

# **Oracle® Transparent Gateway for DRDA**

Installation and User's Guide

10g Release 2 (10.2) for Microsoft Windows

**B16218-03**

November 2008

Oracle Transparent Gateway for DRDA Installation and User's Guide, 10g Release 2 (10.2) for Microsoft Windows

B16218-03

Copyright © 2001, 2008, Oracle. All rights reserved.

Primary Author: Maitreyee Chaliha

Contributing Author: Peter A Castro

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

---

---

# Contents

<b>Preface</b> .....	xv
Audience .....	xv
Documentation Accessibility .....	xv
Related Documents .....	xvi
Conventions .....	xvi
SQL*Plus Prompts .....	xvii
DOS Prompts .....	xvii
Storage Measurements .....	xvii
Directory Names.....	xvii
<b>1 Introduction</b>	
1.1 Introduction to the Oracle Transparent Gateway .....	1-1
1.1.1 Protection of Current Investment.....	1-2
1.2 Release 10g Gateways.....	1-2
1.2.1 Advantages of the Gateway .....	1-2
1.3 Gateway Capabilities.....	1-2
1.3.1 Transparency at All Levels.....	1-3
1.3.2 Extended Database Services.....	1-3
1.3.3 Extended Advanced Networking, Internet and Intranet Support .....	1-4
1.3.4 Dynamic Dictionary Mapping .....	1-4
1.3.5 SQL.....	1-5
1.3.6 Data Definition Language .....	1-5
1.3.7 Data Control Language .....	1-5
1.3.8 Passthrough and Native DB2 SQL .....	1-5
1.3.9 Stored Procedures .....	1-5
1.3.9.1 Oracle Stored Procedures .....	1-5
1.3.9.2 Native DB2 Stored Procedures .....	1-5
1.3.10 Languages .....	1-5
1.3.11 Oracle Database Server Technology and Tools .....	1-6
1.3.12 SQL*Plus .....	1-6
1.3.13 Two-Phase Commit and Multisite Transactions.....	1-6
1.3.14 Site Autonomy .....	1-6

1.3.15	Migration and Coexistence.....	1-6
1.3.16	Security.....	1-6
1.4	Terms .....	1-7
1.5	Architecture .....	1-7
1.6	Implementation.....	1-8
1.7	How the Gateway Works.....	1-9
1.7.1	SQL Differences.....	1-9
1.8	Oracle Tools and the Gateway .....	1-9
1.8.1	SQL*Plus .....	1-10
1.9	Features .....	1-10
1.9.1	Heterogeneous Services Architecture .....	1-10
1.9.2	Performance Enhancements .....	1-10
1.9.3	Fetch Reblocking .....	1-10
1.9.4	Oracle Database 10g Passthrough Supported.....	1-10
1.9.5	Retrieving Result Sets Through Passthrough .....	1-10
1.9.6	Support for TCP/IP .....	1-11
1.9.7	Native Semantics .....	1-11
1.9.8	Columns Supported in a Result Set .....	1-11
1.9.9	EXPLAIN_PLAN Improvement .....	1-11
1.9.10	Heterogeneous Database Integration .....	1-11
1.9.11	Minimum Impact on Existing Systems.....	1-11
1.9.12	Large Base of Data Access .....	1-11
1.9.13	Application Portability .....	1-11
1.9.14	Remote Data Access .....	1-11
1.9.15	Support for Distributed Applications .....	1-12
1.9.16	Application Development and End User Tools .....	1-12
1.9.17	Password Encryption Utility.....	1-13
1.9.18	Support for DB2/OS390 V6, V7, and V8 Stored Procedures.....	1-13
1.9.19	Codepage Map Facility .....	1-13
1.9.20	IBM DB2 Universal Database Support .....	1-13
1.9.21	IBM DB2 Version 5.1 ASCII Tables .....	1-13
1.9.22	Read-Only Support .....	1-13
1.9.23	Support for Graphic and Multibyte Data.....	1-13
1.9.24	Support for DB2/UDB on Intel Hardware .....	1-13
1.9.25	Data Dictionary Support for DB2/UDB.....	1-13

## 2 Release Information

2.1	Product Set.....	2-1
2.2	Changes and Enhancements .....	2-1
2.3	Bugs Fixed in 10g Release 2 (10.2) .....	2-1
2.4	Known Problems.....	2-3
2.5	Known Restrictions.....	2-3
2.5.1	DB2 Considerations.....	2-3
2.5.2	SQL Limitations .....	2-5

## 3 System Requirements

3.1	Hardware Requirements.....	3-1
-----	----------------------------	-----

3.1.1	Processor .....	3-1
3.1.2	Memory .....	3-1
3.1.3	Network Attachment .....	3-2
3.1.4	Disk Space .....	3-2
3.2	Software Requirements .....	3-2
3.2.1	Operating System .....	3-2
3.2.2	DRDA Databases .....	3-2
3.2.3	Communications .....	3-3
3.2.4	Oracle Database server.....	3-3
3.2.5	Oracle Networking Products .....	3-3
3.3	Documentation Requirements .....	3-3

## 4 Installing the Gateway

4.1	Introduction .....	4-1
4.2	Before You Begin.....	4-1
4.3	Checklist for Gateway Installation .....	4-2
4.4	Installation Overview .....	4-2
4.5	Preinstallation.....	4-2
4.6	Installing the Gateway from the Installation Media.....	4-2
4.6.1	Step 1: Log on to the host .....	4-2
4.6.2	Step 2: Load the CD-ROM into the CD-ROM Drive.....	4-2
4.6.3	Step 3: Start the Oracle Universal Installer on Microsoft Windows.....	4-3
4.6.4	Step 4: Step through the Oracle Universal Installer.....	4-3
4.6.5	Step 5: Verify Installation Success .....	4-3
4.7	Installation Complete .....	4-3
4.7.1	Removing the Gateway.....	4-4

## 5 Configuring the DRDA Server

5.1	Checklists for Configuring the DRDA Server.....	5-1
5.1.1	DB2/OS390 .....	5-1
5.1.2	DB2/400 .....	5-1
5.1.3	DB2/UDB (Universal Database).....	5-2
5.1.4	DB2/VM.....	5-2
5.2	DB2/OS390 .....	5-2
5.2.1	Step 1: Configure the Communications Server .....	5-2
5.2.2	Step 2: Define the user ID that owns the package.....	5-2
5.2.3	Step 3: Define the recovery user ID.....	5-3
5.2.4	Step 4: Determine DRDA location name for DB2 instance.....	5-3
5.2.5	Step 5: Configure DB2 Distributed Data Facility for Gateway .....	5-3
5.3	DB2/400 .....	5-3
5.3.1	Step 1: Configure the Communications Server .....	5-3
5.3.2	Step 2: Define the user ID that owns the package.....	5-4
5.3.3	Step 3: Define the recovery user ID.....	5-4
5.3.4	Step 4: Determine DRDA location name for DB2/400 instance .....	5-4
5.4	DB2/UDB (Universal Database) .....	5-4
5.4.1	Step 1: Configure the SNA Communications Server.....	5-4

5.4.2	Step 2: Define the user ID that owns the package.....	5-5
5.4.3	Step 3: Define the recovery user ID.....	5-5
5.4.4	Step 4: Determine DRDA location name for DB2/UDB instance.....	5-5
5.5	DB2/VM .....	5-5
5.5.1	Step 1: Configure the Communications Server .....	5-6
5.5.2	Step 2: Define the user ID that owns the package.....	5-6
5.5.3	Step 3: Define the recovery user ID.....	5-6
5.5.4	Step 4: Determine DRDA location name for DB2/VM instance.....	5-6

## 6 Configuring Microsoft SNA Server or Host Integration Server

6.1	Before You Begin.....	6-1
6.2	Steps for Configuring the Communications Interfaces.....	6-1
6.3	Creating SNA Server Profiles for the Gateway .....	6-2
6.3.1	Independent Versus Dependent LUs .....	6-2
6.4	Creating SNA Definitions for the Gateway .....	6-2
6.4.1	Sample SNA Server Definitions .....	6-2
6.4.2	Definition Types.....	6-3
6.4.3	SNA Server Definitions.....	6-3
6.4.3.1	Server Selection .....	6-4
6.4.3.2	Service Properties .....	6-5
6.4.3.3	Link Service Definition .....	6-5
6.4.3.4	Connection Definition .....	6-7
6.4.3.5	Local LU Definition .....	6-9
6.4.3.6	Mode Definition .....	6-11
6.4.3.7	Remote LU Definition .....	6-13
6.4.3.8	CPI-C Symbolic Destination Names .....	6-14
6.5	Testing the Connection .....	6-15
6.6	Using SNA Session Security Validation .....	6-16
6.7	SNA Conversation Security.....	6-16
6.7.1	SNA Security Option SECURITY=PROGRAM.....	6-17
6.7.2	SNA Security Option SECURITY=SAME .....	6-17

## 7 Configuring IBM Communication Server

7.1	Before You Begin.....	7-1
7.2	Checklist for Configuring the Communications Interfaces.....	7-1
7.3	Creating IBM Communication Server Profiles for the Gateway .....	7-1
7.3.1	Independent Versus Dependent LUs .....	7-2
7.3.2	Creating SNA Definitions for the Gateway .....	7-2
7.3.2.1	Sample IBM Communication Server Definitions .....	7-2
7.4	Definition Types.....	7-3
7.4.1	IBM Communication Server Definitions.....	7-3
7.4.1.1	Creating the Configuration .....	7-3
7.4.1.2	Defining the Node.....	7-4
7.5	Testing the Connection .....	7-17
7.6	Using SNA Session Security Validation .....	7-18
7.7	SNA Conversation Security.....	7-18
7.7.1	SNA Security Option SECURITY=PROGRAM.....	7-19

7.7.2	SNA Security Option SECURITY=SAME .....	7-19
-------	---	------

## 8 Configuring TCP/IP

8.1	Before You Begin.....	8-1
8.1.1	Port Number.....	8-1
8.2	Configuring TCP/IP .....	8-1

## 9 Oracle Net

9.1	Checklists for Oracle Net .....	9-1
9.1.1	Configuring Oracle Net .....	9-1
9.1.2	Advanced Security Encryption .....	9-1
9.1.2.1	Setting Up Advanced Security Encryption for Test .....	9-1
9.1.2.2	Testing Advanced Security Encryptions.....	9-1
9.2	Oracle Net and SQL*Net Introduction .....	9-2
9.3	Oracle Net Overview .....	9-2
9.3.1	Distributed Processing.....	9-2
9.3.2	Distributed Database.....	9-2
9.3.3	Terminology for Oracle Net.....	9-2
9.4	Configuring Oracle Net .....	9-3
9.4.1	Step 1: Modify the listener.ora file .....	9-3
9.4.2	Step 2: Modify the tnsnames.ora file.....	9-3
9.5	Advanced Security Encryption.....	9-4
9.6	Setting Up Advanced Security Encryption for Test.....	9-4
9.6.1	Step 1: Set Advanced Security Encryption Parameters for the Gateway .....	9-4
9.6.2	Step 2: Set Advanced Security Encryption Parameters.....	9-5
9.7	Testing Advanced Security Encryptions .....	9-5
9.7.1	Step 1: Connect the Gateway and Oracle the Integrating Server.....	9-5
9.7.2	Step 2: Reset Configuration Parameters on the Gateway .....	9-5

## 10 Configuring the Gateway

10.1	Configuration Checklist .....	10-1
10.2	Choosing a Gateway System Identifier (SID) .....	10-2
10.2.1	Enter the SID on the Worksheet .....	10-3
10.3	Gateway Configuration.....	10-3
10.4	Configuring the Host.....	10-3
10.4.1	Step 1: Copy the gateway initialization .....	10-3
10.4.2	Step 2: Determine settings for gateway initialization parameters.....	10-3
10.4.2.1	Required Parameters.....	10-4
10.4.2.2	Optional Parameters .....	10-4
10.4.3	Step 3: Tailor the initsid.ora File.....	10-4
10.4.4	Binding the DRDA Gateway Package .....	10-5
10.4.5	Binding Packages on DB2/Universal Database (DB2/UDB) .....	10-5
10.5	DRDA Gateway Package Considerations .....	10-6
10.5.1	Before Binding the DRDA Gateway Package.....	10-6
10.5.1.1	Step 1: Check all DRDA parameter settings .....	10-6
10.5.1.2	Step 2: If using DB2/UDB, then create ORACLE2PC table .....	10-7

10.5.2	Sample SQL scripts .....	10-7
10.5.2.1	Step 1: Run Data Dictionary scripts .....	10-7
10.5.2.2	Step 1a: Upgrading from a previous gateway version .....	10-7
10.5.2.3	Step 1b: Creating the Data Dictionary tables and views .....	10-7
10.5.2.4	Step 2: DB2/UDB or other server.....	10-7
10.5.2.5	Step 2a: If server is DB2/UDB, then grant authority to package .....	10-8
10.5.2.6	Step 2b: If server is not DB2/UDB, then create the ORACLE2PC table .....	10-8
10.6	Backup and Recovery of Gateway Configuration.....	10-8
10.7	Configuring the Oracle Integrating Server .....	10-8
10.7.1	Step 1: Create a database link.....	10-8
10.7.2	Step 2: Create synonyms and views.....	10-8
10.8	Accessing the Gateway from Other Oracle Servers .....	10-8
10.9	Accessing Other DRDA Servers .....	10-9
10.10	Gateway Installation and Configuration Complete.....	10-9

## 11 Using the Gateway

11.1	Processing a Database Link .....	11-1
11.1.1	Creating Database Links .....	11-1
11.1.2	Guidelines for Database Links .....	11-2
11.1.3	Dropping Database Links.....	11-2
11.1.4	Examining Available Database Links .....	11-2
11.1.5	Limiting the Number of Active Database Links .....	11-2
11.2	Accessing the Gateway .....	11-3
11.2.1	Step 1: Log in to the Oracle integrating server .....	11-3
11.2.2	Step 2: Create a database link to the DRDA database .....	11-3
11.2.3	Step 3: Retrieve data from the DRDA database .....	11-3
11.3	Accessing AS/400 File Members .....	11-3
11.4	Using the Synonym Feature .....	11-3
11.5	Performing Distributed Queries .....	11-4
11.5.1	Example of a Distributed Query.....	11-4
11.5.2	Two-Phase Commit Processing .....	11-5
11.5.3	Distributed DRDA Transactions .....	11-5
11.6	Read-Only Gateway .....	11-5
11.7	Replicating in a Heterogeneous Environment .....	11-6
11.7.1	Oracle Database 10g Server Triggers .....	11-6
11.7.2	Oracle Snapshots .....	11-6
11.8	Copying Data from the Oracle Server to the DRDA Server .....	11-6
11.9	Copying Data from the DRDA Server to the Oracle Server .....	11-6
11.10	Tracing SQL Statements .....	11-7

## 12 Developing Applications

12.1	Gateway Appearance to Application Programs.....	12-1
12.1.1	Fetch Reblocking .....	12-2
12.2	Using Oracle Stored Procedures with the Gateway .....	12-2
12.3	Using DRDA Server Stored Procedures with the Gateway .....	12-3
12.3.1	Oracle Application and DRDA Server Stored Procedure Completion .....	12-4
12.3.2	Procedural Feature Considerations with DB2 .....	12-5



12.4	Database Link Behavior .....	12-5
12.5	Oracle Server SQL Construct Processing .....	12-6
12.5.1	Compatible SQL Functions .....	12-6
12.5.2	Translated SQL Functions .....	12-6
12.5.3	Compensated SQL Functions.....	12-6
12.5.4	Native Semantic SQL Functions .....	12-7
12.5.5	DB2/OS390 SQL Compatibility.....	12-7
12.5.6	DB2/Universal Database SQL Compatibility.....	12-9
12.5.7	DB2/400 SQL Compatibility .....	12-12
12.5.8	DB2/VM SQL Compatibility .....	12-15
12.6	Native Semantics.....	12-18
12.6.1	SQL Functions That Can Be Enabled .....	12-18
12.6.2	SQL Functions That Can Be Disabled.....	12-19
12.6.3	SQL Set Operators and Clauses .....	12-19
12.7	DRDA Data Type to Oracle Data Type Conversion .....	12-20
12.7.1	Performing Character String Operations .....	12-21
12.7.2	Converting Character String data types .....	12-21
12.7.3	Performing Graphic String Operations .....	12-21
12.7.4	Performing Date and Time Operations .....	12-22
12.7.4.1	Processing TIME and TIMESTAMP Data.....	12-22
12.7.4.2	Processing DATE Data.....	12-22
12.7.4.3	Performing Date Arithmetic .....	12-23
12.7.5	Dates .....	12-23
12.7.6	HS_NLS_DATE_FORMAT Support .....	12-24
12.7.7	Oracle TO_DATE Function .....	12-24
12.7.8	Performing Numeric Data Type Operations .....	12-25
12.7.9	Mapping the COUNT Function.....	12-25
12.7.10	Performing Zoned Decimal Operations .....	12-25
12.8	Passing Native SQL Statements through the Gateway .....	12-25
12.8.1	Processing DDL Statements through Passthrough.....	12-26
12.8.2	Using the DBMS_HS_PASSTHROUGH.EXECUTE_IMMEDIATE Function .....	12-26
12.8.2.1	Examples.....	12-27
12.8.3	Retrieving Result Sets Through Passthrough.....	12-27
12.8.3.1	Example .....	12-27
12.9	Oracle Data Dictionary Emulation on a DRDA Server .....	12-28
12.9.1	Using the Gateway Data Dictionary .....	12-28
12.9.2	Using the DRDA Catalog.....	12-28
12.10	Defining the Number of DRDA Cursors.....	12-28

## 13 Security Considerations

13.1	Security Overview .....	13-1
13.2	Authenticating Application Logons.....	13-1
13.3	Defining and Controlling Database Links.....	13-2
13.3.1	Link Accessibility.....	13-2
13.3.2	Links and CONNECT Clauses.....	13-2
13.4	TCP/IP Security .....	13-3
13.5	Processing Inbound Connections .....	13-3

13.5.1	User ID Mapping .....	13-3
13.5.1.1	DB2/OS390 .....	13-3
13.5.1.2	DB2/VM .....	13-4
13.5.1.3	DB2/400 .....	13-4
13.5.1.4	DB2/Universal Database.....	13-4
13.6	Passwords in the Gateway Initialization File .....	13-5

## 14 Migration and Coexistence with Existing Gateways

14.1	Migrating Existing V4, V8, or V9 Gateway Instances to New Release .....	14-1
14.1.1	Step 1: Install the new Release .....	14-1
14.1.2	Step 2: Transferring <i>initsid.gtwboot</i> Gateway Boot Initialization parameters. ....	14-1
14.1.3	Step 3: Transferring <i>initsid.ora</i> gateway initialization file parameters. ....	14-2
14.2	Backout Considerations When Migrating to New Releases.....	14-2
14.3	New and Changed Parameters When Migrating to Release 10.....	14-2
14.3.1	New Parameters.....	14-2
14.3.1.1	New Gateway Initialization File Parameters.....	14-2
14.3.2	Parameters That Have Been Changed in Usage.....	14-3
14.3.3	Parameters That Have Been Renamed .....	14-3
14.3.4	Obsolete Parameters.....	14-3
14.4	DRDA Server Considerations .....	14-4
14.5	Oracle Net Considerations.....	14-4

## 15 Error Messages, Diagnosis, and Reporting

15.1	Interpreting Gateway Error Messages .....	15-1
15.1.1	Errors Detected by the Oracle Integrating Server .....	15-1
15.1.2	Errors Detected by the Gateway.....	15-2
15.1.3	Errors Detected in the DRDA Software.....	15-2
15.1.4	Communication Errors .....	15-2
15.1.5	Errors Detected by the Server Database.....	15-3
15.2	Mapped Errors .....	15-3
15.3	Gateway Error Codes .....	15-4
15.4	SQL Tracing and the Gateway .....	15-5
15.4.1	SQL Tracing in the Oracle Database .....	15-5
15.4.2	SQL Tracing in the Gateway .....	15-5

## A Oracle DB2 Data Dictionary Views

A.1	Supported Views.....	A-1
A.2	Data Dictionary View Tables.....	A-2
A.2.1	ALL_CATALOG .....	A-2
A.2.2	ALL_COL_COMMENTS .....	A-2
A.2.3	ALL_CONS_COLUMNS .....	A-2
A.2.4	ALL_CONSTRAINTS .....	A-3
A.2.5	ALL_INDEXES .....	A-3
A.2.6	ALL_IND_COLUMNS.....	A-5
A.2.7	ALL_OBJECTS .....	A-5
A.2.8	ALL_SYNONYMS .....	A-6

A.2.9	ALL_TABLES .....	A-6
A.2.10	ALL_TAB_COLUMNS .....	A-7
A.2.11	ALL_TAB_COMMENTS .....	A-8
A.2.12	ALL_USERS .....	A-9
A.2.13	ALL_VIEWS .....	A-9
A.2.14	COLUMN_PRIVILEGES .....	A-9
A.2.15	DICTIONARY .....	A-10
A.2.16	DUAL .....	A-10
A.2.17	TABLE_PRIVILEGES .....	A-10
A.2.18	USER_CATALOG .....	A-10
A.2.19	USER_COL_COMMENTS .....	A-10
A.2.20	USER_CONSTRAINTS .....	A-11
A.2.21	USER_CONS_COLUMNS .....	A-11
A.2.22	USER_INDEXES .....	A-11
A.2.23	USER_OBJECTS .....	A-13
A.2.24	USER_SYNONYMS .....	A-13
A.2.25	USER_TABLES .....	A-14
A.2.26	USER_TAB_COLUMNS .....	A-15
A.2.27	USER_TAB_COMMENTS .....	A-16
A.2.28	USER_USERS.....	A-16
A.2.29	USER_VIEWS.....	A-17

## **B Sample Files**

B.1	Sample gateway initialization file .....	B-1
B.2	Sample Oracle Net tnsnames.ora File .....	B-2
B.3	Sample Oracle Net listener.ora File .....	B-2

## **C DRDA-Specific Parameters**

C.1	Modifying the Gateway Initialization File .....	C-1
C.2	Setting Parameters in the Gateway Initialization File .....	C-1
C.3	Syntax and Usage.....	C-1
C.4	Gateway Initialization File Parameters.....	C-2
C.4.1	DRDA_CACHE_TABLE_DESC .....	C-2
C.4.2	DRDA_CAPABILITY .....	C-2
C.4.3	DRDA_CODEPAGE_MAP .....	C-2
C.4.4	DRDA_COMM_BUFLN.....	C-2
C.4.5	DRDA_CONNECT_PARM (SNA format) .....	C-3
C.4.6	DRDA_CONNECT_PARM (TCP/IP format) .....	C-3
C.4.7	DRDA_CMSRC_CM_IMMEDIATE .....	C-3
C.4.8	DRDA_DEFAULT_CCSD .....	C-3
C.4.9	DRDA_DESCRIBE_TABLE .....	C-4
C.4.10	DRDA_DISABLE_CALL .....	C-4
C.4.11	DRDA_FLUSH_CACHE .....	C-4
C.4.12	DRDA_GRAPHIC_PAD_SIZE .....	C-4
C.4.13	DRDA_GRAPHIC_LIT_CHECK .....	C-5
C.4.14	DRDA_GRAPHIC_TO_MBCS .....	C-5

C.4.15	DRDA_GRAPHIC_CHAR_SIZE .....	C-5
C.4.16	DRDA_ISOLATION_LEVEL .....	C-5
C.4.17	DRDA_LOCAL_NODE_NAME .....	C-6
C.4.18	DRDA_MBCS_TO_GRAPHIC .....	C-6
C.4.19	DRDA_OPTIMIZE_QUERY .....	C-6
C.4.20	DRDA_PACKAGE_COLLID .....	C-7
C.4.21	DRDA_PACKAGE_CONSTOKEN .....	C-7
C.4.22	DRDA_PACKAGE_NAME .....	C-7
C.4.23	DRDA_PACKAGE_OWNER .....	C-7
C.4.24	DRDA_PACKAGE_SECTIONS .....	C-8
C.4.25	DRDA_READ_ONLY .....	C-8
C.4.26	DRDA_RECOVERY_PASSWORD .....	C-8
C.4.27	DRDA_RECOVERY_USERID .....	C-8
C.4.28	DRDA_REMOTE_DB_NAME .....	C-9
C.4.29	DRDA_SECURITY_TYPE .....	C-9
C.4.30	FDS_CLASS .....	C-9
C.4.31	FDS_CLASS_VERSION .....	C-9
C.4.32	FDS_INSTANCE .....	C-10
C.4.33	HS_FDS_FETCH_ROWS .....	C-10
C.4.34	HS_LANGUAGE .....	C-10
C.4.35	HS-NLS_NCHAR .....	C-10
C.4.36	LOG_DESTINATION .....	C-11
C.4.37	ORA_MAX_DATE .....	C-11
C.4.38	ORA-NLS10 .....	C-11
C.4.39	ORACLE_DRDA_TCTL .....	C-11
C.4.40	ORACLE_DRDA_TRACE .....	C-11
C.4.41	TRACE_LEVEL .....	C-12

## D National Language Support

D.1	Overview of NLS Interactions.....	D-1
D.2	Client and Oracle Integrating Server Configuration .....	D-3
D.3	Gateway Language Interaction with DRDA Server .....	D-4
D.3.1	Gateway Configuration .....	D-4
D.3.2	NLS Parameters in the Gateway Initialization File.....	D-4
D.3.2.1	<b>HS_LANGUAGE</b> .....	D-5
D.3.2.2	HS-NLS_NCHAR .....	D-5
D.3.2.3	<b>HS-NLS_DATE_FORMAT</b> .....	D-5
D.3.2.4	<b>HS-NLS_DATE_LANGUAGE</b> .....	D-5
D.4	Gateway Codepage Map Facility .....	D-5
D.5	Multibyte and Double-Byte Support in the Gateway.....	D-8
D.6	Message Availability .....	D-10
D.7	Example of NLS Configuration.....	D-10

**E Configuration Worksheet**

**F Quick Reference to Oracle SQL Functions**

**G Sample Applications**

G.1	DB2INS	.....	G-1
G.2	ORAIND	.....	G-2

**Index**



---

---

# Preface

The Oracle Transparent Gateway for DRDA for Microsoft Windows provides users with transparent access to DRDA databases as if they were Oracle databases.

## Audience

This guide is intended for anyone responsible for installing, configuring, and administering the gateway, and also for application developers.

Read this guide if you are responsible for tasks such as:

- Installing and configuring the Oracle Transparent Gateway for DRDA
- Setting up gateway security
- Diagnosing gateway errors
- Using the gateway to access tables in DRDA databases
- Writing applications that access DRDA databases through the gateway
- Configuring the SNA server product

You must understand the fundamentals of transparent gateways and the Microsoft Windows operating system before using this guide to install or administer the gateway.

## Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at <http://www.oracle.com/accessibility/>.

### Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

## Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

## TTY Access to Oracle Support Services

To reach AT&T Customer Assistants, dial 711 or 1.800.855.2880. An AT&T Customer Assistant will relay information between the customer and Oracle Support Services at 1.800.223.1711. Complete instructions for using the AT&T relay services are available at <http://www.consumer.att.com/relay/tty/standard2.html>. After the AT&T Customer Assistant contacts Oracle Support Services, an Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process.

## Related Documents

The *Oracle Transparent Gateway for DRDA Installation and User's Guide for Microsoft Windows* is included as part of your product. Also included is:

*Oracle Database Heterogeneous Connectivity Administrator's Guide*

This guide contains information common to all heterogeneous gateways, including important information on functions, parameters, and error messages.

*Oracle Database Administrator's Guide*

*Oracle Database Concepts*

*Oracle Database Error Messages*

*Oracle Database Performance Tuning Guide*

*Oracle Database Security Guide*

*Oracle Database Heterogeneous Connectivity Administrator's Guide*

## Conventions

In this manual, "Windows" refers to any Microsoft Windows operating system.

In examples, an implied carriage return occurs at the end of each line, unless otherwise noted. You must press the **Return** key at the end of a line of input.

Examples of input and output for the gateway and the Oracle environment are shown in a special font:

```
> mkdir D:\ORACLE\your_name
```

All output is shown as it actually appears. For input, refer to the following list. The first part of each line represents the conventions used in this manual, and the second part describes their meanings:

... Horizontal ellipsis points in statements or commands mean that parts of the statement or command (that are not directly related to the example) have been omitted. Vertical ellipsis points in an example also mean that information that is not directly related to the example has been omitted.

*italic font* indicates that a word or phrase of your choice must be substituted for the term in *italic font*, such as your actual member name or directory name.

**boldface text** **Boldface type** in text indicates a term that is defined in the text.



< > Angle brackets enclose user-supplied names.

{ } Curly braces indicate that one of the enclosed arguments is required. Do not enter the braces themselves.

[ ] Square brackets indicate that the enclosed arguments are optional. You can choose one or none. Do not enter the brackets themselves.

| Vertical lines separate choices.

Other punctuation, such as commas, quotes, or the pipe symbol (|), must be entered as shown unless otherwise specified. Directory names, file IDs, and so on, appear in examples. When these names appear in text, they may be highlighted in **bold**. The use of *italics* indicates that those portions of a file ID that appear in *italics* can vary.

## SQL\*Plus Prompts

The SQL\*Plus prompt, `SQL>`, appears in SQL statements and SQL\*Plus command examples. Enter your response at the prompt. Do not enter the text of the prompt, "`SQL>`", in your response.

## DOS Prompts

The DOS prompt, `>`, appears in DOS command examples. Enter your response at the prompt. Do not enter the text of the prompt, "`>`", in your response. A dollar sign (\$) is part of some DOS directory names and should not be confused as a prompt character.

## Storage Measurements

Storage measurements use the following abbreviations:

- KB, for kilobyte, which equals 1,024 bytes
- MB, for megabyte, which equals 1,048,576 bytes
- GB, for gigabyte, which equals 1,073,741,824 bytes

## Directory Names

Throughout this document, there are references to the directories in which product-related files reside. `ORACLE_HOME` is used to represent the Oracle home directory. This is the default location for Oracle products. If you have installed into a location other than `ORACLE_HOME`, replace all references to `ORACLE_HOME` with the drive and path specification you have used.



---

---

# Introduction

The Oracle Transparent Gateway for DRDA enables you to:

- Integrate heterogeneous database management systems so that they appear as a single homogeneous database system
- Read and write data from Oracle applications to data in DB2/OS390, DB2/400, DB2 Universal Database, DB2/VM, and IBM SQL/DS on VM databases in addition to any Oracle database server data.

Read this chapter for information about the architecture, uses, and features of the Oracle Transparent Gateway for DRDA. It contains the following sections:

- [Introduction to the Oracle Transparent Gateway](#)
- [Release 10g Gateways](#)
- [Gateway Capabilities](#)
- [Terms](#)
- [Architecture](#)
- [Implementation](#)
- [How the Gateway Works](#)
- [Oracle Tools and the Gateway](#)
- [Features](#)

## 1.1 Introduction to the Oracle Transparent Gateway

In today's global economy, information is a company's most valuable resource. Whether you need to analyze new markets, tailor your products to meet local demands, increase your ability to handle complex customer information, or streamline operations, your company requires instant access to current and complete information

Company growth and diversification often mean functioning with a collage of applications and geographically scattered data that may be using incompatible networks, platforms, and storage formats. Diverse application standards and storage formats can make integration of information difficult. Oracle offers integration technologies to overcome these technical barriers. Oracle Enterprise Integration Gateways simplify complex systems and remove obstacles to information, thereby providing your company the opportunity to focus on business.

### 1.1.1 Protection of Current Investment

Oracle Transparent Gateway for DRDA gives your company the ability to develop its information systems without forfeiting its investments in current data and applications. The gateway gives you access to the Oracle and DB2 data with a single set of applications while you continue to use existing IBM applications to access your DB2 data. You can also use more productive database tools and move to a distributed database technology without giving up access to the current data.

If you choose to migrate to Oracle Database technology and productivity, then the gateway enables you to control the pace of your migration. As you transfer applications from your previous technology to the Oracle Database, you can use the gateway to move the DB2 data into Oracle databases.

## 1.2 Release 10g Gateways

Oracle Database 10g provides the foundation for the next generation of the Oracle Enterprise Integration Gateways Release 10g, which will deliver enhanced integration capabilities by exploiting Oracle Database 10g Heterogeneous Services. Heterogeneous Services is a component of the Oracle Database 10g server. The Oracle Database 10g server provides the common architecture for future generations of the gateways. For detailed information on Oracle Heterogeneous Services, refer to *Oracle Database Heterogeneous Connectivity Administrator's Guide*.

The version 10 gateways are even more tightly integrated with the Oracle Database 10g server than previous versions, enabling improved performance and enhanced functionality while still providing transparent integration of Oracle and non-Oracle data. For example, connection initialization information is available in the local Oracle Database 10g server, reducing the number of round trips and the amount of data sent over the network. SQL processing is also faster, because statements that are run by an application are parsed and translated once and can then be reused by multiple applications.

Release 10g gateways leverage any enhancements in the Oracle Database 10g server, and you can quickly extend those benefits to the non-Oracle data.

### 1.2.1 Advantages of the Gateway

Oracle Transparent Gateway for DRDA enables Oracle applications to access the DRDA Application Servers, such as DB2 for OS/390 (MVS), through Structured Query Language (SQL). The gateway and the Oracle Database 10g server together create the appearance that all data resides on a local Oracle Database 10g server, though data might be widely distributed. If data is moved from a DRDA Application Server database to an Oracle Database server, then no changes in application design or function are needed. The gateway handles all differences in both data types and SQL functions between the application and the database.

## 1.3 Gateway Capabilities

Oracle Transparent Gateway for DRDA gives you the power to integrate your heterogeneous systems into a single, seamless environment. This integration enables you to make full use of existing hardware and applications throughout your corporatewide environment. You can eliminate the need to rewrite applications for each configuration, and you can avoid the tedious, error-prone process of manual data transfer. Together with the Oracle tools, networking, and data server technology, the Oracle Transparent Gateway for DRDA sets a high standard for seamless, enterprise wide information access.

Oracle Transparent Gateway for DRDA enables applications to read and update DB2 data and Oracle data as if all of the data were stored in a single database. As a result, users and application programmers are not required to know either the physical location or the storage characteristics of the data. This transparency not only permits you to integrate heterogeneous data seamlessly, but also simplifies your gateway implementation, application development, and maintenance.

### 1.3.1 Transparency at All Levels

The Oracle Transparent Gateway for DRDA gives you transparency at every level within your enterprise.

- Location transparency  
Users can access tables by name without needing to understand the physical location of the tables.
- Network transparency  
The gateways exploit Oracle Net technology to enable users to access data across multiple networks without concern for the network architecture or protocols. TCP/IP protocol is supported.
- Operating system transparency  
You can access data that is stored under multiple operating systems without being aware of the operating systems that hold the data.
- Data storage transparency  
Data can be accessed regardless of the database or file format.
- Access method transparency  
You can use a single dialect of SQL for any data store, eliminating the need to code for database-specific access methods or SQL implementations.

### 1.3.2 Extended Database Services

Following are some of the more sophisticated Oracle Database 10g server services that are available through the gateway.

- SQL functions  
Your application can access all of your data using Oracle SQL, which is rich in features. Advanced Oracle Database 10g server functions, such as outer joins, are available even if the target data stores do not support them in a native environment. The method by which the gateways are integrated with the Oracle Database 10g server ensures that the newest features of each database release are always available immediately to the gateway.
- Distributed capabilities  
Heterogeneous data can be integrated seamlessly because Oracle Database distributed capabilities, such as `JOIN` and `UNION`, can be applied to non-Oracle data without any special programming or mapping.
- Distributed query optimization  
The Oracle Database 10g server can use its advanced query optimization techniques to ensure that SQL statements are run efficiently against any of your data. The data distribution and storage characteristics of local and remote data are equally considered.

- Two-phase commit protection

The Oracle server two-phase commit mechanism provides consistency across data stores by ensuring that a transaction that spans data stores is still treated as a single unit of work. Changes are not committed (or permanently stored) in any data store unless the changes can be committed in all data stores that will be affected.
- Stored procedures and database triggers

The same Oracle stored procedures and database triggers can be used to access all of the data, thereby ensuring uniform enforcement of business rules across the enterprise.

### 1.3.3 Extended Advanced Networking, Internet and Intranet Support

The gateway integration with the Oracle Database 10g server extends (to non-Oracle data) the benefits of the Oracle Internet software, and Oracle Net software and extends the benefits of the Oracle client/server and server/server connectivity software. These powerful features include:

- Application server support

Any Internet or intranet application that can access data in Oracle database can also incorporate information from data stores that are accessible through the gateways. Web browsers can connect to Oracle database using any application server product that supports Oracle software.
- Implicit protocol conversion

Oracle Database and Oracle Net can work together as a protocol converter, enabling applications to transparently access other data stores on platforms that do not support the network protocol of the client. An Oracle Database 10g server can use TCP/IP to communicate with the gateway and another data store.
- Advanced Security

Non-Oracle data can be protected from unauthorized access or tampering during transmission to the client. This is done by using the hardware-independent and protocol-independent encryption and CHECKSUM services of Advanced Security.
- Wireless communication

Oracle Mobile Agents, an industry-leading Oracle mobile technology, enables wireless communication to Oracle Database 10g servers or to any databases that are accessible through the gateways. This gives your field personnel direct access to enterprise data from mobile laptop computers.

### 1.3.4 Dynamic Dictionary Mapping

The simple setup of the gateway does not require any additional mapping. Before an application can access any information, the application must be told the structure of the data, such as the columns of a table and their lengths. Many products require administrators to manually define that information in a separate data dictionary stored in a hub. Applications then access the information using the hub dictionary instead of the native dictionaries of each database. This approach requires a great deal of manual configuration and maintenance on your part. As administrators, you must update the data dictionary in the hub whenever the structure of a remote table is changed.

Inefficient duplication is not necessary with Oracle Transparent Gateway for DRDA. The gateway uses the existing native dictionaries of each database. The applications access data using the dictionaries that are designed specifically for each database, which means that no redundant dictionary ever needs to be created or maintained.

### 1.3.5 SQL

Oracle Transparent Gateways ease application development and maintenance by enabling you to access any data using a uniform set of SQL queries. Changes to the location, storage characteristics, or table structure do not require any changes to the applications. ANSI and ISO standard SQL are supported, along with powerful Oracle extensions.

### 1.3.6 Data Definition Language

Oracle applications can create tables in target data stores by using native data definition language (DDL) statements.

### 1.3.7 Data Control Language

You can run native data control language (DCL) statements from an Oracle environment, enabling central administration of user privileges and access levels for heterogeneous data stores.

### 1.3.8 Passthrough and Native DB2 SQL

Running of native DB2 SQL can be passed through the gateway for processing directly against DB2. This enables applications to send statements, such as a DB2 CREATE TABLE, to the gateway for running on a target DB2 system.

### 1.3.9 Stored Procedures

The gateway enables you to exploit both Oracle and non-Oracle stored procedures, leveraging your investments in a distributed, multi database environment. Oracle stored procedures can access multiple data stores easily, without any special coding for heterogeneous data access.

#### 1.3.9.1 Oracle Stored Procedures

Oracle stored procedures enable you to access and update DB2 data by using centralized business rules that are stored in the Oracle Database 10g server. Using Oracle stored procedures can increase database performance by minimizing network traffic. Instead of sending individual SQL statements across the network, an application can send a single EXECUTE command to begin an entire PL/SQL routine.

#### 1.3.9.2 Native DB2 Stored Procedures

The gateway can run DB2 stored procedures using standard Oracle PL/SQL. The Oracle application run the DB2 stored procedure as if it were an Oracle remote procedure.

### 1.3.10 Languages

Any application or tool that supports the Oracle Database 10g server can access over thirty different data sources through the Oracle gateways. A wide variety of open system tools from Oracle and third-party vendors can be used, even if the data is

stored in legacy, proprietary formats. Hundreds of tools are supported, including ad hoc query tools, Web browsers, turnkey applications, and application development tools.

### 1.3.11 Oracle Database Server Technology and Tools

The gateway is integrated into the Oracle Database server technology, which provides global query optimization, transaction coordination for multisite transactions, support for all Oracle Net configurations, and so on. Tools and applications that support the Oracle Database server can be used to access heterogeneous data through the gateway.

### 1.3.12 SQL\*Plus

You can use SQL\*Plus for moving data between databases. This product gives you the ability to copy data from your department databases to corporate Oracle databases.

### 1.3.13 Two-Phase Commit and Multisite Transactions

The gateway can participate as a partner in multisite transactions and two-phase commit. How this occurs depends on the capabilities of the underlying data source, meaning that the gateway can be implemented as any one of the following:

- A full two-phase commit partner
- A commit point site
- A single-site update partner
- A read-only partner

The deciding factors for the implementation of the gateway are the locking and transaction-handling capabilities of the target database.

Oracle Transparent Gateway for DRDA, by default, is configured as a commit point site (that is, commit confirm protocol). Optionally, you can configure the gateway as read-only if you choose to enforce read-only capability through the gateway. Other protocols are not supported. Refer to ["Read-Only Gateway"](#) on page 11-5 in [Chapter 11, "Using the Gateway"](#).

### 1.3.14 Site Autonomy

All Oracle Database server products, including gateways, supply site autonomy. For example, administration of a data source remains the responsibility of the original system administrator. Site autonomy also functions so that gateway products do not override the security measures that are established by the data source or the operating environment.

### 1.3.15 Migration and Coexistence

The integration of a data source through the gateway does not require any changes to be made to applications at the data source. The result is that the Oracle Database server technology is nonintrusive, providing coexistence and an easy migration path.

### 1.3.16 Security

The gateway does not bypass existing security mechanisms. Gateway security coexists with the security mechanisms that are already used in the operating environment of the data source.



Functionally, gateway security is identical to that of an Oracle Database server, as described in the *Oracle Database Administrator's Guide*. Oracle Database security is mapped to the data dictionary of the data source.

## 1.4 Terms

The terms that are used in this guide do not necessarily conform to IBM terminology. The following table presents several terms and their meanings as used within this guide:

Terms	Meaning
DRDA data	Any database data that is accessed through DRDA
DRDA database	The collection of data that belongs to a DRDA Server
DRDA Server	A database server that can be accessed through DRDA. IBM terminology for a DRDA Server is a DRDA Application Server, or AS.
DRDA server type	A specific database product or program that can act as a DRDA server
Oracle integrating server	Any Oracle Database 10g server instance that communicates with the Oracle Transparent Gateway for DRDA to distribute database access operations to a DRDA Server. The Oracle integrating server can also be used for non-gateway applications.
DB2 Universal Database	A generic name for the UNIX-based implementations of DB2. DB2/UDB is frequently used as an abbreviation for DB2 Universal Database.

## 1.5 Architecture

The Oracle Transparent Gateway for DRDA works with the Oracle Database 10g server to shield most of the differences of the non-Oracle database from Oracle applications. This means that the Oracle applications can access the Oracle Database 10g server data and also can access the DRDA database data as if it were Oracle data located at the Oracle integrating server.

The architecture consists of the following main components:

- Client

The client is an Oracle application or tool.

- Oracle integrating server

The Oracle integrating server is an Oracle Database instance that is accessed by an Oracle Database 10g server with procedural and distributed options. Usually, the Oracle integrating server is installed on the same host as the gateway, but this is not a requirement. The Oracle integrating server and the gateway communicate in the normal Oracle server-to-server manner.

If the Oracle integrating server is not on the host where the gateway resides, then you must install the correct Oracle networking software on the platform where the server resides. For Oracle Database 10g, you must install Oracle Net on the Oracle Database 10g server system.

- Oracle Transparent Gateway for DRDA

The gateway must be installed on hosts that are running the appropriate operating system.

If the Oracle integrating server is not on the same host, then you must also install Oracle Net so that the gateway and Oracle Database 10g server can communicate.

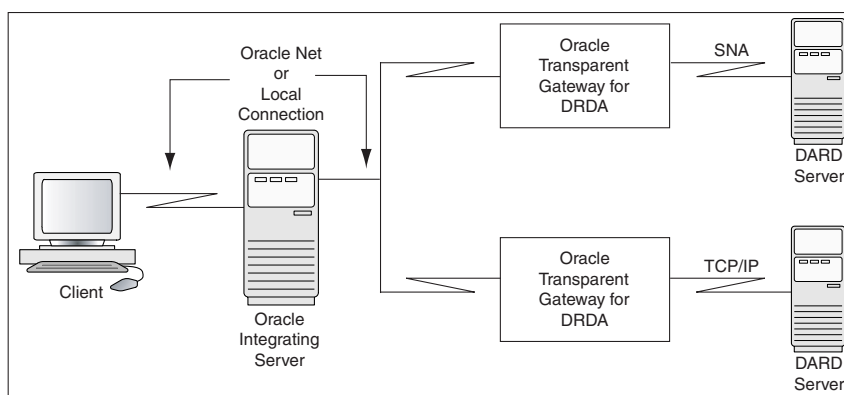
- DRDA Server

The DRDA Server must be a DB2/OS390, DB2/400, DB2 Universal Database, or DB2 server for VM database on a system that is accessible to the host using either the SNA or TCP/IP protocol.

Multiple Oracle Database 10g servers can access the same gateway. A single host gateway installation can be configured to access more than one DRDA Server.

Figure 1–1 illustrates the gateway architecture that was just described.

**Figure 1–1 The Gateway Architecture**



## 1.6 Implementation

When the gateway is installed on your host, it has some of the same components as an Oracle Database instance on Microsoft Windows. The gateway has the following components:

- A base file directory, similar to the one that is associated with the `ORACLE_HOME` environment variable of an Oracle Database instance
- A gateway system identifier (SID), comparable to the `ORACLE_SID` of an Oracle Database instance
- Oracle Net to support communication between the Oracle integrating server and the Oracle Transparent Gateway for DRDA

The gateway does not have:

- Control, redo log, or database files
- The full set of subdirectories and ancillary files that are associated with an installed Oracle Database 10g server

Because the gateway does not have background processes and does not need a management utility such as Oracle Enterprise Manager, you do not need to start the gateway product. Each Oracle Database 10g server user session that accesses a particular gateway creates an independent process on the host. This process runs the gateway session and runs SNA or TCP/IP functions to communicate with a DRDA Server.

## 1.7 How the Gateway Works

The gateway has no database functions of its own. Instead, it provides an interface by which an Oracle Database 10g server can direct part or all of a SQL operation to a DRDA database.

The gateway that is supporting the DRDA Server is identified to the Oracle integrating server by using a database link. The database link is the same construct that is used to identify other Oracle Database 10g server databases. Tables on the DRDA Server are referenced in SQL as:

```
table_name@dblink_name
```

or

```
owner.table_name@dblink_name
```

If you create synonyms or views in the Oracle integrating server database, then you can refer to tables on the DRDA Server by using simple names as though the table were local to the Oracle integrating server.

When the Oracle integrating server encounters a reference to a table that is on the DRDA Server, the applicable portion of the SQL statement is sent to the gateway for processing. Any host variables that are associated with the SQL statement are bound to the gateway and, therefore, to the DRDA Server.

The gateway is responsible for sending these SQL statements to the DRDA Server for processing and for fielding and is also responsible for returning responses. The responses are either data or messages. Any conversions between Oracle data types and DRDA data types are performed by the gateway. The Oracle integrating server and the application read and process only Oracle data types.

### 1.7.1 SQL Differences

Not all SQL implementations are the same. The Oracle Database 10g server supports a larger set of built-in functions than the databases that are currently accessed through the gateway. The Oracle integrating server and the gateway work together to convert SQL to a form that is compatible with the specific DRDA Server.

During this conversion, an Oracle Database 10g server function can be converted to a function that is recognizable to the specific DRDA Server. For example, the Oracle Database 10g server NVL function is converted to the DB2 VALUE function.

Alternatively, the Oracle integrating server withholds functions that are not executable by the DRDA Server, and it performs them after rows are fetched from the DRDA database. This processing generally applies to SELECT statements. The Oracle integrating server and the gateway cannot perform this kind of manipulation on UPDATE, INSERT, or DELETE statements because doing so changes transaction semantics.

## 1.8 Oracle Tools and the Gateway

Use the gateway to run applications, such as Oracle tools, that read and write data that is stored in DRDA databases.

Although the Oracle Transparent Gateway for DRDA provides no new application or development facilities, it extends the reach of existing Oracle tools to include data in non-Oracle databases that support DRDA.

Using the Oracle Transparent Gateway for DRDA with other Oracle products can greatly extend the capabilities of the standalone gateway. The following examples demonstrate how powerful the gateway is with other Oracle tools.

### 1.8.1 SQL\*Plus

Use SQL\*Plus and the Oracle Transparent Gateway for DRDA to create a distributed database system, providing an easy-to-use transfer facility for moving data between the distributed databases. One possible use is to distribute the data in your corporate Oracle Database to departmental DRDA databases. You can also distribute data in your corporate DRDA database to departmental Oracle Databases.

## 1.9 Features

Following is a list of important features that characterize this release of the gateway.

### 1.9.1 Heterogeneous Services Architecture

This release of the Oracle Transparent Gateway for DRDA uses the Oracle Heterogeneous Services component within the Oracle Database 10g server. Heterogeneous Services is the building block for the next generation of Oracle Enterprise Integration Gateways.

For detailed information about Heterogeneous Services, refer to the *Oracle Database Heterogeneous Connectivity Administrator's Guide*.

### 1.9.2 Performance Enhancements

Oracle Transparent Gateway for DRDA contains several internal performance enhancements. This product has shown major improvements in response time and CPU utilization for all relevant address spaces for a variety of workloads compared to version 9 gateways. The actual performance improvement at your site might vary, depending on your installation type and workload.

### 1.9.3 Fetch Reblocking

The array size of the application for `SELECT` is effective between the application and the Oracle integrating server. However, the array block size and the block fetch between the Oracle integrating server and the gateway are controlled by two Heterogeneous Services initialization parameters, `HS_RPC_FETCH_SIZE` and `HS_RPC_FETCH_REBLOCKING`. These parameters are specified in the gateway initialization file. Refer to the *Oracle Database Heterogeneous Connectivity Administrator's Guide* for more information.

### 1.9.4 Oracle Database 10g Passthrough Supported

You can use the Oracle Database 10g `DBMS_HS_PASSTHROUGH.EXECUTE_IMMEDIATE` feature to pass commands or statements (that are available in the DRDA database) through the gateway.

### 1.9.5 Retrieving Result Sets Through Passthrough

Oracle Transparent Gateway for DRDA provides a facility to retrieve result sets from a select SQL statement that is run with passthrough. Refer to ["Retrieving Result Sets Through Passthrough"](#) on page 12-27 for additional information.

## 1.9.6 Support for TCP/IP

This release of the gateway supports the TCP/IP communication protocol between the gateway and the DRDA Server. Refer to [Chapter 8, "Configuring TCP/IP"](#) for further information.

## 1.9.7 Native Semantics

This release of the gateway supports the ability to selectively enable or disable post-processing of various SQL functions by the DRDA Server. Refer to ["Native Semantics"](#) on page 12-18 for further information.

## 1.9.8 Columns Supported in a Result Set

Oracle Transparent Gateway for DRDA supports up to 1000 columns in a result set.

## 1.9.9 EXPLAIN\_PLAN Improvement

The EXPLAIN\_PLAN table contains the actual SQL statements passed to the DRDA Server from the Oracle Database 10g server through the gateway.

## 1.9.10 Heterogeneous Database Integration

The gateway support for ANSI-standard SQL enables read/write access to DRDA databases. Even if your data exists on different platforms in different applications, new applications can use all data, regardless of location.

## 1.9.11 Minimum Impact on Existing Systems

The gateway does not require installation of additional Oracle software on your OS/390 (MVS), AS/400, VM, UNIX or Microsoft Windows target system. The database interface that it uses is provided by IBM and is built into the DRDA database products and SNA or TCP/IP facilities that already exist on these platforms.

Configuring an IBM system for DRDA access typically consists of defining the SNA or TCP/IP resources involved and establishing access security definitions specific to the target database.

## 1.9.12 Large Base of Data Access

DRDA Application Server Function is supported by most IBM DB2 database products.

## 1.9.13 Application Portability

The ability of the gateway to interface with heterogeneous databases makes it possible to develop a single set of portable applications that can be used against both Oracle and IBM databases, and any other databases for which Oracle Corporation provides gateways.

## 1.9.14 Remote Data Access

Location flexibility is maximized because the gateway architecture permits network connections between each of the components. The application can use the Oracle client-server capability to connect to a remote Oracle integrating server through Oracle Net. The Oracle integrating server can connect to a remote gateway using a database

link. The gateway connects to DRDA Servers through SNA or TCP/IP network facilities.

The benefits of remote access are that it:

- Provides a means to allocate the suitable resource to a given task  
You can, for example, move application development off expensive processors and onto cost-efficient workstations or microcomputers.
- Expands the number of available data sources  
Without remote access, you are limited to the data that is available in the local environment. With remote access, your data sources are limited only by your networks.
- Provides a means to tailor an application environment to a given user  
For example, some users prefer a block-mode terminal environment, while others prefer a bit-mapped, graphics-driven terminal environment. Remote access can satisfy both because you are not constrained by the interface environment that is imposed by the location of your data.

### 1.9.15 Support for Distributed Applications

Because the gateway gives your application direct access to DRDA data, you eliminate the need to upload and download large quantities of database data to other processors. Instead, you can access data where it is, when you want it, without having to move the data between systems and thus risk unsynchronized and inconsistent data. Avoiding massive data replication can also reduce aggregate disk storage requirements over all of your systems.

However, if your system design requires moving data among the systems in a network, SQL\*Plus and the gateway can simplify the data transfer. With a single SQL\*Plus command, you can move entire sets of data from one node of the network to another and from one database to another.

You can pass commands and statements that are specific to your DRDA database through the gateway to be run by the DRDA database. For example, you can pass DB2/OS390 commands through the gateway for DB2 to run. You can also run stored procedures defined in non-Oracle databases.

### 1.9.16 Application Development and End User Tools

Through the gateway, Oracle extends the range of application development and user tools that you can use to access the IBM databases. These tools increase application development and user productivity by reducing prototype, development, and maintenance time. Current Oracle users do not have to learn a new set of tools to access data that is stored in DRDA databases. Instead, they can access Oracle and DRDA data with a single set of tools.

With the gateway and the application development tools that are available from Oracle, you can develop a single set of applications to access Oracle data and DRDA data. Users can use the decision support tools that are available from Oracle to access Oracle data and DRDA data. These tools can run on remote systems that are connected through Oracle Net to the Oracle integrating server.

When designing applications, keep in mind that the gateway is designed for retrieval and relatively light transaction loads. The gateway is not currently designed to be a heavy transaction processing system.

### 1.9.17 Password Encryption Utility

This release of the gateway includes a utility to support encryption of plain-text passwords in the gateway initialization file. Refer to [Chapter 13, "Security Considerations"](#) for details.

### 1.9.18 Support for DB2/OS390 V6, V7, and V8 Stored Procedures

This release of the gateway supports the native stored procedure catalogs in DB2 V6, V7, and V8 (`SYSIBM.SYSROUTINES` and `SYSIBM.SYSPARMS`).

### 1.9.19 Codepage Map Facility

This release of the gateway supports external mapping of IBM CCSIDs to Oracle character sets. Refer to ["Gateway Codepage Map Facility"](#) on page D-5 in [Appendix D, "National Language Support"](#).

### 1.9.20 IBM DB2 Universal Database Support

This release supports IBM DB2 Universal Database.

### 1.9.21 IBM DB2 Version 5.1 ASCII Tables

IBM DB2 version 5.1 supports ASCII and EBCDIC character sets. The character set selection is defined during table creation. The Oracle Transparent Gateway for DRDA supports access to EBCDIC tables and ASCII tables. Refer to [Appendix D, "National Language Support"](#).

### 1.9.22 Read-Only Support

This release enables the gateway to be configured as a read-only gateway. In this mode, no modifying of user data is permitted. For more information, refer to ["DRDA\\_READ\\_ONLY"](#) on page C-8.

### 1.9.23 Support for Graphic and Multibyte Data

This release of the gateway adds support for DB2 GRAPHIC and VARGRAPHIC data types. Refer to [Chapter 12, "Developing Applications"](#).

### 1.9.24 Support for DB2/UDB on Intel Hardware

This release of the gateway adds support for DRDA Servers running on Microsoft Windows and Linux on Intel hardware.

### 1.9.25 Data Dictionary Support for DB2/UDB

This release of the gateway adds Oracle data dictionary support for DB2 UDB V7. Refer to ["Sample SQL scripts"](#) for more information.





---

---

## Release Information

This chapter provides information specific to this release of the Oracle Transparent Gateway for DRDA. It includes the following sections:

- [Product Set](#)
- [Changes and Enhancements](#)
- [Bugs Fixed in 10g Release 2 \(10.2\)](#)
- [Known Problems](#)
- [Known Restrictions](#)

### 2.1 Product Set

The following is a list of the production components that are included in the product CD-ROM:

- Oracle Transparent Gateway for DRDA, Release 10.1.0.2.0
- Oracle Net, release 10.2.1.0

### 2.2 Changes and Enhancements

Following is a list of changes and enhancements that are unique to this release of the gateway.

#### **Gateway Password Encryption Tool**

The Gateway Password Encryption tool (`g4drpwd`) has been replaced by a generic feature which is now part of Heterogenous Services. Refer to [Chapter 13, "Security Considerations"](#) for more information.

#### **Product Migration**

Refer [Chapter 14, "Migration and Coexistence with Existing Gateways"](#) for information about migrating product configurations from previous releases for additional changes or requirements.

### 2.3 Bugs Fixed in 10g Release 2 (10.2)

4013463

GARBAGES CONTAINED IN ERROR MESSAGE FROM TG4DRDA

**3882675**

TG4DRDA SELECT FOR UPDATE ERROR WITH G4DRSRVD

**3650803**

MEMORY LEAK IN G4DRSRV DOING SELECT STATEMENT

**3640384**

ORA-28500 ON SELECT FOR UPDATE FROM TG4DRDA

**3610131**

INDEX STATS MAY NOT BE QUERIED CORRECTLY

**3514233**

SETTING DRDA\_OPTIMIZE\_QUERY=TRUE DOES NOT GENERATE TABLE STATS

**3429017**

LINKING ERROR FOR G4DRSRV WHEN USING REDHAT AS V3

**3421215**

IU GUIDE DIDN'T SAY HOW TO CONFIG DRDA\_CONNECT\_PARM IN LINUX

**3287626**

ENGLISH NAME OF "TAIWAN" DOESN'T SEEM TO BE APPROPRIATE

**3143686**

QA - 10G - CAN NOT SELECT FROM DATA DICTIONARY TABLES

**4218317**

COUNT(COLNAME) NOT TRANSLATED TO COUNT(\*)

**4260112**

ORA-1001 WITHOUT THE DETAIL RETURNS FROM TG4DRDA

**4065600**

GARBAGES CONTAINED IN ORA-1 ERROR MESSAGE FROM TG4DRDA

**3965425**

ORA-07445 [\_MEMCPY()+772] REPEATABLE READ ISOLATION LEVEL IS NOT WORKING

**3709345**

PSR 9.2.0.5.0 BREAKS CALL DB2 STORED PROCEDURE WITH DECIMAL PARM.  
SQLCODE -310

**3130329**

TG4DRDA LOOPS IF QRWTSRVR JOB KILLED WHILE GATEWAY IS IN GDJCRCV

## 2.4 Known Problems

The problems that are documented in the following section are specific to the Oracle Transparent Gateway for DRDA and are known to exist in this release of the product. These problems will be fixed in a future gateway release. If you have any questions or concerns about these problems, then contact Oracle Support Services.

A current list of problems is available online. Contact your local Oracle office for information about accessing this online information.

## 2.5 Known Restrictions

The following restrictions are known to exist for the products in this release. Restrictions are not scheduled to change in future releases. Also refer to [Chapter 12, "Developing Applications"](#), for information about limitations when developing your applications.

### Accessing DB2 Alias Objects

If you need to access DB2 alias objects on a remote DB2 system, then you must specify `DRDA_DESCRIBE_TABLE=FALSE` initialization parameter in the gateway initialization file.

### Oracle SQL Command INSERT

When copying data from an Oracle server to a DRDA Server, the Oracle SQL command `INSERT` is not supported. The SQL\*Plus `COPY` command must be used. Refer to [Chapter 11, "Using the Gateway"](#), for more information.

### 2.5.1 DB2 Considerations

#### DD Basic Tables and Views

The owner of DD basic tables and views is OTGDB2. This cannot be changed.

#### SUBSTR Function Post-Processed

The `SUBSTR` function can be used with the Oracle Server in ways that are not compatible with a DRDA Server database such as DB2/OS390. Therefore, the `SUBSTR` function is post-processed. However, it is possible to enable the server to process it natively using the "Native Semantics" feature. Refer to [Chapter 12, "Developing Applications"](#), for details.

#### AVS Mapping User IDs (DB2/VM)

APPC VTAM Support (AVS) has problems mapping user IDs that are sent using lowercase letters or special characters. Contact your IBM representative for additional information about this problem.

#### Support for DRDA Server Character Sets

Support (for character sets that are used by a DRDA Server) is configurable through the gateway Codepage Map Facility. Refer to [Appendix D, "National Language Support"](#) for more information.

#### data type Limitations

Refer to ["DRDA Data Type to Oracle Data Type Conversion"](#) on page 12-20 for detailed information about data types.

### **SAVEPOINT Command Is Not Supported**

Oracle Transparent Gateway for DRDA does not support the Oracle command `SAVEPOINT`.

### **Null Values and Stored Procedures**

Null values are not passed into, or returned from, calls to stored procedures through the gateway.

### **String Concatenation of Numbers**

String concatenation of numbers is not permitted in DB2/400, DB2/UDB, and DB2/OS390. For example, `2 || 2` is not permitted.

### **GLOBAL\_NAMES Initialization Parameter**

If `GLOBAL_NAMES` is set to `TRUE` in the Oracle server `INIT.ORA` file, then to be able to connect to the gateway, you must specify the Heterogeneous Services (HS) initialization parameters, `HS_DB_DOMAIN` and `HS_DB_NAME`, in the Gateway Initialization Parameter file to match the value of the Oracle server `DB_DOMAIN` parameter. Refer to [Chapter 10, "Configuring the Gateway"](#), for more information.

### **Binding the DRDA Package on DB2/UDB**

The DRDA gateway package must be bound on the DRDA Server before the gateway can perform any SQL operations. Because of a DB2/UDB restriction, the `ORACLE2PC` table must be created in the DB2/UDB database before the package can be bound. For details, refer to [Chapter 10, "Configuring the Gateway"](#).

### **Date Arithmetic**

In general, the following types of SQL expression forms do not work correctly with the gateway because of DRDA Server limitations:

*date + number*  
*number + date*  
*date - number*  
*date1 - date2*

DRDA Servers do not permit number addition or subtraction with date data types. The date and number addition and subtraction (*date + number*, *number + date*, *date - number*) forms are sent through to the DRDA Server where they are rejected.

Also, DRDA Servers do not perform date subtraction consistently. When you subtract two dates (*date1 - date2*), differing interpretations of date subtraction in the DRDA Servers cause the results to vary by server.

---

---

**Note:** Avoid date arithmetic expressions in all gateway SQL until date arithmetic problems are resolved.

---

---

### **Row Length Limitation**

Because of a restriction of the DRDA architecture, rows with aggregate length exceeding 32 K bytes in DRDA representation cannot be stored or retrieved.

### **LONG data type in SQL\*Plus**

SQL\*Plus cannot fetch LONG columns from the Oracle Transparent Gateway for DRDA.

### Dictionary Views Are Not Provided for DB2/VM

Currently, the Oracle Transparent Gateway for DRDA provides SQL for defining DB2/OS390, DB2/400, and DB2/UDB views that emulate parts of the Oracle Database dictionary. These are required for certain applications and tools that query dictionary tables. View definitions for DB2/VM are not provided in this release.

### Single Gateway Instance per DRDA Network Interface

When installing the gateway, a proper DRDA network interface must be chosen. Only one DRDA network interface may be chosen and installed per gateway instance. If the gateway product is reinstalled, and if a network interface different from the previous installation is chosen, then the new choice will overlay the current installation. Reconfiguration of the gateway's initialization parameters must occur at this point to ensure proper gateway operation. If you want to have both SNA and TCP/IP DRDA Network Interfaces installed, then you must install two separate gateway homes.

### Stored Procedures and transaction integrity

IBM DB2 has introduced a feature called Commit on Return for stored procedures. This feature enables DB2 to perform an automatic commit after a stored procedure runs successfully. This feature is enabled when the procedure is created. To ensure data integrity, this feature is not supported by the Oracle Transparent Gateway for DRDA in a heterogeneous environment. When attempting to call a stored procedure which has this feature enabled, through the gateway, the gateway will return an error message ORA-28526 or PLS-00201 (identifier must be declared).

---

**Note:** This restriction applies to DB2 for MVS or z/OS as of v5.1 and DB2/UDB as of v8.1.

---

### Stored Procedure and User Defined Function Support

The gateway supports processing of stored procedures and user defined functions through the following DRDA Servers:

DB2/OS390 V4.1 or later

DB2/400 V3.1 or later

DB2/UDB V7.1 or later

## 2.5.2 SQL Limitations

### Oracle ROWID Column

The DB2 ROWID column is not compatible with the Oracle ROWID column. Because the ROWID column is not supported, the following restrictions apply:

- UPDATE and DELETE are not supported with the WHERE CURRENT OF CURSOR clause. To update or delete a specific row through the gateway, a condition style WHERE clause must be used. (Bug No. 205538)

When UPDATE and DELETE statements are used, in precompiler and PL/SQL programs, they rely internally on the Oracle ROWID function.

- Snapshots between Oracle servers and DB2 are not supported. Snapshots rely internally on the Oracle ROWID column.

### Oracle Bind Variables

Oracle bind variables become SQL parameter markers when used with the gateway. Therefore, the bind variables are subject to the same restrictions as SQL parameter markers.

For example, the following statements are not permitted:

```
WHERE :x IS NULL  
WHERE :x = :y
```

### CONNECT BY Is Not Supported

Oracle Transparent Gateway for DRDA does not support `CONNECT BY` in `SELECT` statements.

### COUNT Function Compatibility

The following DRDA server releases do not support all forms of the `COUNT` function, specifically `COUNT(colname)` and `COUNT(ALL colnames)`:

DB2 OS/390 V6,

DB2/VM V6 and V7

The default for all DRDA server platforms (except DB2/VM) is for all forms of `COUNT` to be passed to the DRDA server as it is. For DB2/VM, the forms `COUNT(colname)` and `COUNT(ALL colname)` have been disabled by default and will be post-processed.

If the gateway is to be used with one of the above releases of DRDA servers, then it may be necessary to disable the default usage of this form of `COUNT`.

Refer to [Section 12.7.9, "Mapping the COUNT Function"](#) and [Section 12.6, "Native Semantics"](#) for details on how to disable or enable compatibility for these forms of `COUNT` function.

---

---

## System Requirements

This chapter provides information about hardware and software requirements that is specific to this release of the Oracle Transparent Gateway for DRDA. This chapter includes the following sections:

- [Hardware Requirements](#)
- [Software Requirements](#)
- [Documentation Requirements](#)

### 3.1 Hardware Requirements

The following are the minimum hardware requirements for the Oracle Transparent Gateway for DRDA on Microsoft Windows.

#### 3.1.1 Processor

This gateway requires a host with an Intel or 100% compatible PC with a Pentium-based processor that can run the required version of Microsoft Windows. Refer to the *Oracle Database Installation Guide for Microsoft Windows (32-Bit)* and to the certification matrix on Oracle *MetaLink* for the most up-to-date list of certified hardware platforms and operating system version requirements to operate the gateway for the system. The Oracle *MetaLink* web site can be found at the following URL:

<http://metalink.oracle.com/>

#### 3.1.2 Memory

For this release, 64 MB of real memory is the recommended minimum for running one instance of the gateway. Running additional instances of the Oracle Transparent Gateway for DRDA might require additional real memory or increased swap space to achieve reasonable performance.

The total real memory requirement for each concurrent use of the gateway depends on the following factors:

- Number of concurrent APPC connections opened by each user
- Number of concurrent TCP/IP connections opened by each user
- Number of data items being transferred between the gateway and the remote transaction program

- Additional factors such as configured network buffer size

### 3.1.3 Network Attachment

The hardware requires any network attachment supported by either Microsoft SNA Server for SNA communication or Microsoft Windows Sockets for TCP/IP communication. The network attachment for SNA is typically a Token Ring or SDLC Coaxial attachment. The hardware must support independent LUs if you want concurrent SNA access. The network attachment for TCP/IP is typically an Ethernet attachment.

### 3.1.4 Disk Space

260 MB of disk space is required for installation.

## 3.2 Software Requirements

The system software configuration described in these requirements is supported by Oracle as long as the underlying system software products are supported by their respective vendors. Verify the latest support status with your system software vendors.

### 3.2.1 Operating System

The Oracle Transparent Gateway for DRDA will run on the following operating systems:

- Microsoft Windows NT Server, version 4.0 (with Service Pack 6 or later)
- Microsoft Windows NT Workstation, version 4.0 (with Service Pack 6 or later)
- Microsoft Windows 2000 Server (with Service Pack 2 or later)
- Microsoft Windows 2000 Professional (with Service Pack 2 or later)
- Microsoft Windows 2003 Server
- Microsoft Windows XP Professional

Refer to the certification matrix on Oracle *MetaLink* for the most up-to-date list of certified hardware platforms and operating system version requirements to operate the gateway for your system. The Oracle *MetaLink* Web site can be found at the following URL:

<http://metalink.oracle.com/>

### 3.2.2 DRDA Databases

You must have at least one of the following DRDA servers at a supported release level:

- DB2/OS390
- DB2/VM
- DB2/400
- DB2/Universal Database



### 3.2.3 Communications

Supported SNA network software are:

- Microsoft SNA Server or Client, version 3.0 or version 4.0, or Host Integration Server, Version 5.0
- IBM Communications Server, Version 5.0 or 6.0

---



---

**Note:** Version 5.0 requires the following patches:

- JR12583 (Super fix)
  - JR12539 (individual Local LUs fix)
- 
- 

### 3.2.4 Oracle Database server

The Oracle Database server which is to act as the Oracle integrating server requires the latest released patch set for Oracle Database 10g server release 10.2, 10.1, or Oracle9i server release 9.2.

### 3.2.5 Oracle Networking Products

If the Oracle integrating server is not on the same host as the gateway, then Oracle Net is required to support communication between the Pentium-based host and the Oracle integrating server.

The following Oracle networking products are required on the same system as the Oracle Database 10g server:

- Oracle Net Client 10.2.0.1.0
- an Oracle Adapter, version 10.2.0.1.0

Oracle Net software is included in this Oracle Transparent Gateway for DRDA release. Your gateway license includes a license for Oracle Net and an adapter of your choice. This license restricts the use of Oracle Net for gateway access.

## 3.3 Documentation Requirements

In addition to the documentation provided with the Oracle Transparent Gateway for DRDA distribution kit, the following Oracle documentation is recommended:

- *Oracle Database Administrator's Guide*
- *Oracle Database Installation Guide for Microsoft Windows (32-Bit)*
- *Oracle Database Application Developer's Guide - Fundamentals*
- *Oracle Database Heterogeneous Connectivity Administrator's Guide*
- *Oracle Database Error Messages*
- *Oracle Database Advanced Security Administrator's Guide*
- *Oracle C++ Call Interface Programmer's Guide*
- *Oracle Call Interface Programmer's Guide*
- *SQL\*Plus User's Guide and Reference*
- *Oracle Database PL/SQL User's Guide and Reference*
- *Oracle Database SQL Reference*

- *Oracle Database Net Services Administrator's Guide*
- *Oracle Database Net Services Reference*

In addition to the Oracle documentation, ensure that you have the required documentation for the platform, for the operating system, and for the DRDA Server (DB2/OS390, DB2/400, DB2 Universal Database, or DB2 server for VM).

IBM publications that describe distributed relational databases might also be useful.

---

---

## Installing the Gateway

This chapter provides general information about gateway installation that is specific to this release of the Oracle Transparent Gateway for DRDA for Microsoft Windows. This chapter includes the following sections:

- [Introduction](#)
- [Before You Begin](#)
- [Checklist for Gateway Installation](#)
- [Installation Overview](#)
- [Preinstallation](#)
- [Installing the Gateway from the Installation Media](#)
- [Installation Complete](#)

### 4.1 Introduction

The complete Oracle Transparent Gateway for DRDA for Microsoft Windows installation process is divided into installation and configuration tasks. This process is described in Chapters 4 through 8. If this is the first time the gateway has been installed on your Pentium-based host, then you must perform all the steps documented in these chapters.

The installation tasks include:

- Ensuring that your hardware and software requirements are met
- Loading and installing the gateway software from the distribution medium into your system
- Determining your gateway system identifier
- Reconfiguring your network

An installation checklist follows, which you can use to check off each completed step in the process.

### 4.2 Before You Begin

This chapter requires you to enter parameters that are unique to your system in order to properly configure the gateway. Refer to [Appendix E, "Configuration Worksheet"](#) for a worksheet listing all the installation parameters that you will need to know in

order to complete the configuration process. Ask your network administrator to provide these parameters before you begin.

You will also need to confirm that all hardware and software requirements have been met. Refer to [Chapter 3, "System Requirements"](#) to verify these requirements.

## 4.3 Checklist for Gateway Installation

Use the following checklist for installing the gateway:

- [Step 1: Log on to the host](#)
- [Step 2: Load the CD-ROM into the CD-ROM Drive](#)
- [Step 3: Start the Oracle Universal Installer on Microsoft Windows](#)
- [Step 4: Step through the Oracle Universal Installer](#)
- [Step 5: Verify Installation Success](#)

## 4.4 Installation Overview

The primary installation tasks are presented with the assumption that you will configure the gateway with a single Oracle integrating server and a single DRDA database. The steps for expanding the configuration to multiple integrating servers and multiple DRDA databases are described in [Chapter 10, "Configuring the Gateway"](#).

For general information about installing Oracle products and how to use the Oracle Universal Installer, refer to the *Oracle Database Installation Guide for Microsoft Windows (32-Bit)*.

## 4.5 Preinstallation

`ORACLE_HOME` is the root directory in which Oracle software is installed.

Throughout this book, `ORACLE_HOME` is used to refer to the home directory of the Oracle Transparent Gateway for DRDA for Microsoft Windows, unless specifically stated otherwise.

## 4.6 Installing the Gateway from the Installation Media

The Oracle Universal Installer for Microsoft Windows is provided on the installation media with the gateway.

### 4.6.1 Step 1: Log on to the host

Log on to your host computer as a member of the Administrators group.

### 4.6.2 Step 2: Load the CD-ROM into the CD-ROM Drive

Use any CD-ROM drive that is attached to the Pentium-based host (either locally or as a shared resource) as a logical drive to install the gateway. If the CD-ROM drive cannot copy files to your hard disk, then refer to your CD-ROM documentation. The installation steps are presented with the assumption that the CD-ROM drive is mapped to the G: drive.

To load the gateway distribution CD-ROM:

1. Insert the gateway distribution CD-ROM into the CD-ROM drive.
2. Verify that the drive is assigned to the logical drive that you selected and that you can access files on the CD-ROM.

### 4.6.3 Step 3: Start the Oracle Universal Installer on Microsoft Windows

If you previously installed another Oracle Microsoft Windows product, such as an earlier version of the Oracle server or the gateway, then Oracle Universal Installer has already been set up in the Microsoft Windows program menu.

Start the Oracle Universal Installer from the Start menu rather than by using Microsoft Windows Explorer.

1. From the Start menu, click **Run**.
2. Enter the path and executable file name:

G: \SETUP.EXE

3. Click **OK**.

### 4.6.4 Step 4: Step through the Oracle Universal Installer

The Oracle Universal Installer is a menu-driven utility that guides you through installation of the gateway by prompting you with action items. The action items and the sequence in which they appear depend on your platform. Use the following table as a guide to the installation, following the instructions in the Response column.

**Table 4–1 Steps to Install the Gateway Using the Oracle Universal Installer**

Prompt	Response
Welcome	Click <b>Next</b> .
Specify Home Details	Check that the destination path points to your <i>ORACLE_HOME</i> . Click <b>Next</b> .
Available Product Components	Open the Oracle Transparent Gateways product group and select Oracle Transparent Gateway for DRDA. Open the Oracle Transparent Gateway for DRDA product group, if not already open, and select one protocol from the list of supported protocols. Remove selection from everything else for a standalone gateway installation. Click <b>Next</b> .
DRDA Network Interface Product Software	If the SNA protocol was selected, choose the network interface software suitable for this installation of the gateway. Click <b>Next</b> . If the SNA protocol was not selected, this panel does not appear.
Summary	Verify the products to be installed. Click <b>Next</b> .

### 4.6.5 Step 5: Verify Installation Success

After the Oracle Universal Installer confirms that the installation has ended, verify that the installation was successful. To do this, check the contents of the installation log file, which is located in the C:\Program Files\Oracle\Inventory\logs directory. The default file name is InstallActionsdate.LOG.

## 4.7 Installation Complete

Your gateway installation is now complete. Proceed with the configuration tasks that are described in Chapters 5 through 10.

## 4.7.1 Removing the Gateway

Removing the Oracle Transparent Gateway for DRDA requires the use of the Oracle Universal Installer. Follow the procedures below to remove the gateway:

1. To restart the Oracle Universal Installer, refer to the installation process found earlier in this chapter in "[Installing the Gateway from the Installation Media](#)" on page 4-2, and repeat the following three steps (Steps 1, 2, and 3):
  - a. [Step 1: Log on to the host](#)
  - b. [Step 2: Load the CD-ROM into the CD-ROM Drive](#)
  - c. [Step 3: Start the Oracle Universal Installer on Microsoft Windows](#)
2. When the Welcome panel appears, select **Advanced Installation** and Click **Next**. Then, in the File Locations panel, click **Installed Products**.
3. In the list of installed products, select the Gateway product and any other products that you wish to remove, and click **Remove**.

---

---

## Configuring the DRDA Server

The steps for configuring your remote DRDA Server apply to the following DRDA Servers:

- [Checklists for Configuring the DRDA Server](#)
- [DB2/OS390](#)
- [DB2/400](#)
- [DB2/UDB \(Universal Database\)](#)
- [DB2/VM](#)

Configuring a DRDA database to enable access by the gateway requires actions on the DRDA database and on certain components of the host operating system. Although no Oracle software is installed on the host system, access to, and some knowledge of, the host system and DRDA database are required during the configuration. Refer to the vendor documentation for complete information about your host system and DRDA database.

### 5.1 Checklists for Configuring the DRDA Server

Use the following checklists for configuring the DRDA Server.

#### 5.1.1 [DB2/OS390](#)

- [Step 1: Configure the Communications Server](#)
- [Step 2: Define the user ID that owns the package](#)
- [Step 3: Define the recovery user ID](#)
- [Step 4: Determine DRDA location name for DB2 instance](#)
- [Step 5: Configure DB2 Distributed Data Facility for Gateway](#)

#### 5.1.2 [DB2/400](#)

- [Step 1: Configure the Communications Server](#)
- [Step 2: Define the user ID that owns the package](#)
- [Step 3: Define the recovery user ID](#)
- [Step 4: Determine DRDA location name for DB2/400 instance](#)

### 5.1.3 DB2/UDB (Universal Database)

- Step 1: Configure the SNA Communications Server
- Step 2: Define the user ID that owns the package
- Step 3: Define the recovery user ID
- Step 4: Determine DRDA location name for DB2/UDB instance

### 5.1.4 DB2/VM

- Step 1: Configure the Communications Server
- Step 2: Define the user ID that owns the package
- Step 3: Define the recovery user ID
- Step 4: Determine DRDA location name for DB2/VM instance

## 5.2 DB2/OS390

Experience with OS/390 (MVS), OS/390, TSO, VTAM, and DB2 is required to perform the following steps:

### 5.2.1 Step 1: Configure the Communications Server

If you are using SNA, then configure OS/390 (MVS) VTAM for the SNA connection from the host. Configure DB2 Distributed Data Facility (DDF) for SNA using the Logical Unit (LU) defined. If you are using TCP/IP, then configure the TCP/IP subsystem. Configure DB2's DDF subsystem to use TCP/IP, and assign a primary and recovery port number for the DB2 server.

### 5.2.2 Step 2: Define the user ID that owns the package

During gateway configuration, you will need to run the Bind Package Stored Procedure to bind the gateway package on the DRDA Server. To properly bind the package, the user ID and password that are used when the procedure is run (either implied as the current Oracle user or explicitly defined in the `CREATE DATABASE LINK` command) must have proper authority on the DRDA Server to create the package. This same user ID should be used to create and to own the `ORACLE2PC` (two-phase commit) table. The user ID that is used to bind or rebind the DRDA package must have one or more of the following privileges on the DRDA Server:

- Package privileges of `BIND`, `COPY`, and `EXECUTE`, for example:

```
GRANT BIND    ON PACKAGE drda1.* TO userid
GRANT COPY    ON PACKAGE drda1.* TO userid
GRANT EXECUTE ON PACKAGE drda1.* TO PUBLIC
```

- Collection privilege of `CREATE IN`, for example:

```
GRANT CREATE IN ON PACKAGE drda1 TO USER userid
```

- System privileges of `BINDADD` and `BINDAGENT`, for example:

```
GRANT BINDADD TO USER userid
GRANT BINDAGENT TO USER userid
```

- Database privilege of `CREATETAB`, for example:



```
GRANT CREATETAB ON DATABASE database TO USER userid
```

Choose a user ID now that will own the package and the ORACLE2PC table. Ensure that this user ID is defined to both DB2 and OS/390 (MVS).

### 5.2.3 Step 3: Define the recovery user ID

During gateway configuration, the recovery user ID and password are specified in the gateway initialization file using the `DRDA_RECOVERY_USERID` and `DRDA_RECOVERY_PASSWORD` parameters. If a distributed transaction fails, then the recovery process connects to the remote database using the user ID and password that are defined in these parameters. This user ID must have execute privileges on the package and must be defined to the DRDA database. If the user ID is not specified in `DRDA_RECOVER_USERID`, then the gateway attempts to connect to a user ID of `ORARECOV` when a distributed transaction is in doubt.

Determine the user ID and password that you will use for recovery.

### 5.2.4 Step 4: Determine DRDA location name for DB2 instance

The DRDA location name is required as a gateway parameter. To determine the location name, run the SQL query from a DB2 SPUFI session:

```
SELECT CURRENT SERVER FROM any_table
```

where *any\_table* is a valid table with one or more rows.

If the value returned by this query is blank or null, then the DRDA location name has not been established. Contact the system administrator to arrange to set a location name for the instance.

### 5.2.5 Step 5: Configure DB2 Distributed Data Facility for Gateway

DB2 DDF is the component of DB2 that manages all distributed database operations, both DRDA and non-DRDA.

If your site uses DB2 distributed operations, then DDF is probably operational on the DB2 instance that you plan to access through the gateway. If DDF is not operational, then you must configure it and start it as described in the appropriate DB2 documentation.

Even if DDF is operational on the DB2 instance, it might be necessary to make changes to the DDF Communication Database (CDB) tables to specify the authorization conduct of DRDA sessions from the gateway. This can be done by properly authorized users with a utility such as the DB2 SPUFI utility. If you make changes to CDB tables, then you must stop and restart DDF for the changes to take effect. Refer to [Chapter 13, "Security Considerations"](#), for additional CDB tables and security information.

## 5.3 DB2/400

Experience with DB2/400 and AS/400 is required to perform the following steps:

### 5.3.1 Step 1: Configure the Communications Server

If you are using SNA, then configure AS/400 communications for the SNA connection from the host. Configure DB2/400 for SNA using the LU defined. If you are using TCP/IP, then configure the TCP/IP subsystem, configure DB2/400 to use TCP/IP, and assign a Primary and Recovery port number for the DB2 server.

### 5.3.2 Step 2: Define the user ID that owns the package

During gateway configuration, you will need to run the Bind Package Stored Procedure to bind the gateway package on the DRDA Server. To properly bind the package, the user ID and password that are used when the procedure is run (either implied as the current Oracle user or explicitly defined in the `CREATE DATABASE LINK` command) must have proper authority on the DRDA Server to create the package. This same user ID should be used to create and to own the `ORACLE2PC` (two-phase commit) table. The user ID that is used to bind or rebind the DRDA package must have the following privileges on the DRDA Server:

- Use authority on the `CRTSQLPKG` command
- Change authority on the library in which the package will be created

Choose a user ID now that will own the package and the `ORACLE2PC` table. Ensure that this user ID is defined to DB2/400 and AS/400.

### 5.3.3 Step 3: Define the recovery user ID

During gateway configuration, the recovery user ID and password are specified in the gateway initialization file using the `DRDA_RECOVERY_USERID` and `DRDA_RECOVERY_PASSWORD` parameters. If a distributed transaction fails, then the recovery process connects to the remote database using the user ID and password that are defined in these parameters. This user ID must have execute privileges on the package and must be defined to the DRDA database. If the user ID is not specified in `DRDA_RECOVER_USERID`, then the gateway attempts to connect to a user ID of `ORARECOV` when a distributed transaction is in doubt.

Determine the user ID and password that you will use for recovery.

### 5.3.4 Step 4: Determine DRDA location name for DB2/400 instance

The DRDA location name is required as a gateway parameter. To determine the location name, run the following SQL query from a STRSQL session. If SQL is unavailable on the system, then use the AS/400 command `DSPRDBDIRE` to identify your "LOCAL" DRDA Server.

```
SELECT CURRENT SERVER FROM any_table
```

where *any\_table* is a valid table with one or more rows.

If the value returned by this query is blank or null, then the DRDA location name has not been established. Contact the system administrator to arrange to set a location name for the instance.

## 5.4 DB2/UDB (Universal Database)

Experience with DB2/UDB, configuring the communication subsystem of DB2/UDB, and the host System Administration tools is required to perform the following steps.

### 5.4.1 Step 1: Configure the SNA Communications Server

If you are using SNA, then configure the communications server for the connection from the host. Configure DB2/UBD for SNA using the LU defined. If you are using TCP/IP, then configure the TCP/IP subsystem. Configure DB2/UDB to use TCP/IP, and assign a primary and recovery port number for the DB2 server.

## 5.4.2 Step 2: Define the user ID that owns the package

During gateway configuration, you will need to run the Bind Package Stored Procedure to bind the gateway package on the DRDA Server. To properly bind the package, the user ID and password that are used when the procedure is run (either implied as the current Oracle user or explicitly defined in the `CREATE DATABASE LINK` command) must have proper authority on the DRDA Server to create the package. This same user ID should be used to create and to own the `ORACLE2PC` (two-phase commit) table. The user ID that is used to bind or rebind the DRDA package must have one or more of the following privileges on the DRDA Server:

- Package privileges of `BIND` and `EXECUTE`, for example:

```
GRANT BIND    ON PACKAGE drda1.g2drsqli TO USER userid
GRANT EXECUTE ON PACKAGE drda1.g2drsqli TO PUBLIC
```

- Schema privileges of `CREATEIN`, for example:

```
GRANT CREATEIN ON SCHEMA otgdb2 TO USER userid
GRANT CREATEIN ON SCHEMA drda1 TO USER userid
```

- Database authorities of `CONNECT`, `BINDADD`, and `CREATETAB`, for example:

```
GRANT CONNECT  ON DATABASE TO USER userid
GRANT BINDADD  ON DATABASE TO USER userid
GRANT CREATETAB ON DATABASE TO USER userid
```

Now choose a user ID that will own the package and `ORACLE2PC` table. Ensure that this user ID is defined to both the DB2 instance ID and the operating system.

## 5.4.3 Step 3: Define the recovery user ID

During gateway configuration, the recovery user ID and password are specified in the gateway initialization file using the `DRDA_RECOVERY_USERID` and `DRDA_RECOVERY_PASSWORD` parameters. If a distributed transaction fails, then the recovery process connects to the remote database using the user ID and password that are defined in these parameters. This user ID must have execute privileges on the package and must be defined to the DRDA database. If the user ID is not specified in `DRDA_RECOVER_USERID`, then the gateway attempts to connect to a user ID of `ORARECOV` when a distributed transaction is in doubt.

Determine the user ID and password that you will use for recovery.

## 5.4.4 Step 4: Determine DRDA location name for DB2/UDB instance

The DRDA location name is required as a gateway parameter. To determine the location name, run the SQL query from a DB2 CLI session:

```
SELECT CURRENT SERVER FROM any_table
```

where *any\_table* is a valid table with one or more rows.

If the value returned by this query is blank or null, then the DRDA location name has not been established. Contact your system administrator to arrange to set a location name for the instance.

## 5.5 DB2/VM

Experience with VM, AVS, and DB2/VM is required to perform the following steps:

### 5.5.1 Step 1: Configure the Communications Server

If you are using SNA, then configure VM VTAM and AVS for the SNA connection from the host. If you are using TCP/IP, then configure the TCP/IP service.

### 5.5.2 Step 2: Define the user ID that owns the package

During gateway configuration, you will need to run the Bind Package Stored Procedure to bind the gateway package on the DRDA Server. To properly bind the package, the user ID and password that are used when the procedure is run (either implied as the current Oracle user or explicitly defined in the `CREATE DATABASE LINK` command) must have proper authority on the DRDA Server to create the package. This same user ID should be used to create and to own the `ORACLE2PC` (two-phase commit) table. The user ID that is used to bind or rebind the DRDA package must have the following privileges on the DRDA Server:

- Package privileges of `BIND`, `COPY`, and `EXECUTE`
- Collection privilege of `CREATE IN`
- System privileges of `BINDADD` and `BINDAGENT`

Choose a user ID now that will own the package and `ORACLE2PC` table. Ensure that this user ID is defined to DB2/VM and VM.

### 5.5.3 Step 3: Define the recovery user ID

During gateway configuration, the recovery user ID and password are specified in the gateway initialization file using the `DRDA_RECOVERY_USERID` and `DRDA_RECOVERY_PASSWORD` parameters. If a distributed transaction fails, then the recovery process connects to the remote database using the user ID and password that are defined in these parameters. This user ID must have execute privileges on the package and must be defined to the DRDA database. If the user ID is not specified in `DRDA_RECOVER_USERID`, then the gateway attempts to connect to a user ID of `ORARECOV` when a distributed transaction is in doubt.

Determine the user ID and password that you will use for recovery.

### 5.5.4 Step 4: Determine DRDA location name for DB2/VM instance

The DRDA location name is required as a gateway parameter. To determine the location name, run the SQL query from an *iSQL* session:

```
SELECT CURRENT SERVER FROM any_table
where any_table is a valid table with one or more rows.
```

If the value returned by this query is blank or null, then the DRDA location name has not been established. Contact the system administrator to arrange to set a location name for the instance.

---

---

# Configuring Microsoft SNA Server or Host Integration Server

This chapter describes configuration of the Microsoft SNA Server product on Microsoft Windows for use with the Oracle Transparent Gateway for DRDA. The SNA Server provides the SNA connectivity through the APPC/LU6.2 protocol between the Pentium-based host and the remote DRDA Server. Microsoft Host Integration Server is the successor product to Microsoft SNA Server, but it retains the same configuration information as SNA Server and the steps for configuring SNA Server, therefore, also apply to Host Integration Server. Read this chapter to learn more about creating server profiles.

This chapter contains the following sections:

- [Before You Begin](#)
- [Steps for Configuring the Communications Interfaces](#)
- [Creating SNA Server Profiles for the Gateway](#)
- [Creating SNA Definitions for the Gateway](#)
- [Testing the Connection](#)
- [Using SNA Session Security Validation](#)
- [SNA Conversation Security](#)

## 6.1 Before You Begin

This chapter requires you to enter parameters unique to your system in order to properly configure the SNA Server. Refer to [Appendix E](#) for a worksheet listing all the installation parameters that you will need to know before you can complete the configuration process. Ask your network administrator to provide you with these parameters before you begin.

## 6.2 Steps for Configuring the Communications Interfaces

- Step 1: [Creating SNA Server Profiles for the Gateway](#)
- Step 2: [Creating SNA Definitions for the Gateway](#)
- Step 3: [Testing the Connection](#)

## 6.3 Creating SNA Server Profiles for the Gateway

The Oracle Transparent Gateway for DRDA requires a stored set of definitions, called Side Information Profiles, to support connections between the gateway and DRDA Servers. Each profile consists of a profile name and a profile type, a set of fields describing the profile. The fields in a given profile type are generally a mixture of operating parameter values and names of other SNA profiles relevant to the profile. Each functional part of APPC, such as the Mode, Remote Transaction Program name, and Logical Unit (LU), is described by a distinct profile type.

### 6.3.1 Independent Versus Dependent LUs

Oracle recommends independent LUs for the Oracle Transparent Gateway for DRDA, because they support multiple parallel sessions or conversations. This means the multiple Oracle client applications can be active simultaneously with the same DRDA Server through the independent LU.

Dependent LUs support only a single active session. The CP (SNA Server for Microsoft Windows, in this case) queues additional conversation requests from the gateway server behind an already active conversation. In other words, conversations are single-threaded for dependent LUs.

If a dependent LU is correctly defined, then no alterations to the Oracle Transparent Gateway for DRDA configuration are needed, nor should any changes be needed to the DRDA Server.

The operational impact of dependent LUs is that the first client application can start a conversation through the gateway with the DRDA Server. While that session is active (which could be seconds, minutes, or hours, depending on how the client application and transaction are designed), any other client application starting a session with the same DRDA Server appears to stop responding as it waits behind the previous session.

If a production application really uses only one conversation at any one time, then there should be no impact. However, additional concurrent conversations might be required for testing or other application development. Each requires that additional dependent LUs be defined on the remote host, plus additional SNA Server configuration entries which define the additional dependent LUs on the host.

Additional Side Information Profiles should be defined to use the new dependent LUs. New Oracle Transparent Gateway for DRDA instances should be created and configured to use these new Side Information Profiles.

## 6.4 Creating SNA Definitions for the Gateway

SNA Server definitions can be created and modified in two ways:

- Directly with the `SNACFG` command
- Using menus in SNA Server Manager

Maintenance of SNA definitions is normally done by a user with Administrator authority. This information is intended for the person creating SNA definitions for the gateway. You should have some knowledge of SNA before reading this section.

### 6.4.1 Sample SNA Server Definitions

The `tg4drda\sna\mssna` subdirectory contains a sample set of gateway SNA Server definitions created with the `SNACFG` command. The `snacfg.ctl` file contains sample definitions for SNA Server.

Before building the SNA Server definitions, examine the `snacfg.ctl` file to determine the definitions needed, their contents, and their interrelationships. The file format is text-oriented and each field of each definition is clearly labeled. You can print a copy of the file to use while working with your definitions in an SNA Server Admin or SNA Server Manager session.

You can create and modify these definitions in two ways:

- Install the definitions directly on the system using the `SNACFG` command.

For information on using the `SNACFG` command, refer to the *SNA Server Administration Guide* in the Microsoft SNA Server online documentation.

If you use this method, then you must use SNA Server Manager to review and modify the installed definitions. Because of configuration and naming differences, it is unlikely that they will work without modification.

- Create the definitions.

SNA Server Manager is the recommended method for creating the definitions. You should be able to accept most of the defaults. The default values assigned to many of the fields in a new set of definitions are acceptable for the gateway.

## 6.4.2 Definition Types

There are several types of SNA Server definitions relevant to gateway APPC/LU6.2 operation. Each definition can be created and edited using a corresponding SNA Server Manager menu.

The definitions relevant to the gateway are presented here in hierarchical order. Those definition types that are lowest in the hierarchy are discussed first. This matches the logical sequence in which to create the profiles.

Refer to the Microsoft SNA Server online documentation for a complete discussion of SNA Server definitions. This section is an overview of SNA Server definitions in relation to the Oracle Transparent Gateway for DRDA for Microsoft Windows.

---



---

**Note:** Before beginning to create and edit profiles using SNA Server Admin, you must install the DLC protocol and create the link service. Prior to running SNA Server Admin, use the Microsoft Windows Control Panels Network Manager to install the DLC protocol.

---



---

## 6.4.3 SNA Server Definitions

This section describes the process of creating your SNA definitions for SNA Server version 3, using SNA Server Manager. All the tasks described in this section are performed from within SNA Server Manager. The other primary administration tool is the SNA Server Management Console. Both tools provide access to the same SNA definitions for the Node, but in slightly different views. The SNA Server Manager gives a localized view of the Node, while the SNA Server Management Console presents a more global view, where the local node may be one of many SNA Nodes in a network that is managed by this system. Later versions of SNA Server and Host Integration Server tools may reorganize the profiles placement within the definition tree, but the concepts remain the same. Some extrapolation by the user may be necessary.

**Figure 6–1 SNA Server Manager Main Screen: Select a Server**

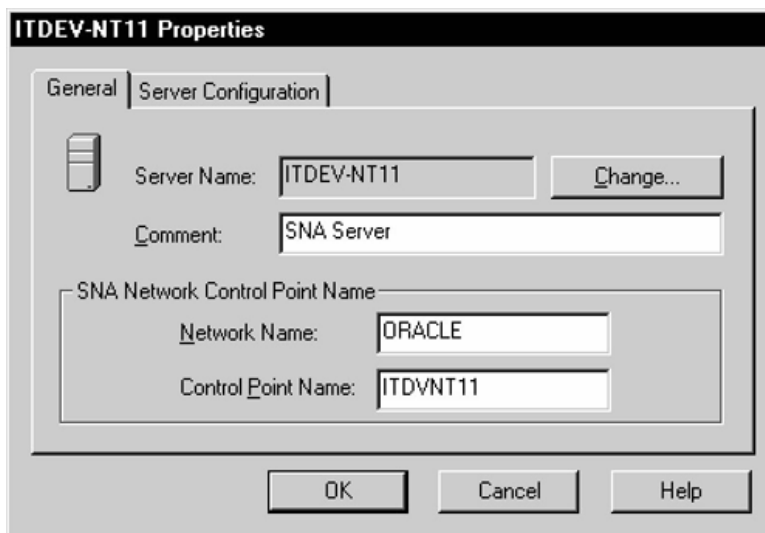


### 6.4.3.1 Server Selection

The correct SNA Server must be selected to ensure that definitions created are for that server. Start the SNA Server Manager.

Click the SNA subdomain under your local system (in this example, ITDEV11) and then click to open the SNA Servers folder. From a list of services for that server, select the SNA Service of your choice (in this illustration, ITDEV-NT11). Click to open it.

**Figure 6–2 Server Properties Dialog Box**

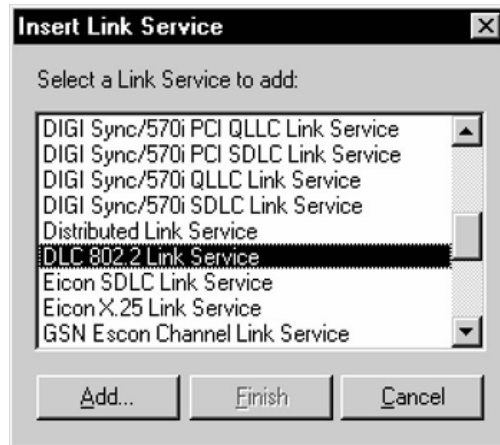




### 6.4.3.2 Service Properties

Each SNA Server must have a primary service definition. From the Service menu in the SNA Server Manager window, select Properties. In the Server Properties dialog box, under the General tab, change the Network Name and Control Point Name as needed. Click **OK**.

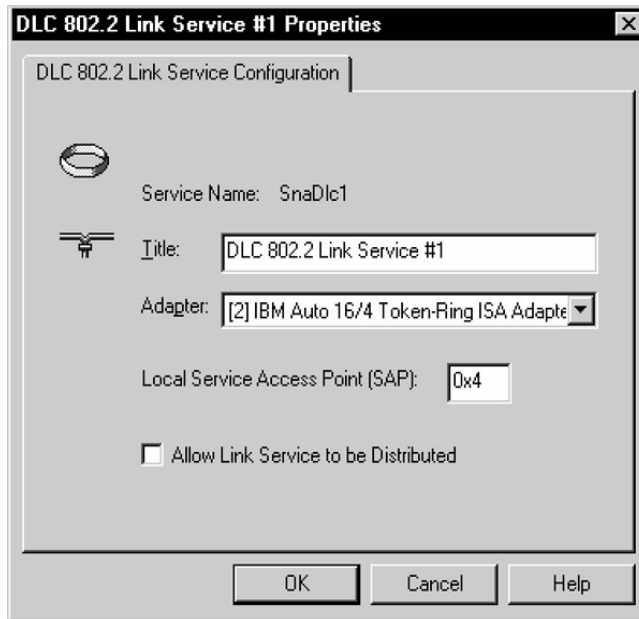
*Figure 6–3 Insert Link Service*



### 6.4.3.3 Link Service Definition

A link service must be installed and configured in order for SNA Server to use the network adapter installed in your workstation. From the Insert menu, select Link Service. In the Insert Link Service dialog box, select the desired Link Service from the selection list and click **Add**. In this example, DLC 802.2 Link Service is selected.

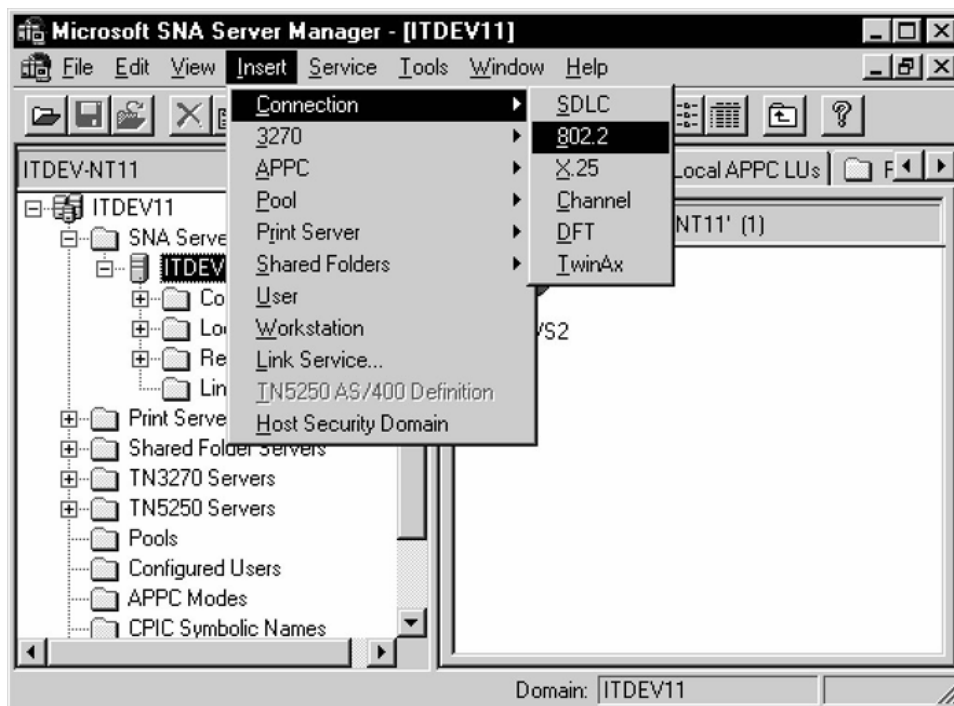
**Figure 6-4 Select Link Service Properties**



Now, the Link Service Properties dialog box is displayed. Note that the contents of this dialog box will vary, depending on which Link Service was selected. In this example, the DLC 802.2 Link Service Properties box dialog is used:

Select the suitable network adapter from the Adapter drop-down list and click **OK**. In the Insert Link Service dialog box, click **OK**. The system now updates the network bindings.

**Figure 6-5 Connection Properties Menu**



#### 6.4.3.4 Connection Definition

You must create a connection definition to define the devices which SNA Server uses to perform SNA communication. From the Insert menu, select Connection and choose the connection type (802.2 is used in this example). The Connection Properties dialog box appears.

**Figure 6–6 General Connection Properties**

The screenshot shows the 'Connection Properties' dialog box with the 'General' tab selected. The 'Name' field contains 'HQMVS2', 'Link Service' is set to 'SnaDlc1', and 'Comment' is '802.2 Connection to MVS'. There is a checkbox for 'Supports Dynamic Remote APPC LU Definition' which is unchecked. Below are three sections: 'Remote End' with radio buttons for 'Host System' (selected), 'Peer System', and 'Downstream'; 'Allowed Directions' with radio buttons for 'Outgoing Calls' (selected), 'Incoming Calls', and 'Both Directions'; and 'Activation' with radio buttons for 'On Server Startup', 'On Demand' (selected), and 'By Administrator'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Select the General tab. Enter a Connection Name. This is the name used by SNA Server to name the connection. This example names the connection HQMVS2. From the Link Service drop-down list, select a link service for the connection. All other settings can be left set to their default values.

**Figure 6–7 Enter Remote Addresses**

The screenshot shows the 'Connection Properties' dialog box with the 'Address' tab selected. The 'Remote Network Address' field contains '400000FFFFFF' and the 'Remote SAP Address' field contains '04'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Select the Address tab. Enter values for Remote Network Address and the Remote SAP address.

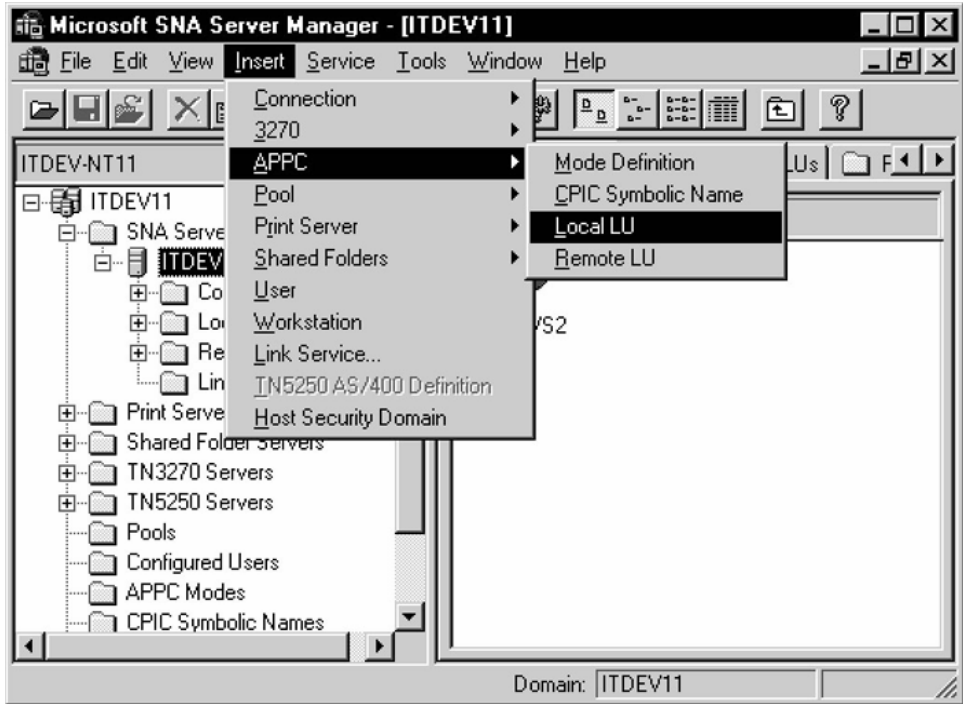
**Figure 6–8 Enter System Identification**

Now, select the System Identification tab. Under Local Node Name, enter the Network Name, Control Point Name, and Local Node ID. Under Remote Node Name, enter the Network Name, Control Point Name, and optionally, the Remote Node ID. The XID Type should be set to Format 3.

**Figure 6–9 Enter DLC Values**

Next, select the DLC tab. In this example, the 802.2 DLC (Token Ring) is being used. For the 802.2 DLC, all of the defaults are usually acceptable. If you need to change any values, then do so now. Now, all the connection properties are set. Click **OK**.

Figure 6-10 Local LU Properties Menu

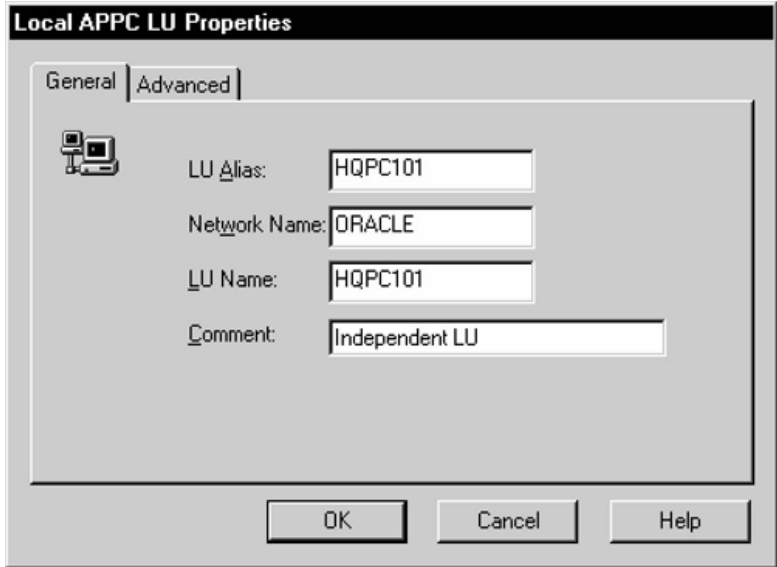


6.4.3.5 Local LU Definition

You must create a local LU definition. The local LU definition describes the SNA LU through which the gateway communicates with DRDA Server systems.

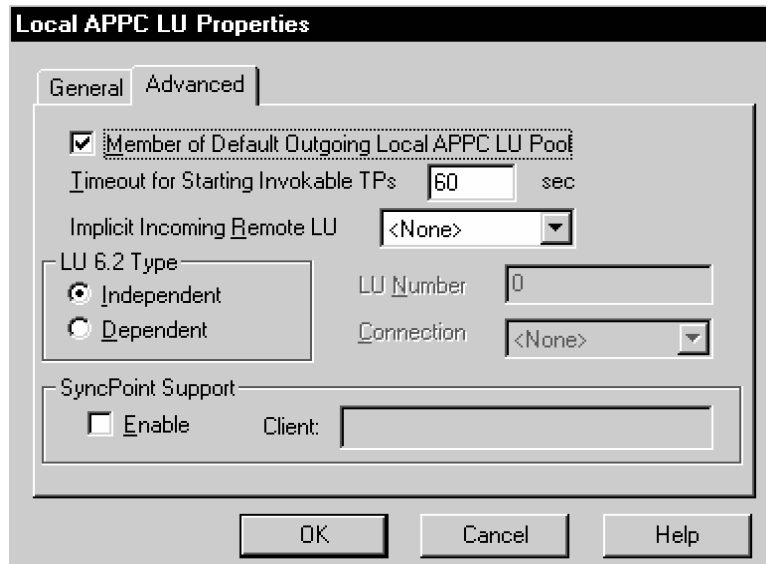
From the Insert menu, select APPC Local LU. The Local APPC LU Properties dialog box appears.

Figure 6-11 Enter Local APPC LU Properties



Select the General tab. Enter LU Alias, Network Name, and LU Name. You should contact the person responsible for your SNA network to determine the correct LU and network names.

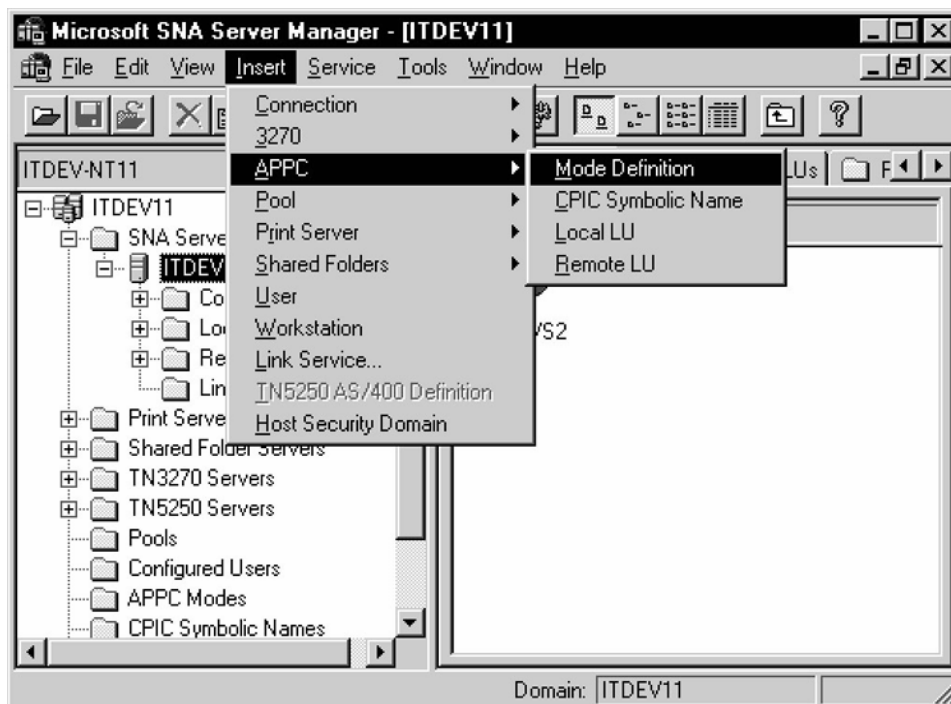
**Figure 6–12 Set Up Parallel Session**



Select the Advanced tab. Check the Member of Default Outgoing Local APPC LU Pool box. Set the LU 6.2 Type to Independent to enable parallel sessions. Ensure that the APPC Syncpoint Support box is not checked.

Now, the Local LU properties are all set. Click **OK** button to continue.

**Figure 6–13 Select APPC Mode Definition**



### 6.4.3.6 Mode Definition

This definition describes an SNA mode entry to be used when establishing sessions between LUs. The mode defined here must match a mode defined on the target system.

From the Insert menu, select APPC Mode Definition. The APPC Mode Properties dialog box appears.

**Figure 6–14 APPC Mode General Properties Dialog Box**

The screenshot shows the 'APPC Mode Properties' dialog box with the 'General' tab selected. The 'Mode Name' field contains 'IBMRDB' and the 'Comment' field contains 'Mode for DRDA'. There are 'OK', 'Cancel', and 'Help' buttons at the bottom.

Select the General tab. Enter the Mode Name. The mode name that you specify must be defined to the DRDA Server communications software. Choose the mode name and other mode parameters after consulting the person responsible for configuring the DRDA Server communications software.

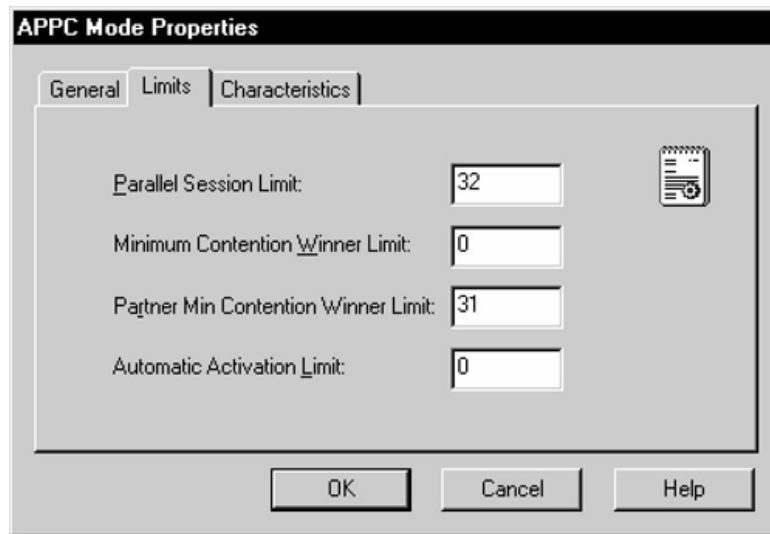
**Figure 6–15 Enter the APPC Mode Limits**

The screenshot shows the 'APPC Mode Properties' dialog box with the 'Limits' tab selected. The 'Parallel Session Limit' is 32, 'Minimum Contention Winner Limit' is 0, 'Partner Min Contention Winner Limit' is 31, and 'Automatic Activation Limit' is 0. There are 'OK', 'Cancel', and 'Help' buttons at the bottom.

Next, select the Limits tab. Enter values for Parallel Session Limit, Minimum Contention Winner Limit, Partner Min Contention Winner Limit, and Automatic Activation Limit. The Parallel Session limit determines the maximum number of

concurrent conversations permitted between the gateway instance and the DRDA Server. This equates to the maximum number of concurrently active remote sessions through the gateway instance.

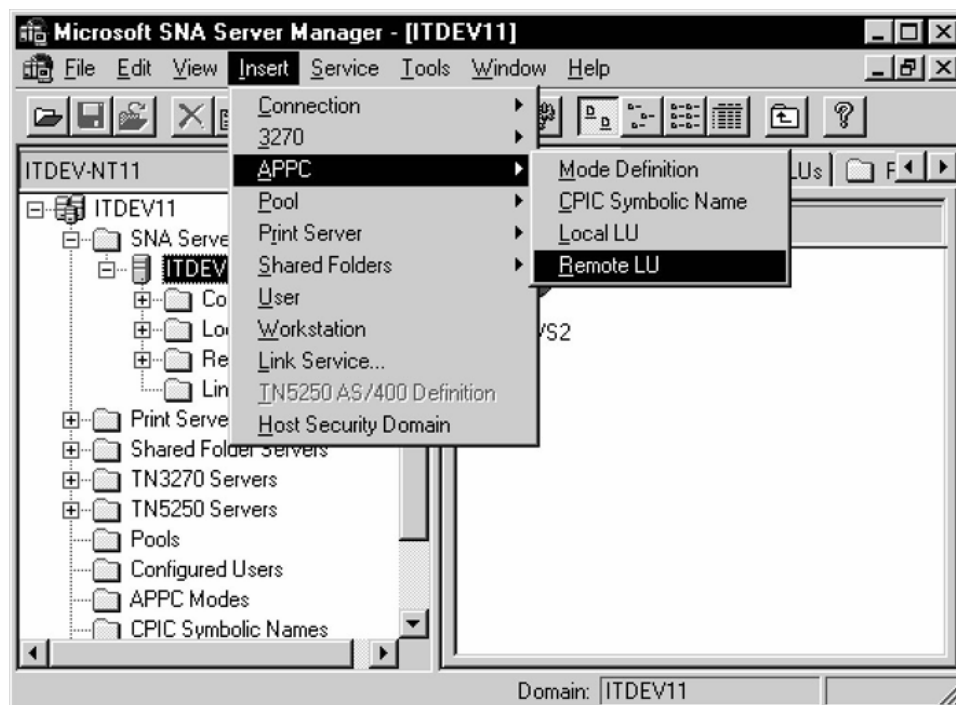
**Figure 6–16 Set APPC Mode Characteristics**



Now, select the Characteristics tab. Enter the Pacing Send Count, Pacing Receive Count, Max Send RU Size, and Max Receive RU size. For optimal performance, check the High Priority Mode box. The pacing and RU size parameters are performance-related and should be tuned to suit your application. For most installations, the values set in the example will be sufficient.

Now, all the APPC mode properties are set. Click **OK** to continue.

**Figure 6–17 APPC Remote LU Menu**





### 6.4.3.7 Remote LU Definition

This definition describes the SNA LU of the DRDA Server system with which the gateway communicates. You must create a remote LU definition for the remote DRDA Server system. From the Insert menu, select APPC Remote LU. The Remote APPC LU Properties dialog box appears.

**Figure 6–18 Enter General Remote APPC LU Properties**

The screenshot shows the 'Remote APPC LU Properties' dialog box with the 'General' tab selected. The fields are as follows:

Connection:	HQMVS2
LU Alias:	D41DLU
Network Name:	ORACLE
LU Name:	D41DLU
Uninterpreted Name:	D41DLU
Comment:	DB2/MVS V4.1

Buttons at the bottom: OK, Cancel, Help.

Select the General tab. Determine the link with which to associate the LU (in the example, HQMVS2). Use the Connection drop-down list to select the connection used to access this LU. Enter the LU Alias, Network Name, LU Name, and Uninterpreted LU Name. You should contact the person responsible for your SNA network to determine the correct LU and network names. Note that you can use the LU Alias to define a name known only to SNA Server, and that name can remain the same even if the remote LU name changes. This helps to reduce the amount of maintenance required when network changes occur.

**Figure 6–19 Remote APPC LU Properties Options**

The screenshot shows the 'Remote APPC LU Properties' dialog box with the 'Options' tab selected. The fields are as follows:

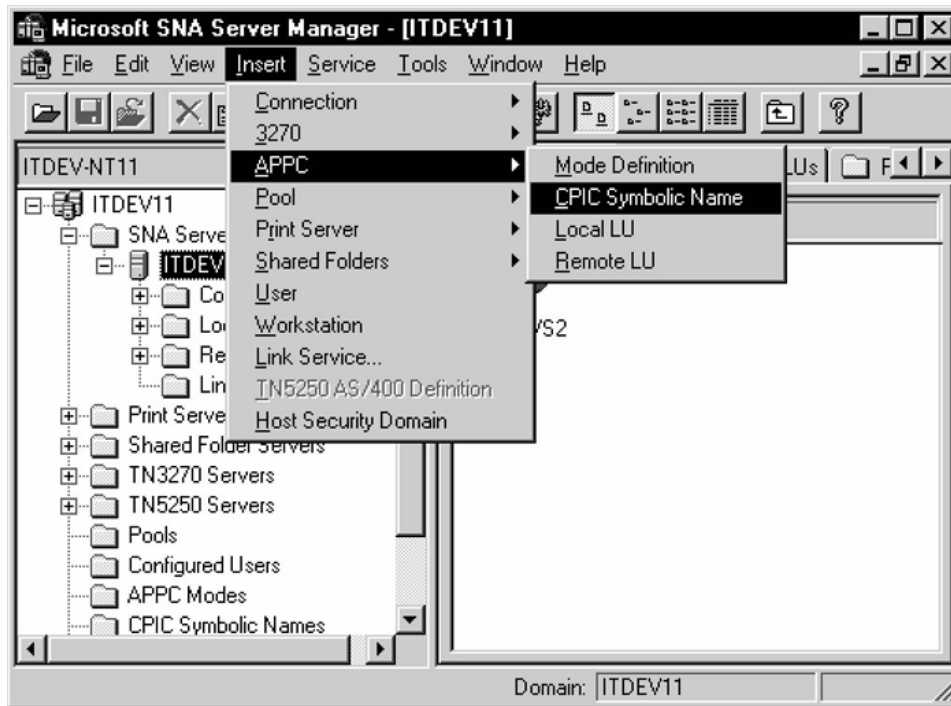
<input checked="" type="checkbox"/> Supports Parallel Sessions
Implicit Incoming Mode: <None>
Session-Level Security:
<input checked="" type="radio"/> No Session-Level Security
<input type="radio"/> Security Key in Hex      Security Key:
<input type="radio"/> Security Key in Characters      Verify Key:

Buttons at the bottom: OK, Cancel, Help.

Now, select the Options tab. Check the Supports Parallel Sessions check box. Use the Implicit Incoming Mode drop-down list to select the mode. Set any security options you need.

The remote APPC LU properties are now set. Click **OK** to continue.

**Figure 6–20** *CPI-C Symbolic Destination Name Window*



#### 6.4.3.8 CPI-C Symbolic Destination Names

Once the Local and Remote Partner definitions and Mode definitions have been created, you can create CPI-C Symbolic Destination Names, also called Side Information Profiles. The Side Information Profiles are used to identify target DRDA Server systems to be accessed through the gateway. From the Insert menu, select APPC CPI-C Symbolic Name. The CPI-C Name Properties dialog box appears.

**Figure 6–21 Enter General CPI-C Name Properties**

The screenshot shows the 'CPIC Name Properties' dialog box with the 'General' tab selected. The 'Name' field contains 'D41DLU' and the 'Comment' field contains 'DB2/MVS V4.1'. Under 'Conversation Security', the 'None' radio button is selected. The 'Mode Name' dropdown menu is set to 'IBMRDB'. There is a 'UserID...' button next to the 'Program' radio button. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Select the General tab. Enter a Name for Side Information. From the Mode Name drop-down list, select the correct mode.

---

**Note:** The DRDA\_CONNECT\_PARM should be assigned the name of the CPI-C Side Information Name entered earlier.

---

**Figure 6–22 Enter CPI-C Name Properties Partner Information**

The screenshot shows the 'CPIC Name Properties' dialog box with the 'Partner Information' tab selected. Under 'Partner TP Name', the 'SNA Service TP [in hex]' radio button is selected and the text field contains '07F6C4C2'. Under 'Partner LU Name', the 'Alias' radio button is selected and the text field contains 'D41DLU'. There are two empty text fields for the 'Fully Qualified' option. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

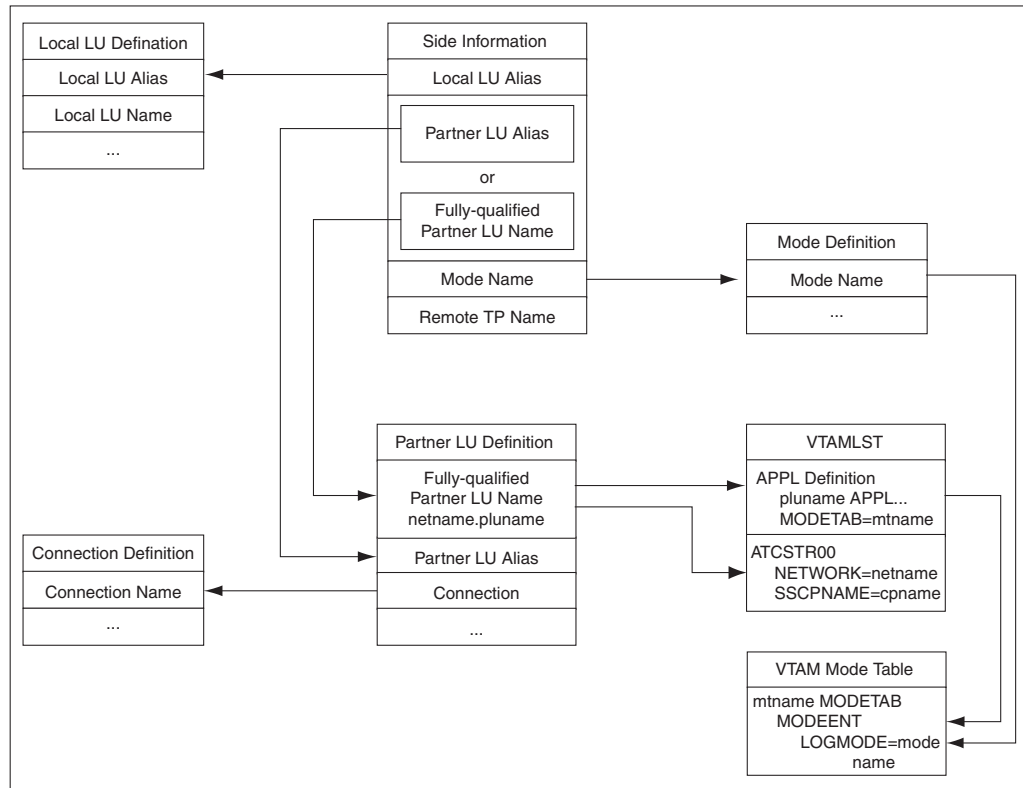
Now, select the Partner Information tab. Select Application TP and enter the TP name. Enter the Partner LU Name alias. Click **OK** to save the Side Information.

## 6.5 Testing the Connection

Before proceeding with the gateway configuration tasks in [Chapter 10, "Configuring the Gateway"](#), ensure that your connection is working. This can be done using SNA Server Manager.

Figure 6–23, "Relationship Between SNA Server Definitions and Host VTAM Definitions" shows the relationship between SNA Server definitions and the VTAM definitions on the host.

**Figure 6–23 Relationship Between SNA Server Definitions and Host VTAM Definitions**



## 6.6 Using SNA Session Security Validation

When the database link request for the gateway begins, the gateway attempts to start an APPC conversation with the DRDA Server. Before the conversation can begin, a session must start between the host Logical Unit (LU) and the DRDA Server LU.

SNA and its various access method implementations (including Microsoft SNA Server) provide security validation at session initiation time, enabling each LU to authenticate its partner. This is carried out entirely by network software before the gateway and server application programs begin their conversation and process conversation-level security data. If session-level security is used, then correct password information must be established in the Pentium-based host Connection Profile and in similar parameter structures in the DRDA Server system that is to be accessed. Refer to Microsoft SNA Server and IBM Communication Server product documentation for detailed information.

## 6.7 SNA Conversation Security

SNA conversation security is determined by the setting of the gateway initialization parameter, `DRDA_SECURITY_TYPE`. This parameter determines whether SNA security option `SECURITY` is set to `PROGRAM` or to `SAME`. Generally, the gateway operates under SNA option `SECURITY=PROGRAM`, but it can also be set to operate under SNA option `SECURITY=SAME`.

### 6.7.1 SNA Security Option SECURITY=PROGRAM

If `DRDA_SECURITY_TYPE=PROGRAM` is specified, then the gateway allocates the conversation with SNA option `SECURITY=PROGRAM` and sends this information to the DRDA Server:

- If the database link has explicit `CONNECT` information, then the specified user ID and password are sent.
- If the database link has no `CONNECT` clause and if the application has logged in to the Oracle integrating server with an explicit user ID and password, then the Oracle user ID and password are sent.
- If the application logs in to the Oracle integrating server with operating system authentication, and if the database link lacks explicit `CONNECT` information, then no user ID and password are sent. If no user ID and password are sent, and if the DRDA Server is not configured to assign a default user ID, then the connection fails.

In general, `SECURITY=PROGRAM` tells the DRDA Server to authenticate the user ID/password combination using whatever authentication mechanisms are available. For example, if DB2/OS390 is the DRDA Server, then RACF can be used. This is not always the case, however, because each of the IBM DRDA Servers can be configured to process inbound user IDs in other ways.

### 6.7.2 SNA Security Option SECURITY=SAME

The `SECURITY=SAME` option is not directly supported by Microsoft SNA Server. `SECURITY=SAME` implicitly validates security using the user account under which the TNS Listener was started. Microsoft SNA Server, however, does not support this type of validation.



---

---

# Configuring IBM Communication Server

This chapter describes configuration of the IBM Communication Server product on MS Windows for use with the Oracle Transparent Gateway for DRDA. IBM Communication Server provides SNA connectivity through the APPC/LU6.2 protocol between the host and the remote DRDA Server. Read this chapter to learn more about creating Communication Server profiles.

This chapter contains the following sections:

- [Before You Begin](#)
- [Checklist for Configuring the Communications Interfaces](#)
- [Creating IBM Communication Server Profiles for the Gateway](#)
- [Definition Types](#)
- [Testing the Connection](#)
- [Using SNA Session Security Validation](#)
- [SNA Conversation Security](#)

## 7.1 Before You Begin

This chapter requires you to enter parameters unique to your system in order to properly configure the IBM Communication Server. Refer to [Appendix E](#) for a worksheet listing all the installation parameters that you will need to know before you can complete the configuration process. Ask your network administrator to provide you with these parameters before you begin.

## 7.2 Checklist for Configuring the Communications Interfaces

- Step 1: [Creating IBM Communication Server Profiles for the Gateway](#)
- Step 2: [Definition Types](#)
- Step 3: [Testing the Connection](#)

## 7.3 Creating IBM Communication Server Profiles for the Gateway

The Oracle Transparent Gateway for DRDA requires a stored set of definitions, called Side Information Profiles, to support connections between the gateway and DRDA Servers. Each profile consists of a profile name and a profile type, a set of fields describing the profile. The fields in a given profile type are generally a mixture of

operating parameter values and names of other SNA profiles relevant to the profile. Each functional part of APPC, such as the Mode, Remote Transaction Program (RTP) name, and Logical Unit (LU), is described by a distinct profile type.

### 7.3.1 Independent Versus Dependent LUs

Oracle recommends independent LUs for the Oracle Transparent Gateway for DRDA, because they support multiple parallel sessions or conversations. This means multiple Oracle client applications can be active simultaneously with the same DRDA Server through the independent LU.

Dependent LUs support only one active session. The CP (IBM Communication Server, in this case) queues additional conversation requests from the gateway server behind an already active conversation. In other words, conversations are single-threaded for dependent LUs.

If a dependent LU is correctly defined, then no alterations to the Oracle Transparent Gateway for DRDA configuration are needed, nor should any changes be needed to the DRDA Server.

The operational impact of dependent LUs is that the first client application can start a conversation through the gateway with the DRDA Server. While that session is active (which could be seconds, minutes, or hours, depending on how the client application and transaction are designed), any other client application starting a session with the same DRDA Server appears to stop responding as it waits behind the previous session.

If a production application really uses only one conversation at any one time, then there should be no impact. However, additional concurrent conversations might be required for testing or other application development. Each requires that additional dependent LUs be defined on the remote host, plus additional IBM Communication Server configuration entries which define the additional dependent LUs on the host.

Additional Side Information Profiles should be defined to use the new dependent LUs. New Transparent Gateway for DRDA instances should be created and configured to use these new Side Information Profiles.

### 7.3.2 Creating SNA Definitions for the Gateway

IBM Communication Server definitions are created using the SNA Node Configuration tool, while the actual operation of the server is done using the SNA Node Operations tool, both of which are provided with IBM Communication Server. Maintenance of SNA definitions is normally done by a user with Administrator authority.

#### 7.3.2.1 Sample IBM Communication Server Definitions

The `tg4drda\sna\commsvr` subdirectory contains a sample set of IBM Communication Server definitions created with the SNA Node Configuration tool. The `oracle.acg` file contains sample definitions for IBM Communication Server.

Before building the IBM Communication Server definitions, examine the `oracle.acg` file to determine the definitions needed, their contents, and their interrelationships. The file format is text-oriented and each field of each definition is clearly labeled. You can print a copy of the file to use while working with your definitions in an SNA Node Configuration session.



## 7.4 Definition Types

There are several types of IBM Communication Server definitions relevant to gateway APPC/LU6.2 operation. Each definition can be created and edited using a corresponding SNA Node Configuration menu.

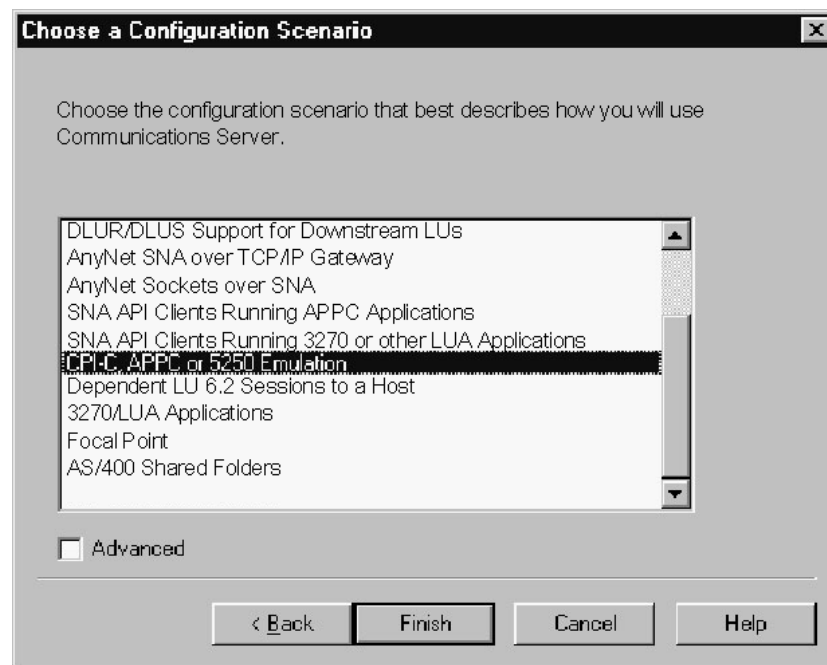
The definitions relevant to the gateway are presented here in hierarchical order. Those definition types that are lowest in the hierarchy are discussed first. This matches the logical sequence in which to create the profiles.

Refer to the IBM Communication Server online documentation for a complete discussion of IBM Communication Server definitions. This section is an overview of IBM Communication Server definitions in relation to the Oracle Transparent Gateway for DRDA.

### 7.4.1 IBM Communication Server Definitions

This section describes the process of creating SNA definitions for IBM Communication Server using the SNA Node Configuration tool. All the tasks described in this section are performed within SNA Node Configuration.

**Figure 7–1** *Choosing a Configuration Scenario*

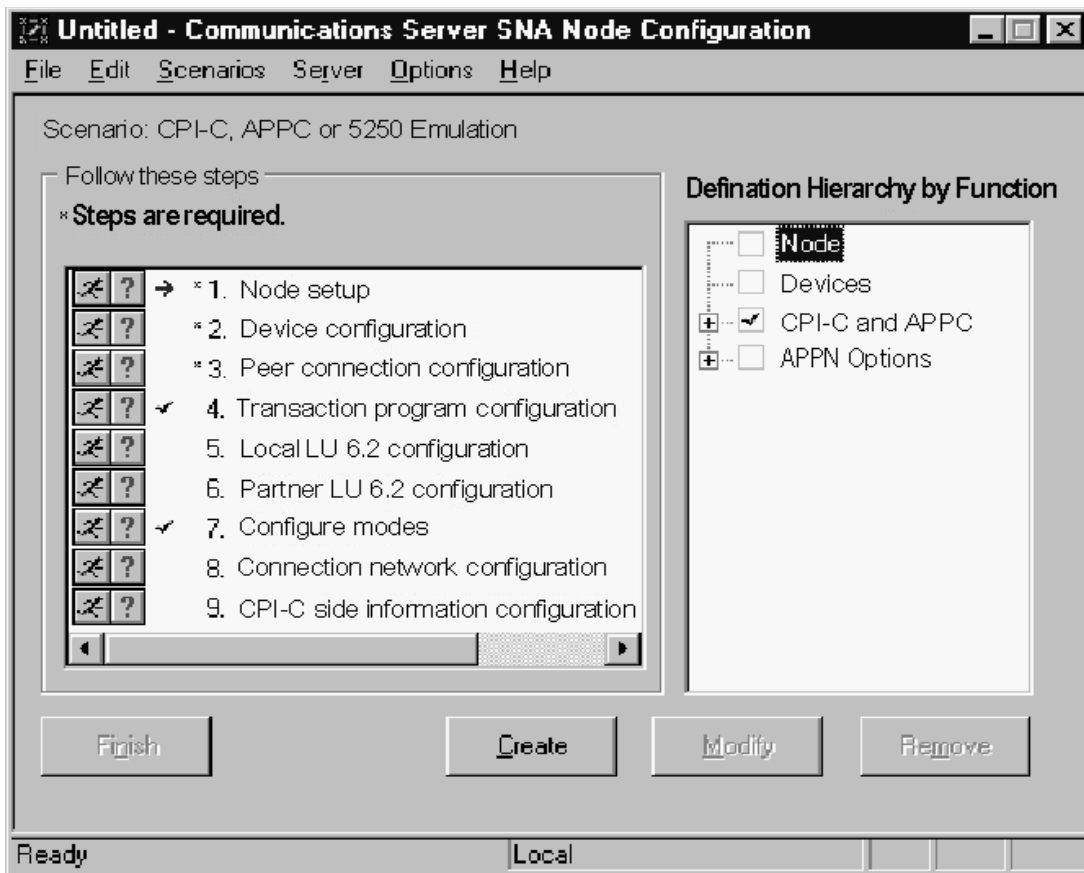


#### 7.4.1.1 Creating the Configuration

SNA Node Configuration will first ask if you are creating a new configuration or loading an existing configuration. The following example is presented with the assumption that a new configuration is being created.

SNA Node Configuration will next prompt you for a configuration scenario. Our example is made assuming that a CPI-C or APPC scenario is being chosen.

Figure 7-2 Creating the Node Configuration



### 7.4.1.2 Defining the Node

Each SNA Server must have a Control Point defined. This is typically called the Node definition. Click **Node** and click **Create**.

**Figure 7-3 Node Definition**

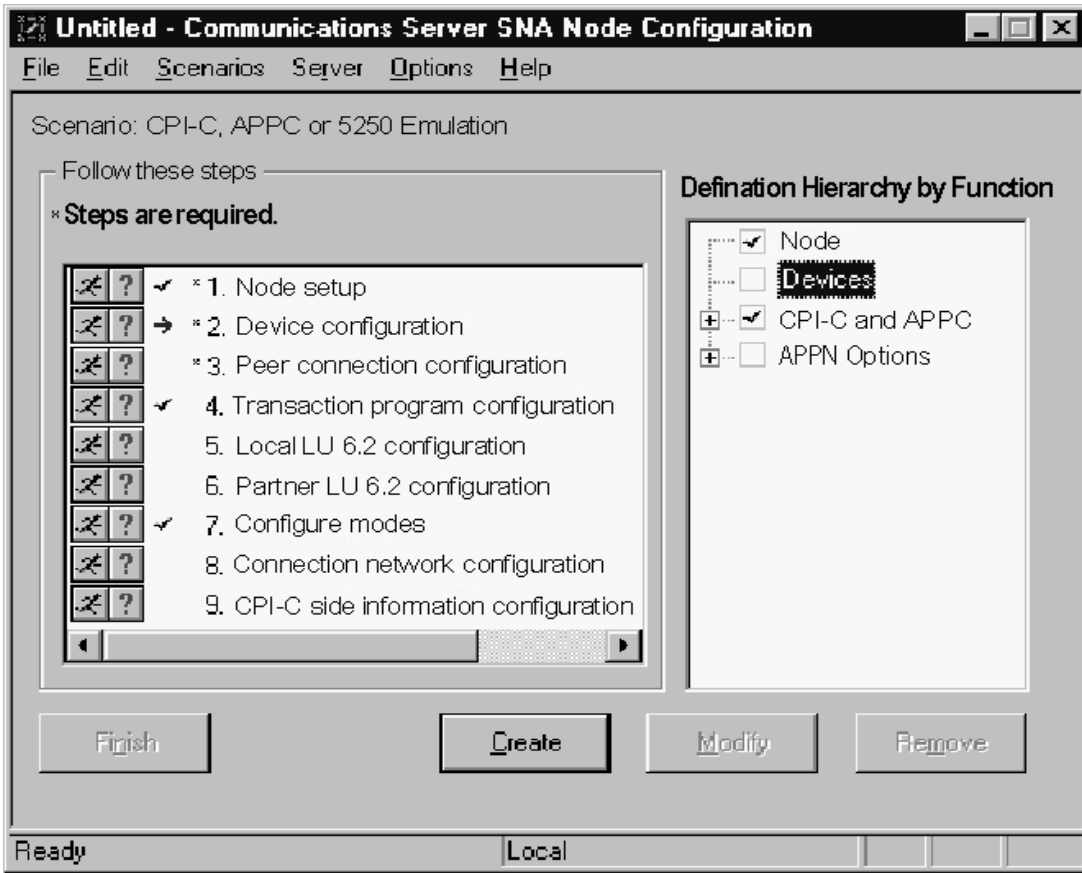
The screenshot shows a dialog box titled "Define the Node" with three tabs: "Basic", "Advanced", and "DLU Requester". The "Basic" tab is selected. It contains three main sections:

- Control Point (CP):** A group box containing "Fully qualified CP name:" with two text boxes containing "ORACLE" and "ITD\VDH2", and "CP alias:" with a text box containing "ITD\VDH2".
- Local Node ID:** A group box containing "Block ID:" with a text box containing "056" and "Physical Unit ID:" with a text box containing "00697".
- Node Type:** A group box containing three radio button options: "End Node" (selected), "Network Node", and "Branch Extender Node".

At the bottom of the dialog box are four buttons: "OK", "Cancel", "Apply", and "Help".

In the Define the Node dialog box, in the Basic tab, enter the Control Point, Local Node ID, and Node Type information. You can also select option in the Advanced tab depending on your SNA network configuration. Click **OK**.

**Figure 7-4 Creating Devices**



Communication devices should be configured next. Select **Devices**, and click **Create**.

**Figure 7-5 Choosing the Device Type**

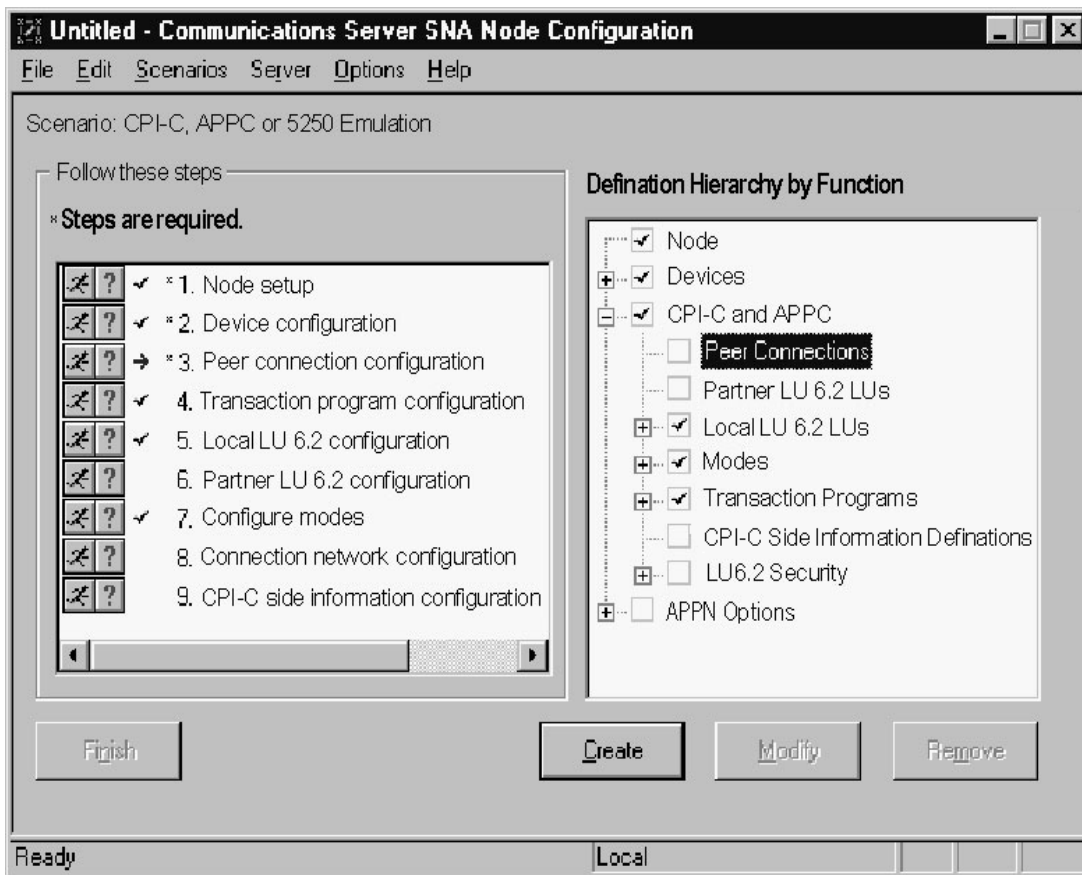


Select the type of device to use for communication. The LAN type is typical for either Ethernet or Token-ring attached network devices.

**Figure 7-6** *Configuring a LAN Device*

In the Basic tab, select the adapter to use and the local SAP. The other tabs may be explored for network tuning parameters. Click **OK**.

Figure 7-7 Creating Peer Connections



Peer connections should be configured next. Select **Peer Connections**, and click **Create**.

**Figure 7-8 Defining the Link station**

The screenshot shows a dialog box titled "Define a LAN Connection" with a close button (X) in the top right corner. The dialog has four tabs: "Basic", "Advanced", "Adjacent Node", and "Reactivation". The "Basic" tab is selected. Inside the dialog, there are several fields and controls:

- "Link station name:" text box containing "MVS08".
- "Device name:" dropdown menu showing "LAN1\_04".
- A button labeled "Discover network addresses...".
- "Destination address:" text box containing "40000000000".
- An unchecked checkbox labeled "Swap address bytes".
- "Remote SAP:" dropdown menu showing "04".

At the bottom of the dialog are four buttons: "OK", "Cancel", "Apply", and "Help".

In the Basic tab, enter a link station name for this connection. Choose the Device for the connection, and enter the destination address and remote SAP.

**Figure 7-9 Defining the Adjacent Node**

The screenshot shows a dialog box titled "Define a LAN Connection" with four tabs: "Basic", "Advanced", "Adjacent Node", and "Reactivation". The "Adjacent Node" tab is selected. The dialog contains the following fields:

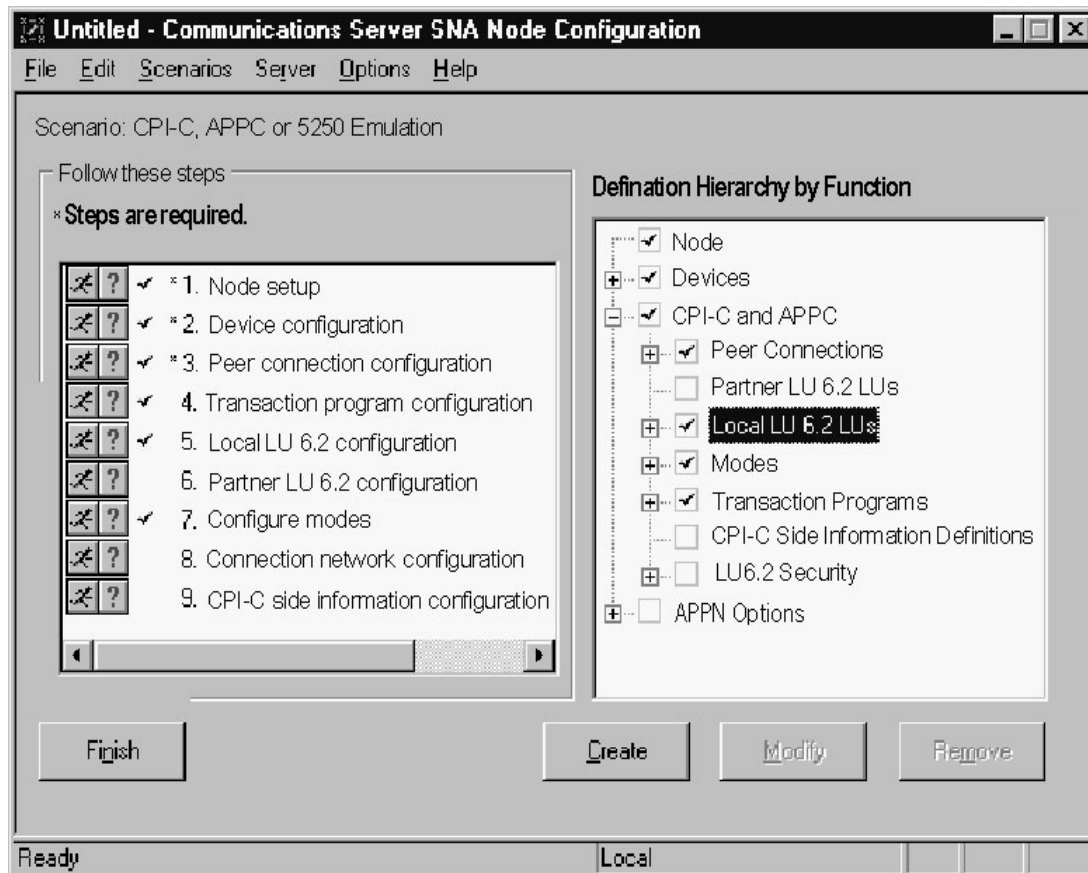
- Adjacent CP name:** Two text boxes containing "ORACLE" and "MVS08".
- Adjacent CP type:** A dropdown menu showing "Network Node".
- TG number:** A dropdown menu showing "1".
- Adjacent node ID:** A container with two sub-fields:
  - Block ID:** A text box containing "000".
  - Physical Unit ID:** A text box containing "00000".

At the bottom of the dialog are four buttons: "OK", "Cancel", "Apply", and "Help".

Select the Adjacent Node tab. Enter the Adjacent CP name of the remote system and pick its CP Type. You may have to choose a different Transmission Group (TG) as the default. Consult your SNA Network Administrator for details. The other tabs may be explored for tuning and link reactivation options. Click **OK**.

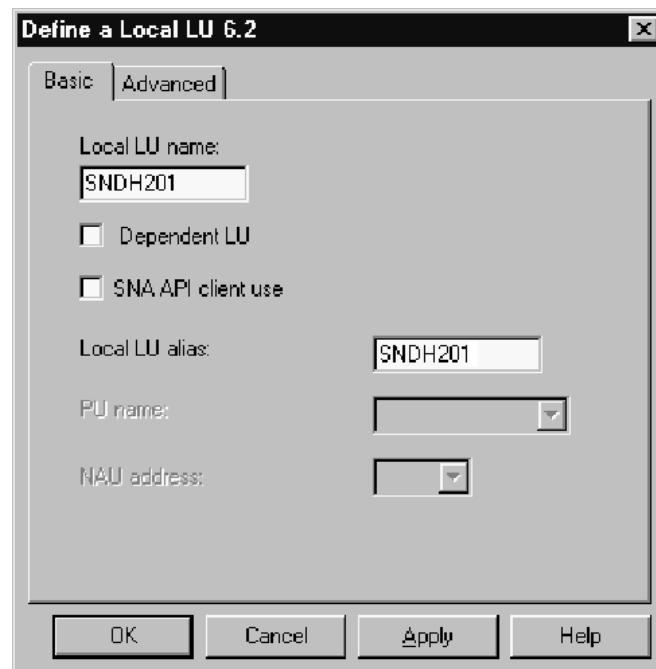


Figure 7-10 Create Local LUs



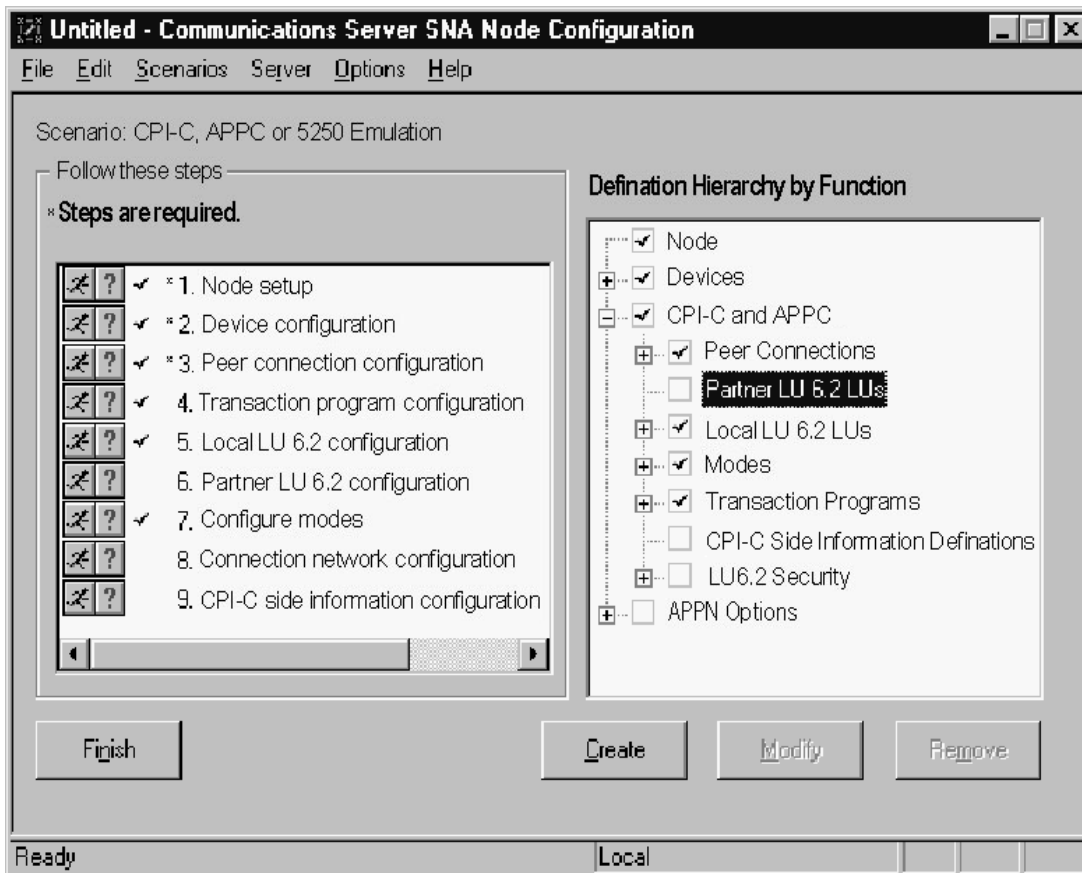
Next, define the local LUs for this Node. Select **Local LU 6.2 LUs**, and click **Create**.

Figure 7-11 Defining Local LUs



In the Basic tab, enter the name of the local LU and an alias, if desired. The name must match the Local LU definition of the remote host for this node. The Advanced tab may be explored for Synchronization support and for LU session limits. Click **OK**.

**Figure 7-12 Create Partner LUs**



Next, define remote Partner LUs for this Node to connect to. Select **Partner LU 6.2 LUs** and click **Create**.

**Figure 7-13 Defining Partner LUs**

The screenshot shows a dialog box titled "Define a Partner LU 6.2" with a close button (X) in the top right corner. The dialog has two tabs: "Basic" (selected) and "Advanced".

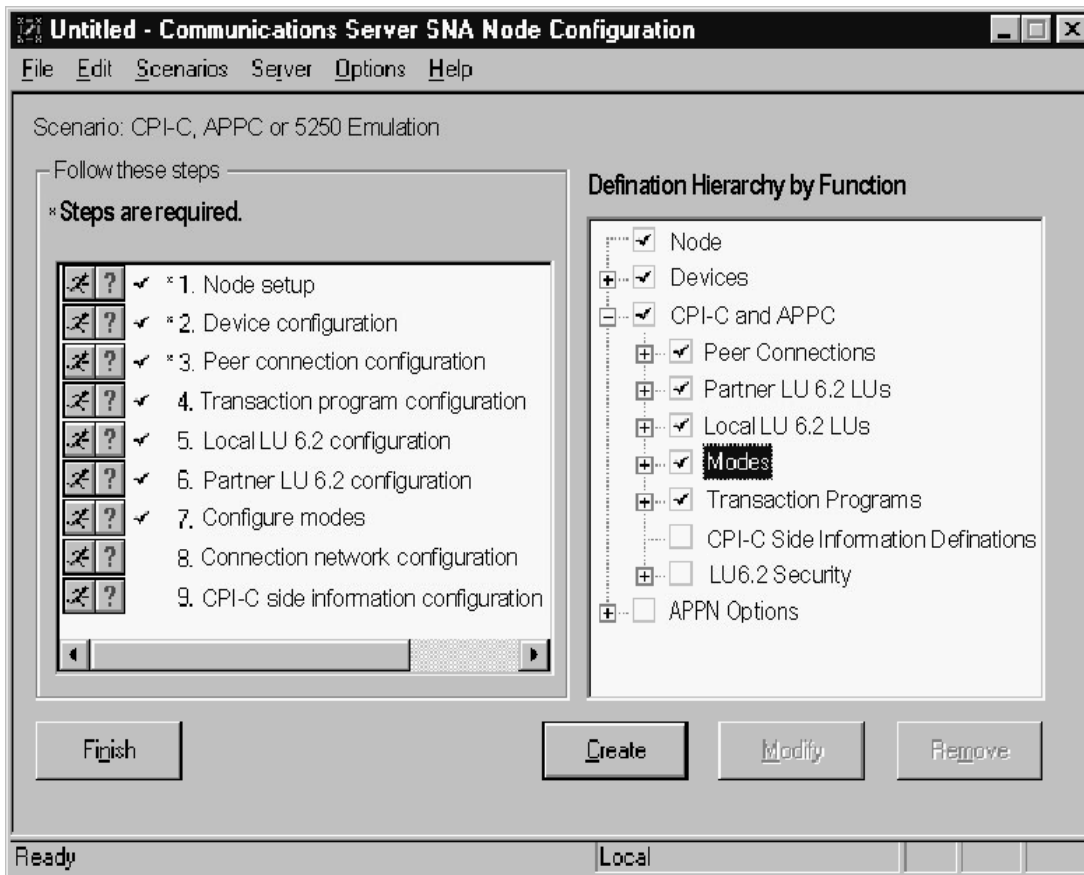
Under the "Basic" tab, the following fields and options are visible:

- Partner LU name:** Two text boxes containing "ORACLE" and "DB2V51LU", separated by a period.
- Wildcard**
- Partner LU alias:** A text box containing "DB2V51LU".
- Fully qualified CP name:** A section with two radio buttons:
  - New**: Below this option are two empty text boxes separated by a period.
  - Existing**: Below this option is a dropdown menu showing "ORACLE.MVS08".

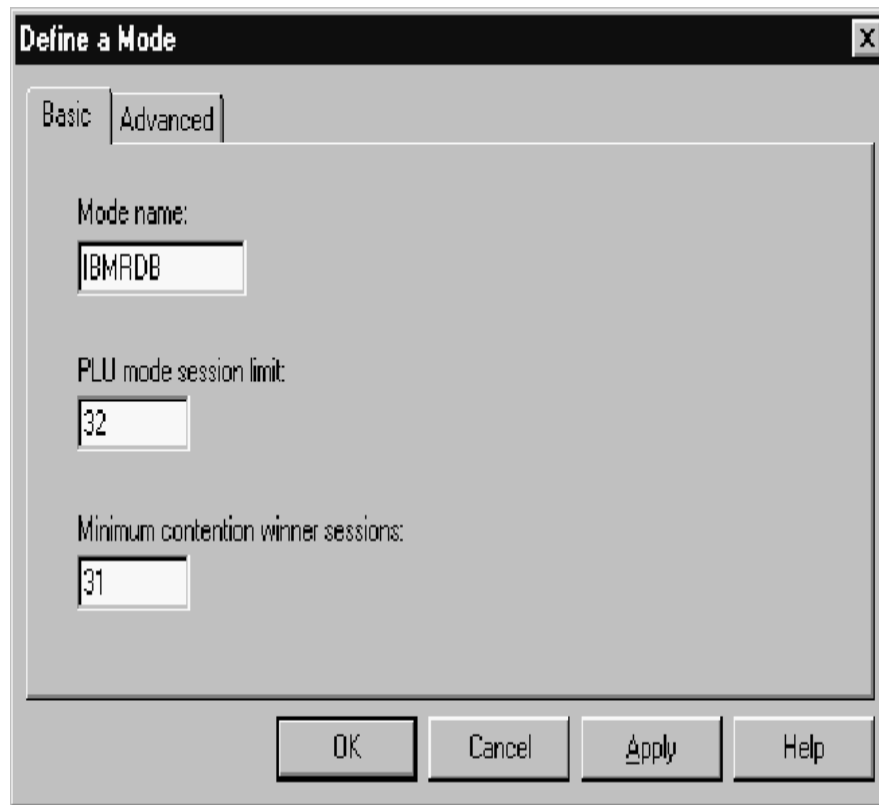
At the bottom of the dialog are four buttons: "OK", "Cancel", "Apply", and "Help".

In the Basic tab, enter the name of the remote or partner LU and an alias, if desired. Select Fully Qualified CP from the existing list. The Advanced tab may be explored for logical record limits and security support. Click **OK**.

Figure 7-14 Creating the IBMRDB Mode



Next, define the IBMRDB mode, which will be used for DRDA connections. Select Modes and click **Create**.

**Figure 7-15 Define the IBMRDB Mode**

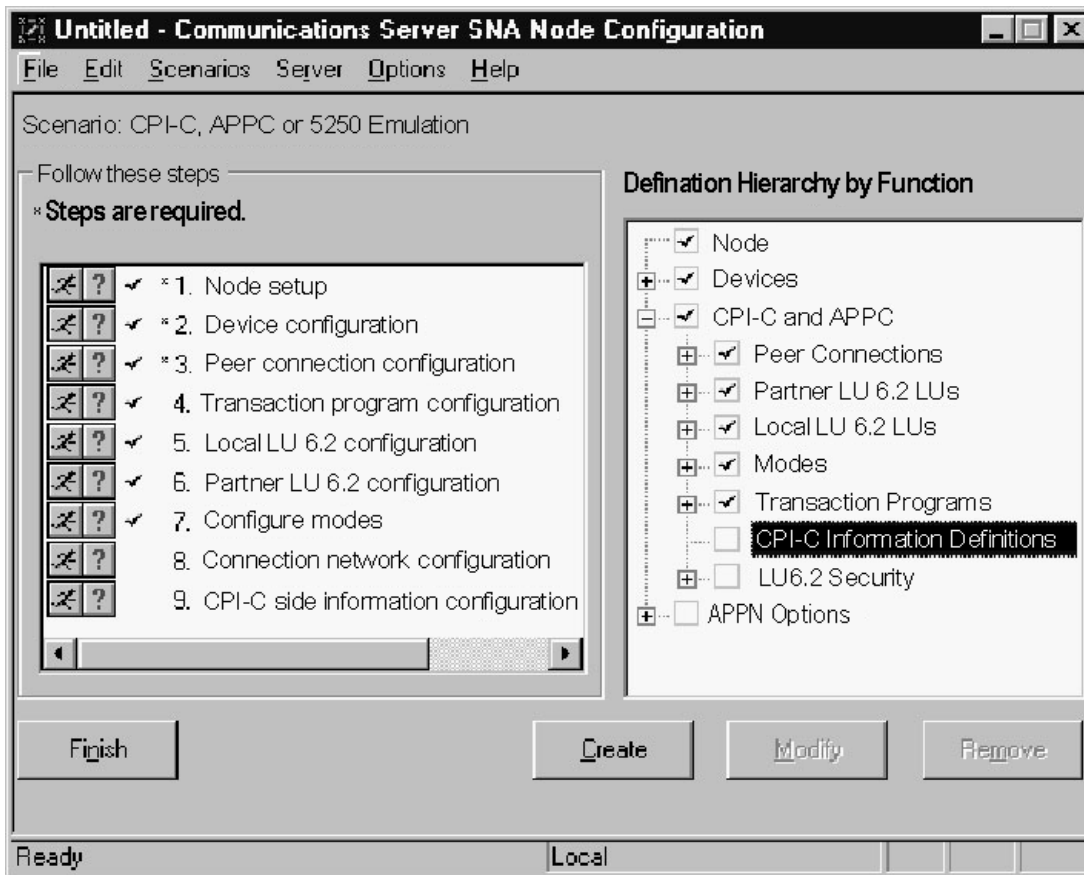
The screenshot shows a dialog box titled "Define a Mode" with a close button (X) in the top right corner. It has two tabs: "Basic" (selected) and "Advanced". The "Basic" tab contains three input fields:

- "Mode name:" with a text box containing "IBMRDB".
- "PLU mode session limit:" with a text box containing "32".
- "Minimum contention winner sessions:" with a text box containing "31".

At the bottom of the dialog box, there are four buttons: "OK", "Cancel", "Apply", and "Help".

In the Basic tab, enter the name IBMRDB and the mode session limits. Consult your SNA Network Administrator for details. The Advanced tab may be explored for pacing and autoactivation session options. Click **OK**.

Figure 7-16 Create the CPI-C Side Information Profile



Next, define the CPI-C profile that will be used by the gateway. Select CPI-C side information definitions and click **Create**.

Figure 7–17 Define the CPI-C Side Information Profile

The screenshot shows a dialog box titled "Define CPI-C Side Information" with a close button (X) in the top right corner. It has two tabs: "Basic" and "Security". The "Basic" tab is active. The fields are as follows:

- Symbolic destination name: DB2V51LU
- Mode name: IBMRDB (dropdown menu)
- Use partner LU name:
- Partner LU name: [ ] . [ ]
- Use partner LU alias:
- Partner LU alias: DB2V51LU (dropdown menu)
- TP name: 076DB
- Service TP:

Buttons at the bottom: OK, Cancel, Apply, Help.

In the Basic tab, enter the Symbolic Destination name. Select IBMRDB for the Mode name drop-down list, and select the Partner LU either by name or by alias. Enter the TP name for the remote DRDA Server. Mode DRDA Servers use the default Service TP name X'07F6C4C2' or '076DB'. Consult your DRDA Server Administrator for the correct TP name. The Advanced tab may be explored for security options.

---

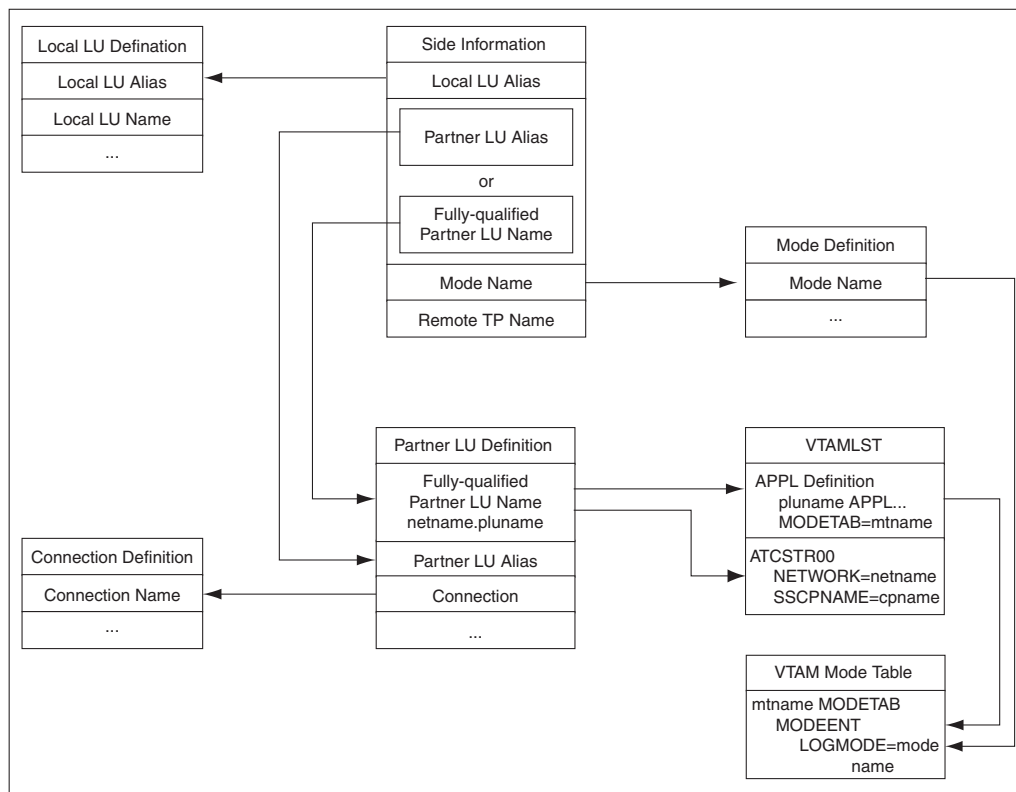
**Note:** The DRDA\_CONNECT\_PARM should be assigned the name of the Symbolic Destination name as entered in [Figure 7–16, "Create the CPI-C Side Information Profile"](#).

---

## 7.5 Testing the Connection

Before proceeding with the gateway configuration tasks in [Chapter 10, "Configuring the Gateway"](#), ensure that your connection is working. This can be done by using the SNA Node Operations tool.

[Figure 7–18, "Relationship Between IBM Communication Server Definitions and Host VTAM Definitions"](#) shows the relationship between IBM Communication Server definitions and the VTAM definitions on the host.

**Figure 7–18 Relationship Between IBM Communication Server Definitions and Host VTAM Definitions**

## 7.6 Using SNA Session Security Validation

When the database link request for the gateway begins, the gateway attempts to start an APPC conversation with the DRDA Server. Before the conversation can begin, a session must start between the host LU and the DRDA Server LU.

SNA and its various access method implementations (including IBM Communication Server) provide security validation at session initiation time, enabling each LU to authenticate its partner. This is carried out entirely by network software before the gateway and server application programs begin their conversation and process conversation-level security data. If session-level security is used, then correct password information must be established in the Pentium-based host Connection Profile and in similar parameter structures in the DRDA Server system that is to be accessed. Refer to Microsoft SNA Server and IBM Communication Server product documentation for detailed information.

## 7.7 SNA Conversation Security

SNA conversation security is determined by the setting of the gateway initialization parameter, `DRDA_SECURITY_TYPE`. This parameter determines whether SNA security option `SECURITY` is set to `PROGRAM` or to `SAME`. Generally, the gateway operates under SNA option `SECURITY=PROGRAM`, but it can also be set to operate under SNA option `SECURITY=SAME`.



### 7.7.1 SNA Security Option SECURITY=PROGRAM

If `DRDA_SECURITY_TYPE=PROGRAM` is specified, then the gateway allocates the conversation with SNA option `SECURITY=PROGRAM` and sends this information to the DRDA Server:

- If the database link has explicit `CONNECT` information, then the specified user ID and password are sent.
- If the database link has no `CONNECT` clause and if the application has logged in to the Oracle integrating server with an explicit user ID and password, then the Oracle user ID and password are sent.
- If the application logs in to the Oracle integrating server with operating system authentication and if the database link lacks explicit `CONNECT` information, then no user ID and password are sent. If no user ID and password are sent and if the DRDA Server is not configured to assign a default user ID, then the connection fails.

In general, `SECURITY=PROGRAM` tells the DRDA Server to authenticate the user ID/password combination using whatever authentication mechanisms are available. For example, if DB2/OS390 is the DRDA Server, then RACF can be used. This is not always the case, however, because each of the IBM DRDA Servers can be configured to process inbound user IDs in other ways.

### 7.7.2 SNA Security Option SECURITY=SAME

The `SECURITY=SAME` option is not directly supported by IBM Communication Server. `SECURITY=SAME` implicitly validates security by using the user account under which the TNS listener was started. IBM Communication Server, however, does not support this type of validation.



---

---

## Configuring TCP/IP

This chapter describes configuring TCP/IP for the Microsoft Windows platforms that are supported by the Oracle Transparent Gateway for DRDA. TCP/IP is a communications facility that is already part of the operating system. No third-party protocol software is required. Read this chapter to learn more about configuring TCP/IP.

This chapter contains the following sections:

- [Before You Begin](#)
- [Configuring TCP/IP](#)

### 8.1 Before You Begin

This chapter requires you to enter parameters that are unique to your system in order to properly configure TCP/IP. Refer to [Appendix E](#) for a worksheet listing all of the installation parameters that you will need to know about before you complete the configuration process. Ask your network administrator to provide you with these parameters before you begin.

#### 8.1.1 Port Number

The DRDA standard specifies that port 446 be used for DRDA services. However, if several DRDA Servers are operating on the same system, then they will need to provide service on different ports. Therefore, the port number that is used by each DRDA Server will need to be extracted from the configuration of each individual DRDA Server. DB2 for OS/390 and DB2/400 typically use the DRDA standard port number, 446, whereas DB2/UDB typically uses 50000 as the port number. Refer to IBM DB2 Administrator and Installation guides for locating and changing these port numbers for the DRDA Server. For additional information, consult your DB2 DBA or system administrator.

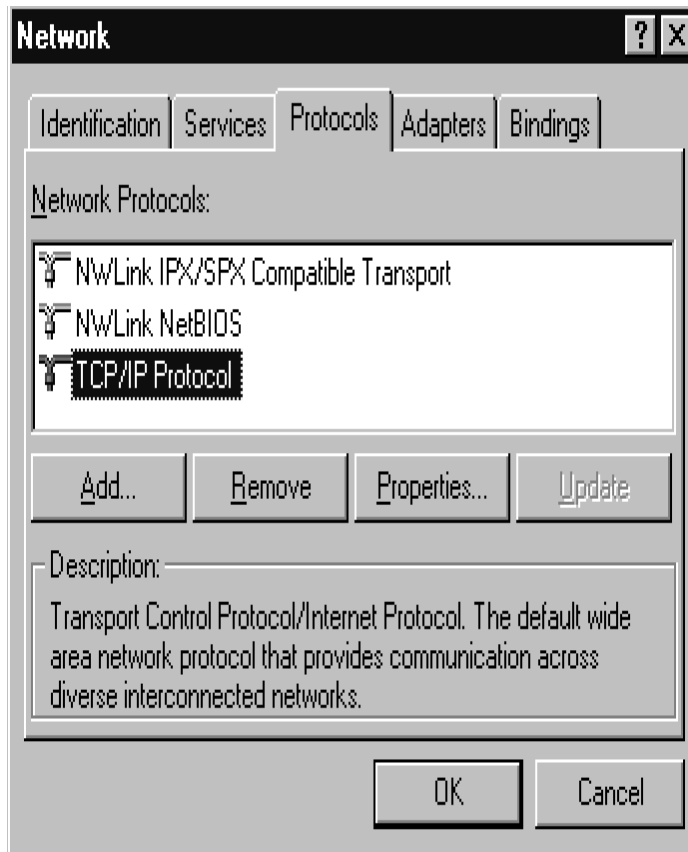
### 8.2 Configuring TCP/IP

The following configuration example is for Microsoft Windows NT 4.0. Other Microsoft Windows operating systems may have these panels in a different location or may present them differently, but the required contents will be essentially the same.

You configure TCP/IP from the network configuration tool in the Microsoft Windows Control Panel.

Select the Protocol tab and select TCP/IP Protocol. Then, click **Properties** to display the Properties panel.

**Figure 8–1 Network Configuration Tool**

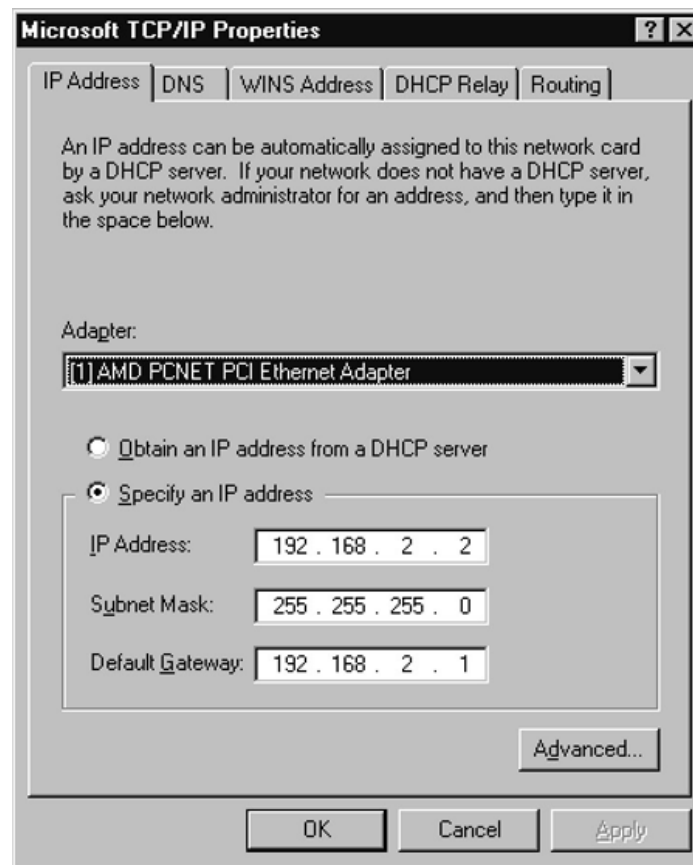


If the TCP/IP Protocol is not already installed, then click **Add** and then select the TCP/IP Protocol.

Configuration consists of assigning a host name, an IP address, and a network mask to a given network interface.

In the IP Address tab, use the drop-down list to select the adapter you will use. Your network administrator can tell you whether you will be using DHCP or a static IP address. If using a static IP, then you must enter the correct values for IP address, subnet mask, and default gateway.

Figure 8-2 TCP/IP Properties Panel



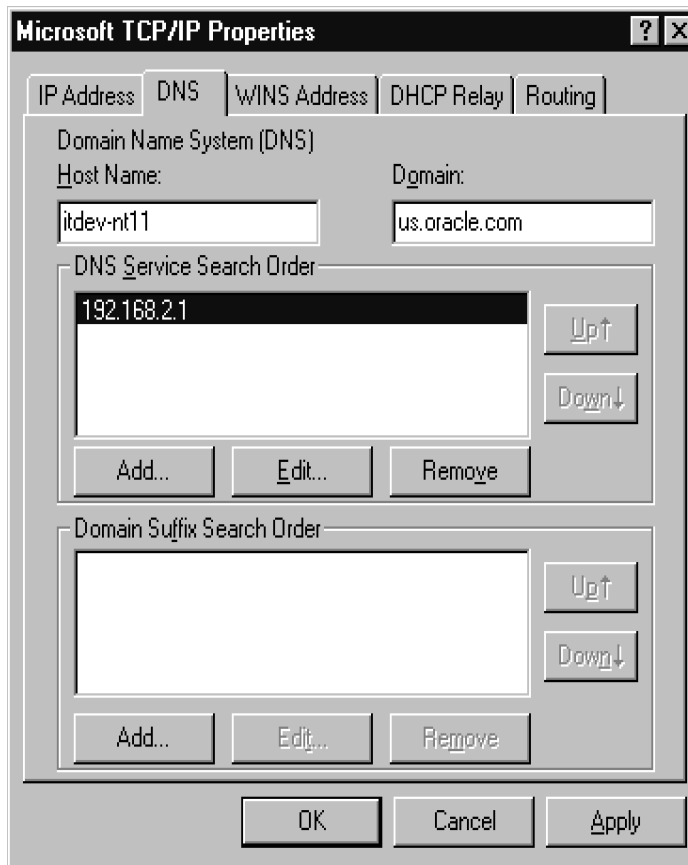
Additional configuration consists of defining a name server IP address or creating entries in the hosts file on the local system. Name server translate host names into IP Addresses when queried on a particular host name. The hosts file provides this same functionality, but in a non-network participating manner.

The Hosts file may be edited with a text editor of your choice. For example, in Microsoft Windows NT, the file is located in:

```
C:\winnt\system32\drivers\etc\hosts
```

where C:\winnt is the Windows NT system root.

To use a name server, you must configure the TCP/IP to use DNS. Select the DNS tab and enter a host name and domain name. Your network administrator will provide these values. Click **Add** below the Domain Suffix Search Order box and enter the IP Address of the name server. You may enter up to three name servers. Click **OK**.

**Figure 8–3 Define a Name Server**

For local configuration (in other words, the gateway and the DRDA Server are on the same system), it may be desirable to use the loop-back address. The IP address is 127.0.0.1 and is typically given the local name ("localhost" or "loopback") in the Hosts file. Using the loop-back address reduces the amount of network overhead by handling the traffic internally without actually talking to the network.

The gateway is configured for TCP/IP using the DRDA\_CONNECT\_PARM initialization file parameter. In an SNA configuration, this parameter would be set to the Side Information Profile name (name set in [Figure 6–21](#) or [Figure 7–17](#)). In a TCP/IP configuration, this parameter should be set to the IP address or Host name of the DRDA Server, which should be followed by the Service Port number of that server. For more information about the port number, refer to "[Port Number](#)" on page 8-1.

---

**Note:** When installing the gateway, you must choose either SNA or TCP/IP for the networking interface. The DRDA\_CONNECT\_PARM must be configured correctly for the chosen networking interface.

---

The rest of the DRDA-specific parameters are unrelated to the communications protocol and may be set the same for either SNA or TCP/IP installations.

Example #1: Configuration for a DRDA Server on a host named 'mvs01.domain.com' (or IP address of 192.168.1.2) with a Service Port number of 446.

```
DRDA_CONNECT_PARM=mvs01.domain.com:446
```

or

```
DRDA_CONNECT_PARM=192.168.1.2:446
```

**Example #2:** Configuration for a DRDA Server on the same host as the gateway with a Service Port number of 446.

```
DRDA_CONNECT_PARM=localhost:446
```

**or**

```
DRDA_CONNECT_PARM=127.0.0.1:446
```

For additional information on configuring TCP/IP, refer to the Microsoft Windows installation and configuration guides.





Oracle Net is an Oracle product providing network communication between Oracle applications, Oracle Servers, and Oracle Gateways across different systems.

This chapter contains the following sections:

- [Checklists for Oracle Net](#)
- [Oracle Net and SQL\\*Net Introduction](#)
- [Oracle Net Overview](#)
- [Configuring Oracle Net](#)
- [Advanced Security Encryption](#)
- [Setting Up Advanced Security Encryption for Test](#)
- [Testing Advanced Security Encryptions](#)

## 9.1 Checklists for Oracle Net

Use the following checklists when you are installing and configuring Oracle Net.

### 9.1.1 [Configuring Oracle Net](#)

- [Step 1: Modify the listener.ora file](#)
- [Step 2: Modify the tnsnames.ora file](#)

### 9.1.2 [Advanced Security Encryption](#)

Use the following checklists for encryption.

#### 9.1.2.1 [Setting Up Advanced Security Encryption for Test](#)

- [Step 1: Set Advanced Security Encryption Parameters for the Gateway](#)
- [Step 2: Set Advanced Security Encryption Parameters](#)

#### 9.1.2.2 [Testing Advanced Security Encryptions](#)

- [Step 1: Connect the Gateway and Oracle the Integrating Server](#)
- [Step 2: Reset Configuration Parameters on the Gateway](#)

## 9.2 Oracle Net and SQL\*Net Introduction

Oracle Net provides connectivity to the Gateway through the use of Protocol Adapters, SQL\*Net, and the TNS Listener. Configuration of Oracle Net is backward compatible with past versions of SQL\*Net. A new facility called Heterogeneous Services (HS) has been added to both Oracle Net and the Gateway to improve the throughput of SQL\*Net data. For additional information, refer to *Oracle Database Net Services Administrator's Guide* and *Oracle Database Heterogeneous Connectivity Administrator's Guide*.

## 9.3 Oracle Net Overview

Oracle Net is a required Oracle product supporting network communications between Oracle applications, Oracle servers, and Oracle gateways across different CPUs or operating systems. It also supports communication across different Oracle databases and CPUs providing distributed database and distributed processing capabilities.

Oracle Net also enables applications to connect to multiple Oracle servers or gateways across a network, selecting from a variety of communications protocols and application program interfaces (APIs) to establish a distributed processing and distributed database environment.

A communications protocol is a set of implemented standards or rules governing data transmission across a network. An API is a set of subroutines providing an interface for application processes to the network environment.

### 9.3.1 Distributed Processing

Dividing processing between a front-end computer running an application and a back-end computer used by the application is known as distributed processing. Oracle Net enables an Oracle tool or application to connect to a remote computer containing an Oracle server or Oracle gateway.

### 9.3.2 Distributed Database

Several databases linked through a network, appearing as a single logical database, are known as a distributed database. An Oracle tool running on a client computer or on an Oracle server running on a host computer can share and obtain information retrieved from other remote Oracle servers. Regardless of the number of database information sources, you might be aware of only one logical database.

### 9.3.3 Terminology for Oracle Net

The following terms are used to explain the architecture of Oracle Net for Microsoft Windows:

**host** is the computer the database resides on and that runs the Oracle server or gateway.

**client (task)** is the application using an Oracle Net driver to communicate with the Oracle server or gateway.

**protocol** is a set of standards or rules governing the operation of a communication link.

**driver** is the part of Oracle Net supporting a given network protocol or communication method.

**network** is a configuration of devices and software connected for information interchange.

## 9.4 Configuring Oracle Net

The gateway must be defined to the TNS listener, and a service name must be defined for accessing the gateway.

### 9.4.1 Step 1: Modify the listener.ora file

Add an entry for the gateway to the listener.ora file. For example:

```
(SID_DESC=
  (SID_NAME=sidname)
  (ORACLE_HOME=C:\oracle\GTWHome)
  (PROGRAM=g4drsrv))
```

Refer to [Appendix B, "Sample Files"](#), for a sample listener.ora file.

---

**Note:** The `PROGRAM=g4drsrv` parameter is required. It specifies to the listener the name of the gateway executable.

---

### 9.4.2 Step 2: Modify the tnsnames.ora file

Add a gateway service name to the tnsnames.ora file on the system where your Oracle integrating server resides. Specify the service name in the `USING` parameter of the database link defined for accessing the gateway from the Oracle Database 10g server.

You can use the IPC protocol only if the Oracle integrating server and the gateway reside on the same system. If you use the IPC protocol adapter, then add an entry like this to tnsnames.ora:

```
linkname1 = (DESCRIPTION=
  (ADDRESS=
    (PROTOCOL=IPC)
    (KEY=ORAIPC) )
  (CONNECT_DATA=(SID=sidname))
  (HS=)
)
```

where:

*linkname1* is the name used to define the database link referencing the gateway.

*ORAIPC* is the IPC key defined in the listener.ora file for the IPC protocol

*sidname* is the gateway SID, the same SID that you used for the entry in the listener.ora file.

If you are using the TCP/IP protocol adapter, then add this entry to tnsnames.ora:

```
linkname2 = (DESCRIPTION=
  (ADDRESS=
    (PROTOCOL=TCP)
    (PORT=port)
    (HOST=hostname) )
  (CONNECT_DATA=(SID=sidname))
  (HS=)
)
```

where:

*linkname2* is the name used to define the database link referencing the gateway

*port* is the default Oracle TCP/IP port number (1541)

*hostname* is the name of your host system

*sidname* is the gateway SID

Refer to "[Sample Oracle Net tnsnames.ora File](#)" on page B-2 for a sample tnsnames.ora file. For more information about configuring Oracle Net, refer to the *Oracle Database Net Services Reference* and *Oracle Database Net Services Administrator's Guide*.

## 9.5 Advanced Security Encryption

Oracle Net supports the CHECKSUM command and the Export encryption algorithms. The following sections describe a basic method of verifying this feature if it is used at your site. The easiest way to determine if Advanced Security encryption is attempting to work is to deliberately set wrong configuration parameters and attempt a connection between the server and client. Incorrect parameters cause the connection to fail.

After receiving the expected failure message, set the configuration parameters to the correct settings and try the connection again. Encryption is working properly if you receive no further error messages.

## 9.6 Setting Up Advanced Security Encryption for Test

The following procedures test Advance Security encryption by the method explained earlier. The incorrect parameter settings produce error 12660

1. Set Advanced Security encryption parameters for the gateway
2. Set Advanced Security encryption parameters for the Oracle integrating server

---

---

**Note:** The international or export version of Advanced Security encryption supports the following encryption types:

- des40
  - rc4\_40
- 
- 

### 9.6.1 Step 1: Set Advanced Security Encryption Parameters for the Gateway

Edit the Oracle Net configuration file on the Microsoft Windows system (gateway system) to add the following parameters and values:

```
SQLNET.CRYPTO_CHECKSUM_SERVER = REJECTED
SQLNET.ENCRYPTION_SERVER = REJECTED
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER = (SHA1)
SQLNET.ENCRYPTION_TYPES_SERVER = (DES40,RC4_40)
SQLNET.CRYPTO_SEED = "abcdefg123456789"
```

The value shown for `SQLNET.CRYPTO_SEED` is only an example. Set it to the value you want. Refer to the *Oracle Database Advanced Security Administrator's Guide* for more information.

## 9.6.2 Step 2: Set Advanced Security Encryption Parameters

Set Advanced Security Encryption parameters for the Oracle integrating server. Edit the Oracle Net configuration file on the Oracle integrating server system to add the following parameters:

```
SQLNET.CRYPTO_CHECKSUM_CLIENT = REQUIRED
SQLNET.ENCRYPTION_CLIENT = REQUIRED
SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT = (SHA1)
SQLNET.ENCRYPTION_TYPES_CLIENT = (DES40,RC4_40)
SQLNET.CRYPTO_SEED = "abcdefg123456789"
```

The value shown for `SQLNET.CRYPTO_SEED` is only an example.

## 9.7 Testing Advanced Security Encryptions

After completing Steps 1 and 2 to set up Advanced Security encryption, you are ready to test the operation of the Advanced Security encryption by using the following steps:

1. Connect the gateway and the Oracle integrating server.
2. Reset configuration parameters on the gateway.

### 9.7.1 Step 1: Connect the Gateway and Oracle the Integrating Server

Use SQL\*Plus to log on to the Oracle integrating server. Access the gateway through a database link. You should receive the following error:

```
ORA-12660: Encryption or crypto-checksumming
```

### 9.7.2 Step 2: Reset Configuration Parameters on the Gateway

Change the following Advanced Security encryption parameters on the gateway to:

```
SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED
SQLNET.ENCRYPTION_SERVER = REQUIRED
```

Attempt the connection between the gateway and the Oracle integrating server again. If no error message is returned and the connection completes, then you can assume that Advanced Security encryption is working properly.



---

---

## Configuring the Gateway

After you have installed the gateway, configured your DRDA Server, and configured your SNA or TCP/IP software, you must configure the gateway.

This chapter contains the following sections:

- [Configuration Checklist](#)
- [Choosing a Gateway System Identifier \(SID\)](#)
- [Gateway Configuration](#)
- [Configuring the Host](#)
- [DRDA Gateway Package Considerations](#)
- [Backup and Recovery of Gateway Configuration](#)
- [Configuring the Oracle Integrating Server](#)
- [Accessing the Gateway from Other Oracle Servers](#)
- [Accessing Other DRDA Servers](#)
- [Gateway Installation and Configuration Complete](#)

### 10.1 Configuration Checklist

#### **Choosing a Gateway System Identifier (SID)**

- [Enter the SID on the Worksheet](#)

#### **Configuring the Host**

- [Step 1: Copy the gateway initialization](#)
- [Step 2: Determine settings for gateway initialization parameters](#)
- [Step 3: Tailor the initsid.ora File](#)

#### **Binding the DRDA Gateway Package**

- [Step 1: Log on to an Oracle integrating server](#)
- [Step 2: Create a database link](#)
- [Step 3: Run the stored procedure GTW\\$\\_BIND\\_PKG](#)

### **Binding Packages on DB2/Universal Database (DB2/UDB)**

- Step 1: Log in to the system where DB2/UDB is running.
- Step 2: Copy the following files.
- Step 3: Connect to the database.
- Step 4: Create the `ORACLE2PC` table:
- Step 5: Commit the transaction:
- Step 6: Optionally, verify that the table was created under the correct user ID:
- Step 7: Disconnect from the session:

### **Before Binding the DRDA Gateway Package**

- Step 1: Check all DRDA parameter settings
- Step 2: If using DB2/UDB, then create `ORACLE2PC` table

### **Sample SQL scripts**

- Step 1: Run Data Dictionary scripts
  - Step 1a: Upgrading from a previous gateway version
  - Step 1b: Creating the Data Dictionary tables and views
- Step 2: DB2/UDB or other server
  - Step 2a: If server is DB2/UDB, then grant authority to package
  - Step 2b: If server is not DB2/UDB, then create the `ORACLE2PC` table

### **Configuring the Oracle Integrating Server**

- Step 1: Create a database link
- Step 2: Create synonyms and views

### **Accessing the Gateway from Other Oracle Servers**

- Step 1. Create a database link with which to access the gateway.
- Step 2. Define synonyms and views for tables.
- Step 3. Perform `GRANT` statements.

### **Accessing Other DRDA Servers**

- Step 1: Configure another APPC profile set for the DRDA Server.
- Step 2: Configure additional DRDA Server instances.
- Step 3: Bind the DRDA package to the DRDA Server.

## **10.2 Choosing a Gateway System Identifier (SID)**

The gateway SID is a string of alphabetic and numeric characters that identifies a gateway instance. The SID is used in the file names of gateway parameter files and in the connection information that is associated with the Oracle server database links that access the gateway.



## 10.2.1 Enter the SID on the Worksheet

Enter the SID in [Appendix E, "Configuration Worksheet"](#).

A separate SID is required for each DRDA Server to be accessed. You might also have multiple SIDs for one DRDA Server to use different gateway parameter settings with that server. For information on configuring additional SIDs, refer to ["Accessing Other DRDA Servers"](#) on page 10-9.

## 10.3 Gateway Configuration

The information in this chapter describes the configuration process for the gateway. All gateway parameters are kept in the `initsid.ora` gateway initialization file, which is stored in the gateway `admin/` directory.

## 10.4 Configuring the Host

The data in this chapter describes the configuration process for the gateway. You should notice that most, if not all, gateway parameters have been moved into the `initsid.ora` initialization file. To configure the host for the Oracle Transparent Gateway for IBM DRDA, you tailor the parameter files for your installation.

To start with one of the provided sample configuration files, proceed to Step 1 below. To create entirely new configuration files, proceed to Step 2.

---

---

**Note:** In previous versions of the gateway, the initialization parameters were stored in the files named `initsid.ora` and `initsid.gtwboot` in the gateway instance directories. With Release 10.1.0.2.0 of the gateway, most parameters that were in `'initsid.gtwboot'` have been moved to `initsid.ora`. The syntax of the `initsid.ora` has been simplified. Refer to [Appendix C](#) for details.

When migrating from previous releases of TG4DRDA, please be aware of these differences.

---

---

### 10.4.1 Step 1: Copy the gateway initialization

Sample gateway initialization files (`initsid.ora`) are shipped on the distribution CD-ROM. These files are in the `ORACLE_HOME\tg4drda\admin` directory:

- `initDB2.ora`, for DB2/OS390 remote servers
- `initDB2VM.ora`, for DB2/VM remote servers
- `initAS400.ora`, for DB2/400 remote servers
- `initDB2UDB.ora`, for DB2/UDB remote servers

Copy one of these sample files into the same directory, renaming it with the name of your gateway SID. For example, if you chose your SID to be DRD1 in ["Choosing a Gateway System Identifier \(SID\)"](#), and if your remote server is DB2, then copy the `initDB2.ora` file and rename it `initDRD1.ora`.

### 10.4.2 Step 2: Determine settings for gateway initialization parameters

Your Configuration Worksheet in [Appendix E](#) should be complete. If not, review the incomplete entries and refer to the sections listed for more information. You need this information to tailor the gateway initialization file, `initsid.ora`.

Refer to [Appendix C, "DRDA-Specific Parameters"](#) for information on the DRDA-specific `initsid.ora` parameters.

### 10.4.2.1 Required Parameters

When you edit your `initsid.ora` file, you must change the values of all the parameters listed in the Configuration Worksheet in [Appendix E](#), using the values in the right-hand column of the worksheet.

You will also need to set certain NLS gateway parameters. For more information on setting these parameters, refer to [Appendix D, "National Language Support"](#).

### 10.4.2.2 Optional Parameters

Several DRDA-specific parameters are not required, but you might want to change them. Unless otherwise indicated, these parameters are described in [Appendix C](#).

**Table 10–1** *Optional DRDA-Specific Parameters*

DRDA parameters	Description
DRDA_DISABLE_CALL	Used to disable stored procedure support for DRDA Servers on which the gateway does not support stored procedures
DRDA_ISOLATION_LEVEL	Defines the package Isolation Level
HS_DB_NAME	Specifies the database SID name and must be set to the gateway SID
DRDA_OPTIMIZE_QUERY	Used for data query optimization
DRDA_PACKAGE_COLLID	Defines the package collection ID
DRDA_PACKAGE_NAME	Defines the name of the package
DRDA_PACKAGE_OWNER	Defines the owner of the package. By default, the owner is the user ID that is used when you run the <code>g4drutl bind</code> utility. This parameter is not valid for SQL/DS.
DRDA_PACKAGE_SECTIONS	Defines the maximum number of concurrent OPEN cursors at the remote server
HS_DB_DOMAIN	Specifies the gateway database domain

The values that are set in your `initsid.ora` file should work for most installations. Edit the values if changes are needed. For information on NLS-related `initsid.ora` parameters, refer to ["NLS Parameters in the Gateway Initialization File"](#) on page D-4.

## 10.4.3 Step 3: Tailor the `initsid.ora` File

After you have copied the sample initialization file, you will need to tailor it to your installation. While many parameters can be left to their defaults, some parameters must be changed for correct operation of the gateway. Give attention to the following DRDA and HS parameters. Also, give attention to the security aspects of the initialization file. [Chapter 13, "Security Considerations"](#), contains details on encryption of passwords that would otherwise be embedded in the initialization file. See [Appendix C](#) for a description of each parameter:

- DRDA\_CONNECT\_PARM
- DRDA\_PACKAGE\_COLLID
- DRDA\_PACKAGE\_NAME

- DRDA\_PACKAGE\_OWNER
- DRDA\_REMOTE\_DB\_NAME
- FDS\_CLASS
- HS\_DB\_NAME
- HS\_DB\_DOMAIN

#### 10.4.4 Binding the DRDA Gateway Package

The product requires a package to be bound on the DRDA Server. The gateway has an internal, stored procedure that must be used to create this package. The internal stored procedure is called from an Oracle integrating server. (Refer to "[Configuring Oracle Net](#)" on page 9-3 of [Chapter 9, "Oracle Net"](#). Also refer to "[Configuring the Oracle Integrating Server](#)" on page 10-8 of this chapter.) Before this package can be bound on the DRDA Server, the gateway initialization file must be correctly configured. Refer to [Appendix C](#).

1. Log on to an Oracle integrating server

Use either SQL\*Plus or Server Manager:

```
> sqlplus system/manager
```

2. Create a database link

Create a database link with a user ID and with a password that has proper authority on the DRDA Server to create packages.

```
SQL> CREATE PUBLIC DATABASE LINK dblink
2 CONNECT TO userid IDENTIFIED BY password
3 USING 'tns_name_entry'
```

---



---

**Note:** The user ID that is creating the public database link must have the "CREATE PUBLIC DATABASE LINK" privilege.

---



---

Refer to "[Configuring the Oracle Integrating Server](#)" later in this chapter.

3. Run the stored procedure GTW\$\_BIND\_PKG

```
SQL> exec GTW$_BIND_PKG@dblink;
SQL> COMMIT;
```

This creates and commits the package. If any errors are reported, then correct the gateway initialization file parameters as needed.

#### 10.4.5 Binding Packages on DB2/Universal Database (DB2/UDB)

If you are connecting to a DB2/UDB DRDA Server, then DB2/UDB requires that you create the ORACLE2PC table before binding the DRDA package. Other DRDA Servers enable you to bind the package before the ORACLE2PC table exists.

To create the ORACLE2PC table:

1. Log in to the system where DB2/UDB is running.

Check that you have the ability to address the DB2/UDB instance where the ORACLE2PC table will reside.

2. Copy the following files.

Copy from the `ORACLE_HOME\tg4drda\install\db2udb` directory:

- `o2pc.sql` (SQL script for creating the table)
- `o2pcg.sql` (SQL script for granting package access to PUBLIC)

3. Connect to the database.

Use the user ID that you will use for binding the package:

```
$ db2 'CONNECT TO database USER userid USING password'
```

---

---

**Note:** The user ID must have CONNECT, CREATETAB, and BINDADD authority to be able to connect to the database, to create the table, and to create the package.

---

---

For more information, refer to "[DB2/UDB \(Universal Database\)](#)" on page 5-4.

4. Create the ORACLE2PC table:

```
$ db2 -tf o2pc.sql
```

5. Commit the transaction:

```
$ db2 'COMMIT'
```

6. Optionally, verify that the table was created under the correct user ID:

```
$ db2 'LIST TABLES FOR USER'  
$ db2 'COMMIT'
```

7. Disconnect from the session:

```
$ db2 'DISCONNECT CURRENT'
```

## 10.5 DRDA Gateway Package Considerations

The DRDA package must be bound with the internal stored procedure `GTW$_BIND_PKG`. You must perform this bind step if this release is the first time the gateway has been installed on the system. If you are upgrading from version 9 of the gateway, then a rebind is not necessary unless the initialization parameters have been changed.

The user ID used to bind or rebind the DRDA package must have the suitable privileges on the remote database, as described in [Chapter 5, "Configuring the DRDA Server"](#).

### 10.5.1 Before Binding the DRDA Gateway Package

Check DRDA parameter settings and create your `ORACLE2PC` table before binding the DRDA gateway package.

#### 10.5.1.1 Step 1: Check all DRDA parameter settings

Check all DRDA parameter settings to be sure that they are set correctly before you start the bind. For example, the default for `DRDA_DISABLE_CALL` works only if your DRDA database supports stored procedures. If not, then you must change the setting. Also, the value for `DRDA_PACKAGE_NAME` must be unique if you have any older

versions of the gateway installed. New packages replace any old packages with the same name, causing versions of the gateway that use the old package to fail. Refer to [Appendix C](#) for information on the parameters and their settings.

#### 10.5.1.2 Step 2: If using DB2/UDB, then create ORACLE2PC table

If your DRDA Server is DB2/UDB, then create the ORACLE2PC table. Refer to "[Binding Packages on DB2/Universal Database \(DB2/UDB\)](#)" on page 10-5 for information on creating the table.

### 10.5.2 Sample SQL scripts

SQL scripts are provided to perform steps such as creating the ORACLE2PC table, removing obsolete tables and views, using previous releases, and creating tables and views to provide data dictionary support. Use the correct subdirectory for your DRDA Server platform:

```
tg4drda\install\db2   for DB2/OS390
tg4drda\install\as400 for DB2/400
tg4drda\install\db2vm for DB2/VM
tg4drda\install\db2udb for DB2/UDB
```

These scripts must be run on the DRDA Server platform using a database native tool (such as SPUI on DB2/OS390), because no tool is provided with the gateway to run these scripts. Note that when running these scripts, the user ID used must be suitably authorized.

#### 10.5.2.1 Step 1: Run Data Dictionary scripts

If your DRDA Server is DB2/OS390, DB2/400, or DB2/UDB, then run the following scripts to create the Data Dictionary tables and view.

#### 10.5.2.2 Step 1a: Upgrading from a previous gateway version

If you are upgrading from a previous version of the gateway then run the `dropold.sql` script to drop the old data dictionary definitions.

#### 10.5.2.3 Step 1b: Creating the Data Dictionary tables and views

Run the `g4ddtab.sql` and `g4ddvwXX.sql` scripts to create the Data Dictionary tables and views:

```
g4ddvwr7.sql DB2/OS390 V7 (RACF security)
g4ddvws7.sql DB2/OS390 V7 (DB2 security)
g4ddvwr8.sql DB2/OS390 V8 (RACF security)
g4ddvws8.sql DB2/OS390 V8 (DB2 security)
g4ddvw51.sql DB2/400 V5.1
g4ddvw52.sql DB2/400 V5.2
g4ddvwu7.sql DB2/UDB V7
g4ddvwu8.sql DB2/UDB V8
```

#### 10.5.2.4 Step 2: DB2/UDB or other server

Depending on the DRDA Server, perform one of the following steps:

### 10.5.2.5 Step 2a: If server is DB2/UDB, then grant authority to package

If your DRDA Server is DB2/UDB, then the `ORACLE2PC` table has already been created (see the previous sections). For all users to be able to use the table, run `o2pcg.sql` granting authority to all users.

### 10.5.2.6 Step 2b: If server is not DB2/UDB, then create the ORACLE2PC table

If your DRDA Server is not DB2/UDB, then the `ORACLE2PC` table must be created. Run `o2pc.sql`.

## 10.6 Backup and Recovery of Gateway Configuration

The configuration of the gateway is stored in the gateway initialization file. These files are stored in `ORACLE_HOME\tg4drda\admin`. Because they are simple text files, you may back them up using an archiving tool of your choice.

## 10.7 Configuring the Oracle Integrating Server

Configure the Oracle integrating server, regardless of the platform on which it is installed. It can be on the host, but this is not required.

### 10.7.1 Step 1: Create a database link

To access the DRDA Server, you must create a public database link. A public database link is the most common of database links. Refer to "[Processing a Database Link](#)" on page 11-1 for information about creating database links. In the following example, the Oracle Database server and the gateway are on the same host.

```
CREATE PUBLIC DATABASE LINK DB2 USING 'tns_name_entry'
```

---

---

**Note:** The user ID that is creating the public database link must have the "CREATE PUBLIC DATABASE LINK" privilege.

---

---

### 10.7.2 Step 2: Create synonyms and views

To facilitate accessing data using the gateway, define synonyms and views for the DRDA data tables. If needed, then perform `GRANT` statements to ensure that the synonyms and views are accessible to the correct groups of users. For more information, refer to "[Using the Synonym Feature](#)" on page 11-3.

## 10.8 Accessing the Gateway from Other Oracle Servers

Perform the following steps for each of the Oracle integrating servers from which you want to access the gateway:

1. Create a database link with which to access the gateway.
2. Define synonyms and views for tables.  
These are for tables that are accessed through the gateway, if needed.
3. Perform `GRANT` statements.

These statements are for the synonyms and views that you create.

Provide local or Oracle Net access from the Oracle servers to the gateway.

## 10.9 Accessing Other DRDA Servers

To access other DRDA Servers from the Oracle integrating server, use the following steps:

1. Configure another APPC profile set for the DRDA Server.

Only Side Information and Partner LU Profiles must be new. You can point to existing configuration information for other profiles unless you need to modify other aspects of the connection. For example, if you are using a different network adapter, then you must configure an entire APPC profile set. No additional profiles need to be configured for TCP/IP.

2. Configure additional DRDA Server instances.

To configure an additional instance, create new gateway initialization files. If you are using Oracle Net, then add entries to the `listener.ora` file and the `tnsnames.ora` file with the new SIDs.

Other components, including the gateway `ORACLE_HOME` directory structure, can be shared among multiple gateway instances.

3. Bind the DRDA package to the DRDA Server.

## 10.10 Gateway Installation and Configuration Complete

The Oracle Transparent Gateway for DRDA installation and configuration process is now complete. The gateway is ready for use.





---

---

## Using the Gateway

Using the gateway involves connecting to the gateway system and the remote DRDA database that is associated with it. Understanding how to process and how to use database links is important. Database links are discussed in detail in the *Oracle Database Administrator's Guide*. Read the database link information in that guide to understand database link processing. Then, read this chapter to understand how to set up a database link to a remote DRDA database.

This chapter contains the following sections:

- [Processing a Database Link](#)
- [Accessing the Gateway](#)
- [Accessing AS/400 File Members](#)
- [Using the Synonym Feature](#)
- [Performing Distributed Queries](#)
- [Read-Only Gateway](#)
- [Replicating in a Heterogeneous Environment](#)
- [Copying Data from the Oracle Server to the DRDA Server](#)
- [Copying Data from the DRDA Server to the Oracle Server](#)
- [Tracing SQL Statements](#)

### 11.1 Processing a Database Link

The database and application administrators of a distributed database system are responsible for managing the necessary database links that define paths to the DRDA database.

#### 11.1.1 Creating Database Links

To create a database link and define a path to a remote database, use the `CREATE DATABASE LINK` statement. The `CONNECT TO` clause specifies the remote user ID and password to use when creating a session in the remote database. The `USING` clause points to a `tnsnames.ora` connect descriptor.

---

---

**Note:** If you do not specify a user ID and a password in the `CONNECT TO` clause, then the Oracle server user ID and password are used. For additional information, refer to [Chapter 13, "Security Considerations"](#).

---

---

The following syntax creates a database link to access information in the DRDA Server database:

```
CREATE PUBLIC DATABASE LINK dblink
CONNECT TO userid IDENTIFIED BY password
USING 'tns_name_entry';
```

where:

*dblink* is the complete database link name.

*userid* is the user ID that is used to establish a session in the remote database. This user ID must be a valid DRDA Server user ID. It must be authorized to any table or file on the DRDA Server that is referenced in the SQL commands. The user ID cannot be longer than eight characters.

*password* is the password that is used to establish a session in the remote database. This must be a valid DRDA Server password. The password cannot be longer than eight characters.

*tns\_name\_entry* specifies the Oracle Net TNS connect descriptor that is used to identify the gateway.

## 11.1.2 Guidelines for Database Links

Database links are active for the duration of a gateway session. If you want to close a database link during a session, then use the `ALTER` session statement.

## 11.1.3 Dropping Database Links

You can drop a database link with the `DROP DATABASE LINK` statement. For example, to drop the public database link named *dblink*, enter the statement:

```
DROP PUBLIC DATABASE LINK dblink;
```

---

---

**Attention:** A database link should not be dropped if it is required to resolve an in-doubt distributed transaction. Refer to the *Oracle Database Administrator's Guide* for additional information about dropping database links.

---

---

## 11.1.4 Examining Available Database Links

The data dictionary of each database stores the definitions of all the database links in that database. Your `USER_DB_LINKS` data dictionary view shows your defined database links. The `ALL_DB_LINKS` data dictionary views show all defined database links.

## 11.1.5 Limiting the Number of Active Database Links

You can limit the number of connections from a user process to remote databases by using the parameter `OPEN_LINKS`. This parameter controls the number of remote

connections that any single user process can use concurrently with a single SQL statement. Refer to the *Oracle Database Administrator's Guide* for additional information about limiting the number of active database links.

## 11.2 Accessing the Gateway

To access the gateway, complete the following steps on the Oracle integrating server.

### 11.2.1 Step 1: Log in to the Oracle integrating server

This is the first step to accessing the gateway.

### 11.2.2 Step 2: Create a database link to the DRDA database

For example, use:

```
CREATE PUBLIC DATABASE LINK DRDA
CONNECT TO user_id IDENTIFIED BY password
USING 'tns_name_entry'
```

### 11.2.3 Step 3: Retrieve data from the DRDA database

This query fetches the TABLE file in the library SECURE, using the name ORACLE as the DRDA Server user profile. The ORACLE user profile must have the suitable privilege on the DRDA Server to access the SECURE.TABLE files:

```
SELECT * FROM SECURE.TABLE@DRDA
```

The following messages are displayed if insufficient privileges were granted to the ORACLE user profile:

```
ORA-1031: insufficient privileges
TG4DRDA V10.2.0.1.0 grc=0, drc=-777 (83TC,0000), errp=ARIXO,
sqlcode=-551, sqlstate=42501, errd=FFFFFF9C,0,0,0,0,0
errmc=USER SELECT SECURE.TABLE
```

## 11.3 Accessing AS/400 File Members

There is nothing specific to DRDA or to the gateway that enables or does not enable access to AS/400 files and file members. However, DB2/400 uses a naming convention that implies that the file member name is the same as the name of the file being addressed. For example, accessing schema.table implies that table is the file name and also that table is the file member name being accessed.

To access file members with names that differ from the associated file name, you must create a view within the file so that DB2/400 can reference the correct file member.

The method involves running the console command Create Logical File (CRTLF). This action creates a logical association between the file name and the file member name.

For additional information, refer to the AS/400 Command documentation or to the DB2/400 SQL reference.

## 11.4 Using the Synonym Feature

You can provide complete data, location, and network transparency by using the synonym feature of the Oracle server. When a synonym is defined, the user need not

know the underlying table or network protocol being used. A synonym can be public, available to all Oracle users. A synonym can also be defined as private, available only to the user who created it. Refer to the *Oracle Database Administrator's Guide* for details on the synonym feature.

The following statement creates a systemwide synonym for the EMP file in the DRDA Server with ownership of Oracle:

```
CREATE PUBLIC SYNONYM EMP FOR ORACLE.EMP@DRDA
```

## 11.5 Performing Distributed Queries

The Oracle Transparent Gateway technology enables the processing of distributed queries that join Oracle servers and DRDA Servers, and any other data store for which Oracle Corporation provides a gateway. These complex operations can be completely transparent to the users requesting the data.

The distributed query optimizer (DQO) capability can provide better performance of distributed queries. Statistical data regarding tables from DRDA Servers is retrieved and passed to the Oracle integrating server. The DQO capability is turned on and off by the DRDA\_OPTIMIZE\_QUERY parameter. Refer to "[DRDA\\_OPTIMIZE\\_QUERY](#)" on page C-6 of [Appendix C, "DRDA-Specific Parameters"](#).

### 11.5.1 Example of a Distributed Query

The following example joins data between an Oracle server, DB2/OS390, and a DRDA Server:

```
SELECT o.custname, p.projno, e.ename, sum(e.rate*p.hours)
FROM orders@DB2 o, EMP@ORACLE7 e, projects@DRDA p
WHERE o.projno = p.projno
AND p.empno = e.empno
GROUP BY o.custname, p.projno, e.ename
```

A combination of views and synonyms, using the following SQL statements, keeps the process of distributed queries transparent to the user:

```
CREATE SYNONYM orders for orders@DB2;
CREATE SYNONYM PROJECTS for PROJECTS@DRDA;
CREATE VIEW details (custname,projno,ename,spend)
AS
SELECT o.custname, p.projno, e.ename, sum(e.rate*p.hours)
FROM orders o, EMP e, projects p
WHERE o.projno = p.projno
AND p.empno = e.empno
GROUP BY o.custname, p.projno, e.ename;
```

This SQL statement retrieves information from these three data stores in one command:

```
SELECT * FROM DETAILS;
```

The results of this command are:

CUSTNAME	PROJNO	ENAME	SPEND
ABC Co.	1	Jones	400
ABC Co.	1	Smith	180
XYZ Inc.	2	Jones	400
XYZ Inc.	2	Smith	180

## 11.5.2 Two-Phase Commit Processing

To fully participate in a two-phase commit transaction, a server must support the `PREPARE TRANSACTION` statement. The `PREPARE TRANSACTION` statement ensures that all participating databases are prepared to `COMMIT` or `ROLLBACK` a specific unit of work.

The Oracle server supports the `PREPARE TRANSACTION` statement. Any number of Oracle servers can participate in a distributed two-phase commit transaction. The `PREPARE TRANSACTION` statement is performed automatically when a `COMMIT` transaction is run explicitly by an application or implicitly at the normal end of the application. No other action is needed.

The gateway does not support the `PREPARE TRANSACTION` statement limiting the two-phase commit protocol when the gateway participates in a distributed transaction. The gateway becomes the commit focal point site of a distributed transaction. Because the gateway is configured as commit/confirm, it is always the commit point site, regardless of the commit point strength setting. The gateway commits the unit of work after verifying that all Oracle databases in the transaction have successfully committed their work. Because the gateway must coordinate the distributed transaction, only one gateway can participate in an Oracle two-phase commit transaction.

Two-phase commit transactions are recorded in the `ORADRD.A.Oracle2PC` table, which is created during installation. This table is created when the `o2pc.sql` script is run. The owner of this table also owns the package. Refer to "[DRDA Gateway Package Considerations](#)" on page 10-6 for more information.

## 11.5.3 Distributed DRDA Transactions

Because the `Oracle2PC` table is used to record the status of a gateway transaction, the table must reside at the database where the DRDA update takes place. Therefore, all updates that take place over the gateway must be local to the IBM database.

---

---

**Note:** Updates to the `Oracle2PC` table cannot be part of an IBM distributed transaction.

---

---

For additional information about the two-phase commit process, refer to the *Oracle Database Administrator's Guide*.

## 11.6 Read-Only Gateway

The read-only option can provide improved performance and security. This improved performance depends on your configuration and parameter selections. A gateway initialization parameter, `DRDA_READ_ONLY`, is used to control whether the gateway is enabled in this mode.

If you enable the read-only feature, then only queries (`SELECT` statements) are permitted by the gateway. The capabilities that control whether updates are permitted through the gateway are not enabled. These capabilities include `INSERT`, `UPDATE`, `DELETE`, and stored-procedure support (pass-through SQL and DB2 stored procedures). Statements attempting to modify records on the DRDA Server are rejected.

Oracle recommends that you do not routinely switch between settings of the `DRDA_READ_ONLY` parameter. If you need both update and `DRDA_READ_ONLY`

functionality, then you should create two separate instances of the gateway with different read-only settings.

## 11.7 Replicating in a Heterogeneous Environment

Oracle Transparent Gateway for DRDA provides a number of options for replicating Oracle and non-Oracle data throughout the enterprise.

### 11.7.1 Oracle Database 10g Server Triggers

When updates are made to the Oracle Database server, synchronous copies of Oracle and non-Oracle data can be maintained automatically by using Oracle Database 10g server triggers.

### 11.7.2 Oracle Snapshots

Oracle Transparent Gateway for DRDA can use the Oracle snapshot feature to automatically replicate non-Oracle data into the Oracle Database server. The complete refresh capability of Oracle Snapshot can be used to propagate a complete copy or a subset of the non-Oracle data into the Oracle Database server at user-defined intervals.

## 11.8 Copying Data from the Oracle Server to the DRDA Server

The COPY command enables you to copy data from an Oracle Database server to a DRDA Server database. The Oracle SQL command INSERT is not supported. If you use the INSERT command:

```
INSERT INTO DRDA_table SELECT * FROM local_table
```

then the following message is displayed:

```
ORA-2025:All tables in the SQL statement must be at the remote database
```

To copy data from your local database to the DRDA Server, use:

```
COPY FROM user id/password@dblink-  
INSERT destination_table -  
USING query
```

For example, to select all rows from the local Oracle EMP table, to insert them into the EMP table on the DRDA Server, and to commit the transaction, use:

```
COPY FROM scott/tiger@Oracle -  
INSERT scott.EMP@DRDA -  
USING SELECT * FROM EMP
```

The SQL\*Plus COPY command supports APPEND, CREATE, INSERT, and REPLACE options. However, INSERT is the only option supported when copying to the DRDA Server. For more information about the COPY command, refer to the *SQL\*Plus User's Guide and Reference*.

## 11.9 Copying Data from the DRDA Server to the Oracle Server

The CREATE TABLE command enables you to copy data from a DRDA Server database to an Oracle Database server. To create a table on your local database and to insert rows from a DRDA Server table, use:

```
CREATE TABLE table_name
```

AS *query*

The following example creates the table `EMP` in your local Oracle database and inserts the rows from the `EMP` table on the DRDA Server:

```
CREATE TABLE EMP
AS SELECT * FROM scott.EMP@DRDA
```

Alternatively, you can use the SQL\*Plus `COPY` command to copy data from a DRDA Server to an Oracle Database server. For more information about the `COPY` command, refer to the *SQL\*Plus User's Guide and Reference*.

## 11.10 Tracing SQL Statements

SQL statements run through the gateway can be changed before reaching the DRDA database. These changes are made to make the format acceptable to the gateway or to make Oracle SQL compatible with DRDA Server SQL. The Oracle integrating server and the gateway can change the statements depending upon the situation.

For various reasons, you might need to assess whether the gateway altered the statement correctly or whether the statement could be rewritten to improve performance. SQL tracing is a feature that enables you to see the changes made to a SQL statement by the Oracle integrating server or the gateway.

SQL tracing reduces gateway performance. Use tracing only while testing and debugging the application. Do not enable SQL tracing when the application is running in a production environment. For more information about enabling SQL tracing, refer to the section on "[SQL Tracing and the Gateway](#)" on page 15-5 in [Chapter 15, "Error Messages, Diagnosis, and Reporting"](#).





---

---

## Developing Applications

The Oracle Transparent Gateway for DRDA enables applications written for the Oracle server to access tables in a DRDA database. This access can be virtually transparent by using synonyms or views of the DRDA tables accessed by a database link. However, there are fundamental SQL, data type, and semantic differences between the Oracle server and DRDA databases. Read this chapter to learn about these differences.

This chapter provides information that is specific to this release of the Oracle Transparent Gateway for DRDA, including the following sections:

- [Gateway Appearance to Application Programs](#)
- [Using Oracle Stored Procedures with the Gateway](#)
- [Using DRDA Server Stored Procedures with the Gateway](#)
- [Database Link Behavior](#)
- [Oracle Server SQL Construct Processing](#)
- [Native Semantics](#)
- [DRDA Data Type to Oracle Data Type Conversion](#)
- [Passing Native SQL Statements through the Gateway](#)
- [Oracle Data Dictionary Emulation on a DRDA Server](#)
- [Defining the Number of DRDA Cursors](#)

### 12.1 Gateway Appearance to Application Programs

An application written to access information in a DRDA database interfaces with an Oracle integrating server. When developing applications, keep the following information in mind:

- You must define the DRDA database to the application by the use of a database link defined at the Oracle integrating server. Your application specifies tables that exist on a DRDA database using the name defined in the database link. For example, assume that a database link is defined so that it names the DRDA database link DRDA, and also assume that an application needs to retrieve data from an Oracle database and from the DRDA database. Use the following SQL statement in your application:

```
SELECT EMPNO, SALARY
FROM EMP, EMPS@DRDA
WHERE
```

In this example, EMP is a table on an Oracle server, and EMP\$ is a table on a DRDA Server. You can also define a synonym or a view on the DRDA Server table, and access the information without the database link suffix.

- You can perform reads and writes of data to a defined DRDA database. SELECT, INSERT, UPDATE, and DELETE are all valid operations.
- A single transaction can write to one DRDA database and to multiple Oracle databases.
- Single SQL statements, using JOIN, can refer to tables in multiple Oracle databases or in multiple DRDA databases, or in both.

### 12.1.1 Fetch Reblocking

The gateway supports fetch reblocking with the HS\_RPC\_FETCH\_REBLOCKING parameter.

When the value of this parameter is set to ON (the default), the array size for SELECT statements is determined by the HS\_RPC\_FETCH\_SIZE value. The HS\_RPC\_FETCH\_SIZE parameter defines the number of bytes sent with each buffer from the gateway to the Oracle Database 10g server. The buffer might contain one or more qualified rows from the DRDA Server. This feature can provide significant performance enhancements, depending on your application design, installation type, and workload.

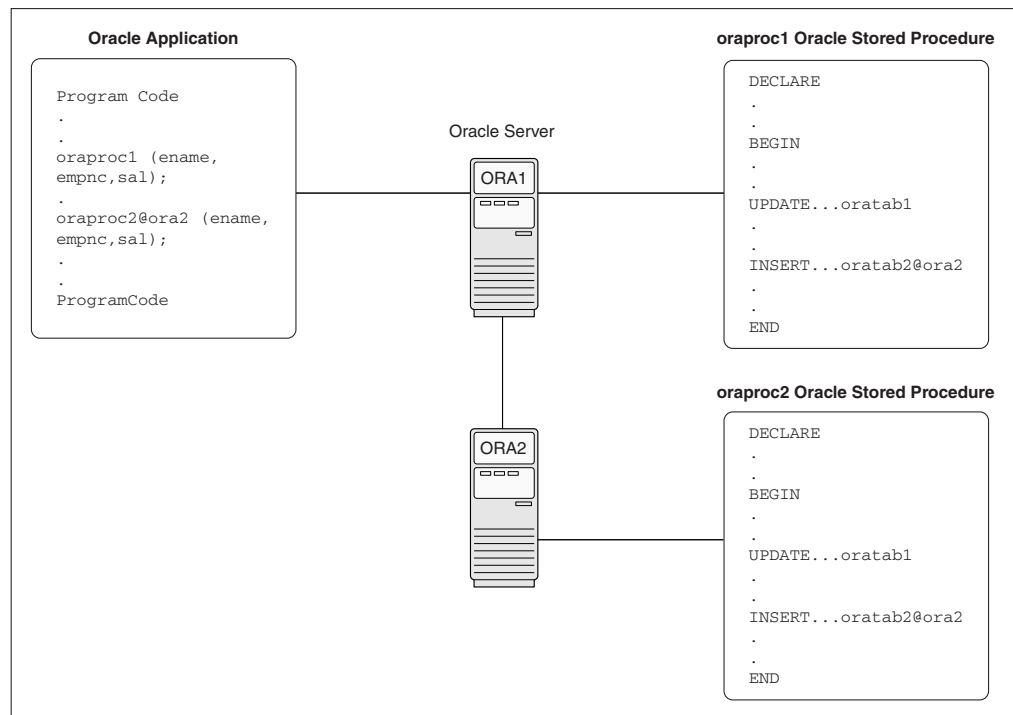
The array size between the client and the Oracle Database 10g server is still determined by the Oracle application.

Refer to [Chapter 10, "Configuring the Gateway"](#) for more information.

## 12.2 Using Oracle Stored Procedures with the Gateway

The gateway stored procedure support is an extension of Oracle stored procedures. An Oracle stored procedure is a schema object that logically groups a set of SQL and other PL/SQL programming language statements together to perform a specific task. Oracle stored procedures are stored in the database for continued use. Applications use standard Oracle PL/SQL to call stored procedures.

Oracle stored procedures can be located in a local instance of the Oracle Database 10g server and a remote instance. The following example shows two stored procedures, oraproc1 and oraproc2. While oraproc1 is a procedure stored in the ORA1 Oracle instance, oraproc2 is a procedure stored in the ORA2 Oracle instance.

**Figure 12–1 Calling Oracle Stored Procedures in a Distributed Oracle Environment**

To maintain location transparency in the application, a synonym can be created:

```
CREATE SYNONYM oraproc2 FOR oraproc2@ora2;
```

After this synonym is created, the application no longer needs to use the database link specification to call the stored procedure at the remote Oracle instance.

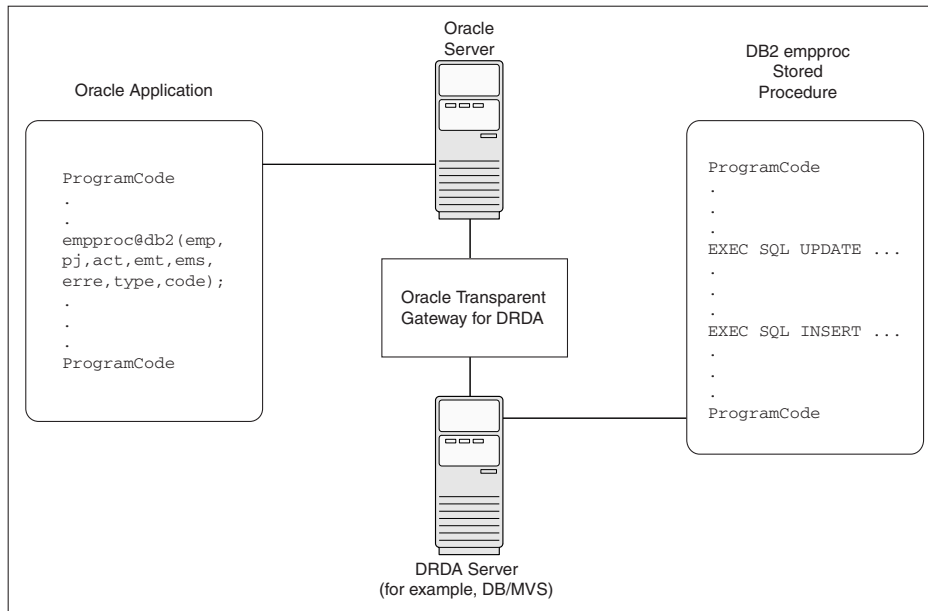
In [Figure 12–1](#), the second statement in `oraproc1` is used to access a table in the ORA2 instance. In the same way, Oracle stored procedures can be used to access DB2 tables through the gateway.

## 12.3 Using DRDA Server Stored Procedures with the Gateway

The procedural feature of the gateway enables calling of native DRDA Server stored procedures. In other words, the stored procedure is no longer defined in the Oracle Database 10g server, but instead, is defined to the DRDA Server (for example, DB2/OS390). Again, standard Oracle PL/SQL is used by the Oracle application to run the stored procedure.

The gateway does not require special definitions to call the DB2 stored procedure. Once the stored procedure is defined to the DRDA Server (e.g., DB2/OS390), the gateway will be able to use the existing DRDA Server definition to run the procedure.

In [Figure 12–2](#), an Oracle application calls the `empproc` stored procedure defined to the DRDA Server (for example, DB2/OS390).

**Figure 12–2 Running DRDA Server Stored Procedures**

From the perspective of the application, running the DB2 stored procedure is no different than calling a stored procedure at a remote Oracle instance.

### 12.3.1 Oracle Application and DRDA Server Stored Procedure Completion

As an example, suppose an Oracle application attempts to call a stored procedure in a DB2/OS390 database. In order for an Oracle application to call a DB2 stored procedure, the DB2 stored procedure must first be created on the DB2 system by using the procedures documented in the IBM reference document for DB2 for OS/390 SQL.

After the stored procedure is defined to DB2, the gateway will be able to access the data using a standard PL/SQL call. For example, an employee name, JOHN SMYTHE, is passed to the DB2 stored procedure REVISE\_SALARY. The DB2 stored procedure retrieves the salary value from the DB2 database to calculate a new yearly salary for JOHN SMYTHE. The revised salary returned in RESULT is used to update the EMP table of an Oracle database server:

```
DECLARE
  INPUT VARCHAR2(15);
  RESULT NUMBER(8,2);
BEGIN
  INPUT := 'JOHN SMYTHE';
  REVISE_SALARY@DB2(INPUT, RESULT);
  UPDATE EMP SET SAL = RESULT WHERE ENAME = INPUT;
END;
```

When the gateway receives a call to run a stored procedure on the DRDA Server (for example, DB2/OS390), it first does a lookup of the procedure name in the server catalog. The information that defines a stored procedure is stored in different forms on each DRDA Server. For example, DB2/OS390 V5.0 uses the table SYSIBM.SYSPROCEDURES, while DB2/OS390 V6.1 uses the tables SYSIBM.SYSROUTINES and SYSIBM.SYSPARMS, and DB2/400 uses the tables QSYS2.SYSPROCS and QSYS2.SYSPARMS. The gateway has a list of known catalogs to search, depending on the DRDA Server being accessed.

The search order of the catalogs is dependent on whether the catalogs support location designators (such as LUNAME in SYSIBM.SYSPROCEDURES), and Authorization or Owner IDs (such as AUTHID in SYSIBM.SYSPROCEDURES or OWNER in SYSIBM.SYSROUTINES).

Some DRDA Servers enable blank or public Authorization qualifiers. If the currently connected DRDA Server supports this form of qualification, then the gateway will apply those naming rules when searching for a procedure name in the catalog.

The matching rules will first search for a Public definition, and then an owner-qualified procedure name. For more detailed information, refer to the IBM reference document for DB2 for OS/390 SQL for the underlying database of the DRDA Server.

### 12.3.2 Procedural Feature Considerations with DB2

The following are special considerations for using the procedural feature with the gateway:

- DB2 stored procedures do not have the ability to coordinate, commit, and rollback activity on recoverable resources such as IMS or CICS transactions. Therefore, if the DB2 stored procedure calls a CICS or IMS transaction, then it is considered a separate unit of work and does not affect the completion of the stored procedure. This means that if you are running a DB2 stored procedure from an Oracle application, and if this procedure calls a CICS or IMS transaction, then the gateway cannot recover from any activity that occurred within the CICS or IMS transaction.

For example, the CICS transaction could roll back a unit of work, but this does not prevent the gateway from committing other DB2 work contained within the DB2 stored procedure.

Likewise, if the DB2 stored procedure updated an irrecoverable resource such as a VSAM file, then the gateway considers this activity separate from its own recoverable unit of work.

- PL/SQL records cannot be passed as parameters when calling a DB2 stored procedure.
- The gateway supports the SIMPLE linkage convention of DB2 stored procedures.

The SIMPLE linkage convention means that the parameters that are passed to and from the DB2 stored procedure cannot be null.

## 12.4 Database Link Behavior

A connection to the gateway is established through a database link when it is first used in an Oracle session. In this context, connection refers to both the connection between the Oracle integrating server and the gateway, and to the DRDA network connection between the gateway and the target DRDA database. The connection remains established until the Oracle session ends. Another session or user can access the same database link and get a distinct connection to the gateway and DRDA database.

Connections to the DRDA database can be limited in an APPC configuration in a parallel session limit, or by other factors, such as memory, gateway parameters, or DRDA Server resources. In a TCP/IP configuration, only resource limits (such as memory) or limits on the number of connections by the DRDA Server will limit the number of connections between the gateway and the DRDA Server.

## 12.5 Oracle Server SQL Construct Processing

One of the most important features of the Oracle Enterprise Integration Gateways family of products is their ability to provide SQL transparency to the user and to the application programmer. Foreign SQL constructs can be categorized into four areas:

- Compatible
- Translated
- Compensated
- Native semantics

### 12.5.1 Compatible SQL Functions

The Oracle integrating server automatically forwards to the DRDA database compatible SQL functions, that is, SQL constructs with the same syntax and meaning on both the Oracle server and DRDA database. These SQL constructs are forwarded unmodified. All of the compatible functions are column functions. Functions that are not compatible are either translated to an equivalent DRDA SQL function or are compensated by the Oracle server after the data is returned from the DRDA database.

### 12.5.2 Translated SQL Functions

Translated functions have the same meaning but different names between the Oracle integrating server and the DRDA database, but all applications must use the Oracle function name. These SQL constructs that are supported with different syntax (such as different function names) by the DRDA database, are automatically translated by the Oracle server and then forwarded to the DRDA database. The Oracle integrating server, transparent to your application, changes the function name before sending it to the DRDA database.

### 12.5.3 Compensated SQL Functions

Some advanced SQL constructs that are supported by the Oracle server may not be supported in the same manner, if at all, by the DRDA database. Compensated functions are those SQL functions that are not recognized by the DRDA Server. If a `SELECT` statement containing one of these functions is passed from the Oracle integrating server to the gateway, then the gateway removes the function before passing the SQL statement to the DRDA Server. The gateway passes the selected DRDA database rows to the Oracle integrating server. The Oracle integrating server then applies the function.

The Oracle server can compensate for the missing or incompatible function by automatically excluding the incompatible SQL construct from the SQL request that is forwarded to the DRDA database. The Oracle server then retrieves the necessary data from the DRDA database and applies the function. This activity is known as postprocessing.

The gateway attempts to pass all SQL functions to DRDA databases. But when a DRDA database does not support a function represented in the computation, then the gateway changes that function. For example, if a program requests:

```
SELECT COS (X_COOR) FROM TABLE_X;
```

from a DB2/OS390 database, which does not support the meaning of `COS`, then the gateway changes the `SELECT` statement to:

```
SELECT X_COOR FROM TABLE_X;
```

All data in the X\_COOR column of TABLE\_X is passed from the DB2/OS390 database to the Oracle integrating server. After the data is moved to the Oracle integrating server, the COS function is performed.

If you are performing operations on large amounts of data stored in a DRDA database, then keep in mind that some functions require postprocessing.

## 12.5.4 Native Semantic SQL Functions

Some SQL functions that are normally compensated may also be overridden, through the Native Semantics facility. If a SQL function has been enabled for Native Semantics, then the function may be passed on to the DRDA database for processing, instead of being compensated (post-processed). Refer to [Native Semantics](#) on page 12-18.

## 12.5.5 DB2/OS390 SQL Compatibility

The ways that the Oracle Database server and gateway handle SQL functions for a DB2/OS390 database are shown in [Table 12-1](#).

**Table 12-1 DB2/OS390 SQL Compatibility, by Oracle SQL Function**

Oracle SQL Function	Compatible	Translated	Compensated	Native Semantics Candidate
ABS			Yes	Yes
ACOS			Yes	Yes
ADD_MONTHS			Yes	
ASCII			Yes	Yes
ASIN			Yes	Yes
ATAN			Yes	Yes
ATAN2			Yes	Yes
AVG	Yes			
BITAND			Yes	Yes
CAST			Yes	Yes
CEIL		CEILING		Yes
CHARTOROWID			Yes	
CHR			Yes	Yes
CONCAT	Yes			
CONVERT			Yes	Yes
COS			Yes	Yes
COSH			Yes	Yes
COUNT(*)	Yes			
COUNT (DISTINCT colname)	Yes			
COUNT (ALL colname)	Yes			COUNTCOL

**Table 12–1 (Cont.) DB2/OS390 SQL Compatibility, by Oracle SQL Function**

<b>Oracle SQL Function</b>	<b>Compatible</b>	<b>Translated</b>	<b>Compensated</b>	<b>Native Semantics Candidate</b>
COUNT (column)	Yes			COUNTCOL
DECODE			Yes	Yes
DUMP			Yes	Yes
EXP			Yes	Yes
FLOOR	Yes			Yes
GREATEST			Yes	Yes
HEXTORAW			Yes	Yes
INITCAP			Yes	Yes
INSTR			Yes	Yes
INSTRB			Yes	Yes
LAST_DAY			Yes	
LEAST			Yes	Yes
LENGTH			Yes	Yes
LENGTHB			Yes	Yes
LN			Yes	Yes
LOG			Yes	Yes
LOWER			Yes	Yes
LPAD			Yes	Yes
LTRIM			Yes	Yes
MAX	Yes			
MIN	Yes			
MOD			Yes	Yes
MONTHS_BETWEEN			Yes	
NEW_TIME			Yes	
NEXT_DAY			Yes	
NLS_INITCAP			Yes	Yes
NLS_LOWER			Yes	Yes
NLS_UPPER			Yes	Yes
NLSSORT			Yes	Yes
NVL		VALUE		
NVL2			Yes	Yes
POWER			Yes	Yes
RAWTOHEX			Yes	Yes
REPLACE			Yes	Yes



**Table 12–1 (Cont.) DB2/OS390 SQL Compatibility, by Oracle SQL Function**

Oracle SQL Function	Compatible	Translated	Compensated	Native Semantics Candidate
REVERSE			Yes	Yes
ROUND			Yes	Yes
ROWIDTOCHAR			Yes	
RPAD			Yes	Yes
RTRIM			Yes	Yes
SIGN			Yes	Yes
SIN			Yes	Yes
SINH			Yes	Yes
SOUNDEX			Yes	
SQRT			Yes	Yes
STDDEV			Yes	Yes
SUBSTR			Yes	Yes
SUBSTRB			Yes	Yes
SUM	Yes			
SYSDATE			Yes	
TAN			Yes	Yes
TANH			Yes	Yes
TO_CHAR			Yes	
TO_DATE			Yes	
TO_MULTI_BYTE			Yes	
TO_NUMBER		DECIMAL		Yes
TO_SINGLE_BYTE			Yes	
TRANSLATE			Yes	Yes
TRIM		STRIP	Yes	Yes
TRUNC			Yes	Yes
UID			Yes	
UPPER			Yes	Yes
USER			Yes	
USERENV			Yes	
VARIANCE			Yes	Yes
VSIZE			Yes	Yes

## 12.5.6 DB2/Universal Database SQL Compatibility

The ways that the Oracle Database server and gateway handle SQL functions for a DB2/UDB database are shown in the following table:

**Table 12–2 DB2/Universal Database SQL Compatibility, by Oracle SQL Function**

Oracle SQL Function	Compatible	Translated	Compensated	Native Semantics Candidate
ABS	Yes			Yes
ACOS			Yes	Yes
ADD_MONTHS			Yes	
ASCII			Yes	Yes
ASIN			Yes	Yes
ATAN			Yes	Yes
ATAN2			Yes	Yes
AVG	Yes			
BITAND			Yes	Yes
CAST			Yes	Yes
CEIL		CEILING		Yes
CHARTOROWID			Yes	
CHR	Yes			Yes
CONCAT	Yes			
CONVERT			Yes	Yes
COS	Yes			Yes
COSH			Yes	Yes
COUNT ( * )	Yes			
COUNT (DISTINCT colname)	Yes			
COUNT (ALL colname)	Yes			COUNTCOL
COUNT (column)	Yes			COUNTCOL
DECODE			Yes	Yes
DUMP			Yes	Yes
EXP	Yes			Yes
FLOOR	Yes			Yes
GREATEST			Yes	Yes
HEXTORAW			Yes	Yes
INITCAP			Yes	Yes
INSTR			Yes	Yes
INSTRB			Yes	Yes
LAST_DAY			Yes	
LEAST			Yes	Yes

**Table 12–2 (Cont.) DB2/Universal Database SQL Compatibility, by Oracle SQL Function**

<b>Oracle SQL Function</b>	<b>Compatible</b>	<b>Translated</b>	<b>Compensated</b>	<b>Native Semantics Candidate</b>
LENGTH			Yes	Yes
LENGTHB			Yes	Yes
LN	Yes			Yes
LOG			Yes	Yes
LOWER		LCASE		Yes
LPAD			Yes	Yes
LTRIM			Yes	Yes
MAX	Yes			
MIN	Yes			
MOD	Yes			Yes
MONTHS_BETWEEN			Yes	
NEW_TIME			Yes	
NEXT_DAY	Yes		Yes	
NLS_INITCAP			Yes	Yes
NLS_LOWER			Yes	Yes
NLS_UPPER			Yes	Yes
NLSSORT			Yes	Yes
NVL		VALUE		
NVL2			Yes	Yes
POWER	Yes			Yes
RAWTOHEX			Yes	Yes
REPLACE	Yes			Yes
REVERSE			Yes	Yes
ROUND	Yes			Yes
ROWIDTOCHAR			Yes	
RPAD			Yes	Yes
RTRIM			Yes	Yes
SIGN	Yes			Yes
SIN	Yes			Yes
SINH			Yes	Yes
SOUNDEX			Yes	
SQRT	Yes			Yes
STDDEV			Yes	Yes
SUBSTR			Yes	Yes

**Table 12–2 (Cont.) DB2/Universal Database SQL Compatibility, by Oracle SQL Function**

Oracle SQL Function	Compatible	Translated	Compensated	Native Semantics Candidate
SUBSTRB			Yes	Yes
SUM	Yes			
SYSDATE			Yes	
TAN	Yes			Yes
TANH			Yes	Yes
TO_CHAR			Yes	
TO_DATE			Yes	
TO_MULTI_BYTE			Yes	
TO_NUMBER		DECIMAL		Yes
TO_SINGLE_BYTE			Yes	
TRANSLATE			Yes	Yes
TRIM			Yes	Yes
TRUNC	Yes			Yes
UID			Yes	
UPPER		UCASE		Yes
USER			Yes	
USERENV			Yes	
VARIANCE			Yes	Yes
VSIZE			Yes	Yes

### 12.5.7 DB2/400 SQL Compatibility

The ways that the Oracle Database server and gateway handle SQL functions for a DB2/400 database are shown in the following table:

**Table 12–3 DB2/400 SQL Compatibility, by Oracle SQL Function**

Oracle SQL Function	Compatible	Translated	Compensated	Native Semantics Candidate
ABS		ABSVAL		Yes
ACOS			Yes	Yes
ADD_MONTHS			Yes	
ASCII			Yes	Yes
ASIN			Yes	Yes
ATAN			Yes	Yes
ATAN2			Yes	Yes
AVG	Yes			

**Table 12-3 (Cont.) DB2/400 SQL Compatibility, by Oracle SQL Function**

<b>Oracle SQL Function</b>	<b>Compatible</b>	<b>Translated</b>	<b>Compensated</b>	<b>Native Semantics Candidate</b>
BITAND			Yes	Yes
CAST			Yes	Yes
CEIL		CEILING		Yes
CHARTOROWID			Yes	
CHR			Yes	Yes
CONCAT	Yes			
CONVERT			Yes	Yes
COS	Yes			Yes
COSH	Yes			Yes
COUNT (*)	Yes			
COUNT (DISTINCT colname)	Yes			
COUNT (ALL colname)	Yes			COUNTCOL
COUNT (column)	Yes			COUNTCOL
DECODE			Yes	Yes
DUMP			Yes	Yes
EXP	Yes			Yes
FLOOR	Yes			Yes
GREATEST			Yes	Yes
HEXTORAW			Yes	Yes
INITCAP			Yes	Yes
INSTR			Yes	Yes
INSTRB			Yes	Yes
LAST_DAY			Yes	
LEAST			Yes	Yes
LENGTH			Yes	Yes
LENGTHB			Yes	Yes
LN	Yes			Yes
LOG			Yes	Yes
LOWER			Yes	Yes
LPAD			Yes	Yes
LTRIM			Yes	Yes
MAX	Yes			

**Table 12-3 (Cont.) DB2/400 SQL Compatibility, by Oracle SQL Function**

<b>Oracle SQL Function</b>	<b>Compatible</b>	<b>Translated</b>	<b>Compensated</b>	<b>Native Semantics Candidate</b>
MIN	Yes			
MOD			Yes	Yes
MONTHS_BETWEEN			Yes	
NEW_TIME			Yes	
NEXT_DAX			Yes	
NLS_INITCAP			Yes	Yes
NLS_LOWER			Yes	Yes
NLS_UPPER			Yes	Yes
NLSSORT			Yes	Yes
NVL		VALUE		
NVL2			Yes	Yes
POWER			Yes	Yes
RAWTOHEX			Yes	Yes
REPLACE			Yes	Yes
REVERSE			Yes	Yes
ROUND			Yes	Yes
ROWIDTOCHAR			Yes	
RPAD			Yes	Yes
RTRIM			Yes	Yes
SIGN			Yes	Yes
SIN	Yes			Yes
SINH	Yes			Yes
SOUNDEX			Yes	
SQRT	Yes			Yes
STDDEV	Yes			Yes
SUBSTR			Yes	Yes
SUBSTRB			Yes	Yes
SUM	Yes			
SYSDATE			Yes	
TAN	Yes			Yes
TANH	Yes			Yes
TO_CHAR			Yes	
TO_DATE			Yes	
TO_MULTI_BYTE			Yes	

**Table 12–3 (Cont.) DB2/400 SQL Compatibility, by Oracle SQL Function**

Oracle SQL Function	Compatible	Translated	Compensated	Native Semantics Candidate
TO_NUMBER		DECIMAL		Yes
TO_SINGLE_BYTE			Yes	
TRANSLATE			Yes	Yes
TRIM			Yes	Yes
TRUNC			Yes	Yes
UID			Yes	
UPPER		TRANSLATE		Yes
USER			Yes	
USERENV			Yes	
VARIANCE		VAR		Yes
VSIZE			Yes	Yes

## 12.5.8 DB2/VM SQL Compatibility

The ways that the Oracle Database server and gateway handle SQL functions for a DB2/VM database are shown in the following table:

**Table 12–4 DB2/VM SQL Compatibility, by Oracle SQL Function**

Oracle SQL Function	Compatible	Translated	Compensated	Native Semantics Candidate
ABS			Yes	Yes
ACOS			Yes	Yes
ADD_MONTHS			Yes	
ASCII			Yes	Yes
ASIN			Yes	Yes
ATAN			Yes	Yes
ATAN2			Yes	Yes
AVG	Yes			
BITAND			Yes	Yes
CAST			Yes	Yes
CEIL				Yes
CHARTOROWID			Yes	
CHR			Yes	Yes
CONCAT	Yes			
CONVERT			Yes	Yes
COS			Yes	Yes

**Table 12–4 (Cont.) DB2/VM SQL Compatibility, by Oracle SQL Function**

<b>Oracle SQL Function</b>	<b>Compatible</b>	<b>Translated</b>	<b>Compensated</b>	<b>Native Semantics Candidate</b>
COSH			Yes	Yes
COUNT (*)	Yes			
COUNT (DISTINCT colname)	Yes			
COUNT (ALL colname)			Yes	
COUNT (COLUMN)			Yes	
DECODE			Yes	Yes
DUMP			Yes	Yes
EXP			Yes	Yes
FLOOR				Yes
GREATEST			Yes	Yes
HEXTORAW			Yes	Yes
INITCAP			Yes	Yes
INSTR			Yes	Yes
INSTRB			Yes	Yes
LAST_DAY			Yes	
LEAST			Yes	Yes
LENGTH			Yes	Yes
LENGTHB			Yes	Yes
LN			Yes	Yes
LOG			Yes	Yes
LOWER			Yes	Yes
LPAD			Yes	Yes
LTRIM			Yes	Yes
MAX	Yes			
MIN	Yes			
MOD			Yes	Yes
MONTHS_BETWEEN			Yes	
NEW_TIME			Yes	
NEXT_DAY			Yes	
NLS_INITCAP			Yes	Yes
NLS_LOWER			Yes	Yes
NLS_UPPER			Yes	Yes



**Table 12–4 (Cont.) DB2/VM SQL Compatibility, by Oracle SQL Function**

Oracle SQL Function	Compatible	Translated	Compensated	Native Semantics Candidate
NLSSORT			Yes	Yes
NVL		VALUE		
NVL2			Yes	Yes
POWER			Yes	Yes
RAWTOHEX			Yes	Yes
REPLACE			Yes	Yes
REVERSE			Yes	Yes
ROUND			Yes	Yes
ROWIDTOCHAR			Yes	
RPAD			Yes	Yes
RTRIM			Yes	Yes
SIGN			Yes	Yes
SIN			Yes	Yes
SINH			Yes	Yes
SOUNDEX			Yes	
SQRT			Yes	Yes
STDDEV			Yes	Yes
SUBSTR			Yes	Yes
SUBSTRB			Yes	Yes
SUM	Yes			
SYSDATE			Yes	
TAN			Yes	Yes
TANH			Yes	Yes
TO_CHAR			Yes	
TO_DATE			Yes	
TO_MULTI_BYTE			Yes	
TO_NUMBER			Yes	Yes
TO_SINGLE_BYTE			Yes	
TRANSLATE			Yes	Yes
TRIM			Yes	Yes
TRUNC			Yes	Yes
UID			Yes	
UPPER			Yes	Yes
USER			Yes	

**Table 12–4 (Cont.) DB2/VM SQL Compatibility, by Oracle SQL Function**

Oracle SQL Function	Compatible	Translated	Compensated	Native Semantics Candidate
USERENV			Yes	
VARIANCE			Yes	Yes
VSIZE			Yes	Yes

## 12.6 Native Semantics

Because some of the advanced SQL constructs that are supported by the Oracle server may not be supported in the same manner (if at all) by the DRDA database, the Oracle server compensates for the missing or incompatible functionality by postprocessing the DRDA database data with Oracle (refer to the previous section, "[Oracle Server SQL Construct Processing](#)", on page 12-6). This feature provides maximum transparency, but may impact performance. In addition, new versions of a particular DRDA database may implement previously unsupported functions or capabilities, or they may change the supported semantics in such a manner as to make them more compatible with Oracle functions.

Some of the DRDA Servers also provide support for user-defined functions. The user may choose to implement Oracle functions natively, thus enabling the DRDA Server to pass the function on to the underlying database implementation (for example, DB2). Native Semantics provides a method of enabling specific capabilities to be processed natively by the DRDA Server.

Various considerations must be taken into account when enabling the Native Semantic feature of a particular function, because Native Semantics has advantages and disadvantages. For example, a trade-off typically exists between transparency and performance. One such consideration is transparency of data coercion. Oracle provides coercion (implicit data conversion) for many SQL functions. This means that if the supplied value for a particular function is not correct, then Oracle will coerce the value to the correct type before processing it. However, with the Native Semantic feature enabled, the value (exactly as provided) will be passed through to the DRDA Server for processing. In many cases, the DRDA Server will not be able to coerce the value to the correct type and will therefore generate an error.

Another consideration involves the compatibility of parameters to a particular SQL function. For instance, the Oracle implementation of SUBSTR permits negative values for the string index, whereas most DRDA Server implementations of SUBSTR do not permit negative values for the string index. However, if the application is implemented to call SUBSTR in a manner that is compatible with the DRDA Server, then the function will act the same in either Oracle or the DRDA Server.

Another consideration is that the processing of a function at the DRDA Server may not be desirable due to resource constraints in that environment. Refer to the [DRDA\\_CAPABILITY](#) parameter on page C-2 of [Appendix C](#) for details on enabling or disabling these capabilities. Refer as well, to the *SQL\*Plus User's Guide and Reference* and *Oracle Database PL/SQL User's Guide and Reference* for the Oracle format of the following capabilities:

### 12.6.1 SQL Functions That Can Be Enabled

The following list contains SQL functions that are not enabled by default. They can be enabled as an option:

**Table 12–5 List of SQL Functions That Can Be Enabled**

Functions			
ABS	ACOS	ASCII	ASIN
ATAN	ATAN2	BITAND	CAST
CEIL	CHR	CONVERT	COS
COSH	COUNTCOL	DECODE	DUMP
EXP	FLOOR	GREATEST	HEXOTRAW
INITCAP	INSTR	INSTRB	LEAST
LENGTH	LENGTHB	LN	LOG
LOWER	LPAD	LTRIM	MOD
NLS_INITCAP	NLS_UPPER	NLS_LOWER	NLSSORT
NVL2	POWER	RAWTOHEX	REPLACE
REVERSE	ROUND	RPAD	RTRIM
SIGN	SIN	SINH	SQRT
STDDEV	SUBSTR	SUBSTRB	TAN
TANH	TO_NUMBER	TRANSLATE	TRIM
TRUNC	UPPER	VARIANCE	VSIZE

## 12.6.2 SQL Functions That Can Be Disabled

The following SQL functions are enabled (ON) by default. They can be disabled as an option:

- COUNTCOL, to control SQL COUNT (column) function
- GROUPBY, to control SQL GROUP BY clause
- HAVING, to control SQL HAVING clause
- ORDERBY, to control SQL ORDER BY clause
- WHERE, to control SQL WHERE clause

ORDERBY controls sort order, which may differ at various sort locations. For example, with ORDERBY ON, a DB2 sort would be based on EBCDIC sorting order, whereas with ORDERBY OFF, an Oracle sort would be based on ASCII sorting order.

Three other functions, GROUPBY, HAVING, and WHERE, can take additional processing time. If you need to minimize the use of expensive resources, then you should choose the settings of these functions so that the processing is performed on the cheaper resource.

## 12.6.3 SQL Set Operators and Clauses

The clauses WHERE and HAVING are compatible for all versions of the DRDA Server, meaning that they are passed unchanged to the DRDA Server for processing. Whether clauses GROUP BY and ORDER BY are passed to the DRDA Server or compensated by the Oracle server is determined by the Native Semantics parameters (refer to the previous section).

The set operators UNION and UNION ALL are compatible for all versions of the DRDA Server, meaning that they are passed unchanged to the DRDA Server for processing.

The set operators `INTERSECT` and `MINUS` are compensated on all versions of the DRDA Server except DB2/UDB. For DB2/UDB, `INTERSECT` is compatible, and `MINUS` is translated to `EXCEPT`.

## 12.7 DRDA Data Type to Oracle Data Type Conversion

To move data between applications and the database, the gateway binds data values from a host variable or literal of a specific data type to a data type interpretable by the database. Therefore, the gateway maps values from any version of the DRDA Server into correct Oracle data types before passing these values back to the application or Oracle tool.

The table lists the data type mapping and restrictions. The DRDA Server data types listed below are general. Refer to documentation for your DRDA database for restrictions on data type size and value limitations.

**Table 12–6 Data Type Mapping and Restrictions**

DRDA Server	Oracle External	Criteria
CHAR(N)	CHAR(N)	N ≤ 255
VARCHAR (N)	VARCHAR2(N) LONG	N ≤ 2000 2000 < N ≤ 32740
LONG VARCHAR(N)	VARCHAR2(N)	N ≤ 2000
LONG VARCHAR(N)	LONG	2000 < N ≤ 32740
CHAR(N) FOR BIT DATA	RAW(N)	N ≤ 255
VARCHAR(N) FOR BIT DATA	RAW(N)	1 ≤ N ≤ 255
VARCHAR(N) FOR BIT DATA	LONG RAW(N)	255 < N ≤ 32740
LONG VARCHAR(N) FOR BIT DATA	RAW(N)	1 ≤ N ≤ 255
LONG VARCHAR(N) FOR BIT DATA	LONG RAW(N)	255 < N ≤ 32740
DATE	DATE	Refer to <a href="#">"Performing Date and Time Operations"</a> on page 12-22
TIME	CHAR(8)	Refer to <a href="#">"Performing Date and Time Operations"</a> on page 12-22
TIMESTAMP	CHAR(26)	Refer to <a href="#">"Performing Date and Time Operations"</a> on page 12-22
GRAPHIC	CHAR(2N)	N ≤ 127
VARGRAPHIC	VARCHAR2(2N) LONG	N ≤ 1000 1000 ≤ N ≤ 16370
LONG VARGRAPHIC	VARCHAR2(2N) LONG	N ≤ 1000 1000 ≤ N ≤ 16370
Floating Point Single	FLOAT(21)	n/a
Floating Point Double	FLOAT(53)	n/a

**Table 12–6 (Cont.) Data Type Mapping and Restrictions**

DRDA Server	Oracle External	Criteria
Decimal (P,S)	NUMBER(P,S)	n/a

### 12.7.1 Performing Character String Operations

The gateway performs all character string comparisons, concatenations, and sorts using the data type of the referenced columns, and determines the validity of character string values passed by applications using the gateway. The gateway automatically converts character strings from one data type to another and converts between character strings and dates when needed.

Frequently, DRDA databases are designed to hold noncharacter binary data in character columns. Applications run on DRDA systems can generally store and retrieve data as though it contained character data. However, when an application accessing this data runs in an environment that uses a different character set, inaccurate data might be returned.

With the gateway running on the host, character data retrieved from a DB2/400, DB2/OS390, or DB2/VM host is translated from EBCDIC to ASCII. When character data is sent to DB2/400, DB2/OS390, or DB2/VM from the host, ASCII data is translated to EBCDIC. When the characters are binary data in a character column, this translation causes the application to receive incorrect information or errors. To resolve these errors, character columns on DB2/400, DB2/OS390, or DB2/VM that hold noncharacter data must be created with the FOR BIT DATA option. In the application, the character columns holding noncharacter data should be processed using the Oracle data types RAW and LONG RAW. The DESCRIBE information for a character column defined with FOR BIT DATA on the host always indicates RAW or LONG RAW.

### 12.7.2 Converting Character String data types

The gateway binds character string data values from host variables as fixed-length character strings. The bind length is the length of the character string data value. The gateway performs this conversion on every bind.

The DRDA VARCHAR data type can be from 1 to 32740 bytes in length. This data type is converted to an Oracle VARCHAR2 data type if it is between 1 and 2000 characters in length. If it is between 2000 and 32740 characters in length, then it is converted to an Oracle LONG data type.

The DRDA VARCHAR data type can be no longer than 32740 bytes, which is much shorter than the maximum size for the Oracle LONG data type. If you define an Oracle LONG data type larger than 32740 bytes in length, then you will receive an error message when it is mapped to the DRDA VARCHAR data type.

### 12.7.3 Performing Graphic String Operations

DB2 GRAPHIC data types store only double-byte string data. Sizes for DB2 GRAPHIC data types typically have maximum sizes which are half that of their character counterparts. For example, the maximum size of a CHAR data type may be 255 characters, whereas the maximum size of a GRAPHIC data type may be 127 characters.

Oracle does not have a direct matching data type, and the gateway therefore converts between Oracle character data types and DB2 Graphic data types. Oracle character data types may contain single, mixed, or double-byte character data. The gateway converts the string data into suitable double-byte-only format depending upon

whether the target DB2 column is a graphic type and whether gateway initialization parameters are set to perform this conversion. For more configuration information, refer to [Appendix C, "DRDA-Specific Parameters"](#) and [Appendix D, "National Language Support"](#).

## 12.7.4 Performing Date and Time Operations

The implementation of date and time data differs significantly in IBM DRDA databases and in the Oracle server. The Oracle server has a single date data type, DATE, that can contain both calendar date and time of day information.

IBM DRDA databases support the following three distinct date and time data types:

- DATE is the calendar date only.
- TIME is the time of day only.
- TIMESTAMP is a numerical value combining calendar data and time of day.

### 12.7.4.1 Processing TIME and TIMESTAMP Data

There is no built-in mechanism that translates the IBM TIME and TIMESTAMP data to Oracle DATE data. An application must process TIME data types to the Oracle CHAR format with a length of eight bytes. An application must process the TIMESTAMP data type in the Oracle CHAR format with a length of 26 bytes.

An application reads TIME and TIMESTAMP functions as character strings and converts or subsets portions of the string to perform numerical operations. TIME and TIMESTAMP values can be sent to an IBM DRDA database as character literals or bind variables of the correct length and format.

### 12.7.4.2 Processing DATE Data

Oracle and IBM DATE data types are mapped to each other. If an IBM DATE is queried, then it is converted to an Oracle DATE with a zero (midnight) time of day. If an Oracle DATE is processed against an IBM DATE column, then the date value is converted to the IBM DATE format, and any time value is discarded.

Character representations of dates are different in Oracle format and IBM DRDA format. When an Oracle application SQL statement contains a date literal, or conveys a date using a character bind variable, the gateway must convert the date to an IBM DRDA-compatible format.

The gateway does not automatically recognize when a character value is going to be processed against an IBM DATE column. Applications are required to distinguish character date values by enclosing them with the Oracle TO\_DATE function notation.

For example, if EMP is a synonym or view that accesses data on an IBM DRDA database, then instead of this SQL statement:

```
SELECT * FROM EMP WHERE HIREDATE = '03-MAR-81'
```

you must use:

```
SELECT * FROM EMP WHERE HIREDATE = TO_DATE('03-MAR-81')
```

In a programmatic interface program that uses a character bind variable for the qualifying date value, you must use this SQL statement:

```
SELECT * FROM EMP WHERE HIREDATE = TO_DATE(:1)
```

The above SQL notation does not affect SQL statement semantics when the statement is run against an Oracle table. The statement remains portable across Oracle and IBM DRDA-accessed data stores.

The TO\_DATE function is not required for dates in any of the following formats:

- YYYY-MM-DD (ISO/JIS)
- DD.MM.YYYY (European)
- MM/DD/YYYY (USA)

For example:

```
SELECT * FROM EMP WHERE HIREDATE = '1981-03-03'
```

The TO\_DATE requirement also does not pertain to input bind variables that are in Oracle date 7-byte binary format. The gateway recognizes such values as dates.

### 12.7.4.3 Performing Date Arithmetic

The following forms of SQL expression generally do not work correctly with the gateway:

*date + number*

*number + date*

*date - number*

*date1 - date2*

The date and number addition and subtraction (*date + number*, *number + date*, *date - number*) forms are sent to the DRDA Server, where they are rejected. The supported servers do not permit number addition or subtraction with dates.

Because of differing interpretations of date subtraction in the supported servers, subtracting two dates (*date1 - date2*) gives results that vary by server.

---



---

**Note:** Avoid date arithmetic expressions in all gateway SQL until date arithmetic problems are resolved.

---



---

## 12.7.5 Dates

Date handling has two categories, two-digit year dates, which are treated as occurring 50 years before or 50 years after the year 2000, and four-digit year dates, which are not ambiguous with regard to the year 2000. Oracle recommends that you set the Oracle Database 10g server and gateway default HS\_NLS\_DATE\_FORMAT parameter to a format including a four-digit year.

Use one of the following methods to enter twenty-first century dates:

- The TO\_DATE function

Use any date format including a four character year field. Refer to the *Oracle Database SQL Reference* for the available date format string options.

For example, TO\_DATE('2008-07-23', 'YYYY-MM-DD') can be used in any SELECT, INSERT, UPDATE, or DELETE statement.

- The HS\_NLS\_DATE\_FORMAT parameter

The `HS_NLS_DATE_FORMAT` parameter defines a default format for the Oracle database server explicit `TO_DATE` functions without a pattern and for implicit string to date conversions.

For example, with `HS_NLS_DATE_FORMAT` defined as `'YYYY-MM-DD'`, `'2008-07-23'` can be used in any `SELECT`, `INSERT`, `UPDATE`, or `DELETE` statement.

## 12.7.6 HS\_NLS\_DATE\_FORMAT Support

The following patterns can be used for the `HS_NLS_DATE_FORMAT`:

**Table 12-7 HS\_NLS\_DATE\_FORMAT Patterns**

DB2 Date Format	Pattern	Example
EUR	DD.MM.YYYY	30.10.1994
ISO	YYYY-MM-DD	1994-10-30
JIS	YYYY-MM-DD	1994-10-30
USA	MM/DD/YYYY	10/30/1994

The Oracle default format of `'DD-MON-YY'` is not permitted with DB2. As a result, the gateway local date exit is provided to change the Oracle default date format of `'DD-MON-YY'` or `'DD-MON-RR'` to the DB2 ISO format of `'YYYY-MM-DD'` before passing the date to DB2.

The following example demonstrates the most efficient way to enter and select date values in the twenty-first century:

```
ALTER SESSION SET HS_NLS_DATE_FORMAT = 'YYYY-MM-DD';
INSERT INTO EMP (HIREDATE) VALUES ('2008-07-23');
SELECT * FROM EMP WHERE HIREDATE = '2008-07-23';
UPDATE EMP SET HIREDATE = '2008-07-24'
  WHERE HIREDATE = '2008-07-23';
DELETE FROM EMP WHERE HIREDATE = '2008-07-24';
```

## 12.7.7 Oracle TO\_DATE Function

The Oracle `TO_DATE` function is preprocessed in SQL `INSERT`, `UPDATE`, `DELETE`, and `SELECT WHERE` clauses. `TO_DATE` functions in `SELECT` result lists are not preprocessed.

The `TO_DATE` function is often needed to provide values to update or compare with date columns. Therefore, the gateway replaces the information included in the `TO_DATE` clause with an acceptable value before the SQL statement is sent to DB2.

Except for the `SELECT` result list, all `TO_DATE` functions are preprocessed and turned into values that are the result of the `TO_DATE` function. Only `TO_DATE(literal)` or `TO_DATE(:bind_variable)` is permitted. Except in `SELECT` result lists, the `TO_DATE(column_name)` function format is not supported.

The preprocessing of the Oracle `TO_DATE` functions into simple values is useful in an `INSERT VALUES` clause because DB2 does not permit functions in the `VALUES` clause. In this case, DB2 receives a simple value in the `VALUES` list. All forms of the `TO_DATE` function (with one, two, or three operands) are supported.



## 12.7.8 Performing Numeric Data Type Operations

IBM versions of the DRDA Server perform automatic conversions to the numeric data type of the destination column (such as integer, double-precision floating point, or decimal). The user has no control over the data type conversion, and this conversion can be independent of the data type of the destination column in the database.

For example, if PRICE is an integer column of the PRODUCT table in an IBM DRDA database, then the update shown in the following example inaccurately sets the price of an ice cream cone to \$1.00 because the IBM DRDA Server automatically converts a floating point to an integer:

```
UPDATE PRODUCT
SET PRICE = 1.50
WHERE PRODUCT_NAME = 'ICE CREAM CONE  ';
```

Because PRICE is an integer, the IBM DRDA Server automatically converts the decimal data value of 1.50 to 1.

## 12.7.9 Mapping the COUNT Function

The Oracle Database server supports the following four operands for the COUNT function:

- COUNT (\*)
- COUNT(DISTINCT colname)
- COUNT(ALL colname)
- COUNT(colname)

Some DRDA servers do not support all forms of COUNT, specifically COUNT(colname) and COUNT(ALL colname). In those cases, the COUNT function and its arguments are translated into COUNT(\*). This may not yield the desired results, especially if the column being counted contains NULL values.

For those DRDA servers that do not support the above forms, it may be possible to achieve equivalent functionality by adding a WHERE clause.

```
SELECT COUNT(colname) FROM table@dblink WHERE colname IS NOT NULL
or
```

```
SELECT COUNT(ALL colname) FROM table@dblink WHERE colname IS NOT NULL
```

Refer to [Chapter 2.5.2, "SQL Limitations"](#) for known DRDA servers which do not support all forms of COUNT.

## 12.7.10 Performing Zoned Decimal Operations

A zoned decimal field is described as packed decimal on an Oracle server. However, an Oracle application such as a Pro\*C program can insert into a zoned decimal column using any supported Oracle numeric data type. The gateway converts this number into the most suitable data type. Data can be fetched from a DRDA database into any Oracle data type, provided that it does not result in loss of information.

## 12.8 Passing Native SQL Statements through the Gateway

The passthrough SQL feature enables an application developer to send a SQL statement directly to the DRDA Server without the statement being interpreted by the Oracle database server. DBMS\_HS\_PASSTHROUGH.EXECUTE\_IMMEDIATE SQL passthrough statements that are supported by the gateway are limited to nonqueries

(INSERT, UPDATE, DELETE, and DDL statements) and cannot contain bind variables. The gateway can run native SQL statements using `DBMS_HS_PASSTHROUGH.EXECUTE_IMMEDIATE`.

`DBMS_HS_PASSTHROUGH.EXECUTE_IMMEDIATE` is a built-in gateway function. This function receives one input argument and returns the number of rows affected by the SQL statement. For DDL statements, the function returns zero.

`DBMS_HS_PASSTHROUGH.EXECUTE_IMMEDIATE` is a reserved name of the gateway and is used specifically for running native SQL.

This release of Oracle Transparent Gateway for DRDA enables retrieval of result sets from queries run with passthrough. The syntax is different from the `DBMS_HS_PASSTHROUGH.EXECUTE_IMMEDIATE` function. Refer to ["Retrieving Result Sets Through Passthrough"](#) on page 12-27 for more information.

### 12.8.1 Processing DDL Statements through Passthrough

As noted above, SQL statements which are processed through the `DBMS_HS_PASSTHROUGH.EXECUTE_IMMEDIATE` function are not interpreted by the Oracle database server. As a result, the Oracle database server will not know if such statements are making any modifications to the DRDA Server. This means that unless you keep the Oracle database's cached information up to date after changes to the DRDA Server, the database may continue to rely upon inaccurate or outdated information in subsequent queries within the same session.

An example of this occurs when you alter the structure of a table by either adding or removing a column. When an application references a table through the gateway (for example, when you perform a query on it), the Oracle database server caches the table definition. Now, suppose that (within the same session) the application subsequently alters the table's form, by using `DBMS_HS_PASSTHROUGH.EXECUTE_IMMEDIATE` to add a column. Then, the next reference to the table (by the application) will return the old column definitions of the table and will ignore the table's new column. This is because the Oracle database server did not process the statement and, so, has no knowledge of the alteration. Because the database does not know of the alteration, it has no reason to requery the table form, and, so, it will use the already-cached form to handle any new queries.

In order for the Oracle database server to acquire the new form of the table, the existing session with the gateway must be closed and a new session must be opened. This can be accomplished in either of two ways:

- By ending the application session with the Oracle database server and starting a new session after modifications have been made to the DRDA Server; or
- By running the `ALTER SESSION CLOSE DATABASE LINK` command after making any modifications to the DRDA Server.

Either of the above actions will void the cached table definitions and will force the Oracle database server to acquire new definitions on the next reference.

### 12.8.2 Using the `DBMS_HS_PASSTHROUGH.EXECUTE_IMMEDIATE` Function

To run a passthrough SQL statement using `DBMS_HS_PASSTHROUGH.EXECUTE_IMMEDIATE`, use the following syntax:

```
number_of_rows = DBMS_HS_PASSTHROUGH.EXECUTE_IMMEDIATE@dblink ('native_DRDA_sql');
```

where:

`number_of_rows` is a variable that is assigned the number of rows that are affected by the passthrough SQL completion. For DDL statements, a zero is returned for the number of rows affected.

`dblink` is the name of the database link that is used to access the gateway.

`native_DRDA_sql` is a valid nonquery SQL statement (except CONNECT, COMMIT, and ROLLBACK). The statement cannot contain bind variables. Native SQL statements that cannot be dynamically prepared are rejected by the DRDA Server. The SQL statement that is passed by the `DBMS_HS_PASSTHROUGH.EXECUTE_IMMEDIATE` function must be a character string. For more information regarding valid SQL statements, refer to the *SQL Reference* for the particular DRDA Server.

### 12.8.2.1 Examples

#### 1. Insert a row into a DB2 table using

`DBMS_HS_PASSTHROUGH.EXECUTE_IMMEDIATE`:

```
DECLARE
    num_rows integer;
BEGIN
    num_rows:=DBMS_HS_PASSTHROUGH.EXECUTE_IMMEDIATE@dblink
('INSERT INTO SCOTT.DEPT VALUES (10, 'PURCHASING', 'PHOENIX')');
END
/
```

#### 2. Create a table in DB2 using `DBMS_HS_PASSTHROUGH.EXECUTE_IMMEDIATE`:

```
DECLARE
    num_rows integer;
BEGIN
    num_rows:=DBMS_HS_PASSTHROUGH.EXECUTE_IMMEDIATE@dblink
('CREATE TABLE MYTABLE (COL1 INTEGER, COL2 INTEGER, COL3 CHAR(14),
    COL4 VARCHAR(13))');
END;
/
```

## 12.8.3 Retrieving Result Sets Through Passthrough

Oracle Transparent Gateway for DRDA provides a facility to retrieve results sets from a SELECT SQL statement entered through passthrough.

### 12.8.3.1 Example

```
DECLARE
    CRS binary_integer;
    RET binary_integer;
    VAL VARCHAR2(10)
BEGIN
    CRS:=DBMS_HS_PASSTHROUGH.OPEN_CURSOR@gtwlink;
    DBMS_HS_PASSTHROUGH.PARSE@gtwlink(CRS, 'SELECT NAME FROM PT_TABLE');
    RET:=0;
    WHILE (TRUE)
    LOOP
        RET:=DBMS_HS_PASSTHROUGH.FETCH_ROW@gtwlink(CRS, FALSE);
        DBMS_HS_PASSTHROUGH.GET_VALUE@gtwlink(CRS, 1, VAL);
        INSERT INTO PT_TABLE_LOCAL VALUES (VAL);
    END LOOP;
EXCEPTION
    WHEN NO_DATA_FOUND THEN
        BEGIN
```

```
        DBMS_OUTPUT.PUT_LINE('END OF FETCH');
        DBMS_HS_PASSTHROUGH.CLOSE_CURSOR@gtwlink(CRS);
    END;
END;
END;
/
```

## 12.9 Oracle Data Dictionary Emulation on a DRDA Server

The gateway optionally augments the DRDA database catalogs with data dictionary views modeled after the Oracle data dictionary. These views are based on the dictionary tables in the DRDA database, presenting that catalog information in views familiar to Oracle users. The views created during the installation of the gateway automatically limit the data dictionary information presented to each user based on the privileges of that user.

### 12.9.1 Using the Gateway Data Dictionary

The gateway data dictionary views provide users with an Oracle-like interface to the contents and use of the DRDA database. Some of these views are required by Oracle products. The gateway supports the DB2/OS390, DB2/400, and DB2/UDB catalog views. DB2/VM catalog views are not available.

You can query the gateway data dictionary views to see the objects in the DRDA database and to determine the authorized users of the DRDA database. Many Oracle catalog views are supported by the Oracle Transparent Gateway for DRDA. Refer to [Appendix A](#) for descriptions of Oracle DB2 catalog views. These views are completely compatible with the gateway.

### 12.9.2 Using the DRDA Catalog

Each DRDA database has its own catalog tables and views, which you might find useful. Refer to IBM documentation for descriptions of these catalogs.

## 12.10 Defining the Number of DRDA Cursors

You can define any number of cursors depending on your application requirements. Oracle recommends that you use the default value of 100. However, if the default is not correct for your application, there are two points to consider when defining the number of cursors for your installation:

1. Each cursor requires an additional amount of storage and additional management.
2. If you change `DRDA_PACKAGE_SECTIONS`, then you must rebind the package.

The parameter `DRDA_PACKAGE_SECTIONS` is specific to the DRDA package. This parameter defines the number of sections (open cursors at the IBM database). For more information about setting the `DRDA_PACKAGE_SECTIONS` parameter, refer to [Appendix C, "DRDA-Specific Parameters"](#).

---

---

## Security Considerations

The gateway architecture involves multiple computer systems that have distinct security capabilities and limitations. This chapter provides information for planning and implementing the security system.

This chapter includes the following sections:

- [Security Overview](#)
- [Authenticating Application Logons](#)
- [Defining and Controlling Database Links](#)
- [TCP/IP Security](#)
- [Processing Inbound Connections](#)
- [Passwords in the Gateway Initialization File](#)

### 13.1 Security Overview

When you connect several systems, generally, the system with the strictest security requirements dictates and rules the system.

Gateway security involves two groups:

- Users and applications that are permitted access to a given gateway instance and DRDA database server
- Server database objects that users and applications are able to query and update

You can control access in the gateway architecture at several points. Control over database object access is provided by each DRDA database server with GRANTs and related native authorization mechanisms based on user ID.

When the gateway is involved in a SQL request, security mechanisms are in effect for each DRDA system component encountered by the gateway. The first system component encountered is the application tool or 3GL program. The last system component encountered is the DRDA database.

### 13.2 Authenticating Application Logons

An application must connect to an Oracle integrating server before using the gateway. The type of logon authentication that you use determines the resulting Oracle user ID and can affect gateway operation. There are two basic types of authentication:

- Oracle authentication

With Oracle authentication, each Oracle user ID has a password known to the Oracle server. When an application connects to the server, it supplies a user ID and password. The Oracle server confirms that the user ID exists and that the password matches the one kept in the database.

- **Operating system authentication**

With operating system authentication, the server's underlying operating system is responsible for authentication. An Oracle user ID that is created with the `IDENTIFIED EXTERNALLY` attribute, instead of a password, is accessed with operating system authentication. To log in to such a user ID, the application supplies a slash ( / ) for a user ID and does not supply a password.

To perform operating system authentication, the server determines the requester's operating system user ID, optionally adds a fixed prefix to it, and uses the result as the Oracle user ID. The server confirms that the user ID exists and is identified externally, but no password checking is done. The underlying assumption is that users were authenticated when they logged in to the operating system.

Operating system authentication is not available on all platforms and is not available in some Oracle Net (client/server) and multithreaded server configurations. Refer to the *Oracle Database Installation Guide for Microsoft Windows (32-Bit)* and Oracle Net documentation to determine the availability of this feature in Microsoft Windows.

For more information about authenticating application logons, refer to the *Oracle Database Reference*.

## 13.3 Defining and Controlling Database Links

The information here is specific to the gateway. For additional information on database links, refer to the *Oracle Database Administrator's Guide*.

### 13.3.1 Link Accessibility

The first point of control for a database link is whether it is accessible to a given user. A public database link can be used by any user ID. A private database link is usable only by the user who created it. The server makes no distinction regarding the type of use (such as read-only and update or write) or which remote objects can be accessed. These distinctions are the responsibility of the DRDA database that is accessed.

### 13.3.2 Links and CONNECT Clauses

The `CONNECT` clause is another security-related attribute of a database link. You can use the `CONNECT` clause to specify an explicit user ID and password, which can differ from the user's Oracle user ID and password. This `CONNECT` user ID and password combination is sent to the gateway when the database link connection is first opened. Depending on gateway options, the gateway might send that user ID and password to the DRDA Server for it to validate.

If a database link is created without a `CONNECT` clause, then the user's Oracle user ID and password are sent to the gateway when the connection is opened. If the user logs in to the Oracle integrating server with operating system authentication, then the gateway receives no user ID or password from the Oracle integrating server. In this case, user ID mapping facilities at the DRDA Server can be used to make such a connection possible if all users on the same Pentium-based host can use the same DRDA database user ID.

## 13.4 TCP/IP Security

TCP/IP does not have any additional configurable security mechanism. The gateway supports a validation mechanism which requires a user ID and a valid password. The security information is passed to the DRDA Server for validation. This type of validation is equivalent to the "SNA Security Option SECURITY=PROGRAM" on page 6-17 or "SNA Security Option SECURITY=PROGRAM" on page 7-19, which is discussed in [Chapter 6, "Configuring Microsoft SNA Server or Host Integration Server"](#) and [Chapter 7, "Configuring IBM Communication Server"](#). The difference between the two methods is that in the SNA configuration, the security validation is performed by the SNA network facilities, while in the TCP/IP configuration, the DRDA Server manually performs the validation.

## 13.5 Processing Inbound Connections

Current DRDA Servers provide options for manipulating the security conduct of an inbound (client) DRDA session request. Refer to IBM documentation for detailed information about the security options discussed in this section. Refer to the section, ["Documentation Requirements"](#) on page 3-3, for a list of IBM documentation.

### 13.5.1 User ID Mapping

User ID mapping is the most useful DRDA Server security capability. User ID mapping refers to changing the user ID associated with an incoming DRDA request to some other user ID known to that server. This is a useful feature if your installation does not have a uniform user ID structure across all systems and databases.

#### 13.5.1.1 DB2/OS390

The DB2 DDF Communication Database (CDB) stores inbound DRDA session security options. These tables, pertinent to inbound sessions, have a role in security processing:

- SYSIBM.LUNAMES table

The SYSIBM.LUNAMES table controls inbound security conduct on an SNA LU basis, affecting all DRDA connections from a particular host system. This table also controls whether inbound connection user IDs are subject to translation or mapping.

- SYSIBM.USERNAMES table

When translation is used, rows in the SYSIBM.USERNAMES table specify translated user IDs by LU name and inbound user ID. Default entries that pertain to all LUs and to all inbound user IDs can be made in both tables. The mapping table can also be used to indicate which inbound user IDs are permitted, from a particular LU or from all LUs, whether or not they are mapped.

This implementation provides a flexible mapping structure. You can specify that all connections from a particular LU use a single DB2 user ID, or that a particular inbound user ID always be mapped to a particular DB2 user ID regardless of origin. A USERNAMES entry with blank LU name and inbound user ID can designate a single default DB2 user ID for all connections unless a more specific entry, by LU name, user ID, or both, exists.

The CDB tables can be updated by a user with update authority using a SQL tool such as the DB2 SPUFI utility. For example, most database administrators, systems programmers, and security officers can update CDB tables. The DB2 DDF component must be stopped and restarted for CDB changes to take effect.

The DB2 non-DRDA-specific security features are also involved in DRDA connections. User IDs are subject to normal DB2 or SAF/RACF validation in addition to connection or sign-on exit processing. Passwords are also subject to validation. Once the connection is established, all normal authorizations or GRANTS associated with the user ID are in effect. The user ID must have execute authority on the gateway DRDA package to process SQL statements.

### 13.5.1.2 DB2/VM

Under VM, DRDA sessions are managed by APPC VTAM Support (AVS), which runs as a disconnected GCS virtual machine. AVS receives incoming APPC connection requests (both DRDA and non-DRDA) and routes the connection to a suitable server virtual machine.

AVS user ID mapping is controlled by internal AVS data structures that are updated with the `AGW ADD USERID` and `AGW DELETE USERID` commands.

A user ID mapping entry converts the inbound user ID before making the DB2/VM connection. The user ID mapping consists of:

- Originating LU name
- Inbound user ID
- The new user ID

You can create default entries that apply to any LU name and to any inbound user ID, and an entry can indicate that the inbound user ID is to be used without mapping.

AVS user ID mapping is functionally similar to the DB2 user ID translation mechanism and can be used to work around a variety of incongruities among user IDs on different systems and databases.

Once any indicated user ID mapping has been done, inbound DRDA connection requests are forwarded to the specified DB2/VM server system. DB2/VM confirms only if the user ID has `CONNECT` authority and, if so, that the connection is complete. At this point, the application's access to DB2/VM objects is controlled by the normal authorities and GRANTS for the connected user ID. The user ID must have execute authority on the gateway DRDA package to process SQL statements.

### 13.5.1.3 DB2/400

DB2/400 does not provide a user ID mapping capability comparable to that in DB2/OS390 and DB2/VM. Normally, the user ID in an incoming DRDA connection request must be a valid user ID on that AS/400 subsystem.

The AS/400 subsystem communications entry for the gateway should specify that the gateway is not a secure location and should include a default user ID of `*NONE`.

Once the application has completed the DRDA connection to the AS/400 subsystem, it is subject to all authorities and GRANTS associated with the user ID in use. The user ID must have execute authority on the gateway DRDA package to run SQL statements.

### 13.5.1.4 DB2/Universal Database

DB2/Universal Database (DB2/UDB) does not provide a user ID mapping capability comparable to that in DB2/OS390 and DB2/VM. Normally, the user ID in an incoming DRDA connection request must be a valid user ID on that host.

Once the gateway has completed the DRDA connection to the host, it is subject to all authorities and GRANTS associated with the user ID in use. The user ID must have execute authority on the gateway DRDA package to run SQL statements.



## 13.6 Passwords in the Gateway Initialization File

The gateway uses user IDs and passwords to access the information in the remote database on the DRDA Server. Some user IDs and passwords must be defined in the gateway initialization file to handle functions such as resource recovery. In today's security-conscious environment, having plain-text passwords that are accessible in the Initialization File is deemed insecure. An encryption feature has been added as part of Heterogeneous Services' generic connectivity to help make this more secure. This feature is accessible by this gateway. With it initialization parameters which contain sensitive values might be stored in an encrypted form. Refer to the manual *Oracle Database Heterogeneous Connectivity Administrator's Guide*, Chapter 4, "Encrypting Initialization Parameters" for information about how to use the feature.

**See Also:** The parameters `DRDA_RECOVERY_USERID` and `DRDA_RECOVERY_PASSWORD` in Appendix C as examples, for more information



---

---

## Migration and Coexistence with Existing Gateways

Migration to new instances of Oracle Transparent Gateway for DRDA from an existing installation is straightforward, provided some guidelines are followed.

This chapter provides information that is specific to this release of the Oracle Transparent Gateway for DRDA and includes the following sections:

- [Migrating Existing V4, V8, or V9 Gateway Instances to New Release](#)
- [Backout Considerations When Migrating to New Releases](#)
- [New and Changed Parameters When Migrating to Release 10](#)
- [DRDA Server Considerations](#)
- [Oracle Net Considerations](#)

### 14.1 Migrating Existing V4, V8, or V9 Gateway Instances to New Release

**Migration** is the process of transforming an installed version of an Oracle database into a later version (compare this with upgrading). For example, transforming an Oracle8*i* database into an Oracle9*i* database is migrating the database. This transformation generally involves running the Oracle migrate (MIG) utility to modify Oracle database control file structures from the format of one version to the format of another version.

**Upgrading** is the process of transforming an Oracle database from an installed release into a later release of the same version. For example, transforming patch release 8.0.3 into patch release 8.0.4 is upgrading.

#### 14.1.1 Step 1: Install the new Release

Install the new release of the gateway in a separate directory, as outlined in [Chapter 4, "Installing the Gateway"](#).

---

---

**Caution:** Do not install the gateway over a previously existing Gateway installation. Doing so will corrupt the existing installation.

---

---

#### 14.1.2 Step 2: Transferring `initsid.gtwboot` Gateway Boot Initialization parameters.

In previous releases, the gateway used two gateway initialization files (`initsid.gtwboot` and `initsid.ora`), or it used a Startup Shell Script (`drdaDB2.sh`) and one initialization file

(*initsid.ora*). In this release, all parameters have been migrated into a single gateway initialization file, *initsid.ora*. Migrating a previous release involves copying the parameters from the *initsid.gtwboot* or Startup Shell Script into *initsid.ora*. The format of the parameters can be found in [Appendix C, "DRDA-Specific Parameters"](#).

### 14.1.3 Step 3: Transferring *initsid.ora* gateway initialization file parameters.

Copy the *initsid.ora* from the old Gateway instance to the new instance. The parameters in the *initsid.ora* gateway initialization file have changed format. Refer to "[Gateway Initialization File Parameters](#)" on page C-2 in [Appendix C, "DRDA-Specific Parameters"](#).

## 14.2 Backout Considerations When Migrating to New Releases

During the migration from older version 4, version 8, or version 9 gateway instances to the latest Oracle Database 10g release, if problems are encountered, then it is always possible to revert to the previous version. Assuming a working version 4 gateway instance exists, change the TNSNAMES.ORA entries from using the Oracle Database 10g gateway instance to the older version 4 instance. Remember to remove the "(HS=)" entry from the Oracle Net connect definition.

Oracle recommends that when you are installing a new release of the gateway and upgrading existing instances, you keep the old gateway home and instance configurations intact and operational, in case there are problems with the upgrade. This will help ensure minimal downtime between changes to different gateway instances.

## 14.3 New and Changed Parameters When Migrating to Release 10

This release of the Oracle Transparent Gateway for DRDA introduces new and changed initialization parameters if you are migrating from a version 4, version 8, or version 9 gateway to the Oracle Database 10g gateway.

### 14.3.1 New Parameters

The following section lists new parameters relevant to migration from version 4 gateways.

#### 14.3.1.1 New Gateway Initialization File Parameters

Parameters introduced in this release of the gateway, listed in the following table, may be added to the gateway initialization file:

- DRDA\_CACHE\_TABLE\_DESC
- DRDA\_GRAPHIC\_LIT\_CHECK
- DRDA\_GRAPHIC\_PAD\_SIZE
- DRDA\_GRAPHIC\_TO\_MBCS
- DRDA\_MBCS\_TO\_GRAPHIC
- DRDA\_PROCDISC\_STMT
- DRDA\_PROCDISCPARMS\_STMT
- DRDA\_PROCCALL\_MASK
- DRDA\_FUNCDESC\_STMT

- DRDA\_FUNCDESCPARMS\_STMT
- DRDA\_FUNCCALL\_MASK
- DRDA\_GRAPHIC\_CHAR\_SIZE

### 14.3.2 Parameters That Have Been Changed in Usage

The usage of the following parameters has changed with version 9 of the gateway:

- DRDA\_CONNECT\_PARM

### 14.3.3 Parameters That Have Been Renamed

The following table presents a list of parameters that have been renamed with version 9 of the gateway, and their corresponding old names. Refer to *Oracle Database Heterogeneous Connectivity Administrator's Guide* for more detailed information about these parameters.

**Table 14–1 Parameters That Have Been Renamed**

New Name	Old Name
HS_COMMIT_STRENGTH_POINT	COMMIT_STRENGTH_POINT
HS_DB_DOMAIN	DB_DOMAIN
HS_DB_INTERNAL_NAME	DB_INTERNAL_NAME
HS_DB_NAME	DB_NAME
HS_DESCRIBE_CACHE_HWM	DESCRIBE_CACHE_HWM
HS_LANGUAGE	LANGUAGE
HS_NLS_DATE_FORMAT	NLS_DATE_FORMAT
HS_NLS_DATE_LANGUAGE	NLS_DATE_LANGUAGE
HS_OPEN_CURSORS	OPEN_CURSORS
HS_ROWID_CACHE_SIZE	ROWID_CACHE_SIZE

### 14.3.4 Obsolete Parameters

The following parameters are now obsolete. Please remove them from your configuration files:

- MODE
- SERVER\_PATH
- DRDA\_OVERRIDE\_FROM\_CODEPAGE
- DRDA\_OVERRIDE\_TO\_CODEPAGE
- ERROR\_LOGGING
- ERROR\_REPORTING
- ERRORTAG
- GATEWAY\_SID
- GROUP\_BY\_OFF
- GTWDEBUG
- INCREMENT\_CURSORS

- DRDA\_CALLDESC\_STMT
- DRDA\_CALLDESC\_PROC

## 14.4 DRDA Server Considerations

Part of the normal installation for the gateway involves binding a package and (as an option) installing data dictionary views on the DRDA Server. This release of the gateway (10.2.0.1.0) is compatible with version 4, version 8, and version 9 packages that have been previously bound. The data dictionary views, however, have changed with this release. If you plan to use the data dictionary views that are provided by the gateway, then you must migrate to the new views. Oracle recommends that you install the new views as outlined in [Chapter 10, "Configuring the Gateway"](#). If you have changed certain DRDA parameters of the gateway initialization parameters as a result of the migration, then a rebind of the package will be required.

## 14.5 Oracle Net Considerations

The gateway uses the Heterogeneous Services (HS) facilities of Oracle and Oracle Net. As such, gateway service name entries in `tnsnames.ora` need a slight modification to tell Oracle Net that the gateway will be using the HS facilities. Refer to ["Configuring Oracle Net"](#) on page 9-3 for detailed information.

---

---

## Error Messages, Diagnosis, and Reporting

This chapter provides information about error messages and error codes. This chapter is specific to this release of the Oracle Transparent Gateway for DRDA, and it includes the following sections:

- [Interpreting Gateway Error Messages](#)
- [Mapped Errors](#)
- [Gateway Error Codes](#)
- [SQL Tracing and the Gateway](#)

### 15.1 Interpreting Gateway Error Messages

The gateway architecture involves a number of separate components. Any component might detect and report an error condition while processing SQL statements that refer to one or more DRDA database tables. This means that error situations can be complex, involving error codes and supporting data from multiple components. In all cases, however, the application ultimately receives a single Oracle error number or return code on which to act.

Because most gateway messages exceed the 70-character message area in the Oracle SQLCA, the programmatic interfaces and Oracle Call Interfaces that you use to access data through the gateway should use SQLGLM or OERHMS to view the entire text of messages. Refer to the programmer's guide to the Oracle precompilers for additional information about SQLGLM, and refer to the *Oracle Call Interface Programmer's Guide* for additional information about OERHMS.

Error conditions encountered when using the gateway can originate from many sources:

- Errors detected by the Oracle integrating server
- Errors detected by the gateway
- Errors detected in the DRDA software, either on the requestor or server side
- Communication errors
- Errors detected by the server database

#### 15.1.1 Errors Detected by the Oracle Integrating Server

Errors detected by the Oracle integrating server are reported back to the application or tool with the standard ORA- type message. Refer to the *Oracle Database Error Messages*

for descriptions of these errors. For example, the following error message occurs when an undefined database link name is specified:

```
ORA-02019: connection description for remote database not found
```

Errors in the ORA-9100 to ORA-9199 range are reserved for the generic gateway layer (components of the gateway that are not specific to DRDA). Messages in this range are documented in *Oracle Database Error Messages*.

### 15.1.2 Errors Detected by the Gateway

Errors detected by the generic gateway are prefixed with HGO- and are documented in the *Oracle Database Error Messages*.

An example of an error message is:

```
HGO-00706: HGO: Missing equal sign for parameter in initialization file.
```

### 15.1.3 Errors Detected in the DRDA Software

Errors detected in the DRDA gateway, on the requestor or server side, are usually reported with error code ORA-28500, followed by a gateway-specific expanded error message. There are two return codes reported in the expanded message:

- `drc` specifies DRDA-specific errors which are documented in "[Gateway Error Codes](#)" on page 15-4.
- `grc` specifies generic gateway errors detected in the DRDA layer. These errors are documented in the *Oracle Database Heterogeneous Connectivity Administrator's Guide*.

---

---

**Note:** Error code ORA-28500 was error code ORA-09100 prior to gateway version 8. Error code ORA-28501 was error code ORA-09101 prior to gateway version 8.

---

---

The values in parentheses that follow the `drc` values are used for debugging by Oracle Support Services. The `errp` field indicates the program (requestor or server) that detected the error. If `errmc` is present, it lists any error tokens.

For example, the following error message is returned when the database name specified (`XNAME`) with the `DRDA_REMOTE_NAME` parameter in the `initsid.ora` file is not defined at the DRDA Server:

```
ORA-28500: connection from ORACLE to a non-Oracle system returned the message:
TG4DRDA v10.2.0.1.0 grc=0, drc=-30061 (839C,0000), errp=GDJRFS2E
errmc=XNAME
```

### 15.1.4 Communication Errors

Communication errors are reported with an ORA-28501 followed by a gateway-specific expanded error message with `drc=-30080` (SNA CPI-C error) or `drc=-30081` (lost session). `errmc` indicates which CPI-C routine encounters the error, followed by the CPI-C error code and error number.

For example, the following error message is returned when there is a failure to establish a session because `DRDA_CONNECT_PARM` in the `initsid.ora` file specifies a Side Information Profile that is not defined:

```
ORA-28501: Target system communication error.
```



```
TG4DRDA v10.2.0.1.0 grc=0, drc=-30081 (839C,0001), errp=GDJICRD
errmc=Initialize_Conversation (CMINIT) 24 0
```

Refer to the appropriate Microsoft Windows or IBM Communication Server documentation for more information.

### 15.1.5 Errors Detected by the Server Database

Errors detected by the server database are reported with an ORA-28500 Oracle Error followed by a gateway-specific expanded error message with `drc=-777` (`sqlcode` follows). This is followed by another error message line that contains the `sqlcode`, `sqlstate`, `errd` (error array), and `errmc` (error tokens) returned from the DRDA Server database. Refer to IBM documentation for the specific database being used. Also refer to ["Mapped Errors"](#) on page 15-3 for some SQL errors that get translated.

---

**Note:** Error code ORA-28500 was error code ORA-09100 prior to gateway version 8. Error code ORA-28501 was error code ORA-09101 prior to gateway version 8.

---

For example, the following error message indicates that the DRDA Server database did not recognize the collection ID or package name specified with the `DRDA_PACKAGE_COLLID` or `DRDA_PACKAGE_NAME` parameters in the `initsid.ora` file:

```
ORA-28500: Target system returned following message:
TG4DRDA v10.2.0.1.0 grc=0, drc=-777 (839C,0000), errp=DSNXEPM
sqlcode=-805, sqlstate=51002, errd=FFFFFFFFC,0,0,FFFFFFFF,0,0
errmc=XB2V2R3..GSQL.A92617CB3FE5470DISTSERV
```

## 15.2 Mapped Errors

Some SQL errors are returned from the DRDA Server database and are translated to an Oracle error code. This is needed when the Oracle instance or gateway provides special handling of an error condition. The mapped `sqlstate` errors are:

**Table 15-1** Mapped `sqlstate` Errors

Description	sqlstate error	Oracle error
No rows selected	02000	0
Unique index constraint violated	23505	ORA-00001
Object does not exist	52004 or 42704	ORA-00942
Object name too long (more than 18 characters), and therefore object does not exist	54003 or 42622	ORA-00942
Insufficient privileges	42501	ORA-01031
Invalid CCSID (unimplemented character set conversion)	22522	ORA-01460
Invalid user name/password; logon denied	N/A	ORA-01017
Divide by zero error	01519 or 01564	ORA-01476

The following is an example of a translated "object does not exist" error:

```
ORA-00942: table or view does not exist
TG4DRDA v10.2.0.1.0 grc=0, drc=-942 (839C,0001), errp=DSNXEDST
```

```
sqlcode=-204, sqlstate=52004, errd=32,0,0,FFFFFFFF,0,0  
errmc=AJONES.CXDCX
```

## 15.3 Gateway Error Codes

Listed below are the common Oracle Transparent Gateway for DRDA error codes that appear in the `drc=` field of the expanded error messages. If you get a `drc` value that does not appear here, contact Oracle Support Services.

### -700 Invalid ORA\_MAX\_DATE specified

**Cause:** An invalid value was specified for `ORA_MAX_DATE` in the `initsid.ora` file.

**Action:** Correct the value of `ORA_MAX_DATE`. Correct format is `ORA_MAX_DATE=YYYY-MM-DD`, where `MM` is in the range of 1 to 12, and `DD` is in the range of 1 to 31 (and must be valid for the month).

### -701 Default CCSID value not supported

**Cause:** The value specified for `DRDA_DEFAULT_CCSID` in the `initsid.ora` file is not supported by the Oracle Transparent Gateway for DRDA.

**Action:** Refer to [Appendix D, "National Language Support"](#), for a list of supported DRDA Server character sets.

### -702 Application Host (bind) variable exceeds 32K

**Cause:** An application program specified a host variable with length greater than the DRDA permitted maximum of 32 K.

**Action:** The application must be modified to take into account DRDA limits.

### -703 Local Character set not supported

**Cause:** The character set specified for the `LANGUAGE` parameter in the `initsid.ora` file is not supported.

**Action:** Refer to [Appendix D, "National Language Support"](#), for a list of supported character sets.

### -704 User ID length greater than maximum

**Cause:** The user ID being used for the allocation of an APPC conversion by the gateway is longer than eight characters.

**Action:** A user ID of length of 8 or less must be used. Refer to [Chapter 13, "Security Considerations"](#), for a discussion of user IDs.

### -705 Password length greater than maximum

**Cause:** The password being used for the allocation of an APPC conversion by the gateway is longer than eight characters.

**Action:** A password of length of 8 or less must be used. Refer to [Chapter 13, "Security Considerations"](#), for a discussion of passwords.

### -777 DRDA Server RDBMS (SQL) Error

**Cause:** Server database detected an application-level SQL error.

**Action:** Refer to ["Interpreting Gateway Error Messages"](#) on page 15-1. `sqlcode` and `sqlstate` indicate host database error. Use this information to fix your application.

### -30060 Invalid User ID/Password (DRDA Server RDBMS Authorization)

**Cause:** You have used a user ID/password that is not acceptable to the DRDA Server database.

**Action:** Refer to [Chapter 13, "Security Considerations"](#), for user ID/password considerations.

#### -30061 RDB not found

**Cause:** The remote database specified with the `DRDA_REMOTE_DB_NAME` parameter is not a valid database at the DRDA Server.

**Action:** Correct the value of the `DRDA_REMOTE_DB_NAME` parameter in the `initsid.ora` file.

#### -30080 Communication Error

**Cause:** The gateway encountered a CPI-C communication error.

**Action:** Retry processing that received error. If it persists, then refer to ["Interpreting Gateway Error Messages"](#) on page 15-1 and report to your system administrator.

#### -30081 Communication Error - lost session

**Cause:** The current DRDA CPI-C session was disconnected.

**Action:** Retry processing that received error. If it persists, then refer to ["Interpreting Gateway Error Messages"](#) on page 15-1 and report it to your system administrator.

## 15.4 SQL Tracing and the Gateway

When developing applications, it is often useful to be able to see the exact SQL statements that are being passed through the gateway. This section describes setting correct trace parameters and setting up the debug gateway.

### 15.4.1 SQL Tracing in the Oracle Database

The Oracle server has a command for capturing the SQL query which is actually sent to the gateway. This command is called `EXPLAIN PLAN`. `EXPLAIN PLAN` is used to determine the execution plan that Oracle follows to run a specified SQL statement. This command inserts a row (describing each step of the execution plan) into a specified table.

If you are using cost-based optimization, then this command also determines the cost of running the statement. The syntax of the command is:

```
EXPLAIN PLAN [ SET STATEMENT_ID = 'text' ]
             [ INTO [schema.]table [@dblink] ] FOR statement
```

For detailed information on this command, refer to the *Oracle Database SQL Reference*.

---

**Note:** In most cases, `EXPLAIN PLAN` should be sufficient to extract the SQL query which is actually sent to the gateway, and thus sent to the DRDA Server. However, certain SQL statement forms have postprocessing performed on them in the gateway. The next section will describe setting up SQL tracing in the gateway.

---

### 15.4.2 SQL Tracing in the Gateway

To enhance speed of the gateway, tracing was not built into the production gateway.

The product ships with a debug version of the gateway for the purposes of tracing and debugging applications.

This process entails changing the listener.ora file to use the debug gateway:

1. Log in as the Administrator user ID of the gateway and set up the environment.

2. Stop the Oracle Net Listener:

```
> lsnrctl stop
```

3. Edit the listener.ora with any text editor:

```
> notepad C:\Oracle\GTWHome\network\admin\listener.ora
```

4. Find the TNS entry for the gateway and change the program this way:

```
PROGRAM=g4drsrvd
```

5. Save the file and exit. Next, restart the Oracle Net Listener:

```
> lsnrctl start
```

6. Edit the gateway's initsid.ora file with any text editor:

```
> notepad C:\Oracle\GTWHome\tg4drda\admin\initsid.ora
```

7. Set the following parameters:

```
TRACE_LEVEL=255  
ORACLE_DRDA_TCTL=debug.tctl
```

---

---

**Note:** Refer to [Appendix C, "DRDA-Specific Parameters"](#) for descriptions of those parameters.

---

---

You may, as an option, add the LOG\_DESTINATION parameter, but it is not required. If you specify a LOG\_DESTINATION, then you may specify just the file name (for example, drda.trc), or you may specify a fully qualified path name. If you specify a LOG\_DESTINATION with just the file name, then the log will be written to the log directory (ORACLE\_HOME\tg4drda\trace) of the gateway. If you do not specify a LOG\_DESTINATION, then a unique log file in a default format will be generated. The log file name will be of the form:

```
gatewaysid_tid.trc
```

Where:

*gateway sid* is the SID of the gateway.

*tid* is the thread identifier (TID) of the gateway service.

An example log file name would be:

```
drdahoa1_3875.trc
```

When searching for the SQL statements which are passed to the DRDA Server, look for the strings '\*\*\* HGAPARS \*\*\*' and '\*\*\* HGAXMSQL \*\*\*'. The string after HGAPARS will be the incoming statement from the Oracle Database 10g RDBMS. The string after HGAXMSQL will be the outgoing statement after any date substitution is done. This is the actual SQL statement which will be given to the DRDA Server.

When you have finished developing your application, revert the PROGRAM= value in the listener.ora file to its previous value and reload the listener to use the production

gateway again. You should also comment out the trace parameters in the gateway initialization files.



---

---

## Oracle DB2 Data Dictionary Views

This appendix includes the Oracle Transparent Gateway for DRDA data dictionary views accessible to all users of an Oracle server. Most views can be accessed by any user with SELECT privileges for DB2 catalog tables.

N/A is used in the following tables to mean that the column is not valid for the gateway.

This appendix contains the following sections:

- [Supported Views](#) on page A-1
- [Data Dictionary View Tables](#) on page A-2

### A.1 Supported Views

The following is a list of Oracle data dictionary views that are supported by the gateway for DB2/OS390, DB2/400, and DB2/UDB DRDA Servers. This release of the gateway does not have data dictionary view support for DB2/VM servers.

- ALL\_CATALOG
- ALL\_COL\_COMMENTS
- ALL\_CONS\_COLUMNS
- ALL\_CONSTRAINTS
- ALL\_INDEXES
- ALL\_IND\_COLUMNS
- ALL\_OBJECTS
- ALL\_SYNONYMS
- ALL\_TAB\_COMMENTS
- ALL\_TABLES
- ALL\_TAB\_COLUMNS
- ALL\_USERS
- ALL\_VIEWS
- COL\_PRIVILEGES
- DICTIONARY
- DUAL
- TABLE\_PRIVILEGES

- USER\_CATALOG
- USER\_COL\_COMMENTS
- USER\_CONSTRAINTS
- USER\_CONS\_COLUMNS
- USER\_INDEXES
- USER\_OBJECTS
- USER\_SYNONYMS
- USER\_TABLES
- USER\_TAB\_COLUMNS
- USER\_TAB\_COMMENTS
- USER\_USERS
- USER\_VIEWS

## A.2 Data Dictionary View Tables

The remainder of this chapter contains tables describing data dictionary views. In the following descriptions, all are supported for DB2/OS390 and DB2/400.

### A.2.1 ALL\_CATALOG

All tables, views, synonyms, and sequences accessible to the user:

Column Name	Description
OWNER	Owner of the object
TABLE_NAME	Name of the object
TABLE_TYPE	Type of object

### A.2.2 ALL\_COL\_COMMENTS

Comments on columns of accessible tables and views:

Column Name	Description
OWNER	Owner of the object
TABLE_NAME	Object name
COLUMN_NAME	Column name
COMMENTS	Comments on column

### A.2.3 ALL\_CONS\_COLUMNS

Information about accessible columns in constraint definitions:

Column Name	Description
OWNER	Owner of the constraint definition
CONSTRAINT_NAME	Name associated with the constraint definition



Column Name	Description
TABLE_NAME	Name associated with table with constraint definition
COLUMN_NAME	Name associated with column specified in the constraint definition
POSITION	Original position of column in definition

## A.2.4 ALL\_CONSTRAINTS

Constraint definitions on accessible tables:

Column Name	Description
OWNER	Owner of the constraint definition
CONSTRAINT_NAME	Name associated with the constraint definition
CONSTRAINT_TYPE	Type of constraint definition
TABLE_NAME	Name associated with table with constraint definition
SEARCH_CONDITION	Text of search condition for table check
R_OWNER	Owner of table used in referential constraint
R_CONSTRAINT_NAME	Name of unique constraint definition for referenced table
DELETE_RULE	Delete rule for referential constraint
STATUS	Status of constraint
DEFERRABLE	Whether the constraint is deferrable
DEFERRED	Whether the constraint was initially deferred
VALIDATED	Whether all data obeys the constraint
GENERATED	Whether the name of the constraint is user or system generated
BAD	Constraint specifies a century in an ambiguous manner
RELY	Whether an enabled constraint is enforced or unenforced
LAST_CHANGE	When the constraint was last enabled or disabled
INDEX_OWNER	N/A
INDEX_NAME	N/A

## A.2.5 ALL\_INDEXES

Description of indexes on tables accessible to the user:

Column Name	Description
OWNER	Owner of the index
INDEX_NAME	Name of the index
INDEX_TYPE	Type of index
TABLE_OWNER	Owner of the indexed object
TABLE_NAME	Name of the indexed object
TABLE_TYPE	Type of the indexed object
UNIQUENESS	Uniqueness status of the index

Column Name	Description
COMPRESSION	N/A
PREFIX_LENGTH	0
TABLESPACE_NAME	Name of the tablespace containing the index
INI_TRANS	N/A
MAX_TRANS	N/A
INITIAL_EXTENT	N/A
NEXT_EXTENT	N/A
MIN_EXTENTS	N/A
MAX_EXTENTS	N/A
PCT_INCREASE	N/A
PCT_THRESHOLD	Threshold percentage of block space permitted per index entry
INCLUDE_COLUMN	Column ID of the last column to be included in index-organized table
FREELISTS	Number of process free lists allocated to this segment
FREELIST_GROUPS	Number of free list groups allocated to this segment
PCT_FREE	N/A
LOGGING	Logging information
BLEVEL	Depth of the index from its root block to its leaf blocks. A depth of 1 indicates that the root block and the leaf block are the same.
LEAF_BLOCKS	Number of leaf blocks in the index
DISTINCT_KEYS	Number of distinct indexed values. For indexes that enforce UNIQUE and PRIMARY KEY constraints, this value is the same as the number of rows in the table.
AVG_LEAF_BLOCKS_PER_KEY	N/A
AVG_DATA_BLOCKS_PER_KEY	N/A
CLUSTERING_FACTOR	N/A
STATUS	State of the index: VALID
NUM_ROWS	Number of rows in the index
SAMPLE_SIZE	Size of the sample used to analyze the index
LAST_ANALYZED	Date on which this index was most recently analyzed
DEGREE	Number of threads per instance for scanning the index
INSTANCES	Number of instances across which the index is to be scanned
PARTITIONED	Whether this index is partitioned
TEMPORARY	Whether the index is on a temporary table
GENERATED	Whether the name of the index is system generated
SECONDARY	N/A
BUFFER_POOL	Whether the index is a secondary object
USER_STATS	N/A

Column Name	Description
DURATION	N/A
PCT_DIRECT_ACCESS	N/A
ITYP_OWNER	N/A
ITYP_NAME	N/A
PARAMETERS	N/A
GLOBAL_STATS	N/A
DOMIDX_STATUS	N/A
DOMIDX_OPSTATUS	N/A
FUNCIDX_STATUS	N/A
JOIN_INDEX	N/A
IOT_REDUNDANT_PKEY_ELIM	N/A

## A.2.6 ALL\_IND\_COLUMNS

ALL\_IND\_COLUMNS describes the columns of indexes on all tables that are accessible to the current user.

Column Names	Description
INDEX_OWNER	Owner of the index
INDEX_NAME	Name of the index
TABLE_OWNER	Owner of the table or cluster
TABLE_NAME	Name of the table or cluster
COLUMN_NAME	Column name or attribute of object type column
COLUMN_POSITION	Position of column or attribute within the index
COLUMN_LENGTH	Indexed length of the column
CHAR_LENGTH	Maximum code point length of the column
DESCEND	Whether the column is sorted in descending order (Y/N)

## A.2.7 ALL\_OBJECTS

Objects accessible to the user:

Column Name	Description
OWNER	Owner of the object
OBJECT_NAME	Name of object
SUBOBJECT_NAME	Name of the subobject
OBJECT_ID	Object number of the object
DATA_OBJECT_ID	Dictionary object number of the segment that contains the object
OBJECT_TYPE	Type of object
CREATED	N/A
LAST_DDL_TIME	N/A

Column Name	Description
TIMESTAMP	N/A
STATUS	State of the object
TEMPORARY	Whether the object is temporary
GENERATED	Was the name of this object system-generated?
SECONDARY	N/A

## A.2.8 ALL\_SYNONYMS

All synonyms accessible to the user:

Column Name	Description
OWNER	Owner of the synonym
SYNONYM_NAME	Name of the synonym
TABLE_OWNER	Owner of the object referenced by the synonym
TABLE_NAME	Name of the object referenced by the synonym
DB_LINK	N/A

## A.2.9 ALL\_TABLES

Description of tables accessible to the user:

Column Name	Description
OWNER	Owner of the table
TABLE_NAME	Name of the table
TABLESPACE_NAME	Name of the tablespace containing the table
CLUSTER_NAME	N/A
IOT_NAME	Name of the index-organized table
PCT_FREE	N/A
PCT_USED	N/A
INI_TRANS	N/A
MAX_TRANS	N/A
INITIAL_EXTENT	N/A
NEXT_EXTENT	N/A
MIN_EXTENTS	N/A
MAX_EXTENTS	N/A
PCT_INCREASE	N/A
FREELISTS	Number of process free lists allocated to this segment
FREELIST_GROUPS	Number of free list groups allocated to this segment
LOGGING	Logging attribute
BACKED_UP	N/A
NUM_ROWS	Number of rows in the table

Column Name	Description
BLOCKS	N/A
EMPTY_BLOCKS	N/A
AVG_SPACE	N/A
CHAIN_CNT	N/A
AVG_ROW_LEN	Average length of a row in the table in bytes
AVG_SPACE_FREELIST_BLOCKS	The average free space of all blocks on a free list
NUM_FREELIST_BLOCKS	The number of blocks on the free list
DEGREE	The number of threads per instance for scanning the table
INSTANCES	The number of instances across which the table is to be scanned
CACHE	Whether the cluster is to be cached in the buffer cache
TABLE_LOCK	Whether table locking is enabled or disabled
SAMPLE_SIZE	Sample size used in analyzing this table
LAST_ANALYZED	Date on which this table was most recently analyzed
PARTITIONED	Indicates whether this table is partitioned
IOT_TYPE	Whether this is an index-organized table
TEMPORARY	Can the current session only see data that it placed in this object itself?
SECONDARY	N/A
NESTED	Whether the table is a nested table
BUFFER_POOL	The default buffer pool for the object
ROW_MOVEMENT	N/A
GLOBAL_STATS	N/A
USER_STATS	N/A
DURATION	N/A
SKIP_CORRUPT	N/A
MONITORING	N/A
CLUSTER_OWNER	N/A
DEPENDENCIES	N/A
COMPRESSION	N/A

### A.2.10 ALL\_TAB\_COLUMNS

Columns of all tables, views, and clusters accessible to the user:

Column Name	Description
OWNER	Owner of the table or view
TABLE_NAME	Table or view name
COLUMN_NAME	Column name

Column Name	Description
DATA_TYPE	Data type of column
DATA_TYPE_MOD	Data type modifier of the column
DATA_TYPE_OWNER	Owner of the data type of the column
DATA_LENGTH	Maximum length of the column in bytes
DATA_PRECISION	N/A
DATA_SCALE	Digits to the right of decimal point in a number
NULLABLE	Does the column permit nulls? Value is <i>n</i> if there is a NOT NULL constraint on the column or if the column is part of a PRIMARY key.
COLUMN_ID	Sequence number of the column as created
DEFAULT_LENGTH	N/A
DATA_DEFAULT	N/A
NUM_DISTINCT	Number of distinct values in each column of the table
LOW_VALUE	For tables with more than three rows, the second lowest and second highest values. These statistics are expressed in hexadecimal notation for the internal representation of the first 32 bytes of the values.
HIGH_VALUE	N/A
DENSITY	N/A
NUM_NULLS	The number of nulls in the column
NUM_BUCKETS	The number of buckets in histogram for the column
LAST_ANALYZED	The date on which this column was most recently analyzed
SAMPLE_SIZE	The sample size used in analyzing this column
CHARACTER_SET_NAME	The name of the character set
CHAR_COL_DECL_LENGTH	The length of the character set
GLOBAL_STATS	N/A
USER_STATS	N/A
AVG_COL_LEN	Average length of the column (in bytes)
CHAR_LENGTH	Displays the length of the column in characters
CHAR_USED	N/A

### A.2.11 ALL\_TAB\_COMMENTS

Comments on tables and views accessible to the user:

Column Name	Description
OWNER	Owner of the object
TABLE_NAME	Name of the object
TABLE_TYPE	Type of object
COMMENTS	Comments on the object

## A.2.12 ALL\_USERS

Information about all users of the database:

Column Name	Description
USERNAME	Name of the user
USER_ID	N/A
CREATED	N/A

## A.2.13 ALL\_VIEWS

Text of views accessible to the user:

Column Name	Description
OWNER	Owner of the view
VIEW_NAME	Name of the view
TEXT_LENGTH	Length of the view text
TEXT	View text. Only the first row of text is returned, even if multiple rows exist.
TYPE_TEXT_LENGTH	Length of the type clause of the typed view
TYPE_TEXT	Type clause of the typed view
OID_TEXT_LENGTH	Length of the WITH OID clause of the typed view
OID_TEXT	WITH OID clause of the typed view
VIEW_TYPE_OWNER	Owner of the type of the view if the view is a typed view
VIEW_TYPE	Type of the view if the view is a typed view
SUPERVIEW_NAME	N/A

## A.2.14 COLUMN\_PRIVILEGES

Grants on columns for which the user is the grantor, grantee, or owner, or PUBLIC is the grantee:

Column Name	Description
GRANTEE	Name of the user to whom access was granted
OWNER	Username of the object's owner
TABLE_NAME	Name of the object
COLUMN_NAME	Name of the column
GRANTOR	Name of the user who performed the grant
INSERT_PRIV	Permission to insert into the column
UPDATE_PRIV	Permission to update the column
REFERENCES_PRIV	Permission to reference the column
CREATED	Timestamp for the grant

## A.2.15 DICTIONARY

List or data dictionary tables:

Column Name	Description
TABLE_NAME	Table name
COMMENTS	Description of table

## A.2.16 DUAL

Column Name	Description
DUMMY	A dummy column

## A.2.17 TABLE\_PRIVILEGES

Grants on objects for which the user is the grantor, grantee, or owner, or PUBLIC is the grantee:

Column Name	Description
GRANTEE	Name of the user to whom access is granted
OWNER	Owner of the object
TABLE_NAME	Name of the object
GRANTOR	Name of the user who performed the grant
SELECT_PRIV	Permission to select from an object
INSERT_PRIV	Permission to insert into an object
DELETE_PRIV	Permission to delete from an object
UPDATE_PRIV	Permission to update an object
REFERENCES_PRIV	N/A
ALTER_PRIV	Permission to alter an object
INDEX_PRIV	Permission to create or drop an index on an object
CREATED	Timestamp for the grant

## A.2.18 USER\_CATALOG

Tables, views, synonyms, and sequences owned by the use:

Column Name	Description
TABLE_NAME	Name of the object
TABLE_TYPE	Type of object

## A.2.19 USER\_COL\_COMMENTS

Comments on columns of user's tables and views:

Column Name	Description
TABLE_NAME	Object name



Column Name	Description
COLUMN_NAME	Column name
COMMENTS	Comments on column

## A.2.20 USER\_CONSTRAINTS

Constraint definitions on user's tables:

Column Name	Description
OWNER	Owner of the constraint definition
CONSTRAINT_NAME	Name associated with the constraint definition
CONSTRAINT_TYPE	Type of constraint definition
TABLE_NAME	Name associated with table with constraint definition
SEARCH_CONDITION	Text of search condition for table check
R_OWNER	Owner of table used in referential constraint
R_CONSTRAINT_NAME	Name of unique constraint definition for referenced table
DELETE_RULE	Delete rule for referential constraint
STATUS	Status of constraint
DEFERRABLE	Whether the constraint is deferrable
DEFERRED	Whether the constraint was initially deferred
VALIDATED	Whether all data obeys the constraint
GENERATED	Whether the name of the constraint is user or system generated
BAD	Constraint specifies a century in an ambiguous manner
LAST_CHANGE	When the constraint was last enabled or disabled
INDEX_OWNER	N/A
INDEX_NAME	N/A

## A.2.21 USER\_CONS\_COLUMNS

Information about columns in constraint definitions owned by the user:

Column Name	Description
OWNER	Owner of the constraint definition
CONSTRAINT_NAME	Name associated with the constraint definition
TABLE_NAME	Name associated with table with constraint definition
COLUMN_NAME	Name associated with column specified in the constraint definition
POSITION	Original position of column in definition

## A.2.22 USER\_INDEXES

Description of the user's own indexes:

Column Name	Description
INDEX_NAME	Name of the index
INDEX_TYPE	Type of index
TABLE_OWNER	Owner of the indexed object
TABLE_NAME	Name of the indexed object
TABLE_TYPE	Type of the indexed object
UNIQUENESS	Uniqueness status of the index
COMPRESSION	N/A
PREFIX_LENGTH	0
TABLESPACE_NAME	Name of the tablespace containing the index
INI_TRANS	N/A
MAX_TRANS	N/A
INITIAL_EXTENT	N/A
NEXT_EXTENT	N/A
MIN_EXTENTS	N/A
MAX_EXTENTS	N/A
PCT_INCREASE	N/A
PCT_THRESHOLD	Threshold percentage of block space permitted per index entry
INCLUDE_COLUMN	Column ID of the last column to be included in index-organized table
FREELISTS	Number of process freelists allocated to this segment
FREELIST_GROUPS	Number of freelist groups allocated to this segment
PCT_FREE	N/A
LOGGING	Logging information
BLEVEL	Depth of the index from its root block to its leaf blocks. A depth of 1 indicates that the root and leaf block are the same.
LEAF_BLOCKS	Number of leaf blocks in the index
DISTINCT_KEYS	Number of distinct indexed values. For indexes that enforce UNIQUE and PRIMARY KEY constraints, this value is the same as the number of rows in the table.
AVG_LEAF_BLOCKS_PER_KEY	N/A
AVG_DATA_BLOCKS_PER_KEY	N/A
CLUSTERING_FACTOR	N/A
STATUS	State of the indexes: VALID
NUM_ROWS	Number of rows in the index
SAMPLE_SIZE	Size of the sample used to analyze the index
LAST_ANALYZED	Date on which this index was most recently analyzed
DEGREE	Number of threads per instance for scanning the index

Column Name	Description
INSTANCES	Number of instances across which the index is to be scanned
PARTITIONED	Whether this index is partitioned
TEMPORARY	Whether the index is on a temporary table
GENERATED	Whether the name of the index is system generated
SECONDARY	N/A
BUFFER_POOL	Whether the index is a secondary object
USER_STATS	N/A
DURATION	N/A
PCT_DIRECT_ACCESS	N/A
ITYP_OWNER	N/A
ITYP_NAME	N/A
PARAMETERS	N/A
GLOBAL_STATS	N/A
DOMIDX_STATUS	N/A
DOMIDX_OPSTATUS	N/A
FUNCIDX_STATUS	N/A
JOIN_INDEX	N/A
IOT_REDUNDANT_PKEY_ELIM	N/A

### A.2.23 USER\_OBJECTS

Objects owned by the user:

Column Name	Description
OBJECT_NAME	Name of object
SUBOBJECT_NAME	Name of the subobject
OBJECT_ID	Object number of the object
DATA_OBJECT_ID	Dictionary object number of the segment that contains the object
OBJECT_TYPE	Type of object
CREATED	N/A
LAST_DDL_TIME	N/A
TIMESTAMP	N/A
STATUS	State of the object: VALID
TEMPORARY	Whether the object is temporary
GENERATED	Was the name of this object system generated?
SECONDARY	N/A

### A.2.24 USER\_SYNONYMS

The user's private synonyms:

Column Name	Description
SYNONYM_NAME	Name of the synonym
TABLE_OWNER	Owner of the object referenced by the synonym
TABLE_NAME	Name of the object referenced by the synonym
DB_LINK	N/A

## A.2.25 USER\_TABLES

Description of the user's own tables:

Column Name	Description
TABLE_NAME	Name of the table
TABLESPACE_NAME	Name of the tablespace containing the table
CLUSTER_NAME	N/A
IOT_NAME	Name of the index organized table
PCT_FREE	N/A
PCT_USED	N/A
INI_TRANS	N/A
MAX_TRANS	N/A
INITIAL_EXTENT	N/A
NEXT_EXTENT	N/A
MIN_EXTENTS	N/A
MAX_EXTENTS	N/A
PCT_INCREASE	N/A
FREELISTS	Number of process freelists allocated to this segment
FREELIST_GROUPS	Number of freelist groups allocated to this segment
LOGGING	Logging information
BACKED_UP	N/A
NUM_ROWS	Number of rows in the table
BLOCKS	N/A
EMPTY_BLOCKS	N/A
AVG_SPACE	N/A
CHAIN_CNT	N/A
AVG_ROW_LEN	Average length of a row in the table in bytes
AVG_SPACE_FREELIST_BLOCKS	The average freespace of all blocks on a freelist
NUM_FREELIST_BLOCKS	The number of blocks on the freelist
DEGREE	The number of threads per instance for scanning the table
INSTANCES	The number of instances across which the table is to be scanned
CACHE	Whether the cluster is to be cached in the buffer cache

Column Name	Description
TABLE_LOCK	Whether table locking is enabled or disabled
SAMPLE_SIZE	Sample size used in analyzing this table
LAST_ANALYZED	Date on which this table was most recently analyzed
PARTITIONED	Indicates whether this table is partitioned
IOT_TYPE	If this is an index organized table
TEMPORARY	Can the current session only see data that it placed in this object itself?
SECONDARY	N/A
NESTED	If the table is a nested table
BUFFER_POOL	The default buffer pool for the object
ROW_MOVEMENT	N/A
GLOBAL_STATS	N/A
USER_STATS	N/A
DURATION	N/A
SKIP_CORRUPT	N/A
MONITORING	N/A
CLUSTER_OWNER	N/A
DEPENDENCIES	N/A
COMPRESSION	N/A

### A.2.26 USER\_TAB\_COLUMNS

Columns of user's tables, views, and clusters:

Column Name	Description
TABLE_NAME	Table, view, or cluster name
COLUMN_NAME	Column name
DATA_TYPE	data type of column
DATA_TYPE_MOD	data type modifier of the column
DATA_TYPE_OWNER	Owner of the data type of the column
DATA_LENGTH	Maximum length of the column in bytes
DATA_PRECISION	N/A
DATA_SCALE	Digits to the right of decimal point in a number
NULLABLE	Does the column permit nulls? Value is <i>n</i> if there is a NOT NULL constraint on the column or if the column is part of a PRIMARY key.
COLUMN_ID	Sequence number of the column as created
DEFAULT_LENGTH	N/A
DATA_DEFAULT	N/A
NUM_DISTINCT	Number of distinct values in each column of the table

Column Name	Description
LOW_VALUE	For tables with more than three rows, the second lowest and second highest values. These statistics are expressed in hexadecimal notation for the internal representation of the first 32 bytes of the values.
HIGH_VALUE	N/A
DENSITY	N/A
NUM_NULLS	The number of nulls in the column
NUM_BUCKETS	The number of buckets in histogram for the column
LAST_ANALYZED	The date on which this column was most recently analyzed
SAMPLE_SIZE	The sample size used in analyzing this column
CHARACTER_SET_NAME	The name of the character set
CHAR_COL_DECL_LENGTH	The length of the character set
GLOBAL_STATS	N/A
USER_STATS	N/A
AVG_COL_LEN	Average length of the column (in bytes)
CHAR_LENGTH	Displays the length of the column in characters
CHAR_USED	N/A

### A.2.27 USER\_TAB\_COMMENTS

Comments on the tables and views owned by the user:

Column Name	Description
TABLE_NAME	Name of the object
TABLE_TYPE	Type of object
COMMENTS	Comments on the object

### A.2.28 USER\_USERS

Information about the current user:

Column Name	Description
USERNAME	Name of the user
USER_ID	N/A
ACCOUNT_STATUS	Indicates if the account is locked, expired or unlocked
LOCK_DATE	Date the account was locked
EXPIRE_DATE	Date of expiration of the account
DEFAULT_TABLESPACE	N/A
TEMPORARY_TABLESPACE	N/A
CREATED	N/A
EXTERNAL_NAME	User external name

## A.2.29 USER\_VIEWS

Text of views owned by the user:

Column Name	Description
VIEW_NAME	Name of the view
TEXT_LENGTH	Length of the view text
TEXT	First line of the view text
TYPE_TEXT_LENGTH	Length of the type clause of the typed view
TYPE_TEXT	Type clause of the typed view
OID_TEXT_LENGTH	Length of the WITH OID clause of the typed view
OID_TEXT	WITH OID clause of the typed view
VIEW_TYPE_OWNER	Owner of the type of the view if the view is a typed view
VIEW_TYPE	Type of the view if the view is a typed view
SUPERVIEW_NAME	N/A





---

---

## Sample Files

This appendix contains sample files of gateway initialization and Oracle Net tnsnames.ora and listener.ora files.

- [Sample gateway initialization file](#) on page B-1
- [Sample Oracle Net tnsnames.ora File](#) on page B-2
- [Sample Oracle Net listener.ora File](#) on page B-2

### B.1 Sample gateway initialization file

The following sample gateway initialization file (inithoa1.ora) needs customization. For information on customizing this file, refer to ["Configuring the Host"](#) on page 10-3 in [Chapter 10, "Configuring the Gateway"](#). Also, refer to [Appendix C](#).

```
#
# HS specific parameters
#
FDS_CLASS=TG4DRDA_DB2MVS
#TRACE_LEVEL=255
#LOG_DESTINATION=DB2.log
#ORACLE_DRDA_TCTL=debug.tctl
HS_COMMIT_POINT_STRENGTH=255
HS_NLS_DATE_FORMAT=YYYY-MM-DD
HS_LANGUAGE=AMERICAN_AMERICA.WE8ISO8859P1
HS_RPC_FETCH_REBLOCKING=off
HS_RPC_FETCH_SIZE=32767
HS_FDS_FETCH_ROWS=20
#
# DRDA specific parameters
#
DRDA_CONNECT_PARM=DRDAON1
DRDA_REMOTE_DB_NAME=DB2V7R1
DRDA_PACKAGE_COLLID=ORACLE
DRDA_PACKAGE_NAME=G2DRSQL
DRDA_PACKAGE_CONSTOKEN=A92617CB3FE54701
DRDA_RECOVERY_USERID=ORADRDA
DRDA_RECOVERY_PASSWORD=ORADRDA
DRDA_ISOLATION_LEVEL=CS
#DRDA_PACKAGE_OWNER=ORADRDA
#DRDA_DISABLE_CALL=TRUE
```

## B.2 Sample Oracle Net tnsnames.ora File

For information on tailoring the tnsnames.ora file for the gateway, refer to the instructions for "[Configuring Oracle Net](#)" on page 9-3.

```
ipc-ora=(DESCRIPTION=
  (ADDRESS=
    (PROTOCOL=IPC)
    (KEY=ORCL)
  )
  (CONNECT_DATA=(SID=ORA102))
  (HS=)
)
ipc-gw=(DESCRIPTION=
  (ADDRESS=
    (PROTOCOL=IPC)
    (KEY=ORCL)
  )
  (CONNECT_DATA=(SID=drdahoal))
  (HS=)
)
)
```

## B.3 Sample Oracle Net listener.ora File

For information on tailoring the listener.ora file for the gateway, refer to the instructions in "[Configuring Oracle Net](#)" on page 9-3.

```
#
# Sample listener.ora file for the Transparent Gateway for IBM DRDA
# Version Date: Jan-01-2002
# Filename: Listener.ora
#
LISTENER =
  (ADDRESS_LIST =
    (ADDRESS= (PROTOCOL= IPC) (KEY= ORCL))
  )

SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC=
      (SID_NAME=drdahoal)
      (ORACLE_HOME=C:\Oracle\GTWHome)
      (PROGRAM=g4drsrv)
    )
  )

STARTUP_WAIT_TIME_LISTENER = 0
INBOUND_CONNECT_TIMEOUT_LISTENER = 10
TRACE_LEVEL_LISTENER = OFF
```

This sample listener.ora file resides in the `ORACLE_HOME\network\admin` directory. If the listener uses the Oracle Net TCP/IP adapter instead of the IPC adapter, then replace these lines under the `LISTENER` keyword:

```
(ADDRESS=
  (PROTOCOL=IPC)
  (KEY=ORCL)
```

```
with  
    )  
    (ADDRESS=  
      (PROTOCOL=TCP)  
      (HOST=your_IP_node_name)  
      (PORT=your_port_number)  
    )
```



---

---

## DRDA-Specific Parameters

This appendix contains the DRDA-specific parameters defined in the gateway initialization file. Read and understand the information on each parameter, taking special note of parameters that have defaults that do not apply to your system.

This appendix contains the following sections:

- [Modifying the Gateway Initialization File](#) on page C-1
- [Setting Parameters in the Gateway Initialization File](#) on page C-1
- [Syntax and Usage](#) on page C-1
- [Gateway Initialization File Parameters](#) on page C-2

### C.1 Modifying the Gateway Initialization File

If you change any parameters in the gateway initialization file, then you must stop and restart the gateway in order for them to take effect. If you change certain parameters, then you must also rebind the DRDA package. Any parameters that affect the DRDA package have a note in their description that rebinding is required.

### C.2 Setting Parameters in the Gateway Initialization File

Parameters specific to the gateway are stored in the gateway initialization file, *initsid.ora*.

### C.3 Syntax and Usage

Parameters and their values are specified according to the syntax rules put forth by heterogeneous services. The general form is:

```
[set] [private] drda_parameter = drda_parameter_value
```

where:

- *drda\_parameter* is one of the DRDA parameters
- *drda\_parameter\_value* is a character string with contents dependent on the *drda\_parameter*

The *set* and *private* keywords are optional and have the following effect. If the *set* keyword is present, then the parameter and its value will be pushed into the process environment. If the *private* keyword is present, then the parameter and its value will not be uploaded to the Oracle server. In general, Oracle recommends that the

`private` keyword not be used unless the parameter contains sensitive information (a user ID or password, for example).

For further information on heterogeneous services and initialization parameters, see the section "Setting Initialization Parameters" in the *Oracle Database Heterogeneous Connectivity Administrator's Guide*.

## C.4 Gateway Initialization File Parameters

Following is a list of gateway-specific initialization file parameters and their descriptions. In addition to these parameters, generic Heterogeneous Services initialization file parameters may be set. Refer to the *Oracle Database Heterogeneous Connectivity Administrator's Guide* for a list of additional parameters.

### C.4.1 DRDA\_CACHE\_TABLE\_DESC

**Default value:** TRUE

**Range of values:** {TRUE|FALSE}

**Syntax:** DRDA\_CACHE\_TABLE\_DESC={TRUE|FALSE}

DRDA\_CACHE\_TABLE\_DESC directs the gateway to cache table descriptions once per transaction. This can reduce the number of table lookups requested of the DRDA Server by Oracle and can speed up processing of SQL statements. You may wish to turn this option off if you will be altering the structure of a remote table and if you will be examining it within the same transaction.

### C.4.2 DRDA\_CAPABILITY

**Default value:** none

**Range of values:** Refer to [Native Semantics](#) on page 12-18

**Syntax:** DRDA\_CAPABILITY={FUNCTION/{ON|OFF}}, . . .

DRDA\_CAPABILITY specifies which Oracle mapped functions will be treated natively. In other words, no special preprocessing or postprocessing will be done for these functions. They will be passed to the DRDA Server unmodified.

### C.4.3 DRDA\_CODEPAGE\_MAP

**Default value:** codepage.map

**Range of values:** any valid file path

**Syntax:** DRDA\_CODEPAGE\_MAP=*codepage.map*

DRDA\_CODEPAGE\_MAP specifies the location of the codepage map. You may specify only the file name, which will be searched for within the `ORACLE_HOME\tg4drda\admin` directory, or you may specify the full path name of the file.

### C.4.4 DRDA\_COMM\_BUFLLEN

**Default value:** 32767

**Range of values:** 512 through 32767

**Syntax:** DRDA\_COMM\_BUFLLEN=*num*

DRDA\_COMM\_BUFLLEN specifies the communications buffer length. This is a number indicating the size of the SNA send/receive buffer in bytes.

#### C.4.5 DRDA\_CONNECT\_PARM (SNA format)

**Default value:** DRDACON1

**Range of values:** any alphanumeric string 1 to 8 characters in length

**Syntax:** RDA\_CONNECT\_PARM=*name*

DRDA\_CONNECT\_PARM specifies the Side Information name. Refer to [Chapter 6, "Configuring Microsoft SNA Server or Host Integration Server"](#) and [Chapter 7, "Configuring IBM Communication Server"](#) for details.

#### C.4.6 DRDA\_CONNECT\_PARM (TCP/IP format)

**Default value:** DRDACON1:446

**Range of values:** Any alphanumeric string 1 to 255 characters in length

**Syntax:** DRDA\_CONNECT\_PARM={*hostname/ip\_address*}{:*port*}

DRDA\_CONNECT\_PARM specifies the TCP/IP host name or IP Address of the DRDA Server and, as an option, the Service Port number on which the DRDA Server is listening. For more information about the port number, refer to ["Port Number"](#) on page 8-1.

#### C.4.7 DRDA\_CMSRC\_CM\_IMMEDIATE

**Default value:** FALSE

**Range of values:** {TRUE |FALSE}

**Syntax:** DRDA\_CMSRC\_CM\_IMMEDIATE={*TRUE*/*FALSE*}

DRDA\_CMSRC\_CM\_IMMEDIATE sets the SNA session allocation mode. A setting of FALSE will cause the gateway to wait for a free session if no free sessions exist. A setting of TRUE will cause the gateway to fail the allocation immediately if no free sessions exist.

#### C.4.8 DRDA\_DEFAULT\_CCSID

**Default value:** none

**Range of values:** any supported DRDA Server CCSID

**Syntax:** DRDA\_DEFAULT\_CCSID=*ccsid*

DRDA\_DEFAULT\_CCSID specifies the default CCSID or character set code page for character set conversions when the DRDA Server database indicates that a character string has a CCSID of 65535. DRDA Servers use CCSID 65535 for columns specified as "FOR BIT DATA". In most cases, this parameter should not be specified, permitting CCSID 65535 to be treated as an Oracle RAW data type.

This parameter is for supporting databases (in particular, DB2/400) that use CCSID 65535 as the default for all tables created. Permitting CCSID 65535 to be treated as another CCSID can save such sites from having to modify every table.

---

---

**WARNING:** Specifying any value for `DRDA_DEFAULT_CCSD` causes all "FOR BIT DATA" columns to be handled as text columns that need character set conversion and, therefore, any truly binary data in these columns can encounter conversion errors (ORA-28527).

---

---

### C.4.9 DRDA\_DESCRIBE\_TABLE

**Default value:** TRUE

**Range of values:** {TRUE | FALSE}

**Syntax:** `DRDA_DESCRIBE_TABLE={TRUE|FALSE}`

`DRDA_DESCRIBE_TABLE` directs the gateway to use the DRDA operation "Table Describe" to return the description of tables. This is an optimization that reduces the amount of time and resources that are used to look up the definition of a table.

---

---

**Note:** This feature is not compatible with DB2 aliases or Synonyms. If you will be using DB2 aliases, then be sure this option is not enabled.

---

---

### C.4.10 DRDA\_DISABLE\_CALL

**Default value:** TRUE

**Range of values:** {TRUE | FALSE}

**Syntax:** `DRDA_DISABLE_CALL={TRUE|FALSE}`

`DRDA_DISABLE_CALL` controls stored procedure usage, and it is also used to control how the package is bound on the target database. This parameter should be set to FALSE only for supported target DRDA servers and should be set to TRUE otherwise. See [Section 2.5.1, "DB2 Considerations"](#) for supported target servers.

---

---

**Rebinding Required:** Any change to this parameter requires you to rebind.

---

---

### C.4.11 DRDA\_FLUSH\_CACHE

**Default value:** SESSION

**Range of values:** {SESSION | COMMIT}

**Syntax:** `DRDA_FLUSH_CACHE={SESSION|COMMIT}`

`DRDA_FLUSH_CACHE` specifies when the cursor cache is to be flushed. With `DRDA_FLUSH_CACHE=COMMIT`, the cursor cache is flushed whenever the transaction is committed. With `DRDA_FLUSH_CACHE=SESSION`, the cache is not flushed until the session terminates.

### C.4.12 DRDA\_GRAPHIC\_PAD\_SIZE

**Default value:** 0

**Range of values:** 0 through 127

**Syntax:** `DRDA_GRAPHIC_PAD_SIZE=num`



DRDA\_GRAPHIC\_PAD\_SIZE is used to pad the size of a Graphic column as described by the DRDA Server. This is sometimes necessary depending on the character set of the DRDA database and the Oracle database. If the Oracle database is based on EBCDIC and the DRDA database is based on ASCII, then a pad size of 2 may be needed.

### C.4.13 DRDA\_GRAPHIC\_LIT\_CHECK

**Default value:** FALSE

**Range of values:** {TRUE|FALSE}

**Syntax:** DRDA\_GRAPHIC\_LIT\_CHECK={TRUE|FALSE}

DRDA\_GRAPHIC\_LIT\_CHECK directs the gateway to evaluate string literals within INSERT SQL statements to determine if they need to be converted to double-byte format for insertion into a Graphic column at the DRDA Server database. This is done by querying the column attributes of the table in the SQL statement to determine if a string literal is being applied to a column with a Graphic data type. If the table column is Graphic, and if this parameter is TRUE, then the gateway will rewrite the SQL statement with the literal converted to double-byte format. Existing double-byte characters in the string will be preserved, and all single-byte characters will be converted to double-byte characters.

### C.4.14 DRDA\_GRAPHIC\_TO\_MBCS

**Default value:** FALSE

**Range of values:** {TRUE|FALSE}

**Syntax:** DRDA\_GRAPHIC\_TO\_MBCS={TRUE|FALSE}

DRDA\_GRAPHIC\_TO\_MBCS directs the gateway to convert Graphic data that has been fetched from the DRDA Server into Oracle multibyte data, translating double-byte characters into single-byte characters where possible.

### C.4.15 DRDA\_GRAPHIC\_CHAR\_SIZE

**Default value:** 4

**Range of values:** 1 through 4

**Syntax:** DRDA\_GRAPHIC\_CHAR\_SIZE=num

DRDA\_GRAPHIC\_CHAR\_SIZE is used to define the character conversion size to be used for GRAPHIC data types. It is a tuning parameter which affects the maximum size of a GRAPHIC data type when the column is described.

### C.4.16 DRDA\_ISOLATION\_LEVEL

**Default value:** CHG for DB2/400, CS for DB2/OS390, DB2/UDB, DB2/VM

**Range of values:** {CHG|CS|RR|ALL|NC}

**Syntax:** DRDA\_ISOLATION\_LEVEL={CHG|CS|RR|ALL|NC}

DRDA\_ISOLATION\_LEVEL specifies the isolation level that is defined to the package when it is created. All SQL statements that are sent to the remote DRDA database are run with this isolation level. Isolation level seriously affects performance of applications. Use caution when specifying an isolation level other than the default. For information on isolation levels, refer to IBM database manuals.

The following table lists isolation levels and their descriptions. The levels are specified in ascending order of control, with CHG having the least reliable cursor stability and RR having the most. Note that higher stability uses more resources on the server and can lock those resources for extended periods.

**Table C-1 Isolation Levels and Their Descriptions**

Level	Description
CHG	Change (default for DB2/400)
CS	Cursor Stability (default for DB2/UDB, DB2/OS390, and DB2/VM)
RR	Repeatable Read
ALL	ALL
NC	No Commit

---



---

**Rebinding Required:** Any change to this parameter requires you to rebind.

---



---

#### C.4.17 DRDA\_LOCAL\_NODE\_NAME

**Default value:** AIX\_RS6K

**Range of values:** any alphanumeric string 1 to 8 characters in length

**Syntax:** DRDA\_LOCAL\_NODE\_NAME=*name*

DRDA\_LOCAL\_NODE\_NAME specifies the name by which the gateway will be known to the DRDA Server. This name is used internally by the DRDA Server to identify the local node.

#### C.4.18 DRDA\_MBCS\_TO\_GRAPHIC

**Default value:** FALSE

**Range of values:** {TRUE | FALSE}

**Syntax:** DRDA\_MBCS\_TO\_GRAPHIC={ *TRUE* / *FALSE* }

DRDA\_MBCS\_TO\_GRAPHIC directs the gateway to convert multibyte data (that has been sent from Oracle to the DRDA database) into pure double-byte characters. This parameter is primarily intended to be used with bind variables to ensure that the data is properly formatted and will therefore be acceptable to the DRDA Server. It applies only to INSERT SQL statements that are using bind variables. When used in combination with the DRDA\_GRAPHIC\_LIT\_CHECK parameter, this parameter can help ensure that data that is being inserted into a Graphic column is handled correctly by the target DRDA Server.

#### C.4.19 DRDA\_OPTIMIZE\_QUERY

**Default value:** TRUE

**Range of values:** {TRUE | FALSE}

**Syntax:** DRDA\_OPTIMIZE\_QUERY={ *TRUE* / *FALSE* }

DRDA\_OPTIMIZE\_QUERY turns on or off the distributed query optimizer (DQO) capability. Refer to [Performing Distributed Queries](#) on page 11-4 in [Chapter 11, "Using](#)

the Gateway". The DQO capability is useful for optimizing queries that access large amounts of data, but it can add overhead to small queries.

This parameter is valid only if the DRDA Server is DB2/OS390 or DB2/VM. If the DRDA Server is DB2/400 or DB2/UDB, then you must set the value to `FALSE`.

#### C.4.20 DRDA\_PACKAGE\_COLLID

**Default value:** ORACLE

**Range of values:** an alphanumeric string 1 to 18 characters in length

**Syntax:** DRDA\_PACKAGE\_COLLID=*collection\_id*

DRDA\_PACKAGE\_COLLID specifies the package collection ID. Note that in DB2/400, the collection ID is actually the name of an AS/400 library.

---



---

**Rebinding Required:** Any change to this parameter requires you to rebind the package.

---



---

#### C.4.21 DRDA\_PACKAGE\_CONSTOKEN

**Default value:** none, use the sample provided

**Range of values:** a 16-digit hexadecimal number

**Syntax:** DRDA\_PACKAGE\_CONSTOKEN=*hexnum*

DRDA\_PACKAGE\_CONSTOKEN specifies the package consistency token. This is a 16-digit hexadecimal representation of an 8-byte token. Oracle Corporation recommends that you do not change the consistency token. The consistency token used at run time must match the one used when the package is bound. The value depends on the DRDA Server being used.

---



---

**Rebinding Required:** Any change to this parameter requires you to rebind the package.

---



---

#### C.4.22 DRDA\_PACKAGE\_NAME

**Default value:** G2DRSQL

**Range of values:** an alphanumeric string 1 to 18 characters in length

**Syntax:** DRDA\_PACKAGE\_NAME=*name*

DRDA\_PACKAGE\_NAME specifies the package name. Note that the package is stored in the DRDA Server under this name as a SQL resource. Refer to the DRDA Server documentation for length limitations on package names. Many typical implementations restrict the length to 8 characters.

---



---

**Rebinding Required:** Any change to this parameter requires that you rebind the package.

---



---

#### C.4.23 DRDA\_PACKAGE\_OWNER

**Default value:** none

**Range of values:** any valid user ID

**Syntax:** DRDA\_PACKAGE\_OWNER=*userid*

DRDA\_PACKAGE\_OWNER specifies the database user ID that owns the package. This enables the owner to be a user other than the connected user ID when the package is created. The package owner must be the same user as the owner of the ORACLE2PC table. This is not valid for DB2/VM.

---

---

**Rebinding Required:** Any change to this parameter requires you to rebind the package.

---

---

## C.4.24 DRDA\_PACKAGE\_SECTIONS

**Default value:** 100

**Range of values:** any integer between 1 and 65535

**Syntax:** DRDA\_PACKAGE\_SECTIONS=*num*

DRDA\_PACKAGE\_SECTIONS specifies the number of cursors declared at the remote database when the package is bound. This is the maximum number of open cursors permitted at any one time. Change this parameter only if an application needs more than 100 open concurrent cursors.

---

---

**Rebinding Required:** Any change to this parameter requires you to rebind the package.

---

---

## C.4.25 DRDA\_READ\_ONLY

**Default value:** FALSE

**Range of values:** {TRUE | FALSE}

**Syntax:** DRDA\_READ\_ONLY={*TRUE* | *FALSE*}

DRDA\_READ\_ONLY specifies whether the gateway runs in a read-only transaction mode. In this mode, SQL statements which modify data are not permitted.

## C.4.26 DRDA\_RECOVERY\_PASSWORD

**Default value:** none

**Range of values:** any valid password

**Syntax:** DRDA\_RECOVERY\_PASSWORD=*passwd*

DRDA\_RECOVERY\_PASSWORD is used with the DRDA\_RECOVERY\_USERID parameter. The recovery user connects to the IBM database if a distributed transaction is in doubt. For more information, refer to ["Two-Phase Commit Processing"](#) on page 11-5. Also refer to [Chapter 13, "Security Considerations"](#) for information about security and about encrypting passwords.

## C.4.27 DRDA\_RECOVERY\_USERID

**Default value:** ORARECOV

**Range of values:** any valid user ID

**Syntax:** DRDA\_RECOVERY\_USERID=*userid*

DRDA\_RECOVERY\_USERID specifies the user ID that is used by the gateway if a distributed transaction is in doubtful state. This user ID must have execute privileges on the package and must be defined to the IBM database.

If a distributed transaction is in doubtful state, then the Oracle integrating server determines the status of the transaction by connecting to the IBM database, using the DRDA\_RECOVERY\_USERID. If this parameter is missing, the gateway attempts to connect to a user ID of ORARECOV. For more information, refer to ["Two-Phase Commit Processing"](#) on page 11-5.

#### C.4.28 DRDA\_REMOTE\_DB\_NAME

**Default value:** DB2V2R3

**Range of values:** an alphanumeric string 1 to 18 characters in length

**Syntax:** DRDA\_REMOTE\_DB\_NAME=*name*

DRDA\_REMOTE\_DB\_NAME specifies the DRDA Server location name. This is an identifying name that is assigned to the server for DRDA purposes. A technique for determining this name by using a SQL SELECT statement is discussed in each of the server-specific installation sections in [Chapter 5, "Configuring the DRDA Server"](#).

#### C.4.29 DRDA\_SECURITY\_TYPE

**Default value:** PROGRAM

**Range of values:** {PROGRAM|SAME}

**Syntax:** DRDA\_SECURITY\_TYPE={ *PROGRAM* / *SAME* }

DRDA\_SECURITY\_TYPE specifies the type of security used for SNA communications. For more information about types of security and about setting DRDA\_SECURITY\_TYPE, refer to [Chapter 13, "Security Considerations"](#). Also refer to Chapter 15 for information about security and encrypting passwords.

#### C.4.30 FDS\_CLASS

**Default value:** TG4DRDA\_DB2MVS

**Range of values:** Refer to the list below for valid values

**Syntax:** FDS\_CLASS=*TG4DRDA\_DB2MVS*

FDS\_CLASS specifies the capability classification used by the Oracle Database server and the gateway. These values might change from release to release, depending on whether the gateway capabilities change.

**The valid default values for FDS\_CLASS are as follows:**

**For a DB2/OS390 database:** TG4DRDA\_DB2MVS

**For a DB2/VM database:** TG4DRDA\_DB2VM

**For a DB2/400 database:** TG4DRDA\_DB2400

**For a DB2/UDB database:** TG4DRDA\_DB2UDB

#### C.4.31 FDS\_CLASS\_VERSION

**Default value:** 10.1.0.2.0

**Range of values:** 10.1.0.2.0

**Syntax:** FDS\_CLASS\_VERSION=1

FDS\_CLASS\_VERSION specifies the version of the FDS\_CLASS capabilities. Do not specify this parameter unless directed to do so by Oracle Support Services.

### C.4.32 FDS\_INSTANCE

**Default value:** DRD1

**Range of values:** the name of the gateway SID

**Syntax:** FDS\_INSTANCE=*drdahoa1*

FDS\_INSTANCE specifies a subset of the FDS\_CLASS capabilities that may be modified by the user, based on initialization file parameters. If you do not specify this parameter, then its value will be the Oracle SID that is defined in the TNS Listener entry.

### C.4.33 HS\_FDS\_FETCH\_ROWS

**Default value:** 20

**Range of values:** any integer between 1 and 1000

**Syntax:** HS\_FDS\_FETCH\_ROWS=*num*

HS\_FDS\_FETCH\_ROWS specifies the fetch array size. This is the number of rows to fetch at one time from the DRDA Server and to return to the Oracle Database server. This parameter will be affected by the HS\_RPC\_FETCH\_SIZE and HS\_RPC\_FETCH\_REBLOCKING parameters. For further information on these parameters, refer to the section "Controlling the Array Fetch Between Agent and Non-Oracle Database server" in the *Oracle Database Heterogeneous Connectivity Administrator's Guide*.

### C.4.34 HS\_LANGUAGE

**Default value:** none

**Range of values:** any valid language specification

**Syntax:** HS\_LANGUAGE=*language[\_territory.character\_set]*

HS\_LANGUAGE specifies the language and the character set that the gateway will use to interact with the DRDA Server. Care must be taken in choosing the value of these parameters, especially when the gateway will be accessing GRAPHIC data. For additional details, refer to [Appendix D, "National Language Support"](#) and to the *Oracle Database Heterogeneous Connectivity Administrator's Guide*.

### C.4.35 HS\_NLS\_NCHAR

**Default value:** none

**Range of values:** any valid character set specification

**Syntax:** HS\_NLS\_NCHAR=*character\_set*

HS\_NLS\_NCHAR specifies the character set that the gateway will use to interact with the DRDA Server when accessing GRAPHIC data. Set this parameter to the same value as the character set component of the HS\_LANGUAGE parameter. For additional details, refer to [Appendix D, "National Language Support"](#) and to the *Oracle Database Heterogeneous Connectivity Administrator's Guide*.

### C.4.36 LOG\_DESTINATION

**Default value:** `ORACLE_HOME\tg4drda\log\gateway sid_pid.log`

**Range of values:** any valid file path

**Syntax:** `LOG_DESTINATION=logpath`

LOG\_DESTINATION specifies the destination for gateway logging and tracing. This parameter should specify a file. If the file already exists, then it will be overwritten.

After any failure to open the log path, a second attempt to open the default is made.

Usually, LOG\_DESTINATION should specify a directory. If it is specified as a file and if two or more users simultaneously use the same instance of the gateway, then they are writing to the same log. The integrity of this log is not guaranteed. If you do not specify this parameter, then the default is assumed.

### C.4.37 ORA\_MAX\_DATE

**Default value:** `4712-12-31`

**Range of values:** any valid date less than 4712-12-31

**Syntax:** `ORA_MAX_DATE=yyyy-mm-dd`

ORA\_MAX\_DATE specifies the gateway maximum date value. If the fetched date value is larger than 4712-12-31, then the gateway replaces the date value with the value defined by the ORA\_MAX\_DATE parameter. Any date between January 1, 4712 BC and December 31, 4712 AD is valid.

### C.4.38 ORA\_NLS10

**Default value:** `ORACLE_HOME\nls\data`

**Range of values:** any valid NLS directory path

**Syntax:** `SET ORA_NLS10=nlspath`

ORA\_NLS10 specifies the directory to which the gateway loads its character sets and other language data. Normally, this parameter does not need to be set. Some configurations, however, may require that it be set.

### C.4.39 ORACLE\_DRDA\_TCTL

**Default value:** none

**Range of values:** any valid file path

**Syntax:** `ORACLE_DRDA_TCTL=tracecontrolpath`

ORACLE\_DRDA\_TCTL specifies the path to the DRDA internal trace control file. This file contains module tracing commands. A sample file is stored in `ORACLE_HOME\tg4drda\admin\debug.tctl`. This parameter is used for diagnostic purposes.

### C.4.40 ORACLE\_DRDA\_TRACE

**Default value:** value specified for LOG\_DESTINATION

**Range of values:** any valid file path

**Syntax:** `ORACLE_DRDA_TRACE=logpath`

ORACLE\_DRDA\_TRACE is used to specify a different log path for DRDA internal tracing. This tracing is separate from the rest of the gateway tracing, as specified by the LOG\_DESTINATION parameter. By default, this parameter will append the DRDA internal trace to the gateway trace. This parameter is used for diagnostic purposes.

#### **C.4.41 TRACE\_LEVEL**

**Default Value:** 0

**Range of values:** 0-255

**Syntax:** TRACE\_LEVEL=*number*

TRACE\_LEVEL specifies a code tracing level. This value determines the level of detail which is logged to the gateway log file during processing. This parameter is primarily used for diagnostics.



---

---

# National Language Support

This appendix documents the National Language Support (NLS) information for the Oracle Transparent Gateway for DRDA. This supplements the general Oracle NLS information found in the *Oracle Database Application Developer's Guide - Fundamentals*.

National Language Support enables users to interact with Oracle applications in their native language, using their conventions for displaying data. The Oracle NLS architecture is data-driven, enabling support for specific languages and character encoding schemes to be added without any changes in source code.

There are a number of different settings in the gateway, DRDA Server, Oracle Database 10g server, and client that affect NLS processing. In order for translations to take place correctly, character settings of these components must be compatible.

This appendix contains the following sections:

- [Overview of NLS Interactions](#)
- [Client and Oracle Integrating Server Configuration](#)
- [Gateway Language Interaction with DRDA Server](#)
- [Gateway Codepage Map Facility](#)
- [Multibyte and Double-Byte Support in the Gateway](#)
- [Message Availability](#)
- [Example of NLS Configuration](#)

## D.1 Overview of NLS Interactions

[Figure D-1](#) illustrates NLS interactions within your system, including each component of your system and the parameters of each component that affect NLS processing in a distributed environment. [Table D-1](#) describes the architecture illustrated in [Figure D-1](#).

**Figure D-1 Architecture of NLS Interactions with Your System Components**

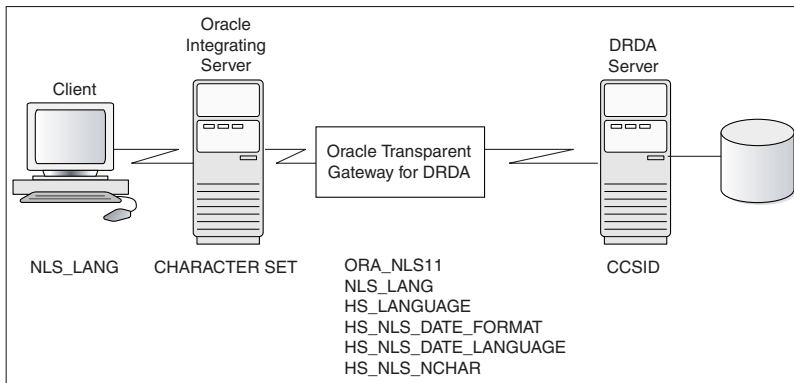


Table D-1 describes in detail the parameters and variables needed for NLS processing within each of your system environments: the client environment, the Oracle integrating server, the gateway, and the DRDA Server.

**Table D-1 Parameters Needed for NLS Processing in Your System Environments**

Environment	Parameter or Variable	Description
Client	NLS_LANG	An environmental variable. NLS_LANG sets the NLS environment that is used by the database, both for the server session and for the client application. This ensures that the language environments of both database and client application are automatically the same. Because NLS_LANG is an environment variable, it is read by the client applications at startup time. The client communicates the information defined in NLS_LANG to the server when it connects. Refer to "Client and Oracle Integrating Server Configuration" on page D-3 for detailed information.
Oracle integrating server	CHARACTER SET	This option is set during creation of the database. CHARACTER SET determines the character encoding scheme that is used by the database. CHARACTER SET is defined at database creation in the CREATE DATABASE statement. All data columns of type CHAR, VARCHAR2, and LONG have their data stored in the database character set. Refer to "Client and Oracle Integrating Server Configuration" on page D-3 for detailed information.
Oracle Transparent Gateway for DRDA	ORA_NLS11	An environmental variable. ORA_NLS11 determines where the gateway loads its character sets and other language data. Refer to "Gateway Language Interaction with DRDA Server" on page D-4 for detailed information.
Oracle Transparent Gateway for DRDA	NLS_LANG	An environmental variable. NLS_LANG defines the character set that is used for communication between the gateway and the Oracle integrating server. Refer to "Gateway Language Interaction with DRDA Server" on page D-4 for detailed information.
Oracle Transparent Gateway for DRDA	HS_LANGUAGE	An initialization parameter HS_LANGUAGE defines the character set that is used for communication between the gateway and the DRDA Server. Refer to "Gateway Language Interaction with DRDA Server" on page D-4 for detailed information.

**Table D-1 (Cont.) Parameters Needed for NLS Processing in Your System Environments**

Environment	Parameter or Variable	Description
Oracle Transparent Gateway for DRDA	HS_NLS_NCHAR	An initialization parameter. HS_NLS_NCHAR defines the NCHAR character set that is used for communications between the gateway and the DRDA Server. This parameter is required when the gateway will be accessing GRAPHIC or multibyte data on the DRDA Server. Set this parameter to the same value as the character set component of the HS_LANGUAGE parameter. For detailed information, refer to <a href="#">"Gateway Language Interaction with DRDA Server"</a> on page D-4.
Oracle Transparent Gateway for DRDA	HS_NLS_DATE_FORMAT	An initialization parameter. HS_NLS_DATE_FORMAT specifies the format for dates that are used by the DRDA Server. Refer to <a href="#">"Gateway Language Interaction with DRDA Server"</a> on page D-4 for detailed information.
Oracle Transparent Gateway for DRDA	HS_NLS_DATE_LANGUAGE	An initialization parameter. HS_NLS_DATE_LANGUAGE specifies the language that is used by the DRDA Server for day and month names, and for date abbreviations. Refer to <a href="#">"Gateway Language Interaction with DRDA Server"</a> on page D-4 for detailed information.
DRDA Server	CCSID	CCSID is the server character set that is mapped in the gateway to the equivalent Oracle character set. The CCSID specifies the character set that the DRDA database uses to store data. It is defined when you create your database. Refer to <a href="#">"Gateway Codepage Map Facility"</a> on page D-5.

## D.2 Client and Oracle Integrating Server Configuration

A number of NLS parameters control NLS processing between the Oracle Database server and client. You can set language-dependent action defaults for the server, and you can set language-dependent action for the client that overrides these defaults. For a complete description of NLS parameters, refer to the NLS chapter in the *Oracle Database Administrator's Guide*. These parameters do not directly affect gateway processing. However, you must ensure that the client character set (which is specified by the Oracle Database server NLS\_LANG environment variable) is compatible with the character sets that you specify on the gateway and on the DRDA Server.

When you create the Oracle Database, the character set that is used to store data is specified by the CHARACTER SET clause of the CREATE DATABASE statement. After the database is created, the database character set cannot be changed unless you re-create the database.

Normally, the default for CHARACTER SET is US7ASCII, which supports only the 26 Latin alphabetic characters. If you have specified 8-bit character sets on the gateway and DRDA Server, then you must have a compatible 8-bit character set defined on your database. To check the character set of an existing database, run the command:

```
SELECT USERENV('LANGUAGE') FROM DUAL;
```

For more information, refer to ["Specifying Character Sets"](#) in the *Oracle Database Administrator's Guide*.

Note that this does not mean that the gateway character set must be the same as the Oracle server character set. The Oracle Net facility will be performing implicit conversion between the Oracle server character set and the gateway character set.

## D.3 Gateway Language Interaction with DRDA Server

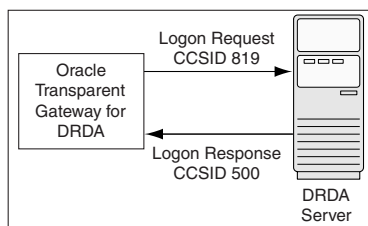
During logon of the gateway to the DRDA Server, initial language information is exchanged between the Gateway and the server. First, the gateway sends to the DRDA Server the CCSID it will be conversing in. In the following example, the Oracle character set "WE8ISO8859P1" is mapped to CCSID 819 (an ASCII Code Page). This CCSID is sent to the DRDA Server. The DRDA Server responds with the CCSID that it will be conversing in. This will be the CCSID with which the DB2 database was generated. Also, in the following example, this is CCSID 500, an EBCDIC code page. [Figure D-2, "Gateway Language Interaction with DRDA Server"](#), illustrates this process.

A DB2 instance will map unknown CCSIDs using the `SYSDIBM.SYSSTRINGS` table (this table has different names for the various DB2 versions). It is possible to add additional character set mappings to this table using DB2 utilities. Please refer to the DB2 Installation documentation for details.

The setting of the `HS_LANGUAGE` parameter in the gateway `initsid.ora` determines which CCSID is used by the gateway for the conversation. Similarly, the setting of the `HS-NLS_NCHAR` parameter determines which CCSID will be used by the gateway for GRAPHIC data interchange. For the list of supported ASCII-based Oracle character sets that are mapped to CCSIDs, refer to ["Gateway Codepage Map Facility"](#) on page D-5.

Note again that the gateway character set need not be the same as the Oracle Database server character set. In many cases, it is not feasible to set the gateway character set equal to the Oracle Database server character set because the DRDA Server will not have a valid translation for it. Instead, choose a character set that will have the most complete intersection with the character set that is used by the DRDA Server. The Oracle Net facility will do any translation between the gateway character set and the Oracle server character set.

**Figure D-2 Gateway Language Interaction with DRDA Server**



### D.3.1 Gateway Configuration

After the gateway is installed, you must change several parameters to customize for NLS support.

### D.3.2 NLS Parameters in the Gateway Initialization File

Four parameters in the gateway initialization file (`initsid.ora`) affect NLS:

- `HS_LANGUAGE`
- `HS-NLS_NCHAR`
- `HS-NLS_DATE_FORMAT`
- `HS-NLS_DATE_LANGUAGE`

### D.3.2.1 HS\_LANGUAGE

`HS_LANGUAGE` defines the character set that is used for communication between the gateway and the DRDA Server. It specifies the conventions such as: the language used for messages from the target system; names of days and months; symbols for AD, BC, AM, and PM; and default language sorting mechanism.

The syntax of the `HS_LANGUAGE` parameter is:

```
HS_LANGUAGE=language[_territory.character_set]
```

where:

*language* can be any valid language.

*territory* is optional, and defaults to `AMERICA`.

*character\_set* is optional and defaults to `US7ASCII`. This must be an ASCII base character set name, and it should match a character set listed in the gateway code page map. Refer to "[Gateway Codepage Map Facility](#)" on page D-5 for the list of supplied character set mappings.

If you omit the `HS_LANGUAGE` parameter from `initsid.ora`, then the default setting is `AMERICAN_AMERICA.US7ASCII`. EBCDIC character sets are not supported. The values for *language* and *territory* (such as `AMERICAN_AMERICA`) must be valid, but they have no effect on translations.

### D.3.2.2 HS-NLS\_NCHAR

`HS-NLS_NCHAR` specifies the character set that is used by the gateway to interchange GRAPHIC data. For correct compatibility, set it to the same character set name that is specified in the `HS_LANGUAGE` parameter. If it is set to a character set other than that specified in `HS_LANGUAGE`, or if it is omitted, then translation errors will occur.

### D.3.2.3 HS-NLS\_DATE\_FORMAT

`HS-NLS_DATE_FORMAT` specifies the format for dates used by the DRDA Server.

The syntax of the `NLS_DATE_FORMAT` parameter is:

```
HS-NLS_DATE_FORMAT=date_format
```

where *date\_format* must be `YYYY-MM-DD`, the ISO date format. If this parameter is set to any other value or is omitted, then you receive an error when updating, deleting from, selecting from, or inserting into, a table with date columns.

### D.3.2.4 HS-NLS\_DATE\_LANGUAGE

`HS-NLS_DATE_LANGUAGE` specifies the language used by the DRDA Server for day and month names, and for date abbreviations. Because ISO date format contains numbers only, this parameter has no effect on gateway date processing and should be omitted.

## D.4 Gateway Codepage Map Facility

The gateway now has a user-specifiable facility to map IBM Coded Character Set Identifiers (CCSIDs) to Oracle Character Sets for the purpose of data translation.

The map name defaults to `codepage.map` and is located in the directory `ORACLE_HOME\tg4drda\admin`. Refer to [Appendix C, "DRDA-Specific Parameters"](#) for more detailed information about the `DRDA_CODEPAGE_MAP` parameter.

The map has two different forms of syntax. The first form of syntax defines a mapping between a CCSID and an Oracle Database character set:

```
[S|D|M] CCSID direction Oracle_CharacterSet {shift}
```

where:

S designates a single-byte character set

D designates a double-byte character set

M designates a multibyte character set

CCSID is the IBM coded character set identifier

*direction* is one of the following:

- = means mapping is bidirectional
- < means mapping is one-way, Oracle character set to CCSID
- > means mapping is one-way, CCSID to Oracle character set

*Oracle\_CharacterSet* is the name of a valid Oracle character set.

*shift* indicates a character set that requires Shift OUT/IN processing. Set this attribute only for EBCDIC-based double-byte and multibyte mappings.

The second form of syntax defines a mapping of a multibyte CCSID to its single-byte and double-byte CCSID equivalents:

```
MBC multi = single double
```

where:

*multi* is the multibyte CCSID

*single* is the single-byte CCSID

*double* is the double-byte CCSID

This facility is intended as a way of mapping CCSIDs which were not previously mapped as shipped with the gateway. You must contact Oracle Support Services before modifying this map.

The following are the contents of the map as shipped with the Oracle Transparent Gateway for DRDA;

```
# Copyright (c) 2001, 2003, Oracle Corporation. All rights reserved.
# Transparent Gateway for IBM DRDA - CodePage/Oracle CharacterSet Map
# S==Single-byte, D==Double-byte, M==Multi-byte, MBC==SBC DBC mapping
#
# Single-byte codepage mappings
#
S 37 = WE8EBCDIC37 # United States/Canada EBCDIC
S 273 = D8EBCDIC273 # Austria/Germany EBCDIC
S 277 = DK8EBCDIC277 # Denmark/Norway EBCDIC
S 278 = S8EBCDIC278 # Finland/Sweden EBCDIC
S 280 = I8EBCDIC280 # Italy EBCDIC
S 284 = WE8EBCDIC284 # Latin America/Spain EBCDIC
S 285 = WE8EBCDIC285 # United Kingdom EBCDIC
S 297 = F8EBCDIC297 # France EBCDIC
#S 420 = AR8EBCDICX # Arabic Bilingual (USA English) EBCDIC
S 420 = AR8XBASIC # Arabic Bilingual (USA English) EBCDIC
S 424 = IW8EBCDIC424 # Israel (Hebrew) EBCDIC
S 437 = US8PC437 # Personal Computer,USA ASCII
S 500 = WE8EBCDIC500 # International EBCDIC
```

```

S 813 = EL8ISO8859P7 # Greek ASCII
S 819 = WE8ISO8859P1 # ISO/ANSI Multilingual ASCII
S 838 = TH8TISEBCDIC # Thai w/Low-Tone Marks & Ancient Chars EBCDIC
S 850 < US7ASCII # Multilingual Page - Personal Computer ASCII
S 850 = WE8PC850 # Multilingual Page - Personal Computer ASCII
S 864 = AR8ISO8859P6 # Arabic - Personal Computer ASCII
S 870 = EE8EBCDIC870 # Latin 2, Multilingual/ROECE EBCDIC
S 871 = WE8EBCDIC871 # Iceland - CECP EBCDIC
S 875 = EL8EBCDIC875 # Greece EBCDIC
S 904 > US7ASCII # Traditional Chinese - PC-Data ASCII
S 912 = EE8ISO8859P2 # Latin 2 8-bit ASCII
S 916 = IW8ISO8859P8 # Israel (Hebrew) ASCII
S 1025 = CL8EBCDIC1025 # Cyrillic, Multiling EBCDIC
S 1086 = IW8EBCDIC1086 # Israel EBCDIC
S 1252 = WE8MSWIN1252 # Latin 1 - MS-Windows ASCII
S 1253 = EL8MSWIN1253 # Greek - MS-Windows ASCII
S 28709 > WE8EBCDIC37 # United States/Canada (CP28709==CP37) EBCDIC
#
# Multibyte codepage mappings
#
#S 833 > KO16DBCS # Korean Extended single-byte EBCDIC
#D 834 > KO16DBCS shift # Korean double-byte EBCDIC
#M 933 = KO16DBCS shift # Korean Mixed multi-byte EBCDIC

#MBC 933 = 833 834 # Korean Mixed multi-byte EBCDIC
#
#S 1088 > KO16MSWIN949 # Korean KS single-byte PC-Data ASCII
#D 951 > KO16MSWIN949 # Korean KS double-byte PC-Data ASCII
#M 949 = KO16MSWIN949 # Korean KS multi-byte PC-Data ASCII
#MBC 949 = 1088 951 # Korean KS multi-byte PC-Data ASCII
#
#S 891 > KO16KSC5601 # Korean single-byte ASCII
#S 1040 > KO16KSC5601 # Korean single-byte ASCII
#D 926 > KO16KSC5601 # Korean double-byte ASCII
#M 934 = KO16KSC5601 # Korean multi-byte ASCII
#M 944 > KO16KSC5601 # Korean multi-byte ASCII
#MBC 934 = 891 926 # Korean multi-byte ASCII
#MBC 944 = 1040 926 # Korean multi-byte Extended ASCII
#
#S 28709 > ZHT16DBCS # Traditional Chinese single-byte EBCDIC
#D 835 > ZHT16DBCS shift # Traditional Chinese double-byte EBCDIC
#M 937 = ZHT16DBCS shift # Traditional Chinese multi-byte EBCDIC
#MBC 937 = 28709 835 # Traditional Chinese multi-byte EBCDIC
#
#S 1114 > ZHT16MSWIN950 # Traditional Chinese single-byte ASCII
#D 947 > ZHT16MSWIN950 # Traditional Chinese double-byte ASCII
#M 950 = ZHT16MSWIN950 # Traditional Chinese multi-byte ASCII
#MBC 950 = 1114 947 # Traditional Chinese multi-byte ASCII
#
#S 836 > ZHS16DBCS # Simplified Chinese single-byte EBCDIC
#D 837 > ZHS16DBCS shift # Simplified Chinese double-byte EBCDIC
#M 935 = ZHS16DBCS shift # Simplified Chinese multi-byte EBCDIC
#MBC 935 = 836 837 # Simplified Chinese multi-byte EBCDIC
#
#S 1027 > JA16DBCS # Japanese single-byte EBCDIC
#D 300 > JA16DBCS shift # Japanese double-byte EBCDIC
#D 4396 > JA16DBCS shift # Japanese double-byte EBCDIC
#M 939 = JA16DBCS shift # Japanese multi-byte EBCDIC
#M 5035 > JA16DBCS shift # Japanese multi-byte EBCDIC

```

```

#MBC 939 = 1027 300      # Japanese multi-byte      EBCDIC
#MBC 5035 = 1027 4396   # Japanese multi-byte      EBCDIC
#
#S 290 > JA16EBCDIC930  # Japanese single-byte     EBCDIC
#D 300 > JA16EBCDIC930 shift # Japanese double-byte     EBCDIC
#D 4396 > JA16EBCDIC930 shift # Japanese double-byte     EBCDIC
#M 930 = JA16EBCDIC930 shift # Japanese multi-byte      EBCDIC
#M 5026 > JA16EBCDIC930 shift # Japanese multi-byte      EBCDIC
#MBC 930 = 290 300      # Japanese multi-byte      EBCDIC
#MBC 5026 = 290 4396   # Japanese multi-byte      EBCDIC
#

```

Refer to the following list to check the character set of an existing database:

- **for DB2/OS390:** Ask your system administrator. There is no single command you use.
- **for DB2/400:** Run the command `DSPSYSVAL SYSVAL(QCCSID)`
- **for DB2/UDB:** Ask your system administrator. There is no single command you use.
- **for DB2/VM:** Run the statement `ID`. This shows you the default CCSIDs used at startup.

## D.5 Multibyte and Double-Byte Support in the Gateway

To enable the gateway to properly handle double-byte and multibyte data, you must configure the code page map facility with proper multibyte maps and (as an option) you can set the following gateway configuration parameters:

- `DRDA_GRAPHIC_LIT_CHECK`
- `DRDA_GRAPHIC_TO_MBCS`
- `DRDA_MBCS_TO_GRAPHIC`
- `DRDA_GRAPHIC_PAD_SIZE`
- `DRDA_GRAPHIC_CHAR_SIZE`

Refer to [Appendix C, "DRDA-Specific Parameters"](#), for the values of these parameters.

Configuring the code page map requires knowledge of the code pages that have been configured in the DRDA Server database as well as knowledge of compatible Oracle Database character sets.

IBM coded character set identifiers (CCSIDs) are used to indicate which code pages are configured as the primary codepage for the database, as well as any translation character sets loaded into the database. Some DRDA Servers, such as with DB2, have a translation facility in which character set transforms are mapped between two compatible character sets. For DB2/OS390, these transforms are stored in the table `SYSIBM.SYSSTRINGS` and transform on the CCSID codepage to another CCSID codepage. In `SYSSTRINGS`, `IN` and `OUT` columns specify the CCSIDs that are used in the transform. Typical transforms are from ASCII to EBCDIC and back again. Two transforms are therefore used for two given CCSIDs.

Multibyte codepages are a composite of a single-byte codepage and a double-byte codepage. As an example, the Korean EBCDIC multi-byte codepage, CCSID 933, is composed of two codepages, codepage 833 (for single-byte) and codepage 834 (for double-byte). The DRDA Server, therefore, can send data to the gateway in any of these three codepages, and the gateway must translate suitably depending on which



codepage the data is associated with. Because CCSID 933 is an EBCDIC-based codepage, and the gateway must use an ASCII-based codepage, we identify an equivalent set of codepages, which are ASCII-based. An example would be the Korean multibyte codepage, CCSID 949, which is composed of two codepages, codepage 1088 (for single-byte) and codepage 951 (for double-byte).

The codepage map facility is used to map these CCSIDs into the equivalent Oracle Database character sets. Unlike IBM CCSIDs, Oracle Database character sets are unified (in that single-byte and double-byte character sets have been combined into one set) and are thus identified by one ID instead of three IDs. In our previous example, the equivalent Oracle Database Character Set for the ASCII Korean codepages would be KO16MSWIN949, and the EBCDIC Korean codepages would be KO16DBCS. These are identified to the gateway by using a set of mapping entries in the **codepage.map** file.

First, the EBCDIC Korean sets are:

```
S  833 > KO16DBCS      # Korean Extended single-byte      EBCDIC
D  834 > KO16DBCS shift # Korean double-byte              EBCDIC
M  933 = KO16DBCS shift # Korean Mixed multi-byte        EBCDIC
MBC 933 = 833 834      # Korean Mixed multi-byte        EBCDIC
```

Notice that the multibyte set is a bidirectional map to KO16DBCS, while the single and double codepages are mapped one-way to KO16DBCS. Because only one bidirectional CCSID to Oracle Database character set entry for a given pair can exist, we directly map the multibyte sets. And because the single-byte and double-byte CCSIDs are ostensibly subsets of KO16DBCS, we map them as one-way entries. Note that double-byte and multibyte maps are tagged with the shift attribute. This is required for EBCDIC double-byte and multibyte codepages as part of the shift out/in encapsulation of data. Note that the single-byte map is not marked because single-byte sets are not permitted to contain double-byte data and thus will never use shift encapsulation. Also note that the MBC entry ties the codepages together.

The ASCII Korean sets are similarly mapped and are:

```
S  1088 > KO16MSWIN949 # Korean KS single-byte PC-Data      ASCII
D   951 > KO16MSWIN949 # Korean KS double-byte PC-Data     ASCII
M   949 = KO16MSWIN949 # Korean KS multi-byte PC-Data      ASCII
MBC 949 = 1088 951     # Korean KS multi-byte PC-Data      ASCII
```

Notice that the multibyte set is a bidirectional map to KO16MSWIN949, while the single and double codepages are mapped one-way to KO16MSWIN949. Because only one bidirectional CCSID to Oracle Database character set entry for a given pair can exist, we directly map the multibyte sets. And because the single-byte and double-byte CCSIDs are ostensibly subsets of KO16MSWIN949, we map them as one-way entries. Note that there is no shift attribute in any of these mappings. This is because ASCII-based sets do not use shift out/in encapsulation. Instead, ASCII-based sets use a different method (which does not use a shift out/in protocol) to identify double-byte characters.

The above entries supply the necessary codepage mappings for the gateway. To complete the example, we need to specify the correct character set in the HS\_LANGUAGE and HS-NLS\_NCHAR parameters in the gateway initialization file. The gateway initialization parameters would look as follows:

```
HS_LANGUAGE=AMERICAN_AMERICA.KO16MSWIN949
HS-NLS_NCHAR=KO16MSWIN949
```

Note that the specified character set must be ASCII-based.

This takes care of configuration of the gateway. The last step is to set up transforms between the EBCDIC codepages and the ASCII codepages in the DRDA Server database. Normally, the gateway would use a total of six transforms, one of each pair in both directions. You may save some table space by installing only the ASCII-to-EBCDIC transforms. The reasoning is that the DRDA Server needs to translate only the ASCII data that is sent by the gateway, but the DRDA Server does not need to send ASCII data. The gateway will receive the EBCDIC data and translate as needed. This one-sided data transfer methodology is called "receiver-makes-right", meaning that the receiver must translate whatever character set the sender uses. In our example, the DRDA Server is EBCDIC-based, so it will send all data in EBCDIC. The server, therefore, does not need to have an EBCDIC-to-ASCII transform because the server will never use the transform.

In our previous example, the DRDA Server database is assumed to be EBCDIC, which is likely to be true for a DB2/OS390 database. For a DB2/UDB database, however, this is not likely to be true. Because most DB2/UDB databases are running on ASCII-based computers, they will likely be created with ASCII-based codepages. In such cases, the gateway needs to have only one set of codepage map definitions, which are those for the ASCII set. Also, because both the DRDA Server and the gateway will be using the same codepages, no character set transforms need to be loaded into the DB2 database. This can help reduce the amount of CPU overhead that is associated with character translation.

One final note concerning codepage map entries: Be aware that some multi-byte codepages may be composed of single-byte CCSIDs that are already defined in the codepage.map file that is provided with the product. If you are adding a new set of entries to support a multibyte set, then comment out the provided entries so that your new entries will be used correctly.

Additional codepage mappings, which are not already provided, are possible. You may construct entries such as those in our examples, given knowledge of the IBM CCSIDs and the Oracle Database character sets. Because this can be complex (given the IBM documentation of codepage definitions and Oracle Database Character Set definitions), thoroughly test your definitions for all desired character data values before putting them into production.

If you are uncertain, then contact Oracle Support Services to request proper codepage mapping entries.

## D.6 Message Availability

Whether a language message module is available depends on which modules are installed in the Oracle product set running on the server. If message modules for a particular language set are not installed, then specifying that language with a language parameter does not display messages in the requested language.

## D.7 Example of NLS Configuration

Following is an example of all the settings needed to configure the gateway, DRDA Server, Oracle server, and client so that a language and character set are working compatibly across the system. In this example, the settings enable a customer in Germany to interact with the gateway in German:

### **Gateway *initsid.ora* file:**

```
HS_LANGUAGE=AMERICAN_AMERICA.WE8ISO8859P1
HS-NLS_DATE_FORMAT=YYYY-MM-DD
```

**DRDA Server CCSID:**

273 (D8EBCDIC273)

**Oracle server and client setting for database:**

```
SELECT USERENV('language') FROM DUAL;  
USERENV('LANGUAGE')
```

```
-----  
AMERICAN_AMERICA.WE8ISO8859P1
```

**Oracle server and client environment variables:**

```
NLS_LANG=GERMAN_GERMANY.WE8ISO8859P1
```



---



---

## Configuration Worksheet

### Information That You Need in Order to Configure the Gateway and the Communications Interfaces (SNA Server and TCP/IP)

**Table E-1** List of Parameters Needed to Configure the Gateway

Reason	Name of Parameter Needed	Your Specific Parameters Here
For: Gateway's Oracle Home	<ul style="list-style-type: none"> <li>▪ ORACLE_HOME</li> </ul>	_____
For: Gateway's System ID	<ul style="list-style-type: none"> <li>▪ ORACLE_SID</li> </ul>	_____
For: SNA Server Definition	<ul style="list-style-type: none"> <li>▪ SNA Subdomain</li> <li>▪ SNA Service</li> </ul>	_____ _____
For: Primary Service Definition	<ul style="list-style-type: none"> <li>▪ Network Name</li> <li>▪ Control Point Name</li> </ul>	_____ _____
For: SNA Server Link Service	<ul style="list-style-type: none"> <li>▪ Suitable Link Service Identification (example: DLC 80202 Link Service)</li> </ul>	_____
For: Link Service Properties	<ul style="list-style-type: none"> <li>▪ Suitable Network Adapter information (example: IBM Auto 16/4 Token-Ring Adapter)</li> </ul>	_____
For: Creating a General Connection Definition	<ul style="list-style-type: none"> <li>▪ Suitable Connection Type (Example: 802.2)</li> <li>▪ Connection Name</li> <li>▪ Suitable Link Service</li> </ul>	_____ _____ _____
For: Connection Properties Address	<ul style="list-style-type: none"> <li>▪ Remote Network Address</li> <li>▪ Remote SAP Address</li> </ul>	_____ _____
For: System Identification: Local Node Name and Remote Node Name	<ul style="list-style-type: none"> <li>▪ For each: Network Name</li> <li>▪ Control Point Name</li> <li>▪ Local Node ID</li> <li>▪ Remote Node ID</li> </ul>	_____ _____ _____ _____
For: DLC values	possible change of default values	_____
For: Creating a Local LU Definition:	<ul style="list-style-type: none"> <li>▪ LU Alias</li> <li>▪ LU Name</li> </ul>	_____ _____
For: General APPC Mode Definition	<ul style="list-style-type: none"> <li>▪ Mode Name</li> </ul>	_____

**Table E-1 (Cont.) List of Parameters Needed to Configure the Gateway**

Reason	Name of Parameter Needed	Your Specific Parameters Here
For: APPC Mode Limits	<ul style="list-style-type: none"> <li>■ Parallel Session Limit</li> <li>■ Minimum Contention Winner Limit</li> <li>■ Partner Min Contention Winner Limit</li> <li>■ Automatic Activation Limit</li> </ul>	<p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p>
For: APPC Mode Characteristics	<ul style="list-style-type: none"> <li>■ Pacing Send Count</li> <li>■ Pacing Receive Count</li> <li>■ Max Send RU Size</li> </ul>	<p>_____</p> <p>_____</p> <p>_____</p>
For: Remote LU Definition, General Properties	<ul style="list-style-type: none"> <li>■ Suitable Connection name</li> <li>■ LU ALias</li> <li>■ Network Name</li> <li>■ Uninterpreted Network Name</li> </ul>	<p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p>
For: Remote LU Properties Options	<ul style="list-style-type: none"> <li>■ Any Security Options needed</li> </ul>	<p>_____</p>
For: Creating CPI-C Symbolic Destination Names (Side Information Profiles), general information	<ul style="list-style-type: none"> <li>■ Suitable Name for each Side Information Profile</li> <li>■ Suitable Mode</li> </ul>	<p>_____</p> <p>_____</p>
For: Partner Information in CPI-C Name Properties	<ul style="list-style-type: none"> <li>■ TP Name</li> <li>■ Partner LU Name Alias</li> </ul>	<p>_____</p> <p>_____</p>
For: Configuring TCP/IP	<ul style="list-style-type: none"> <li>■ Local Host name, Domain Name</li> <li>■ IP Address</li> <li>■ Network Mask</li> <li>■ Name Server IP Address</li> <li>■ DRDA Server Host name or IP Address</li> <li>■ DRDA Server Service Port Number</li> </ul>	<p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p>
For: Recovery user ID	<ul style="list-style-type: none"> <li>■ DRDA_RECOVERY_USERID</li> </ul>	<p>_____</p>
For: Recovery Password	<ul style="list-style-type: none"> <li>■ DRDA_RECOVERY_PASSWORD</li> </ul>	<p>_____</p>
For: Remote Database Name	<ul style="list-style-type: none"> <li>■ DRDA_REMOTE_DB_NAME</li> </ul>	<p>_____</p>
For: Connection Parameter	<ul style="list-style-type: none"> <li>■ DRDA_CONNECT_PARM</li> </ul>	<p>_____</p>
For: Remote collection ID	DRDA_PACKAGE_COLLID	<p>_____</p>
For: Remote package name	DRDA_PACKAGE_NAME	<p>_____</p>
For: Owner ID of DRDA package	DRDA_PACKAGE_OWNER	<p>_____</p>
For: DB Name used with Oracle server	HS_DB_NAME	<p>_____</p>
For: DB Domain used with Oracle server	HS_DB_DOMAIN	<p>_____</p>

---

---

**Note:** The user ID that is used to bind or rebind the DRDA package must have the following privileges on the remote database; your database administrator will need to provide these.

- package privileges of BIND, COPY, and EXECUTE
  - collection privilege of CREATE IN
  - system privileges of BINDADD and BINDAGENT
- 
-





---



---

## Quick Reference to Oracle SQL Functions

Following are the Oracle SQL functions:

**Table F-1 Oracle SQL Functions in Alphabetic Order**

Functions			
ABS	ACOS	ADD_MONTHS	ASIN
ASCII	ATAN	ATAN2	CEIL
CHAR_TO_ROWID	CHR	CONVERT	COS
COSH	DECODE	DUMP	EXP
FLOOR	GREATEST	HEXTORAW	INITCAP
INSTR	INSTRB	LAST_DAY	LEAST
LENGTH	LENGTHB	LN	LOG
LOWER	LPAD	LTRIM	MOD
MONTHS_BETWEEN	NEW_TIME	NEXT_DAY	NLS_INITCAP
NLS_LOWER	NLS_UPPER	NLSSORT	POWER
RAWTOHEX	REPLACE	ROUND	ROWIDTOCHAR
RPAD	RTRIM	SIGN	SIN
SINH	SOUNDEX	SQRT	STDDEV
SUBSTR	SUBSTRB	SYSDATE	TAN
TANH	TO_CHAR	TO_DATE	TO_LABEL
TO_MULTI_BYTE	TO_NUMBER	TO_SINGLE_BYTE	TRANSLATE
TRUNC	UID	UPPER	USER
USERENV	VARIANCE	VSIZE	BITAND



---

## Sample Applications

This appendix contains sample applications that can be used with the gateway:

- [DB2INS](#) on page G-1
- [ORAIND](#) on page G-2

### G.1 DB2INS

DB2INS is a sample DB2 stored procedure that inserts a row into a DB2 table. This procedure uses the SIMPLE linkage convention.

```

/*****/
/*
/* This DB2 stored procedure inserts values for the DNAME and LOC
/* columns of DB2 user table SCOTT.DEPT.
/*
/* The SCOTT.DEPT table is defined to DB2 as
/*     DEPTNO INTEGER, DNAME CHAR(14), LOC VARCHAR(13).
/*
/* This procedure receives 3 input parameters from the calling
/* program which contain the values to insert for DEPTNO, DNAME, and
/* LOC.
/*
/* The linkage convention used for this stored procedure is SIMPLE.
/*
/* The output parameter for this procedure contains the SQLCODE from
/* the INSERT operation.
/*
/* The entry in the DB2 catalog table SYSIBM.SYSPROCEDURES for this
/* stored procedure might look like this:
/*
/* INSERT INTO SYSIBM.SYSPROCEDURES
/* (PROCEDURE, AUTHID, LUNAME, LOADMOD, LINKAGE, COLLID, LANGUAGE,
/* ASUTIME, STAYRESIDENT, IBMREQD, RUNOPTS, PARMLIST)
/* VALUES
/* ('DB2INS', ' ', ' ', 'DB2INS', ' ', 'DB2DEV', 'C', '0', ' ',
/* 'N', ' ', 'A INT IN, B CHAR(14) IN, C VARCHAR(13) IN,
/* D INT OUT, E CHAR(10) OUT');
/*****/
#pragma runopts(plist(os))
#include <stdlib.h>
EXEC SQL INCLUDE SQLCA;
/*****/
/* Declare C variables for SQL operations on the parameters. These
/* are local variables to the C program which you must copy to and
/* from the parameter list provided to the stored procedure.
*/

```

```

/*****/

EXEC SQL BEGIN DECLARE SECTION;
long dno;          /* input parm - DEPTNO */
char dname[15];   /* input parm - DNAME */
char locale[14];  /* input parm - LOC */
EXEC SQL END DECLARE SECTION;
main(argc,argv)
int argc;
char *argv[];
{
/*****/
/* Copy the input parameters into the area reserved in the local */
/* program for SQL processing. */
/*****/
    dno = *(int *) argv[1];
    strcpy(dname, argv[2]);
    strcpy(locale, argv[3]);
/*****/
/* Issue SQL INSERT to insert a row into SCOTT.DEPT */
/*****/
EXEC SQL INSERT INTO SCOTT.DEPT VALUES(:dno, :dname, :locale);
/*****/
/* Copy SQLCODE to the output parameter list. */
/*****/
    *(int *) argv[4] = SQLCODE;
}

```

## G.2 ORAIND

ORAIND is a sample host program that calls a DB2 stored procedure (DB2INS) to insert a row into a DB2 table.

```

/*****/
/* This sample Proc program calls DB2 stored procedure DB2INS to */
/* insert values into the DB2 user table SCOTT.DEPT. This calling */
/* program uses embedded PL/SQL to call the stored procedure. */
/*****/
#include <stdio.h>
EXEC SQL BEGIN DECLARE SECTION;
    VARCHAR    username[20];
    VARCHAR    password[20];
    int        dept_no;
    char       dept_name[14];
    VARCHAR    location[13];
    int        code;
    char       buf[11];
    int        x;
EXEC SQL END DECLARE SECTION;
EXEC SQL INCLUDE SQLCA;
main()
{
/*****/
/* Setup Oracle user id and password */
/*****/
    strcpy(username.arr, "SCOTT");          /* copy the username */
    username.len = strlen(username.arr);
    strcpy(password.arr, "TIGER");        /* copy the password */
    password.len = strlen(password.arr);

```

```

EXEC SQL WHENEVER SQLERROR GOTO sqlerror;
/*****
/* Logon to Oracle */
*****/
EXEC SQL CONNECT :username IDENTIFIED BY :password;
printf("\nConnected to ORACLE as user: %s\n", username.arr);
/* Delete any existing rows from DB2 table */
EXEC SQL DELETE FROM SCOTT.DEPT@GTWLINK;
EXEC SQL COMMIT;

/*----- begin pl/sql block -----*/
/*****
/* Insert 1 row into DB2 table SCOTT.DEPT by invoking DB2 stored */
/* procedure DB2INS. The DB2 stored procedure will perform the */
/* INSERT. */
/* */
/* SCOTT.DEPT table is defined on DB2 as: */
/* */
/* DEPTNO INTEGER; */
/* DNAME CHAR(14); */
/* LOC VARCHAR(13); */
/* */
*****/
EXEC SQL EXECUTE
BEGIN
    :dept_no := 10;
    :dept_name := 'GATEWAY';
    :location := 'ORACLE';
    DB2INS@GTWLINK(:dept_no, :dept_name, :location, :code);
END;
END-EXEC;
/*----- end pl/sql block -----*/
/*****
/* Check the SQLCODE returned from the stored procedures INSERT. */
*****/
if (code == 0)
    printf("DB2INS reports successful INSERT\n");
else
{
    printf("DB2INS reports error on INSERT.\nSQLCODE=%d\n",code);
    goto sqlerror;
}
/*****
/* Verify row insertion. Query the data just inserted. */
*****/
EXEC SQL SELECT deptno, dname, loc INTO
    :dept_no, :dept_name, :location
FROM SCOTT.DEPT@GTWLINK WHERE deptno = 10;
printf("\nData INSERTed was:\n");
printf("\ndeptno = %d, dname = %s, loc = %s\n",
    dept_no, dept_name, location.arr);
/*****
/* Logoff from Oracle */
*****/
EXEC SQL COMMIT RELEASE;
printf("\n\nHave a good day\n\n");
exit(0);
sqlerror:
    printf("\n% .70s \n", sqlca.sqlerrm.sqlerrmc);

```

```
EXEC SQL WHENEVER SQLERROR CONTINUE;  
EXEC SQL ROLLBACK RELEASE;  
exit(1);  
}
```

## A

access method transparency (introduction), 1-3

accessing

DRDA Servers, 10-9

gateway, 10-8

action items of Oracle Universal Installer, 4-3

Advanced Security

CHECKSUM command, 9-4

encryption

export encryption algorithms, 9-4

international version types supported, 9-4

resetting configuration parameters on

gateway, 9-5

setting test parameters for gateway, 9-4

setting test parameters for Oracle integrating server, 9-5

setting up for test, 9-4

testing gateway and Oracle integrating server, 9-5

function on the gateway, 1-4

test error

error 12660, 9-4

testing advanced security encryption, 9-5

AGW ADD USERID command, 13-4

AGW DELETE USERID command, 13-4

AIX\_RS6K, default value for

DRDA\_LOCAL\_NODE\_NAME, C-6

alias

DB2, C-4

objects, DB2, known restrictions, 2-3

ALL\_CATALOG view, A-2

ALL\_COL\_COMMENTS view, A-2

ALL\_CON\_COLUMNS view, A-2

ALL\_CONSTRAINTS view, A-3

ALL\_DB\_LINKS data dictionary view, 11-2

ALL\_INDEXES view, A-3

ALL\_OBJECTS view, A-5

ALL\_SYNONYMS view, A-6

ALL\_TAB\_COMMENTS view, A-8

ALL\_TABLES view, A-6

ALL\_USERS view, A-9

ALL\_VIEWS view, A-9

allocation mode, SNA session,

DRDA\_CMSRC\_CM\_IMMEDIATE, C-3

ALTER session statement, 11-2

ANSI-standard SQL

gateway capabilities, 1-5

heterogeneous database integration, 1-11

API (application program interface), Oracle Net, 9-2

APPC

concurrent connections, 3-1

configuring another profile, 10-9

database link behavior, 12-5

DB2/VM, 13-4

mode definition, 6-11

password length, 15-4

user ID length, 15-4

APPC VTAM Support (AVS)

also see AVS, 13-4

mapping user ID, 2-3

APPEND command

supported by COPY, 11-6

application

application program interface defined, see API, 9-2

authenticating logons, 13-1

development on the gateway, 1-12

portability, 1-11

server support, 1-4

architecture of the gateway, 1-7

array size

fetch reblocking, 1-10

how determined, 12-2

AS/400

command DSPRDBDIRE, 5-4

configuring communications, 5-3

defining user ID, 5-4

library name, DRDA\_PACKAGE\_COLLID, C-7

ASCII

code page, D-4

sort order, 12-19

tables, known restrictions, 1-13

translated from EBCDIC, 12-21

US7ASCII, D-5

US7ASCII,NLS, D-3

authority

CONNECT, 13-4

execute, 13-4

autonomy, site, 1-6

AVS

also see APPC VTAM Support, 2-3

- configuring, 5-6
- DB2/VM, 13-4
- mapping user IDs (DB2/VM), 2-3
- user ID mapping, 13-4

## B

---

- binary data, non-character, 12-21
- Bind Package Stored Procedure
  - DB2/400, 5-4
  - DB2/OS390, 5-2
  - DB2/UDB, 5-5
  - DB2/VM, 5-6
- bind privilege
  - configuration worksheet, E-3
  - DB2/400, 5-4
  - DB2/OS390, 5-2
  - DB2/UDB, 5-5
  - DB2/VM, 5-6
- bind variables
  - native SQL passthrough, 12-26
  - restrictions, 2-6
- BINDADD authority, binding packages on
  - DB2/UDB, 10-6
- BINDADD privilege
  - configuration worksheet, E-3
  - DB2/OS390, 5-2
  - DB2/UDB, 5-5
  - DB2/VM, 5-6
- BINDAGENT privilege
  - configuration worksheet, E-3
  - DB2/OS390, 5-2
  - DB2/VM, 5-6
- binding the DRDA package
  - authority of user ID and password
    - DB2/400, 5-4
    - DB2/OS390, 5-2
    - DB2/UDB, 5-5
    - DB2/VM, 5-6
  - backward compatibility, 14-4
  - configuring the host, 10-5
  - on DB2/UDB, 10-5
  - upgrading from version 3, 10-5
- bug
  - bugs fixed in release 10.1.0.2.0, 2-1
- debugging
  - drc values used by Oracle Support Services, 15-2
  - setting trace parameters, 15-5
  - SQL tracing reduces gateway performance, 11-7
  - number 205538, 2-5
- DRDA\_DISABLE\_CALL
  - default, 10-6
  - sample Gateway Initialization File, B-1
- empproc stored procedure, 12-3
- Oracle Call Interface, 15-1
- PL/SQL, 12-4
- stored procedure
  - location transparency with synonym, 12-3
  - null values not passed, 2-4
  - using standard Oracle PL/SQL, 12-2
- capabilities, DRDA server, native semantics, 12-18
- CCSID
  - 65535 as the default for all tables created, C-3
  - CCSID (coded character set identifiers),
    - defined, D-8
  - code page mapping facility, D-5
  - DRDA Server, NLS, D-3
  - external mapping to supported Oracle character sets, Codepage Map Facility, 1-13
- changed parameters, 14-3
- changes in this release
  - IBM DB2 Version 5.1 EBCDIC and ASCII Tables, 1-13
  - IBM DB2/UDB supported, 1-13
  - read-only support, 1-13
- CHARACTER SET
  - clause, client/server configuration, D-3
  - parameter description, D-2
- character sets
  - and code page map facility, D-5
  - ASCII, known restrictions, 1-13
  - codepage, DRDA\_DEFAULT\_CCSID specifies default CCSID, C-3
  - EBCDIC, known restrictions, 1-13
  - supported, codepage map facility, 1-13
- character strings
  - converting character string data types, 12-21
  - performing character string operations, 12-21
- checklist
  - DRDA Server configuration, 5-1
  - gateway configuration, 10-1
  - gateway installation, 4-2
  - Oracle Net, 9-1
- CHECKSUM command
  - also see Advanced Security, 1-4
  - Oracle Net, Advanced Security Encryption, 9-4
- CICS transaction, 12-5
- clauses
  - CHARACTER SET, client/server configuration, D-3
  - CONNECT TO, 11-1
  - GROUP BY, 12-19
  - HAVING, 12-19
  - ORDER BY, 12-19
  - SQL
    - DELETE, 12-24
    - INSERT, 12-24
    - SELECT WHERE, 12-24
    - UPDATE, 12-24
    - TO\_DATE, 12-24

## C

---

- call
  - a CICS or IMS transaction, 12-5
  - DB2 stored procedure
    - DRDA Server definition, 12-3
    - look up in server catalog, 12-4



- USING, 11-1
- VALUES, 12-24
- WHERE
  - compatible for all versions of DRDA Server, 12-19
  - SQL limitations, Oracle ROWID column, 2-5
  - WHERE CURRENT OF CURSOR, ROWID column, 2-5
- client, defined in gateway architecture, 1-7
- code page map facility
  - for data translation, D-5
- code tracing, C-12
- codepage map facility
  - configuring support for character sets, 2-3
  - supported by gateway, 1-13
- coercion of data, defined, 12-18
- collection privilege - CREATE IN
  - configuration worksheet, E-3
  - DB2/OS390, 5-2
  - DB2/VM, 5-6
- collection privilege - CREATETAB, DB2/OS390, 5-2
- column
  - date columns function, 12-24
  - Oracle ROWID, 2-5
  - supported in a result set, 1-11
- commands
  - AGW ADD USERID, 13-4
  - AGW DELETE USERID, 13-4
  - CHECKSUM
    - advanced security, 1-4
    - supported by Oracle Net, 9-4
  - COPY
    - known restriction for INSERT, 2-3
    - SQL\*Plus command, 11-6
  - CREATE DATABASE LINK, 5-6
  - EXECUTE, 1-5
  - EXPLAIN PLAN, 15-5
  - INSERT, known restriction, 2-3
- commit confirm protocol, 1-6
- Communication Database (CDB) tables, DDF, 5-3
- communications requirements, 3-3
- compatible SQL set operators and clauses, 12-19
- concatenation restrictions, 2-4
- concurrent connections
  - APPC, 3-1
  - TCP/IP, 3-1
- configuring
  - additional DRDA Servers, 10-9
  - AS/400 communications, 5-3
  - AVS, 5-6
  - binding DRDA package, 10-6
  - checklist for gateway, 10-1
  - checklists for DRDA Server, 5-1
  - DB2/400, 5-3
  - DB2/OS390, 5-2
  - DB2/UDB, 5-4
  - list of parameters needed to configure the gateway, E-1
  - Oracle integrating server, 10-8
  - Oracle Net, 9-3
  - OS/390 (MVS) VTAM, 5-2
  - other Oracle servers, 10-8
  - SNA server, creating profiles, 6-2, 7-1
  - TCP/IP
    - for AS/400, 5-3
    - for DB2/VM, 5-6
    - for MS Windows, 8-1
    - for OS/390, 5-2
    - VM VTAM on DB2/VM, 5-6
    - workstation for gateway, 10-3
- CONNECT authority
  - binding packages on DB2/UDB, 10-6
  - DB2/UDB, 5-5
  - user ID mapping on DB2/VM, 13-4
- CONNECT BY not supported, known restrictions, 2-6
- CONNECT TO clause, 11-1
- connection
  - definition, 6-7
  - testing, 6-15, 7-17
- conversion
  - data types, 12-20
  - errors, C-4
- convert
  - character string data types, 12-21
  - character string operations, 12-21
  - DATE, 12-22
  - floating point to integer, 12-25
  - inbound user ID, 13-4
  - into most suitable data type, 12-25
  - to the numeric data type, 12-25
- converter, protocol, 1-4
- COPY
  - copying data from the DRDA server, 11-6
  - copying data from the Oracle server, 11-6
  - privilege
    - configuration worksheet, E-3
    - DB2/OS390, 5-2
    - DB2/VM, 5-6
  - SQL\*Plus COPY command
    - Oracle server to DRDA server, 11-6
    - substituted for INSERT, 2-3
- COS function, 12-7
- COUNT function, 12-25
- CPI-C routine, 15-2
- CPI-C Symbolic Destination Names, 6-14
- CREATE command, supported by COPY, 11-6
- CREATE DATABASE LINK
  - command, binding package on DB2/VM, 5-6
  - statement, defining path to remote database, 11-1
- CREATE DATABASE statement, client/server configuration, D-3
- CREATE IN privilege
  - configuration worksheet, E-3
  - DB2/OS390, 5-2
  - DB2/VM, 5-6
- CREATE PUBLIC DATABASE LINK privilege
  - binding the DRDA gateway package, 10-5
  - configuring Oracle integrating server, 10-8
- CREATE TABLE statement, 1-5

- CREATEIN privilege, DB2/UIDB, 5-5
- CREATETAB authority, 10-6
- CREATETAB privilege
  - DB2/OS390, 5-2
  - DB2/UIDB, 5-5
- creating a database link, 11-1
- cursor
  - defining the number of, 12-28
  - number of cursors,
    - DRDA\_PACKAGE\_SECTIONS, C-8
  - stability, DRDA\_ISOLATION\_LEVEL, C-6

## D

---

- data coercion, defined, 12-18
- data control language (DCL), 1-5
- data definition language (DDL), 1-5
- data dictionary
  - support, 10-7
  - using, 12-28
  - views
    - ALL\_DB\_LINKS, 11-2
    - considerations for migration from previous releases, 14-4
    - list and descriptions, A-2
    - not supported for DB2/VM, A-1
    - Oracle Emulation on DRDA Server, 12-28
    - supported for DB2/OS390, DB2/UIDB, and DB2/400 servers, A-1
    - USER\_DB\_LINKS shows defined database links, 11-2
- data storage transparency (introduction), 1-3
- data type
  - column (ALL\_TAB\_COLUMNS), A-8
  - column (USER\_TAB\_COLUMNS), A-15
  - conversion
    - between Oracle and DRDA, 1-9
    - control over, 12-25
    - converting character string data types, 12-21
    - gateway mapping and restrictions, 12-20
    - performing character string operations, 12-21
  - date, 2-4
  - differences between Oracle server and DRDA databases, 12-1
  - DRDA Server data types list, 12-20
  - known restrictions, 2-3
  - mapping, 12-20
  - numeric
    - zoned decimal field, 12-25
  - Oracle data types RAW and LONG RAW, 12-21
  - performing character string operations, 12-21
  - restrictions, 12-20
  - size and value limitations, 12-20
  - supported by IBM DRDA, 12-22
  - supported by IBM DRDA databases, 12-22
- data types
  - DATE, as calendar date only, 12-22
  - GRAPHIC, 12-21
  - LONG
    - converting character string data types, 12-21

- known restrictions, 2-4
- LONG RAW, translating ASCII to EBCDIC, 12-21
- Oracle and IBM DATA data types are mapped to each other, 12-22
- Oracle and IBM DATE, 12-22
- processing TIME data types to Oracle DATE, 12-22
- RAW
  - CCSID 65535, C-3
  - translating ASCII to EBCDIC, 12-21
- TIME, time of day only, 12-22
- TIMESTAMP, combining calendar data and time of day, 12-22
- VARCHAR, 12-21
- database
  - authorities - CONNECT, BINDADD, and CREATETAB, 5-5
  - catalogs, 12-28
  - link
    - behavior, 12-5
    - binding DRDA gateway package, 10-5
    - creating, 11-1
    - defining and controlling, 13-2
    - dropping links, 11-2
    - examining, 11-2
    - guidelines, 11-2
    - limits, 11-2
    - processing, 11-1
    - public, 10-8
    - suffix, 12-1
    - to identify the gateway, 1-9
    - native tool, 10-7
    - triggers, 1-4
- date
  - 2 or 4 digits, 12-23
  - arithmetic, known restrictions, 2-4
  - columns function, 12-24
  - data types and DRDA server restriction, 2-4
  - data types supported by IBM DRDA, 12-22
  - date handling has two categories, 12-23
  - gateway local date exit for DB2 ISO format, 12-24
  - HS-NLS\_DATE\_FORMAT
    - parameter, date handling, 12-23
    - patterns, 12-24
  - operations, 12-22
  - statements, SELECT, INSERT, UPDATE, DELETE, 12-23
  - TO\_DATE function
    - date handling, 12-23
    - preprocessed in SQL, 12-24
- DATE data type
  - implementation, 12-22
  - processing DATE data, 12-22
- DB\_DOMAIN parameter, 2-4
- DB2
  - 02pcg.sql granting authority, 10-8
  - alias objects, known restrictions, 2-3
  - aliases, not compatible with
    - DRDA\_DESCRIBE\_TABLE, C-4
  - CICS, IMS, 12-5

- data access, 1-5
- Distributed Data Facility (DDF), 5-3
- DRDA\_DESCRIBE\_TABLE compatibility, C-4
- IBM DB2 version 5.1 ASCII Tables, 1-13
- native SQL, 1-5
- native stored procedures, 1-5
- procedural feature considerations, 12-5
- SPUFI utility, 5-3
- SQL statements, 12-27
- statements, CREATE TABLE, 1-5
- stored procedures, considerations for use, 12-5
- with OS/390, 5-2
- DB2/400
  - catalog view, 12-28
  - configuring the DRDA Server, 5-3
  - data dictionary views supported by gateway, A-1
  - defining user ID, 5-4
  - DRDA\_DEFAULT\_CCSID, C-3
  - DRDA\_ISOLATION\_LEVEL, C-6
  - DRDA\_OPTIMIZE\_QUERY, C-7
  - DRDA\_PACKAGE\_COLLID, C-7
  - userid mapping, different capability, 13-4
- DB2INS sample DB2 stored procedure, G-1
- DB2/OS390
  - catalog view, 12-28
  - configuring, 5-2
  - data dictionary views supported by gateway, A-1
  - DRDA\_ISOLATION\_LEVEL, C-6
  - DRDA\_OPTIMIZE\_QUERY, C-7
  - userid mapping, 13-3
  - V6, V7 and V8 stored procedures supported, 1-13
  - with SPUFI, 10-7
- DB2/UDB
  - catalog view, 12-28
  - configuring, 5-4
  - configuring the DRDA Server, 5-4
  - data dictionary views not supported, A-1
  - DRDA\_ISOLATION\_LEVEL, C-6
  - DRDA\_OPTIMIZE\_QUERY, C-7
  - grant authority, 10-8
  - known restrictions, 2-4
  - ORACLE2PC table, binding packages, 10-7
  - supported, changes in this release, 1-13
  - userid mapping, 13-4
- DB2/VM
  - catalog view, 12-28
  - configuring, 5-5
  - data dictionary views not supported, A-1
  - database and SQL functions, 12-15
  - DRDA\_ISOLATION\_LEVEL, C-6
  - DRDA\_OPTIMIZE\_QUERY, C-7
  - DRDA\_PACKAGE\_OWNER, C-8
  - instance, DRDA location name, 5-6
  - server machine, 13-4
  - userid mapping, 13-4
- DBMS\_HS\_PASSTHROUGH.EXECUTE\_IMMEDIATE
  - E function
  - limited to nonqueries, 12-25
  - native SQL passthrough, 12-26
  - syntax, 12-26
- DD basic tables, known restrictions, 2-3
- DDF
  - subsystem, 5-2
- DDL statement
  - native SQL passthrough, 12-26
  - number of rows affected, 12-27
- debugging
  - error codes, 15-2
  - SQL tracing, 15-5
  - your application, 11-7
- de-installing the gateway, 4-4
- DELETE
  - known restrictions, 2-5
  - operation, 12-2
  - SQL clause, 12-24
  - statement
    - dates, 12-23
    - native SQL passthrough, 12-26
    - transaction semantics, 1-9
    - with read-only gateway, 11-5
- Dependent LU, 6-2, 7-2
- DESCRIBE
  - character string operations, 12-21
- diagnostic parameter, C-11
- dictionary
  - mapping, 1-4
  - tables, 12-28
- DICTIONARY view, A-10
- disk space requirements, 3-2
- distributed
  - applications, support for, 1-12
  - database, 9-2
  - distributed query optimizer (DQO), better performance of distributed queries, 11-4
  - operations, DB2, 5-3
  - processing, 9-2
  - queries
    - example of, 11-4
    - two-phase commit, 11-5
    - transaction, DRDA\_RECOVERY\_USERID, C-9
  - distributed query optimizer (DQO), DRDA-specific parameters, C-6
- double-byte support, D-8
- DQO
  - also see distributed query optimizer, 11-4
  - DRDA-specific parameters, C-6
- drc error code, 15-2
- DRDA
  - catalog, 12-28
  - database requirements, 3-2
  - defining number of cursors, 12-28
  - location name
    - for DB2/UDB instance, 5-5
    - for DB2/VM instance, 5-6
  - session security options, 13-3
- DRDA Application Server Function, 1-11
- DRDA Server
  - accessing, 10-9
  - capabilities, native semantics, 12-18
  - CCSID

- character set to store data in DRDA database, D-3
- gateway code page map facility, D-5
- parameters needed for NLS, D-3
- character sets, known restrictions, 2-3
- configuring
  - DB2/400, 5-3
  - DB2/OS390, 5-2
  - DB2/UDB, 5-4
  - DB2/VM, 5-5
- considerations for binding packages, 14-4
- database link behavior, 12-5
- functions, native semantics, 12-18
- gateway architecture definition, 1-8
- Hostname or IP Address (configuring TCP/IP, worksheet), E-2
- port number (TCP/IP), 8-1
- Service Port Number (configuring TCP/IP, worksheet), E-2
- stored procedures, native to DRDA server, 12-3
- DRDA\_CAPABILITY parameter, 12-18
- DRDA\_CMSRC\_CM\_IMMEDIATE parameter, description, C-3
- DRDA\_CODEPAGE\_MAP parameter, D-5
- DRDA\_COMM\_BUFLLEN parameter, description, C-3
- DRDA\_CONNECT\_PARM (SNA format) parameter, description, C-3 (TCP/IP format) parameter, description, C-3
- configuring IBM Communication Server, 7-17
- configuring Microsoft SNA server or host server, 6-15
- parameter
  - communication errors, 15-2
  - configuring the gateway for TCP/IP, 8-4
- DRDA\_DEFAULT\_CCsid parameter, description, C-3
- DRDA\_DESCRIBE\_TABLE parameter
  - description, C-4
  - known restrictions, 2-3
- DRDA\_DESCRIBE\_TABLE=FALSE initialization parameter, 2-3
- DRDA\_DISABLE\_CALL parameter
  - binding the DRDA gateway package, 10-6
  - description, C-4
- DRDA\_FLUSH\_CACHE parameter, description, C-4
- DRDA\_GRAPHIC\_LIT\_CHECK parameter, description, C-5
- DRDA\_GRAPHIC\_PAD\_SIZE parameter, description, C-4
- DRDA\_GRAPHIC\_TO\_MBCS parameter, description, C-5
- DRDA\_ISOLATION\_LEVEL parameter, description, C-5
- DRDA\_LOCAL\_NODE\_NAME parameter, description, C-6
- DRDA\_MBCS\_TO\_GRAPHIC parameter, description, C-6
- DRDA\_OPTIMIZE\_QUERY parameter
  - description, C-6
  - DQO capability turned ON and OFF, 11-4
- DRDA\_PACKAGE\_COLLID parameter
  - description, C-7
  - errors detected by server database, 15-3
- DRDA\_PACKAGE\_CONSTOKEN parameter, description, C-7
- DRDA\_PACKAGE\_NAME parameter
  - description, C-7
  - detecting errors, 15-3
  - value must be unique, 10-6
- DRDA\_PACKAGE\_OWNER parameter, description, C-7
- DRDA\_PACKAGE\_SECTIONS parameter
  - description, C-8
  - number of open cursors at IBM database, 12-28
- DRDA\_READ\_ONLY parameter
  - description, C-8
  - read-only gateway, 11-5
- DRDA\_RECOVER\_USERID parameter
  - DB2/400, 5-4
  - DB2/OS390, 5-3
- DRDA\_RECOVERY\_PASSWORD parameter
  - DB2/OS390, 5-3, 5-4
  - DB2/UDB, 5-5
  - DB2/VM, 5-6
  - description, C-8
- DRDA\_RECOVERY\_USERID parameter
  - DB2/400, 5-4
  - DB2/UDB, 5-5
  - DB2/VM, 5-6
  - description, C-8
- DRDA\_REMOTE\_DB\_NAME parameter, description, C-9
- DRDA\_SECURITY\_TYPE parameter, description, C-9
- DROP DATABASE LINK statement, 11-2
- dropold.sql script, 10-7
- DSPRBDIRE command, 5-4
- dynamic dictionary mapping, 1-4

## E

---

- EBCDIC
  - character set support, D-5
  - code page, D-4
  - DRDA server CCSID, D-11
  - sort order, 12-19
  - tables, known restrictions, 1-13
  - translated to ASCII, 12-21
- EMP
  - creating system-wide synonym for EMP file, 11-4
  - table, 11-6
- empproc
  - stored procedure, 12-3
- encryption
  - export encryption algorithms, 9-4
  - types for Advanced Security, 9-4
- environment
  - distributed, 12-3
  - heterogeneous, replicating in, 11-6

- variable, NLS\_LANG, D-3
- environmental variable
  - NLS\_LANG, D-2
  - ORA\_NLS33, D-2
- errd
  - error array returned from DRDA server
    - database, 15-3
  - example of translated, mapped error, 15-4
  - example, retrieving data, 11-3
- errmc
  - (error tokens), 15-3
  - communication errors, 15-2
  - errmc field lists any error tokens, 15-2
  - example of translated, mapped error, 15-4
  - example, retrieving data, 11-3
- errp
  - errors detected by the DRDA server
    - database, 15-3
  - errp field indicates program that detected
    - error, 15-2
  - example of translated, mapped error, 15-3
  - example, retrieving data, 11-3
- error
  - 12660 (test error for Advanced Security), 9-4
  - basic description, 15-1
  - change
    - ORA-09100 to ORA-28500, 15-2
    - ORA-09101 to ORA-28501, 15-2
  - codes
    - drc, 15-2
    - grc, 15-2
  - communication, 15-2
  - condition, 15-1
  - conversion, C-4
  - date, D-5
  - detected
    - by gateway, 15-2
    - by integrating Oracle instance, 15-2
    - by server database, 15-3
    - in DRDA software, 15-2
  - drc= field
    - 300xx, 15-4
    - 7xx, 15-4
  - HGO-00706, 15-2
  - host database, 15-4
  - interpreting error messages, 15-1
  - mapped sqlstate, 15-3
  - messages & codes, main chapter, 15-1
  - messages, Oracle LONG data type larger than
    - 32740 bytes, 12-21
  - number, return code, 15-1
  - ORA-00001, index constraint violated, 15-3
  - ORA-00942
    - object does not exist, 15-3
    - object name too long, 15-3
  - ORA-01017, logon denied, 15-3
  - ORA-01031, insufficient privileges, 15-3
  - ORA-01460, invalid CCSID, 15-3
  - ORA-01476, divide by zero, 15-3
  - ORA-02019, undefined database link name is

- specified, 15-2
- ORA-28500
  - was ORA-09100, 15-2
  - detected by server database, 15-3
  - example, collection ID or package name not
    - recognized, 15-3
- ORA-28501
  - was ORA-09101, 15-2
  - communication error, 15-2
  - Side Information Profile not defined, 15-2
- ORA-28527, conversion errors, C-4
- ORA-9100 to ORA-9199, reserved for generic
  - gateway layer, 15-2
- Oracle error code for mapped errors, 15-3
- server database, 15-3
- specific error codes, 15-4
- tokens listed by errmc for errors
  - detected by DRDA gateway, 15-2
  - detected by server database, 15-3
- translation, 12-21
  - while binding the gateway package, 10-5
  - with Native Semantics, 12-18
- EXCEPT set operator, 12-20
- execute authority
  - DB2/400, 13-4
  - DB2/UDB, 13-4
  - DB2/VM, 13-4
  - on the gateway DRDA package, 13-4
- EXECUTE command, 1-5
- EXECUTE privilege
  - configuration worksheet, E-3
  - DB2/OS390, 5-2
  - DB2/UDB, 5-5
  - DB2/VM, 5-6
- exits, gateway local date, 12-24
- EXPLAIN PLAN command, 15-5
- EXPLAIN\_PLAN table, features of the
  - gateway, 1-11
- export encryption algorithms, 9-4

## F

- FDS\_CLASS parameter, description, C-9
- FDS\_CLASS\_VERSION parameter, description, C-9
- FDS\_INSTANCE parameter, description, C-10
- features of the gateway
  - main topic, 1-10
  - application development and end-user tools, 1-12
  - application portability, 1-11
  - columns supported in a result set, 1-11
  - distributed applications supported, 1-12
  - EXPLAIN\_PLAN improvement, 1-11
  - fetch reblocking, 1-10
  - heterogeneous database integration, 1-11
  - heterogeneous services architecture, 1-10
  - large base of data access, 1-11
  - minimum impact on existing systems, 1-11
  - Native Semantics, 1-11
  - Oracle Database 10g passthrough
    - supported, 1-10

- Oracle snapshot, 11-6
- performance enhancements, 1-10
- remote data access, 1-11
- retrieving result sets through passthrough, 1-10
- support for TCP/IP, 1-11
- fetch array size, with HS\_FDS\_FETCH\_ROWS, C-10
- fetch reblocking
  - features of the gateway, 1-10
  - supported with
    - HS\_RPC\_FETCH\_REBLOCKING, 12-2
- fetch date, ORA\_MAX\_DATE parameter,
  - description, C-11
- fields
  - errmc, lists any error tokens, 15-2
  - errp, indicates program that detected error, 15-2
- files
  - initsid.ora
    - invalid ORA\_MAX\_DATE specified, 15-4
    - parameter not recognized, 15-3
  - installation log file, verifying successful
    - installation, 4-3
  - listener.ora
    - configure additional instance, 10-9
    - IPC key defined in, 9-3
  - member name, 11-3
  - sample
    - gateway initialization, tnsnames.ora,
      - listener.ora, B-1
    - listener.ora, B-2
  - tnsnames.ora
    - configuring additional DRDA Server
      - instance, 10-9
      - modifying the file, 9-3
    - VSAM, 12-5
- FOR BIT DATA
  - DRDA\_DEFAULT\_CCSID, C-3
  - indicates RAW or LONG RAW, 12-21
  - option, 12-21
- free session,
  - DRDA\_CMSRC\_CM\_IMMEDIATE, C-3
- functions
  - COS, 12-7
  - COUNT, 12-25
  - DBMS\_HS\_PASSTHROUGH.EXECUTE\_IMMEDIATE, 12-26
  - DRDA server, native semantics, 12-18
  - GROUPBY, 12-19
  - HAVING, 12-19
  - ROWID, with UPDATE or DELETE, 2-5
  - SQL, SUBSTR, 12-18
  - SUBSTR
    - known restrictions, 2-3
  - TO\_DATE
    - entering twenty-first century dates, 12-23
    - Oracle function, preprocessed in SQL, 12-24
    - processing DATE data, 12-22
  - WHERE, 12-19

## G

- g4ddtab.sql script, 10-7
- g4ddview.sql script, 10-7
- gateway
  - access, 10-8
  - advantages
    - migration and coexistence, 1-6
    - security, 1-6
    - server technology and tools, 1-6
    - site autonomy, 1-6
    - two-phase commit and multi-site
      - transactions, 1-6
    - use of SQL, 1-2
  - application tools, 1-12
  - architecture, 1-7
  - benefits of integration with Oracle Database 10g
    - server, 1-4
  - configuration, 10-3
  - definition of terms, 1-7
  - de-installing, 4-4
  - features, main topic, 1-10
  - gateway and Oracle integrating server not on same
    - host, 1-7
  - installing, 4-2
  - interface function, 1-9
  - local date exit, 12-24
  - logging, LOG\_DESTINATION, C-11
  - migration problems, backout considerations, 14-2
  - parameter, 5-6
  - performance, 12-18
  - performance enhancements, 1-10
  - service name entries in the tnsnames.ora, 14-4
  - SQL differences, 1-9
  - stored procedures (Oracle and non-Oracle), 1-5
  - supported languages
    - CCSID, D-3
    - codepage map facility, D-5
  - tracing
    - LOG\_DESTINATION, C-11
    - SQL statements, 11-7
- Gateway Initialization File
  - parameter
    - list, C-2
    - new since V4 gateway, 14-2
    - reported errors, 10-5
  - sample, B-1
- Gateway Initialization Parameter,
  - DRDA\_READ\_ONLY, 11-5
- Gateway System Identifier (SID), defined, 10-2
- GCS virtual machine, 13-4
- GLOBAL\_NAMES
  - known restrictions, 2-4
- GRANT
  - DB2/VM security, 13-4
  - statement, synonyms and views, 10-8
- granting authority to a package for DB2, 10-8
- GRAPHIC data type, 12-21
- graphic string operations, unsupported, 12-21
- grc error code, 15-2
- GROUP BY clause, 12-19

GROUPBY function, 12-19  
GTW\$\_BIND\_PKG  
    configuring the host, 10-5  
    gateway package considerations, 10-6

## H

---

hardware requirements, memory, 3-1  
HAVING  
    clause compatible for all versions of DRDA Server, 12-19  
    SQL Functions That Can Be Disabled, 12-19  
heterogeneous database integration, 1-11  
Heterogeneous Services (HS)  
    see also HS, 1-2  
    component of the Oracle Database 10g server, 1-2  
    parameter syntax and usage, C-1  
HGO-00706 error, 15-2  
host  
    architecture, 1-8  
    components when installed on gateway, 1-8  
    creating an independent process, 1-8  
    database error, 15-4  
    networking needs, 3-3  
    relationship to gateway and Oracle server, 1-7  
    variable  
        converting character string data types, 12-21  
        moving data between applications and the database, 12-20  
HS (Heterogeneous Services)  
    architecture features, 1-10  
    Oracle Net considerations, 14-4  
HS= (TNSNAMES parameter for Oracle Net)  
    gateway migration problems, 14-2  
    modify tnsnames.ora file, 9-3  
HS\_DB\_DOMAIN parameter, 2-4  
HS\_DB\_NAME parameter, 2-4  
HS\_FDS\_FETCH\_ROWS parameter,  
    description, C-10  
HS\_LANGUAGE parameter, description, C-10  
HS-NLS\_DATE\_FORMAT  
    NLS parameters for initsid.ora file, D-5  
    parameter, 12-23  
    support, 12-24  
HS-NLS\_DATE\_LANGUAGE, D-5  
HS-NLS\_NCHAR  
    parameter description, C-10  
    parameters in the Gateway Initialization File, D-5  
HS\_RPC\_FETCH\_REBLOCKING parameter  
    fetch reblocking described, 12-2  
    gateway features, 1-10  
HS\_RPC\_FETCH\_SIZE parameter  
    fetch reblocking described, 12-2  
    gateway features, 1-10

## I

---

IBM Communication Server  
    definitions, 7-3  
    server selection, 7-3

implementation, gateway components, 1-8  
implicit data conversion, 12-18  
implicit protocol conversion, 1-4  
IMS transaction, 12-5  
IN and OUT columns, multi-byte support, D-8  
inbound connections  
    processing, 13-3  
Independent LU  
    configuring IBM Communication Server, 7-2  
    configuring Microsoft SNA Server, 6-2  
initsidraho1.ora  
    sample Gateway Initialization File, B-1  
initialization parameters  
    new since V4 gateway, 14-2  
initsid.gtw file  
    sample, 10-3  
initsid.gtwboot  
    file, migrating, 14-1  
    parameters moved to initsid.ora, 10-3  
initsid.ora file  
    containing initsid.gtwboot parameters, 10-3  
    invalid ORA\_MAX\_DATE specified, 15-4  
    migrating, 14-1  
    NLS parameters, D-4  
    parameter not recognized, 15-3  
    parameters have changed format, 14-2  
    sample, 10-3  
    simplified syntax, see Appendix C, 10-3  
    tailoring, 10-4  
input bind variables, 12-23  
INSERT  
    command  
        known restriction, 2-3  
        supported by COPY, 11-6  
    operation, 12-2  
    Oracle SQL command, known restrictions, 2-3  
    SQL clause, 12-24  
    statement  
        dates, 12-23  
        native SQL passthrough, 12-26  
        transaction semantics, 1-9  
    with read-only gateway, 11-5  
installation  
    checklists  
        configuring the gateway, 10-1  
        DRDA Server, 5-1  
        gateway, 4-2  
        Oracle Net, 9-1  
    configuring multiple DRDA Servers  
        details, 10-9  
        overview, 4-2  
    configuring multiple integrating servers  
        details, 10-8  
        overview, 4-2  
    from CD, 4-2  
    log file, INSTALL.LOG, 4-3  
    overview, 4-2  
INSTALL.LOG, 4-3  
internal tracing, C-12  
Internet and intranet support, 1-4

INTERSECT, set operators, 12-20  
IPC adapter, B-2  
ISO standard  
  SQL, 1-5  
isolation level, DRDA\_ISOLATION\_LEVEL, C-5

## J

---

JOIN capability, 1-3  
JOIN SQL statement, 12-2

## K

---

keywords  
  LISTENER, sample listener.ora file, B-2  
known restrictions  
  main topic, 2-3  
  accessing DB2 alias objects, 2-3  
  AVS mapping user IDs, 2-3  
  bind variables become SQL parameter markers, 2-6  
  binding the DRDA gateway package on DB2/UDB, 2-4  
  CONNECT BY not supported, 2-6  
  data type limitations, 2-3  
  date arithmetic, 2-4  
  DD basic tables and views, 2-3  
  dictionary views not provided for DB2/VM, 2-5  
  DRDA server character sets, 2-3  
  GLOBAL\_NAMES parameter, 2-4  
  LONG data type in SQL\*Plus, 2-4  
  null values and stored procedures, 2-4  
  Oracle ROWID column, 2-5  
  row length, 2-4  
  row length limitation, 2-4  
  SAVEPOINT, 2-4  
  single gateway instances per DRDA network interface, 2-5  
  string concatenation, 2-4  
  SUBSTR function post-processed, 2-3

## L

---

LANGUAGE parameter, D-5  
languages  
  SQL\*Plus, 1-6  
  tools supported through the gateway, 1-5  
link  
  also see Database Link, 12-5  
  service definition, 6-5  
linkage conventions  
  SIMPLE with nulls, 12-5  
listener  
  sample Oracle Net listener.ora file, B-2  
LISTENER keyword, sample listener.ora file, B-2  
listener.ora file  
  configuring additional DRDA Server instances, 10-9  
  IPC key defined, 9-3  
  sample, B-2  
literal

  character literals, 12-22  
  date, 12-22  
  specific data type, 12-20  
  TO\_DATE, 12-24  
Local LU definition, 6-9  
location transparency (introduction), 1-3  
log file, installation, verifying success, 4-3  
LOG\_DESTINATION parameter  
  description, C-11  
  used with ORACLE\_DRDA\_TRACE, C-12  
logging, LOG\_DESTINATION, C-11  
LONG columns, known restrictions, 2-4  
LONG data type  
  converting character string data types, 12-21  
  known restrictions, 2-4  
LONG RAW data type, translating ASCII to EBCDIC, 12-21  
LUs  
  dependent, 7-2  
  independent, 7-2  
  independent and dependent, 6-2  
  local definition, alias, network name, 6-9  
  remote definition, 6-13

## M

---

mapped sqlstate errors, 15-3  
mapping user IDs, known restrictions, 2-3  
memory, hardware requirements, 3-1  
Microsoft Windows Sockets, network attachment, 3-2  
migration  
  defined, 14-1  
  migrating the gateway instance, 14-4  
  obsolete parameters, 14-3  
  problems, backout considerations, 14-2  
MINUS  
  set operator, 12-20  
Mobile Agents, 1-4  
Mode definition, 6-11  
multi-byte support, D-8

## N

---

National Language Support  
  initsid.ora parameters, D-4  
  overview, D-1  
Native Semantics  
  main topic, 12-18  
  gateway features, 1-11  
  parameters, 12-19  
  with SUBSTR function, 2-3  
native SQL passthrough, 12-25  
network  
  configuration tool, 8-1  
  Oracle Net configuration, 9-3  
  requirements, 3-2  
  transparency (introduction), 1-3  
NLS  
  also see National Language Support, D-1



- DRDA server character sets
  - codepage map facility, D-5
  - parameters needed for NLS processing, D-3
- NLS parameters, configuration on client and Oracle servers, D-3
- NLS\_LANG
  - environment variable
    - client-server configuration, D-3
    - parameters needed for NLS processing, D-2
  - server-side parameter, D-2
- non-character binary data, 12-21
- null
  - rows, mapping the COUNT function, 12-25
  - values
    - known restrictions, 2-4
    - mapping the COUNT function, 12-25
- number of cursors,
  - DRDA\_PACKAGE\_SECTIONS, C-8
- numbers, concatenation restrictions, 2-4
- numeric data type
  - conversion, destination column, 12-25
  - zoned decimal operations, 12-25

## O

- o2pc.sql
  - binding the DRDA gateway package, 10-8
  - two-phase commit processing, 11-5
- obsolete parameters since V4 gateway, 14-3
- open cursors, at the IBM database, 12-28
- OPEN\_LINKS parameter, 11-2
- operating system requirements, 3-2
- operating system transparency (introduction), 1-3
- operations, SELECT, INSERT, UPDATE, DELETE, 12-2
- operators
  - UNION, 12-19
  - UNION ALL, 12-19
- option
  - binding packages, 10-6
  - data dictionary views, 12-28
  - date format string, 12-23
  - DRDA session security, 13-3
  - FOR BIT DATA, 12-21
  - Oracle server, 1-7
  - read-only
    - gateway configuration, 1-6
    - no updates permitted by gateway, 11-5
  - replicating, 11-6
  - security conduct, 13-3
  - service port number,
    - DRDA\_CONNECT\_PARM, C-3
  - SNA security
    - configuring IBM Communication Server, 7-18
    - configuring Microsoft SNA Server or Host Integration Server, 6-16
  - SQL functions that can be disabled, 12-19
  - SQL functions that can be enabled, 12-18
  - SQL\*Plus COPY command, 11-6
- ora

- listener.ora file, 10-9
- tnsnames.ora file, 9-3
- ORA\_MAX\_DATE parameter, description, C-11
- ORA\_NLS33 parameter
  - description (default value), C-11
  - needed in system environment, D-2
- ORA-00001 error, index constraint violated, 15-3
- ORA-00942 error
  - object does not exist, 15-3
  - object name too long, 15-3
- ORA-01017 error, logon denied, 15-3
- ORA-01031 error, insufficient privileges, 15-3
- ORA-01460 error, invalid CCSID, 15-3
- ORA-01476 error, divide by zero, 15-3
- ORA-02019 error, undefined database link name is specified, 15-2
- ORA1 Oracle instance, 12-2
- ORA-28500 error
  - was ORA-09100, 15-2
  - example, collection ID or package name not recognized, 15-3
- ORA-28501 error
  - was ORA-09101, 15-2
  - communication error, 15-2
  - Side Information Profile not defined, 15-2
- ORA-28527, conversion errors, C-4
- ORA-9100 error, 15-2
- ORA-9199 error, 15-2
- Oracle
  - error code, mapped errors, 15-3
  - error number or return code, 15-1
  - products compatibility, 1-9
  - RAW data type, C-3
  - snapshots, 11-6
  - stored procedure, defined, 12-2
- Oracle Database 10g server
  - introduction, 1-2
  - relationship to host, 1-7
  - services
    - list, 1-3
    - database triggers, 1-4
    - distributed capabilities, 1-3
    - distributed query optimization, 1-3
    - SQL, 1-3
    - stored procedures, 1-4
    - two-phase commit protection, 1-4
- Oracle integrating server
  - architecture, 1-7
  - configuration, 10-8
  - defined in gateway architecture, 1-7
  - gateway and Oracle integrating server not on same host, 1-7
  - requirements, 3-3
- Oracle Net
  - and application development, 1-12
  - and remote data access, 1-11
  - and server coexistence, 1-7
  - API, 9-2
  - compatibility with SQL\*Net, 9-2
  - configuring, 9-3

- distributed
    - database, 9-2
    - processing, 9-2
  - editing to set up security test, 9-4
  - gateway and Oracle integrating server not on same host, 1-7
  - gateway migration problems, 14-2
  - Heterogeneous Services (HS) facility, 9-2
  - introduction, 9-2
  - migration considerations, 14-4
  - operating system authentication, 13-2
  - overview, 9-2
  - purpose, 1-8
  - requirements, 3-3
  - sample files, B-1
  - sample listener.ora file, B-2
  - support (introduction), 1-6
  - support for CHECKSUM and encryption, 9-4
  - terminology, 9-2
  - Oracle ROWID column, 2-5
  - Oracle ROWID function, with UPDATE or DELETE, 2-5
  - ORACLE\_DRDA\_TCTL parameter, description, C-11
  - ORACLE\_DRDA\_TRACE parameter, description, C-11
  - ORACLE\_HOME, preinstallation and caution notice, 4-2
  - ORACLE2PC table
    - before binding gateway package, 10-7
    - binding packages on DB2/UDB, 10-5
    - DB2/400, 5-4
    - DB2/OS390, 5-2
    - DB2/UDB, 5-5
    - DB2/UDB, granting authority to package, 10-8
    - DB2/VM, 5-6
    - distributed DRDA transactions, 11-5
    - DRDA\_PACKAGE\_OWNER description, C-8
  - ORADRDA.ORACLE2PC table, two-phase commit, 11-5
  - ORAIND sample DB2 stored procedure, G-2
  - oraproc1, stored procedure, 12-2
  - oraproc2, stored procedure, 12-2
  - ORARECOV user ID
    - DB2/400, 5-4
    - DB2/OS390, 5-3
    - DB2/UDB, 5-5
    - DB2/VM, 5-6
    - DRDA\_RECOVERY\_USERID description, C-9
  - ORA2 Oracle instance, 12-2
  - ORDER BY clause, 12-19
  - OS/390 (MVS) VTAM, configuring, 5-2
- P**
- 
- package
    - collection id, DRDA\_PACKAGE\_COLLID, C-7
    - consistency token,
      - DRDA\_PACKAGE\_CONSTOKEN, C-7
    - privileges - BIND and EXECUTE, DB2/UDB, 5-5
    - privileges - BIND, COPY, and EXECUTE
      - configuration worksheet, E-3
      - DB2/OS390, 5-2
      - DB2/VM, 5-6
  - packed decimal, 12-25
  - parameter
    - changed, 14-3
    - checking settings, 10-6
    - diagnostic, C-11
    - gateway, 5-6
    - list of parameters needed to configure the gateway, E-1
    - Native Semantics, 12-19
    - new since V4 gateway, 14-2
    - obsolete since V4 gateway, 14-3
    - parameter syntax and usage, C-1
    - renamed since V4 gateway, 14-3
  - parameters
    - DB\_DOMAIN, 2-4
    - DRDA\_CAPABILITY, 12-18
    - DRDA\_CODEPAGE\_MAP
      - described, C-2
      - mapping IBM CCSID, D-5
    - DRDA\_CONNECT\_PARM
      - configuring IBM Communication Server, 7-17
      - configuring Microsoft SNA server or host server, 6-15
      - configuring the gateway for TCP/IP, 8-4
    - DRDA\_DESCRIBE\_TABLE, known restrictions, 2-3
    - DRDA\_DISABLE\_CALL, 10-6
    - DRDA\_PACKAGE\_NAME, 10-6
    - DRDA\_PACKAGE\_SECTIONS, open cursors, 12-28
    - DRDA\_READ\_ONLY, read-only gateway, 11-5
    - DRDA\_RECOVERY\_PASSWORD
      - DB2/400, 5-4
      - DB2/OS390, 5-3
      - DB2/UDB, 5-5
      - DB2/VM, 5-6
    - DRDA\_RECOVERY\_USERID
      - DB2/400, 5-4
      - DB2/OS390, 5-3
      - DB2/UDB, 5-5
      - DB2/VM, 5-6
    - FDS\_CLASS, description, C-9
    - FDS\_CLASS\_VERSION, description, C-9
    - FDS\_INSTANCE, description, C-10
    - Gateway Initialization File
      - DRDA\_CACHE\_TABLE\_DESC, C-2
      - DRDA\_CAPABILITY, C-2
      - DRDA\_CMSRC\_CM\_IMMEDIATE, C-3
      - DRDA\_CODEPAGE\_MAP, C-2
      - DRDA\_COMM\_BUFLLEN, C-3
      - DRDA\_CONNECT\_PARM
        - communication errors, 15-2
        - configuring the gateway for TCP/IP, 8-4
        - DRDA\_CONNECT\_PARM (SNA format), C-3

DRDA\_CONNECT\_PARM (TCP/IP format), C-3  
 DRDA\_DEFAULT\_CCSD, C-3  
 DRDA\_DESCRIBE\_TABLE, C-4  
 DRDA\_DISABLE\_CALL, C-4  
 DRDA\_FLUSH\_CACHE, C-4  
 DRDA\_GRAPHIC\_LIT\_CHECK, C-5  
 DRDA\_GRAPHIC\_PAD\_SIZE, C-4  
 DRDA\_GRAPHIC\_TO\_MBCS, C-5  
 DRDA\_ISOLATION\_LEVEL, C-5  
 DRDA\_LOCAL\_NODE\_NAME, C-6  
 DRDA\_MBCS\_TO\_GRAPHIC, C-6  
 DRDA\_OPTIMIZE\_QUERY, 11-4, C-6  
 DRDA\_PACKAGE\_COLLID, 15-3, C-7  
 DRDA\_PACKAGE\_CONSTOKEN, C-7  
 DRDA\_PACKAGE\_NAME, 15-3, C-7  
 DRDA\_PACKAGE\_OWNER, C-7  
 DRDA\_PACKAGE\_SECTIONS, C-8  
 DRDA\_READ\_ONLY, C-8  
 DRDA\_RECOVERY\_PASSWORD, C-8  
 DRDA\_RECOVERY\_USERID, C-8  
 DRDA\_REMOTE\_DB\_NAME, C-9  
 DRDA\_SECURITY\_TYPE, C-9  
 HS\_FDS\_FETCH\_ROWS, C-10  
 HS\_LANGUAGE, C-10  
 HS-NLS\_NCHAR, C-10  
 LOG\_DESTINATION, C-11  
 ORA\_MAX\_DATE, C-11  
 ORA-NLS33, C-11  
 ORACLE\_DRDA\_TCTL, C-11  
 ORACLE\_DRDA\_TRACE, C-11  
 TRACE\_LEVEL, C-12  
 HS\_DB\_DOMAIN, 2-4  
 HS\_DB\_NAME, 2-4  
 HS-NLS\_DATE\_FORMAT, 12-23  
 HS\_RPC\_FETCH\_REBLOCKING gateway features, 1-10 gateway support for fetch reblocking, 12-2  
 HS\_RPC\_FETCH\_SIZE gateway features, 1-10 gateway support for fetch reblocking, 12-2  
 LOG\_DESTINATION, description, C-12  
 NLS\_DATE\_FORMAT, 12-23  
 OPEN\_LINKS, 11-2  
 passthrough  
   DBMS\_HS\_PASSTHROUGH.EXECUTE\_IMMEDIATE gateway features, 1-10  
   DBMS\_HS\_PASSTHROUGH.EXECUTE\_IMMEDIATE syntax using the passthrough function, 12-26 example, 12-27 gateway feature, 1-5 native SQL through the gateway, 12-25 result sets example, 12-27 result sets from queries, 12-26 retrieving result sets, 12-27 SQL feature, 12-25 performance enhancements with fetch reblocking, 12-2  
 PL/SQL  
   call, 12-4  
   records, 12-5  
   routine, 1-5  
   running stored procedures, 12-3  
   standard Oracle, 1-5  
   stored procedure, 12-2  
 port number  
   446 as default for DRDA services (TCP/IP), 8-1  
   5000 as default for DRDA services (TCP/IP), 8-1  
   for DRDA Server (TCP/IP), 8-1  
   Primary  
     DB2/400, 5-3  
     DB2/OS390, 5-2  
   Recovery  
     DB2/400, 5-3  
     DB2/OS390, 5-2  
 post processing  
   defined, 12-6  
   native semantics, 12-18  
   post-processed SQL functions, overview, 12-6  
   SQL tracing, 15-5  
 PREPARE TRANSACTION statement, two-phase commit, 11-5  
 primary port number  
   DB2/400, 5-3  
   DB2/OS390, 5-2  
 privileges  
   BIND  
     configuration worksheet, E-3  
     DB2/OS390, 5-2  
     DB2/UDB, 5-5  
     DB2/VM, 5-6  
   BINDADD  
     configuration worksheet, E-3  
     DB2/OS390, 5-2  
     DB2/UDB, 5-5  
     DB2/VM, 5-6  
   BINDAGENT  
     configuration worksheet, E-3  
     DB2/OS390, 5-2  
     DB2/VM, 5-6  
   CONNECT  
     DB2/UDB, 5-5  
   COPY  
     configuration worksheet, E-3  
     DB2/OS390, 5-2  
     DB2/VM, 5-6  
   CREATE IN  
     configuration worksheet, E-3  
     DB2/OS390, 5-2  
     DB2/VM, 5-6  
   CREATE PUBLIC DATABASE LINK  
     binding the DRDA gateway package, 10-5  
     configuring the Oracle integrating server, 10-8  
   CREATEIN  
     DB2/UDB, 5-5  
   CREATETAB  
     DB2/OS390, 5-2  
     DB2/UDB, 5-5

- data dictionary limitations, 12-28
  - EXECUTE
    - configuration worksheet, E-3
    - DB2/OS390, 5-2
    - DB2/UDB, 5-5
    - DB2/VM, 5-6
  - procedure
    - stored procedures
      - REVISE\_SALARY, example, 12-4
      - using DRDA server, 12-3
      - with read-only gateway, 11-5
  - procedures
    - DB2
      - DB2INS, sample, G-1
      - ORAIND, sample, G-2
  - processing time, with GROUPBY, HAVING, WHERE, 12-19
  - processor requirements, 3-1
  - profile set, APPC, configuring, 10-9
  - protocol
    - commit confirm, 1-6
    - communications and DRDA-specific parameters, 8-4
    - communications protocols with Oracle Net, 9-2
    - converter, 1-4
    - definition, 9-2
    - implicit protocol conversion, 1-4
    - network, 11-4
    - Oracle Net Protocol Adapters, 9-2
    - protocol-independent encryption, 1-4
    - two-phase commit, 11-5
  - protocols
    - IPC, 9-3
    - SNA, for the DRDA server, 1-8
    - TCP/IP
      - for the DRDA server, 1-8
      - how supported, 1-11
      - implicit protocol conversion, 1-4
  - public database link, 10-8
- Q**
- 
- queries, distributed, 11-4
- R**
- 
- RAW data type
    - DRDA\_DEFAULT\_CCSDID description, C-3
    - translating ASCII to EBCDIC, 12-21
  - read-only gateway
    - main topic, 11-5
    - option, DRDA\_READ\_ONLY, C-8
  - read-only support, changes in this release, 1-13
  - rebind
    - DRDA\_DISABLE\_CALL, C-4
    - DRDA\_ISOLATION\_LEVEL, C-6
    - DRDA\_PACKAGE\_COLLID, C-7
    - DRDA\_PACKAGE\_CONSTOKEN, C-7
    - DRDA\_PACKAGE\_NAME, C-7
    - DRDA\_PACKAGE\_OWNER, C-8
    - DRDA\_PACKAGE\_SECTIONS, C-8
  - recovery port number
    - DB2/400, 5-3
    - DB2/OS390, 5-2
  - recovery user ID and password
    - DB2/400, 5-4
    - DB2/OS390, 5-3
    - DB2/UDB, 5-5
    - DB2/VM, 5-6
  - remote
    - computer, 9-2
    - connections, 11-2
    - data, 1-3
    - data access, 1-11
    - database
      - configuration worksheet, E-3
      - copy data from Oracle Database server to DRDA Server database, 11-6
      - creating database links, 11-2
      - DB2/400, 5-4
      - DB2/OS390, 5-3
      - DB2/UDB, 5-5
      - DB2/VM, 5-6
      - defining a path, 11-1
      - DRDA gateway package considerations, 10-6
      - DRDA\_PACKAGE\_SECTIONS, C-8
      - example error message, 15-2
      - gateway error codes, 30061, RDB not found, 15-5
    - DB2 system, 2-3
    - DRDA database,
      - DRDA\_ISOLATION\_LEVEL, C-5
    - instance, 12-2
    - LU definition, 6-13
    - objects, 13-2
    - Oracle instance
      - running a DB2 stored procedure, 12-4
      - synonym for calling a stored procedure, 12-3
    - Oracle servers, 9-2
    - procedure, 1-5
    - table, 1-4
    - transaction program, 3-1
    - userid and password, 11-1
  - renamed parameters, 14-3
  - REPLACE
    - command, supported by COPY, 11-6
  - replication in heterogeneous environment, 11-6
  - requirements
    - hardware, 3-1
    - software, 3-2
  - restrictions, 2-3
  - RESULT, 12-4
  - result sets
    - columns in, 1-11
    - features of the gateway, 1-10
  - return code, error, 15-1
  - REVISE\_SALARY
    - stored procedure example, 12-4
  - row length
    - known restrictions, 2-4

ROWID  
known restrictions, 2-5  
Oracle column, 2-5  
with UPDATE or DELETE, 2-5

## S

sample  
files  
gateway initialization, tnsnames.ora,  
listener.ora, B-1  
initsid.gtw, 10-3  
initsid.ora, 10-3  
Gateway Initialization File, initsrdahoa1.ora, B-1  
listener.ora file, B-2  
SQL scripts, 10-7  
SAVEPOINT, known restrictions, 2-4  
schema privileges - CREATEIN, 5-5  
scripts  
dropold.sql, 10-7  
g4ddtab, 10-7  
g4ddview.sql, 10-7  
security  
Advanced Security, 1-4  
DRDA\_SECURITY\_TYPE, C-9  
encryption, 9-4  
overview, 13-1  
site autonomy, 1-6  
validation for SNA, 6-16, 7-18  
validation for TCP/IP, 13-3  
SELECT  
and array size, 1-10  
operation, 12-2  
SQL statement, 12-27  
statement  
compensated SQL functions, 12-6  
dates, 12-23  
fetch reblocking, 12-2  
retrieve results sets, 12-27  
with read-only gateway, 11-5  
SELECT WHERE SQL clause, 12-24  
semantics, 12-18  
server selection, 6-4, 7-3  
service port number,  
DRDA\_CONNECT\_PARM, C-3  
session, connection, 12-5  
set operators  
compatibility, 12-19  
EXCEPT, 12-20  
INTERSECT, 12-20  
MINUS, 12-20  
SQL set operators and clauses, 12-20  
shift attribute, multi-byte support, D-9  
SID  
choosing a gateway SID, 10-2  
configuring additional DRDA server  
instances, 10-9  
Gateway System Identifier, defined, 10-2  
Side Information Profile  
communication error, 15-2  
definition, 6-2, 7-1  
SIMPLE linkage convention  
DB2INS, sample DB2 stored procedure, G-1  
of DB2 stored procedures, 12-5  
site autonomy, 1-6  
SNA, 5-4  
configuring  
AS/400 communications, 5-3  
OS/390 communications, 5-2  
VM communications, 5-6  
conversation security, 6-16, 7-18  
CPI-C error, 15-2  
facilities, 1-11  
functions, 1-8  
LU, 13-3  
protocol  
DRDA server support, 1-8  
remote access, 1-12  
security validation  
IBM Communication Server, 7-18  
Microsoft SNA Server or Host Integration  
Server, 6-16  
versus TCP/IP security, 13-3  
security, DRDA\_SECURITY\_TYPE, C-9  
SECURITY=PROGRAM, 6-17, 7-19  
SECURITY=SAME, 6-17, 7-19  
send/receive buffer, C-3  
session allocation mode,  
DRDA\_CMSRC\_CM\_IMMEDIATE, C-3  
SNA Server  
connection definition, 6-7  
CPI-C symbolic destination names, 6-14  
definitions  
creating side information profiles, 7-1  
creating SNA definitions for SNA Server  
version 3, 6-3  
side information profiles, 6-2  
for Windows NT, 6-2  
link service definition, 6-5  
local LU definition, 6-9  
mode definition, 6-11  
remote LU definition, 6-13  
server selection, 6-4  
testing the connection, 6-15  
SNA Server for Windows NT  
dependent LUs, 7-2  
independent LUs, 7-2  
testing the connection, 7-17  
SNACFG command, 6-3  
snacfg.ctl file, 6-2, 7-2  
snapshots  
known restrictions, 2-5  
Oracle snapshot feature, 11-6  
software requirements, 3-2  
sort order  
with ORDERBY, 12-19  
SPUFI on DB2/OS390, 10-7  
SQL  
main topic, 1-5  
ANSI standard, 1-5

- clause compatibility, 12-19
- clauses
  - DELETE, 12-24
  - INSERT, 12-24
  - SELECT WHERE, 12-24
  - UPDATE, 12-24
- constructs, Oracle processing, 12-6
- differences in the gateway, 1-9
- functions
  - and Native Semantics, 12-18
  - quick reference list, F-1
  - SUBSTR, 12-18
- ISO standard, 1-5
- native DB2, 1-5
- passthrough
  - described, 12-25
  - retrieving results sets example, 12-27
  - using
    - DBMS\_HS\_PASSTHROUGH.EXECUTE\_I  
MMEDIATE, 12-26
- statements
  - DB2, 12-27
  - DRDA\_ISOLATION\_LEVEL, C-5
  - passing through gateway, 12-25
  - run through the gateway, 11-7
  - using JOIN, 12-2
- syntax, 12-25
- tracing
  - improving performance, 11-7
  - tracing errors in the Oracle Database, 15-5
- SQL functions
  - column functions, 12-6
  - compatible, defined, 12-6
  - compensated, defined, 12-6
  - DB2/400, 12-12
  - DB2/OS390, 12-7
  - DB2/UDB, 12-9
  - DB2/VM, 12-15
  - that can be disabled, 12-19
  - that can be enabled, 12-18
  - translated
    - defined, 12-6
    - with Native Semantics, 12-18
- SQL set operators and clauses, 12-20
- SQL\*Net
  - Heterogeneous Services (HS) facility, 9-2
  - replaced by Oracle Net, 9-2
- SQL\*Plus
  - connecting gateway to Oracle integrating  
server, 9-5
  - copying data from Oracle server to DRDA  
Server, 11-6
  - extending gateway uses, 1-10
  - introduction, 1-6
- sqlstate, mapped sqlstate errors, 15-3
- stability, of cursor,
  - DRDA\_ISOLATION\_LEVEL, C-6
- Startup Shell Script
  - migration, 14-1
- statements
  - CREATE DATABASE LINK, 11-1
  - CREATE DATABASE, client/server  
configuration, D-3
  - DB2 CREATE TABLE, 1-5
  - DDL
    - nonqueries supported by gateway  
passthrough, 12-26
    - number of rows affected by  
passthrough, 12-27
  - DELETE
    - and TO\_DATE function, 12-23
    - nonqueries supported by gateway  
passthrough, 12-26
  - DROP DATABASE LINK, 11-2
  - GRANT, 10-8
  - INSERT
    - and TO\_DATE function, 12-23
    - nonqueries supported by gateway  
passthrough, 12-26
  - passing SQL through gateway, 12-25
  - PREPARE TRANSACTION, two-phase  
commit, 11-5
  - SELECT
    - and TO\_DATE function, 12-23
    - compensated SQL functions, 12-6
    - fetch reblocking, array size, 12-2
    - retrieve results sets, 12-27
    - with read-only gateway, 11-5
  - SQL
    - DB2, 12-27
    - JOIN, 12-2
    - SELECT, 12-27
  - UPDATE
    - and TO\_DATE function, 12-23
    - nonqueries supported by gateway  
passthrough, 12-26
- stored procedure
  - creating on DB2, 12-4
- DB2
  - considerations for use, 12-5
  - native to DRDA server, 12-3
  - with read-only gateway, 11-5
- DB2INS, sample, G-1
- extended database services, 1-4
- GTW\$\_BIND\_PKG, 10-5
- native DB2, 1-5
- Oracle and non-Oracle, 1-5
- Oracle Database 10g server
  - using, 12-2
- Oracle database server
  - local instance, 12-2
  - PL/SQL, 12-2
  - remote instance, 12-2
- Oracle, description, 1-5
- ORAIND, sample, G-2
- restriction, 2-4
- REVISE\_SALARY, example, 12-4
- usage, C-4
- using DRDA server, 12-3

- string concatenation, known restrictions, 2-4

string index, with Native Semantics, 12-18  
Structured Query Language, also see SQL, 1-2  
SUBSTR

SQL function  
known restrictions, 2-3  
Oracle implementation permits negative values, 12-18  
with Native Semantics, 2-3

synonym  
feature, 11-3  
for location transparency, 12-3  
how the gateway works, 1-9  
system privileges - BINDADD and BINDAGENT  
configuration worksheet, E-3  
DB2/OS390, 5-2  
DB2/VM, 5-6

## T

table  
create a table in DB2, 12-27  
insert a row into a DB2 table, 12-27  
TABLE\_PRIVILEGES view, A-10  
tables  
ORACLE2PC, 10-7, 10-8  
ORACLE2PC, distributed transactions, 11-5  
ORADRD.AORACLE2PC, two-phase commit, 11-5  
tailoring  
initsid.ora file, 10-3  
TCP/IP  
affecting memory requirements, 3-1  
concurrent connections, 3-1  
configuration chapter, 8-1  
configuration worksheet, E-1  
configuring  
for AS/400, 5-3  
for OS/390, 5-2  
for VM, 5-6  
to use DNS, 8-3  
using DRDA\_CONNECT\_PARM parameter, 8-4  
database link behavior, 12-5  
default port number, 9-4  
DRDA\_CONNECT\_PARM, C-3  
facilities, 1-11  
format, gateway initialization file parameter, C-3  
functions, 1-8  
gateway architecture, connecting to DRDA Server, 1-8  
known restrictions, DRDA Network Interfaces, 2-5  
modifying tnsnames.ora in Oracle Net, 9-3  
protocol  
access across multiple networks - transparency, 1-3  
DRDA server support, 1-8  
implicit protocol conversion, 1-4  
remote access, 1-12  
sample Oracle Net listener.ora file, B-2

security validation, 13-3  
support, 1-11  
you must choose either SNA or TCP/IP for the Networking Interface, 8-4  
terminology defined, 1-7  
tg4drda\sna\commsvr subdirectory, sample SNA Server definitions, 7-2  
tg4drda\sna\mssna subdirectory, sample SNA Server definitions, 6-2  
TIME data type, 12-22  
time operations, 12-22  
TIMESTAMP data type, 12-22  
TNSNAMES.ORA  
changes to, during migration problems, 14-2  
tnsnames.ora  
adding a gateway service name, 9-3  
configuring additional DRDA Server instances, 10-9  
connect descriptor, 11-1  
using the HS facilities, 14-4  
TO\_DATE function  
Oracle function preprocessed in SQL, 12-24  
processing DATE data, 12-22  
twenty-first century dates, 12-23  
token  
error tokens, 15-2  
package consistency,  
DRDA\_PACKAGE\_CONSTOKEN, C-7  
trace control, C-11  
TRACE\_LEVEL parameter, C-12  
tracing  
code, C-12  
LOG\_DESTINATION, C-11  
ORACLE\_DRDA\_TRACE, C-12  
SQL statements, 11-7  
trade-off, Native Semantics, 12-18  
transaction mode, read-only,  
DRDA\_READ\_ONLY, C-8  
transactions  
CICS, 12-5  
IMS, 12-5  
transform  
character set transforms with multi-byte support, D-8  
not required for DRDA Server, D-10  
transparency  
and performance, 12-18  
main topic, gateway transparency, 1-3  
triggers for Oracle Database 10g server, 11-6  
TSO, 5-2  
two-phase commit  
ORACLE2PC table  
DB2/400, 5-4  
DB2/OS390, 5-2  
DB2/UIDB, 5-5  
DB2/VM, 5-6  
protection, 1-4  
transactions, distributed queries, 11-5  
unsupported statement, 11-5

## U

---

UNION  
  capability, 1-3  
  operator, 12-19

UNION ALL  
  operator, 12-19

UPDATE  
  known restrictions, 2-5  
  operation, 12-2  
  SQL clause, 12-24  
  statement  
    dates, 12-23  
    native SQL passthrough, 12-26  
    transaction semantics, 1-9  
    with read-only gateway, 11-5

upgrading, defined, 14-1

user privileges, 12-28

USER\_CATALOG view, A-10

USER\_COL\_COMMENTS view, A-10

USER\_CONS\_COLUMNS view, A-11

USER\_CONSTRAINTS view, A-11

USER\_DB\_LINKS data dictionary view, 11-2

USER\_INDEXES view, A-11

USER\_OBJECTS view, A-13

USER\_SYNONYMS view, A-13

USER\_TAB\_COLUMNS view, A-15

USER\_TAB\_COMMENTS view, A-16

USER\_TABLES view, A-14

USER\_USERS view, A-16

USER\_VIEWS view, A-17

userid mapping  
  DB2/400, 13-4  
  DB2/OS390, 13-3  
  DB2/VM, 13-4  
  security, 13-3

userid translation  
  DB2, 13-4

USING clause, 11-1

## V

---

VALUES clause, 12-24

VARCHAR data type, 12-21

variable  
  bind, 12-26  
  input bind, 12-23

view  
  catalog  
    DB2/400, 12-28  
    DB2/OS390, 12-28  
    DB2/UDB, 12-28  
    DB2/VM, 12-28  
  creating, 10-8  
  data dictionary, 12-28

VSAM file, 12-5

VTAM  
  DB2/OS390, 5-2  
  DB2/VM VTAM configuring, 5-6

## W

---

WHERE clause  
  compatible for all versions of DRDA  
    Server, 12-19  
  SQL limitations, Oracle ROWID column, 2-5

WHERE CURRENT OF CURSOR clause, ROWID  
  column, 2-5

WHERE function, 12-19

wireless communication, 1-4

workarounds, 2-3

## Z

---

zoned decimal operations, 12-25