfe von RACF bzw. einem äquivalenten Sicherheitsprodukt. Ist die Gültigkeitsprüfung erfolgreich, stellt AVS eine Verbindung zu dem Anwendungs-Server her und übermittelt die Benutzer-ID zur Gültigkeitsprüfung für die Datenbank.

Ist die Suche in der Tabelle nicht erfolgreich, nimmt AVS an, daß sich der TPN möglicherweise in einem anderen VM-System im TSAF-Verbund befindet, stellt eine Verbindung zur lokalen TSAF-Maschine her und leitet die Benutzer-ID, das Kennwort und den TPN an diese Maschine weiter. Die TSAF-Maschine fragt die übrigen TSAF-Maschinen im TSAF-Verbund ab. Bestätigt eine dieser Maschinen das Vorhandensein des TPN in ihrer Ressourcentabelle, stellt die lokale TSAF-Maschine eine Verbindung zur fernen TSAF-Maschine her und übermittelt Benutzer-ID und Kennwort zur Überprüfung anhand des VM-Verzeichnisses dieser Maschine. Ist die Gültigkeitsprüfung erfolgreich, stellt die ferne TSAF-Maschine eine Verbindung zum Anwendungs-Server her und übermittelt die Benutzer-ID zur Gültigkeitsprüfung für die Datenbank.

Wenn der Anwendungs-Requester Unterstützung für verteilte DRDA-Arbeitseinheiten in Anspruch nehmen will, richtet er einen geschützten Dialog (d. h. SYNCLEVEL=SYNCPT) mit dem Anwendungs-Server unter DB2 für VM ein. CMS erstellt vor der Verbindungsherstellung zu DB2 für VM eine CMS-Arbeitseinheit für den geschützten Dialog auf der Maschine unter DB2 für VM. DB2 für VM verwendet diese CMS-Arbeitseinheit anschließend bei jedem Arbeitsvorgang für den Requester. Nach dem Arbeitsbeginn für den Requester registriert DB2 für VM diese CMS-Arbeitseinheit beim CRR-Synchronisationspunktmanager (CRR Sync Point Manager). Wenn DB2 danach im geschützten Dialog eine SNA-Markierung für Festschreiben (COMMIT) bzw. Zurücksetzen (ROLLBACK) empfängt, weist DB2 den CRR-Synchronisationspunktmanager an, die Arbeitseinheit festzuschreiben bzw. zurückzusetzen. Der CRR-Synchronisationspunktmanager steuert die COMMIT- bzw. ROLLBACK-Operation und weist den CRR Recovery Server an, bei Bedarf eine Synchronisationspunktprotokollierung auszuführen.

Je nach Komplexität der Verbindungswege können an dem APPC-Dialog zwischen Anwendungs-Requester und Anwendungs-Server weitere Systeme beteiligt sein. Alle Zwischenverbindungen werden jedoch vom VM-System verwaltet, und sie sind für den Anwendungs-Requester oder die Benutzeranwendung transparent. Die APPC/VM-Schnittstelle ermöglicht Anwendungs-Servern unter DB2 für VM den Datenaustausch mit APPC-Anwendungsprogrammen an folgenden Standorten:

- Im selben VM-System
- In einem anderen VM-System
- In einem VM-System innerhalb eines SNA-Netzwerks, auf dem AVS und VTAM ausgeführt werden
- In einem VM-System innerhalb eines anderen TSAF-Verbunds, auf dem AVS und VTAM ausgeführt werden
- In einem Nicht-VM-System innerhalb eines SNA-Netzwerks, das das LU 6.2-Protokoll unterstützt
- In einem System eines anderen Herstellers als IBM innerhalb eines SNA-Netzwerks, das das LU 6.2-Protokoll unterstützt

## Implementierung von DB2 für VM

Wie in Abb. 29 gezeigt, kann eine VM-Anwendung nur über den Anwendungs-Requester (Ressourcenadapter) von DB2 für VM auf eine Datenbank eines Anwendungs-Servers von DB2 für VM oder eines DRDA-Anwendungs-Servers zugreifen. Eine Datenbank auf einem Anwendungs-Server unter DB2 für VM kann SQL-Anforderungen von jedem Anwendungs-Requester unter DB2 für VM oder DRDA-Anwendungs-Requester empfangen.

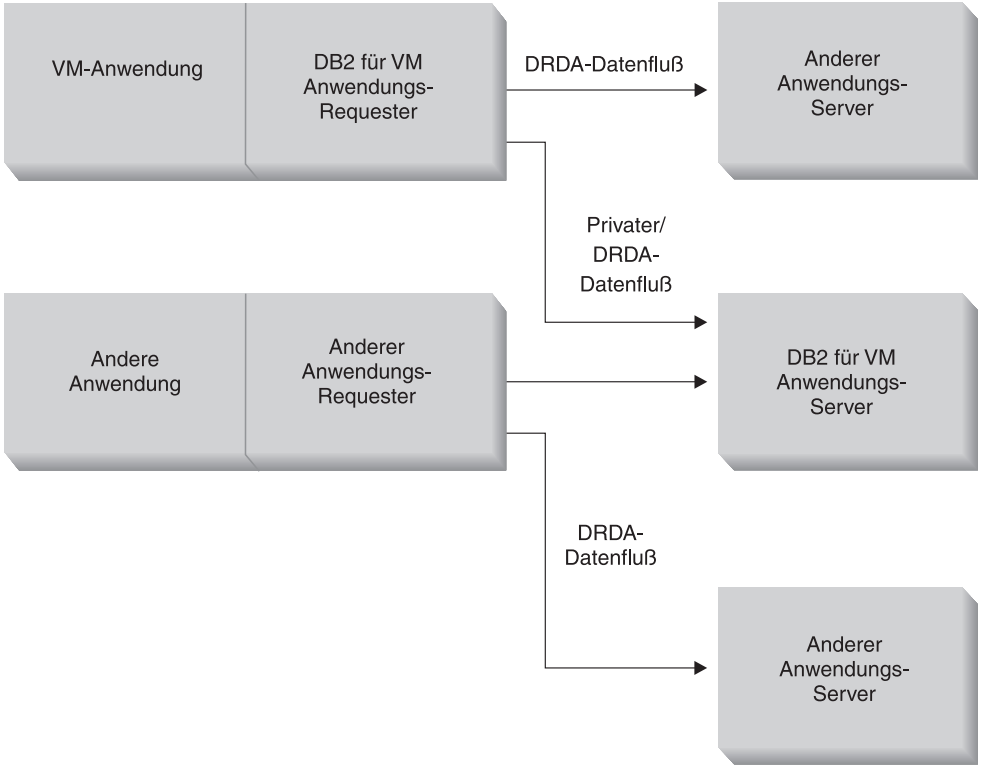


*Abbildung 29. Anwendungs-Requester und Anwendungs-Server unter DB2 für VM*

## Optionen für Vorverarbeitung und Ausführung einer Anwendung

DB2 für VM unterstützt im Befehl SQLINIT drei Verarbeitungsoptionen, die dem Benutzer und dem Datenbankadministrator das Aktivieren der Unterstützung für verteilte Datenbanken ermöglichen. Vor Beginn der Vorverarbeitung bzw. der Ausführung der Anwendung kann der Benutzer eine der folgenden SQLINIT-Optionen angeben:

**PROTOCOL(SQLDS)**

Fordert die Verwendung des privaten SQLDS-Protokolls an. Dies ist die Standardoption. Sie kann zwischen einem Anwendungs-Requester und -Server unter DB2 für VM in einer lokalen oder fernen Umgebung verwendet werden. Der Anwendungs-Server von DB2 für VM nimmt an, daß der Requester dieselben CCSIDs wie der Server verwendet. Die vom Requester über SQLINIT konfigurierten CCSID-Standardwerte [5] werden ignoriert, und dem Dialog wird keine LU 6.2-LUWID zugeordnet. Wenn Sie überall nur Systeme mit DB2 für VM und dieselbe Standard-CCSID verwenden, ist diese Option am effektivsten.

**PROTOCOL(AUTO)**

Fordert den Anwendungs-Requester von DB2 für VM auf festzustellen, ob der Anwendungs-Server ein gleichartiges oder ein andersartiges System ist. Anschließend wird für ein gleichartiges System automatisch die Verwendung eines privaten SQLDS-Protokolls bzw. für ein andersartiges System die Verwendung des DRDA-Protokolls ausgewählt. Die Option kann zwischen gleichartigen (lokalen und fernen) und andersartigen Systemen verwendet werden. Wenn für den Anwendungs-Server nicht PROTOCOL=SQLDS festgelegt ist, können auf dem Anwendungs-Requester und -Server unterschiedliche Standard-CCSIDs verwendet werden. Die Anforderungen und Antworten werden entsprechend umgewandelt. Die Option AUTO ist in folgenden Fällen zu empfehlen:

- Wenn Sie auf gleichartige und andersartige Systeme zugreifen müssen
- Wenn die Standard-CCSIDs auf Requester und Server unterschiedlich sind (und die Option PROTOCOL auf dem Anwendungs-Server nicht SQLDS ist)
- Wenn jedem Dialog eine LU 6.2-LUWID zugeordnet sein muß, damit Sie einen Prozeß problemlos zum Ursprungsstandort zurückverfolgen können (dies ist hilfreich, wenn Sie in Ihrem Netzwerk mit verteilten Datenbanken eine große Anzahl von fernen Systemen mit DB2 für VM zu verwalten haben)

---

5. In DB2 für VM geben Anwendungs-Requester und Anwendungs-Server die Standard-CCSID mit Hilfe der Option CHARNAME für SQLINIT bzw. SQLSTART an. CHARNAME ist ein symbolischer Name, der intern den entsprechenden CCSIDs zugeordnet wird.

**PROTOCOL(DRDA)**

Zwingt den Anwendungs-Requester unter DB2 für VM, bei der Kommunikation mit dem Anwendungs-Server nur das DRDA-Protokoll zu verwenden. Diese Option kann zwischen gleichartigen (lokalen und fernen) und andersartigen Systemen verwendet werden. Wenn der Anwendungs-Server ein gleichartiges System ist, wird zwischen den beiden Systemen mit DB2 für VM das DRDA-Protokoll verwendet. Der Anwendungs-Requester und der Anwendungs-Server können über unterschiedliche Standard-CCSIDs verfügen. Die Anforderungen und Antworten werden entsprechend umgewandelt. Sie können diese Option zwischen zwei Systemen mit DB2 für VM zu Testzwecken oder für bestimmte Anwendungen verwenden, bei denen durch die Verwendung des DRDA-Protokolls aufgrund größerer Puffer zum Senden und Empfangen von Daten ein höherer Durchsatz erzielt werden kann.

Tabelle 3 vergleicht die Funktionsbeschreibungen der SQLINIT-Verarbeitungsoptionen des Anwendungs-Requesters unter DB2 für VM.

*Tabelle 3. Vergleich der SQLINIT-Verarbeitungsoptionen des Anwendungs-Requesters unter DB2 für VM*

| **[SQLDS]** | **[ AUTO ]** | **[DRDA]** |
|---|---|---|
| Beide Partner müssen Systeme mit DB2 für VM sein. | Verbindung zu jedem DRDA-System möglich. | Verbindung zu jedem DRDA-System möglich. |
| Lokale Kommunikation mit Partner über TSAF oder AVS/VTAM möglich. | Lokale Kommunikation mit einem System mit DB2 für VM oder mit einem fernen System mit DB2 für VM über TSAF bzw. AVS möglich. Bei andersartigen Systemen muß über AVS kommuniziert werden. | Lokale Kommunikation mit einem System mit DB2 für VM oder mit einem fernen System mit DB2 für VM über TSAF bzw. AVS möglich. Bei andersartigen Systemen muß über AVS kommuniziert werden. |
| Unterstützt statisches, dynamisches und erweitertes dynamisches SQL. | Unterstützt statisches, dynamisches und erweitertes dynamisches SQL. | Unterstützt statisches, dynamisches und erweitertes dynamisches SQL[6]. |
| Von SQLINIT für den Anwendungs-Requester definierte CCSIDs werden vom Anwendungs-Server unter DB2 für VM ignoriert. | Von SQLINIT für den Anwendungs-Requester definierte CCSIDs werden vom Anwendungs-Server unter DB2 für VM beachtet, und entsprechende Umwandlungen werden ausgeführt (wenn der Anwendungs-Server ebenfalls auf AUTO gesetzt ist). | Von SQLINIT für den Anwendungs-Requester definierte CCSIDs werden vom Anwendungs-Server unter DB2 für VM beachtet, und entsprechende Umwandlungen werden ausgeführt. |

6. Erweitertes dynamisches SQL wird für den DRDA-Datenfluß unterstützt, indem eine Umwandlung in statische oder dynamische Anweisungen ausgeführt wird. Dabei gelten verschiedene Einschränkungen.

*Tabelle 3. Vergleich der SQLINIT-Verarbeitungsoptionen des Anwendungs-Requesters unter DB2 für VM (Forts.)*

| | | |
|---|---|---|
| Feste Blockgröße von 8 KB; Aufruf OPEN gibt keine Zeilen zurück; Anwendungs-Requester muß den Cursor explizit schließen. | Verbindung von DB2 für VM mit DB2 für VM: SQLDS-Methode; alle anderen Verbindungen: DRDA-Methode | Variable Blockgröße von 1 KB bis 32 KB; stärker komprimierte Datenpaketierung; Aufruf OPEN gibt einen Zeilenblock zurück; Anwendungs-Server kann den Cursor implizit schließen, so daß der Anwendungs-Requester keinen CLOSE-Aufruf senden muß. |
| Kann mit Cursoranweisungen INSERT und PUT jeweils einen Zeilenblock mit fester Blockgröße von 8 KB gleichzeitig einfügen. | Verbindung von DB2 für VM mit DB2 für VM: SQLDS-Methode; alle anderen Verbindungen: DRDA-Methode | PUT-Anweisungen werden in reguläre Einfügungen einzelner Zeilen umgewandelt und zeilenweise abgesendet. |
| Alle für DB2 für VM spezifischen Befehle werden unterstützt. | Verbindung von DB2 für VM mit DB2 für VM: SQLDS-Methode; alle anderen Verbindungen: DRDA-Methode | Bedienerbefehle von DB2 für VM, einige Anweisungen von DB2 für VM und einige ISQL- und DBSU-Befehle werden nicht unterstützt (siehe das Handbuch *DB2 for VSE & VM SQL Reference*). |
| LUWID wird nicht unterstützt. | LUWID wird unterstützt. | LUWID wird unterstützt. |

## Optionen zum Starten der Datenbank-Server-Maschine

In diesem Abschnitt werden die verschiedenen Optionen zum Starten der Datenbank-Server-Maschine beschrieben.

### Parameter PROTOCOL

Beim Starten der Datenbank-Server-Maschine kann der Datenbankadministrator eine der folgenden Optionen für den Parameter PROTOCOL angeben.

**SQLDS**

Die empfohlene Standardoption, wenn der Anwendungs-Server nur Unterstützung für Anwendungs-Requester unter DB2 für VM oder für Anwendungsanfragen von DB2 für VSE bei gemeinsamer Benutzung der VSE-Gastmaschine bereitstellen muß. Der Anwendungs-Server verwendet nur den privaten Datenfluß (SQLDS). Der Anwendungs-Server reagiert auf die vom Anwendungs-Requester ausgewählte Verarbeitungsoption. Wenn ein Requester unter DB2 für VM die Einstellung PROTOCOL(SQLDS) verwendet, wird die Verarbeitung auf dem Server unter DB2 für VM regulär mit privatem Datenfluß fortgesetzt. Wenn der Requester unter DB2 für VM die Einstellung PROTOCOL(AUTO) verwendet, weist der Server unter DB2 für VM den Requester an, auf privaten Datenfluß umzuschalten. Zwischen dem Anwendungs-Requester und dem Anwendungs-Server werden keine CCSID-Informationen ausgetauscht. Der Anwendungs-Server geht davon aus, daß die CCSIDs des Anwendungs-Requesters mit denen des Anwendungs-Servers übereinstimmen. Wenn der Requester unter DB2 für VM die Einstellung PROTOCOL(DRDA) verwendet, wird der Dialog beendet. Wenn ein Anwendungs-Requester mit einer anderen DB2-Version als DB2 für VSE &VM versucht, auf den Server unter DB2 für VM zuzugreifen, wird der Dialog beendet.

**AUTO**

Die empfohlene Option, wenn der Anwendungs-Server die Unterstützung für das private Protokoll und das DRDA-Protokoll bereitstellen muß. Die Anwendungs-Requester unter DB2 für VM, die die Einstellung PROTOCOL(SQLDS) oder PROTOCOL(AUTO) verwenden, kommunizieren über den privaten Datenfluß. Für einen Anwendungs-Requester, der die Einstellung SQLDS verwendet, werden keine CCSID-Informationen ausgetauscht, und der Anwendungs-Server geht davon aus, daß die CCSIDs des Anwendungs-Requesters mit denen des Anwendungs-Servers übereinstimmen. Für einen Requester, der die Einstellung AUTO verwendet, werden CCSID-Informationen ausgetauscht, und die CCSID-Umwandlung von Anforderungen und Antworten wird entsprechend ausgeführt. Der DRDA-Datenfluß ist für alle Requester ohne DB2 für VM und für alle Requester unter DB2 für VM erforderlich, die die Einstellung PROTOCOL(DRDA) verwenden.

### Parameter SYNCPNT

Dieser Parameter gibt an, ob ein Synchronisationspunktmanager (SPM) zum Koordinieren von verteilten DRDA-2-Arbeitseinheiten für das Lesen und Schreiben auf mehreren Systemen verwendet wird.

Wenn Y angegeben wird, verwendet der Server einen Synchronisationspunktmanager (sofern möglich), um zweiphasige Festschreibungen und Resynchronisationsfunktionen zu koordinieren. Wenn N angegeben wird, verwendet der Anwendungs-Server keinen SPM, um zweiphasige Festschreibungen durchzuführen. Wenn N angegeben wird, ist der Anwendungs-Server auf verteilte Arbeitseinheiten für Lesen auf mehreren Systemen und Schreiben auf einem einzigen System begrenzt, und der Server kann das System sein, auf das geschrieben wird. Wenn Y angegeben wird, für den Anwendungs-Server jedoch kein Synchronisationspunktmanager zur Verfügung steht, wird der Server so betrieben, als ob N angegeben wurde.

Die Standardeinstellung ist SYNCPNT=Y, wenn die Einstellung PROTOCOL=AUTO verwendet wird. Bei Verwendung der Einstellung PROTOCOL=SQLDS wird der Parameter SYNCPNT auf N gesetzt.

## Konfigurieren des Anwendungs-Requesters in einer VM-Umgebung

DB2 für VM implementiert die Unterstützung für DRDA-Anwendungs-Requester als integralen Bestandteil des Ressourcenadapters, der sich zusammen mit der Anwendung auf der virtuellen Maschine des Endbenutzers befindet. Sie können die Anwendungs-Requester-Unterstützung auch verwenden, wenn die virtuelle Maschine des lokalen Datenbankmanagers nicht aktiv ist. Sie können die Unterstützung für den DRDA-Anwendungs-Requester aktivieren, indem Sie SQLINIT EXEC mit PROTOCOL(AUTO) oder mit PROTOCOL(DRDA) ausführen (siehe den Abschnitt „Optionen für Vorverarbeitung und Ausführung einer Anwendung” auf Seite 143).

Wenn DB2 für VM als Anwendungs-Requester fungiert, kann eine Verbindung zu einem Anwendungs-Server unter DB2 für VM oder zu jedem anderen Server-Produkt, das die DRDA-Architektur unterstützt, hergestellt werden. Damit der Anwendungs-Requester unter DB2 für VM den Zugriff auf verteilte Datenbanken bereitstellen kann, müssen Sie folgende Maßnahmen durchführen können:

- „Bereitstellen von Netzwerkinformationen” auf Seite 148. Der Anwendungs-Requester muß in der Lage sein, RDB_NAME-Werte entgegenzunehmen und in SNA NETID.LUNAME-Werte umzuwandeln. DB2 für VM verwendet das CMS-Kommunikationsverzeichnis zum Katalogisieren von RDB_NAME-Werten und ihrer zugehörigen Netzwerkparameter. Mit Hilfe des Kommunikationsverzeichnisses kann der Anwendungs-Requester beim Absetzen von Anforderungen für verteilte Datenbanken die erforderlichen SNA-Informationen an VTAM übermitteln.

- „Gewährleisten der Sicherheit” auf Seite 156. Damit der Anwendungs-Server Anforderungen für ferne Datenbanken entgegennehmen kann, muß der Anwendungs-Requester die Sicherheitsinformationen bereitstellen, die der Anwendungs-Server benötigt. DB2 für VM verwendet das Kommunikationsverzeichnis und das Benutzerverzeichnis auf der Anwendungs-Requester-Seite sowie wahlfrei das Benutzerverzeichnis oder RACF auf der Anwendungs-Server-Seite, um beim Absetzen einer Anforderung für verteilte Datenbanken die erforderlichen Netzwerksicherheitsinformationen bereitzustellen.
- „Darstellen von Daten” auf Seite 161. Der Anwendungs-Requester muß über eine CCSID verfügen, die mit dem Anwendungs-Server kompatibel ist.

## Bereitstellen von Netzwerkinformationen

Viele Verarbeitungsprozesse in einer verteilten Datenbankumgebung erfordern das Austauschen von Nachrichten mit anderen Netzwerkstandorten. Für die korrekte Durchführung dieses Prozesses sind folgende Schritte erforderlich:

1. Definieren des lokalen Systems
2. Definieren der fernen Systeme
3. Definieren des Kommunikationssubsystems
4. Einstellen von RU-Größe und Nachrichtendosierung
5. Vorbereiten des Anwendungs-Requesters unter DB2 für VM

### Definieren des lokalen Systems

Der Anwendungs-Requester unter DB2 für VM und der Anwendungs-Server unter DB2 für VM sind voneinander unabhängig. Der Anwendungs-Requester unter DB2 für VM leitet Verbindungsanforderungen direkt an lokale oder ferne Anwendungs-Server weiter. Er definiert sich jedoch nicht selbst als Ziel für eingehende Verbindungsanforderungen. Nur der Anwendungs-Server unter DB2 für VM kann eingehende Verbindungsanforderungen annehmen (oder zurückweisen). Deshalb identifiziert der Anwendungs-Requester unter DB2 für VM im Unterschied zu DB2 Universal Database für OS/390 keine eigenen RDB_NAME-Werte und Transaktionsprogrammnamen.

Definieren Sie den Anwendungs-Requester unter DB2 für VM im SNA-Netzwerk wie folgt:

1. Definieren Sie AVS-Gateway-Namen mit APPL-Definitionsanweisungen für VTAM.

   Der Anwendungs-Requester benötigt definierte Gateway-Namen (z. B. die LU-Namen), um abgehende Anforderungen an das Netzwerk weiterzuleiten. Abb. 30 auf Seite 149 zeigt ein Beispiel hierfür. Diese Anweisungen befinden sich auf der virtuellen VTAM-Maschine. Beim Starten von VTAM werden die Gateways gegenüber dem Netzwerk identifiziert, aber sie werden erst aktiviert, wenn die für die Steuerung zuständige virtuelle

AVS-Maschine gestartet wird. Jede virtuelle AVS-Maschine kann auf einem VM-Host mehrere Gateways definieren.

```
                VBUILD  TYPE=APPL
************************************************************
*                                                          *
*  Gateway-Definition für System mit DB2 für VM Toronto    *
*                                                          *
************************************************************
TORGATE  APPL  APPC=YES,                                   X
               AUTHEXIT=YES,                               X
               AUTOSES=1,                                  X
               DMINWNL=10,                                 X
               DMINWNR=10,                                 X
               DSESLIM=20,                                 X
               EAS=9999,                                   X
               MAXPVT=100K,                                X
               MODETAB=RDBMODES,                           X
               PARSESS=YES,                                X
               SECACPT=ALREADYV,                           X
               SYNCLVL=SYNCPT,                             X
               VPACING=2
```

*Abbildung 30. Beispiel für eine AVS-Gateway-Definition*

Die folgende Liste beschreibt die Schlüsselwörter der VTAM-Anweisung APPL, die für die Themen dieses Handbuchs von Bedeutung sind. (Die VTAM-Anweisung APPL unterstützt wesentlich mehr Schlüsselwörter, als in diesem Beispiel gezeigt werden).

**TORGATE**
VTAM verwendet den APPL-Anweisungskennsatz als Gateway-Namen (LU-Namen). In Abb. 30 wird der Gateway TORGATE definiert. Die VTAM-Anweisung APPL gibt keine Netzwerk-ID (NETID) an. Die NETID wird für alle VTAM-Anwendungen im VTAM-System automatisch zugeordnet.

**AUTOSES=1**
Der Gateway TORGATE gibt an, daß automatisch eine SNA-Konfliktgewinnersitzung gestartet wird, wenn Sie einen APPC-Befehl zum Ändern der Sitzungsanzahl (CNOS - Change Number of Sessions) absetzen. Sie müssen für AUTOSES für AVS einen Wert ungleich Null angeben, damit Sie in jedem Fall darauf hingewiesen werden, wenn die CNOS-Verarbeitung fehlschlägt. Sie brauchen nicht alle APPC-Sitzungen zwischen zwei beliebigen Partnerpaaren der verteilten Datenbankumgebung automatisch zu starten. Wenn der Wert für AUTOSES unter der Konfliktgewinnerbegrenzung (DMINWNL) liegt, verzögert VTAM das Starten der übrigen Sitzungen, bis sie von einer Anwendung für verteilte Datenbanken benötigt werden.

**DMINWNL=10**

Der Gateway TORGATE gibt an, daß dieses System mit DB2 für VM der Konfliktgewinner in mindestens 10 Sitzungen ist. Die CNOS-Verarbeitung verwendet den Parameter DMINWNL als Standardwert; er kann jedoch für jeden Partner durch Absetzen des Befehls AGW CNOS auf der virtuellen AVS-Maschine außer Kraft gesetzt werden.

**DMINWNR=10**

Der Gateway TORGATE gibt an, daß dieses Partnersystem der Konfliktgewinner in mindestens 10 Sitzungen ist. Die CNOS-Verarbeitung verwendet den Parameter DMINWNR als Standardwert; er kann jedoch für jeden Partner durch Absetzen des Befehls AGW CNOS auf der virtuellen AVS-Maschine außer Kraft gesetzt werden.

**DSESLIM=20**

Die Gesamtzahl zulässiger Sitzungen (Konfliktgewinner und Konfliktverlierer) zwischen dem Gateway TORGATE und allen verteilten Partnersystemen für einen bestimmten Modusgruppennamen beträgt 20. Die CNOS-Verarbeitung verwendet den Parameter DSESLIM als Standardwert; er kann jedoch für jeden Partner durch Absetzen des Befehls AGW CNOS auf der virtuellen AVS-Maschine außer Kraft gesetzt werden. Wenn der Partner die im Parameter DSESLIM, DMINWNL oder DMINWNR angegebene Anzahl Sitzungen nicht unterstützen kann, vereinbart der CNOS-Prozeß für diese Parameter neue Werte, die für den Partner akzeptabel sind.

**EAS=9999**

Ein Schätzwert für die Gesamtzahl Sitzungen, die von dieser VTAM-LU benötigt werden.

**MODETAB=RDBMODES**

Der Name der VTAM-Modustabelle ist RDBMODES. Diese Tabelle enthält alle Modusnamen, die dieser Gateway zur Verbindung mit anderen Partnern der verteilten Datenbank verwenden kann.

**SECACPT=ALREADYV**

Dieser Parameter für die Sicherheitsakzeptanz gibt die höchste Sicherheitsstufe für den APPC-Dialog an, die von diesem Gateway beim Empfang einer von einem fernen Partner abgesetzten Anforderung für verteilte Datenbanken unterstützt wird. SECACPT=ALREADYV wird empfohlen. Die Option ALREADYV unterstützt folgende Sicherheitsstufen:

- SECURITY=NONE - eine Anforderung, die keine Sicherheitsinformationen enthält. DB2 für VM weist DRDA-Anforderungen zurück, die diese Sicherheitsstufe verwenden.

- SECURITY=PGM - eine Anforderung, in der die Benutzer-ID und das Kennwort des Requesters enthalten sind. DB2 für VM akzeptiert DRDA-Anforderungen, die diese Sicherheitsstufe verwenden.
- SECURITY=SAME - gibt eine bereits überprüfte Anforderung an, die nur die Benutzer-ID des Requesters enthält.

**SYNCLVL=SYNCPT**

Der Parameter SYNCLVL gibt die Stufe der Synchronisationsunterstützung für AVS an. Der Wert SYNCPT gibt an, daß die Synchronisationsstufen NONE, CONFIRM und SYNCPT unterstützt werden. Wenn der AVS-Gateway für verteilte DRDA-2-Arbeitseinheiten auf einem Server unter DB2 für VM verwendet werden soll, geben Sie den Wert SYNCPT an. Wenn KEINE verteilten Arbeitseinheiten verwendet werden, geben Sie den Wert CONFIRM an (d. h. NONE und CONFIRM werden unterstützt, SYNCPT aber nicht).

**VERIFY=NONE**

Gibt die Sicherheitsstufe für SNA-Sitzungen (Partner-LU-Prüfung) an, die für dieses System mit DB2 für VM erforderlich ist. Der Wert NONE gibt an, daß keine Partner-LU-Prüfung erforderlich ist.

DB2 für VM schränkt Ihre Auswahl für das Schlüsselwort VERIFY nicht ein, aber die von Ihnen verwendete VTAM-Version kann diese Auswahl beeinflussen. In einem nicht gesicherten Netzwerk wird für DB2 für VM die Einstellung VERIFY=REQUIRED empfohlen. Wenn Sie VERIFY=OPTIONAL angeben, führt VTAM die Partner-LU-Prüfung nur für solche Partner durch, die diese Unterstützung bereitstellen. VERIFY=REQUIRED bewirkt, daß VTAM diejenigen Partner zurückweist, die keine Partner-LU-Prüfung ausführen können.

**VPACING=2**

Dieser Parameter stellt den Nachrichtendosierungszähler für Sitzungen ein, der für Übertragungen zwischen der Partner-LU und diesem Gateway verwendet wird. Die Sitzungsnachrichtendosierung ist für Systeme mit verteilten Datenbanken von großer Bedeutung.

2. Aktivieren Sie den Gateway.

   Die Gateway-Aktivierung wird von der virtuellen AVS-Maschine aus durchgeführt, die auf demselben Host wie der Anwendungs-Requester unter DB2 für VM (oder auf einem anderen Host im selben TSAF-Verbund) ausgeführt wird. Fügen Sie einen Befehl AGW ACTIVATE GATEWAY GLOBAL in das Profil der AVS-Maschine ein, oder setzen Sie

diesen Befehl interaktiv über die Konsole der AVS-Maschine ab, damit der Gateway bei jedem Starten der AVS-Maschine aktiviert wird.

3. Verwenden Sie den Befehl AGW CNOS, um die Anzahl Sitzungen zwischen dem Gateway und jeder seiner Partner-LUs zu vereinbaren.

   Stellen Sie sicher, daß der Wert für MAXCONN im Benutzerverzeichnis der AVS-Gateway-Maschine groß genug ist, um die Gesamtzahl erforderlicher Sitzungen zu unterstützen.

   Setzen Sie den Befehl AGW DEACTIVE GATEWAY auf der virtuellen AVS-Maschine ab, um den Gateway zu inaktivieren. Die Gateway-Definition bleibt erhalten. Der Gateway kann mit dem Befehl AGW ACTIVATE GATEWAY GLOBAL jederzeit erneut aktiviert werden.

   Beschreibungen der AVS-Befehlsformate finden Sie im Handbuch *VM/ESA Connectivity Planning, Administration and Operation*.

4. Stellen Sie sicher, daß die VTAM-NETID während der Installation für das Datenbankverwaltungssystem von DB2 für VM definiert wird.

   Die NETID für den Host, auf dem sich der Anwendungs-Requester befindet (oder für andere Hosts im selben TSAF-Verbund), wird von VTAM bereitgestellt, sobald die Anforderung in das Netzwerk gelangt. Die NETID wird in der CMS-Datei SNA NETID gespeichert und befindet sich auf der Produktionsplatte von DB2 für VM, auf die der Anwendungs-Requester zugreift. Der Anwendungs-Requester verwendet diese NETID zur Generierung der LUWID, die bei jedem Datenaustausch mit übertragen wird.

### Definieren der fernen Systeme

Sie müssen die fernen Systeme definieren, indem Sie die LU-Namen registrieren, die VTAM die Lokalisierung der gewünschten Netzwerkzieladresse ermöglichen. Beim Starten identifiziert AVS die globalen Gateway-Namen (LU-Namen), die zum Weiterleiten von SQL-Anforderungen über das Netzwerk an VTAM zur Verfügung stehen. Ein Gateway-Name muß innerhalb einer Gruppe von LU-Namen, die vom lokalen VTAM-System erkannt werden, eindeutig sein, damit eingehende und abgehende Anforderungen zum richtigen LU-Namen weitergeleitet werden. Dies ist das beste Verfahren, um die Eindeutigkeit von Gateway-Namen im Benutzernetzwerk sicherzustellen. Außerdem vereinfacht es den Definitionsprozeß für VTAM-Ressourcen.

Wenn eine Anwendung unter DB2 für VM Daten von einem fernen System anfordert, sucht DB2 für VM im Kommunikationsverzeichnis von CMS nach den folgenden Informationen, die sich auf das ferne System beziehen:

- Gateway-Name (Name der lokalen LU)
- Name der fernen LU
- Name des fernen Transaktionsprogramms (TPN)
- Erforderliche Dialogsicherheitsstufe für den Anwendungs-Server

- Benutzer-ID zum Identifizieren des Anwendungs-Requesters auf dem Anwendungs-Server
- Kennwort, das den Anwendungs-Requester zum Zugreifen auf den Anwendungs-Server berechtigt
- Modusname, der die Sitzungskenndaten für die Verbindung mit dem Anwendungs-Server beschreibt
- RDB_NAME

Das CMS Communications Directory ist eine CMS-Datei mit dem Dateityp NAMES, die von einem Administrator für das System mit DB2 für VM erstellt und verwaltet wird. Als Administrator können Sie diese Datei mit XEDIT erstellen und die gewünschten Einträge zum Identifizieren aller potentiellen DRDA-Partner hinzufügen. Jeder Verzeichniseintrag besteht aus einer Reihe von Kennzeichen mit den zugeordneten Werten. Abb. 31 zeigt einen Beispieleintrag. Beim Ausführen eines Suchvorgangs wird der Suchbegriff mit dem Wert des Kennzeichens :dbname jedes Eintrags der Datei verglichen, bis eine Übereinstimmung gefunden wird oder das Ende der Datei erreicht ist. In dem Beispiel in Abb. 31 möchte der Verkaufsmanager von Toronto einen monatlichen Verkaufsbericht für die Geschäftsstelle in Montreal durch Fernzugriff auf die Datenbank MONTREAL_SALES erstellen.

```
  SCOMDIR  NAMES    A1  V 132  Trunc=132 Size=10 Line=1 Col=1 Alt=8
====>
00001  :nick.MTLSALES
00002                 :tpn.SALES
00003                 :luname.TORGATE MTLGATE
00004                 :modename.BATCH
00005                 :security.PGM
00006                 :userid.SALESMGR
00007                 :password.GREATMTH
00008                 :dbname.MONTREAL_SALES
00009
```

*Abbildung 31. Beispieleintrag in einem CMS Communications Directory*

Das Kennzeichen :tpn identifiziert den Namen des Transaktionsprogramms, durch das der Anwendungs-Server aktiviert wird. Der erste Teil des Kennzeichens :luname gibt den AVS-Gateway (die lokale LU) an, über den auf das SNA-Netzwerk zugegriffen wird. Der zweite Teil gibt den Namen der fernen LU an. Das Kennzeichen :modename gibt den VTAM-Modus an, der die Kenndaten der zwischen den lokalen und fernen LUs zugeordneten Sitzungen definiert. Beispiele für diese Kenndaten sind Größe der Anforderungseinheit (Request Unit, RU), Nachrichtendosierung und Serviceklasse (Class of Service, COS). Das Kennzeichen :security gibt die Sicherheitsstufe an, die für den Dialog zwischen Anwendungs-Requester und Anwendungs-Server verwendet werden soll.

Das CMS Communications Directory befindet sich auf einem öffentlichen Systemdatenträger, auf den alle Anwendungs-Requester in einem bestimmten VM-System zugreifen können. Jedes Programm oder Produkt, das Fernzugriff über VTAM benötigt, kann das CMS Communications Directory verwenden.

Sie können auf zwei Ebenen des CMS Communications Directoryses zugreifen: die Systemebene und die Benutzerebene. Beispielsweise können Sie auf Systemebene ein Verzeichnis auf einem öffentlichen Systemdatenträger erstellen, auf den alle Anwendungs-Requester in einem bestimmten VM-System zugreifen können. Außerdem können Sie ein eigenes Verzeichnis auf Benutzerebene erstellen, um vorhandene Einträge zu überschreiben oder neue Einträge hinzuzufügen, die in dem Verzeichnis auf Systemebene nicht enthalten sind. Das Verzeichnis auf Benutzerebene wird zuerst durchsucht. Bleibt die Suche erfolglos, wird anschließend das Verzeichnis auf Systemebene durchsucht. Das Verzeichnis auf Systemebene ist eine Erweiterung des Verzeichnisses auf Benutzerebene. Es wird nur durchsucht, wenn die gesuchten Werte im Verzeichnis auf Benutzerebene nicht gefunden werden.

Jedes dieser Verzeichnisse wird gegenüber der Anwendung identifiziert und durch den CMS-Befehl SET COMDIR aktiviert. Beispielsweise können Sie mit der folgenden Befehlsfolge sowohl das Verzeichnis auf Systemebene als auch das Verzeichnis auf Benutzerebene (auf den Miniplatten S bzw. A) identifizieren, jedoch nur das Verzeichnis auf Systemebene für Suchvorgänge aktivieren:

```
SET COMDIR FILE SYSTEM SCOMDIR NAMES S

SET COMDIR FILE USER UCOMDIR NAMES A

SET COMDIR OFF USER
```

Eine ausführliche Beschreibung des CMS-Kommunikationsverzeichnisses finden Sie im Handbuch *VM/ESA Connectivity Planning, Administration and Operation*. Der CMS-Befehl SET COMDIR wird im Handbuch *VM/ESA CMS Command Reference* beschrieben.

### Definieren des Kommunikationssubsystems

In der VM-Umgebung wird die Kommunikationsverwaltung von einer Kombination mehrerer Komponenten ausgeführt. Die an der Kommunikation zwischen gleichartigen DRDA-Systemen beteiligten Komponenten sind APPC/VM, das CMS-Kommunikationsverzeichnis, TSAF, AVS und VTAM.

APPC/VM ist die LU 6.2-API auf Assemblerebene, die vom Anwendungs-Requester unter DB2 für VM zur Anforderung von Übertragungsdiensten verwendet wird. Das CMS Communications Directory stellt die Weiterleitungs- und Sicherheitsinformationen des verteilten Partnersystems zur Verfügung. AVS aktiviert den Gateway und wandelt den abgehenden APPC/VM-Datenfluß in einen APPC/VTAM-Datenfluß sowie den eingehenden APPC/VTAM-Datenfluß in einen APPC/VM-Datenfluß um.

APPC/VM, TSAF und AVS sind davon abhängig, daß die Anforderungen durch das CMS-Kommunikationsverzeichnis, VTAM und *IDENT an den richtigen DRDA-Partner weitergeleitet werden.

Damit VTAM mit den im CMS-Kommunikationsverzeichnis angegebenen Partneranwendungen kommunizieren kann, müssen Sie folgende Informationen bereitstellen:

1. Definieren Sie die LU-Namen aller Anwendungs-Requester und Anwendungs-Server für VTAM. Plazierung und Syntax dieser Definitionen hängen davon ab, wie das ferne System logisch und physisch mit dem VTAM-System verbunden ist.
2. Erstellen Sie in der VTAM-Modustabelle für jeden Modusnamen, der im CMS-Kommunikationsverzeichnis angegeben ist, einen Eintrag. Diese Einträge beschreiben die Größe der Anforderungseinheit (Request Unit, RU), die Größe des Nachrichtendosierungsfensters und die Serviceklasse für einen bestimmten Modusnamen.
3. Wenn Sie die Partner-LU-Prüfung (Sicherheit auf Sitzungsebene) verwenden wollen, stellen Sie VTAM- und RACF-Profile (oder gleichwertige Angaben) für den Prüfalgorithmus bereit.

**Überlegungen zur AVS-Sitzungsbegrenzung:** Wenn ein Anwendungs-Requester über AVS mit einem fernen Anwendungs-Server kommuniziert, wird eine Verbindung eingeleitet. Wird durch diese Verbindung die geltende Sitzungsbegrenzung überschritten, versetzt AVS die Verbindung in den Wartestatus, bis wieder eine Sitzung verfügbar wird. Sobald eine Sitzung verfügbar wird, ordnet AVS die zurückgestellte Verbindung dieser Sitzung zu, und die Steuerung wird an die Benutzeranwendung zurückgegeben. Zur Vermeidung dieser Situation sollten Sie die maximale Auslastung im voraus einplanen, indem Sie im Grenzwert für die Sitzungsbegrenzung einige zusätzliche Verbindungen zulassen. Stellen Sie sicher, daß der Wert für MAXCONN im Benutzerverzeichnis der AVS-Maschine groß genug ist, um die maximale Auslastung durch APPC/VM-Verbindungen zu unterstützen.

### Einstellen von RU-Größe und Nachrichtendosierung

Die in der VTAM-Modustabelle von Ihnen definierten Einträge geben die Größe der Anforderungseinheiten (RU-Größe) und die Zähler für die Nachrichtendosierung (Pacing Count) an. Fehlende oder fehlerhafte Definitionen für diese Werte können sich nachteilig auf alle VTAM-Anwendungen auswirken.

Bedenken Sie bei der Wahl der RU-Größe, Sitzungsbegrenzungen und Nachrichtendosierungszähler, welche Auswirkungen diese Werte auf das vorhandene SNA-Netzwerk haben können. Überprüfen Sie beim Installieren eines neuen verteilten Datenbanksystems die folgenden Punkte:

- Stellen Sie für VTAM-CTC-Verbindungen sicher, daß der Parameterwert für MAXBFRU groß genug ist, um Ihre RU-Größe plus der 29 Byte, die VTAM als SNA-Anforderungs- und Übertragungskopf hinzufügt, zu verarbeiten. MAXBFRU wird in Einheiten von 4 KB gemessen, d. h. der Wert für MAXBFRU muß mindestens 2 betragen, um eine RU-Größe von 4 KB zu unterstützen.
- Stellen Sie für NCP-Verbindungen sicher, daß der Wert für MAXDATA groß genug ist, um Ihre RU-Größe plus 29 Byte zu verarbeiten. Wenn Sie als RU-Größe 4 KB angegeben haben, muß der Wert für MAXDATA mindestens 4125 betragen.

  Wenn Sie den NCP-Parameter MAXBFRU angeben, wählen Sie einen Wert aus, der für Ihre RU-Größe plus 29 Byte ausreicht. Bei NCP definiert der Parameter MAXBFRU die Anzahl der VTAM-E/A-Puffer für die PIU. Wenn Sie für IOBUF eine Puffergröße von 441 angeben, reicht die Einstellung MAXBFRU=10 für die RU-Größe 4 KB aus, weil 10*441 größer ist als 4096+29.
- Im Handbuch *DRDA Connectivity Guide* wird beschrieben, wie Sie die Auswirkung der verteilten Datenbank auf den VTAM-IOBUF-Pool einschätzen können. Wenn ein zu großer Anteil der IOBUF-Poolressource belegt ist, hat dies nachteilige Auswirkungen auf die Leistung aller VTAM-Anwendungen.

#### Vorbereiten des Anwendungs-Requesters unter DB2 für VM

Für den Anwendungs-Requester unter DB2 für VM ist DRDA-Unterstützung möglicherweise nicht installiert. Führen Sie folgende Schritte aus, um den Anwendungs-Requester unter DB2 für VM auf DRDA-Kommunikation vorzubereiten:

1. Installieren Sie die DRDA-Unterstützung mit Hilfe der ausführbaren Datei ARISDBMA:
   - Verwenden Sie „ARISDBMA DRDA(ARAS=Y)”, wenn Sie Unterstützung für den Requester und Server installieren.
   - Verwenden Sie „ARISDBMA DRDA(AR=Y)”, wenn Sie Unterstützung lediglich für den Requester installieren.

   Weitere Informationen finden Sie im Handbuch *DB2 for VM System Administration*.
2. Stellen Sie ARISQLLD LOADLIB von DB2 für VM nach dem Absetzen des Befehls ARISDBMA wieder her. Weitere Informationen finden Sie im Kapitel *Using a DRDA Environment* des Handbuchs *DB2 for VM System Administration*.

### Gewährleisten der Sicherheit

Wenn ein fernes System die Verarbeitung für verteilte Datenbanken im Auftrag einer SQL-Anwendung ausführt, muß es in der Lage sein, die Sicherheits-

anforderungen des Anwendungs-Requesters, des Anwendungs-Servers und des verwendeten Netzwerks zu erfüllen. Diese Anforderungen betreffen einen oder mehrere der folgenden Bereiche:

- Auswählen von Endbenutzernamen
- Sicherheitsparameter des Netzwerks
- Sicherheit des Datenbankmanagers
- Von einem externen Sicherheitssubsystem implementierte Sicherheit

### Auswählen von Endbenutzernamen

In SQL und LU 6.2 wird jedem Endbenutzer eine Benutzer-ID aus 1 bis 8 Zeichen zugeordnet. Der Wert dieser Benutzer-ID muß zwar innerhalb eines bestimmten Betriebssystems, jedoch nicht unbedingt im gesamten SNA-Netzwerk eindeutig sein. Beispielsweise kann es im System TORONTO einen Benutzer mit dem Namen JONES und im System MONTREAL einen weiteren Benutzer dieses Namens geben. Wenn diese beiden Benutzer dieselbe Person sind, entsteht dadurch kein Konflikt. Ist jedoch der Benutzer JONES in TORONTO nicht identisch mit dem Benutzer JONES in MONTREAL, kann das SNA-Netzwerk (und können folglich auch die verteilten Datenbanksysteme innerhalb dieses Netzwerks) den Benutzer JONES in TORONTO nicht von dem Benutzer JONES in MONTREAL unterscheiden. Wird diese Situation nicht durch geeignete Maßnahmen verhindert, können diese beiden Benutzer die Berechtigungen des jeweils anderen benutzen.

Zur Vermeidung solcher Namenskonflikte unterstützt DB2 für VM die Umsetzung für Endbenutzernamen. Das System erzwingt jedoch keine Umsetzung von Benutzer-IDs. Wenn eine solche, vom System erzwungene Umsetzung erforderlich ist, stellen Sie sicher, daß auf dem Anwendungs-Server die richtige Namensumsetzung für eingehende Anforderungen ausgeführt wird.

*Namensumsetzung für abgehende Anforderungen* wird mit Hilfe des CMS Communications Directoryses durchgeführt. Ein Eintrag im CMS Communications Directory muß die Angabe `:security.PGM` enthalten. In diesem Fall werden die entsprechenden Werte der Kennzeichen :userid und :password in der Verbindungsanforderung an den fernen Standort (Anwendungs-Server) übermittelt.

Durch Erstellen des in Abb. 32 auf Seite 158 gezeigten Eintrags wird der Benutzer mit der ID JONES auf dem lokalen System (TORONTO) auf die Benutzer-ID JONEST abgebildet, wenn sich dieser Benutzer am Anwendungs-Server MONTREAL_SALES_DB im System MONTREAL anmeldet. Auf diese Weise wird die Mehrdeutigkeit der Benutzer-ID behoben.

```
  UCOMDIR  NAMES    A1  V 132  Trunc=132 Size=10 Line=1 Col=1 Alt=8
====>
00001  :nick.MTLSALES
00002                 :tpn.SALES
00003                 :luname.TORLU MTLGATE
00004                 :modename.BATCH
00005                 :security.PGM
00006                 :userid.JONEST
00007                 :password.JONESPW
00008                 :dbname.MONTREAL_SALES_DB
00009
```

*Abbildung 32. Namensumsetzung für abgehende Anforderungen*

### Netzwerksicherheit

Nach dem Auswählen des Endbenutzernamens, der den Anwendungs-Requester am fernen Standort (Anwendungs-Server) repräsentiert, muß der Anwendungs-Requester die erforderlichen LU 6.2-Netzwerksicherheitsinformationen zur Verfügung stellen. LU 6.2 stellt die folgenden drei Hauptsicherheitseinrichtungen für das Netzwerk zur Verfügung:

- Sicherheit auf Sitzungsebene, angegeben durch den Parameter VERIFY in der VTAM-Anweisung APPL
- Sicherheit auf Dialogebene, angegeben im CMS Communications Directory
- Verschlüsselung

Der Anwendungs-Server ist zuständig für die Verwaltung der Datenbankressourcen und legt deshalb auch fest, welche Netzwerksicherheitseinrichtungen vom Anwendungs-Requester bereitgestellt werden müssen. Sie müssen die Sicherheitsanforderungen des Anwendungs-Servers im Kommunikationsverzeichnis des Anwendungs-Requesters aufzeichnen, indem Sie den entsprechenden Wert für das Kennzeichen :security einstellen.

Folgende Sicherheitsoptionen werden von DRDA für die SNA-Dialogsicherheit unterstützt:

**SECURITY=SAME**

Diese Option wird auch als bereits geprüfte Sicherheit bezeichnet, weil nur die ID des Endbenutzers (Anmelde-ID) zum fernen System gesendet wird. Das Kennwort wird nicht gesendet. Diese Stufe der Dialogsicherheit wird verwendet, wenn im Kommunikationsverzeichnis des Anwendungs-Requesters für den betreffenden Anwendungs-Server `:security.SAME` angegeben ist. Bei Verwendung dieser Option wird keine Umsetzung von Endbenutzernamen für abgehende Anforderungen ausgeführt. Die Anmelde-ID des CMS-Benutzers wird als Benutzer-ID zum fernen DRDA-Standort übermittelt. Das Kennzeichen :userid im CMS Communications Directory wird für :security.SAME ignoriert.

**SECURITY=PGM**

Diese Option bewirkt, daß ID und Kennwort des Endbenutzers zur Gültigkeitsprüfung an das ferne System (Anwendungs-Server) gesendet werden. Diese Sicherheitsoption wird verwendet, wenn im Eintrag des CMS Communications Directoryses des Anwendungs-Requesters `:security.PGM` angegeben ist. Bei Verwendung dieser Option wird die Umsetzung von Endbenutzernamen für abgehende Anforderungen ausgeführt.

DB2 für VM bietet keine Unterstützung für Kennwortverschlüsselung. Das Kennwort kann im Kennzeichen `:password` angegeben oder mit Hilfe einer Verzeichnisanweisung APPCPASS im Benutzerverzeichniseintrag des Endbenutzers gespeichert werden. Das Angeben in der Anweisung APPCPASS bietet die größtmögliche Kennwortsicherheit. Wenn das Kennwort nicht als Eintrag im CMS Communications Directory angegeben ist, wird der Benutzereintrag im Systemverzeichnis (VM-Verzeichnis) nach einer Anweisung APPCPASS durchsucht.

**Anweisung APPCPASS:** Die Anweisung APPCPASS des VM-Systems bietet die größtmögliche Sicherheit für die Kombination aus Benutzer-ID und Kennwort, die vom Anwendungs-Requester zum Herstellen einer Verbindung zu einem Anwendungs-Server verwendet wird. Die Flexibilität der Anweisung APPCPASS ermöglicht das Speichern von Sicherheitsinformationen auf folgende Arten:

- **Benutzer-ID und Kennwort:** In diesem Fall müssen die Kennzeichen :userid und :password im CMS Communications Directory leer sein.
- **Nur Benutzer-ID:** In diesem Fall muß das Kennzeichen :userid im CMS Communications Directory leer sein, und das Kennzeichen :password muß auf das Kennwort des Benutzers gesetzt sein.
- **Nur Kennwort:** In diesem Fall muß das Kennzeichen :password im CMS Communications Directory leer sein, und das Kennzeichen :userid muß auf die ID des Benutzers gesetzt sein.

Abb. 33 auf Seite 160 zeigt den Fall, in dem die Benutzer-ID im Kommunikationsverzeichnis des Benutzers und das Kennwort im VM-Verzeichniseintrag des Benutzers gespeichert ist. Die Benutzer-ID im Kommunikationsverzeichniseintrag ist auf MTLSOU gesetzt, aber das Kennwort ist nicht definiert. Das Kennwort ist im VM-Verzeichniseintrag des Benutzers gespeichert.

```
  UCOMDIR  NAMES    A1  V 132  Trunc=132 Size=8  Line=1 Col=1 Alt=8
====>
00001  :nick.MTLSALES
00002                 :tpn.SALES
00003                 :luname.TORGATE MTLGATE
00004                 :modename.BATCH
00005                 :security.PGM
00006                 :userid.MTLSOU
00007                 :password.
00008                 :dbname.MONTREAL_SALES_DB
00009
```

*Abbildung 33. Beispieleintrag im Kommunikationsverzeichnis ohne definiertes Kennwort*

Wenn APPC/VM die Verbindung zwischen dem Anwendungs-Requester und dem Anwendungs-Server mit der Dialogsicherheit SECURITY=PGM einleitet, liest APPC/VM die Werte der Kennzeichen :userid und :password und leitet sie an den Anwendungs-Server weiter. Wenn ein oder beide Kennzeichen leer sind, wird der VM-Verzeichniseintrag des Benutzers nach den fehlenden Informationen durchsucht. In diesem Fall muß der VM-Verzeichniseintrag die folgende Anweisung APPCPASS enthalten:

```
APPCPASS TORGATE MTLGATE MTLSOU Q6VBN8XP
```

Diese Anweisung teilt APPC/VM mit, daß der Benutzer (Anwendungs-Requester), der die Verbindung über den (lokalen) AVS-Gateway TORGATE, die Partner-LU namens MTLGATE und die Benutzer-ID MTLSOU anfordert, das Kennwort Q6VBN8XP an den Anwendungs-Server senden soll. Der Benutzer ist durch diese beiden Identifikationsangaben auf dem Anwendungs-Server bekannt.

Das Einfügen der Anweisung APPCPASS im VM-Verzeichnis ist nicht Sache des Endbenutzers. Der Endbenutzer muß vielmehr eine entsprechende Anfrage an den VM-Systemprogrammierer richten.

Weitere Informationen zur Sicherheit auf Dialogebene und zur Anweisung APPCPASS finden Sie im Handbuch *VM/ESA Connectivity Planning, Administration, and Operation*.

### Sicherheit des Datenbankmanagers

Im Rahmen der umfassenden DRDA-Sicherheitseinrichtungen für verteilte Datenbanken kann der Anwendungs-Requester mit darüber entscheiden, welche Benutzer Anforderungen an verteilte Datenbanken absetzen dürfen. In DB2 für VM kann der Anwendungs-Requester in folgenden drei Bereichen an den Sicherheitsfunktionen für verteilte Datenbanken beteiligt sein:

**Umsetzung von Benutzernamen für abgehende Anforderungen**

Mit der Umsetzung von Benutzernamen für abgehende Anforderungen können Sie den Zugriff auf einen bestimmten Anwendungs-Server anhand der Identität des Endbenutzers einschränken, von dem die

Anforderung ausgeht. DB2 für VM versucht zunächst, den Namen des Endbenutzers umzusetzen, bevor die Anforderung an den fernen Standort übermittelt wird. Die sicherste Methode bietet jedoch eine Herkunftsüberprüfung und Namensumsetzung für eingehende Anforderungen durch den Anwendungs-Server, weil Benutzer von VM-Anwendungs-Requestern die Möglichkeit haben, die Namensumsetzung für abgehende Anforderungen über ihr CMS-Kommunikationsverzeichnis außer Kraft zu setzen.

**Vorverarbeiten von Anwendungen**

Endbenutzer können eine Vorverarbeitung von Anwendungen für einen bestimmten Anwendungs-Server mit Hilfe der Prozedur SQLPREP EXEC von DB2 für VM oder über den Befehl RELOAD PACKAGE des Dienstprogramms DBSU (Database Service Utility) veranlassen. DB2 für VM schränkt die Verwendung dieser Services nicht ein. Führt ein Endbenutzer die Vorverarbeitung einer Anwendung durch, so wird er dadurch zum Eigner des resultierenden Pakets.

**Ausführen von Anwendungen**

Damit ein Endbenutzer von DB2 für VM eine ferne Anwendung ausführen kann, muß der betreffende Endbenutzer am fernen Standort (Anwendungs-Server) über die Berechtigung zum Ausführen des fernen Pakets verfügen, das dieser Anwendung zugeordnet ist. Der Ersteller (Eigner) des Pakets ist automatisch berechtigt, das Paket auszuführen. Anderen Endbenutzern kann die Berechtigung zum Ausführen des Pakets durch die Anweisung GRANT EXECUTE von DB2 für VM erteilt werden. Auf diese Weise kann der Eigner einer Anwendung für verteilte Datenbanken individuell steuern, welche Benutzer die Anwendung verwenden dürfen.

### Sicherheitssubsystem

Das externe Sicherheitssubsystem auf VM-Systemen wird entweder durch RACF oder durch gleichwertige Produkte bereitgestellt, die eine mit RACF kompatible Schnittstelle zur Verfügung stellen. Der Anwendungs-Requester unter DB2 für VM hat keine direkte Schnittstelle zum externen Sicherheitssubsystem. Das externe Sicherheitssubsystem wird nicht zum Bereitstellen von Kennwörtern für die Dialogsicherheit verwendet. Wenn Sie Sicherheit auf Sitzungsebene verwenden, wird das externe Sicherheitssubsystem von VTAM aufgerufen, um die Gültigkeit des Namens der fernen LU im Rahmen der Partner-LU-Gültigkeitsprüfung zu überprüfen.

## Darstellen von Daten

Der Anwendungs-Requester muß über die entsprechenden Standardwerte für CHARNAME und CCSID verfügen. Durch Auswählen der korrekten Werte

wird die Integrität der Darstellung von Zeichendaten sichergestellt und zugleich der mit der CCSID-Umwandlung verbundene Systemaufwand reduziert.

Beispiel: Wenn Ihr Anwendungs-Requester unter DB2 für VM mit Codepage 37 und Zeichensatz 697(CP/CS 37/697) für amerikanisches Englisch generiert wird, sollte der Anwendungs-Requester ENGLISH als Standardwert für CHARNAME definieren. Der Grund hierfür ist, daß CP/CS 37/697 der CCSID 37 entspricht, die ihrerseits dem Wert ENGLISH für CHARNAME entspricht.

Der Standardwert für CHARNAME eines neu installierten oder durch Migration umgestellten Systems ist INTERNATIONAL mit CCSID 500. Dies ist für Ihre Installation wahrscheinlich *nicht* korrekt. Verwenden Sie den folgenden Befehl, um die Werte für die aktuellen Standard-CCSIDs anzuzeigen:

```
SQLINIT QUERY
```

Der korrekte CCSID-Wert für den Anwendungs-Requester wird von den Umsetzungstabellen auf dem Anwendungs-Server möglicherweise nicht unterstützt. Wenn dies der Fall ist, können Sie die Verbindung auf eine der folgenden Arten herstellen:

- Veranlassen Sie, daß die CCSID-Umsetzungstabelle des Anwendungs-Servers aktualisiert wird, so daß die Umsetzung zwischen der Standard-CCSID des Anwendungs-Requesters und der Standard-CCSID des Anwendungs-Servers unterstützt wird (Informationen zum Hinzufügen der Unterstützung für die CCSID-Umsetzung finden Sie in den Produkthandbüchern des Anwendungs-Servers).
- Definieren Sie für den Anwendungs-Requester eine andere Standard-CCSID, die vom Anwendungs-Server unterstützt wird. Dies kann zu Problemen bei der Datenintegrität führen. Deshalb sollten Sie sich vorher unbedingt über die möglichen Auswirkungen im klaren sein. Ein Beispiel für eine solche Auswirkung könnte wie folgt aussehen:

  Ein Anwendungs-Requester verwendet eine mit CP/CS 37/697 definierte Steuereinheit. Der Anwendungs-Server unterstützt keine Umsetzung von CCSID 37, er unterstützt jedoch eine Umsetzung von CCSID 285 (die Einstellung CHARNAME UK-ENGLISH (britisches Englisch) für SQL/DS).

  Wenn der Standardwert des Anwendungs-Requesters in britisches Englisch für CHARNAME (mit der CCSID 285) geändert wird, kann die Datenintegrität nicht aufrecht erhalten werden. Wenn der Anwendungs-Server beispielsweise ein Zeichen für britisches Pfund (Â) übermittelt, zeigt der Anwendungs-Requester statt dessen ein Dollarzeichen ($) an. Bei anderen Zeichen können sich ebenfalls Veränderungen ergeben.

Zum Ändern des CCSID-Werts eines Anwendungs-Requesters unter DB2 für VM müssen Sie den Parameter CHARNAME der Prozedur SQLINIT EXEC angeben. Ausführlichere Informationen hierzu finden Sie im Handbuch *DB2 for VM System Administration*.

Der korrekte CCSID-Wert für den Anwendungs-Server wird von den Umsetzungstabellen auf dem Anwendungs-Requester möglicherweise nicht unterstützt. Wenn dies der Fall ist, können Sie die Verbindung auf eine der folgenden Arten herstellen:

- Aktualisieren Sie die vom Anwendungs-Requester verwendete Umsetzungstabelle, so daß die Umsetzung zwischen der Standard-CCSID des Anwendungs-Servers und der Standard-CCSID des Anwendungs-Requesters unterstützt wird. Ausführliche Informationen zum Aktualisieren der Systemtabelle SYSTEM.SYSSTRINGS finden Sie im Handbuch *DB2 for VM System Administration*. Diese Tabelle wird zur Erstellung der CMS-Datei ARISSTR MACRO verwendet, die vom Anwendungs-Requester zur Unterstützung der CCSID-Umsetzung verwendet wird.
- Veranlassen Sie, daß die Standard-CCSID des Anwendungs-Servers geändert wird. Dies sollte nur durchgeführt werden, wenn es wirklich erforderlich ist. Beachten Sie dabei unbedingt die angestrebte Zielsetzung bei der Auswahl der Standard-CCSID des Anwendungs-Servers. Die Standard-CCSID des Anwendungs-Servers wirkt sich auf alle Anwendungs-Requester aus, die eine Verbindung zu diesem Server herstellen, sowie auf die für den Anwendungs-Server verwendete Bediener-Workstation und auf die in Tabellen auf dem Anwendungs-Server gespeicherten Daten.

## Prüfliste zum Aktivieren eines DRDA-Anwendungs-Requesters unter DB2 für VM

Die folgende Prüfliste faßt die erforderlichen Schritte zum Aktivieren eines DRDA-Anwendungs-Requesters für DRDA-Kommunikation zusammen, ausgehend von der Annahme, daß Ihr VM-System mit der Zugriffsmethode ACF/VTAM für die Fernverarbeitung installiert ist und daß die zur Kommunikation mit den fernen Systemen erforderlichen VTAM-Definitionen (z. B. NCP-Definitionen) vollständig vorhanden sind.

1. Definieren Sie den lokalen AVS-Gateway für VTAM.
2. Installieren Sie DRDA-Unterstützung auf dem Anwendungs-Requester unter DB2 für VM mit Hilfe der ausführbaren Datei ARISDBMA.
3. Definieren Sie ein CMS-Kommunikationsverzeichnis, und fügen Sie dem VM-Verzeichnis auf der VM-Anwendungsmaschine andere erforderliche APPCPASS-Anweisungen hinzu. Aktivieren Sie das Kommunikationsverzeichnis mit dem CMS-Befehl SET COMDIR.
4. Starten Sie VTAM und AVS, damit VM-Anwendungen über das SNA-Netzwerk kommunizieren können.

5. Setzen Sie die ausführbare Datei SQLINIT ab, geben Sie die Standarddatenbank, das zu verwendende Protokoll und die zu verwendenden CCSIDs mit Hilfe der Parameter DBNAME, PROTOCOL und CHARNAME an.
6. Bereiten Sie Anwendungen auf dem fernen Server vor.

## Konfigurieren des Anwendungs-Servers in einer VM-Umgebung

Die Anwendungs-Server-Unterstützung von DB2 für VM ermöglicht die Verwendung von DB2 für VM als Server für DRDA-Anwendungs-Requester. Folgende Anwendungs-Requester können mit einem Anwendungs-Server unter DB2 für VM verbunden werden:

- Requester unter DB2 für VM
- Requester unter DB2 Universal Database für OS/390
- Requester unter OS/400
- Requester unter DB2 für AIX
- Jeder Anwendungs-Requester mit einem DB2-Produkt, wie DB2 CONNECT, und jedes andere Produkt, das die Protokolle für DRDA-Anwendungs-Requester unterstützt und Verbindung zu einem Anwendungs-Server unter DB2 für VM herstellen kann

Jedem mit einem Anwendungs-Server unter DB2 für VM verbundenen Anwendungs-Requester ermöglicht der Anwendungs-Server unter DB2 für VM den Zugriff auf Datenobjekte (z. B. Tabellen), die lokal auf dem Anwendungs-Server unter DB2 für VM gespeichert sind. Der Anwendungs-Requester muß ein Paket erstellen, das die SQL-Anweisungen der Anwendung auf dem Anwendungs-Server unter DB2 für VM enthält, damit die Verbindung hergestellt werden kann.

Damit der Anwendungs-Server unter DB2 für VM Anforderungen für verteilte Datenbanken verarbeiten kann, müssen Sie folgende Schritte ausführen:

1. Definieren des Anwendungs-Servers für das lokale Kommunikationssubsystem
2. Gewährleisten der erforderlichen Sicherheit
3. Gewährleisten der Datendarstellung

## Bereitstellen von Netzwerkinformationen

### Definieren des Anwendungs-Servers

Damit der Anwendungs-Server Anforderungen für verteilte Datenbanken empfangen kann, definieren Sie den Anwendungs-Server für das lokale Kommunikationssubsystem, und ordnen Sie einen eindeutigen Wert für RDB_NAME zu.

Gehen Sie wie folgt vor, um den Anwendungs-Server zu definieren:

1. Definieren Sie den Anwendungs-Server unter DB2 für VM für das SNA-Netzwerk. Wählen Sie den Gateway-Name und den RDB_NAME-Wert für den Anwendungs-Server unter DB2 für VM aus, und befolgen Sie anschließend die Prozeduren im Abschnitt „Bereitstellen von Netzwerkinformationen" auf Seite 148. Der von Ihnen für DB2 für VM ausgewählte RDB_NAME muß allen Benutzern (Anwendungs-Requestern) mitgeteilt werden, die möglicherweise eine Verbindung zu diesem Anwendungs-Server unter DB2 für VM herstellen wollen.

   Die Netzwerk-ID (NETID) ist in VTAM als Startparameter definiert, und alle Anforderungen für verteilte Datenbanken des Anwendungs-Requesters werden korrekt dorthin weitergeleitet. Der Anwendungs-Server unter DB2 für VM legt die NETID nicht fest.

   Der Anwendungs-Server unter DB2 für VM legt nicht fest, welcher Gateway zum Weiterleiten eingehender Anforderungen für verteilte Datenbanken des Anwendungs-Requesters verwendet wird. Dies wird stets vom Anwendungs-Requester gesteuert. Für den Anwendungs-Requester unter DB2 für VM werden diese Angaben im CMS Communications Directory durch die Kennzeichen :luname und :tpn festgelegt.

   Der Anwendungs-Requester muß einen AVS-Gateway auswählen, der mit dem Parameter SYNCLVL=SYNCPT für VTAM definiert wurde, damit der Anwendungs-Server unter DB2 für VM verteilte Arbeitseinheiten unterstützen kann. Stellen Sie sicher, daß der AVS-Gateway für die Unterstützung verteilter Arbeitseinheiten definiert wurde.
2. Erstellen Sie auf dem VM-System einen CRR Recovery Server zum Verwalten verteilter Arbeitseinheiten für Anwendungs-Server unter DB2 für VM. Führen Sie dazu die im Handbuch *VM/ESA Installation Guide* beschriebenen Schritte aus, um die von IBM gelieferten Server und Dateipools nach der Installation zu laden. Dazu gehört das Definieren eines CRR-Servers (VMSERVR) und eines CRR-Dateipools (VMSYSR). Stellen Sie sicher, daß

beim Starten von CRR Recovery Server ein LUNAME angegeben wird, der dem Namen eines AVS-Gateways entspricht, für den SYNCLVL=SYNCPT angegeben wurde.

3. Stellen Sie sicher, daß das Benutzerverzeichnis für die Anwendungs-Server-Maschine eine IUCV-Anweisung *IDENT enthält. Diese Anweisung identifiziert den Server als eine globale Ressource.
4. Erstellen Sie in der VTAM-Modusnamentabelle für jeden Modusnamen, der von einem Anwendungs-Requester angefordert wird, einen Eintrag. Diese Einträge beschreiben die Sitzungskenndaten wie RU-Größe, Nachrichtendosierungszähler und Serviceklasse für einen bestimmten Modusnamen.
5. Definieren Sie Sitzungsbegrenzungen für die Anwendungs-Requester, eine die Verbindung zu dem Anwendungs-Server unter DB2 für VM herstellen. Die VTAM-Anweisung APPL definiert Standardwerte für die Sitzungsbegrenzungen aller Partnersysteme. Verwenden Sie zum Definieren eindeutiger Standardwerte für einen bestimmten Partner den Befehl AGW CNOS auf der virtuellen AVS-Maschine, die am Standort des Anwendungs-Servers läuft. (Sitzungsbegrenzungen werden normalerweise vom Anwendungs-Requester angefordert.)

   Bedenken Sie beim Auswählen der RU-Größe, Sitzungsbegrenzungen und Nachrichtendosierungszähler, welche Auswirkungen diese Werte auf den VTAM-Pool IOBUF haben.

**Zuordnen des Server-Namens zu einer RESID:** Ressourcen-ID (RESID) ist die VM-Bezeichnung für Transaktionsprogrammname. In der VM-Umgebung wird dafür normalerweise ein alphanumerischer Name mit einer Länge von bis zu 8 Byte definiert. In der Regel wird eine RESID definiert, die mit dem Server-Namen identisch ist, um die Systemverwaltung zu vereinfachen.
Abb. 34 zeigt eine Beispieldatei RESID NAMES.
In Abb. 33 auf Seite 160 finden Sie den Kommunikationsverzeichniseintrag, in

```
  RESID  NAMES    A1  V 132  Trunc=132 Size=4  Line=1 Col=1 Alt=3
====>
00001  :nick.MTLTPN
00002                 :dbname.MONTREAL_SALES_DB
00003                 :resid.SALES
00004
```

*Abbildung 34. Beispieldatei RESID NAMES*

dem dieser Wert für dbname und diese RESID (als TPN) definiert sind. Wenn der Name des Anwendungs-Servers nicht mit der RESID identisch sein darf, verwendet der Anwendungs-Server unter DB2 für VM die Datei RESID NAMES zur Zuordnung der Namen. Diese Zuordnung ist erforderlich, wenn Sie:

- eine RESID verwenden, die sich vom Server-Namen unterscheidet

- einen Server-Namen verwenden, der länger als 8 Zeichen ist
- eine RESID mit einem 4 Byte langen hexadezimalen Wert verwenden (z. B. den DRDA-Standard-TPN X'07F6C4C2')

Bei der Installation wird standardmäßig der Server-Name verwendet, der in der Prozedur SQLDBINS EXEC als RESID angegeben ist. Wenn Sie einen Zuordnungseintrag in der Datei RESID NAMES erstellen wollen, geben Sie den Parameter RESID in der Prozedur SQLDBINS an.

Wenn Sie die Datenbank mit SQLSTART DB(server_name) starten, fragt DB2 für VM die entsprechende RESID ab und informiert das VM-System darüber, daß diese Ressource von VM gesteuert werden soll. Wird in der Datei RESID NAMES kein Eintrag gefunden, geht DB2 für VM davon aus, daß die RESID mit dem Server-Namen identisch ist, und instruiert VM entsprechend. Weitere Informationen finden Sie im Handbuch *DB2 for VM System Administration*.

#### Vorbereiten und Starten des Anwendungs-Servers unter DB2 für VM

Für den Anwendungs-Server unter DB2 für VM ist DRDA-Unterstützung möglicherweise nicht installiert. Führen Sie folgende Schritte aus, um den Anwendungs-Server unter DB2 für VM auf DRDA-Kommunikation vorzubereiten:

1. Installieren Sie die DRDA-Unterstützung mit Hilfe der ausführbaren Datei ARISDBMA:
   - Verwenden Sie „ARISDBMA DRDA(ARAS=Y)”, wenn Sie Unterstützung für den Requester und Server installieren.
   - Verwenden Sie „ARISDBMA DRDA(AS=Y)”, wenn Sie Unterstützung lediglich für den Server installieren.

   Weitere Informationen finden Sie im Handbuch *VM/ESA System Administration*.
2. Stellen Sie ARISQLLD LOADLIB von DB2 für VM nach dem Absetzen des Befehls ARISDBMA wieder her. Weitere Informationen finden Sie im Kapitel *Using a DRDA Environment* des Handbuchs *DB2 for VM System Administration*.

### Gewährleisten der Sicherheit

Wenn ein Anwendungs-Requester eine Anforderung für eine verteilte Datenbank an den Anwendungs-Server unter DB2 für VM weiterleitet, können dabei folgende Sicherheitsaspekte eine Rolle spielen:

- Umsetzung von Endbenutzernamen für eingehende Anforderungen
- Sicherheitsparameter des Netzwerks
- Sicherheit des Datenbankmanagers
- Von einem externen Sicherheitssubsystem implementierte Sicherheit

### Endbenutzernamen

In SQL und LU 6.2 wird jedem Endbenutzer eine Benutzer-ID mit 1 bis 8 Byte zugeordnet. Der Wert dieser Benutzer-ID muß zwar innerhalb eines bestimmten Betriebssystems, jedoch nicht unbedingt im gesamten SNA-Netzwerk eindeutig sein. Zur Behebung von Namenskonflikten kann DB2 für VM wahlfrei die von AVS bereitgestellte Umsetzungsfunktion für Benutzer-IDs verwenden, allerdings nur unter folgenden Bedingungen:

- Der Anwendungs-Server unter DB2 für VM muß in einer VM/ESA-Umgebung ausgeführt werden
- Die eingehende Verbindungsanforderung muß über einen AVS-Gateway weitergeleitet werden
- Der Partner-Anwendungs-Requester muß die Dialogsicherheit SECURITY=SAME verwenden (in der SNA-Terminologie auch als *bereits geprüft* bezeichnet)

Wenn eine Verbindung über AVS mit der Option SECURITY=SAME zu einem Server weitergeleitet wird, ist die AVS-Umsetzung für Benutzer-IDs erforderlich. Der auf der AVS-Maschine abgesetzte Befehl AGW ADD USERID muß den Benutzern, die über eine bestimmte ferne LU oder einen bestimmten AVS-Gateway eine Verbindung anfordern, die Zugriffsberechtigung erteilen. Es muß eine Zuordnung für alle eingehenden LUs und Benutzer-IDs vorhanden sein, die mit SECURITY=SAME eine Verbindung herstellen. Der Befehl ist flexibel anwendbar, d. h. Sie können alle Benutzer-IDs von einer bestimmten LU bzw. alle fernen LUs generisch akzeptieren. Sie haben aber auch die Möglichkeit, nur eine bestimmte Gruppe von Benutzer-IDs von einer bestimmten LU zu akzeptieren.

Wenn Sie den Befehl AGW ADD USERID zum Berechtigen der eingehenden (bereits geprüften) Benutzer-IDs auf der lokalen AVS-Maschine verwenden, wird vom Host keine Gültigkeitsprüfung durchgeführt. Dies bedeutet, daß die Verbindung auch dann akzeptiert wird, wenn die berechtigte ID auf dem Host möglicherweise nicht vorhanden ist.

Die aktuelle Berechtigung der AVS-Benutzer-ID kann auf folgende zwei Arten geändert werden:

- Durch Stoppen von AVS mit dem Befehl AGW STOP; dadurch wird die Berechtigung der Benutzer-ID vollständig auf Leerwerte gesetzt.
- Durch Löschen der Benutzer-ID mit dem Befehl AGW DELETE USERID

Am Beispiel identischer Benutzer-IDs in verschiedenen Städten wird deutlich, wie die AVS-Umsetzungsfunktion einen Namenskonflikt beheben kann. Angenommen im System von Toronto gibt es eine Benutzer-ID JONES, und im System von Montreal existiert ein weiterer Benutzer mit derselben ID. Wenn JONES von Montreal auf Daten im System von Toronto zugreifen möchte, kann durch folgende Maßnahmen im System von Toronto der mögliche

Namenskonflikt behoben und verhindert werden, daß JONES von Montreal die für JONES von Toronto erteilten Zugriffsberechtigungen verwenden kann:

1. Der AVS-Bediener muß mit dem Befehl AGW ADD USERID die ID des Benutzers in Montreal in eine lokale Benutzer-ID umsetzen. Beispiel: Wenn der Bediener den Befehl `AGW ADD USERID MTLGATE JONES MONTJON` absetzt, wird der Benutzer von Montreal im System von Toronto als MONTJON identifiziert. Wenn alle Benutzer von Montreal (über die ferne LU MTLGATE) die Verbindung herstellen können und lokal anhand ihrer fernen Benutzer-IDs identifiziert werden, muß der Bediener den Befehl `AGW ADD USERID MTLGATE * =` absetzen. Diese AVS-Befehle können auch dem AVS-Profil hinzugefügt werden, damit sie beim Starten von AVS automatisch ausgeführt werden.
2. Der Datenbankadministrator muß mit dem Befehl GRANT von DB2 für VM eine Reihe von Berechtigungen speziell für die umgesetzte Benutzer-ID (in diesem Fall für MONTJON) erteilen.

Diese Aktionen können auch auf dem System von Montreal ausgeführt werden, um sicherzustellen, daß JONES von Toronto beim Zugriff auf ferne Daten im System von Montreal die für JONES von Montreal erteilten Berechtigungen nicht benutzen kann.

Die AVS-Befehle zur Unterstützung der Umsetzung für Benutzer-IDs sind im Handbuch *VM/ESA Connectivity Planning, Administration and Operation* beschrieben.

### Netzwerksicherheit

LU 6.2 stellt die folgenden drei Hauptsicherheitseinrichtungen für das Netzwerk zur Verfügung:

- Sicherheit auf Sitzungsebene
- Sicherheit auf Dialogebene
- Verschlüsselung

Eine Beschreibung zum Angeben der Sicherheit auf Sitzungsebene für DB2 für VM finden Sie in „Netzwerksicherheit” auf Seite 158. Der Anwendungs-Server unter DB2 für VM verwendet die Sicherheit auf Sitzungsebene in derselben Weise wie der Anwendungs-Requester unter DB2 für VM.

Der Anwendungs-Requester kann entweder eine bereits geprüfte Benutzer-ID (SECURITY=SAME) oder eine Benutzer-ID mit Kennwort (SECURITY=PGM) senden. Wenn eine Benutzer-ID mit Kennwort gesendet wird, überprüft CP, RACF oder ein gleichwertiges Produkt diese Angaben anhand des VM-Verzeichnisses auf dem Anwendungs-Server-Host. Schlägt die Gültigkeitsprüfung fehl, wird die Verbindungsanforderung zurückgewiesen, andernfalls

wird sie akzeptiert. Enthält die Anforderung nur eine Benutzer-ID, akzeptiert DB2 für VM die Anforderung, ohne die Benutzer-ID auf ihre Gültigkeit zu prüfen.

**Anmerkung:** DB2 für VM stellt keine Verschlüsselungsfunktion bereit, weil VM/ESA Verschlüsselung nicht unterstützt.

### Sicherheit des Datenbankmanagers

Der Anwendungs-Server unter DB2 für VM überprüft, ob die von VM angegebene Benutzer-ID über die Berechtigung CONNECT zum Zugreifen auf die Datenbank verfügt, und weist die Verbindung zurück, wenn diese Berechtigung nicht vorliegt.

Als Eigner der Datenbankressourcen steuert der Anwendungs-Server unter DB2 für VM die Datenbanksicherheitsfunktionen für SQL-Objekte, die sich auf dem Anwendungs-Server unter DB2 für VM befinden. Der Zugriff auf die von DB2 für VM verwalteten Objekte wird durch eine Reihe von Zugriffsrechten gesteuert, die der Administrator des Systems mit DB2 für VM oder der Eigner des jeweiligen Objekts den Benutzern erteilen kann. Der Anwendungs-Server unter DB2 für VM steuert zwei Objektklassen:

- **Pakete:** Einzelne Endbenutzer erhalten die Berechtigung zum Erstellen, Ersetzen und Ausführen der Pakete durch die Anweisung GRANT von DB2 für VM. Wenn ein Endbenutzer ein Paket erstellt, erhält dieser Benutzer automatisch die Berechtigung zum Ausführen und Ersetzen eines Pakets. Anderen Endbenutzern muß mit der Anweisung GRANT EXECUTE ausdrücklich die Berechtigung zum Ausführen eines Pakets auf dem Anwendungs-Server unter DB2 für VM erteilt werden. Das Zugriffsrecht RUN kann für einzelne Endbenutzer oder für PUBLIC erteilt werden, d. h. alle Benutzer dürfen das Paket ausführen.

  Nach der Vorverarbeitung einer Anwendung in DB2 für VM enthält das Paket die im Anwendungsprogramm enthaltenen SQL-Anweisungen. Diese SQL-Anweisungen werden wie folgt klassifiziert:

  – **Statisches SQL:** Dies bedeutet, die SQL-Anweisung und die SQL-Objekte, auf die in der Anweisung verwiesen wird, sind der Anwendung zum Zeitpunkt der Vorverarbeitung bekannt. Der Ersteller des Pakets muß über die Berechtigung zum Ausführen für jede der statischen SQL-Anweisungen in dem Paket verfügen.

    Wenn ein Endbenutzer das Recht zum Ausführen eines Pakets erhält, verfügt er damit automatisch über die Berechtigung zum Ausführen aller statischen SQL-Anweisungen in dem Paket. Dies bedeutet, daß Endbenutzer keine DB2-Tabellenzugriffsrechte auf dem VM-System benötigen, wenn das Paket ausschließlich statische SQL-Anweisungen enthält.

  – **Dynamisches SQL:** Bezeichnet eine SQL-Anweisung, die vor Ausführung des Pakets nicht bekannt ist. Die SQL-Anweisung wird von dem betreffenden Programm erstellt und durch die Anweisung SQL PREPARE

oder die Anweisung EXECUTE IMMEDIATE für DB2 für VM dynamisch vorverarbeitet. Wenn ein Endbenutzer eine dynamische SQL-Anweisung ausführt, muß er über die erforderlichen Tabellenzugriffsrechte zum Ausführen der SQL-Anweisung verfügen. Da die SQL-Anweisung bei der Erstellung des Pakets noch nicht bekannt ist, wird dem Endbenutzer die erforderliche Berechtigung vom Paketeigner nicht automatisch erteilt.

- **SQL-Objekte:** Dies können Tabellen, Sichten und Synonyme sein. Benutzern von DB2 für VM können verschiedene Berechtigungsstufen zum Erstellen, Löschen, Ändern oder Lesen einzelner SQL-Objekte erteilt werden. Diese Berechtigung ist für die Vorverarbeitung statischer SQL-Anweisungen und zum Ausführen dynamischer SQL-Anweisungen erforderlich.

#### Sicherheitssubsystem

Die Verwendung dieses Subsystems durch den Anwendungs-Server unter DB2 für VM ist wahlfrei. Wenn der Anwendungs-Server die Identität des LU-Namens des Anwendungs-Requesters überprüfen muß, ruft VTAM das Sicherheitssubsystem auf, um den Datenaustausch für die Partner-LU-Prüfung auszuführen. Die Entscheidung über die Ausführung der Partner-LU-Prüfung wird unter Berücksichtigung des Werts getroffen, der im Parameter VERIFY der VTAM-Anweisung APPL für den Gateway angegeben ist, über den der Anwendungs-Server unter DB2 für VM eingehende Anforderungen für verteilte Datenbanken empfängt.

Das Sicherheitssubsystem kann von CP auch aufgerufen werden, um die Benutzer-ID und das Kennwort zu prüfen, die vom Anwendungs-Requester gesendet wurden. Wenn RACF als Sicherheitssubsystem verwendet wird und Sie nicht über ein RACF-Systemprofil verfügen, wird die Gültigkeitsprüfung von RACF ausgeführt. Wenn Sie über ein RACF-Systemprofil (z. B. RACFPROF) verfügen, führen Sie die folgenden Instruktionen aus, um diese Gültigkeitsprüfung von RACF anzufordern:

```
RALTER VMXEVENT RACFPROF DELMEM (APPCPWVL/NOCTL

RALTER VMXEVENT RACFPROF ADDMEM (APPCPWVL/CTL

SETEVENT REFRESH RACFPROF
```

### Darstellen von Daten

Sie müssen für CHARNAME und CCSID die für Ihre Installation am besten geeigneten Standardwerte auswählen. Durch Auswählen der optimalen Werte wird die Integrität der Darstellung von Zeichendaten sichergestellt und zugleich der mit der CCSID-Umwandlung verbundene Systemaufwand reduziert.

Beispiel: Wenn auf Ihren Anwendungs-Server unter DB2 für VM nur lokale Benutzer von Workstations aus zugreifen, deren Steuereinheiten mit Codepage 37 und Zeichensatz 697 (CP/CS 37/697) für amerikanisches Englisch generiert

werden, sollten Sie für den Anwendungs-Requester ENGLISH als Standardwert für CHARNAME definieren. Der Grund hierfür ist, daß CP/CS 37/697 der CCSID 37 entspricht, die ihrerseits dem Wert ENGLISH für CHARNAME entspricht.

Zur Vermeidung unnötiger CCSID-Umwandlung sollten Sie für den Anwendungs-Server dieselbe Standard-CCSID auswählen wie für diejenigen Anwendungs-Requester, die am häufigsten auf Ihren Anwendungs-Server zugreifen.

Das folgende Beispiel zeigt, welche Konflikte zwischen diesen beiden Zielsetzungen auftreten können:

- Ein Anwendungs-Server hat weniger als fünf lokale Anwendungs-Requester (für VM-Anwendungs-Requester würde der Protokollparameter auf SQL/DS gesetzt) und zahlreiche (etwa 100) Anwendungs-Requester, die über das DRDA-Protokoll auf den Anwendungs-Server zugreifen. Die Steuereinheiten der lokalen Anwendungs-Requester sind mit CP/CS 37/697 definiert. Die fernen Anwendungs-Requester verwenden CCSID 285.

  Wenn der Standardwert des Anwendungs-Servers für CHARNAME auf ENGLISH gesetzt ist, bleibt damit die Datenintegrität für die lokalen Anwendungs-Requester gewahrt, aber für alle fernen Anwendungs-Requester ist zusätzlicher Systemaufwand für die CCSID-Umwandlung erforderlich.

  Wenn der Standardwert des Anwendungs-Servers für CHARNAME auf UK-ENGLISH gesetzt ist, wird zusätzlicher Systemaufwand bei der CCSID-Umwandlung für alle fernen Anwendungs-Requester vermieden, aber es entstehen Probleme bei der Datenintegrität für die lokalen Anwendungs-Requester (bestimmte Daten werden auf den lokalen Anwendungs-Requestern nicht korrekt angezeigt, z. B. wird anstelle des Zeichens für britisches Pfund (£) das Dollarzeichen ($) angezeigt).

Fragen Sie die Tabelle SYSTEM.SYSOPTIONS ab, um die aktuelle CCSID des Systems anzuzeigen. Die Standard-CCSID des Anwendungs-Servers ist normalerweise der Wert für CCSIDMIXED. Wenn dieser Wert Null ist, hat die Standard-CCSID des Systems den Wert für CCSIDSBCS. Die Werte für CHARNAME, CCSIDSBCS, CCSIDMIXED und CCSIDGRAPHIC in dieser Tabelle werden bei jedem Starten der Datenbank mit den verwendeten Systemstandardwerten aktualisiert. Die Werte in dieser Tabelle entsprechen möglicherweise nicht immer den Systemstandardwerten. Ein Benutzer mit der Berechtigung DBA könnte diese Werte geändert haben, obwohl diese Vorgehensweise nicht zu empfehlen ist. Zum Ändern der Standard-CCSID des Anwendungs-Servers müssen Sie den Parameter CHARNAME der Prozedur SQLSTART EXEC beim nächsten Starten des Anwendungs-Servers angeben. Ausführliche Informationen hierzu finden Sie im Handbuch *VM/ESA System Administration*.

Für eine neu installierte Datenbank ist INTERNATIONAL der Standardwert für den Parameter CHARNAME des Anwendungs-Servers, und die Standard-CCSID des Anwendungs-Servers ist 500. Dies ist für Ihr System wahrscheinlich *nicht* korrekt. In einem durch Migration umgestellten System ist ENGLISH der Standardwert für CHARNAME, und die Standard-CCSID ist 37.

## Prüfliste zum Aktivieren eines DRDA-Anwendungs-Servers unter DB2 für VM

Die folgende Prüfliste faßt die zum Aktivieren eines DRDA-Anwendungs-Servers für DRDA-Kommunikation erforderlichen Schritte zusammen, ausgehend von der Annahme, daß Ihr VM-System mit der Zugriffsmethode ACF/VTAM für die Fernverarbeitung installiert ist und daß die zur Kommunikation mit den fernen Systemen erforderlichen VTAM-Definitionen (z. B. NCP-Definitionen) vollständig vorhanden sind.

1. Definieren Sie den lokalen AVS-Gateway für VTAM.
2. Erstellen Sie einen CRR Recovery Server. Stellen Sie sicher, daß der von CRR Recovery Server angegebene LUNAME mit dem Namen eines AVS-Gateways übereinstimmt, der SYNCLVL=SYNCPNT-Dialoge verwalten kann.
3. Installieren Sie DRDA-Unterstützung auf dem Anwendungs-Server unter DB2 für VM mit Hilfe der ausführbaren Datei ARISDBMA.
4. Fügen Sie dem Benutzerverzeichnis auf der VM-Server-Maschine eine IUCV-Anweisung *IDENT hinzu, damit sie sich selbst als globale Ressource angeben kann.
5. Definieren Sie lokale Benutzer-IDs und Kennwörter für CP, die von fernen Anwendungs-Requestern verwendet werden. Falls erforderlich, ordnen Sie fernen Benutzer-IDs mit dem AVS-Befehl AGW ADD USERID lokale VM-Benutzer-IDs zu.
6. Erstellen Sie in der VTAM-Modusnamentabelle für jeden Modusnamen, der von einem Anwendungs-Requester angefordert wird, einen Eintrag.
7. Starten Sie VTAM und AVS, damit VM-Anwendungen über das SNA-Netzwerk kommunizieren können.
8. Definieren Sie Sitzungsbegrenzungen für alle Partnersysteme, auf denen Anwendungs-Requester eingerichtet sind.
9. Starten Sie den Anwendungs-Server unter DB2 für VM mit den Parametern DBNAME, PROTOCOL und SYNCPNT. Stellen Sie nach dem Starten des Datenbankmanagers sicher, daß er sich selbst als globale Ressource angegeben hat.
10. Bereiten Sie Anwendungen auf dem Anwendungs-Server unter DB2 für VM vor.

## DB2 für VSE - Übersicht

In der VSE/ESA-Betriebsumgebung stellt DB2 für VSE die Anwendungs-Server-Funktion für eine DRDA-Umgebung bereit. Die Anwendungs-Requester-Funktion wird nicht bereitgestellt. In diesem Abschnitt werden die verschiedenen Komponenten von DB2 für VSE und von VSE beschrieben, die an der Verarbeitung für verteilte Datenbanken beteiligt sind. Über diese Komponenten kann das Datenbankverwaltungssystem unter DB2 für VSE mit fernen DRDA-Anwendungs-Requestern in einem SNA-Netzwerk kommunizieren.

**CICS(ISC)**
Die CICS-Komponente (CICS - Customer Information Control System) für die Kommunikation zwischen Systemen stellt die SNA-LU 6.2-Funktionen (APPC-Funktionen) für den Anwendungs-Server unter DB2 für VSE zur Verfügung.

**CICS(SPM)**
Die CICS-Komponente zur Synchronisationspunktverwaltung ist integraler Bestandteil der Unterstützung verteilter DRDA-Arbeitseinheiten unter DB2 für VSE. Sie fungiert als Synchronisationspunktteilnehmer und ist für die Koordination der zweiphasigen Festschreibung auf einem VSE/ESA-System zuständig.

**CICS(TRUE)**
Der funktionsbezogene CICS-Benutzerausgang ist eine von der Transaktion AXE (APPC-XPCC-Exchange) verwendete Schnittstelle zum CICS-Synchronisationspunktmanager.

**ACF/VTAM**
CICS(ISC) verwendet VTAM für VSE zum Einrichten bzw. Binden von LU-LU-Sitzungen für/an ferne Systeme. DB2 für VSE verwendet LU 6.2-Basisdialoge über diese Sitzungen, um mit fernen DRDA-Anwendungs-Requestern zu kommunizieren.

**AXE** Die Transaktion AXE (APPC-XPCC-Exchange) ist eine CICS-Transaktion, die von dem fernen DRDA-Anwendungs-Requester aktiviert wird. Sie bestimmt den Leitweg für den DRDA-Datenstrom zwischen dem fernen Anwendungs-Requester und dem Anwendungs-Server unter DB2 für VSE mit Hilfe der CICS-LU 6.2-Unterstützung und der VSE-XPCC-Funktionen (Cross Partition Communication Protocol).

**Verzeichnis DBNAME**
Das Verzeichnis DBNAME (Verzeichnis der Datenbanknamen) ordnet eine eingehende Dialogzuordnungsanforderung einem vorgegebenen Anwendungs-Server zu, der vom eingehenden TPN definiert wird. Weitere Informationen finden Sie im Handbuch *SQL/DS System Administration Guide for VSE*.

**XPCC** Die partitionsübergreifende DFV-Steuerung (XPCC - Cross Partition Communication Control) ist die VSE-Makroschnittstelle, die die Datenübertragung zwischen VSE-Partitionen ermöglicht.

## Anwendungs-Server - Beispiel für Kommunikationsdatenfluß

Abb. 35 zeigt, welche Rolle die einzelnen Komponenten bei der Einrichtung der Verbindung (Link) zwischen den Anwendungs-Servern unter DB2 für VSE und den fernen Anwendungs-Requestern spielen.

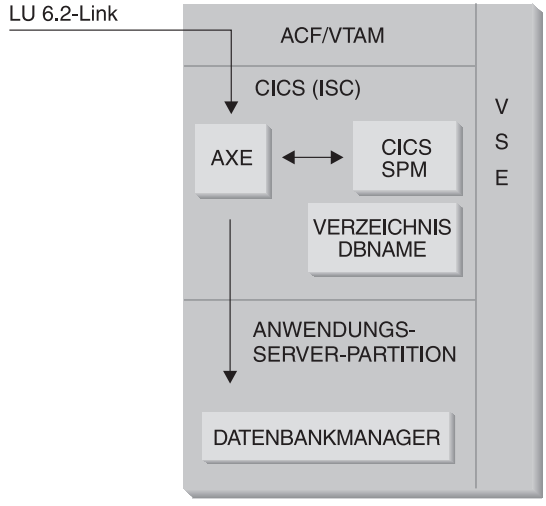


*Abbildung 35. Zugriff auf den Anwendungs-Server*

Der Anwendungs-Requester setzt ein APPC-Verb ALLOCATE mit einem bestimmten LU- und Transaktionsprogrammnamen (TPN) ab, um einen LU 6.2-Dialog mit dem Anwendungs-Server einzurichten. Mit dem LU-Namen wird die Anforderung ALLOCATE über VTAM an CICS weitergeleitet. Nach dem Empfang des Verbs ALLOCATE prüft CICS, ob eine Transaktion AXE mit diesem TPN definiert ist, und führt eine CICS-Anmeldung durch. Wenn für die CICS-Verbindung die Dialogsicherheitsstufe VERIFY definiert ist, werden vom Anwendungs-Requester sowohl Benutzer-ID als auch Kennwort erwartet und beim Anmelden verwendet. Die CICS-Anmeldetabelle (DFHSNT) muß mit diesen Angaben (Benutzer-ID und Kennwort) aktualisiert werden, damit die Verbindung akzeptiert wird. Wenn die Sicherheitsstufe IDENTIFY definiert ist, ist nur die Benutzer-ID erforderlich, und CICS überläßt die Sicherheitsprüfung dem fernen System. Ist die Sicherheitsprüfung erfolgreich, startet CICS die Transaktion AXE, um Anforderungen und Antworten zwischen dem Anwendungs-Requester und einem Anwendungs-Server zu übermitteln. Der vom Anwendungs-Requester verwendete TPN muß im Verzeichnis DBNAME von DB2 für VSE als Zeiger auf einen im Betrieb befindlichen Server unter DB2 für VSE innerhalb des VSE-Systems definiert sein.

Wenn der Anwendungs-Requester Unterstützung für verteilte Arbeitseinheiten in Anspruch nehmen will, gibt er im APPC-Verb ALLOCATE für SYNCLEVEL den Wert SYNCPT an. Nach dem Starten der Transaktion AXE fragt der Anwendungs-Requester CICS ab, um den Wert für SYNCLVL im Dialog festzustellen. Wenn der Wert SYNCPT ist, geschieht folgendes:

- Falls erforderlich, aktiviert die Transaktion AXE Unterstützung für TRUE, damit sie mit dem CICS-Synchronisationspunktmanager kommunizieren kann.
- Die Transaktion registriert die logische Arbeitseinheit für den CICS-Synchronisationspunktmanager.

### Einschränkungen

Im Unterschied zu seinem VM-Gegenstück akzeptiert der Anwendungs-Server unter DB2 für VSE DRDA-Daten von fernen Anwendungs-Requestern. Private Protokolle werden nicht unterstützt. Daher können VM-Anwendungs-Requester auf einen VSE-Server mit PROTOCOL=SQLDS nicht zugreifen.

Der DRDA-Server von DB2 für VSE kann nicht durch gemeinsame Benutzung von VSE-Gastmaschinen Anforderungen von fernen Anwendungs-Requestern an einen Server unter DB2 für VM weiterleiten. Solche Anforderungen müssen direkt an den DRDA-Server unter DB2 für VM übermittelt werden.

## Startparameter für den Anwendungs-Server

### Parameter RMTUSERS

Durch Angeben des Parameters RMTUSERS beim Starten des Anwendungs-Servers kann der Datenbankadministrator die maximale Anzahl ferner Anwendungs-Requester festlegen, die eine Verbindung zu dem Server herstellen dürfen. Dieser Wert ist vergleichbar mit dem Wert für MAXCONN im VM-Verzeichnis der Server-Maschine mit der Datenbank unter DB2 für VM. Dieser Parameter ermöglicht eine gleichmäßige Aufteilung der Transaktionsfolge auf lokale und ferne Verarbeitung.

Wenn der Wert für RMTUSERS größer ist als die Anzahl verfügbarer Agenten von DB2 für VSE (definiert durch NCUSER), müssen einige ferne Benutzer warten, bis ein Agent von DB2 für VSE ihre Anforderungen bearbeiten kann. Normalerweise wird ein Agent von DB2 für VSE einem wartenden Benutzer erneut zugeordnet, sobald eine logische Arbeitseinheit (Logical Unit of Work, LUW) beendet ist. Der Anwendungs-Server unter DB2 für VSE unterstützt privilegierten Zugriff, d. h. ein ferner Benutzer kann einen Agenten von DB2 für VSE für mehrere LUWs bis zum Ende des Dialogs reservieren.

### Parameter SYNCPNT

Dieser Parameter gibt an, ob ein Synchronisationspunktmanager (SPM) zum Koordinieren von verteilten DRDA-2-Arbeitseinheiten für das Lesen und Schreiben auf mehreren Systemen verwendet wird.

Wenn Y angegeben wird, verwendet der Server einen Synchronisationspunktmanager (sofern möglich), um zweiphasige Festschreibungen und Resynchronisationsfunktionen zu koordinieren. Wenn N angegeben wird, verwendet der Anwendungs-Server keinen SPM, um zweiphasige Festschreibungen durchzuführen. Wenn N angegeben wird, ist der Anwendungs-Server auf Arbeitseinheiten für Lesen auf mehreren Systemen und Schreiben auf einem einzigen System begrenzt, und der Server kann das System sein, auf das geschrieben wird. Wenn Y angegeben wird, für den Anwendungs-Server jedoch kein Synchronisationspunktmanager zur Verfügung steht, wird der Server so betrieben, als ob N angegeben wurde.

Die Standardeinstellung ist SYNCPNT=Y, wenn RMTUSERS größer als Null ist. Bei Verwendung der Einstellung RMTUSERS=0 wird der Parameter SYNCPNT auf N gesetzt.

## Konfigurieren des Anwendungs-Servers in einer VSE-Umgebung

Die Anwendungs-Server-Unterstützung von DB2 für VSE ermöglicht die Verwendung von DB2 für VSE als Server für DRDA-Anwendungs-Requester. Folgende Anwendungs-Requester können mit einem Anwendungs-Server unter DB2 für VSE verbunden werden:

- Requester unter DB2 für VM
- Requester unter DB2 Universal Database für OS/390
- Requester unter DB2
- Requester unter OS/400
- Jeder Anwendungs-Requester mit einem DB2-Produkt, einschließlich DB2 CONNECT, und jedes andere Produkt, das die Protokolle für DRDA-Anwendungs-Requester unterstützt und eine Verbindung zu einem Anwendungs-Server unter DB2 für VSE herstellen kann

### Bereitstellen von Netzwerkinformationen

Folgende Schritte sind erforderlich, um die Netzwerkverbindung zum VSE-Anwendungs-Server herzustellen:

1. Einrichten der CICS-LU 6.2-Sitzungen mit den fernen Systemen
2. Definieren des Anwendungs-Servers

#### Einrichten von CICS-LU 6.2-Sitzungen

Der Anwendungs-Server unter DB2 für VSE kommuniziert über CICS-LU 6.2-Verbindungen mit seinem Anwendungs-Requester. Die für diesen Zweck

verwendete CICS-Partition muß über LU 6.2-Verbindungen zu den fernen Systemen verfügen, in denen sich die Anwendungs-Requester befinden. Ausführliche Informationen zum Definieren und Einrichten von CICS-LU 6.2-Verbindungen zu fernen Systemen finden Sie im Handbuch *CICS/VSE Intercommunications Guide*.

**CICS-Installation und Ressourcendefinition für LU 6.2-Verbindung:**

1. Installieren Sie die für ISC (Intersystem Communication) erforderlichen Module.

   Sie müssen folgende Module mit Hilfe von SIT oder durch Überschreiben der während der Initialisierung festgelegten Werte in Ihr System aufnehmen:

   - Die EXEC-Schnittstellenprogramme (geben Sie EXEC=YES an, oder akzeptieren Sie den Standardwert)
   - Die systemübergreifenden Kommunikationsprogramme (geben Sie ISC=YES an)
   - Das durch DFHSG PROGRAM=TCP generierte Workstation-Steuerprogramm (eine Version mit den Angaben ACCMETH=VTAM, CHNASSY=YES und VTAMDEV=LUTYPE6 ist erforderlich)

2. Installieren Sie Unterstützung für die CICS-Funktion zur Neustartresynchronisation (CICS Restart Resynchronization).

   Wenn die CICS-Funktion zur Neustartresynchronisation bei der Installation des CICS-Systems nicht installiert wurde, müssen Sie die folgenden CICS-Tabellen aktualisieren, um die CICS-Funktion zur Neustartresynchronisation (CICS Restart Resynchronization) zu aktivieren:

```
      DFHJCT    Journalsteuertabelle

                Ein Journal für das CICS-Systemprotokoll muß in
                DFHJCT unter Angabe von JFILEID=SYSTEM in einem
                Makro DFHJCT TYPE=ENTRY definiert werden.

   DFHPCT     Programmsteuerungstabelle

                Geben Sie folgendes ein, um den DFHPCT-Eintrag
                für CICS-Neustartresynchronisation zu generieren:

                    DFHPCT TYPE=GROUP,FN=RMI

   DFHPPT     Verarbeitungsprogrammtabelle

                Geben Sie folgendes ein, um den DFHPPT-Eintrag
                für CICS-Neustartresynchronisation zu generieren:

                    DFHPPT TYPE=GROUP,FN=RMI

   DFHSIT     Systeminitialisierungstabelle

                Das Makro DFHSIT muß den Parameter JCT enthalten.
```

```
                Geben Sie JCT=YES bzw. JCT=(jj<,....>) an. Dabei
                ist jj der Parameterwert für SUFFIX aus dem Makro DFHJCT
                TYPE=INITIAL, das die Journaldatei des CICS-
                Systemprotokolls definiert.
```

3. Definieren Sie CICS für VTAM für VSE.

   Damit LU 6.2-Verbindungen unterstützt werden, muß CICS für VTAM für VSE als ein VTAM-Anwendungshauptknoten definiert werden. Der in der VTAM-Anweisung APPL codierte Name des Anwendungshauptknotens ist die APPLID für die in SIT durch den Parameter APPLID angegebene CICS-Partition. Sie ist der von VTAM (und deshalb auch von den CICS-Kommunikationspartnern) zum Identifizieren des CICS-Systems verwendete LU-Name.

   Siehe Abb. 36.

```
                  VBUILD  TYPE=APPL
*************************************************************************
*                                                                       *
*    LU-Definition für VSE SQL/DS-System in Toronto                     *
*                                                                       *
*************************************************************************
VSEGATE  APPL  ACBNAME=VSEGATE,
               AUTH=(ACQ,SPO,VPACE),
               APPC=NO,
               SONSCIP=YES,
ESA=30
               MODTAB=RDBMODES,
               PARSESS=YES,
               VPACING=0
```

*Abbildung 36. VTAM-APPL-Beispieldefinition für CICS*

**AUTH=(ACQ,SPO,VPACE)**
ACQ ermöglicht CICS das Einrichten von LU 6.2-Sitzungen.

SPO ermöglicht CICS das Absetzen des Befehls MODIFY vtam-name USERVAR.

VPACE ermöglicht die Nachrichtendosierung für systemübergreifenden Datenfluß.

**ESA=30**
Diese Option gibt die Anzahl netzwerkadressierbarer Einheiten an, mit denen CICS Sitzungen herstellen kann. Die angegebene Anzahl muß die Gesamtzahl paralleler Sitzungen für dieses CICS-System mit einschließen.

**PARSESS=YES**
Gibt LUTYPE6-Unterstützung für Parallelsitzungen an.

**SONSCIP=YES**

Gibt die Unterstützung für Sitzungsausfallhinweise (Session Outage Notification, SON) an. SON ermöglicht CICS in bestimmten Fällen, eine fehlgeschlagene Sitzung ohne Eingreifen eines Bedieners wiederherzustellen.

**APPC=NO**

Dies ist erforderlich, damit CICS VTAM-Makros verwenden kann. CICS setzt keine APPCCMD-Makroinstruktionen ab.

**Anmerkung:** SYNCLVL=SYNCPT ist nicht erforderlich, weil APPC=NO angegeben ist. CICS verwaltet alle SYNCPT-Aktivitäten auf Synchronisationspunktebene für verteilte Arbeitseinheiten.

4. Definieren Sie Verbindungen zu fernen Systemen mit dem LU 6.2-Protokoll.
   a. Definieren Sie alle fernen LUs für CICS.

      Verwenden Sie dazu den Befehl CEDA DEFINE CONNECTION in RDO (Ressource Definition Online):

      - Geben Sie den fernen LU-Namen im Parameter NETNAME an.
      - Geben Sie PROTOCOL=APPC an, um sicherzustellen, daß LU 6.2-Protokolle verwendet werden.
      - Geben Sie AUTOCONNECT=YES und INSERVICE=YES an, damit die installierte Verbindung automatisch hergestellt wird und die Sitzungen automatisch angefordert werden.
      - Geben Sie die Sicherheit auf Dialogebene mit dem Parameter ATTACHSEC an. ATTACHSEC=IDENTIFY ist die für DRDA erforderliche minimale Sicherheitsstufe.
      - Geben Sie die Sicherheit auf Sitzungsebene mit dem Parameter BINDPASSWORD an. Standardmäßig wird keine Sicherheit auf Sitzungsebene verwendet.

      Weitere Informationen zur Sicherheit auf Dialog- und Sitzungsebene finden Sie in „Gewährleisten der Sicherheit” auf Seite 185.

   b. Definieren Sie LU 6.2-Sitzungsgruppen im fernen System.

      Verwenden Sie den Befehl CEDA DEFINE SESSIONS zum Definieren von Gruppen mit Parallelsitzungen für jede Verbindung zu einem fernen System:

      - Geben Sie den (oben definierten) Namen der Verbindung im Parameter CONNECTION an.
      - Geben Sie den Eintrag für die VTAM-Anmeldemodustabelle im Parameter MODENAME an.
      - Geben Sie mit dem Parameter MAXIMUM folgendes an:
        – Maximale Anzahl Sitzungen

– Maximale Anzahl Sitzungen, die als Konfliktgewinner unterstützt werden sollen

Geben Sie die von der Kommunikationssoftware der DRDA-Anwendungs-Requester, z. B. IBM Communications Server für OS/2, verwendeten Werte an.

Das Angeben eines höheren Werts für SENDSize und RECEIVESize verbessert möglicherweise die Datenübertragungsgeschwindigkeit, erfordert aber auch mehr virtuellen Speicher im Netzwerk. 4 KB ist die Größe aller im SNA-Netzwerk unterstützten Ebenen. Stellen Sie daher die Größe des Sende- und Empfangspuffers beim Konfigurieren des DRDA-Servers auf 4 KB ein. Passen Sie diese Parameter nach der erfolgreichen Herstellung von Verbindungen seitens ferner Benutzer an den optimalen Wert an.

c. Definieren Sie Benutzer-IDs und Kennwörter für CICS.

   Definieren Sie alle Benutzer in der CICS-Anmeldetabelle (DFHSNT). Prüfen Sie die Gültigkeit einer Benutzer-ID durch Ausführen einer CESN-Anmeldung auf einer CICS-Workstation. Die lokale Anmeldung muß erfolgreich verlaufen.

d. Definieren Sie die Lademodule (Phasen) für CICS mit dem Befehl CEDA DEFINE PROGRAM:

   1) ARICAXED - AXE-Transaktion
   2) ARICDIRD - Verzeichnis DBNAME und Suchroutine
   3) ARICDAXD - Transaktionsroutinen DAXP und DAXT
   4) ARICDEBD - Verarbeitungsroutine für Unterstützung von CICS TRUE
   5) ARICDRAD - CICS TRUE selbst
   6) ARICDR2 - DR2DFLT-Steuerblock

   Für jedes dieser Module muß die Option LANGUAGE=ASSEMBLER angegeben werden.

e. Definieren Sie für jeden vom Anwendungs-Requester angegebenen TPN (Transaktionsprogrammnamen) mit dem Befehl CEDA DEFINE TRANSACTION eine Transaktion AXE:

   - Geben Sie den TPN mit dem Parameter TRANSACTION an.
   - Geben Sie die Phase mit PROGRAM=ARICAXED an.
   - Geben Sie einen zweiten hexadezimalen Transaktionsnamen mit dem Parameter XTRANID an.

   Definieren Sie zugleich durch Angabe von PROGRAM=ARICDAXD die Transaktionen DAXP und DAXT.

**Beispieldefinitionen:** Beispieldefinitionen finden Sie im Handbuch *DRDA Connectivity Guide*.

### Definieren des Anwendungs-Servers

1. Aktualisieren Sie das Verzeichnis DBNAME von DB2 für VSE.

   Fügen Sie dem Verzeichnis DBNAME für jede oben definierte Transaktion mit dem Befehl CEDA DEFINE TRANSACTION einen Eintrag hinzu. Wenn LU 6.2-Sitzungen eingerichtet sind, kann ein ferner Anwendungs-Requester einen Dialog mit dem Anwendungs-Server unter DB2 für VSE starten. Dazu wird ein LU 6.2-Dialog mit dem Anwendungs-Server unter Angabe eines TPN (Transaktionsprogrammnamens) zugeordnet. Dieser TPN muß die CICS-Transaktions-ID der Transaktion AXE sein, die für die Weiterleitung von Anforderungen zum oder vom Server unter DB2 für VSE zuständig ist. Der TPN muß sich in demjenigen Verzeichnis DBNAME von DB2 für VSE befinden, das dem Server von DB2 für VSE zugeordnet ist, auf den der Anwendungs-Requester zugreifen soll. Der Administrator der Datenbank unter DB2 für VSE ist für das Aktualisieren des Verzeichnisses DBNAME und das Benachrichtigen der fernen Benutzer über die TPN-Server-Zuordnung zuständig.

   Sowohl der TPN als auch der dazugehörige Server-Name (der im Verzeichnis DBNAME definierte Datenbankname) müssen für den Anwendungs-Requester identifiziert werden:

   - Der Anwendungs-Requester verwendet den TPN zum Initialisieren der AXE-Router-Transaktion.
   - Der Anwendungs-Requester gibt den Server-Namen im einleitenden DRDA-Datenfluß als Zieldatenbanknamen an. Der Server unter DB2 für VSE verwendet diesen Server-Namen, um sicherzustellen, daß der Anwendungs-Requester auf den richtigen Server zugreift. Bei einer Abweichung von Server-Namen erhält der Anwendungs-Requester keinen Zugriff auf den Server, und der Anwendungs-Requester beendet den Dialog.

2. Verwenden Sie die Prozedur ARISBDID zum Erstellen und Assemblieren des Verzeichnisses DBNAME (Member ARISDIRD.A).

Ausführlichere Informationen hierzu finden Sie im Handbuch *DB2 for VSE System Administration*.

### Vorbereiten und Starten des Anwendungs-Servers unter DB2 für VSE

1. Die Transaktion AXE verwaltet ein Fehlerprotokoll in Form einer CICS Temporary Storage Queue mit dem Namen ARIAXELG. Dieses Fehlerprotokoll enthält hilfreiche Fehlernachrichten mit Angaben zu Kommunikationsproblemen und abnormalen Beendigungen der DRDA-Sitzungen. Definieren Sie dieses Protokoll mit CICS TST als wiederherstellbar (recoverable).
2. Führen Sie die Prozedur ARIS342D aus, um die Unterstützung für DRDA-Anwendungs-Server zu installieren.
3. Falls erforderlich, setzen Sie die Transaktion DAXP ab, um die Standardwerte für Kennwort und Sprache anzugeben, die verwendet werden, wenn

Unterstützung für CICS TRUE für einen bestimmten Server aktiviert ist. Ausführlichere Informationen hierzu finden Sie im Handbuch *DB2 for VSE Operation*.

4. Starten Sie DB2 für VM mit den Parametern DBNAME, RMTUSERS und SYNCPNT:
   - Der verwendete DBNAME muß im Verzeichnis DBNAME definiert sein.
   - Der Parameter RMTUSERS muß ungleich Null sein.
   - Geben Sie SYNCPNT=Y an, um die Unterstützung für verteilte Arbeitseinheiten zu aktivieren.
5. Allen fernen Benutzern müssen vom Server unter DB2 für VSE unterschiedliche Berechtigungsstufen erteilt worden sein. Ausführlichere Informationen hierzu finden Sie im Handbuch *DB2 for VSE Database Administration*.

**Fehlerbestimmung:**

- Wenn der Anwendungs-Requester seine Partner-CICS über einen gültigen TPN (definiert im Verzeichnis DBNAME) erreicht hat, wird eine Transaktion AXE gestartet. Der Auslastungszähler im Programm ARICAXED wird um eins erhöht (Überprüfung durch Ausführen von CEMT I PR(ARICAXED) ).
- Führen Sie eine lokale Anmeldung mit der Transaktion CESN unter Verwendung von Benutzer-ID und Kennwort des fernen Benutzers aus, um sicherzustellen, daß in der CICS-Anmeldetabelle eine ferne Benutzer-ID eingerichtet ist. Die lokale Anmeldung muß erfolgreich verlaufen.
- Wenn der Server unter DB2 für VSE aktiv ist und eine Anwendung zuerst Funktionen auf verteilten DRDA-2-Arbeitseinheiten ausführt, wird Unterstützung für TRUE auf einem Server automatisch aktiviert. Sie werden mit der Nachricht ARI0187I darüber informiert, daß die Unterstützung für TRUE erfolgreich aktiviert wurde. Wird allerdings die Nachricht ARI0190E angezeigt, die auf einen Fehler beim Aktivieren von TRUE hinweist, wurden bereits vorher auf der Konsole Fehlernachrichten angezeigt, die Sie sich noch einmal ansehen sollten.
- Wenn das DRDA-Anwendungsprogramm den Prüfcode X'08063426' oder X'FFFE0101' empfängt, weist dies eventuell darauf hin, daß von CICS keine weiteren Sitzungen zur Verfügung gestellt werden können. Dazu kann es kommen, wenn alle Sitzungen entweder im Gebrauch sind oder aufgelöst werden sollen,

UNBIND aber noch nicht beendet wurde. CICS kann keine weiteren Sitzungen zur Verfügung stellen, wenn zu viele gleichzeitig ablaufende Transaktionen mit kurzer Dauer ankommen. Erhöhen Sie in diesem Fall die Anzahl der im Parameter MAXIMUM des Befehls CEDA DEFINE SESSIONS angegebenen Sitzungen, um die Sitzungen zu berücksichtigen, die aufgelöst werden sollen, für die jedoch UNBIND noch nicht beendet wurde.

## Gewährleisten der Sicherheit

Der Anwendungs-Server unter DB2 für VSE ist im Hinblick auf die systemübergreifende Kommunikationssicherheit von CICS abhängig. CICS stellt mehrere Sicherheitsstufen zur Verfügung:

- Bindezeitsicherheit

  Es handelt sich um die CICS-Implementierung der LU-LU-Prüfung auf SNA-LU 6.2-Sitzungsebene. Die Implementierung der Bindezeitsicherheit ist in der LU 6.2-Architektur wahlfrei. Auf der Anwendungs-Server-Seite kann sie beim Definieren einer Verbindung zum Anwendungs-Requester durch Angeben eines Parameters BINDPASSWORD im Befehl CEDA DEFINE CONNECTION aktiviert werden. Auf der Anwendungs-Requester-Seite muß die Partner-LU, die den Anwendungs-Requester bedient, ebenfalls Bindezeitsicherheit unterstützen und dasselbe Kennwort für die Partner-LU-Prüfung verwenden.

  Sie können die Bindezeitsicherheit dazu verwenden, ferne Systeme, die nicht über die entsprechende Berechtigung verfügen, daran zu hindern, Sitzungen mit CICS einzurichten (zu binden).

- Verbindungssicherheit

  Durch die Verbindungssicherheit kann ein fernes System (und der darauf befindliche DRDA-Anwendungs-Requester) auf die Zuordnung einer bestimmten Gruppe von AXE-Transaktionen begrenzt werden.

  Beispielsweise könnten Sie zwei AXE-Transaktionen definieren: AXE2 mit Sicherheitsschlüssel 2 und AXE3 mit Sicherheitsschlüssel 3. Anwendungs-Requestern eines fernen Systems könnte nun die Bedienersicherheit 3 (z. B. mit dem Parameter OPERSECURITY im Befehl CEDA DEFINE SESSION) zugeordnet werden, so daß sie nur eine Verbindung zu AXE3 herstellen können. Dabei könnte AXE3 keine Berechtigung für privilegierten Zugriff auf den Server haben, während AXE2 privilegierten Zugriff erhält. Eine Beschreibung des privilegierten Zugriffs von fernen Anwendungs-Requestern auf den Anwendungs-Server finden Sie im Handbuch *DB2 for VSE System Administration*.

  Informationen zum Aktivieren der Verbindungssicherheit finden Sie im Handbuch *CICS Intercommunication Guide*.

- Benutzersicherheit

Es handelt sich um die CICS-Implementierung der SNA LU 6.2-Sicherheit auf Dialogebene mit Identifikationsprüfung für Endbenutzer.

Bei der Benutzersicherheit wird die Benutzer-ID anhand der CICS-Anmeldetabelle (DFHSNT) geprüft, bevor eine Anforderung zum Starten eines Dialogs akzeptiert wird. Beispielsweise dürfen DRDA-Anwendungs-Requester, die nicht in der CICS-Anmeldetabelle definiert sind, keine Verbindung zu einer AXE-Transaktion herstellen, um einen Dialog mit dem Server unter DB2 für VSE zu starten. Die Benutzersicherheitsstufe für ein fernes System kann mit dem Parameter ATTACHSEC im Befehl CEDA DEFINE CONNECTION aktiviert werden. Folgende drei Stufen stehen für die Verbindungssicherheit zur Verfügung:

- LOCAL: Wird von DRDA nicht unterstützt.
- IDENTIFY: Entspricht SECURITY=SAME (oder: bereits definiert) in der LU 6.2-Terminologie. Bei dieser Sicherheitsstufe „vertraut" CICS darauf, daß das ferne System eine Benutzerprüfung durchführt, bevor Dialoganforderungen für den Server unter DB2 für VSE akzeptiert werden. Bei der CICS-Anmeldung muß nur die Benutzer-ID angegeben werden. Wird jedoch zusätzlich ein Kennwort angegeben, führt CICS die Anmeldung mit dem Kennwort aus.
- VERIFY: Entspricht SECURITY=PGM in der LU 6.2-Terminologie. Bei dieser Sicherheitsstufe erwartet CICS, daß vom fernen System beim Zuordnen des Dialogs sowohl Benutzer-ID als auch Kennwort übermittelt werden. Die Verbindung wird zurückgewiesen, wenn kein Kennwort angegeben ist.

- Verbindliche SNA LU 6.2-Verschlüsselung auf Sitzungsebene; wird nicht unterstützt.

Der Anwendungs-Server ist zuständig für die Verwaltung der Datenbankressourcen und legt deshalb auch fest, welche Netzwerksicherheitseinrichtungen vom Anwendungs-Requester bereitgestellt werden müssen. Beispielsweise müssen Sie bei Verwendung eines Anwendungs-Requesters unter DB2 für VM die Anforderungen für Dialogsicherheit des Anwendungs-Servers im Kommunikationsverzeichnis des Anwendungs-Requesters eintragen, indem Sie den entsprechenden Wert für das Kennzeichen :security definieren, wie in Abb. 37 auf Seite 187 gezeigt:

```
:nick.VSE1     :tpn.TOR3
               :luname.TORGATE VSEGATE
               :modename.IBMRDB
               :security.PGM
               :userid.SALESMGR
               :password.PROFIT
               :dbname.TORONTO3



Dabei gilt: TOR3    - Auf Datenbank TORONTO3 abgebildete Transaktions-ID
            TORGATE - VM/APPC-Gateway
            VSEGATE - APPLID der als Gateway zu TORONTO3 verwendeten
                      CICS/VSE-Partition
            SALESMGR/PROFIT - USERID/PASSWORD definiert in DFHSNT von
                              VSEGATE und berechtigt in TORONTO3
            TORONTO3 - Der im Startparameter DBNAME angegebene Name
                       für den Start des Anwendungs-Servers unter DB2
                       für VSE (oder Name der Standarddatenbank aus dem
                       Verzeichnis DBNAME bei Übergehen von DBNAME beim
                       Start)
```

*Abbildung 37. Beispieleintrag in CMS-Kommunikationsverzeichnis*

### Sicherheit des Datenbankmanagers

Die Benutzer-ID-Umsetzung wird vom VSE-Anwendungs-Server nicht unterstützt. CICS verwendet die vom Requester übermittelte Benutzer-ID unverändert.

Sobald die Transaktion AXE von einem Anwendungs-Requester gestartet wurde, fragt sie die Benutzer-ID von CICS ab und leitet sie an den Server unter DB2 für VSE weiter. Zum Einstellen der erforderlichen Benutzerberechtigungsstufe für Datenbankressourcen müssen Sie die Benutzer-ID im Katalog SYSTEM.SYSUSERAUTH von DB2 für VSE aktualisieren.

Der Anwendungs-Server unter DB2 für VSE überprüft, ob die von CICS angegebene Benutzer-ID über die Berechtigung CONNECT zum Zugreifen auf die Datenbank verfügt, und weist die Verbindung zurück, wenn diese Berechtigung nicht vorliegt.

Als Eigner der Datenbankressourcen steuert der Anwendungs-Server unter DB2 für VSE die Datenbanksicherheitsfunktionen für SQL-Objekte, die sich auf dem Anwendungs-Server unter DB2 für VSE befinden. Der Zugriff auf die von DB2 für VSE verwalteten Objekte wird durch eine Reihe von Zugriffsrechten gesteuert, die der Systemadministrator von DB2 für VSE oder der Eigner des jeweiligen Objekts den Benutzern erteilen kann. Der Anwendungs-Server unter DB2 für VSE steuert zwei Objektklassen:

- **Pakete:** Einzelne Endbenutzer erhalten die Berechtigung zum Erstellen, Ersetzen und Ausführen der Pakete durch die Anweisung GRANT von DB2

für VSE. Wenn ein Endbenutzer ein Paket erstellt, erhält dieser Benutzer automatisch die Berechtigung zum Ausführen und Ersetzen eines Pakets. Anderen Endbenutzern muß mit der Anweisung GRANT EXECUTE ausdrücklich die Berechtigung zum Ausführen eines Pakets auf dem Anwendungs-Server unter DB2 für VSE erteilt werden. Das Zugriffsrecht RUN kann für einzelne Endbenutzer oder für PUBLIC erteilt werden, d. h. alle Benutzer dürfen das Paket ausführen.

Nach der Vorverarbeitung einer Anwendung in DB2 für VSE enthält das Paket die im Anwendungsprogramm enthaltenen SQL-Anweisungen. Diese SQL-Anweisungen werden wie folgt klassifiziert:

– **Statisches SQL:** Dies bedeutet, die SQL-Anweisung und die SQL-Objekte, auf die in der Anweisung verwiesen wird, sind der Anwendung zum Zeitpunkt der Vorverarbeitung bekannt. Der Ersteller des Pakets muß über die Berechtigung zum Ausführen für jede der statischen SQL-Anweisungen in dem Paket verfügen.

  Wenn ein Endbenutzer das Recht zum Ausführen eines Pakets erhält, verfügt er damit automatisch über die Berechtigung zum Ausführen aller statischen SQL-Anweisungen in dem Paket. Dies bedeutet, daß Endbenutzer keine DB2-Tabellenzugriffsrechte auf dem VSE-System benötigen, wenn das Paket ausschließlich statische SQL-Anweisungen enthält.

– **Dynamisches SQL:** Bezeichnet eine SQL-Anweisung, die vor Ausführung des Pakets nicht bekannt ist. Die SQL-Anweisung wird von dem betreffenden Programm erstellt und durch die Anweisung SQL PREPARE oder die Anweisung EXECUTE IMMEDIATE für DB2 für VSE dynamisch vorverarbeitet. Wenn ein Endbenutzer eine dynamische SQL-Anweisung ausführt, muß er über die erforderlichen Tabellenzugriffsrechte zum Ausführen der SQL-Anweisung verfügen. Da die SQL-Anweisung bei der Erstellung des Pakets noch nicht bekannt ist, wird dem Endbenutzer die erforderliche Berechtigung vom Paketeigner nicht automatisch erteilt.

• **SQL-Objekte:** Dies können Tabellen, Sichten und Synonyme sein. Benutzern von DB2 für VSE können verschiedene Berechtigungsstufen zum Erstellen, Löschen, Ändern oder Lesen einzelner SQL-Objekte erteilt werden. Diese Berechtigung ist für die Vorverarbeitung statischer SQL-Anweisungen und zum Ausführen dynamischer SQL-Anweisungen erforderlich.

### Darstellen von Daten

Siehe „Darstellen von Daten” auf Seite 171.

## Prüfliste zum Aktivieren eines DRDA-Anwendungs-Servers unter DB2 für VSE

Die folgende Prüfliste faßt die zum Aktivieren eines DRDA-Anwendungs-Servers erforderlichen Schritte zusammen, ausgehend von der Annahme, daß Ihr VSE-System mit der Zugriffsmethode ACF/VTAM für die Fernverarbeitung installiert ist und daß die zur Kommunikation mit den fernen Systemen erforderlichen VTAM-Definitionen (z. B. NCP-Definitionen) vollständig vorhanden sind.

1. Installieren Sie die Unterstützung für CICS-ISC und für die CICS-Funktion zur Neustartresynchronisation.
2. Definieren Sie CICS für VTAM für VSE.
3. Assemblieren Sie die Tabelle VTAM LOGMODE mit dem Eintrag IBM-RDB.
4. Assemblieren Sie die CICS-Anmeldetabelle mit allen definierten fernen Benutzer-IDs und Kennwörtern.
5. Starten Sie CICS mit den richtigen SIT-Informationen:
   - ISC=YES
   - TST=YES, ARIAXELG definiert als RECOVERABLE in DFHTST und assembliert
   - APPLID=LU-Name (wie in der VTAM-Anweisung APPL definiert)
6. Definieren Sie die fernen Systeme für CICS (RDO darf verwendet werden):
   - CEDA DEF CONNECTION
   - CEDA DEF SESSION
   - CEDA DEF PROGRAM
   - CEDA DEF TRANSACTION

   Diese Anweisungen müssen alle Definitionen in einer einzigen Gruppe (z. B. mit dem Namen IBMG) enthalten. Installieren Sie die Gruppe mit: CEDA INSTALL GROUP(IBMG).
7. Aktualisieren Sie das Verzeichnis DBNAME (ARISDIRD.A):
   - Definieren Sie alle im Verzeichnis aufgeführten TPN für CICS. Nicht für CICS definierte TPN können nicht verwendet werden.
   - Definieren Sie jeden DRDA-Anwendungs-Server unter DB2 für VSE in dem Verzeichnis mit einem gültigen TPN.
8. Führen Sie die Prozedur ARISBDID aus, um das aktualisierte Verzeichnis DBNAME zu assemblieren.
9. Bereiten Sie den Server unter DB2 für VSE wie folgt vor:
   - Führen Sie die Prozedur ARIS342D aus, um die DRDA-Unterstützung zu installieren.

- Wenn Online-Anwendungen für DB2 für VSE (z. B. ISQL) in der CICS-Partition ausgeführt werden, erteilen Sie Planungsberechtigung (Schedule Authority) für die in der CICS-SIT-Tabelle angegebene CICS-APPLID.
- Erteilen Sie Berechtigungen für alle fernen Benutzer.

10. Falls erforderlich, führen Sie die CICS-Transaktion DAXP aus.
11. Starten Sie DB2 für VSE mit dem richtigen Parameter RMTUSERS und (wahlfrei) mit den Parametern DBNAME und SYNCPNT.
12. Bereiten Sie Anwendungen auf dem VSE-DRDA-Anwendungs-Server vor.

# Anhang A. Häufige Verbindungsprobleme

In diesem Anhang werden die häufigsten Symptome von Verbindungsproblemen auf einer Workstation unter DB2 UDB bei der Verwendung von DB2 Connect und einem DRDA-Anwendungs-Server unter DB2 UDB aufgelistet:

- „Die häufigsten DB2-Verbindungsprobleme”
- „Die häufigsten Probleme beim DRDA-AS mit DB2 UDB” auf Seite 201.

Diese Informationen sollen Ihnen den Prozeß der Fehlerbehebung erleichtern. Weitere Informationen finden Sie auch in den Handbüchern *Fehlernachrichten*, *Troubleshooting Guide* und *DB2 Connect Benutzerhandbuch*.

## Die häufigsten DB2-Verbindungsprobleme

In diesem Abschnitt werden die häufigsten Symptome von Verbindungsproblemen bei der Verwendung von DB2 Connect aufgelistet. Für jedes Problem werden Ihnen folgende Informationen zur Verfügung gestellt:

- Eine Kombination aus Nachrichtennummer und Rückkehrcode (oder protokollspezifischem Rückkehrcode) für die Nachricht. Jede Kombination aus Nachricht und Rückkehrcode hat eine separate Überschrift, und die Überschriften sind der Nachrichtennummer und dann dem Rückkehrcode nach geordnet.
- Es wird ein `Symptom` angegeben, in der Regel in Form einer Beispielnachrichtenauflistung.
- Es wird eine `Lösung` vorgeschlagen, die die wahrscheinliche Ursache des Fehlers angibt. In einigen Fällen werden eventuell mehrere Lösungen vorgeschlagen.

**Anmerkungen:**

1. Die aktuellsten Informationen zum empfohlenen Stand der Software-Fehlerberichtigung finden Sie im Handbuch *Einstieg* Ihres Produkts und in den letzten Release-Informationen.
2. Bei Kombinationen aus Nachricht und Rückkehrcode für APPC-Kommunikation wird eventuell auch ein SNA-Prüfcode angegeben. Derzeit müssen SNA-Prüfcodeinformationen für eine bestimmte Nachricht vom SNA-Subsystem abgerufen werden.

   Manchmal können SNA-Prüfcodes über die Systemprotokolle angezeigt werden. Ob dies der Fall ist oder nicht, hängt vom verwendeten SNA-Subsystem ab, und in einigen Situationen müssen Sie das Problem eventuell mit einer aktiven SNA-Ablaufverfolgung reproduzieren, um die Prüfcodeinformationen abzurufen.

3. Der Begriff Gateway bezieht sich auf DB2 Connect Enterprise Edition.

## SQL0965 oder SQL0969

### Symptom

Die Nachrichten SQL0965 und SQL0969 können mit einer Anzahl verschiedener Rückkehrcodes von DB2 Universal Database für AS/400, DB2 Universal Database für OS/390, DB2 für MVS/ESA und DB2 für VM &VSE abgesetzt werden.

Wenn eine dieser Nachrichten angezeigt wird, müssen Sie den ursprünglichen SQL-Code in der Dokumentation für das Datenbank-Server-Produkt nachschlagen, das die Nachricht abgesetzt hat.

### Lösung

Der von der Host-Datenbank empfangene SQL-Code kann nicht umgesetzt werden. Korrigieren Sie das Problem basierend auf dem Fehlercode, und wiederholen Sie den fehlgeschlagenen Befehl.

## SQL1338 während CONNECT

### Symptom / Ursache

Der symbolische Bestimmungsname wurde nicht definiert oder ist nicht ordnungsgemäß definiert.

Dazu kann es zum Beispiel kommen, wenn ein APPC-Knoten verwendet wird und der im DB2-Knotenverzeichnis angegebene symbolische Bestimmungsname nicht mit einem CPI-DFV-Eintrag in der Konfiguration des lokalen Subsystems für APPC-Datenfernverarbeitung übereinstimmt.

Eine weitere Ursache kann sein, daß auf Ihrer Maschine mehrere SNA-Stapelspeicher installiert sind. Sie müssen eventuell PATH und LIBPATH überprüfen, um sicherzustellen, daß zuerst auf den Stapelspeicher verwiesen wird, den Sie verwenden wollen.

### Lösungen

1. Stellen Sie sicher, daß der im DB2-Knotenverzeichniseintrag angegebene Profilname für die CPIC-Nebeninformationen mit der SNA-Konfiguration übereinstimmt (er ist von der Groß-/Kleinschreibung abhängig).
2. Sie müssen eventuell PATH und LIBPATH überprüfen, um sicherzustellen, daß zuerst auf den SNA-Stapelspeicher verwiesen wird, den Sie verwenden wollen.

## SQL1403N während CONNECT

### Symptom

SQL1403N Angegebene Benutzer-ID und/oder Kennwort sind/ist falsch.

### Lösung

1. Für den Benutzer konnte auf der DB2 Connect-Workstation keine Identifikationsüberprüfung durchgeführt werden. Ermitteln Sie, ob für den Benutzer auf der DB2 Connect-Workstation eine Identifikationsüberprüfung durchgeführt werden soll.

   Ist dies der Fall, stellen Sie sicher, daß in der Anweisung CONNECT das richtige Kennwort angegeben ist, falls es erforderlich ist.

   Ist dies nicht der Fall, wurde der Eintrag für das Systemdatenbankverzeichnis mit AUTHENTICATION SERVER (dies ist die Standardeinstellung, wenn AUTHENTICATION nicht explizit angegeben ist) falsch katalogisiert. Wenn letzteres zutrifft, katalogisieren Sie den Eintrag erneut mit AUTHENTICATION DCS bzw. CLIENT.

2. Das Kennwort kann nicht an die Ziel-Server-Datenbank gesendet werden, weil es nicht verfügbar ist. Wenn der Eintrag für das Systemdatenbankverzeichnis mit AUTHENTICATION DCS katalogisiert wird, muß ein Kennwort vom DB2 Client an die Ziel-Server-Datenbank übergeben werden. Auf bestimmten Plattformen, zum Beispiel AIX, kann das Kennwort nur abgerufen werden, wenn es in der Anweisung CONNECT bereitgestellt wird.

## SQL5043N

### Symptom

Die Unterstützung für mindestens ein Übertragungsprotokoll konnte nicht gestartet werden. Die Kernfunktionalität des Datenbankmanagers wurde jedoch erfolgreich gestartet.

Vielleicht wurde das TCP/IP-Protokoll auf dem DB2 Connect-Gateway nicht gestartet. Möglicherweise hat zuvor eine erfolgreiche Client-Verbindung bestanden.

Wenn `diaglevel = 4`, enthält `db2diag.log` eventuell einen Eintrag wie zum Beispiel den folgenden:

```
   1997-05-30-14.09.55.321092   Instance:svtdbm5   Node:000
PID:10296(db2tcpcm)   Appid:none
common_communication  sqlcctcpconnmgr_child   Probe:46
DIA3205E Die Socket-Adresse "30090", die in der
TCP/IP-
Servicedatei definiert und
für die TCP/IP-Server-
Unterstützung erforderlich ist, wird von einem anderen

Prozeß verwendet.
```

### Lösung

Diese Warnung ist ein Symptom dafür, daß DB2 Connect als Gateway für ferne Clients Schwierigkeiten beim Handhaben von mindestens einem Über-

tragungsprotokoll hat. Diese Protokolle können vom Typ TCP/IP oder APPC und andere sein, und in der Nachricht wird in der Regel angegeben, daß eines der für DB2 Connect definierten Übertragungsprotokolle nicht ordnungsgemäß konfiguriert ist.

Eine mögliche Ursache ist häufig, daß die Profilvariable DB2COMM nicht definiert oder falsch definiert ist. Im allgemeinen ist das Problem das Ergebnis einer Abweichung zwischen der Variablen DB2COMM und den in der Datenbankmanagerkonfiguration definierten Namen (zum Beispiel svcename, nname oder tpname).

Ein mögliches Szenario ist, daß zuvor erfolgreich eine Verbindung hergestellt wurde und daß dann die Fehlernachricht SQL5043 angezeigt wird, obwohl die Konfiguration nicht geändert wurde. Dazu kann es bei Verwendung des TCP/IP-Protokolls kommen, wenn das ferne System die Verbindung aus einem bestimmten Grund abnormal beendet. Wenn dies auftritt, kann eine Verbindung weiterhin auf dem Client vorhanden sein, und es ist eventuell möglich, die Verbindung durch Absetzen der untenstehenden Befehle ohne weiteres Eingreifen wiederherzustellen.

Sehr wahrscheinlich hat einer der Clients, der mit dem Gateway verbunden ist, noch eine Kennung am TCP/IP-Anschluß. Geben Sie auf jeder Client-Maschine, die mit dem Gateway verbunden ist, folgende Befehle ein:

1. db2 terminate
2. db2stop

## SQL30020

### Symptom

SQL30020N Die Ausführung schlug aufgrund eines Verteilungsprotokollfehlers (Distributed Protocol Error) fehl. Dieser Fehler beeinflußt die erfolgreiche Ausführung der nachfolgenden Befehle und SQL-Anweisungen.

### Lösungen

Wenden Sie sich bei diesem Fehler an den Service.

Überprüfen Sie das Verzeichnis db2dump auf einen ffdc-Speicherauszug (pid.000). Formatieren Sie diese Speicherauszugsdatei anschließend mit `db2fdump`, und suchen Sie in der Ergebnisdatei nach ″ERROR″. Hier wird eventuell ein Verweis auf MVS ABEND aufgelistet. Überprüfen Sie in diesem Fall die MVS-Konsole auf weitere Informationen, und schlagen Sie den Code für abnormale Beendigung im Handbuch *DB2 for MVS Messages and Codes* nach.

## SQL30060

### Symptom
SQL30060N ″<berechtigungs-ID>″ verfügt nicht über die Berechtigung, die Operation ″<operation>″ auszuführen.

### Lösung
Beim Herstellen der Verbindung zu DB2 für MVS bzw. DB2 für OS/390 wurden die Kommunikationsdatenbanktabellen nicht ordnungsgemäß aktualisiert. Weitere Informationen finden sie in:

- *DB2 Connect Einstieg*

## SQL30061

### Symptom
Verbindung zu falschem Datenbank-Server-Standort auf dem Host oder System IBM AS/400; keine Zieldatenbank gefunden.

### Lösung
Im DCS-Verzeichniseintrag wurde eventuell der falsche Server-Datenbankname angegeben. Wenn es dazu kommt, wird SQLCODE -30061 an die Anwendung zurückgegeben.

Überprüfen Sie den DB2-Knoten, die Datenbank und die DCS-Verzeichniseinträge. Das Feld für den Zieldatenbanknamen im DCS-Verzeichniseintrag muß mit dem Namen der Datenbank basierend auf der Plattform übereinstimmen. Bei einer Datenbank unter DB2 Universal Database für OS/390 muß der zu verwendende Name beispielsweise mit dem Namen übereinstimmen, der im Feld ″LOCATION=standortname″ des BSDS (Boot Strap Data Set) verwendet wird und der auch in der Nachricht DSNL004I (LOCATION=standort) angezeigt wird, wenn DDF (Distributed Data Facility) gestartet wird.

Zudem enthält das Handbuch *Einstieg* für DB2 Connect Beispiele zum Aktualisieren der DB2-Kataloge. Informationen dazu finden Sie im Schritt zur Aktualisierung der DB2-Verzeichnisse in jedem Kapitel, das die SNA-Konfiguration beschreibt, oder im Kapitel über die Konfiguration von Datenbanken für DB2 Connect auf dem Host oder System IBM AS/400 und im Abschnitt über die Konfiguration der TCP/IP-Verbindung.

Die korrekten Befehle für einen APPC- oder APPN-Knoten sind:

```
db2 catalog appc node <knotenname> remote <symb.-bestimmungsname> security program
db2 catalog dcs database <lokaler-name> as <tatsächlicher-datenbankname>
db2 catalog database <lokaler-name> as <alias> at node <knotenname>
             authentication dcs
```

Die korrekten Befehle für einen TCP/IP-Knoten sind:

```
db2 catalog tcpip node <knotenname> remote <host-name-oder-adresse>
            server <anschlußnummer-oder-servicename>
db2 catalog dcs database <lokaler-name> as <tatsächlicher-datenbankname>
db2 catalog database <lokaler-name> as <alias> at node <knotenname>
            authentication dcs
```

Setzen Sie zum Verbinden der Datenbank folgenden Befehl ab:

```
db2 connect to <alias> user <benutzername> using <kennwort>
```

## SQL30073 mit Rückkehrcode 119C während CONNECT

### Symptom

Die Nachricht SQL30073 wird mit dem Rückkehrcode 119C abgesetzt. Dazu kommt es, wenn die Ziel-Server-Datenbank die vom DB2-Client (über DB2 Connect) verwendete Codepage nicht unterstützt. Die Codepage wird von der Konfiguration der Betriebsumgebung abgeleitet, in der der DB2-Client ausgeführt wird.

Weitere Informationen finden Sie im Handbuch *Systemverwaltung*.

### Lösung

Dieses Problem kann häufig gelöst werden, indem Sie eine Berichtigung auf dem Ziel-Server-Datenbanksystem installieren. Wenden Sie sich an die geeignete Serviceorganisation, beziehen Sie die für dieses Symptom empfohlenen Berichtigungen, und wenden Sie diese an.

Als temporäre Lösung kann der Benutzer die Standard-Codepage durch Einstellen der Umgebungsvariablen DB2CODEPAGE überschreiben. Überprüfen Sie die länderspezifischen Angaben, bzw. stellen Sie DB2CODEPAGE=850 ein.

Auf UNIX-Plattformen kann der Benutzer eventuell zu einer anderen Codepage umschalten, indem er die Umgebungsvariable LANG auf einen anderen Wert setzt.

## SQL30081N mit Rückkehrcode 1

### Symptom

Das Symptom ist die folgende Nachricht plus SNA-Prüfcode:

```
  db2 connect to <datenbankname> user <benutzer-ID>
  Kennwort eingeben für <benutzer-ID>:
SQL30081N  Übertragungsfehler.
  Verwendetes
  Übertragungsprotokoll: "APPC".
  Verwendete Übertragungs-API: "CPI-C".
  Position, an der
  der Fehler festgestellt wurde: "".
```

```
Übertragungsfunktion, die
den Fehler feststellte:
"cmallc".
Protokollspezifische(r) Fehlercode(s): "1", "*", "0x10030021".    SQLSTATE=08001
```

**Lösung(en)**

In diesem Beispiel ist der Prüfcode 10030021.

Im folgenden werden die häufigsten Prüfcodes für diese Fehlernachricht und die jeweiligen vorgeschlagenen Lösungen angegeben:

1. `SQL30081N mit Rückkehrcode 1 und SNA-Prüfcode 0877002C`

   Es wurde ein falscher Netzwerkname angegeben.

2. `SQL30081N mit Rückkehrcode 1 und SNA-Prüfcode ffff0003`

   Es wurde die falsche MAC-Adresse angegeben, oder die SNA-Verbindung ist nicht aktiv.

3. `SQL30081N mit Rückkehrcode 1 und SNA-Prüfcode 10030021`

   Es liegt eine Abweichung vom LU-Typ vor.

4. `SQL30081N mit Rückkehrcode 1 und SNA-Prüfcode 084B6031`

   MAXDBAT in DSNZPARM (bei einem Host unter DB2 für MVS oder DB2 für OS/390) ist auf 0 gesetzt.

Andere Vorschläge:

1. Definieren Sie die LU beim Erstellen des lokalen LU-Profils als die Standard-LU. Führen Sie zum Beispiel im Fenster Liste mit SNA-Einrichtungen in CM/2 einen der beiden folgenden Schritte aus:
   - Wählen Sie das Markierungsfeld Diese lokale LU als Aliasnamen der lokalen Standard-LU verwenden aus.
   - Stellen Sie die Profil- oder Umgebungsvariable `APPCLLU` auf dem Gateway-System unter DB2 Connect Enterprise Edition auf den lokalen LU-Namen ein. Sie können dazu auf OS/2-Systemen zum Beispiel die Datei CONFIG.SYS editieren oder auf Windows NT-Systemen die Systemsteuerung verwenden.
2. Überprüfen Sie, ob SNA auf dem DB2 Connect-Gateway gestartet wurde.
3. Wenn Sie mit DB2 für MVS bzw. DB2 für OS/390 arbeiten, überprüfen Sie, ob der DDF-Adreßraum (DDF - Distributed Data Facility) gestartet wurde und ob DB2 ausgeführt wird.

## SQL30081N mit Rückkehrcode 2

### Symptom
Die Nachricht SQL30081N wird mit Rückkehrcode 2 und SNA-Prüfcode 08120022 empfangen.

### Lösung
Der Parameter NUMILU für NCP (Host-Ende der Programmverbindung (Link)) ist eventuell auf den Standardwert (0) gesetzt. Überprüfen Sie dies. Ändern Sie ggf. die NCP-Definition, bevor Sie den Vorgang nach der Aktivierung der Änderung wiederholen.

## SQL30081N mit Rückkehrcode 9

### Symptom
Das Symptom ist die folgende Nachricht (der SNA-Prüfcode ist in diesem Fall nicht erforderlich):

```
   db2 connect to <datenbank> user <benutzer-ID>
SQL30081N  Übertragungsfehler.
  Verwendetes Übertragungsprotokoll: "APPC".
  Verwendete Übertragungs-API: "CPI-C".
  Position, an der der Fehler festgestellt wurde: "".
  Übertragungsfunktion, die den Fehler feststellte:"cmsend".
  Protokollspezifische(r) Fehlercode(s): "9", "*", "0x10086021".    SQLSTATE=08001
```

### Lösung
Das Problem ist, daß der Name des Transaktionsprogramms (TPNAME) auf dem DB2 Connect-System nicht ordnungsgemäß definiert ist. Sie haben zum Beispiel eventuell Ihre SNA-Konfiguration aktualisiert, sie jedoch noch nicht auf dem DB2 Connect-Gateway geprüft. Weitere Einzelangaben finden Sie im Handbuch *DB2 Connect Enterprise Edition für OS/2 und Windows Einstieg* bzw. *DB2 Connect Personal Edition Einstieg*.

## SQL30081N mit Rückkehrcode 10

### Symptom
Das Symptom ist die folgende Nachricht (der SNA-Prüfcode ist nicht erforderlich):

```
SQL30081N  Übertragungsfehler.
  Verwendetes Übertragungsprotokoll: "APPC".
  Verwendete Übertragungs-API: "CPI-C".
  Position, an der der Fehler festgestellt wurde: "".
  Übertragungsfunktion, die den Fehler feststellte: "cmrcv".
  Protokollspezifische(r) Fehlercode(s): "10", "*", "*".
   SQLSTATE=08001
```

### Lösung
Überprüfen Sie, ob DB2 ordnungsgemäß installiert wurde.

Wird ein Gateway unter DB2 Connect für OS/2 verwendet, wird eventuell folgende Nachricht angezeigt, wenn der Transaktionsprogrammname nicht ordnungsgemäß definiert ist:

```
Protokollspezifische(r) Fehlercode(s): "10", "*", "0x084C0000".
SQLSTATE=08001
```

In diesem Fall muß der TP-Name beispielsweise in CM/2 wie folgt definiert werden:

```
Name des Transaktionsprogramms (TP-Name)  = 'tpname'    (benutzerdefiniert)
OS/2-Programmpfad und Dateiname = nicht verwendet
```

und (auf der nächsten CM/2-Konfigurationsanzeige)

```
Darstellungsart - Hintergrund
Betriebsart - Warteschlangenbetrieb - Vom Bediener vorher geladen
```

## SQL30081N mit Rückkehrcode 20

### Symptom

```
 SQL30081N  Übertragungsfehler.
Verwendetes Übertragungsprotokoll: "APPC".
Verwendete Übertragungs-API: "CPI-C".
Position, an der der Fehler festgestellt wurde: "".
Übertragungsfunktion, die den Fehler feststellte: "xcstp".
Protokollspezifische(r) Fehlercode(s): "20", "*", "*".
 SQLSTATE=08001
```

### Lösung

Stellen Sie sicher, daß das SNA-Subsystem auf dem DB2 Connect-System gestartet wurde.

## SQL30081N mit Rückkehrcode 27

### Symptom

Die Nachricht SQL30081N wird mit Rückkehrcode 27 und SNA-Prüfcode 800Axxxx empfangen.

### Lösung

Die VTAM-Pfadinformationseinheit (PIU) ist zu groß.

## SQL30081N mit Rückkehrcode 79

### Symptom

```
 SQL30081N  Übertragungsfehler.
Verwendetes Übertragungsprotokoll: "TCP/IP".
Verwendete Übertragungs-API: "SOCKETS".
Position, an der der Fehler festgestellt wurde: "".
Übertragungsfunktion, die den Fehler feststellte: "connect".
Protokollspezifische(r) Fehlercode(s): "79", "*", "*".
 SQLSTATE=08001
```

### Lösung(en)

Dieser Fehler kann auftreten, wenn ein ferner Client keine Verbindung zu einem DB2 Connect-Gateway herstellen kann. Dazu kann es auch kommen, wenn die Verbindung vom DB2 Connect-Gateway zu einem Host hergestellt wird.

1. Die Profilvariable DB2COMM ist auf dem DB2 Connect-Gateway eventuell falsch eingestellt. Überprüfen Sie dies. Zum Beispiel muß der Befehl db2set db2comm=tcpip in sqllib/db2profile angezeigt werden, wenn DB2 Enterprise - Extended Edition unter AIX ausgeführt wird.
2. Eventuell gibt es eine Abweichung zwischen dem TCP/IP-Servicenamen und/oder den Anschlußnummerangaben auf dem DB2-Client und dem DB2 Connect-Gateway. Prüfen Sie die Einträge in den TCP/IP-Dateien services auf beiden Maschinen.
3. Überprüfen Sie, ob DB2 auf dem DB2 Connect-Gateway gestartet wurde. Setzen Sie diaglevel der Datenbankmanagerkonfiguration mit dem folgenden Befehl auf 4:

   ```
   db2 update dbm cfg using diaglevel 4
   ```

   Überprüfen Sie nach dem Stoppen und Neustart von DB2 in der Datei db2diag.log, ob die DB2-TCP/IP-Datenfernverarbeitung gestartet wurde. Es wird eine Ausgabe angezeigt, die der folgenden ähnelt:

   ```
   1998-02-03-12.41.04.861119   Instance:svtdbm2   Node:00
   PID:86496(db2sysc)   Appid:none
   common_communication  sqlcctcp_start_listen   Probe:80
   DIA3000I Die Protokollunterstützung für "TCPIP" wurde erfolgreich gestartet.
   ```

## SQL30081N mit protokollspezifischem Fehlercode 10032

### Symptom

```
 SQL30081N  Übertragungsfehler.
Verwendetes Übertragungsprotokoll: "TCP/IP".
Verwendete Übertragungs-API: "SOCKETS".
Position, an der der Fehler festgestellt wurde: "9.21.85.159".
Übertragungsfunktion, die den Fehler feststellte: "send".
Protokollspezifische(r) Fehlercode(s): "10032",   "*", "*".
 SQLSTATE=08001
```

### Lösung

Diese Fehlernachricht wird eventuell empfangen, wenn versucht wird, die Verbindung zu einer Maschine zu trennen, auf der die TCP/IP-Datenfernverarbeitung bereits fehlgeschlagen ist. Korrigieren Sie das Problem mit dem TCP/IP-Subsystem.

Starten Sie dazu auf den meisten Maschinen einfach das TCP/IP-Protokoll erneut. Gelegentlich ist der Neustart der gesamten Maschine erforderlich.

## Die häufigsten Probleme beim DRDA-AS mit DB2 UDB

In diesem Abschnitt werden die häufigsten Problemszenarios bei Verwendung des DRDA-AS mit DB2 UDB aufgelistet.

### Übertragungsfehler während CONNECT

Stellen Sie sicher, daß die folgenden Angaben ordnungsgemäß für DB2 UDB eingestellt sind.

#### APPC/SNA LU 6.2

1. SNA-Konfiguration

   Stellen Sie sicher, daß der Transaktionsprogrammname konfiguriert ist, falls er erforderlich ist.

   Wenn die Sicherheitseinstufung SAME vom DRDA-AR verwendet werden soll, stellen Sie sicher, daß sie für die LU des DRDA-AR aktiviert ist.
2. Parameter TPNAME der Datenbankmanagerkonfiguration
3. Umgebungsvariable DB2COMM für die Aufnahme von APPC eingestellt

Stellen Sie sicher, daß db2start ohne Warnung beendet wird.

#### TCP/IP

1. Datei `services`
2. Parameter SVCENAME der Datenbankmanagerkonfiguration
3. Umgebungsvariable DB2COMM für die Aufnahme von TCPIP eingestellt; Stellen Sie sicher, daß db2start ohne Warnung beendet wird.

### DRDA-Fehler während CONNECT

#### APPC/SNA LU 6.2

Wenn der SNA-Server für AIX verwendet wird, stellen Sie sicher, daß sich der Gruppenname für die ausführbare Datei ~/sqllib/adm/db2sysc im Feld für die Namen der gesicherten Gruppen, ″Trusted group names″, im Profil ″SNA System Defaults″ der SNA-Konfiguration befindet.

#### TCP/IP

Wenn der DRDA-AR DB2 für OS/390 ist, stellen Sie sicher, daß die folgenden Korrekturen angewendet wurden: APAR PQ05771/PTF UQ06843 und APAR PQ07537/PTF UQ09146.

### Fehler ″Datenbank nicht gefunden″ während CONNECT

Stellen Sie sicher, daß der DRDA-AR mit dem Aliasnamen für die Zieldatenbank unter DB2 UDB konfiguriert ist.

### Sicherheitsfehler während CONNECT über APPC/SNA LU 6.2

Für die Einstellung AUTHENTICATION in der Datenbankmanagerkonfiguration unter DB2 UDB gelten besondere Bestimmungen, wenn die Verbindung von einem DRDA-AR über APPC/SNA LU 6.2 hergestellt wird. Wenn Sie auf einen Sicherheitsfehler stoßen, stellen Sie sicher, daß die Einstellung AUTHENTICATION der Datenbankmanagerkonfiguration wie folgt ordnungsgemäß festgelegt ist:

1. Client

   Bei dieser Einstellung funktionieren Verbindungen der Sicherheitseinstufung SAME und PROGRAM.

2. Server

   Bei dieser Einstellung funktionieren nur Verbindungen der Sicherheitseinstufung PROGRAM zum DRDA-AS mit DB2 UDB unter AIX mit SNA-Server und unter OS/2 mit CS/2 Version 4 (mit konfiguriertem Synchronisationspunktmanager).

3. DCS

   AUTHENTICATION DCS kann nun mit dem DRDA-AS unter DB2 UDB Version 7 verwendet werden, um APPC-Verbindungen von DRDA-Clients zuzulassen, die die Sicherheitseinstufung SAME verwenden (kein Kennwort erforderlich), und zugleich die Authentifizierung SERVER (Kennwort erforderlich) für alle anderen Client-Anforderungen zu erzwingen.

   Bei dieser Einstellung funktioniert folgendes:

   a. DRDA-AS mit DB2 UDB unter AIX mit SNA-Server und unter OS/2 mit CS/2 Version 4 (mit konfiguriertem Synchronisationspunktmanager):

      ```
      Sicherheitseinstufung SAME
      ```

   b. DRDA-AS mit DB2 UDB unter OS/2 mit CM/2 1.11, Windows NT und Sun Solaris:

      ```
      Sicherheitseinstufung SAME oder PROGRAM
      ```

Diese Unterschiede bestehen, weil einige Kommunikationssubsysteme ein eingehendes Kennwort nicht an DB2 UDB weiterleiten.

### Fehler während BIND

Eventuell wird ein SQL-Kommunikationsbereich mit dem SQLCODE-Wert -4930 zurückgegeben, wenn eine vom DRDA-AS angegebene Bindeoption nicht unterstützt wird. Das Feld SQLERRMC enthält Informationen zur Bindeoption, die den Fehler verursacht.

# Anhang B. Bemerkungen

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, daß nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb der Produkte, Programme oder Dienstleistungen in Verbindung mit Fremdprodukten und Fremddienstleistungen liegt beim Kunden, soweit nicht ausdrücklich solche Verbindungen erwähnt sind.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanfragen sind schriftlich an IBM Europe, Director of Licensing, 92066 Paris La Defense Cedex, France, zu richten. Anfragen an obige Adresse müssen auf englisch formuliert werden.

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen bekanntgegeben. IBM kann jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Web-Sites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Web-Sites dar. Das über diese Web-Sites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Web-Sites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne daß eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Canada Limited
Office of the Lab Director
1150 Eglinton Ave. East
North York, Ontario
M3C 1H7
CANADA

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der Internationalen Nutzungsbedingungen der IBM für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Garantie, daß diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Informationen über Produkte anderer Hersteller als IBM wurden von den Herstellern dieser Produkte zur Verfügung gestellt, bzw. aus von ihnen veröffentlichten Ankündigungen oder anderen öffentlich zugänglichen Quellen entnommen. IBM hat diese Produkte nicht getestet und übernimmt im Hinblick auf Produkte anderer Hersteller keine Verantwortung für einwandfreie Funktion, Kompatibilität oder andere Ansprüche. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten der IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele der IBM.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogrammes illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden, Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHT-LIZENZ:

Diese Veröffentlichung enthält Beispielanwendungsprogramme, die in Quellensprache geschrieben sind. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, verwenden, vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Beispielprogramme geschrieben werden. Die in diesem Handbuch aufgeführten Beispiele sollen lediglich der Veranschaulichung und zu keinem anderen Zweck dienen. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet.

Kopien oder Teile der Beispielprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

© (Name Ihrer Firma) (Jahr). Teile des vorliegenden Codes wurden aus Beispielprogrammen der IBM Corp. abgeleitet. © Copyright IBM Corp. _Jahr / Jahre angeben_. Alle Rechte vorbehalten.

## Neue deutsche Rechtschreibung

Durch die Einführung der neuen deutschen Rechtschreibung bei IBM zum 1. September 1999 kann es vorkommen, dass in dem vorliegenden Handbuch bestimmte Wörter sowohl nach der alten als auch nach der neuen Schreibweise verwendet werden, und zwar immer dann, wenn auf existierende Handbuchkapitel und/oder Programmteile zurückgegriffen wird.

## Änderungen in der IBM Terminologie

Die ständige Weiterentwicklung der deutschen Sprache nimmt auch Einfluss auf die IBM Terminologie. Durch die daraus resultierende Umstellung der IBM Terminologie kann es u. U. vorkommen, dass in diesem Handbuch sowohl alte als auch neue Termini gleichbedeutend verwendet werden. Dies ist der Fall, wenn auf ältere existierende Handbuchkapitel und/oder Programmteile zurückgegriffen wird.

Aufgrund kurzfristiger Änderungen der Software, die in die Dokumentation nicht mehr aufgenommen werden konnten, entsprechen die in den Handbüchern aufgeführten Programmelemente möglicherweise nicht den im eigentlichen Programm angezeigten Elementen.

## Marken

Folgende Namen sind in gewissen Ländern Marken der International Business Machines Corporation.

ACF/VTAM
AISPO
AIX
AIX/6000
AIXwindows
AnyNet
APPN
IBM System AS/400
BookManager
CICS
C Set++
C/370
DATABASE 2
DataHub
DataJoiner
DataPropagator
DataRefresher
DB2
DB2 Connect
DB2 Extenders
DB2 OLAP Server
DB2 Universal Database
Distributed Relational
Database Architecture
DRDA
eNetwork
Extended Services
FFST
First Failure Support Technology
IBM
IMS
IMS/ESA
LAN DistanceMVS
MVS/ESA
MVS/XA
Net.Data
OS/2
OS/390
OS/400
PowerPC
QBIC
QMF
RACF
RS/6000
IBM System /370
SP
SQL/DS
SQL/400
System/370
IBM System /390
SystemView
VisualAge
VM/ESA
VSE/ESA
VTAM
WebExplorer
WIN-OS/2

Folgende Namen sind in gewissen Ländern Marken oder eingetragene Marken anderer Unternehmen:

Microsoft, Windows und Windows NT sind Marken oder eingetragene Marken von Microsoft Corporation.

Java und alle auf Java basierenden Marken und Logos sowie Solaris sind in gewissen Ländern Marken von Sun Microsystems, Inc.

Tivoli und NetView sind in gewissen Ländern Marken von Tivoli Systems Inc.

UNIX ist eine eingetragene Marke und wird ausschließlich von der X/Open Company Limited lizenziert.

Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken anderer Unternehmen sein.

# Index

## D



## E



## F



## G



## H



## I



## K



## L



## M



## N

## O



## P



## R



## S

# Kontaktaufnahme mit IBM

Bei technischen Problemen lesen Sie bitte die entsprechenden Korrekturmaßnahmen im Handbuch *Troubleshooting Guide* und führen Sie diese aus, bevor Sie sich mit der IBM Kundenunterstützung in Verbindung setzen. Mit Hilfe dieses Handbuchs können Sie Informationen sammeln, die die DB2-Kundenunterstützung zur Fehlerbehebung verwenden kann.

Wenn Sie weitere Informationen benötigen oder eines der DB2 Universal Database-Produkte bestellen möchten, setzen Sie sich mit einem IBM Ansprechpartner in einer lokalen Geschäftsstelle oder einem IBM Software-Vertriebspartner in Verbindung.

Telefonische Unterstützung erhalten Sie über folgende Nummern:

- Unter 0180 3/313 233 erreichen Sie Hallo IBM, wo Sie Antworten zu allgemeinen Fragen erhalten.
- Unter 0190/772 243 erreichen Sie die DB2 Helpline, wo Sie Antworten zu DB2-spezifischen Problemen erhalten.

## Produktinformationen

Telefonische Unterstützung erhalten Sie über folgende Nummern:

- Unter 0180 3/313 233 erreichen Sie Hallo IBM, wo Sie Antworten zu allgemeinen Fragen erhalten.
- Unter 0180/55 090 können Sie Handbücher telefonisch bestellen.

**http://www.ibm.com/software/data/**
Auf den DB2-World Wide Web-Seiten erhalten Sie aktuelle DB2-Informationen wie Neuigkeiten, Produktbeschreibungen, Schulungspläne und vieles mehr.

**http://www.ibm.com/software/data/db2/library/**
Mit **DB2 Product and Service Technical Library** können Sie auf häufig gestellte Fragen, Berichtigungen, Handbücher und aktuelle technische DB2-Informationen zugreifen.

**Anmerkung:** Diese Informationen stehen möglicherweise nur auf Englisch zur Verfügung.

**http://www.elink.ibmlink.ibm.com/pbl/pbl/**
Auf der Web-Site für die Bestellung internationaler Veröffentlichungen (International Publications) finden Sie Informationen zum Bestellverfahren.

**http://www.ibm.com/education/certify/**
Das 'Professional Certification Program' auf der IBM Web-Site stellt Zertifizierungstestinformationen für eine Reihe von IBM Produkten, u. a. auch DB2, zur Verfügung.

**ftp.software.ibm.com**
Melden Sie sich als *anonymous* an. Im Verzeichnis `/ps/products/db2` finden Sie Demo-Versionen, Berichtigungen, Informationen und Tools zu DB2 und vielen zugehörigen Produkten.

**comp.databases.ibm-db2, bit.listserv.db2-l**
Über diese Internet-Newsgroups können DB2-Benutzer Ihre Erfahrungen mit den DB2-Produkten austauschen.

**Für Compuserve: GO IBMDB2**
Geben Sie diesen Befehl ein, um auf IBM DB2 Family Forums zuzugreifen. Alle DB2-Produkte werden über diese Foren unterstützt.

In Anhang A des Handbuchs *IBM Software Support Handbook* finden Sie Informationen dazu, wie Sie sich mit IBM in Verbindung setzen können. Rufen Sie die folgende Web-Seite auf, um auf dieses Dokument zuzugreifen: http://www.ibm.com/support/. Wählen Sie anschließend die Verbindung zum IBM Software Support Handbook am unteren Rand der Seite aus.

**Anmerkung:** In einigen Ländern sollten sich die IBM Vertragshändler an die innerhalb ihrer Händlerstruktur vorgesehene Unterstützung wenden, nicht an die IBM Unterstützungsfunktion.

# Antwort

**DB2-Konnektivität -**
**Ergänzung**
**Version 7**

**IBM Form SDB2-CONN-SU**

Anregungen zur Verbesserung und Ergänzung dieser Veröffentlichung nehmen wir gerne entgegen. Bitte informieren Sie uns über Fehler, ungenaue Darstellungen oder andere Mängel.

Zur Klärung technischer Fragen sowie zu Liefermöglichkeiten und Preisen wenden Sie sich bitte entweder an Ihre IBM Geschäftsstelle, Ihren IBM Geschäftspartner oder Ihren Händler.

**Unsere Telefonauskunft ″HALLO IBM″ (Telefonnr.: 01803/31 32 33) steht Ihnen ebenfalls zur Klärung allgemeiner Fragen zur Verfügung.**

Kommentare:

Danke für Ihre Bemühungen.

Sie können ihre Kommentare betr. dieser Veröffentlichung wie folgt senden:
- Als Brief an die Postanschrift auf der Rückseite dieses Formulars
- Als E-Mail an die folgende Adresse: comment@tcvm.vnet.ibm.com

| | |
|---|---|
| Name | Adresse |
| Firma oder Organisation | |
| Rufnummer | E-Mail-Adresse |

**Antwort**
SDB2-CONN-SU

IBM Deutschland Informationssysteme GmbH
SW NLS Center

70548 Stuttgart

Teilenummer: SDB2-CONN-SU

Gedruckt in Deutschland