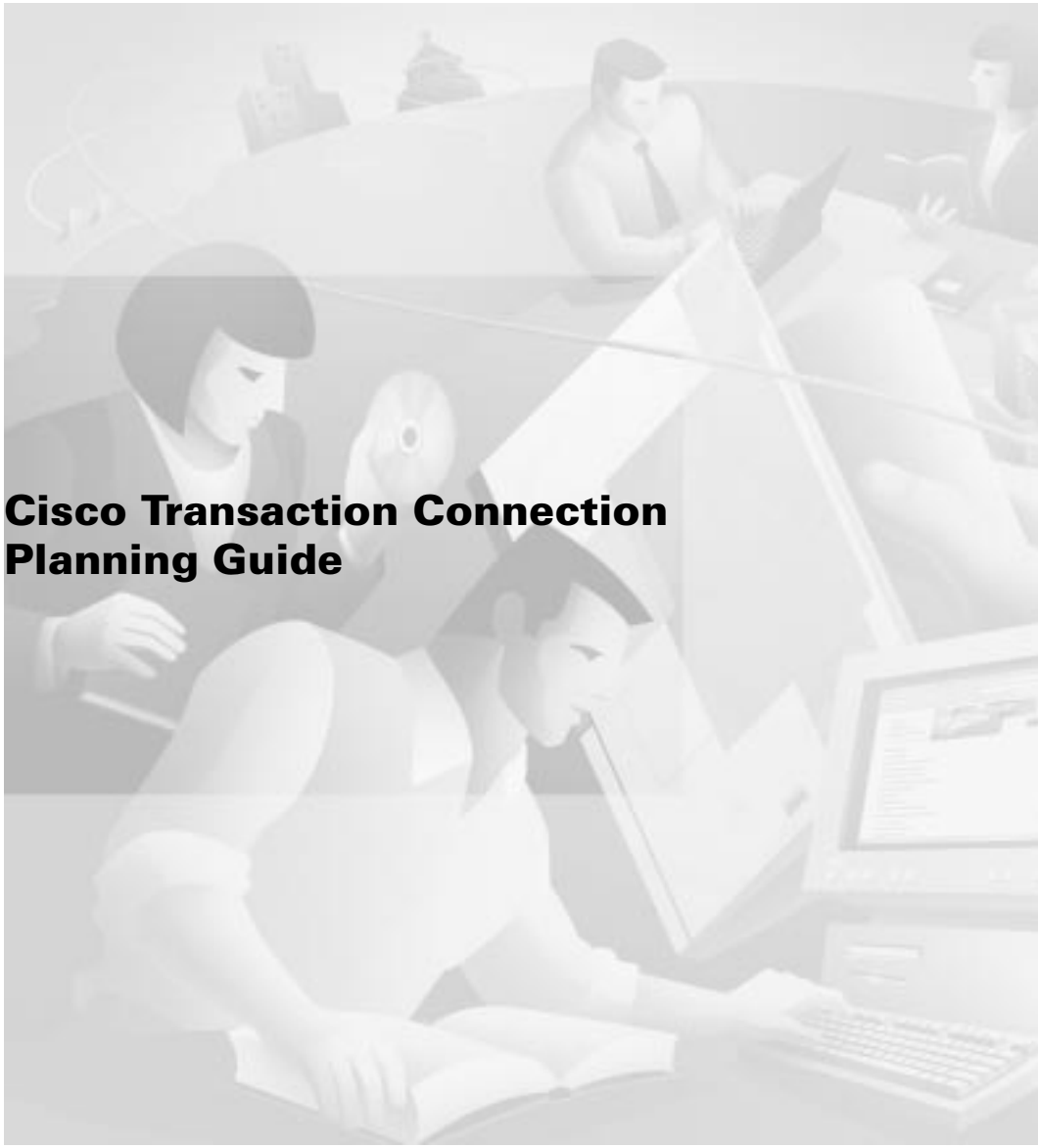


Cisco Transaction Connection Planning Guide

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CONTENTS

CHAPTER 1

Introduction

Cisco Transaction Connection Overview

Cisco Transaction Connection (CTRC) is a Cisco IOS Software feature that enables access to host resident operational data in Customer Information Control System (CICS) and IBM relational database management system (DB2). It became available in then Cisco IOS Release 12.05(XN).

CTRC is available on the following platforms:

- Cisco 7200 Series routers
- Cisco 7500 Series routers

CTRC and DB2

The CTRC, previously called Cisco Database Connection (CDBC), enables access to IBM's DB2 database resources from TCP/IP desktops and servers. It supports the Distributed Relational Database Architecture (DRDA).

CTRC provides a gateway between client workstations using DRDA requestors on TCP/IP networks and IBM DB2 databases on Systems Network Architecture (SNA) networks. Many of the available workstation-based DRDA requestors are Open Database Connectivity (ODBC) clients. ODBC is a call-level interface developed by Microsoft. It allows an application to use a single interface to access database management systems from different vendors.

CTRC accepts DRDA client requests over TCP/IP, and either converts the messages to SNA before sending them to DB2, or passes TCP messages on to DB2 across TCP/IP. On the reply, CTRC converts the SNA messages to TCP/IP and sends them across the network, back to the client.

CTRC supports TCP/IP pass through to DB2 systems that support direct TCP/IP access. In this case, TCP/IP can be used instead of SNA for connection between the router and the host database.

CTRC supports Workload Manager for OS/390. For more information on Workload Manager, refer to the document *OS/390 MVS Planning: Workload Management (GC28-1761).*

CTRC also supports Password Expiration Management (PEM) in SNA networks where PEM is supported to match functionality provided in DRDA over TCP/IP.

CTRC and CICS

CTRC enables access to CICS from TCP/IP clients and servers. It allows Cisco routers to use the Intersystem Communication Protocol, and provides a gateway between CICS common clients running under Windows or UNIX on TCP/IP networks and CICS online transaction monitoring systems on IBM Multiple Virtual Storage (MVS) hosts running SNA.

Note The IBM CICS Universal Client is also known as IBM CICS Common Client or the CICS Client. The terms are used interchangeably. In this document, CICS by itself refers to the CICS Server unless otherwise indicated.

CTRC supports the IBM CICS Universal Client using the Extended Call Interface (ECI) and the Extended Presentation Interface (EPI). The ECI lets non-CICS client applications invoke CICS transaction programs. The EPI lets distributed applications call CICS transactions that were originally accessed via 3270 terminals.

CTRC also supports clients that use the Microsoft Common Object Module Transaction Interface (COMTI), IBM TXSeries running as clients, and other standard ISC-TCP based requestors.

CTRC supports route configuration for a CICS transaction. Each transaction can be routed to a specific CICS region.

CTRC Network Topologies

Figures 1 through 3 show a few of the network topologies in which the CTRC router can be deployed. The Sample Router Configurations appendix provides a sample router and host configurations.

Figure 1-1 Cisco Router Configured with the CTRC Feature for CICS Communications

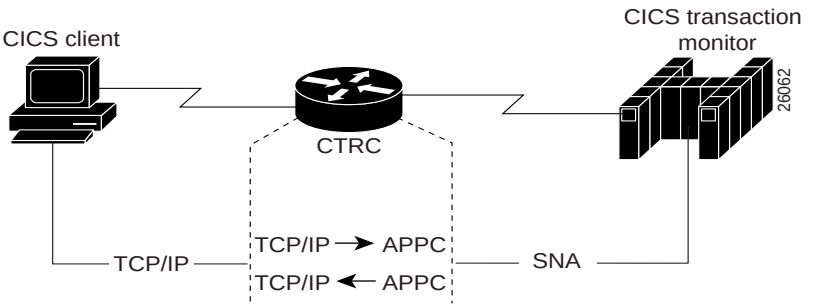


Figure 1-2 Cisco Router Configured with the CTRC Feature for DB2 Communications (SNA Host Network)

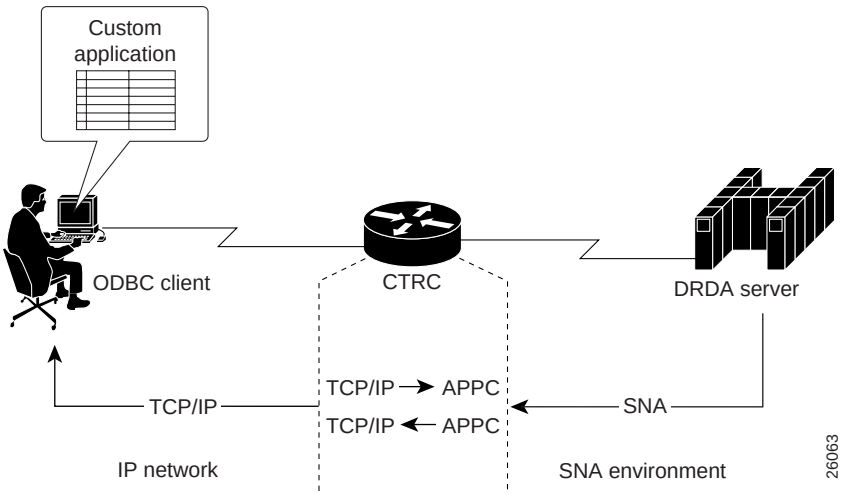
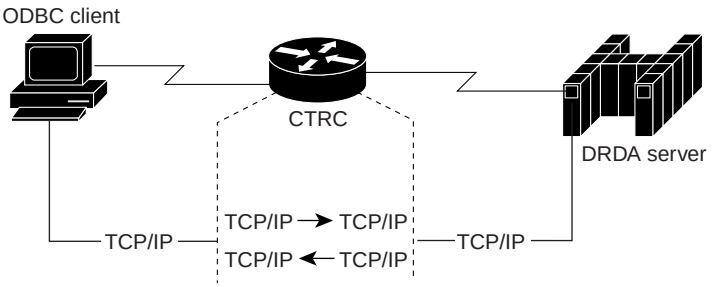


Figure 1-3 Cisco Router Configured with the CTRC Feature for DB2 (TCP/IP Pass Through)



Note Licensing of the CTRC router is based on the cpname assigned to the router in the SNA Switching Services configuration. You must install and start SNA Switching Services with at least a minimal configuration to support the TCP/IP connections. Refer to the "Configuring Cisco Transaction Connection" section of the *Cisco IOS Bridging and IBM Networking Configuration Guide* for more information about configuring the CTRC license and the switching services that CTRC requires.

Supported Servers and Clients

The following sections describe the hosts and clients that CTRC currently supports for access to CICS and DB2.

Supported DB2 Versions

CTRC accepts database requests from end user workstations and servers running an ODBC driver using the DRDA protocol to communicate with IBM databases.

CTRC supports the following DB2 versions:

- DB2 for OS/390 (DB2/MVS) 2.3 and later
- DB2/400 2.2 and later

- DB2/UDB 2.2 and later
- DB2 for VM/VSE (SQL/DS) 3.3 and later

Supported CICS Servers

CTRC supports the following CICS servers:

Note Versions marked with an asterisk (*) have limited server support. These versions support ECI but they do not support EPI or the Terminal Emulation function.

- CICS Transaction Server for OS/390
- CICS/400 Version 3.1
- CICS on Open Systems and NT (TXSeries)
- CICS/ESA Version 3.3*
- CICS/ESA Version 4.1
- CICS/MVS Version 2.12.*
- CICS/VSE Version 2.3
- CICS/VSE Version 2.2*
- CICS for OS/2 Version 2.01 or later

Supported CICS Servers as Clients

CTRC supports the following CICS Servers connected as clients:

- TXSeries for AIX version 4.2 or later
- TXSeries for NT version 4.2 or later

Supported DB2 Clients

CTRC supports connectivity to DB2 from clients that use the following standard interfaces:

- Open Database Connectivity (ODBC)
- Java Database Connectivity (JDBC)
- Object Linking and Embedding (OLE)
- Remote Data Objects (RDO)
- Call Level Interface (CLI)

Supported CICS Clients

CTRC supports connectivity to CICS from the following clients:

- IBM Universal Client, version 2.0 or later, using EPI or the ECI
- IBM TXSeries running as clients
- Microsoft COMTI

Migration Issues

The following are known issues when migrating from CDBC (CTRC Version 1.0) to CTRC Version 2.0:

- Replacement of Cisco Advanced Peer-to-Peer Networking (APPN) feature by SNA Switching services (SNASw) requires reconfiguration of SNA resources in the Cisco IOS Software.
- CTRC allows up to two connections without a license key.
- CTRC support is not available in the Cisco 4500 or 4700 series routers.

Included in this Manual

The remaining chapters and appendix in this document describe the following steps required to configure CTRC:

- Preparing the Host for DB2
- Preparing the Host for CICS
- Setting up DB2 and CICS Clients
- Sample Router Configurations for DB2 and CICS

Refer to the "Cisco Transaction Connection" sections of the *Cisco IOS Bridging and IBM Networking Configuration Guide* and the *Cisco IOS Bridging and IBM Networking Command Reference* for more information about configuring CTRC and using the CTRC commands.

For More Information

The following documents, published by IBM, provide additional information that you may find helpful when setting up CTRC. The document titles and part numbers, which are provided in parentheses, were current when these lists were prepared but are subject to change by IBM.

IBM CICS Documentation

- *CICS Family: Communicating from CICS on System/390* (SC33-1697-01)
- *CICS Server Support for CICS Clients* (SC33-1779-00)
- *CICS Transaction Server for OS/390 V1R2 CICS Intercommunication Guide* (SC33-1695)
- *CICS/MVS Intercommunication Guide* (SC33-0519)
- *Communicating from CICS for MVS/ESA and CICS for VSE/ESA* (SC33-0825)

- *TXSeries: CICS Administration Guide* (SC33-1174)
- *TXSeries: CICS Administration Reference* (SC33-1563)
- *TXSeries: CICS Intercommunication Guide* (SC09-3900)
- *Revealed! CICS Transaction Gateway with More CICS Clients Unmasked* (SG24-5277)

IBM DB2 Documentation

- *DB2 UDB for OS/390 Version 6 Installation Guide* (GC26-9008)
- *DB2 for OS/390 Version 5 Installation Guide* (GC26-8970)
- *DB2 for MVS/ESA Version 4 Installation Guide* (GC26-3456)
- *DRDA Connectivity Guide* (SC26-4783)
- *WOW! DRDA Supports TCP/IP: DB2 Server for OS/390 and DB2 Universal Database* (SG24-2212)
- *OS/390 Workload Manager Implementation and Exploitation* (SG24-5326)
- *Distributed Relational Database Cross Platform Connectivity and Application* (SG24-4311)
- *OS/390 MVS Planning: Workload Management* (GC28-1761)

CHAPTER 2

Preparing the Host for DB2

This chapter highlights the tasks involved in preparing DB2 and an MVS host to accept connections through the CTRC router. If you are using direct TCP/IP to connect to the MVS host, you can skip this chapter, although you do need to configure the CTRC license and the SNA Switching Services to support the TCP/IP connections (see the "Cisco Transaction Connection" section of the *Cisco IOS Bridging and IBM Networking Configuration Guide*).

Preparing DB2 on an MVS Host

Preparing DB2 on an MVS host for access through CTRC primarily involves configuring the Distributed Data Facility (DDF). DDF is the component of DB2/MVS that processes Distributed Relational Database Architecture (DRDA) requests. DDF must be active for a desktop to connect to DB2 using StarSQL or any other DRDA requestor client. If your organization has not implemented distributed database capabilities, DDF might not be configured and active.

This section highlights the tasks that are especially important for supporting a connection through CTRC:

- Virtual Telecommunications Access Method (VTAM)
  - Log Mode Table Entry
  - Major Node Definitions
- APPL Statement
- DDF Record in the Bootstrap Data Set (BSDS)

- Starting DDF
- DB2 Communications Database
- Password Expiration Management

Virtual Telecommunications Access Method

VTAM handles network communications for MVS for direct VTAM and SNA gateway configurations. The VTAM system programmer creates a mode table entry and major node definitions in VTAM for the CTRC connection. The following sections provide information about the mode table entry and major node definitions required for CTRC. Consult the VTAM documentation for detailed information about configuring VTAM, which also may be referred to as eNetwork Communications Server for OS/390.

Logmode Table Entry

The logmode table entry contains information that governs how conversations take place in VTAM. It defines pacing, RU sizes and class of service (COS) parameters. The mode entry can be placed in any mode table under VTAM—the default mode table or the one used in the APPL statement (see the "APPL Statement" section on page 2-4) for the LU definitions for DB2.

Following example shows a mode table entry for APPC, with a LOGMODE name of IBMRDB. Make a note of the LOGMODE name, because you need to use the same name for the DLOGMODE value in the major node definitions and also in the SNA configuration. The PSERVIC field identifies the LU traffic protocol—the value shown in the following example is for an independent LU using LU 6.2.

```
IBMRDB   MODEENT  LOGMODE=IBMRDB,
                  FMPROF=X'13',
                  TSPROF=X'01',
                  PRIPROT=X'B0',
                  SECPROT=X'B0',
                  COMPROT=X'50A1',
                  RUSIZES=X'8989',
                  TYPE=0,
                  PSNDPAC=X'03',
                  SRVCPAC=X'03',
                  SSNDPAC=X'02',
                  PSERVIC=X'060200000000000000002F00'
```

Major Node Definitions

The VTAM system programmer creates an XCA major node definition for the connection to the CTRC router. Additionally, a switched major node definition and a Cross Domain Resource definition can be created to represent the LU for the CTRC router.

In the switched major node definition, the DLOGMOD value must match the LOGMODE value in the mode table entry. The name of IBMRDB is specified for both the LOGMODE value in the previous example and in the following switched major node definition example.

```
S02CTRC    VBUILD     TYPE=SWNET
* CTRC  DOWNSTREAM  PU
CTRCPU    PU       ADDR=01,
       CPNAME=           CTRCBOX,
       ANS=CONT,
       DISCNT=NO,
       IRETRY=NO,
       ISTATUS=ACTIVE,
       PUTYPE=2,
       SECNET=NO,
       MAXDATA=521,
       MAXOUT=2,
       MAXPATH=1,
       USSTAB=USSS,
       MODETAB=ISTINCLM,
       DLOGMOD=           IBMRDB,
       CONNTYPE=           APPN
*
CTRCCIP  PATH  GRPNM=G02E20A,CALL=IN
*
CTRCBOX  LU       LOCADDR=00,      INDEPENDENT LU
                  DLOGMOD=IBMRDB,
```

Make a note of the values for the LU and PU names, and the CPNAME, DLOGMOD, and CONNTYPE parameters because you must specify the same values in the SNA configuration. See the “Switched Major Node for Router” section on page A-4 for additional configuration examples.

APPL Statement

The APPL statement defines the DB2 subsystem to VTAM to support remote access. If your DB2 system is not already supporting remote access, you must create an appropriate APPL statement.

The following example shows an APPL statement. Make a note of the APPL statement label, which is DSNV510 in the following example, and the password, if one is specified. You need to specify the same values when you configure or update the DDF record in the Bootstrap Data Set (BSDS).

```
DB2APPL    VBUILD    TYPE=APPL
DSNV510    APPL      AUTH=(ACQ),
                     APPC=YES,
                     AUTOSES=1,
                     DMINWNL=10,
                     DMINWNR=10,
                     DSESLIM=20,
                     MODETAB=ISTINCLM,
                     SECACPT=ALREADYV,
                     SRBEXIT=YES,
                     VERIFY=NONE,
                     VPACING=2
```

DDF Record in BSDS

To obtain system installation parameters during startup, DB2 reads the BSDS. The DDF record in the BSDS contains information used by DDF to connect to VTAM.

If you are installing DB2, use the DDF installation panel DSNTIPR to provide the following parameters. If DB2 is already installed, use the change log inventory utility (DSNJU003) to update this information in BSDS.

- DDF location name
- DDF LUNAME
- Password used when connecting DB2 to VTAM, if a password is required
- IP port used for TCP/IP access

Record the DDF location name. You will use it for the Database Server Name during data source configuration on the desktop. You also can determine the DDF location name from the syslog. Look for a DB2 message DSNL004I (starting DDF) that contains the location name. Also record the DDF LUNAME, which you will need for SNA configuration.

The following example updates the BSDS with a location name of DB2510, LU name of DSNV510 for SNA access, a password of STARPASS, and a port of 446 for TCP/IP communications. The RESPORT and PORT parameters are required for TCP/IP access. If you are using SNA only, then you can omit them.

```
//*
//DSNTLOG  EXEC  PGM=DSNJU003,COND=(4,LT)
//STEPLIB   DD   DISP=SHR,DSN=DSN510.SDSNLOAD
//SYSUT1    DD   DISP=OLD,DSN=DSN5CAT.BSDS01
//SYSUT2    DD   DISP=OLD,DSN=DSN5CAT.BSDS02
//SYSPRINT  DD   SYSOUT=*
//SYSUDUMP  DD   SYSOUT=*
//SYSIN     DD   *
            DDF  LOCATION=DB2510,LUNAME=DSNV510,
                 PASSWORD=STARPASS,RESPORT=5020,PORT=446
//*
```

LOCATION is used as the RDB name. If your system does not require a password to connect DB2 to VTAM, replace the PASSWORD parameter with NOPASSWD. For complete information about configuring DDF, consult IBM's DB2/MVS installation documentation.

Starting DDF

Use the following command to start DDF:

```
-START DDF
```

This command requires authority of SYSOPR or higher.

When DDF starts successfully, the following messages are displayed:

```
DSNL003I - DDF IS STARTING
DSNL004I - DDF START COMPLETE LOCATION locname LU netname.luname
```

If DDF has not been properly installed, the START DDF command fails and displays the following message:

```
DSN9032I - REQUESTED FUNCTION IS NOT AVAILABLE
```

If DDF has already been started, the START DDF command fails and displays the following message:

```
DSNL001I - DDF IS ALREADY STARTED
```

DB2 Communications Database

The DB2 host maintains a database table that defines the network attributes of remote systems. To enable communication between a CTRC client and the DB2 host, there must be an entry in this table. On DB2 for OS/390 or later, the name of this table is SYSIBM.LUNAMES. For DB2 on MVS version 4.1, the name of this table is SYSIBM.SYSLUNAMES. Table 2-1 describes the table entry parameters and indicates which are applicable to one or both versions of the table.

Table 2-1 DB2 Communications Database Table Entry

Parameter	SYSLUNAMES	LUNAMES	Description
LUNAME	•	•	LUNAME of the remote system. An empty string means that any LU is valid for this row.
SYSMODENAME	•	•	VTAM logon mode name used for DB2 for MVS/ESA intersystem conversations. A blank frame indicates that IBMDB2LM should be used. Use the mode name specified in the modetab.
ENCRYPTPSWDS	•	•	Indicates whether passwords exchanged with this partner are encrypted. Use the default value of NO for passing passwords between a client and DB2 host using CTRC.
MODESELECT	•	•	If ‘Y’, the SYSMODESELECT table is used to obtain the mode name for each outbound distributed database request. If not ‘Y’, the mode name IBMDB2LM is used for system-directed access requests, and the mode name IBMRDB is used for DRDA requests.

Table 2-1 DB2 Communications Database Table Entry (continued)

Parameter	SYSLUNAMES	LUNAMES	Description
USERNAMES	•	•	Indicates the level of come-from checking and user ID translation required. It also specifies the security parameters this DB2 for MVS/ESA subsystem uses when requesting data from the remote partner (outbound security requirements). 'I' indicates an "inbound" ID is subject to translation. 'O' indicates an "outbound" ID, sent to the corresponding LUNAME and subject to translation. 'B' indicates that both inbound and outbound IDs are subject to translation. A blank indicates no translation for inbound or outbound IDs.
USERSECURITY	•		Network security acceptance options required of the remote system when the DB2 for MVS/ESA system acts as a server for the remote system (inbound security requirements).
SECURITY_IN		•	Defines the security options that are accepted by this host when an SNA client connects. "V" for "verify" indicates that the incoming connection request must include a password. "A" for "already verified" indicates the request does not require a password, although the password is checked if it is sent.
SECURITY_OUT		•	Defines the security option that is used when local DB2 SQL applications connect to any remote server associated with this LUNAME. "A" for "already verified" indicates that outbound connection requests contain an authorization id and no password. "P" for "password" indicates that outbound connection requests contain an authorization id and password. 'R' for "RACF PassTicket" indicates that outbound connection requests contain a userid and RACF PassTicket.

The following command inserts a row into the SYSIBM.SYSLUNAMES table that any LU can use because the value of the LUNAME column is an empty string:

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

The following command inserts a row into the SYSIBM.LUNAMES table that any LU can use:

```
INSERT INTO SYSIBM.LUNAMES (LUNAME, SECURITY_IN, ENCRYPTPSWDS,
USERNAMES) VALUES (' ', 'V', 'N', ' ');
```

Password Expiration Management

Users of DRDA applications (such as StarSQL) can change their host password using CTRC's Password Expiration Management (PEM) feature. This feature is supported by CTRC using IP pass through and APPC. CTRC's PEM support for IP pass through is provided for DB2 for OS390 V5 or later. PEM support when using Advance Program-to-Program Communications (APPC) is provided by either APPC/MVS or CICS.

PEM Support for IP Passthrough

There is no CTRC configuration required for PEM support as it is native in DRDA over TCP. However the DB2 host must be enabled to support the PEM. To enable PEM support on DB2 for OS390 V5 or later, you must configure and use extended security using either:

- DSNTIPR (DDF) panel on the DB2 installation dialog
- Customized configuration job DSNTIJUZ, with the option EXTSEC=YES specified

Refer to the *DB2 Installation Guide* for details on setting up and using extended security.

Note If you are using DB2 for OS390 V5, install the maintenance fix PTF UQ21052. The IBM APAR PQ15977 describes the problems fixed by this PTF. This maintenance fix is not required for later releases.

PEM Support for APPC

The CTRC PEM support over APPC is is implemented using SNA TPs. Therefore, CTRC requires that a surrogate subsystem, such as APPC/MVS or CICS be used to change passwords. Both APPC/MVS and CICS support the SNA TPs.

To allow PEM support for DB2 connections, use the **dbconn pem** configuration command to turn on PEM support as appropriate for the CTRC routers handling the connections. In the **dbconn pem** command configuration statement, specify the LU name of the APPC/MVS base configuration. APPC/MVS configuration statements are in SYS1.PARMLIB(APPCPMxx). Consult your MVS systems programmer to obtain the name of the target LU that will be used by CTRC. The PEM support does not require any explicit definitions of the SNA TPs. Following is an example LUADD statement, such as found in SYS1.PARMLIB:

```
LUADD ACBNAME(MVSLU01) BASE TPDATA(SYS1.APPCTP)
```

The following is an example VTAM APPL definition for the APPC/MVS LU:

```
MVSLU01     APPL       ACBNAME=MVSLU01,     ACBNAME FOR APPC
                       APPC=YES,
                       AUTOSES=0,
                       DDRAINL=NALLOW,
                       DLOGMOD=APPCSNA,
                       DMINWNL=5,
                       DMINWNR=5,
                       DRESPL=NALLOW,
                       DSESLIM=10,
                       LMDENT=19,
                       PARSESS=YES,
                       SECACPT=CONV,
                       SRBEXIT=YES,
                       VPACING=1
```

CICS support for SNA TPs is provided in resource group DFHISC. You must install this group and configure CICS for CTRC support as described in Chapter 3, “Preparing CICS Connections.” When you configure the CTRC router to support PEM for CICS connections, use the CICS APPLID as the rlu value in the **dbconn pem** command configuration statement.

CHAPTER 3

Preparing CICS Connections

Overview of Preparing the Host for CICS

Preparing the host for CICS has two major steps:

- Defining CICS for Intersystem Communications
- Defining the CTRC Router to VTAM

CTRC connects to CICS using the SNA LU6.2 (APPC) communication protocol. The SNA functions are provided by a separate SNA product on the host, and CICS uses the services of that product. On a mainframe host, the SNA product is VTAM (also known as eNetwork Communications Server). You must configure both the CICS product and the associated SNA product.

If you have previously configured a DBCONN connection using SNA and your TXCONN connections are going to the same host, the router link is already defined to VTAM and you can skip this chapter.

Defining CICS for Intersystem Communications

To define CICS for the ISC, complete the following steps:

Note If you have already configured another product, such as TXSeries for AIX, to connect to CICS, you may have performed many of these steps.

Step 1 Configure the VTAM APPL definition for parallel sessions.

Step 2 Configure CICS for ISC.

Step 3 Install the supplied resource definition group, DFHCLNT.

Step 4 Define the CSCC transient data queue.

Step 5 Install APPC connections to the clients.

Step 6 Install client virtual terminals.

Step 7 Specify the level of security to be used for client-CICS Transaction Server for OS/390 links.

Step 8 Specify the code pages to be used for data conversion.

Defining the CTRC Router to VTAM

If you are currently using CICS, the CICS Transaction Server and VTAM have already defined their network name and LU names. The CTRC router must be defined to CICS and VTAM so that the host recognizes and accepts session initiation requests from it. For each CTRC router, the system programmer must create a new CONNECTION definition in CICS, and new PU, LU, and MODEENT definition statements in VTAM.

VTAM handles network communications for MVS for direct VTAM and SNA gateway configurations. The VTAM must contain a mode table entry and major node definitions for the CTRC router link. Consult your VTAM documentation for detailed instructions on configuring VTAM. You might want to take advantage of VTAM's support for dynamic definition of independent LU's, which also is described in the VTAM documentation.

Logmode Table Entry

The logmode table entry contains information that governs how conversations take place in VTAM. It defines pacing, RU sizes and Class of Service (COS) parameters. The mode entry can be placed in any mode table under VTAM—the default mode table or the mode table used in the APPL statement for CICS's LU definition (see the APPL Statement section on page 3-4). If you are using CTRC for CICS and DB2 access and you have already defined a mode for DB2, you can use the same mode for both subsystems.

The name you specify for LOGMODE, which is IBMRDB in the following example mode table entry, must be the same as the DLOGMOD name in the major node definitions and in the SNA configuration. The PSERVIC field identifies the LU traffic protocol—the value shown in the following example is for an independent LU using LU 6.2.

```
IBMRDB  MODEENT  LOGMODE=IBMRDB,
                 FMPROF=X'13',
                 TSPROF=X'07',
                 PRIPROT=X'B0',
                 SECPROT=X'B0',
                 COMPROT=X'50A1',
                 RUSIZES=X'8989',
                 TYPE=0,
                 PSNDPAC=X'03',
                 SRVCPAC=X'03',
                 SSNDPAC=X'02',
                 PSERVIC=X'060200000000000000002F00'
```

Major Node Definitions

The VTAM must contain major node definitions for the connection to the CICS host from the router. You can use a switched, non-switched, or channel-attached major node. Switched major nodes are most commonly used with CTRC. In the major node definitions, the DLOGMOD value must match the LOGMODE value in the mode table entry.

Make a note of the PU and LU names, and the CPNAME, DLOGMOD and CONNTYPE parameter values because you need to specify the same values in the SNA configuration and in the CICS APPC CONNECTION and SESSION definitions.

The following example shows a switched major node definition with an independent LU:

```
S02CTRC    VBUILD     TYPE=SWNET
* CTRC  DOWNSTREAM  PU
CTRCPU   PU       ADDR=01,
       CPNAME=           CTRCBOX,
       ANS=CONT,
       DISCNT=NO,
       IRETRY=NO,
       ISTATUS=ACTIVE,
       PUTYPE=2,
       SECNET=NO,
       MAXDATA=521,
       MAXOUT=2,
       MAXPATH=1,
       USSTAB=USSS,
       MODETAB=ISTINCLM,
       DLOGMOD=          IBMRDB,
       CONNTYPE=          APPN
*
CTRCCIP  PATH  GRPNM=G02E20A,CALL=IN
*
CTRCBOX  LU       LOCADDR=00,      INDEPENDENT LU
       DLOGMOD=          IBMRDB,
```

The “Sample Router Configurations” appendix contains additional configuration examples.

Define CICS for Intersystem Communication

APPL Statement

The APPL statement defines the CICS subsystem to VTAM to support remote access. If your CICS subsystem is not already supporting remote access, you must create an appropriate APPL statement.

The following example shows an APPL statement that defines CICS to VTAM:

```
A02CICS  VBUILD   TYPE=APPL
CICSB    APPL     AUTH=(ACQ,SPO,PASS,VPACE),
                  MODETAB=ISTINCLM,
                  DLOGMOD=IBMRDB,
                  HAVAIL=YES,
                  VPACING=9,
                  EAS=10000,
                  PARSESS=YES,
                  APPC=NO,
                  SONSCIP=YES
```

Make a note of the APPL statement label, which is CICSB in the example, and the password if one is specified, because you need to specify the same values in the SNA configuration.

System Initialization Parameters

Set ISC=YES in the CICS system initialization table (SIT). The following example shows override to the CICS system initialization parameters:

```
APPLID=(CICSB),
GMTEXT='CICS TS V1.2',
AUXTR=OFF,
EDSALIM=80M,
FCT=NO,
ISC=YES,
MXT=100,
  .
  .
  .
```

DFHCLNT Resource Group

You must install the CICS-supplied resource definition group, DFHCLNT. This group includes definitions of the CICS internal transactions, CCIN and CTIN, and the programs they use.

CSCC Transient Data Queue

Messages relating to Client support are written to the CSCC transient data queue. You must define CSCC to CICS. There is a sample definition in the supplied resource definition group, DFHDCTG. The sample defines CSCC as an indirect extra partition destination, pointing to CSSL.

Installing the APPC Connections to CTRC

You must install APPC connections to CTRC. The connections can be single- or parallel-session links. Install APPC connections to CICS either by creating static definitions for the router or using an autoinstall. Each method is described in the following sections.

Creating Static Definitions for Router Connections

You can use CEDA DEFINE and INSTALL commands to create static definitions. For more information about defining APPC connections, see the *CICS Intercommunication Guide*.

The following example shows a CONNECTION definition named CTRC. Note that the NETNAME value must be the same as the CTRC router's LU name, which is CTRCBOX in this example. Setting the AUTOCONNECT option to YES allows CICS to dynamically activate the router connection.

```
DEFINE
       CONNECTION(CTRC)
       DESCRIPTION(CTRC)
       AUTOCONNECT(YES)
       NETNAME(CTRCBOX)
       ACCESSMETHOD(VTAM)
       PROTOCOL(APPC)
       SINGLESESS(NO)
       ATTACHSEC(IDENTIFY)
       BINDPASSWORD(NO)
       BINDSECURITY(NO)
       USEDFLTUSER(YES)
```

The following example shows a SESSIONS definition. Note that the value for the CONNECTION parameter must be the same as the name of the CONNECTION definition, which is CTRC for this example.

```
DEFINE
       SESSIONS(CTRC)
       CONNECTION(CTRC)
       MODENAME(IBMRDB)
       PROTOCOL(APPC)
       MAXIMUM(64,1)
       SENDSIZE(4096)
       RECEIVESIZE(4096)
```

Using Autoinstall for Router Connections

Another method of installing router connections is to use autoinstall. If you use autoinstall you must create suitable CONNECTION and SESSIONS template definitions.

For information about autoinstall and defining templates, see the *CICS Resource Definition Guide*. For information about customizing your autoinstall user program to handle APPC connections, see the *CICS Customization Guide*.

Installing Client Virtual Terminals

Virtual terminals are used by the External Presentation Interface (EPI) and terminal emulator functions of the CICS Clients products. Both IBM-supplied autoinstall programs support virtual terminal autoinstall. Refer to the *CICS Customization Guide* for detailed information on autoinstall for virtual terminals.

Security

CICS supports the Bind, Link, and User security models.

Bind Security

Bind-time security currently cannot be configured on Cisco routers. Therefore, specify BINDSECURITY(NO) on the CONNECTION definitions that define the router to CICS.

Link Security

Link security provides the lowest level of resource security for intercommunication links. It defines the total set of resources that can be accessed across the connection.

To set link security for a CICS Client connection, specify a userid for the SECURITYNAME link option of the CONNECTION definition. Next, define a profile to your External Security Manager for the link userid. Connection users can to access only those resources that the link userid is authorized to access.

If you do not specify a userid for the SECURITYNAME option, the authority of the link is that of the CICS default user.

User Security

User (attach-time) security defines how individual users of an intercommunication link are checked. It also affects the resources that individual users are able to access. Unless you specify LOCAL user security (in which case all potential users share the authority of the link userid), you must define user profiles to your External Security Manager.

Data Conversion

When a CICS client sends a request, the server controller calls a routine that supports code page translations and data conversions. Regardless of whether translations and conversions are required, you need to create or modify a DFHCNV table to allow the server controller to handle incoming requests. The use of the DFHCNV macro for defining the table is described in the *CICS Family, Communicating from CICS on System/390* document.

The following example shows the DFHCNV table entries:

```
PRINT   NOGEN
DFHCNV   TYPE=INITIAL,SRVERCP=037,CLINTCP=437
DFHCNV   TYPE=FINAL
END     DFHCNVBA
```

Note It is not necessary to code the pages used with CICS clients on the CLINTCP and SRVERCP operands of the DFHCNV TYPE=INITIAL macro.

CHAPTER 4

CTRC Client Setup

This chapter includes information for setting up clients for access to DB2 and CICS.

Setting Up DB2 DRDA Client Connections

To configure a connection between a DRDA-based Client and a DB2 database, you must define a data source to the ODBC driver. For each DB2 database that will be accessed, you need to specify the following data source information to configure the ODBC driver to use the CTRC router:

- Relational database (RDB) name of the DB2 database you want to access. This value must match the rdbname that you specify with the **dbconn server** command to configure the CTRC router for communicating with DB2. The RDB name also much match the DDF location defined on the DB2 host (see the “DDF Record in BSDS” section on page 2-4).
- Router’s hostname or the IP address of the interface that will accept the connection requests.
- Port number on which the CTRC router is listening for connection requests. The default is 446.

The procedures for configuring a data source are specific to the client implementation. Refer to the documentation for your DRDA client for details.

Setting up the CICS Client

CTRC supports the IBM CICS Universal Client, IBM TXSeries running as clients, and Microsoft COMTI clients. These clients connect to the Cisco router via TCP/IP.

Setting Up CICS Universal ClientConnections

To set up the CICS Universal Client, perform the following tasks:

Step 1 Install the Universal Client for your platform.

Step 2 Choose TCP/IP as your network connection.

Step 3 To have the Universal Client connect to your CTRC server, add an entry in the Server section of the CICSCLI.INI file to define the CTRC server. The following example entry defines a router named CTRCBOX; substitute the LU name of your router for CTRCBOX:

```
Server = CTRCBOX
Description = TCP/IP Server
Protocol = TCPIP
NetName = CTRCBOX
Port = 1435
```

Step 4 If necessary, stop and restart the Universal Client to have the changes take effect and connect to the CTRC server.

If you have multiple servers configured in CICSCLI.INI, some applications might display a list of servers from which to choose. If security is turned on in CICS, a user/password dialog box might appear after selecting a CICS Server.

If you have specified UseDfltUser=NO and AttachSec=Verify in your APPC Connection definition on CICS, a userid and password will be required to use the CICS Terminal. If you are using ECI, pass the userid and password using a command such as:

```
cicscli /c=ctrcbox /u=p390 /p=p390
```

The CICS Terminal status line displays the virtual terminal name. When you enter a command on the terminal (for example, CEOT), you will see the SYSID and APPLID of the CICS system to which you are connected.

To connect through multiple connections, increase the MaxServers value in the client section of the CICSCLI.INI file from the default of 1.

Setting Up TXSeries as a CTRC Client

To connect a machine running TXSeries to another CICS host through a CTRC connection, you must create the following CICS resource definitions:

- Listener Definition
- Communications Definition
- Program Definition for each remote program you want to use

You use the **cicsadd** command to add CICS resource definitions on TXSeries, specifying the values appropriate for your definition in place of the variables shown in italic in the following command syntax.

```
cicsadd -c className[-r regionName] [-P | -B] [-f fileName] [-m
modelId] resourceName [attributeName=attributeValue ...]
```

To use the CTRC router, the value for the *resourceName* in the Communications Definition (CD) must be the same as the *attributeValue* specified for the RemoteSysId attribute in the Program Definition. The ListenerName specified in the CD must match the name of the Listener Definition. For example, issuing the following command creates a Communications Definition for the CTRC router with a *resourceName* of CTRC and a ListenerName of TCP.

```
cicsadd -c cd -r TX6000 -B CTRC ResourceDescription=”Connection thru
CTRC” ConnectionType=cics_tcp ListenerName=TCP OutboundUserIds=sent
RemoteCodePageTR=”IBM-037” RemoteNetworkName=”CICSB”
RemoteSysSecurity=trusted RemoteTCPAddress=”ctrcbox”
RemoteTCPPort=1435 RemoteLUName=”CTRCBOX”
```

To use a remote program named PNG1, the Program Definition for PNG1 must set the RemoteSysId attribute to CTRC, as shown in the following command:

```
cicsadd -c pd -r TX6000 -B PNG1 ResourceDescription=”eciPing back end”
RemoteSysId=CTRC RemoteName=PNG1 RSLKey=public
```

You specify the protocol that the CICS client will use in the Listener Definition. For example, to allow the TXSeries client to connect to the CICS region specified in the previous example commands, TX6000, add a Listener Definition for TCP/IP as shown in the following command.

```
cicsadd -c ld -r TX6000 -B TCP ResourceDescription="TCP/IP Listener"
Protocol=TCP
```

Refer to the IBM TXSeries CICS documentation for more information about specifying CICS resource definitions on TXSeries:

Setting Up COMTI Client Connections

When a COMTI application is built using Microsoft's COMTI Component Builder, it must be defined with the following information to provide remote access to CICS:

- "CICS and IMS via TCP/IP" as the remote environment type
- "CICS" as the target environment
- "MS Link" as the server mode

For the COMTI client to access CICS using the CTRC router, you must define CTRC as a TCP Remote Environment. Use Miscrosoft's COMTI Manager to define the remote environment with the following values:

- Select "CICS and IMS using TCP/IP" as the remote environment type
- Specify the IP address and TCP port address as configured on the CTRC router
- Specify a name and comment for the new remote environment

Refer to the *Microsoft COM Transaction Integrator Online Guide* for details about setting up and using COMTI.

Appendix

Sample Router Configurations

Table A-1 summarizes the correspondence between key VTAM and DB2 parameters on DB2/MVS and the Cisco Transaction Connection router configuration parameters.

Table A-1 Correspondence Between VTAM and DB2 Parameters

Subsystem	MVS/OS390 Parameter	CTRC Router Parameter
VTAM-DB2 APPL	APPL statement label in VTAM-DB2 APPL	dbconn server rlu
VTAM-CICS-APPL	APPL statement label in VTAM-CICS APPL	txconn dest rlu
VTAM-MODE ENTRY	LOGMODE	dbconn server mode txconn dest mode
VTAM - PU/LU	CPNAME	snasw cpname
VTAM - XCA	CUADDR	Csna
	ADAPTNO	Adapter
DB2-DDF	LOCATION	dbconn server rdbname
	LU	dbconn server rlu
	PORT	dbconn server port

VTAM and DB2 Parameter Mappings

The following sections give more detail about how to locate some of these values in DB2/VTAM. For more information about preparing VTAM, see the “preparing the Host for DB2” chapter.

APPL Statement Label

The APPL statement label is the word immediately preceding the APPL parameter in the DB2 APPL statement. The CTRC configuration examples use DSNV510 for the APPL statement label (see the “APPL Statement” section on page 2-4).

LOGMODE

The LOGMODE is a parameter in the logmode table entry. See the LOGMODE parameter for information and examples of logmode table entries showing the LOGMODE = <LOGMODE> parameter.

CPNAME

The CPNAME is a parameter in the major node definition. See the CPNAME parameter.

LOCATION

The LOCATION is the database name. It is part of the DDF record. See the “DDF Record in BSDS” section on page 2-4 for an example of a DDF record showing the LOCATION name.

CUADDR and ADAPTNO

The VTAM XCA definition defines values for the physical and virtual configuration for a Channel Interface Processor (CIP) card on the router (see the “XCA for a CIP-Attached Router” section on page A-5).

Example VTAM Parameter Listings

DB2 APPL

```
DSNAPPL    VBUILD     TYPE=APPL
DSNV510    APPL       AUTH=(ACQ),
                       APPC=YES,
                       AUTOSES=1,
                       DMINWNL=2048,
                       DMINWNR=2048,
                       DSESLIM=4096,
                       EAS=65535,
                       MODETAB=ISTINCLM,
                       DLOGMOD=IBMRDB,
                       SECACPT=ALREADYV,
                       SRBEXIT=YES,
                       VERIFY=NONE,
                       VPACING=1,
                       SYNCLVL=SYNCPT,
                       ATNLOSS=ALL
```

CICS APPL

```
A02CICS    VBUILD     TYPE=APPL
CICSB      APPL       AUTH=(ACQ,SPO,PASS,VPACE),
                      MODETAB=ISTINCLM,
                      DLOGMOD=IBMRDB,
                      HAVAIL=YES,
                      VPACING=9,
                      EAS=10000,
                      PARSESS=YES,
                      APPC=NO,
                      SONSCIP=YES
```

MODE ENTRY

```
IBMRDB    MODEENT   LOGMODE=IBMRDB
         FMPROF=X'13',
         TSPROF=X'07',
         PRIPROT=X'B0',
         SECPROT=X'B0',
         COMPROT=X'50B1',
         RUSIZES=X'8989',
         PSNDPAC=X'03',
         SRVCPAC=X'03',
                  PSERVIC=X'060200000000000000002F00'
```

Switched Major Node for Router

```
S02CTRC     VBUILD     TYPE=SWNET
* CTRC  DOWNSTREAM  PU
CTRCPU    PU       ADDR=01,
       CPNAME=           CTRCBOX,
       ANS=CONT,
       DISCNT=NO,
       IRETRY=NO,
       ISTATUS=ACTIVE,
       PUTYPE=2,
       SECNET=NO,
       MAXDATA=521,
       MAXOUT=2,
       MAXPATH=1,
       USSTAB=USSS,
       MODETAB=ISTINCLM,
       DLOGMOD=          IBMRDB,
       CONNTYPE=APPN
*
CTRCCIP  PATH  GRPNM=G02E20A,CALL=IN
*
CTRCBOX   LU       LOCADDR=00,      INDEPENDENT LU
       DLOGMOD=          IBMRDB,
```

Sample VTAM Configuration for CICS

The VTAM XCA definition supplies the values for the physical and virtual configurations for a CIP card on the router.

XCA for a CIP-Attached Router

```
XCAE20    VBUILD  TYPE=XCA
XPE20R    PORT    CUADDR=E20,
                  ADAPNO=1,
                  SAPADDR=4,
                  MEDIUM=RING,
                  DELAY=0,
                  TIMER=60
G02E20A   GROUP ANSWER=ON,CALL=INOUT,DIAL=YES,ISTATUS=ACTIVE
*
K02T201S  LINE
P02T201S    PU
*
K02T202S  LINE
P02T202S    PU
*
```

XCA for Token Ring Attached Router

```
XCAE40    VBUILD  TYPE=XCA
XPE40R    PORT    CUADDR=E40,
                  ADAPNO=1,
                  SAPADDR=4,
                  MEDIUM=RING,
                  DELAY=0,
                  TIMER=30
G02E40A   GROUP DIAL=YES,CALL=INOUT,ANSWER=ON,ISTATUS=ACTIVE
*
K02T001S  LINE
P02T001S    PU
*
K02T002S  LINE
P02T002S    PU
*
```

Sample Router Configurations for CICS and DB2

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname CTRCBOX
!
ip domain-name starquest.com
cns event-service server
!
source-bridge ring-group 100
!
interface FastEthernet0/0
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
 media-type MII
 half-duplex
!
!
interface TokenRing4/1
 mac-address 4000.1111.0505
 no ip address
 no ip directed-broadcast
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 early-token-release
 ring-speed 16
 llc2 ack-max 2
!
interface Ethernet6/1
 mac-address 4200.0000.0505
 ip address 198.147.235.2
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Channel3/0
 ip address 192.168.1.1 255.255.255.0
 no ip directed-broadcast
```

```
 no keepalive
 channel-protocol S4
csna 0100 20
!
interface Channel3/2
 no ip address
 no ip directed-broadcast
 no keepalive
 lan TokenRing 1
  source-bridge 10 2 100
  adapter 1 4000.0123.9999
!
interface Virtual-TokenRing0
  mac-address 4000.2222.3333
  source-bridge 50 1 100
  source-bridge spanning
!
snasw cpname CTRCBOX
snasw port TOK1 TokenRing4/1
snasw port SRB Virtual-TokenRing0
snasw link BUDDCIP port SRB rmac 4000.0123.9999
snasw link BUDDY port TOK1 rmac 4000.0200.0448
snasw location DSNV510 owning-cp STARW.BUDDCP (see Note below)
!
dbconn license SM6FB088F100CL020BFFD45EA2FF24DB connections 500
expiration-date
000000
!
txconn destination CICSC rlu CICSC mode IBMRDB
txconn destination CICSB rlu CICSB mode IBMRDB
!
txconn server CICSB destination CICSB port 1435
!
dbconn server DB2BUDD port 446 rdbname DB2510 rlu STARW.DSNV510 mode
IBMRDB
dbconn tcpserver GAZTCP port 452 rdbname GAZELLE remote-ip-address
198.147.235.39 remote-port 446
dbconn pem DB2BUDD rlu MVSLU01 mode #INTER
```

Note The SNAsw location is used only for LEN connections. Do not use this statement if the host is running APPN.

To determine if you need the SNASw location statement and the owning CP name perform the following steps.

Step 1 Configure the SNASw CPNAME, PORT, and LINK statements.

Step 2 Start the SNASw link:

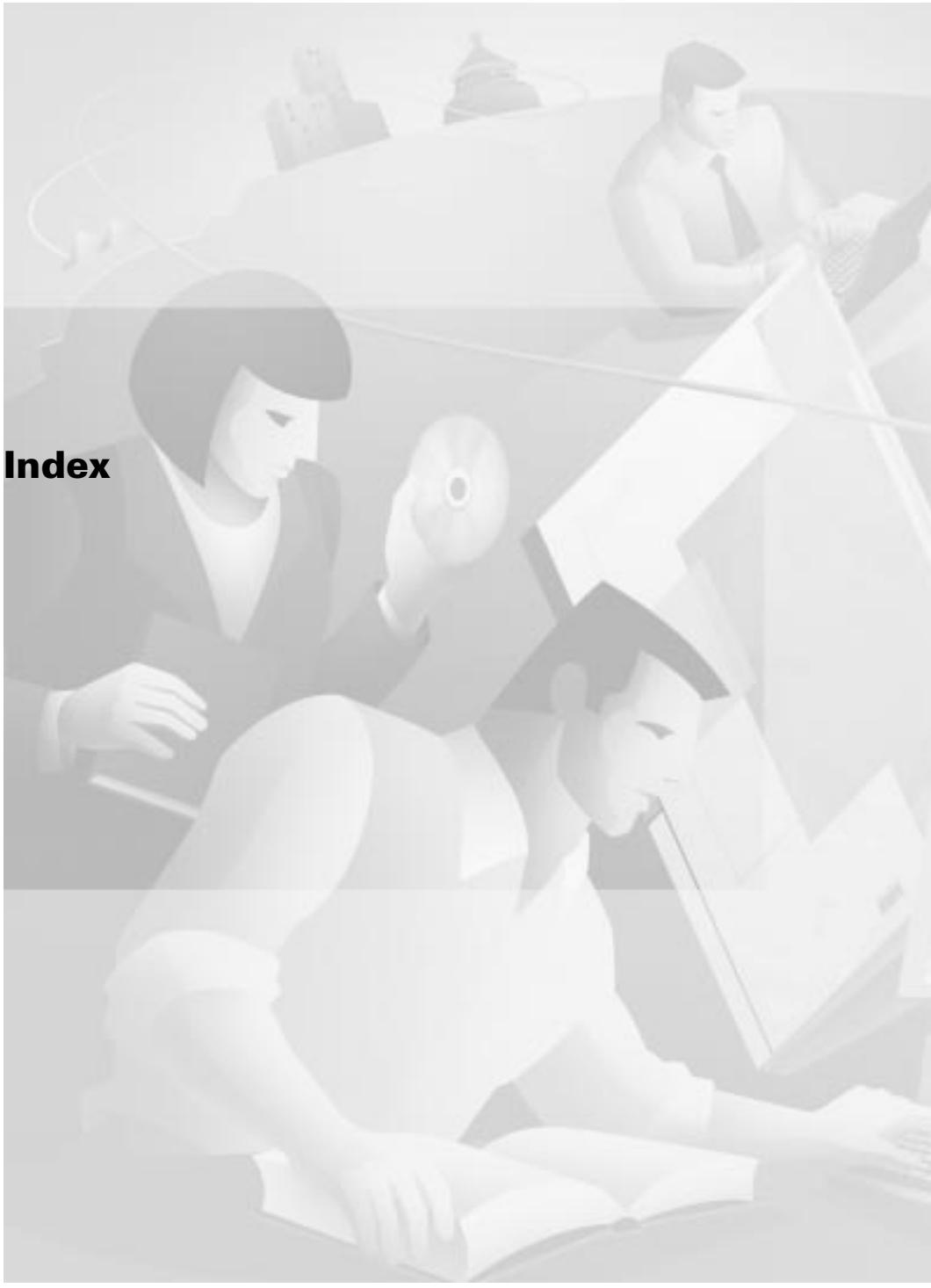
```
snasw start link BUDDY
```

Step 3 Examine the status of the link:

```
show snasw link
```

If the Node Type is LEN Node, the SNASw location statement is necessary. The owning CP Name appears under the Adjacent CP Name column.

Index



INDEX

A

B

C

D

H

I

L

M

P

R

S

T

U

V

W

X