Oracle® Tuxedo

Mainframe Adapter for TCP CICS User's Guide

Release 22c
F86391-03
October 2024

Oracle Tuxedo Mainframe Adapter for TCP CICS User’s Guide, Release 22c

F86391-03

Primary Author: Preeti Gandhe

Contributing Authors: Tulika Das

Contributors: Maggie Li

Contents

List of Figures

List of Tables

Preface

Oracle Tuxedo Mainframe Adapter for TCP (CICS) (hereafter referenced as TMA TCP for CICS) is a gateway connectivity feature that makes it possible for non-transactional tasks within Oracle Tuxedo regions to access services provided by CICS application programs and vice-versa. An Oracle Tuxedo region, or administrative domain, is a single computer or network of computers that shares a single Oracle Tuxedo configuration.

This document covers the following topics:

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1

Introducing Oracle Tuxedo Mainframe Adapter for TCP (CICS)

The TMA TCP for CICS software is designed to provide transparent CICS program access from within an Oracle Tuxedo domain and Oracle Tuxedo access from within a CICS region.

The following information introduces the TMA TCP for CICS product:

1.1 What You Need to Know

This document is primarily for CICS system administrators who configure and administer TMA TCP. In addition, programmers can find useful pointers for developing client programs and service routines that send data through to the remote TMA TCP gateway.

Programmers who work with TMA TCP should be familiar with CICS applications development.

System administrators who work with TMA TCP must be familiar with the following concepts, tools, and procedures:

- TCP/IP networking
- IBM CICS Sockets Interface
- Defining new resources to CICS
- Standard CICS monitoring tools

1.2 Oracle TMA TCP for CICS Architecture

Oracle TMA TCP for CICS is composed of four CICS programs running within a CICS region:

- Handler
- Application Handler
- Pre-requester
- Requester

It uses the Sockets Interface and Sockets for CICS Listener that is shipped with the IBM TCP/IP for CICS TS Sockets Interface. There are two different processing scenarios to consider:

- Requests that originate in a remote Oracle Tuxedo domain and request services offered by CICS

- Requests that originate in a CICS region and request services offered by a remote Oracle Tuxedo domain

1.3 Oracle TMA TCP Functionality

The following functionality is available in the TMA TCP product.

- Domains-based Gateway Connectivity
- Security
- Domain Name Server Support
- Dynamic Configuration
- Load Balancing of a Requester
- Automatic Enabling of LMID

1.3.1 Domains-based Gateway Connectivity

The TMA TCP product has a domains-based architecture supporting bidirectional communications, request/response support, and concurrent support for the CICS interface.

1.3.2 Security

The TMA TCP product grants access to Tuxedo services based on a user name supplied by CICS.

The TMA TCP for CICS product can start CICS transactions or link to programs. Oracle Tuxedo provides the user ID to the TMA TCP product to check for appropriate security prior to initiating the transactions.

1.3.3 Domain Name Server Support

The TMA TCP product supports domain name server (DNS) resolution of IP addresses. This support allows you to change the IP address at the Domain Name Server to implement address changes without reconfiguring the TMA TCP gateway.

1.3.4 Dynamic Configuration

The TMA TCP product supports dynamic configuration updates for some of the TMA TCP configuration parameters. You can modify the configuration without shutting down and restarting the TMA TCP product. For more information about dynamic configuration, refer to the Dynamically Configuring TMA TCP for CICS section.

1.3.5 Load Balancing of a Requester

The TMA TCP for CICS supports Requester load balancing. TMA TCP for CICS provides configuration for multiple services with the same name and the ability to associate them with different unique LMIDs. This configuration enables load balancing of the Requesters.

1.3.6 Automatic Enabling of LMID

The TMA TCP for CICS supports automatic enabling of a given Requester which is already disabled. The `AUTO ENABLE LMID` option is provided in the Requester configuration. When the

option is set to E (Enable), the Pre-Requester automatically enables the LMID and starts the Requester and processes the request.

1.4 Oracle TMA TCP for CICS Components

There are four programs used in processing remotely and locally initiated requests.

- Handler
- Application Handler
- Pre-requester
- Requester

Two administrative tools are also available:

- An online CICS administrative tool for configuring and maintaining the TMA TCP for CICS gateway
- An administrative tool (`BDWN`) for terminating the four programs listed above

- The TMA TCP for CICS Handler
- The TMA TCP for CICS Application Handler
- The TMA TCP for CICS Pre-requester
- The TMA TCP for CICS Requester
- IBM TCP/IP Sockets Interface
- IBM TCP/IP Sockets for CICS Supplied Listener
- IBM User Maintained Tables (UMT)

1.4.1 The TMA TCP for CICS Handler

A TMA TCP Handler is a CICS program that communicates with the TMA TCP gateway over TCP/IP. Specifically, the Handler communicates Oracle Tuxedo requests to a CICS region. A Handler is started automatically within a CICS region when Oracle Tuxedo issues the first service request destined for that CICS region.

The Handler is responsible for accepting a connection request, taking control of the socket connection, and continuing communication with the Requester in the Oracle Tuxedo domain for the life of the socket connection. The Handler interfaces as necessary with the Application Handler to process service requests originating from the TMA TCP gateway Requester. If multiplexing or security is enabled, the Handler starts the Application Handler and waits for the next service request. The Handler periodically checks for completed requests. When a request has been completed, the Handler retrieves the response data from the Application Handler and transmits that data back to the Requester. The Handler also periodically checks to ensure that no active service requests have timed out.

If the multiplex count is 1 and security is disabled, or if the service request originated from a version of TMA TCP gateway prior to Version 3.0, the Handler executes the target user application, waits for the application to return data, transmits that data back to the TMA TCP gateway, then waits for the TMA TCP gateway to send another service request.

1.4.2 The TMA TCP for CICS Application Handler

The Application Handler is started by and receives request information from the Handler. The Application Handler executes the target user application, waits for the application to return data, and returns the data to the Handler.

1.4.3 The TMA TCP for CICS Pre-requester

The Pre-Requestor program is used as an interface between your CICS client program and the TMA TCP for CICS Requester. The CICS Requester, which is described in the next section, is the program that talks with the remote Oracle Tuxedo domain. From your CICS client program you call the Pre-requester by issuing an `EXEC CICS LINK`.

1.4.4 The TMA TCP for CICS Requester

The Requester program is responsible for making and maintaining the sockets connection with the remote Oracle Tuxedo region. After receiving request information from the Pre-requester, the Requester sends that information to Oracle Tuxedo. The Requester then receives any response data returned by Oracle Tuxedo and sends it back to the Pre-requester, which in turn gives the information back to the client program that had called it.

1.4.5 IBM TCP/IP Sockets Interface

The sockets interface must be enabled before TMA TCP for CICS can communicate over TCP/IP. This procedure is true for any CICS program which uses the sockets API. The IBM TCP/IP Sockets Interface is not supplied by Oracle Systems, Inc. You can purchase it directly from IBM. The supplied transaction that accompanies the IBM TCP/IP Sockets for CICS product is used to enable the sockets interface under CICS. Complete documentation is provided with the IBM product.

- Using Other Supported TCP/IP Sockets Products

1.4.5.1 Using Other Supported TCP/IP Sockets Products

This document refers to the IBM TCP/IP sockets interface product. If you are using another supported TCP/IP product consult that product's documentation for equivalent components.

1.4.6 IBM TCP/IP Sockets for CICS Supplied Listener

The IBM TCP/IP Sockets for CICS Supplied Listener is responsible for capturing the initial connection request and passing that request along to the TMA TCP for CICS Handler. It is a piece of the IBM TCP/IP Sockets for CICS product which you must purchase directly from IBM. The listener should be installed and configured as outlined in the manual shipped with the product.

1.4.7 IBM User Maintained Tables (UMT)

The Connection file, `BEAVCON`, defaults to a user maintained table (UMT). If you choose to change this file to a `VSAM` file you must add the transaction `BDWN` to `PLTSI` for CICS. This transaction's primary function is to shut down all the active Requesters, but one of its secondary functions is to remove all the entries from the Connection file. The Connection file must be empty before initializing activity.

1.5 Processing Scenarios

This section describes the TMA TCP for CICS processing scenarios.

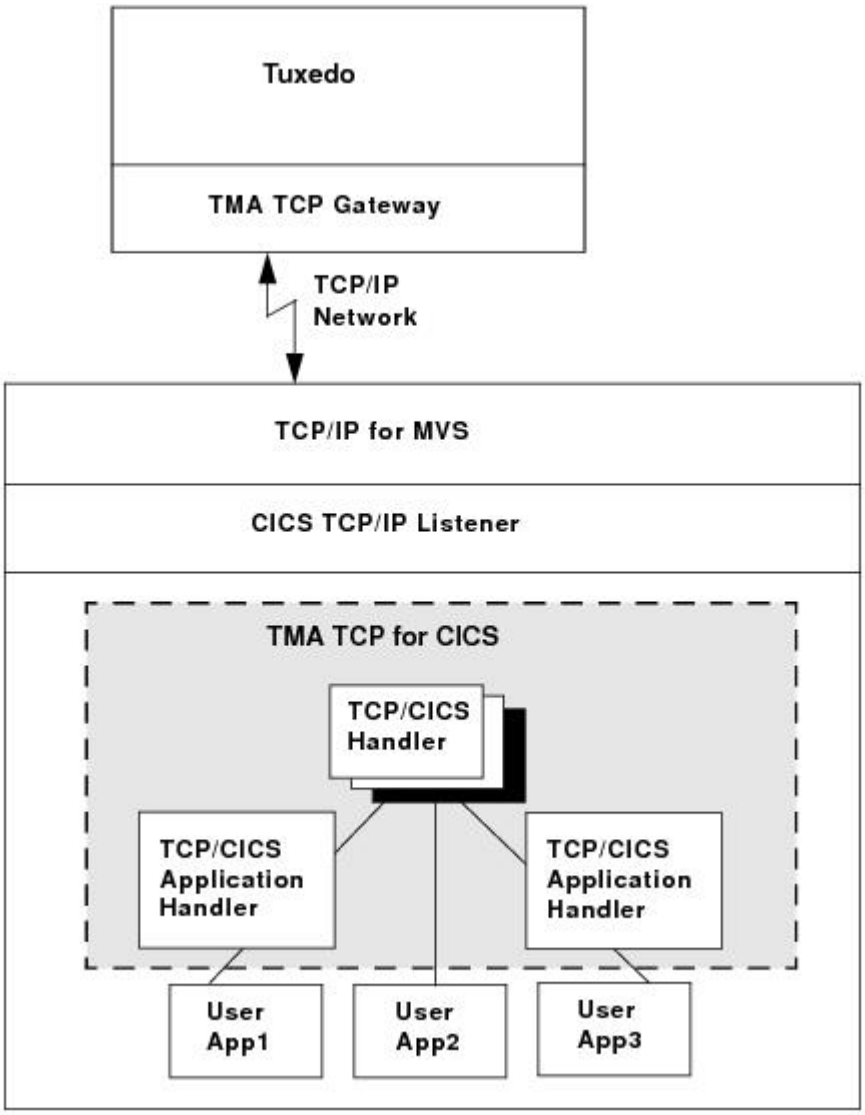
- Requests from within an Oracle Tuxedo Domain
- Requests from within CICS

1.5.1 Requests from within an Oracle Tuxedo Domain

Because of the way Oracle Tuxedo maps services to servers, service requests from remote Oracle Tuxedo regions to TMA TCP are transparent to the user, the Oracle Tuxedo developer, and the CICS programmer.

As the following figure illustrates, TMA TCP for CICS extends this transparent access by routing Oracle Tuxedo's requests for CICS program services through TCP/IP network software.

Figure 1-1 Oracle Tuxedo to TMA TCP for CICS Routing



As the following figure illustrates, TMA TCP for CICS fits between the CICS user application and TCP/IP.

When Oracle Tuxedo client programs send requests to remote systems (in this case, CICS) TMA TCP gateway transforms those requests into messages formatted appropriately for transmission to the remote system. Also, when remote systems respond, TMA TCP gateway transforms these responses into replies that local client programs can process.

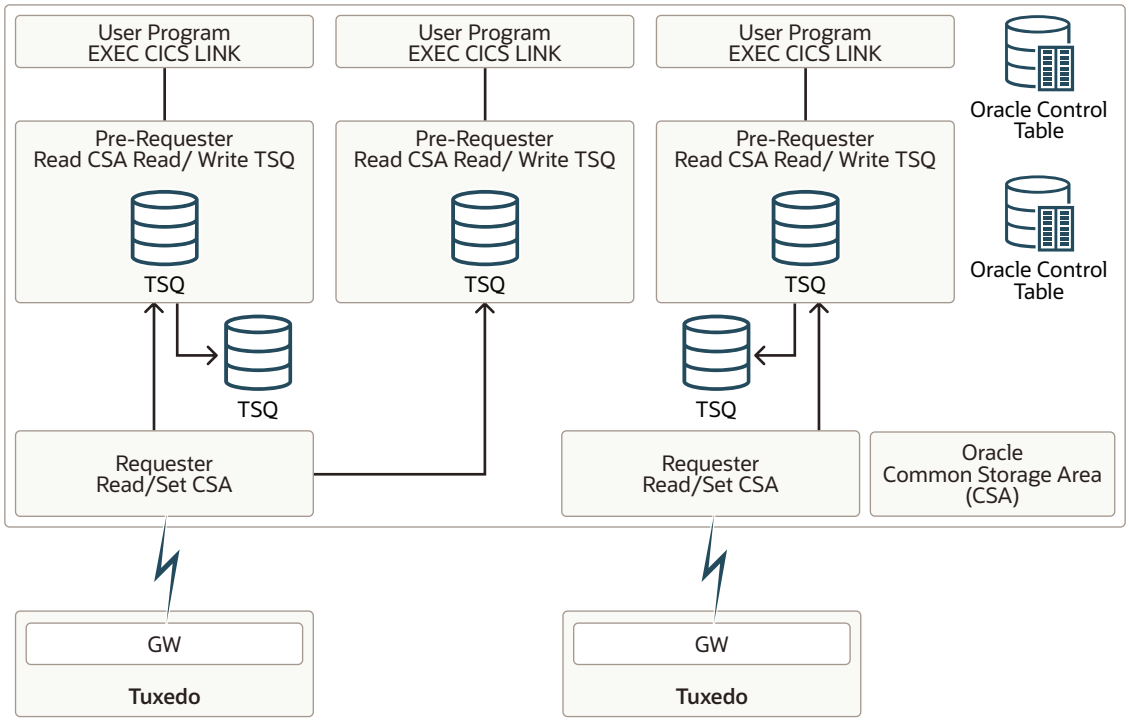
The TMA TCP for CICS software is implemented as an ordinary CICS program which communicates with the Sockets Interface. It accepts connection requests from the TMA TCP gateway and returns standard replies.

Simultaneous socket connections can exist between one TMA TCP for CICS gateway (a set of TMA Handlers within a single CICS region) and all remote TMA TCP gateway Requesters. Each socket connection is established automatically when a new TMA TCP gateway Requester in the Oracle Tuxedo domain establishes communication with the TMA TCP for CICS gateway.

1.5.2 Requests from within CICS

The mechanism used to send requests initiated from a CICS program to a remote Oracle Tuxedo domain is invisible to the user and significantly abstracted from the CICS programmer. Your company's CICS program issues an `EXEC CICS LINK` command to the Oracle TMA gateway. In the data passed with the `EXEC CICS LINK` command, the programmer supplies the name of the service and the data to be used as input to that service. When the `EXEC CICS LINK` command returns, the reply to the request is placed in that same data area. If there was a problem satisfying the service request, meaningful return codes are sent back.

Figure 1-2 Oracle TMA Client Gateway Configuration



As the following figure illustrates the configuration of the Oracle TMA client gateway. A client program (your CICS program) issues an `EXEC CICS LINK` command to the Pre-requester. The

Pre-requester verifies that the service name is valid and identifies the Requester to which it should it should pass the request. The Pre-requester starts a different Requester for each configured remote endpoint. The Requester then sends the request to the remote Oracle Tuxedo domain and waits for a response. Once the response is returned, the Requester notifies the Pre-requester and hands the response to the Pre-requester, which then returns the response to the client program.

1.6 Getting Started with TMA TCP for CICS

The following list describes all the tasks you must perform before you can begin using TMA TCP for CICS.

- Ensure that MVS TCP/IP is installed and configured.
- Ensure that the Sockets for CICS interface and supplied listener are installed and configured. The listener product comes with the Sockets for CICS interface.
- From the MVS TCP/IP administrator, find out at which port and address your supplied listener should listen. Give this information to the Oracle Tuxedo administrator so that the remote TMA TCP gateway component knows where to find the CICS TCP/IP listener.
- Find out on which ports TMA TCP gateway is listening. This information is necessary when you begin setting up services.
- Follow the installation instructions for TMA TCP given in the *Oracle TMA TCP Installation Guide*.
- Using the administration tool (described in Configuring and Administering Oracle TMA TCP for CICS) define the services and remote endpoints for use by TMA TCP. The best way to approach this is to talk to the Oracle Tuxedo administrator and choose one service only. Attempting to set up all the services at once would be a complex task, but after you learn how to set up one service, you should have no difficulty setting up the others.
- Add an `EXEC LINK` statement to one of your CICS programs and set up the data area as described in Understanding How Oracle TMA TCP for CICS Works.
- Consult your Oracle Tuxedo administrator about service names (what to call a service and what Oracle Tuxedo names it) and the layout of data each service expects to ensure there are no consistency problems.

2

Understanding How Oracle TMA TCP for CICS Works

To understand how the Oracle Tuxedo Mainframe Adapter for TCP (CICS) (hereafter referenced as TMA TCP for CICS) product works, you must know how the product performs the following functions.

Each of these operations is described in the following sections. Additionally, this document describes some programming considerations that may be useful when you develop or change programs that interoperate with TMA TCP for CICS.

- Starting the Listener Program
- Running Oracle TMA TCP for CICS
- Translating Data with TMA TCP gateway

2.1 Starting the Listener Program

The Listener program is supplied by IBM and is part of the Sockets for CICS software product which must be purchased from IBM.

> **Note:**
>
> Before you can use TMA TCP for CICS, you must install and configure both IBM TCP/IP and the Sockets for CICS product as outlined in the documentation that accompanies those products.

The Listener's job is to wait for connection requests at a particular network address and port of your choosing. When the Listener receives a connection request it invokes the appropriate CICS program automatically, based on the name supplied as part of the Listener's connection protocol buffer. For example, if the Listener receives a connection request from TMA TCP gateway running on a remote Oracle Tuxedo node, it processes the connection and invokes the TMA TCP Handler.

- Configuring CICS Socket to Start or Stop

2.1.1 Configuring CICS Socket to Start or Stop

- You can let the CICS Socket interface start or stop automatically by modifying the CICS Program List Table (PLT):
  - Startup (PLTPI)
    To start the IP CICS socket interface automatically, enter the following in PLTPI after the `DFHDELIM` entry:

```
DFHPLT TYPE=INITIAL,SUFFIX=SI
DFHPLT TYPE=ENTRY,PROGRAM=DFHDELIM
DFHPLT TYPE=ENTRY,PROGRAM=EZACIC20
```

```
DFHPLT TYPE=FINAL
END
```

– Shutdown (PLTSD)
To shut down the IP CICS Socket interface automatically (including all other IP CICS sockets enabled programs), make the following entry in PLTSD before the `DFHDELIM` entry:

```
DFHPLT TYPE=INITIAL,SUFFIX=SD
DFHPLT TYPE=ENTRY,PROGRAM=EZACIC20
DFHPLT TYPE=ENTRY,PROGRAM=DFHDELIM
DFHPLT TYPE=FINAL
END
```

- You can also start or stop the CICS TCP/IP manually, using the CICS EZAO operator transaction.

2.2 Running Oracle TMA TCP for CICS

The TMA TCP Handler is invoked automatically by the Listener process. Once invoked, the Handler takes control of the socket connection and retains control until either the Handler is shut down or until there is a network problem that affects the socket connection. The Handler processes service requests up to the configured multiplex count. To process more service requests than the configured multiplex count, TMA TCP gateway starts more than one Handler. For limitations of the IBM Sockets for CICS Listener, refer to the appropriate IBM product documentation.

2.2.1 Initializing the Handler

The very first service request that is sent from the TMA TCP gateway running on a remote Oracle Tuxedo node causes the following to occur.

1. CICS Sockets Listener starts the TMA TCP for CICS Handler
2. Listener issues a `givesocket()` function call
3. Handler issues a `takesocket()` function call
4. Listener resumes listening for new connection requests
5. Handler communicates directly with the remote TMA TCP gateway using TCP/IP

2.2.2 Processing Remote Service Requests

1. The TMA TCP Handler receives the request from the remote TMA TCP gateway (in the Oracle Tuxedo region) over TCP/IP. If necessary, the data is translated and/or converted into the proper data format or layout.

2. If the multiplex count is 1 and security is disabled, or if the service request came from a version of TMA TCP gateway prior to Version 3.0, then the following tasks occur.
   a. The Handler issues a CICS `LINK` command to execute the program specified in the TMA TCP protocol header. With the `LINK` command it also passes along any request data provided by the client application that made the original Oracle Tuxedo service request.
   b. The Handler waits for the CICS program to finish and receives any returned data from the CICS program.
   c. The Handler transmits the response to the remote TMA TCP gateway.
   d. The Handler stays connected to the remote gateway awaiting another service request.
3. If the multiplex count is greater than 1 or security is enabled, then the following tasks occur.
   a. The Handler issues an `EXEC CICS START TRANS` call with the transaction specified in the Inbound Service File for the service specified in the TMA TCP protocol header. The transaction should be the same as the Application Handler program.

      > **Note:**
      >
      > If security is enabled, the `EXEC CICS START TRANSID` call uses the user ID specified in the TMA TCP protocol header.

   b. For any completed service requests, the Handler retrieves the response data from the Application Handler.
   c. The Handler transmits the response to the remote TMA TCP gateway gateway.
   d. The connection between the Handler and the gateway remains and the Handler waits for another service request.

For `tpacall/TPNOREPLY` requests, the remote program is invoked by a `CICS START TRANSID` command and no data is returned to the original caller. In this case, a unique transaction must be defined for the service. Use the Inbound Service Information screen to enter this unique transaction name rather than using the transaction name that starts the Application Handler.

2.2.3 Shutting Down the Handler

When the network connection is lost, the Handler process automatically shuts down. The next service request sent causes the Listener to automatically start a new Handler, if necessary.

Use the supplied shutdown transaction `BDWN` to terminate active TMA TCP for CICS programs. Depending on the options specified, this causes *all* Handlers to shut down gracefully. The name of the `BDWN` transaction may have been changed at your site during installation, so verify the name.

2.2.3.1 Using BDWN to Shut Down the Handler

You can use the `BDWN` transaction in a CICS region with the following parameters to shut down Handlers in various ways. The command line syntax for `BDWN` is illustrated in the following listing.

Listing BDWN Command Line Syntax for Handlers

```
BDWN [ALL | CLEANUP | HANDLER I | HANDLER]
```

BDWN
Shuts down all Handlers or all Requesters or both. It also frees shared memory that was allocated by a Handler that has abended without freeing the shared memory that it allocated. You can specify optional parameters with the `BDWN` transaction to shut down Handlers immediately or after the processing of all requests has completed. The default is `ALL`.

ALL
Shuts down all Handlers and Requesters gracefully allowing them to complete all processing of all requests that were received before the execution of the `BDWN` transaction. Specifying `ALL` also frees any shared memory.

This is the default for `BDWN`.

CLEANUP
Frees any shared memory of Handlers that have abended. `CLEANUP` does *not* shut down any Handlers or Requesters.

HANDLER I
Shuts down all Handlers immediately and frees any shared memory of Handlers that have abended. This parameter does *not* shut down any Requesters.

HANDLER
Shuts down all Handlers gracefully allowing them to complete all processing off all requests that were received before the execution of the `BDWN` transaction. This parameter also frees any shared memory of Handlers that have abended. It does *not* shut down any Requesters.

2.2.4 Starting the Requester Program

The Requester is started automatically when the first service request for it is made by a CICS client program. At that point, the Requester establishes a connection with its remote endpoint and updates its control tables with run-time information for use by subsequent requests. If the connection with the remote endpoint is lost for any reason, the Requester attempts to re-establish the connection automatically. After a configured number of unsuccessful connection attempts, the Requester marks itself disabled.

If the gateway receives additional service requests, they are accommodated as long as the maximum multiplex count for the existing connection is not exceeded. Also, additional connections are opened, as necessary, until the configured maximum connection count is reached or all requests are accommodated.

2.2.5 Processing TMA TCP for CICS Originated Service Requests

1. The CICS client program (your program) issues an `EXEC CICS LINK` command to the TMA TCP for CICS Pre-requester.
2. The Pre-requester verifies that the request is valid, and then determines whether a Requester has been started for the specific endpoint for which this request is destined. If a Requester is not already running, the Pre-requester starts one.
3. The request is then handed over to the Requester.
4. The Requester transmits the request information to the remote Oracle Tuxedo domain.

5. If the request is a type that needs a response, the Requester receives that response back from Oracle Tuxedo, and hands the data over to the Pre-requester.
6. The Pre-requester issues an `EXEC CICS RETURN` command to the client program (your program). The client receives its response in the `COMMAREA`.

2.2.6 Shutting Down the Requester

There are two ways to shut down the Requester:

- Use the administrative tool (described in Configuring and Administering Oracle TMA TCP for CICS) to disable the Requester. This method causes the selected Requester to clean up its tables and shut down gracefully. It also prohibits any service requests invoking it. When you are ready, use the administrative tool to enable the Requester.
- Use the supplied shutdown transaction `BDWN`. This method causes ALL Requesters to shut down gracefully. The name of the `BDWN` transaction may have been changed at your site during installation. Check with the person who installed TMA TCP for CICS at your site.
- Using BDWN to Shut Down the Requester

2.2.6.1 Using BDWN to Shut Down the Requester

You can use the `BDWN` transaction in a CICS region with the following parameters to shut down Requesters in various ways. The command line syntax for `BDWN` is illustrated in the following listing.

Listing BDWN Command Line Syntax for Requesters

```
BDWN [ALL | REQUESTER I | REQUESTER]
```

BDWN
Shuts down all Handlers or all Requesters or both. It also frees shared memory used by the Requesters associated with each logical machine ID (`LMID`). You can specify optional parameters with the `BDWN` transaction to shut down Handlers or Requesters immediately or after processing of all requests has completed. The default is `ALL`.

ALL
Shuts down all Handlers and Requesters gracefully allowing them to complete all processing of all requests that were received before the execution of the `BDWN` transaction. Specifying `ALL` also frees any shared memory.

This is the default for `BDWN`.

REQUESTER I
Shuts down all Requesters immediately and frees memory associated with each `LMID`. This parameter does *not* shut down any Handlers.

REQUESTER
Shuts down all Requesters gracefully allowing them to complete all processing off all requests that were received before the execution of the `BDWN` transaction. It also frees memory associated with each `LMID`. This parameter does *not* shut down any Handlers.

2.3 Translating Data with TMA TCP gateway

Due to the way TMA TCP gateway translates and converts data on the remote Oracle Tuxedo system, the CICS programmer does not need to do anything to prepare data that is destined for the remote Oracle Tuxedo system.

The key to this high degree of transparency is the TMA TCP gateway configuration. It is through this mechanism that environmental differences, such as naming conventions and data formats, are concealed from programmers and programs.

Although all data is converted and translated automatically by the remote TMA TCP gateway, the rules implemented are outlined in the following subsections to assist the CICS programmer in understanding how the data is manipulated. It is important for the CICS programmer to remember that this information is written from the point of view of the Oracle Tuxedo environment.

When a client program on the remote Oracle Tuxedo system sends data to (or receives data from) a service routine on a different model of computer, TMA TCP gateway automatically translates data as required. Translation involves changing the representation of intrinsic data types by changing attributes such as word length and byte order.

The following subsections describe the basic rules that TMA TCP gateway follows when it translates data and provide detailed information about how TMA TCP gateway handles string and numeric data.

2.3.1 Oracle Tuxedo Terminology

The following terms are some commonly used Oracle Tuxedo terms for buffer types.

Table 2-1 Oracle Tuxedo Terminology

Term	Definition
`STRING`	A buffer of character data that is terminated by the first null character in the buffer. Typically, character string buffers undergo translation when sent to a system that is different from the sending system.
`CARRAY`	A `CARRAY` is a buffer of raw data that contains no terminating character and that undergoes no conversion or translation; the data is sent from one system to another without modification. A `CARRAY` is an exemplary buffer type for a graphics file.
`VIEW`	A `VIEW` buffer is a collection of field definitions that can be treated as a single entity. It is comparable to a record layout in COBOL or a structure in C.
`FML`	`FML` (Fielded Manipulation Language) buffers are variable length, dynamic, self-describing buffers. Each field in the buffer has its own descriptive header. In Oracle Tuxedo, `FML` buffers can be tied closely to `VIEW` buffers so that conversion from one to the other is direct.

2.3.2 Data Translation Rules

The following table lists the data translation rules that TMA TCP gateway follows.

Table 2-2 Data Translation Rules

Field Type	Translation Rules
CARRAY	Passed untranslated as sequences of bytes
STRING and CHAR	Translated from ASCII to EBCDIC (if needed)
SHORT	Translated to S9(4) COMP
LONG	Translated to S9(9) COMP
FLOAT	Translated to COMP-1
DOUBLE	Translated to COMP-2

> **Note:**
>
> Oracle Tuxedo provides a field type named dec_t that supports decimal values within VIEWs. The TMA TCP gateway product translates these fields into machine independent representations of packed decimals. For example, dec_t(m,n) becomes S9(2*m-(n+1))V9(n) COMP-3. Therefore, a decimal field with a size of 8,5 corresponds to S9(10)V9(5) COMP-3.

The following table summarizes the translation rules between C and IBM/370 data types.

Table 2-3 Translation Rules Between C and IBM/370 Data Types

Remote Data Type	Description	View Field Type/ Length
PIC X(n)	Alpha-numeric Characters	string / n
PIC X	Single Alpha-numeric Character	char
PIC X(n)	Raw Bytes	carray / n
PIC X	Single Numeric Byte	carray / 1
PIC S9(4) COMP	16-bit Integer	short
PIC S9(9) COMP	32-bit Integer	long
COMP-1	Single-precision Floating Point	float
COMP-2	Double-precision Floating Point	double
PIC S9((m+(n+1))/2)V9 (n) COMP-3	Packed Decimal	dec_t / m,n

2.3.3 Strings and Numeric Data: A Closer Look

This subsection provides suggestions that help you develop VIEW definitions for input and output buffers and records. It also explains how string data and numeric data are treated in the TMA TCP gateway environment.

- Including NULL Characters in String Length Calculations
- Converting Numeric Data

2.3.3.1 Including NULL Characters in String Length Calculations

When you create `VIEW` definitions for input and output records that are used by CICS applications, do not specify an extra position for the terminating NULL characters that are used in string fields.

For example, when a CICS application program expects 10 characters in an input record, specify *10* for that field, not 10 plus 1.

> **Note:**
>
> Although TMA TCP gateway does not require strings to be NULL-terminated, it respects NULL termination. Therefore, when TMA TCP gateway detects a NULL (zero) character within a string, it does not process any subsequent characters. To pass full 8-bit data that contains embedded NULL values, use a `CARRAY` type field or buffer.

The character set translations performed by TMA TCP gateway can be fully localized, in accordance with the X/Open XPG Portability Guides. ASCII and EBCDIC translations are loadable from message files. The TMA TCP gateway software contains default behaviors which should meet the requirements of most English-language applications. However, you may find it necessary to customize tables. See the Oracle TMA TCP gateway User Guide for complete instructions.

2.3.3.2 Converting Numeric Data

You can convert numeric data into different data types easily, provided that you have enough range in the intermediate and destination types to handle the maximum value you need to represent.

For example, you can convert an FML field of double into a packed decimal field on the remote target system by specifying an appropriate `dec_t type VIEW` element.

In addition, you can convert numeric values into strings (and the reverse). For example, while FML buffers do not directly support the `dec_t type`, you can place decimal values in string fields and map these to `dec_t fields` within `VIEW` definitions.

3
Configuring Oracle TMA TCP Security

The Oracle TMA TCP product supports a security feature that allows a requester from Oracle Tuxedo services to pass a user ID through the CICS server interfaces for verification through a third-party security package. The following topics explain the how to set up security:

- Service Request Processing with Security
- Setting Up Security for TMA TCP for CICS
- Security Enforcement: SSL/TLS Support

3.1 Service Request Processing with Security

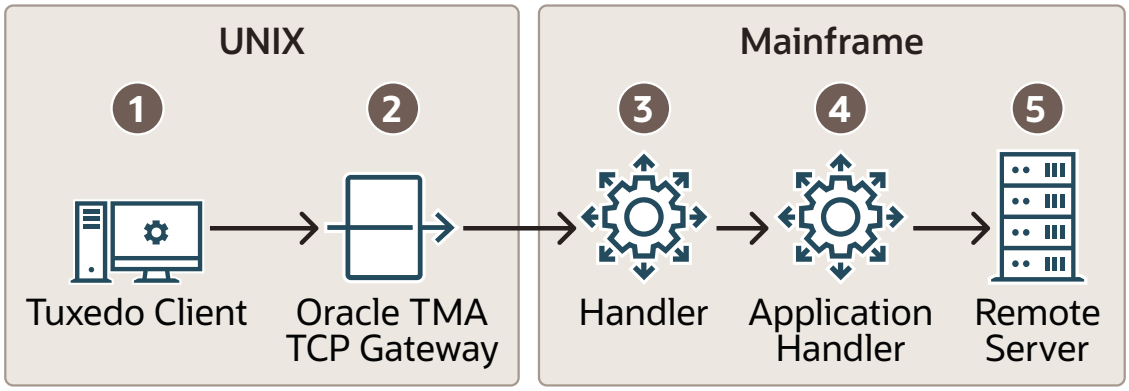
The following sections describe the process flow for security verification of a service request.

- Security Checking from UNIX to Mainframe
- Security Checking from Mainframe to UNIX

3.1.1 Security Checking from UNIX to Mainframe

The following figure depicts the process flow for security verifications from TMA TCP for CICS on UNIX to a mainframe.

Figure 3-1 Security Checking for UNIX to Mainframe Transactions



1. When the TMA TCP gateway client program performs a `tpinit()`, the user's Tuxedo identity is validated against the `tpusr` file.
2. When the client program issues a `tpcall()` or `tpacall()`, Tuxedo verifies (against the `tpacl` file) the user is authorized to invoke the gateway service.
3. With each request, the TMA TCP gateway passes the user's Tuxedo identity to the remote TMA TCP for CICS gateway (to the Handler).

> **Note:**
>
> To pass authority checking, the user's Tuxedo identity must match the mainframe user ID exactly.
>
> TMA TCP 22c Gateway functionality is different from TMA TCP 12.1.3 Gateway and earlier.
>
> For TMA TCP 12.1.3 Gateway to establish connection with TMA TCP 22c CICS, RP001 requires to be installed (released in March 2024). This enables inter-operability between TMA TCP Gateway 22c and TMA TCP Gateway 12.1.3.
>
> To establish TMA TCP 12.1.3 Gateway initial connection, connection security (specified as `RMTNAME` and `PASSWORD` in the GWICONFIG file) is passed from TMA TCP gateway to remote gateway. `RMTNAME` and `PASSWORD` must match the values configured on the remote gateway for the connection to be established.

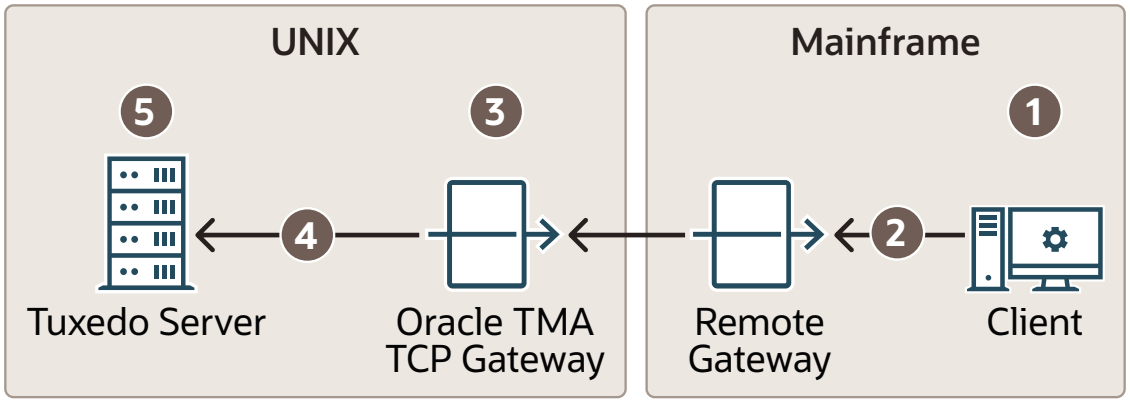
4. The remote TMA TCP for CICS gateway Handler initiates an Application Handler to act on behalf of the specified user ID.
5. The Application Handler calls the specified service using system security to check authorization.

> **Note:**
>
> You may need to update your surrogate security definitions to allow the successful invocation of the CICS application program (`EXEC CICS START TRANSID`). See your mainframe security administrator if your site has this requirement.

3.1.2 Security Checking from Mainframe to UNIX

The following figure depicts the process flow for security verifications from a mainframe to TMA TCP gateway on UNIX.

Figure 3-2 Security Checking for Mainframe to UNIX Transactions



1. The user ID, established at mainframe log in, is checked by system security to verify that the user has permission to start a client transaction.

2. The user ID is checked by system security to verify that the user has permission to send a request to the gateway.
3. With each request, the gateway passes the user ID to the Tuxedo gateway.

> **Note:**
>
> To pass authority checking, the user's Tuxedo identity must match the mainframe user ID exactly.

4. The TMA TCP gateway maps the mainframe user ID to a Tuxedo user ID and issues the service request on behalf of that user.
5. The Tuxedo server performs access checks (based on the `tpacl` file) to verify that the user has access to the requested service.

3.2 Setting Up Security for TMA TCP for CICS

The TMA TCP for CICS product supports enhanced security. This interface allows a requester from Oracle Tuxedo services to pass a User ID through the CICS server interface for authorization through your security package. For field definitions, refer to the Configuring and Administering Oracle TMA TCP for CICS section.

- Securing Inbound Services
- Securing User Connections
- Securing Outbound Connections from CICS to CICS
- Securing Outbound Connections from CICS to IMS
- Securing Outbound Connections from CICS to UNIX
- Securing Outbound Services

3.2.1 Securing Inbound Services

Complete the following tasks to enable the security feature for each inbound service.

1. Set up transaction security through the mainframe with the security administrator.
2. Specify `SECURITY=Y` in the Inbound Services screen for each service you want to secure. When `SECURITY=Y`, the gateway attempts to start user programs with the username that initiated the request as reported by the remote system.
   If `SECURITY=N`, the gateway starts user programs using the gateway's user ID (as controlled by the socket listener).

3.2.2 Securing User Connections

For TMA TCP 12.1.3 Gateway and earlier, complete the following steps to enable security for each connection.

1. Specify `SECURITY=C` in the Handler Configuration screen.
2. Enter `ACCOUNT` and `PASSWORD` values in the User Connection Account screen.
   Verify that the parameter values for `ACCOUNT` and `PASSWORD` in the User Connection Account match the `RMTACCT` and `PASSWORD` values in the TMA TCP gateway `GWICONFIG` file `*FOREIGN`

section when SECURITY=C. If these values do not match and SECURITY=C, a security error occurs.

If SECURITY=F, the gateway allows a connection without any verification.

For TMA TCP 12.2.2 Gateway and later, Original user name and password validation for TMA TCP connection validation is obsoleted. The magic number is used instead to enhance the connection validation. A connection is established irrespective of the SECURITY flag, and ACCOUNT and PASSWORD is not validated.

3.2.3 Securing Outbound Connections from CICS to CICS

Complete the following tasks to enable the security feature for each outbound connection.

1. Specify SECURITY=Y on the appropriate Requester screen.
2. Enter ACCOUNT and PASSWORD values on the appropriate Requester screen.
   Verify that the parameter values for ACCOUNT and PASSWORD in the Requester screen match the ACCOUNT and PASSWORD values in the User Connection Account screen.

   When SECURITY=Y, the requester program sends the ACCOUNT and PASSWORD to the remote CICS system on connection initiation. When SECURITY=N, the gateway attempts to make a connection without any verification.

> **Note:**
>
> The security for connection validation is obsolete.

3.2.4 Securing Outbound Connections from CICS to IMS

Complete the following tasks to enable the security feature for each outbound connection.

1. Specify SECURITY=Y on the appropriate Requester screen.
2. Enter ACCOUNT and PASSWORD values on the appropriate Requester screen.
   Verify that the parameter values for ACCOUNT and PASSWORD in the Requester screen match the ACCOUNT and PASSWORD values in the GATEWAY TYPE=REMOTE statement.

   When SECURITY=Y, the requester program sends the ACCOUNT and PASSWORD to the remote IMS system on connection initiation. When SECURITY=N, the gateway attempts to make a connection without any verification.

> **Note:**
>
> The security for connection validation is obsolete.

3.2.5 Securing Outbound Connections from CICS to UNIX

For TMA TCP 12.1.3 Gateway and earlier, complete the following steps to enable security for each outbound connection.

1. Specify LMID TYPE=X on the appropriate Requester screen.
2. Enter ACCOUNT and PASSWORD values on the appropriate Requester screen.

Verify that the parameter values for `ACCOUNT` and `PASSWORD` in the Requester screen match the `RMTACCT` and `PASSWORD` values in the `*FOREIGN` section of the TMA TCP gateway in the `GWICONFIG` file.

When `LMID TYPE=X`, the requester program sends the `ACCOUNT` and `PASSWORD` to the remote UNIX system on connection initiation.

For the TMA TCP 12.2.2 Gateway and later, complete the following step to enable security for each connection.

1. Specify `LMID TYPE=T` on the appropriate Requester screen.
   Original user name and password validation for TMA TCP connection validation is obsoleted. The magic number is used instead to enhance the connection validation.

   In addition, if `LMID TYPE=X`, the transaction fails and throws the error "`Invalid LMID Type X for 12.2.2 and latest Tuxedo versions.`" in the CICS log.

3.2.6 Securing Outbound Services

Complete the following tasks to enable the security feature for each outbound service.

1. Enable security for the corresponding outbound connection.
2. Specify `SECURITY=Y` on the appropriate Outbound Service screen.
3. Set up security for the appropriate users on the target system.

3.3 Security Enforcement: SSL/TLS Support

The Oracle TMA TCP for CICS interface supports secure communication over network links between Oracle TMA TCP gateways and Oracle TMA TCP CICS applications. Using TLS1.2, the data is encrypted.

Oracle TMA TCP gateway supports the following options:

- **TCP**: It is compatibility with the previous version of the Oracle TMA TCP CICS component, which means raw TCP connections without SSL support, with no policy files, rules, or certificates.
- **SSL (default value)**: It refers to the connection between the Handler/ Requestor on the CICS side and the Oracle TMA TCP gateway on the Tuxedo end are SSL enabled with two-way authentication, which has been configured with AT-TLS rules, policy agents, and certificates.

Ciphers supported: in addition to a wide range of ciphers supported by z/OS:

- `TLS_RSA_WITH_AES_256_CBC_SHA256`
- `TLS_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_RSA_WITH_AES_128_CBC_SHA256`
- `TLS_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
- Setting Up the Policy Agent, AT-TLS, and Certificates
- Securing Inbound Services to Add TLS Support

- Securing Outbound Services to Add TLS Support

3.3.1 Setting Up the Policy Agent, AT-TLS, and Certificates

For secure transmission of data, Oracle TMA TCP for CICS utilizes IBM's Policy Agent and AT-TLS rules, along with a certificate setup in the keyring.

In z/OS Communications Server, the Policy Agent (PAGENT) implements and enforces a set of rules and policies that govern how users and applications can access network resources.

Application Transparent Transport Layer Security (AT-TLS) is IBM's solution for providing secure connectivity between SSL/TLS-enabled applications and existing mainframe applications. It enables Secure Socket Layer (SSL) security on the mainframe. It is the Policy Agent (PAGENT) that configures the encryption and decryption policies. The PAGENT policy determines which traffic on the mainframe TCP/IP stack should be secured with SSL.

AT-TLS provides a secure session on behalf of an application, therefore no changes to the application code are required. Oracle TMA TCP for CICS utilizes this feature to enable secure communication.

Refer to *IBM's z/OS Communications Server - IP CICS Sockets Guide* for information on applications that use IP CICS Socket API for TCP/IP client-server systems with AT-TLS rules.

A network administrator who defines network policies using PAGENT and AT-TLS rules must refer to the following IBM documentation.

- *z/OS Communications Server - IP Configuration Guide*
- *z/OS Communications Server - IP Configuration Reference*

Setting up Keyring and Certificate

You configure certificates on the mainframe by using ESM (Enterprise Security Manager) tools such as RACF. For CICS SSL applications, the keyring's user ID must be CICS user ID (SYSCICS). Keyrings are generated and associated with their respective CICS regions.

Refer to *IBM's z/OS Security Server RACF Command Language Reference* for keyring setup and to create a self-signed CA certificate.

Using an Oracle wallet, you can set Oracle TMA TCP Gateway certificates containing three parts.

- Self-signed CA certificate
- A user certificate that the CA certificate has signed is mentioned above.
- Private key

Server Authentication

When authenticating a server, the client verifies the validity of the server's certificate, which must be signed by a trusted Certificate Authority (CA).

Client Authentication

When client authentication is used, the server verifies that the client's certificate is valid and signed by a Certificate Authority trusted by the server.

3.3.2 Securing Inbound Services to Add TLS Support

The TMA TCP for CICS Inbound flow uses Sockets for CICS Listener. Follow these steps to enable TLS Support.

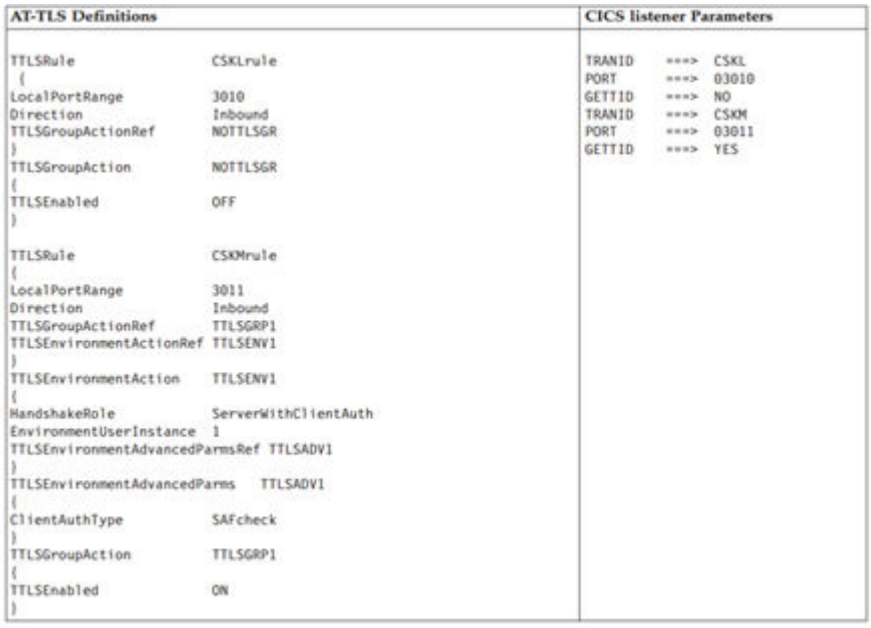
1. Configure and enable mutual TLS on the client side – `SSL`.
2. Enable the `GETTID` (Get AT-TLS ID) parameter to get client certificates and user IDs from AT-TLS by setting it to `YES` in the IBM listener configuration via EZAC transaction.
   If the status is `ENABLED`, the listener can get client certificates and user IDs through AT-TLS enabled in the TCP/IP stack.
3. Ensure to check both client and server certificates for two-way authentication:
   a. CICS keyring must have client and server certificates.
   b. Tuxedo wallet must have client and server certificates.
4. Define and load `AT-TLS` inbound rule (`CICS_SERVER`) in policy agent for configured port on IBM Listener, follow the listing.
   TTLSEnvironmentAction must specify HandshakeRole as ServerWithClientAuth with ApplicationControlled off.

   Listing Sample reference for TTLSEnvironmentAction, HandshakeRole, ApplicationControlled

```
TTLS Condition Summary:                 NegativeIndicator: Off
   Local Address:
    FromAddr:           All
    ToAddr:             All
   Remote Address:
    FromAddr:           All
    ToAddr:             All
   LocalPortFrom:       3010              LocalPortTo:       3010
   RemotePortFrom:      0                 RemotePortTo:      0
   JobName:                               UserId:
   ServiceDirection:    Inbound

HandshakeRole:              ServerWithClientAuth
    SuiteBProfile:              Off
    TTLSKeyringParms:
     Keyring:                   SYSCICS/CICSRING
    TTLSEnvironmentAdvancedParms:
     SSLv2:                     Off
     SSLv3:                     Off
     TLSv1:                     Off
     TLSv1.1:                   Off
     TLSv1.2:                   On
     TLSv1.3:                   Off
     MiddleBoxCompatMode:       Off
     ApplicationControlled:     Off
```

Figure 3-3 Sample Inbound AT-TLS rule - from IBM's IP CICS Sockets Guide



AT-TLS Definitions

```
TTLSRule                CSKLrule
 {
LocalPortRange          3010
Direction               Inbound
TTLSGroupActionRef      NOTTLSGR
}
TTLSGroupAction         NOTTLSGR
{
TTLSEnabled             OFF
}

TTLSRule                CSKMrule
{
LocalPortRange          3011
Direction               Inbound
TTLSGroupActionRef      TTLSGRP1
TTLSEnvironmentActionRef TTLSENV1
}
TTLSEnvironmentAction   TTLSENV1
{
HandshakeRole           ServerWithClientAuth
EnvironmentUserInstance 1
TTLSEnvironmentAdvancedParmsRef TTLSADV1
}
TTLSEnvironmentAdvancedParms  TTLSADV1
{
ClientAuthType          SAFcheck
}
TTLSGroupAction         TTLSGRP1
{
TTLSEnabled             ON
}
```

CICS listener Parameters

```
TRANID    ===>  CSKL
PORT      ===>  03010
GETTID    ===>  NO
TRANID    ===>  CSKM
PORT      ===>  03011
GETTID    ===>  YES
```

3.3.3 Securing Outbound Services to Add TLS Support

The outbound flow of TMA TCP for CICS uses the CICS Socket interface. Follow these steps to enable TLS Support for outbound flow.

1. Configure and enable mutual TLS on the server side – `SSL`.
2. It is required to set up certificates on both the client and server sides to enable two-way authentication:
   a. CICS keyring must have client and server certificates
   b. Tuxedo wallet must have client and server certificates
3. Define and load `AT-TLS` outbound rule (`CICS_CLIENT`) in policy agent for remote address and remote port range.
   The TTLSEnvironmentAction statement in `AT-TLS CICS_CLIENT` rule must contain HandshakeRole as Client and ApplicationControlled must be off.

Listing Sample reference for TTLSEnvironmentAction, HandshakeRole, ApplicationControlled

```
TTLS Condition Summary:                 NegativeIndicator: Off
   Local Address:
    FromAddr:           All
    ToAddr:             All
   Remote Address:
    FromAddr:           111.111.111.111
    ToAddr:             111.111.111.111
   LocalPortFrom:       0                 LocalPortTo:       0
   RemotePortFrom:      1111              RemotePortTo:      1111
   JobName:                               UserId:
   ServiceDirection:    Outbound
```

```
HandshakeRole:              Client
    SuiteBProfile:              Off
    TTLSKeyringParms:
     Keyring:                   SYSCICS/CICSRING
    TTLSEnvironmentAdvancedParms:
     SSLv2:                     Off
     SSLv3:                     Off
     TLSv1:                     Off
     TLSv1.1:                   Off
     TLSv1.2:                   On
     TLSv1.3:                   Off
     MiddleBoxCompatMode:       Off
     ApplicationControlled:     Off
```

Figure 3-4 Sample Outbound AT-TLS rule - from IBM's IP CICS Sockets Guide

AT-TLS Definitions

```
TTLSRule                        ClientRule1
    {
RemotePortRange          3010
Userid                   CICS1
Direction                Outbound
TTLSGroupActionRef       NOTTLSGR
}
TTLSGroupAction                 NOTTLSGR
{
TTLSEnabled              OFF
}

TTLSRule                        ClientRule2
{
RemotePortRange          3011
Direction                Outbound
TTLSGroupActionRef       TTLSGRP2
TTLSEnvironmentActionRef TTLSENV2
}
TTLSEnvironmentAction           TTLSENV2
{
HandshakeRole            Client
EnvironmentUserInstance  1
}
TTLSGroupAction                 TTLSGRP2
{
TTLSEnabled              ON
}
```

4

Configuring and Administering Oracle TMA TCP for CICS

It is the responsibility of the Oracle Tuxedo administrator to set up the configuration file, but close coordination with the Oracle Tuxedo application developer and the CICS programmer is necessary.

The following subsections describe the Oracle Tuxedo Mainframe Adapter for TCP (CICS) (hereafter referenced as TMA TCP for CICS) Maintenance System. The Oracle TMA TCP for CICS Maintenance System is an online CICS application for use in configuring, maintaining, and administering the TMA TCP for CICS gateway. The following topics explain the Maintenance System:

To start the administration system, enter the transaction code as defined to CICS in the installation procedure. If the name was not changed during installation, the name of the transaction is BEAM.

4.1 Menu Navigation

You can access any of the following six groups of menus for maintaining connections, requesters, outbound services, the user connection account, inbound services, and Handler configuration. The following table describes how you can use each group of menus.

Table 4-1 Menu Groups

Menu Type	Use
Connection	To monitor and control configured and active connections
Requester	To configure and maintain remote endpoints
Outbound Service Information	To configure each remote service and specify which Requester to use for each service
User Connection Account	To create and maintain user accounts

Table 4-1 (Cont.) Menu Groups

Menu Type	Use
Inbound Service Information	To configure services residing locally that are accessed remotely
Handler Configuration	To configure and maintain the local endpoint

Each of these topics is discussed in more detail in the following sections.

4.2 The Main Menu

The Main menu (`BEAM`) gives you access to all the maintenance screens.

```
BEAPMNU                  ORACLE TMA TCP FOR CICS
BEAM       M1

                                       SELECTION SCREEN
       TABLE
OPERATION
  ----------------
-----------
   C - CONNECTION                                                    1 -
INSERT
   R - REQUESTER                                                     2 -
UPDATE
   S - OUTBOUND SERVICE INFORMATION                                  3 -
INQUIRE
   U - USER CONNECTION ACCOUNT                                       4 -
DELETE
   I - INBOUND SERVICE INFORMATION                                   5 -
BROWSE
   H - HANDLER CONFIGURATION

                               SELECTION: __                         (e.g.
R3)
ENTER: PROCESS, PF3: EXIT
```

- Usage

4.2.1 Usage

Use the Main menu to access the screens that make up the maintenance system. To move from the Main menu to a sub-menu, enter the appropriate two-character code. The first character in the code denotes the area in which you want to operate; the second character denotes the operation you want to perform on that area.

The following table lists the codes for the areas of operation.

Table 4-2 Main Menu (BEAM) Sub-menu Codes

Code	Area of Operation
C	Connections
R	Requesters
S	Outbound Service Information
U	User Connection Account
I	Inbound Service Information
H	Handler Configuration

The following table lists the codes for the allowable operations.

Table 4-3 Main Menu (BEAM) Operation Codes

Code	Allowable Operation
1	Insert
2	Update
3	Inquire
4	Delete
5	Browse

Because some operations are not available in all three areas, the following table lists the valid combinations.

Enter This Code	To Access This Screen
C2	Update Connection
C3	Inquire Connection
C5	Browse Connection
R1	Insert Requester
R2	Update Requester
R3	Inquire Requester
R4	Delete Requester
R5	Browse Requester
S1	Insert Outbound Service Information
S2	Update Outbound Service Information
S3	Inquire Outbound Service Information
S4	Delete Outbound Service Information
S5	Browse Outbound Service Information
U1	Insert User Connection Account
U2	Update User Connection Account
U3	Inquire User Connection Account
U4	Delete User Connection Account
U5	Browse User Connection Account
I1	Insert Inbound Service Information
I2	Update Inbound Service Information

Enter This Code	To Access This Screen
I3	Inquire Inbound Service information
I4	Delete Inbound Service Information
I5	Browse Inbound Service Information
H2	Update Handler Configuration
H3	Inquire Handler Configuration

You can use the maintenance system screens to view and alter a connection, but not to insert (`create`) or delete a connection. Connections are created and deleted by TMA TCP for CICS in its normal operation.

The maintenance system checks the two-character selection code that you enter and displays the appropriate screen if the code is valid. If the code you enter is not valid, you receive an error message.

4.3 The Connection Screens

The three screens available for maintaining connection instances are labeled Update, Inquiry, and Browse. The respective screens allow you to make an inquiry concerning a specific connection, to browse a list of all connections, or to disable/enable a connection.

A connection instance is an established TCP/IP connection between a remote endpoint and a Requester or a Handler. For the purposes of TMA TCP for CICS, a remote endpoint is an TMA TCP gateway executing within a remote Oracle Tuxedo domain.

4.3.1 PF Keys

The following function keys are available on various connection screens.

Table 4-4 Function Keys

Function Key	Definitions
ENTER	Process the selection code entered
PF3	Transfer to Main Menu
PF5	Transfer to Connections Browse screen
PF7	Display the previous page of records
PF8	Display the next page of records

> **Note:**
>
> If you enter data and press `PF3` or `PF5` before pressing `ENTER`, the current operation process is aborted and the new screen is displayed.

4.3.2 Update Connection Screen (C2)

Use the UPDATE CONNECTION screen to update a record from the Connection file. When the screen initially displays, the LOGICAL MACHINE NAME and TYPE fields are unprotected. Enter a valid LOGICAL MACHINE NAME (gateway ID) and TYPE and press ENTER. The screen re-displays showing the data from the record you specified and the STATUS field is unprotected. The message RECORD READY FOR UPDATE displays. You can now make changes to the record.

```
BEAPCON                          ORACLE TMA TCP FOR CICS
BEAM       C2

                                     UPDATE CONNECTION


                              LOGICAL MACHINE NAME:

                              TYPE:

                              STATUS:

                              MAX MSG SIZE:

                              REQUESTER TASK NUMBER:
                              NUMBER REQUESTS:
                              NUMBER SUCCESS REQS:
                              NUMBER RECONNECTS:
                              NUMBER OPEN SOCKETS:
                              NUMBER SESSIONS ACTIVE:

 ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.3.2.1 Fields

Field Name	Description
LOGICAL MACHINE NAME	This field name is the gateway ID. Give it a unique name up to 16 characters. Example: (bankmach1) For Requesters, this field name is the LMID associated with the service that the Requester is requesting. For a Handler, this field name is BEAH followed by the task number. The task number of the Handler is given in the BEALOG.
TYPE	The type of connection. Specify I for incoming connections or O for outgoing connections.
STATUS	The status of the connection. Specify E to enable the connection. Specify D for normal shutdown which allows initiated tasks to complete prior to disconnecting. Specify A for immediate shutdown which aborts all initiated tasks and disconnects.
MAX MSG SIZE	The largest message allowed to be sent across this connection. The maximum is 32000. Example: (31000)

Field Name	Description
REQUESTER TASK NUMBER	The task number of the Requester that is currently associated with the LOGICAL MACHINE NAME. If there is not an active Requester, the task number is for the Requester most recently associated with that LMID. For a Handler, this field is blank; the task number is part of the LMID.
NUMBER REQUESTS	The number of service requests made during this connection.
NUMBER SUCCESS REQS	The number of successful communications.
NUMBER RECONNECTS	The number of successful connections.
NUMBER OPEN SOCKETS	The number of sockets that are currently opened by the Requester.
NUMBER SESSIONS ACTIVE	The number of active sessions on this connection.

4.3.3 Inquire Connection Screen (C3)

Use this screen to inquire about a record from the Connection file. When the screen is initially displayed, the LOGICAL MACHINE NAME and TYPE fields are unprotected. Enter a valid LOGICAL MACHINE NAME (gateway ID) and TYPE and press ENTER. The screen is re-displayed with the data from the record you specified and the LOGICAL MACHINE NAME and TYPE fields are unprotected.

```
 BEAPCON                     ORACLE TMA TCP FOR CICS
BEAM    C3

                               INQUIRE CONNECTION


                          LOGICAL MACHINE NAME:

                          TYPE:

                          STATUS:

                          MAX MSG SIZE:

                          REQUESTER TASK NUMBER:
                          NUMBER REQUESTS:
                          NUMBER SUCCESS REQS:
                          NUMBER RECONNECTS:
                          NUMBER OPEN SOCKETS:
                          NUMBER SESSIONS ACTIVE:


 ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.3.3.1 Fields

Field Name	Description
LOGICAL MACHINE NAME	This name is the gateway ID. Specify a unique name up to 16 characters. Example: (bankmach1) For Requesters, this name is the LMID associated with the service that the Requester is requesting. For a Handler, this name is BEAH followed by the task number. The task number of the Handler is given in the BEALOG.
TYPE	The type of connection. I represents incoming connections or O represents outgoing connections
STATUS	The status of the connection. E means the connection is enabled. D means the connection is designated for a normal shutdown, which allows initiated tasks to complete prior to disconnecting. A means the connection shuts down immediately, aborts all initiated tasks, and disconnects.
MAX MSG SIZE	The largest message allowed to be sent across this connection. The maximum is 32000. Example: (31000)
REQUESTER TASK NUMBER	The task number of the Requester that is currently associated with the LOGICAL MACHINE NAME. If there is not an active Requester, the task number is for the Requester most recently associated with that LMID. For a Handler, this field is blank; the task number is part of the LMID.
NUMBER REQUESTS	The number of service requests made during this connection.
NUMBER SUCCESS REQS	The number of successful communications.
NUMBER RECONNECTS	The number of successful connections.
NUMBER OPEN SOCKETS	The number of sockets that are currently opened by the Requester.
NUMBER SESSIONS ACTIVE	The number of active sessions on this connection.

4.3.4 Browse Connection Screen (C5)

Use this screen to browse records in the Connection file and to select individual records for further processing. If you access this screen from the Main menu, the first record on file is displayed at the top of the screen. If you access this screen from the Connection Update screen or the Inquire screen, the list starts with the key received from that screen.

To select a record for processing enter a valid selection code in the SEL CDE field. For example, to make an inquiry about a record, enter "3". If you enter more than one selection code, the first one is used and all others are ignored. After the selection code is validated and processed, the screen for that process is displayed, and the record key appears in the LOGICAL MACHINE NAME field.

```
 BEAPCON                     ORACLE TMA TCP FOR CICS
BEAM       C5

                                BROWSE CONNECTION


 SEL     LOGICAL MACHINE    STA    MAXMSG    NUMBER    NUMBER    NUMBER    SOCK
SESS    ACT
 CDE           NAME         TUS     SIZE      REQS     SUCREQ    RECONS    ETS
IONS    IVE TYPE
```

```
 ---     ---------------  ---   ------   ------   ------   ------   ----
----   --- ----

  _       ________________  _     _____    _____   _____   _____      __
__     _   _
  _       ________________  _     _____    _____   _____   _____      __
__     _   _
  _       ________________  _     _____    _____   _____   _____      __
__     _   _
  _       ________________  _     _____    _____   _____   _____      __
__     _   _
  _       ________________  _     _____    _____   _____   _____      __
__     _   _
  _       ________________  _     _____    _____   _____   _____      __
__     _   _
  _       ________________  _     _____    _____   _____   _____      __
__     _   _
  _       ________________  _     _____    _____   _____   _____      __
__     _   _
  _       ________________  _     _____    _____   _____   _____      __
__     _   _
  _       ________________  _     _____    _____   _____   _____      __
__     _   _

 * SELCDE = (2: UPD, 3: INQ)
   ENTER: PROCESS, PF3: MENU, PF7: PREV, PF8: NEXT
 BEG/END OF FILE
```

4.4 The Requester Screens

A Requester is responsible for collecting request information to be sent to the remote Oracle Tuxedo domain. The Requester establishes network connectivity, transmits data to Oracle Tuxedo, and receives data from Oracle Tuxedo. Each Requester is responsible for one and only one remote endpoint (or one TCP/IP address/port combination). You can configure multiple Requesters to point to the same endpoint, but each Requester can have only one endpoint.

On the following maintenance screens, each instance of the Requester is given a logical machine ID (`LMID`). You can give a Requester any unique `LMID` that is meaningful to you. Every service name is associated with one `LMID`. This method allows the Requester to know which remote machine is responsible for a particular service.

- PF Keys
- Insert Requester Screen (R1)
- Update Requester Screen (R2)
- Inquire Requester Screen (R3)
- Delete Requester Screen (R4)
- Browse Requester Screen (R5)

4.4.1 PF Keys

The following table lists function keys available on various requester screens.

Function Key	Function
ENTER	Process the selection code entered
PF3	Transfer to Main menu
PF5	Transfer to Requester Browse screen
PF7	Display the previous page of records
PF8	Display the next page of records

> **Note:**
>
> If you enter data and press PF3 or PF5 before pressing ENTER, the operation process is aborted and the appropriate screen is displayed.

4.4.2 Insert Requester Screen (R1)

Use this screen to configure a new Requester by inserting a new record into the Requester file.

When the screen is first displayed, all the fields are unprotected. Type the required data, then press ENTER. After the data is validated and processed, the screen is re-displayed and all the fields are unprotected.

```
 BEAPREQ                    ORACLE TMA TCP FOR CICS
BEAM     R1

                              INSERT REQUESTER

   LMID:       ________________           MULTIPLEX_CNT:     __
   DNS: ____________________________________________________________________
   HOST ADDRESS: ________________
   PORT NUMBER: _____
                                        MIN TIME (MILLISEC): _____
   SECURITY(Y/N): _                     MAX TIME (MILLISEC): _____
   ACCOUNT ID: ________                 DELTA TIME (MILLISEC): _____
   PASSWORD:                            IDLE TIME (SECONDS): _____
                                        REQ IDLE TIME (SECONDS): _____
   MAX QUEUE SIZE: _____                LATENCY TIME (SECONDS): __
   MAX MSG SIZE: _____                  MAX CONNS: __
   RETRY LIMIT: _____

   LMID TYPE: _                       QUEUE NAME 1: ________
   START TRAN-ID: ____                QUEUE NAME 2: ________
   CICS DATA: ___                     AUTO ENABLE LMID(E/D): _

   ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.4.2.1 Fields

Field Name	Description
LMID	This name is the logical machine name or gateway ID. Give it a unique name up to 16 characters. Example: (bankmach1)
DNS	The host name that the domain name service recognizes.
HOST ADDRESS	The TCP/IP dot address. Example: (199.99.99.99)
PORT NUMBER	The TCP port. Check with the TCP/IP administrator for available ports. Example: (1234)
SECURITY	The status of connection-level security. Y specifies that security is on and N denotes that security is off.
	Note: For additional security information, refer to the "Configuring Oracle TMA TCP Security" section.
ACCOUNT ID	An eight-character ID. This ID must be the same ID that is used on the Oracle Tuxedo-side configuration. Coordinate with the Oracle Tuxedo Administrator. Required if there is an entry in the PASSWORD field. Example: (CICS001A)
PASSWORD	An eight-character password. This password must be the same as on the Oracle Tuxedo-side configuration. Coordinate with the Oracle Tuxedo Administrator. Required if there is an entry in the ACCOUNT ID field. Example: (LETMEIN2)
MAX QUEUE SIZE	Specifies the size of the local queue where requests are stored for servicing. A typical setting is 200.
MAX MSG SIZE	The largest message allowed to be sent across this connection. The maximum is 32000. Example: (4096)
RETRY LIMIT	If the connection fails, this number determines how many attempts the system makes to reestablish the connection before marking the connection disabled. Example: (5).
LMID TYPE	The type of gateway the remote system is running (C for CICS, I for IMS, T for TCP, X for Tuxedo Older versions (12.1.3 and earlier))
	Note: For additional information on LMID Type X, refer to the "Configuring Oracle TMA TCP Security" section. LMID Type X is invalid for TMA TCP Gateway 12.2.2 and the latest versions.
START TRANID	The ID of the transaction to be started if the remote system type is CICS.
CICS DATA	A string to be passed to the IBM TCP/IP Listener for use with the TMA TCP for CICS gateway. The default is " ".
MULTIPLEX CNT	The number of concurrent requests for each connection.
MIN TIME	The minimum length of time (in milliseconds) for a socket read to wait for data to be processed.

Field Name	Description
MAX TIME	The maximum length of time (in milliseconds) for a socket read to wait for data to be processed.
DELTA TIME	The time increase (in milliseconds) from MIN TIME to MAX TIME.
IDLE TIME	The amount of time in seconds that a connection is idle before it is closed. IDLE TIME must be a smaller amount of time than REQ IDLE TIME. A typical setting is 30 seconds.
REQ IDLE TIME	The amount of time in seconds that a Requester is idle before it terminates. A typical setting is 120 seconds.
LATENCY TIME	Network time and system processing time added to give a true system wait time (in seconds).
MAX CONNS	The maximum number of connections the Requester opens. The maximum value is 50 for IBM TCP/IP.
QUEUE NAME 1	The unique name of a TS Q that is used for communications between the Pre-requester and the Requester.
QUEUE NAME 2	The unique name of a TS Q that is used for communications between the Pre-requester and the Requester.
AUTO ENABLE LMID(E|D)	This field is used for auto enabling of LMID. Enter E to automatically enable a disabled Requester LMID for TMA TCP for CICS gateway. Enter D Kriito disable the automatic enabling of a disabled Requester LMID for TMA TCP for CICS gateway.

4.4.3 Update Requester Screen (R2)

Use this screen to update a record from the Requester file. The fields are the same as the ones on the Requester Insert screen, but on this screen you can change the values.

When the screen is first displayed, the LMID field is unprotected. Enter a logical machine name and press ENTER. The screen is re-displayed showing the data from the requested record. The HOST ADDRESS, PORT NUMBER, ACCOUNT ID, PASSWORD, MAX MSG SIZE, and CONNECT RETRY LIMIT fields are unprotected. The following message is displayed: RECORD READY FOR UPDATE.

After the changes you entered are validated and processed, the screen is re-displayed and the LMID field is unprotected.

```
 BEAPREQ                    ORACLE TMA TCP FOR CICS
BEAM     R2

                                UPDATE REQUESTER

 LMID:           ________________          MULTIPLEX_CNT:   __
 DNS: ____________________________________________________________________
 HOST ADDRESS: ________________
 PORT NUMBER: _____
                                           MIN TIME (MILLISEC): _____
 SECURITY(Y/N): _                          MAX TIME (MILLISEC): _____
 ACCOUNT ID: ________                      DELTA TIME (MILLISEC): _____
 PASSWORD:                                 IDLE TIME (SECONDS): _____
                                           REQ IDLE TIME (SECONDS): _____
 MAX QUEUE SIZE: _____                     LATENCY TIME (SECONDS): __
 MAX MSG SIZE: _____                       MAX CONNS: __
 RETRY LIMIT: _____
```

```
LMID TYPE: _                              QUEUE NAME 1: ________
START TRAN-ID: ____                       QUEUE NAME 2: ________
CICS DATA: ___                            AUTO ENABLE LMID(E/D): _

ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.4.3.1 Fields

Field Name	Description
LMID	This name is the logical machine name or gateway ID. Give it a unique name up to 16 characters. Example: (bankmach1)
DNS	The host name that the Domain Name Service recognizes.
HOST ADDRESS	The TCP/IP dot address. Example: (199.99.99.99)
PORT NUMBER	The TCP port. Check with the TCP/IP administrator for available ports. Example: (1234)
SECURITY	The status of security. Y specifies that security is on and N denotes that security is off.
	Note: For additional security information, refer to “Configuring Oracle TMA TCP Security”.
ACCOUNT ID	An eight-character ID for connection security. This ID must be the same ID that is used on the Oracle Tuxedo-side configuration. Coordinate with the Oracle Tuxedo Administrator. Required if there is an entry in the PASSWORD field. Example: (CICS001A)
PASSWORD	An eight-character password for connection security. This password must be the same as on the Oracle Tuxedo-side configuration. Coordinate with the Oracle Tuxedo Administrator. Required if there is an entry in the ACCOUNT ID field. Example: (LETMEIN1)
MAX QUEUE SIZE	Specifies the size of the local queue where requests are stored for servicing. A typical setting is 200.
MAX MSG SIZE	The largest message allowed to be sent across this connection. The maximum is 32000. Example: (4096)
RETRY LIMIT	If the connection fails, this number determines how many attempts the system makes to reestablish the connection before marking the connection disabled. Example: (5)

Field Name	Description
LMID TYPE	The type of gateway the remote system is running (C for CICS, I for IMS, T for Tuxedo)
START TRANID	The ID of the transaction to be started if the remote system type is CICS.
CICS DATA	A string to be passed to the IBM TCP/IP Listener for use with the TMA TCP for CICS gateway. The default is " ".
MULTIPLEX CNT	The number of concurrent requests for each connection.
MIN TIME	The minimum length of time (in milliseconds) for a socket read to wait for data to be processed.
MAX TIME	The maximum length of time (in milliseconds) for a socket read to wait for data to be processed.
DELTA TIME	The time increase (in milliseconds) from MIN TIME to MAX TIME.
IDLE TIME	The amount of time in seconds that a connection is idle before it is closed. IDLE TIME must be a smaller amount of time than REQ IDLE TIME. A typical setting is 30 seconds.
REQ IDLE TIME	The amount of time in seconds that a Requester is idle before it terminates. A typical setting is 120 seconds.
LATENCY TIME	Network time and system processing time added to give a true system wait time (in seconds).
MAX CONNS	The maximum number of connections the Requester opens. The maximum value is 50 for IBM TCP/IP.
QUEUE NAME 1	The unique name of a TS Q that is used for communications between the Pre-requester and the Requester.
QUEUE NAME 2	The unique name of a TS Q that is used for communications between the Pre-requester and the Requester.
AUTO ENABLE LMID(E|D)	Enter E to automatically enable a disabled Requester LMID for TMA TCP for CICS gateway. Enter D to disable the automatic enabling of a disabled Requester LMID for TMA TCP for CICS gateway.

4.4.4 Inquire Requester Screen (R3)

Use this screen to make an inquiry about a record from the Requester file. The screen is initially displayed with the LOGICAL MACHINE NAME field unprotected. Enter the logical machine name and press ENTER. The screen is re-displayed with the data from the requested record and the LOGICAL MACHINE NAME field is unprotected.

```
 BEAPREQ                  ORACLE TMA TCP FOR CICS
BEAM     R3

                           INQUIRE REQUESTER

 LMID: ________________                    MULTIPLEX_CNT: __
```

```
DNS: ____________________________________________________________
HOST ADDRESS: _______________
PORT NUMBER: _____
                                                MIN TIME (MILLISEC): _____
SECURITY(Y/N): _                                MAX TIME (MILLISEC): _____
ACCOUNT ID: ________                            DELTA TIME (MILLISEC): _____
PASSWORD:                                       IDLE TIME (SECONDS): _____
                                                REQ IDLE TIME (SECONDS): _____
MAX QUEUE SIZE: _____                           LATENCY TIME (SECONDS): __
MAX MSG SIZE: _____                             MAX CONNS: __
RETRY LIMIT: _____

LMID TYPE: _                                    QUEUE NAME 1: ________
START TRAN-ID: ____                             QUEUE NAME 2: ________
CICS DATA: ___                                  AUTO ENABLE LMID(E/D): _

ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.4.4.1 Fields

Field Name	Description
LMID	This name is the logical machine name or gateway ID. This name is a unique name up to 16 characters. Example: (bankmach1)
DNS	The host name that the domain Name Service recognizes.
HOST ADDRESS	The TCP/IP dot address. Example: (199.99.99.99)
PORT NUMBER	The TCP/IP port. Check with the TCP/IP administrator for available ports. Example: (1234)
SECURITY	The status of security. Y specifies that security is on and N denotes that security is off.
ACCOUNT ID	An eight-character ID. This ID must be the same ID that is used on the Oracle Tuxedo-side configuration. Coordinate with the Oracle Tuxedo Administrator. Required if there is an entry in the PASSWORD field. Example: (CICS001A)

> **Note:**
>
> For additional security information, refer to the "Configuring Oracle TMA TCP Security" section.

Field Name	Description
PASSWORD	An eight-character password. This password must be the same as the password used on the Oracle Tuxedo-side configuration. Coordinate with the Oracle Tuxedo Administrator. Required if there is an entry in the ACCOUNT ID field. Example: (LETMEIN1)
MAX QUEUE SIZE	Specifies the size of the local queue where requests are stored for servicing. A typical setting is 200.
MAX MSG SIZE	The largest message allowed to be sent across this connection. The maximum is 32000. Example: (4096)
RETRY LIMIT	If the connection fails, this number determines how many attempts the system makes to reestablish the connection before marking the connection disabled. Example: (5).
LMID TYPE	The type of gateway the remote system is running (C for CICS, I for IMS, T for Tuxedo)
START TRANID	The ID of the transaction to be started if the remote system type is CICS.
CICS DATA	A string to be passed to the IBM TCP/IP Listener for use with the TMA TCP for CICS gateway. The default is " ".
MULTIPLEX CNT	The number of concurrent requests for each connection.
MIN TIME	The minimum length of time (in milliseconds) for a socket read to wait for data to be processed.
MAX TIME	The maximum length of time (in milliseconds) for a socket read to wait for data to be processed.
DELTA TIME	The time increase (in milliseconds) from MIN TIME to MAX TIME.
IDLE TIME	The amount of time in seconds that a connection is idle before it is closed. IDLE TIME should be a smaller amount of time than REQ IDLE TIME. A typical setting is 30 seconds
REQ IDLE TIME	The amount of time in seconds that a Requester is idle before it terminates. A typical setting is 120 seconds.
LATENCY TIME	The amount of time in seconds that a Requester is idle before it terminates. A typical setting is 120 seconds.
MAX CONNS	The maximum number of connections the Requester opens. The maximum value is 50 for IBM TCP/IP.
QUEUE NAME 1	The unique name of a TS Q that is used for communications between the Pre-requester and the Requester.
QUEUE NAME 2	The unique name of a TS Q that is used for communications between the Pre-requester and the Requester.

Field Name	Description
AUTO ENABLE LMID(E|D)	Enter E to automatically enable a disabled Requester LMID for TMA TCP for CICS gateway. Enter D to disable the automatic enabling of a disabled Requester LMID for TMA TCP for CICS gateway.

4.4.5 Delete Requester Screen (R4)

Use this screen to delete a record from the Requester file.

Warning: Deleting a Requester record can have serious ramifications. Think carefully before performing this operation. If there are any Service records that point to this GWID, any client calls to those services are rejected because Oracle TMA does not know to which remote machine the request should go.

The screen is initially displayed with the LOGICAL MACHINE NAME field unprotected. Enter the logical machine name and press ENTER. The screen is then re-displayed with the data from the requested record and the LOGICAL MACHINE NAME field is protected. The following message is displayed: TO CONFIRM DELETE, PRESS ENTER AGAIN.

```
 BEAPREQ                      ORACLE TMA TCP FOR CICS
BEAM     R4

                                  DELETE REQUESTER

 LMID: ________________                          MULTIPLEX_CNT: __
 DNS: ____________________________________________________________
 HOST ADDRESS: ________________
 PORT NUMBER: _____
                                                 MIN TIME (MILLISEC): _____
 SECURITY(Y/N): _                                MAX TIME (MILLISEC): _____
 ACCOUNT ID: ________                            DELTA TIME (MILLISEC): _____
 PASSWORD:                                       IDLE TIME (SECONDS): _____
                                                 REQ IDLE TIME (SECONDS): _____
 MAX QUEUE SIZE: _____                           LATENCY TIME (SECONDS): __
 MAX MSG SIZE: _____                             MAX CONNS: __
 RETRY LIMIT: _____

 LMID TYPE: _                                    QUEUE NAME 1: ________
 START TRAN-ID: ____                             QUEUE NAME 2: ________
 CICS DATA: ___                                  AUTO ENABLE LMID(E/D): _

 ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.4.5.1 Fields

Field Name	Description
LMID	This name is the logical machine name or gateway ID. This name is a unique name up to 16 characters. Example: (bankmach1)
DNS	The host name that the domain Name Service recognizes.
HOST ADDRESS	The TCP/IP dot address. Example: (199.99.99.99)
PORT NUMBER	The TCP/IP port. Check with the TCP/IP administrator for available ports. Example: (1234)
SECURITY	The status of security. Y specifies that security is on and N denotes that security is off.
	Note: For additional security information, refer to the "Configuring Oracle TMA TCP Security" section.
ACCOUNT ID	An eight-character ID. This name must be the same ID that is used on the Oracle Tuxedo-side configuration. Coordinate with the Oracle Tuxedo Administrator. Required if there is an entry in the PASSWORD field. Example: (CICS001A)
PASSWORD	An eight-character password. This password must be the same as on the Oracle Tuxedo-side configuration. Coordinate with the Oracle Tuxedo Administrator. Required if there is an entry in the ACCOUNT ID field. Example: (LETMEIN1)
MAX QUEUE SIZE	Specifies the size of the local queue where requests are stored for servicing. A typical setting is 200.
MAX MSG SIZE	The largest message allowed to be sent across this connection. The maximum is 32000. Example: (4096)
RETRY LIMIT	If the connection fails, this number determines how many attempts the system makes to reestablish the connection before marking the connection disabled. Example: (5).
LMID TYPE	The type of gateway the remote system is running (C for CICS, I for IMS, T for Tuxedo)
START TRANID	The ID of the transaction to be started if the remote system type is CICS.
CICS DATA	A string to be passed to the IBM TCP/IP Listener for use with the TMA TCP for CICS gateway. The default is " ".

Field Name	Description
MULTIPLEX CNT	The number of concurrent requests for each connection.
MIN TIME	The minimum length of time (in milliseconds) for a socket read to wait for data to be processed.
MAX TIME	The maximum length of time (in milliseconds) for a socket read to wait for data to be processed.
DELTA TIME	The time increase (in milliseconds) from MIN TIME to MAX TIME.
IDLE TIME	The amount of time in seconds that a connection is idle before it is closed. IDLE TIME should be a smaller amount of time than REQ IDLE TIME. A typical setting is 30 seconds.
REQ IDLE TIME	The amount of time in seconds that a Requester is idle before it terminates. A typical setting is 120 seconds.
LATENCY TIME	Network time and system processing time added to give a true system wait time (in seconds).
MAX CONNS	The maximum number of connections the Requester opens. The maximum value is 50 for IBM TCP/IP.
QUEUE NAME 1	The unique name of a TS Q that is used for communications between the Pre-requester and the Requester.
QUEUE NAME 2	The unique name of a TS Q that is used for communications between the Pre-requester and the Requester.
AUTO ENABLE LMID(E|D)	Enter E to automatically enable a disabled Requester LMID for TMA TCP for CICS gateway. Enter D to disable the automatic enabling of a disabled Requester LMID for TMA TCP for CICS gateway

4.4.6 Browse Requester Screen (R5)

Use this screen to browse a list of the records in the Requester file. Additionally, you can select a record for further processing by entering a valid selection code in the first column of that record's row.

If you access this screen from the Main menu, the first record on file is displayed at the top of the screen. If you access this screen from the Insert, Update, Inquire, or Delete screens, the key received from that screen determines which records are displayed.

To choose a record, enter a valid selection code in the SEL CDE field next to that record. For example, to make an inquiry about a record, enter "3". If you enter more than one selection code, the first one is used and the others are ignored.

After the entry in the SEL CDE field is validated and processed, the screen for that process is displayed and the record key appears in the LOGICAL MACHINE NAME field.

```
BEAPREQ                    ORACLE TMA TCP FOR CICS
BEAM     R5

                                BROWSE REQUESTER
```

```
 SEL      LOGICAL MACHINE        HOST         PORT   MAXM   CONN   LMID
START
 CDE           NAME            ADDRESS       NUM    SIZE   R-LIM  TYPE
TRNID
 ---      ----------------   --------------- -----  -----  -----  ----
-----

 _        ________________   ________________ _____  _____  _____  _      ____
 _        ________________   ________________ _____  _____  _____  _      ____
 _        ________________   ________________ _____  _____  _____  _      ____
 _        ________________   ________________ _____  _____  _____  _      ____
 _        ________________   ________________ _____  _____  _____  _      ____
 _        ________________   ________________ _____  _____  _____  _      ____
 _        ________________   ________________ _____  _____  _____  _      ____
 _        ________________   ________________ _____  _____  _____  _      ____
 _        ________________   ________________ _____  _____  _____  _      ____
 _        ________________   ________________ _____  _____  _____  _      ____

 * SELCDE = (1: INS, 2: UPD, 3: INQ, 4: DEL)
 ENTER: PROCESS, PF3: MENU, PF7: PREV, PF8: NEXT
 RECORD NOT FOUND
```

4.5 The Outbound Service Information Screens

A service is a name associated with some component of work. That component of work might be a banking transaction, an airline flight reservation, or an order for a dozen widgets. In Oracle Tuxedo, a client program that needs work done makes a “service request.” A process called a server performs the work described in the service request on behalf of the client, then returns the results of its efforts back to the client. In MVS this process would be referred to as a call to a “black box.”

In a CICS application that uses TMA TCP for CICS, a service name is passed in the data area in an `EXEC CICS LINK` command and the results are returned in that same area. The service screens use the terms “service name” and “remote service name.” The service name (such as, `CIC01XXYYZZ`) is what the service is known as to your CICS environment and the remote service name (such as, `WITHDRAWL`) is what the service is known as to Oracle Tuxedo. For simplicity, you can make both names the same, but if naming conventions differ, you can use different names.

- PF Keys
- Insert Outbound Service Information Screen (S1)
- Update Outbound Service Information Screen (S2)
- Inquire Outbound Service Information Screen (S3)
- Delete Outbound Service Information Screen (S4)
- Browse Outbound Service Information Screen (S5)

4.5.1 PF Keys

The following table lists function keys available on various outbound service screens.

Function Key	Function
ENTER	Process the selection code entered
PF3	Transfer to Main menu
PF5	Transfer to Browse screen
PF7	Display the previous page of records
PF8	Display the next page of records

> **Note:**
>
> If you enter data and press PF3 or PF5 before pressing ENTER, the operation process is aborted and the appropriate screen is displayed.

4.5.2 Insert Outbound Service Information Screen (S1)

Use this screen to insert a record into the service name file. The screen is first displayed with all fields unprotected. Enter the required data in the appropriate fields and press ENTER. After the data is validated and processed, the screen is re-displayed and all the fields are unprotected.

```
BEAPSVC                     Oracle TMA TCP FOR CICS
BEAM       S1

                       INSERT OUTBOUND SERVICE INFORMATION


                          SERVICE NAME:

                          LOGICAL MACHINE NAME:

                          REMOTE SERVICE NAME:

                          SERVICE TIMEOUT(SEC):

                          SECURITY(Y/N):



 ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.5.2.1 Fields

Field Name	Description
SERVICE NAME	The service name as it is known to the CICS programmer.

Field Name	Description
LOGICAL MACHINE NAME	This name is a symbolic name as it was defined on the Requester Insert screen. It denotes the remote machine on which this service should be processed.
REMOTE SERVICE NAME	The name as it is known in the remote Oracle Tuxedo domain.
SERVICE TIMEOUT	The number of seconds to wait for timing out this service request.
SECURITY	The status of request-level security. Y specifies that security is on and N denotes that security is off.

4.5.3 Update Outbound Service Information Screen (S2)

Use this screen to update a record from the service name file. When the screen is first displayed, the SERVICE NAME field is unprotected. Enter the service name and press ENTER. The screen is then re-displayed with the data from the requested record and the LOGICAL MACHINE NAME, REMOTE SERVICE NAME, SERVICE TIMEOUT(SEC), and SECURITY fields are unprotected. The following message is displayed: RECORD READY FOR UPDATE.

After the changes are validated and processed, the screen is re-displayed and the SERVICE NAME field is unprotected.

```
 BEAPSVC                    ORACLE TMA TCP FOR CICS
BEAM        S2

                     UPDATE OUTBOUND SERVICE INFORMATION


                      SERVICE NAME:

                      LOGICAL MACHINE NAME:

                      REMOTE SERVICE NAME:

                      SERVICE TIMEOUT(SEC):

                      SECURITY(Y/N):




 ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.5.3.1 Fields

Field Name	Description
SERVICE NAME	The service name as it is known to the CICS programmer.
LOGICAL MACHINE NAME	This name is a symbolic name as it was defined on the Update Outbound Service Information screen. It denotes the remote machine on which this service should be processed.
REMOTE SERVICE NAME	The name as it is known in the remote Oracle Tuxedo domain.
SERVICE TIMEOUT	The number of seconds to wait for timing out this service request.
SECURITY	The status of security. Y specifies that security is on and N denotes that security is off.

4.5.4 Inquire Outbound Service Information Screen (S3)

Use this screen to make an inquiry about a record from the SERVICE NAME file. The screen is initially displayed with the SERVICE NAME field unprotected. Enter the service name and press ENTER. The screen is re-displayed with the data from the requested record and the SERVICE NAME field is unprotected.

```
BEAPSVC                    ORACLE TMA TCP FOR CICS
BEAM       S3

                       INQUIRE OUTBOUND SERVICE INFORMATION


                            SERVICE NAME:

                            LOGICAL MACHINE NAME:

                            REMOTE SERVICE NAME:

                            SERVICE TIMEOUT(SEC):

                            SECURITY(Y/N):




 ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.5.4.1 Fields

Field Name	Description
SERVICE NAME	The service name as it is known to the CICS programmer.
LOGICAL MACHINE NAME	This name is a symbolic name as it was defined on the Inquire Outbound Service Information screen. It denotes the remote machine on which this service should be processed.
REMOTE SERVICE NAME	The name as it is known in the remote Oracle Tuxedo domain.
SERVICE TIMEOUT	The number of seconds to wait for timing out this service request.
SECURITY	The status of security. Y specifies that security is on and N denotes that security is off.

4.5.5 Delete Outbound Service Information Screen (S4)

Use this screen to delete records from the service name file. The screen is initially displayed with the SERVICE NAME field unprotected. Type the service name and press ENTER. The screen is re-displayed with the data from the record requested and all the fields protected.

The following message is displayed: TO CONFIRM DELETE, PRESS ENTER: AGAIN. After you press enter to confirm the deletion, the screen is re-displayed and the SERVICE NAME field is unprotected.

```
BEAPSVC                          ORACLE TMA TCP FOR CICS
BEAM       S4

                              DELETE OUTBOUND SERVICE INFORMATION


                                 SERVICE NAME:

                                 LOGICAL MACHINE NAME:

                                 REMOTE SERVICE NAME:

                                 SERVICE TIMEOUT(SEC):

                                 SECURITY(Y/N):




 ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.5.5.1 Fields

Field Name	Description
SERVICE NAME	The service name as it is known to the CICS programmer.
LOGICAL MACHINE NAME	This name is a symbolic name as it was defined on the Delete Outbound Service Information screen. It denotes the remote machine on which this service must be processed.
REMOTE SERVICE NAME	The name as it is known in the remote Oracle Tuxedo domain.
SERVICE TIMEOUT	The number of seconds to wait for timing out this service request.
SECURITY	The status of security. Y specifies that security is on and N denotes that security is off.

4.5.6 Browse Outbound Service Information Screen (S5)

Use this screen to browse the records in the service name file. If you access this screen from the Main menu the first record on file is displayed at the top of the screen. If you access this screen from the Insert, Update, Inquire, or Delete screens, the list starts with the record key received from that screen.

To select a record for processing, enter a valid selection code. For example, to make an inquiry about a record, enter "3". If you enter more than one selection code, the first one is used, and the others are ignored. After the selection code is validated and processed, the screen for that process is displayed and the record key appears in the SERVICE NAME field.

```
BEAPSVC                    ORACLE TMA TCP FOR CICS
BEAM       S5

                                BROWSE SERVICE NAME


 SEL       SERVICE         LOGICAL MACHINE      REMOTE SERVICE      SERVICE
 CDE        NAME                 NAME                NAME
TIMEOUT        SEC
 ---    ----------------   ----------------     ----------------
-------        ---

 _      ________________   ________________     ________________
______          _
 _      ________________   ________________     ________________
______          _
 _      ________________   ________________     ________________
______          _
 _      ________________   ________________     ________________
______          _
 _      ________________   ________________     ________________
______          _
 _      ________________   ________________     ________________
______          _
 _      ________________   ________________     ________________
```

```
_____          _
 _     ________________    ________________    ________________
_____          _
 _     ________________    ________________    ________________
_____          _
 _     ________________    ________________    ________________
_____          _

 * SELCDE = (1 -INS, 2 -UPD, 3 -INQ, 4 -DEL)
ENTER: PROCESS, PF3: MENU, PF7: PREV, PF8: NEXT
RECORD NOT FOUND
```

4.6 The User Connection ACCOUNT Screens

A Handler is responsible for receiving service requests from the remote Oracle Tuxedo domain. The User Connection `ACCOUNT` screens allow for dynamic manipulation of accounts allowed to connect with a Handler when a Handler is configured with security enabled.

The security for user connection is obsolete and replaced by inner connection validation.

- PF Keys
- Insert User Connection ACCOUNT Screen (U1)
- Update User Connection ACCOUNT Screen (U2)
- Inquire User Connection ACCOUNT Screen (U3)
- Delete User Connection ACCOUNT Screen (U4)
- The Browse User Connection ACCOUNT Screen (U5)

4.6.1 PF Keys

The following table lists function keys available on various user account screens.

Function Key	Function
`ENTER`	Process the selection code entered
`PF3`	Transfer to Main menu
`PF5`	Transfer to Browse screen
`PF7`	Display the previous page of records
`PF8`	Display the next page of records

> **Note:**
>
> If you enter data and press `PF3` or `PF5` before pressing `ENTER`, the operation process is aborted and the appropriate screen is displayed.

4.6.2 Insert User Connection ACCOUNT Screen (U1)

Use this screen to add a new Connection `ACCOUNT` by inserting a new record into the user file.

When the screen is first displayed, all the fields are unprotected. Type the required data as described in the table below, then press ENTER. After the data is validated and processed, the screen is re-displayed and all the fields are unprotected.

```
BEAPUSR                    ORACLE TMA TCP FOR CICS
BEAM       U1

                        INSERT USER CONNECTION ACCOUNT



                             ACCOUNT:

                             PASSWORD:









 ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.6.2.1 Fields

Field Name	Description
ACCOUNT	An eight-character ID. This name must be the same ID that is used on the Oracle Tuxedo-side configuration. Coordinate with the Oracle Tuxedo Administrator. Required if there is an entry in the PASSWORD field. Example: (CICS001A)
PASSWORD	An eight-character password. This password must be the same as on the Oracle Tuxedo-side configuration. Coordinate with the Oracle Tuxedo Administrator. Required if there is an entry in the ACCOUNT ID field. Example: (LETMEIN1)

4.6.3 Update User Connection ACCOUNT Screen (U2)

Use this screen to update a record on the account file. When the screen is first displayed, the ACCOUNT field is unprotected. Enter the account ID, and press ENTER. The screen is then re-displayed with the data from the requested record and the PASSWORD field is unprotected. The following message is displayed: RECORD READY FOR UPDATE.

After the changes are validated and processed, the screen is re-displayed and the ACCOUNT field is unprotected.

```
 BEAPUSR                   ORACLE TMA TCP FOR CICS
BEAM       U2
                      UPDATE USER CONNECTION ACCOUNT
```

```
                                ACCOUNT:

                                PASSWORD:




 ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.6.3.1 Fields

Field Name	Description
ACCOUNT	An eight-character ID. This name must be the same ID that is used on the Oracle Tuxedo-side configuration. Coordinate with the Oracle Tuxedo Administrator. Required if there is an entry in the PASSWORD field. Example: (CICS001A)
PASSWORD	An eight-character password. This password must be the same as on the Oracle Tuxedo-side configuration. Coordinate with the Oracle Tuxedo Administrator. Required if there is an entry in the ACCOUNT ID field. Example: (LETMEIN1)

4.6.4 Inquire User Connection ACCOUNT Screen (U3)

Use this screen to make an inquiry about a record from the account file. The screen is initially displayed with the ACCOUNT field unprotected. Enter the ACCOUNT and press ENTER. The screen is re-displayed with the data from the requested record and the ACCOUNT field is unprotected.

```
 BEAPUSR                 ORACLE TMA TCP FOR CICS
BEAM      U3

                    INQUIRE USER CONNECTION ACCOUNT




                              ACCOUNT:

                             PASSWORD:
```

```
ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.6.4.1 Fields

Field Name	Description
ACCOUNT	An eight-character ID. This name must be the same ID that is used on the Oracle Tuxedo-side configuration. Coordinate with the Oracle Tuxedo Administrator. Required if there is an entry in the PASSWORD field. Example: (CICS001A)
PASSWORD	An eight-character password. This password must be the same as on the Oracle Tuxedo-side configuration. Coordinate with the Oracle Tuxedo Administrator. Required if there is an entry in the ACCOUNT ID field. Example: (LETMEIN1)

4.6.5 Delete User Connection ACCOUNT Screen (U4)

Use this screen to delete a record from the account file. The screen is initially displayed with the ACCOUNT field unprotected. Type the service name and press ENTER. The screen is re-displayed with the data from the record requested and all the fields protected.

The following message is displayed: TO CONFIRM DELETE, PRESS ENTER: AGAIN. After you press enter to confirm the deletion, the screen is re-displayed and the ACCOUNT field is unprotected.

```
 BEAPUSR                    ORACLE TMA TCP FOR CICS
BEAM       U4

                       DELETE USER CONNECTION ACCOUNT



                              ACCOUNT:

                             PASSWORD:









 ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.6.5.1 Fields

Field Name	Description
ACCOUNT	An eight-character ID. This name must be the same ID that is used on the Oracle Tuxedo-side configuration. Coordinate with the Oracle Tuxedo Administrator. Required if there is an entry in the PASSWORD field. Example: (CICS001A)
PASSWORD	An eight-character password. This password must be the same as on the Oracle Tuxedo-side configuration. Coordinate with the Oracle Tuxedo Administrator. Required if there is an entry in the ACCOUNT ID field. Example: (LETMEIN1)

4.6.6 The Browse User Connection ACCOUNT Screen (U5)

Use this screen to browse the records in the account file. If you access this screen from the Main menu the first record on file is displayed at the top of the screen. If you access this screen from the Insert, Update, Inquire, or Delete screens, the list starts with the record key received from that screen.

To select a record for processing, enter a valid selection code. For example, to make an inquiry about a record, enter "3". If you enter more than one selection code, the first one is used, and the others are ignored.

```
BEAPUSR                    ORACLE TMA TCP FOR
CICS                                        BEAM       U5

                         BROWSE USER CONNECTION

 SEL
 CDE          ACCOUNT
-----        ----------
  _           ________
  _           ________
  _           ________
  _           ________
  _           ________
  _           ________
  _           ________
  _           ________
  _           ________
  _           ________

  * SELCDE = (1: INS, 2: UPD, 3: INQ, 4: DEL)
    ENTER: PROCESS, PF3: MENU, PF7: PREV, PF8: NEXT
BEG/END OF FILE
```

4.7 The Inbound Service Information Screens

A service is a name associated with some component of work. That component of work can be a banking transaction, an airline flight reservation, or an order for a dozen widgets. In Oracle Tuxedo, a client program that needs work done makes a service request. A server performs the work described in the service request on behalf of the client, then returns the results of its efforts back to the client. In MVS this would be referred to as a call to a “black box.”

The service screens use the terms `LOCAL SERVICE NAME` and `REMOTE SERVICE NAME`. The `LOCAL SERVICE NAME` (such as, `CIC01XXYYZZ`) is what the service is known as to your CICS environment and the `REMOTE SERVICE NAME` (such as, `WITHDRAWL`) is what the service is known as to Oracle Tuxedo. For simplicity, you can make both names the same; however, different names can be used. Changes to the inbound service file are only picked up when the Handler is restarted.

4.7.1 PF Keys

The following table lists function keys available on various inbound service screens.

Function Key	Function
`ENTER`	Process the data entered
`PF3`	Transfer to Main menu
`PF5`	Transfer to Browse screen
`PF7`	Display the previous page of records
`PF8`	Display the next page of records

> **Note:**
>
> If you enter data and press `PF3` or `PF5` before pressing `ENTER`, the operation process is aborted and the appropriate screen is displayed.

4.7.2 Insert Inbound Service Information Screen (I1)

Use this screen to insert a record into the service name file. The screen is first displayed with all fields unprotected. Enter the required data in the following fields and press `ENTER`. After the data is validated and processed, the screen is re-displayed and all the fields are unprotected.

```
 BEAPISN                   ORACLE TMA TCP FOR CICS
BEAM       I1
```

```
                    INSERT INBOUND SERVICE INFORMATION


                    REMOTE SERVICE NAME:

                    LOCAL SERVICE NAME:

                    TRANSACTION NAME:

                    MAX MESSAGE SIZE:

                    SECURITY (Y/N):




 ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.7.2.1 Fields

Field Name	Description
REMOTE SERVICE NAME	The service name as it is known in the remote Oracle Tuxedo domain.
LOCAL SERVICE NAME	The service name as it is known to the CICS programmer

Field Name	Description
TRANSACTION NAME	The name of the CICS transaction that is started to process this service request. This transaction is usually the transaction for the Application Handler program which is BEAA by default. For information about programming services without a reply, refer to the “Programming Oracle Tuxedo Mainframe Adapter for TCP (CICS)” section. **Note:** Services sending requests using a tpacall with the TPNOREPLY flag set must have a unique TRANSACTION NAME associated with it. Do not use the TRANSACTION NAME for the Application Handler program or an error message results.
MAX MESSAGE SIZE	The largest message allowed to be sent across this connection. The maximum is 32000. This size is the size of the actual data; TMA TCP manages additional message size through its internal headers.
SECURITY	The status of security. Y enables security for the specified service and N disables security for the specified service

4.7.3 Update Inbound Service Information Screen (I2)

Use this screen to update a record in the inbound service name file. The screen is first displayed with the REMOTE SERVICE NAME field unprotected. Enter the remote service name and press ENTER. The screen is re-displayed with the data from the requested record and the LOCAL SERVICE NAME, TRANSACTION NAME, MAX MESSAGE SIZE, and SECURITY fields unprotected. The following message displays: RECORD READY FOR UPDATE.

After the changes are validated and processed, the screen is re-displayed and the REMOTE SERVICE NAME field is unprotected.

```
BEAPISN                    ORACLE TMA TCP FOR CICS
BEAM       I2

                      UPDATE INBOUND SERVICE INFORMATION
```

```
                    REMOTE SERVICE NAME:

                    LOCAL SERVICE NAME:

                    TRANSACTION NAME:

                    MAX MESSAGE SIZE:

                   SECURITY (Y/N):




 ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.7.3.1 Fields

Field Name	Description
REMOTE SERVICE NAME	The service name as it is known in the remote Oracle Tuxedo domain.
LOCAL SERVICE NAME	The service name as it is known to the CICS programmer.
TRANSACTION NAME	The name of the CICS transaction that is started to process this service request. This transaction is usually the transaction for the Application Handler program which is BEAA by default. For information about programming services without a reply, refer to the “Programming Oracle Tuxedo Mainframe Adapter for TCP (CICS)” section.

Note:

Services sending requests using a tpacall with the TPNOREPLY flag set must have a unique TRANSACTION NAME associated with it. Do not use the TRANSACTION NAME for the Application Handler program or an error message results

Field Name	Description
MAX MESSAGE SIZE	The largest message allowed to be sent across this connection. The maximum is 32000. This is the size of the actual data; TMA TCP manages additional message size through its internal headers.
SECURITY	The status of security. Y enables security for the specified service and N disables security for the specified service.

4.7.4 Inquire Inbound Service Information Screen (I3)

Use this screen to inquire about a record in the inbound service name file. The screen is first displayed with the REMOTE SERVICE NAME field unprotected. Enter the remote service name and press ENTER. The screen is re-displayed with the data from the requested record and the REMOTE SERVICE NAME field unprotected.

```
BEAPISN                          ORACLE TMA TCP FOR CICS
BEAM       I3

                               INQUIRE INBOUND SERVICE INFORMATION


                              REMOTE SERVICE NAME:

                              LOCAL SERVICE NAME:

                              TRANSACTION NAME:

                              MAX MESSAGE SIZE:

                              SECURITY (Y/N):




 ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.7.4.1 Fields

Field Name	Description
REMOTE SERVICE NAME	The service name as it is known in the remote Oracle Tuxedo domain.
LOCAL SERVICE NAME	The service name as it is known to the CICS programmer.

Field Name	Description
TRANSACTION NAME	The name of the CICS transaction that is started to process this service request. This transaction is usually the transaction for the Application Handler program which is BEAA by default. For information about programming services without a reply, refer to the “Programming Oracle Tuxedo Mainframe Adapter for TCP (CICS)” section.
	Note: Services sending requests using a tpacall with the TPNOREPLY flag set must have a unique TRANSACTION NAME associated with it. Do not use the TRANSACTION NAME for the Application Handler program or an error message results.
MAX MESSAGE SIZE	The largest message allowed to be sent across this connection. The maximum is 32000. This is the size of the actual data; TMA TCP manages additional message size through its internal headers.
SECURITY	The status of security. Y specifies that security is on and N denotes that security is off.

4.7.5 Delete Inbound Service Information Screen (I4)

Use this screen to delete a record in the inbound service name file. The screen is first displayed with the REMOTE SERVICE NAME field unprotected. Enter the remote service name and press ENTER. The screen is re-displayed with the data from the record requested and all fields protected. The following message displays: TO CONFIRM DELETE, PRESS ENTER AGAIN. After you press ENTER to confirm the deletion, the screen is re-displayed and the REMOTE SERVICE NAME field is unprotected.

```
 BEAPISN                        ORACLE TMA TCP FOR CICS
BEAM       I4

                              DELETE INBOUND SERVICE INFORMATION


                                 REMOTE SERVICE NAME:

                                 LOCAL SERVICE NAME:
```

```
                                    TRANSACTION NAME:

                                    MAX MESSAGE SIZE:

                                    SECURITY (Y/N):




ENTER: PROCESS, PF3: MENU, PF5: BROWSE
```

- Fields

4.7.5.1 Fields

Field Name	Description
REMOTE SERVICE NAME	The service name as it is known in the remote Oracle Tuxedo domain.
LOCAL SERVICE NAME	The service name as it is known to the CICS programmer.
TRANSACTION NAME	The name of the CICS transaction that is started to process this service request. This service request is usually the transaction for the Application Handler program. For information about programming services without a reply, refer to the “Programming Oracle Tuxedo Mainframe Adapter for TCP (CICS)” section. **WARNING:** Services sending requests using a tpacall with the TPNOREPLY flag set must have a unique TRANSACTION NAME associated with it. Do not use the TRANSACTION NAME for the Application Handler program or an error message results.
MAX MESSAGE SIZE	The largest message allowed to be sent across this connection. The maximum is 32000. This is the size of the actual data; TMA TCP manages additional message size through its internal headers.
SECURITY	The status of security. Y specifies that security is on and N denotes that security is off.

4.7.6 The Browse Inbound Service Screen (I5)

Use this screen to browse the records in the inbound service name file. If you access this screen from the Main menu, the first record on file is displayed at the top of the screen. If you access this screen from the Insert, Update, Inquire, or Delete screens, the list starts with the record key received from that screen.

To select a record for processing, enter a valid selection code. For example, to make an inquiry about a record, enter “3”. If you enter more than one selection code, the first one is used, and

the others are ignored. After the selection code is validated and processed, the screen for that process is displayed and the record key appears in the `REMOTE SERVICE NAME` field.

```
 BEAPISN                 ORACLE TMA TCP FOR CICS
BEAM       I5

                      BROWSE INBOUND SERVICE


 SEL    REMOTE SERVICE       LOCAL SERVICE     TRAN     MAXM
 CDE        NAME                 NAME          NAME     SIZE      SEC
 ---    ----------------    ----------------   ----     -----     ---

  _  ________________       ________________   ____     _____     _
  _  ________________       ________________   ____     _____     _
  _  ________________       ________________   ____     _____     _
  _  ________________       ________________   ____     _____     _
  _  ________________       ________________   ____     _____     _
  _  ________________       ________________   ____     _____     _
  _  ________________       ________________   ____     _____     _
  _  ________________       ________________   ____     _____     _
  _  ________________       ________________   ____     _____     _
  _  ________________       ________________   ____     _____     _

 * SELCDE = (1 -INS, 2 -UPD, 3 -INQ, 4 -DEL)
 ENTER: PROCESS, PF3: MENU, PF7: PREV, PF8: NEXT
 RECORD NOT FOUND
```

4.8 The Handler Configuration Screens

A Handler is responsible for receiving service requests from the remote Oracle Tuxedo domain. The Handler Configuration screens allow for dynamic manipulation of the configuration used by all Handler programs in the system.

> **Note:**
>
> To apply changes that have been made to the Handler Configuration file, you must restart the Handler.

- PF Keys
- Update Handler Configuration Screen (H2)
- Inquire Handler Configuration Screen (H3)

4.8.1 PF Keys

The following table lists the function keys available on various user account screens.

Function Key	Function
ENTER	Process the data entered
PF3	Transfer to Main menu

> **Note:**
>
> If you enter data and press `PF3` before pressing `ENTER`, the operation process is aborted and the appropriate screen is displayed.

4.8.2 Update Handler Configuration Screen (H2)

Use this screen to update the configuration record on the user file. If a record does not exist, one is inserted into the user file. When the screen first displays, all fields are unprotected. After the changes are validated and processed, the screen is re-displayed.

```
 BEAPUSR                      ORACLE TMA TCP FOR CICS
BEAM       H2

                           UPDATE HANDLER CONFIGURATION


                          SECURITY:                        Y

                          MULTIPLEX COUNT:                 99

                          MIN TIME (MILLISECS):            200

                          MAX TIME (MILLISECS):            300

                          DELTA TIME (MILLISECS):           5

                          IDLE TIME (SECONDS):              0



 ENTER: PROCESS, PF3: MENU
 UPDATE COMPLETED
```

- Fields

4.8.2.1 Fields

Field Name	Description
SECURITY	The status of gateway security. Y and C denotes that security is activated. N and F denotes that security is not activated. If this field is set to N or F, the ACCOUNT and PASSWORD fields are not verified prior to establishing a connection. For TMA TCP 12.2.2 Gateway and later, the security for connection validation is obsolete. Connection is established without validating ACCOUNT and PASSWORD, regardless of SECURITY flag.
MULTIPLEX CNT	The number of concurrent incoming service requests for each Handler.
MIN TIME	The minimum length of time (in milliseconds) for a socket read to wait for data to be processed.
MAX TIME	The maximum length of time (in milliseconds) for a socket read to wait for data to be processed.
DELTA TIME	The time increase (in milliseconds) from MIN TIME to MAX TIME.
IDLE TIME	The amount of time in seconds a Handler is idle before it terminates.

> **Note:**
>
> For additional information on Security, refer to the "Configuring Oracle TMA TCP Security" section.

4.8.3 Inquire Handler Configuration Screen (H3)

Use this screen to make an inquiry about the configuration record from the user file. The screen is displayed with the data from the requested record and all fields are protected.

```
BEAPUSR                    ORACLE TMA TCP FOR CICS
BEAM       H3

                        INQUIRE HANDLER CONFIGURATION


                    SECURITY:                      Y

                    MULTIPLEX COUNT:               99

                    MIN TIME (MILLISECS):          200
```

```
                                MAX TIME (MILLISECS):          300

                                DELTA TIME (MILLISECS):         5

                                IDLE TIME (SECONDS):            0



   ENTER: PROCESS, PF3: MENU
INQUIRE COMPLETED
```

- Fields

4.8.3.1 Fields

Field Name	Description
SECURITY	The status of gateway security. Y and C denotes that security is activated. N and F denotes that security is not activated. If this field is set to N or F, the ACCOUNT and PASSWORD fields are not verified prior to establishing a connection.
MULTIPLEX CNT	The number of concurrent incoming service requests for each Handler.
MIN TIME	The minimum length of time (in milliseconds) for a socket read to wait for data to be processed.
MAX TIME	The maximum length of time (in milliseconds) for a socket read to wait for data to be processed.
DELTA TIME	The time increase (in milliseconds) from MIN TIME to MAX TIME.
IDLE Time	The amount of time in seconds a program is idle before it terminates.

4.9 Dynamically Configuring TMA TCP for CICS

Dynamic configuration means that new configuration information affects currently running Handlers or Requesters without shutting them down. The new configuration information also affects Handlers and Requesters that are started after the information is entered. You can make the following changes to the TMA TCP for CICS gateway configuration dynamically.

All other configuration tasks are not dynamic, including Inbound Service Information and Handler Configuration. To process configuration information in these cases, the corresponding Requesters and Handlers must be shut down.

- Modifying Outbound Services
- Modifying User Connection Accounts
- Modifying Connections
- Deleting Requester LMIDs

4.9.1 Modifying Outbound Services

You can dynamically configure outbound services by inserting a new record into the service name file, modifying an existing record in the service name file, or deleting a record in the service name file. Use the appropriate maintenance screens to accomplish the necessary task, S1 to insert, S2 to update, or S4 to delete. For field definitions, refer to the The Outbound Service Information Screens section.

4.9.2 Modifying User Connection Accounts

You can dynamically configure User Connection Accounts and enable accounts to connect to Handlers by inserting a new account into the user account file, modifying an existing user account, or deleting a user account. Use the appropriate maintenance screens to accomplish the necessary task, U1 to insert, U2 to update, or U4 to delete. For field definitions, refer to theThe User Connection ACCOUNT Screens section.

> **Note:**
>
> Changes to the User Connection Accounts do not affect Handlers that are currently connected, but only Handlers that connect after the change is made. The changes for connection validation are obsolete.

4.9.3 Modifying Connections

You can dynamically configure the status of a connection. Using the Update Connection screen (C2), you can enable, disable, or abort the connection for a given `LMID`. Dynamically configuring the status of a connection has an immediate effect on the corresponding Requesters. For field definitions, refer to the The Connection Screens section.

> **Note:**
>
> Because the data in the Update Connection screen is transient, setting the `LMID` status to disable does not persist after the CICS region is shut down and then restarted. The Requester file, however, is persistent.

4.9.4 Deleting Requester LMIDs

Each instance of the Requester is given a logical machine name (`LMID`). You can give a Requester any unique `LMID` that is meaningful to you. Every service name is associated with one or more `LMID`s. This method allows the Requester to identify which remote machine is responsible for a particular service. You can dynamically delete an `LMID` using the Update Requester screen (R2). This dynamic change only affect Pre-requesters immediately.

> **Note:**
>
> Requesters that are currently running do not read the information in the requester file and are not affected by this dynamic change.

4.10 Administering the Gateways

Oracle Tuxedo has a set of `tmadmin` and `dmadmin` commands for the administration of the TMA TCP gateways. For detailed information about these commands, refer to the Oracle Tuxedo documentation.

5

Programming Oracle Tuxedo Mainframe Adapter for TCP (CICS)

The following subsections identify issues that CICS programmers should be aware of when they develop or modify application programs that operate with Oracle Tuxedo Mainframe Adapter for TCP (CICS) (hereafter referenced as TMA TCP for CICS):

- Client Application Considerations
- Server Application Considerations

5.1 Client Application Considerations

The following sections identify issues that CICS programers should be aware of when they develop or modify application programs that interoperate with TMA TCP for CICS as clients.

To make requests to remote Oracle Tuxedo domains from CICS application programs, use the `EXEC CICS LINK` command. The exact layout of the request/response data area is discussed in a later section.

- Buffer Layout Issues
- Making Calls from a CICS Client Program
- Error Handling

5.1.1 Buffer Layout Issues

The layout of the data buffer sent between CICS and Oracle Tuxedo should be agreed upon by the CICS applications programmer, the Oracle Tuxedo applications developer, and the Oracle Tuxedo administrator to ensure consistency and proper configuration. There are no limitations on the CICS programmer concerning native COBOL or C data types.

5.1.2 Making Calls from a CICS Client Program

To make a service call from a CICS program to a remote Oracle Tuxedo domain, make an `EXEC CICS LINK` call to the Pre-requester. The service you want to access must be configured by the Oracle TMA Administrator, but from a programming point of view the `LINK` call is all you need. The following COBOL record is in the COBOL copybook `client.cbl`.

Listing COBOL Record

```
01 REQUEST-RECORD.
    05 REQUEST-HEADER.
         10 DATALEN             PIC S9(08) COMP.
         10 SVCNAME[16]         PIC X(16).
         10 REQUESTCD           PIC S9(08) COMP.
         10 RETURNCD            PIC S9(08) COMP.
         10 REQRETURNCD         PIC S9(08) COMP.
```

```
    05 REQUEST-DATA.
         10 DATA-AREA           PIC X(DATALEN).
```

The layout of the structure in C that must be passed in the `LINK` call is shown in the listing. The following C structures are in the `clienth.h INCLUDE` file.

Listing C Structures

```
typedef struct CLIENTHDR
{
 long DataLen;              /* THE LEN OF THE DATA FROM AND TO APPL */
 char SvcName[16];          /* THE SERVICE NAME */
 long RequestCd;            /* THE REQUEST COMMAND FROM THE APPL */
 long ReturnCd;             /* THE RETURN CODE TO THE APPL */
 long ReqReturnCd;          /* THE RETURN CODE FROM THE PREQ AND REQ */
} CLIENTHDR;

typedef struct CMAREA
{
CLIENTHDR CltHdr;                       /*HEADER */
 char Request_data[MAX_DATA_LENGTH];  /* REQUEST DATA */
} CMAREA;
```

The variables in the previous COBOL and C examples are defined as follows.

DataLen
The length of the data in the `Request_data` field.

SvcName
The service request name (ask the administrator for the names).

RequestCd
A predefined numeric value that indicates the type of call this is.

BEA_REQUEST_NORESPONSE
Value is 7. A No Reply Service Request. In this case the request is sent over to Oracle Tuxedo for the service to be performed, but no response data is sent back.

BEA_REQUEST_RESPONSE
Value is 5. A Request/Response Request. A request is sent to Oracle Tuxedo and a response is expected back.

Code	Value
BEA-REQUEST-RESPONSE	+5.
BEA-REQUEST-NORESPONSE	+7.

ReturnCd
This code is the return code from the CICS Requester. All return codes are listed in the following table. Notify the administrator if any of the return codes indicate a processing or network problem.

> **Note:**
>
> For a complete description of these codes, refer to the Codes Returned to a CICS Client Program

Code	Value
BEA-NORMAL	+0
BEA-ERR-LENGTH	+1
BEA-ERR-MISSING-SRV-NAME	+2
BEA-ERR-REQ-CODE	+3
BEA-ERR-SRC-NOT-FOUND	+4
BEA-ERR-READ-UMT	+5
BEA-ERR-SERVER	+6
BEA-ERR-POST	+7
BEA-ERR-CANCEL	+8
BEA-ERR-WAIT	+9
BEA-ERR-LMID-NOT-FOUND	+10
BEA-ERR-START-TRANSID	+11
BEA-ERR-DISABLE-ACQUIRING	+12
BEA-ERR-DISABLE-NOT-FND	+13
BEA-ERR-DISABLE-NOT-RESPOND	+14
BEA-ERR-DISABLE	+15
BEA-ERR-ALLOC	+16
BEA-ERR-TIMEOUT	+17
BEA-ERR-TSQ	+18
BEA-ERR-SOCKET-FAILURE	+19
BEA-ERR-PROTOCOL	+20
BEA-ERR-QUEUE-OVERFLOW	+21

ReqReturnCd
This code is the return code from the Oracle Tuxedo Domain. See the Oracle Tuxedo documentation for a complete list of Tuxedo error codes.

Request_data
This area is the area where request data gets placed and in which your returned data arrives. The length depends on how long this particular service is configured. Check with the administrator for each service. The maximum value is 32000.

- Examples

5.1.2.1 Examples

The following sample is an example of a COBOL CICS client program.

Listing COBOL CICS Client Program Example

```
IDENTIFICATION DIVISION.
 PROGRAM-ID.     TESTCLN.
 ENVIRONMENT     DIVISION.
 CONFIGURATION SECTION.
 SOURCE-COMPUTER. IBM-3090.
 OBJECT-COMPUTER. IBM-3090.
 DATA DIVISION.
 WORKING-STORAGE SECTION.
 01 FILLER   PIC X(32) VALUE 'SAMPLE COBOL CICS CLIENT PROGRAM'.
 01 MSG-AREA.
 05 M-DATA             PIC X(42) VALUE SPACES.
 05 M-RCDE             PIC Z(05) VALUE ZEROS.
 01 WS-COMMAREA.
 05 WC-DATALEN         PIC S9(9) COMP-4.
 05 WC-SVCNAME         PIC X(16).
 05 WC-REQUESTCD       PIC S9(9) COMP-4.
 05 WC-RETURNCD        PIC S9(9) COMP-4.
 05 WC-REQRETURNCD     PIC S9(9) COMP-4.
 05 WC-REQDATA         PIC X(14).
 LINKAGE SECTION.
 01 DFHCOMMAREA        PIC X(14).
 PROCEDURE DIVISION.
 A100-ENTRY.
 MOVE +14                  TO WC-DATALEN.
 MOVE 'TOLOWER'            TO WC-SVCNAME.
 MOVE +5                   TO WC-REQUESTCD.
 MOVE 'THIS IS A TEST'     TO WC-REQDATA.
 EXEC CICS LINK PROGRAM('BEAPRERQ')
           COMMAREA(WS-COMMAREA)
           LENGTH(LENGTH OF WS-COMMAREA)
 END-EXEC.
 IF RETURNCD = 0
    MOVE 'SUCCESSFUL CALL, RETURN DATA IS IN WC-DATA'
      TO MSG-DATA
 ELSE
   MOVE 'PROCESS ERROR OCCURRED, RETURN CODE EQUAL '
     TO MSG-DATA
   MOVE RETURNCD TO M-RCDE
 END-IF.
 EXEC CICS SEND TEXT FROM(MSG-AREA) LENGTH(47)
           ERASE TERMINAL FREEKB CURSOR(0)
 END-EXEC.
 A200-EXIT.
     EXEC CICS RETURN END-EXEC.
```

The following is an example of a C CICS client program.

Listing C CICS Client Program Example

```
long resp, resp2;
unsigned short int lmsg;
struct CMAREA carea;
```

```
carea.CltHdr.DataLen = strlen(sendbuf);
memcpy(carea.CltHdr.SvcName, "ECHO", 4);
carea.CltHdr.RequestCd = BEA_REQUEST_RESPONSE;
memcpy(carea.Request_data, "This is a test", 14);
lmsg=sizeof(carea);
/* Use the name defined during installation */
EXEC CICS LINK PROGRAM("PREREQ")
                          COMMAREA(&carea)
                          LENGTH(lmsg) RESP(resp) RESP2(resp2);
if(carea.CltHdr.ReturnCd || carea.CltHdr.ReqReturnCd)
           process error;
else
           successful call, returned data is in Request_data;
```

> **Note:**
>
> C Programmers, do not include the NULL terminator on any strings. In the previous example, the `memxxx` calls were used instead of the `strxxx` calls. This example is typical when using C and CICS together. For more information see your *C for CICS* documentation.

5.1.3 Error Handling

You may encounter the following three types of errors while using TMA TCP for CICS:

- Gateway errors (communications problems)
- MVS or CICS errors
- Application errors

The following subsections explain how TMA TCP handles these different kinds of errors.

- Gateway Errors
- MVS or CICS Errors
- Application Errors

5.1.3.1 Gateway Errors

When local or remote gateway errors occur they are logged in the Oracle Tuxedo `ULOG` file on the remote Oracle Tuxedo node and in the `BEALOG` file (a TD Queue defined during installation) within the CICS region. All associated service requests fail and if the TMA gateways are able to communicate with each other, error messages are communicated between them.

5.1.3.2 MVS or CICS Errors

For requests originating in the Oracle Tuxedo domain, if the remote target system does not make it possible for TMA TCP for CICS to detect particular types of failure, the TMA TCP gateway (the Oracle Tuxedo domain) blocking time-out parameter can be tuned to provide timely detection of problems. This configuration parameter is set in the remote TMA TCP gateway system; discuss any changes you want to make with the administrator of that system.

Problems with requests that originate in the CICS region are also logged to the `BEALOG` file. Additionally, time-out periods for these requests can be tuned using the TMA TCP for CICS administration tool.

For more information about the blocking time-out parameter, refer to the *Oracle TMA TCP gateway User Guide*.

5.1.3.3 Application Errors

If an error occurs that makes the Handler unable to execute a certain program (such as, the program does not exist or is disabled) the Handler sends a message back to the TMA TCP gateway. If any other type of error occurs within an application program and the Handler is not notified of the problem, a time-out message is sent from the Handler back to the remote gateway.

For requests originating with CICS, Oracle Tuxedo returns information about specific problems, if possible. If there are network problems that prohibit the transmission of data, the request receives a timeout error.

5.2 Server Application Considerations

The following subsections identify issues that CICS programmers must be aware of when they develop or modify application programs that interoperate with TMA TCP for CICS as servers.

A CICS application program that processes requests originating from a remote Oracle Tuxedo domain is written like a CICS application program that is invoked with the `CICS LINK` command.

The CICS programs that work best for satisfying Oracle Tuxedo requests are the ones that perform a certain operation and return information to the caller. The CICS services requested by a Oracle Tuxedo client program must entail a single request/response scenario.

CICS service programs that are called from Oracle Tuxedo clients must be careful if they give up control, as when performing an `EXEC CICS XCTL` operation. To ensure that the response data is returned to the client, chaining programs must pass the original `COMMAREA` during the XCTL so that it may be `RETURN`ed to the TMA TCP for CICS Handler by the final program in the chain.

- Programming Services with a Response
- Programming Services without a Response
- Modifying the Length of the Return Message

5.2.1 Programming Services with a Response

Service programs expected to send a response to the client use the `EXEC CICS LINK` command to execute. The `COMMAREA` option contains a pointer to the raw data; therefore, no header is sent. As a result, the request data is available to the service programs in the `COMMAREA`.

5.2.2 Programming Services without a Response

Service programs that do not send replies back to the requester execute using transactions started by the `EXEC CICS START` command. The `FROM` option of this command contains a pointer to the raw data; therefore, no header is sent. As a result, such service programs must use an `EXEC CICS RETRIEVE` command with the `SET` option containing a pointer to the raw data.

> **Note:**
>
> Define a unique transaction for each service that does not send a reply and enter the name of that transaction in the `TRANSACTION NAME` field of the Inbound Service Information screen for the corresponding service.

An example of a service sending no reply is one requested by a client using a tpacall with the `TPNOREPLY` flag set.

5.2.3 Modifying the Length of the Return Message

You can manage the actual size of the return message the system sends over the gateway on a per request basis. This is different than simply limiting the message size for a particular service using the `MAX MESSAGE` field of the Inbound Service Information screen. To limit the size of the return message per request, the service program must `ADDRESS` the TWA using the copybook or the include file delivered in the `"YOURHLQ".BEATCPC.INCLUDE` file.

- Modifying Return Message Lengths for C Programs
- Modifying Return Message Lengths for COBOL Programs

5.2.3.1 Modifying Return Message Lengths for C Programs

To modify the return message length on a per request basis, specify the message length in the `rtnMsgSize` field in a `TWA_CONNECT` structure defined in the `TWAINCL` file.

5.2.3.2 Modifying Return Message Lengths for COBOL Programs

To modify the return message length on a per request basis, specify the message length in the `RTN-MSG-SIZE` field in a `TWA_CONNECT` record layout in the copybook `TWACOPY`.

A

Error and Informational Messages

The following topics describe TMA TCP for CICS messages:

A.1 Messages Returned to the Remote Gateway

Most of the messages produced from Oracle Tuxedo Mainframe for TCP (CICS) (hereafter referenced as TMA TCP for CICS) are sent back to the remote TMA TCP gateway and written to the `ULOG` on that system.

Message	Description
`ORACLE TMA / CICS server process initiated.`	The Handler process has been started.
`Welcome to ORACLE TMA TCP for CICS.`	The connect process has completed successfully.
`Goodbye.`	The disconnect process has completed successfully.
`Service` *svcname* `not found.`	The requested service was not found in the inbound service name file.
`Client has already logged in.`	A client process has attempted to establish a connection when a connection already existed. (The connection request protocol was resent.)
`Client has not logged in.`	A client process has made a request to the TMA TCP for CICS gateway but has not yet established a login connection. (The connection request protocol was never sent.)
`ORACLE TMA / CICS server is active.`	This message is returned to the remote Tuxedo gateway when a PING request is sent to the TMA TCP for CICS gateway from the tmadmin administration tool.
`Invalid password.`	The password specified in the TMA TCP gateway configuration file does not match the password specified when the CICS supplied listener was configured.
`Invalid client account.`	The account code specified in the TMA TCP gateway configuration file does not match the account code specified when the CICS supplied listener was configured.
`Sorry-System Resource is protected by CICS.`	The mode command was executed through the tmadmin tool on Tuxedo and the administrative request specified is not available in the CICS region.
`Data too long, please check message header.`	A message received is larger than the maximum allowable message length.

Message	Description
`Data too short, please check message header.`	A message was received and was smaller than the smallest expected message.
`Message header is incorrect.`	An invalid protocol header was received. This can occur if there was a transmission error or if a message was sent to the gateway without having gone through the TMA TCP gateway on the remote Tuxedo node.
`This transaction is not defined in CICS.`	A CICS transaction code was mapped to a service name in the TMA TCP gateway configuration file for a transaction code that is unknown to CICS.
`Application Handler abnormally terminated.`	The Application Handler terminated prior to completing the service request. This message usually occurs when a service has timed out. Verify that you are not expecting a reply from a service that does not send one.
`Requested Service timed out.`	The requested service did not complete within the time provided in the message header from the remote Tuxedo gateway.
`Unable to start another session.`	The Handler is already processing the maximum number of service requests configured as the multiplex count.
`Unable to start transaction.`	A CICS error occurred attempting to start the transaction.
`Error occurred in Application Handler.`	The Application Handler encountered a CICS error.
`Security error occurred in Application Handler.`	The Application Handler encountered a CICS security error.

A.2 Messages Written to the TMA TCP for CICS Log

Occasionally, messages are written directly to the CICS log configured specifically for TMA TCP for CICS. For more information about configuring the CICS log, refer to the Configuring and Administering Oracle TMA TCP for CICS section.

Message	Description
`Goodbye.`	The disconnect process has completed successfully.
`Service` *`svcname`* `not found.`	The requested service was not found in the inbound service name file
`Client has already logged in.`	A client process has attempted to establish a connection when a connection already existed. (The connection request protocol was resent.)
`Client has not logged in.`	A client process has made a request to the TMA TCP for CICS gateway but has not yet established a login connection. (The connection request protocol was never sent.)
`Invalid password.`	The password specified in the TMA TCP gateway configuration file does not match the password specified when the CICS supplied listener was configured.
`Invalid client account.`	The account code specified in the TMA TCP gateway configuration file does not match the account code specified when the CICS supplied listener was configured.
`Data too long, please check message header.`	A message received is larger than the maximum allowable message length.

Message	Description
`Application Handler abnormally terminated.`	The Application Handler terminated prior to completing the service request. This message usually occurs when a service has timed out. Verify that you are not expecting a reply from a service that does not send one.
`Requested Service timed out.`	The requested service did not complete within the time provided in the message header from the remote Tuxedo gateway.
`Unable to start another session.`	The Handler is already processing the maximum number of service requests configured as the multiplex count.
`Unable to start transaction.`	A CICS error occurred attempting to start the transaction.
`Error occurred in Application Handler.`	The Application Handler encountered a CICS error.
`Security error occurred in Application Handler.`	The Application Handler encountered a CICS security error.
`DNS Lookup Failed for HOST(host) ERRNO(errno)`	The DNS lookup function failed for the given host name.
`Dotted IP address (address) malformed.`	There was an erroneous IP address passed into the `ConvertAddress` function.
`Invalid data pointer (pointer).`	There was an invalid data buffer pointer passed into the `BufferHeader` function.
`Socket CONNECT Failed. ERRNO=errno`	The Socket `CONNECT` function failed.
`fcntl(F_SETFL) Failed. ERRNO=errno FLAGS=hexcode`	The file control function with the `F_SETFL` option failed in the connect socket function.
`fcntl (F_GETFL) Failed. ERRNO=errno`	The file control function with the `F_GETFL` option failed in the connect socket function.
`Socket CREATE Failed. ERRNO=errno`	The Socket `CREATE` function failed.
`WRITE on Socket Failed. ERRNO=errno`	The Socket `WRITE` function failed
`initapi Failed. ERRNO=errno`	The Socket initialization function failed.
`RETRIEVE Failed. RESP=hexcode RESP2=hexcode`	The `CICS RETRIEVE` command failed when it tried to access the buffer passed to the TMA TCP gateway Handler from the Sockets for CICS Listener.
`Load Control Failed. RESP=hexcode RESP2=hexcode`	A `CICS LOAD PROGRAM` command failed. The Handler was unable to load the control programs `OTPCICS01` or `OTPCICS02`.
`Start Task Failed. RESP=hexcode RESP2=hexcode`	A CICS `START` command failed when the Handler tried to issue a `START` on the specified user program.
`Link Program Failed. RESP=hexcode RESP2=hexcode`	A CICS `LINK` command failed. The Handler was unable to `LINK` to the specified user program.
`GETMAIN Failed. RESP=hexcode RESP2=hexcode`	The CICS `GETMAIN` command failed.
`Take Socket Failed. ERRNO=errno`	The TMA TCP Handler was unable to take control of the TCP/IP socket.
`Error on Select. ERRNO=errno`	The Sockets `SELECT` function failed.
`Read on Socket Failed. ERRNO=errno`	An error was encountered while attempting to read from the active socket.

Message	Description
`Socket SEND Failed. RC=rc ERRNO=errno`	An error was encountered while issuing a send over the active socket.
`Handler connected successfully.`	The client request is allowed because the account and password codes are authorized to use the TMA TCP gateway.
`ORACLE TMA TCP Server CTOS is shutting down.`	The TMA TCP gateway Handler is shutting down.
`Verifying User Account.`	The Handler is verifying that the account and password codes supplied by TMA TCP gateway on the remote Tuxedo gateway are valid.
`Handler initialization complete.`	The TMA TCP Handler has successfully initialized.
`Normal shutdown requested, x requests pending.`	The TMA TCP Handler shuts down after the currently pending requests complete.
`Handler exceeded maximum idle time.`	The TMA TCPHandler has exceeded the configured `IDLE TIME`.
`ORACLE TMA Handler is shutting down.`	The TMA TCP Handler is shutting down.
`Client disconnected.`	The client has been disconnected from the TMA TCP Handler.
`Read of file failed, resp(hexcode)`	A CICS `READ` command failed.
`Freemain did not work, resp(hexcode)`	A CICS `FREEMAIN` command failed.
`Getmain shared failed: resp(hexcode)`	A CICS `GETMAIN(SHARED)` command failed.
`Delete from file failed, resp(hexcode)`	A CICS `DELETE` command failed
`Write to file failed, resp(hexcode)`	A CICS `WRITE` command failed.
`Rewrite of file failed, resp(hexcode)`	A CICS `REWRITE` command failed.
`Read(update) of file failed, resp(hexcode)`	A CICS `READ(UPDATE)` command failed.
`Unauthorized Client Rejected.`	The client request are not allowed because the account and/or password codes are not authorized.
`deleteq ts did not work, resp(hexcode)`	A CICS `DELETEQ TS` command failed.
`Unable to start transaction`	A CICS error occurred attempting to start the transaction
`Security Violation: Invalid user for this transaction`	The user ID sent with a request by the client does not match the user ID set in the mainframe security for this transaction.
`The Handler is designed to run in the background.`	A user has attempted to start the Handler from a terminal.
`The appHandler is designed to run in the background.`	A user, from a terminal, has attempted to start the transaction that initiates the Application Handler.
`App Handler received corrupted header, exiting.`	The Application Handler is terminating on initialization because there is a problem with the header it received. This would occur, for example, if the transaction for the Application Handler was given in the Inbound Service Information screen as the transaction to start a service with no reply.

Message	Description
opcode is not CONNECT on connection.	The Requester has received a reply that should be the acknowledgment of a connection request; however, the message does not contain the correct opcode.
Trying connection, but already connected.	The Requester has received a reply containing an opcode indicating a response to a connection request; however, the connection already exists.
Read on sockets failed. Connection closed by other side.	The Handler terminated because the socket status indicated that the client side had closed the connection.
LMID is disabled. Auto enabling LMID , LMID name>	The pre-requester is dynamically enabling an LMID which is disabled. This message will be displayed only when the AUTO ENABLE option is set to E.

A.3 Codes Returned to a CICS Client Program

The following codes are returned to a CICS client program on return from a LINK to TMA TCP. For system level problems, please notify your CICS administrator.

Message	Description
BEA_NORMAL	Value 0 Successful Return From Service Call.
BEA_ERR_LENGTH	Value 1 There was an error regarding the length of the message sent or the length value specified.
BEA_ERR_MISSING_SRV_NAME	Value 2 A service request was made but no service name was provided.
BEA_ERR_REQ_CODE	Value 3 A service call was made with an invalid or missing request code.
BEA_ERR_SRC_NOT_FOUND	Value 4 The service that was called cannot be found in the outbound service table.
BEA_ERR_READ_UMT	Value 5 Check the FCT entry for the CONNECTIONS dataset.
BEA_ERR_SERVER	Value 6 There was a problem accessing the Requester. Check that it is enabled.
BEA_ERR_POST	Value 7 A CICS Post error occurred in TMA TCP.
BEA_ERR_CANCEL	Value 8 A CICS Cancel error occurred in TMA TCP.
BEA_ERR_WAIT	Value 9 A CICS Wait error occurred in TMA TCP.
BEA_ERR_LMID_NOT_FOUND	Value 10 The service name provided specified a non-existent LMID
BEA_ERR_START_TRANSID	Value 11 A CICS START error occurred in TMA TCP.
BEA_ERR_DISABLE_ACQUIRING	Value 12 There was a problem getting an LMID to use for this service request.
BEA_ERR_DISABLE_NOT_FND	Value 13 The service name provided specifies an invalid LMID or is missing the LMID
BEA_ERR_DISABLE_NOT_RESPOND	Value 14 The Requester for handling this service name is not responding.
BEA_ERR_DISABLE	Value 15 The LMID associated with the requested service is not enabled.
BEA_ERR_ALLOC	Value 16 The Pre-requester was unable to allocate the memory necessary to process a request.

Message	Description
BEA_ERR_TIMEOUT	Value 17 The Pre-requester has timed out the request. This could occur either during processing by the Pre-requester, before the request is sent, or because the Pre-requester did not receive a response in time.
BEA_ERR_TSQ	Value 18 The Pre-requester was unable to write the request to the appropriate TS queue.
BEA_ERR_SOCKET_FAILURE	Value 19 The Requester closed a socket because the socket was in a state inconsistent with the requested operation.
BEA_ERR_PROTOCOL	Value 20 The Requester closed a socket because the session data was corrupt.
BEA_ERR_QUEUE_OVERFLOW	Value 21 The Requester has aborted a request because the pending request queue for the Requester is too full.

A.4 Informational Process Messages

Message	Description	Action
"RECORD READY FOR UPDATE"	The record selected is ready to be updated.	Make the changes and press ENTER to process.
"UPDATE COMPLETED"	The changes made to the record selected for update have been processed.	Select another record to update, or press PF3 or PF5.
"TO CONFIRM DELETE, PRESS ENTER:AGAIN"	The record selected is ready to be deleted.	Press ENTER to delete the selected record of press PF3 or PF5 to abort the delete.
"DELETE COMPLETED"	The record selected for delete has been deleted.	Select another record to delete, or press PF3 or PF5.
"INQUIRE COMPLETED"	The record selected for inquiry has been processed.	Select another record to inquiry, or press PF3 or PF5.
"INSERT COMPLETED"	The record entered has been inserted into the file.	Enter another record, or press PF3 or PF5.

A.5 Data Field Error Messages

Message	Description	Action
"INVALID FUNCTION KEY, OPTIONS=(ENTER: ,PF3:)"	The PFKey pressed is not valid in this operation	Press a valid PFKey. See OPTIONS=.
"INVALID FUNCTION KEY, OPTIONS=(ENTER: , PF3:,PF5:)"	The PFKey pressed is not valid in this operation.	Press a valid PFKey. See OPTIONS=.

Message	Description	Action
"INVALID FUNCTION KEY, OPTIONS=(ENTER:, PF3:, PF7:,PF8:)"	The PFKey pressed is not valid in this operation.	Press a valid PFKey. See OPTIONS=.
"INVALID LOGICAL MACHINE NAME"	The LOGICAL MACHINE NAME entered is not valid.	Enter a valid INVALID LOGICAL MACHINE NAME (i.e., LMIDNJ). Must not start with a space, null, or underscore.
"INVALID HOST ADDRESS"	The HOST ADDRESS entered is not valid	Enter a valid HOST ADDRESS (i.e., 1234.1234.99).Must not start with a space, null, or underscore.
"HOST ADDRESS or DNS NAME REQUIRED"	Neither the HOST ADDRESS nor the DNS NAME have been entered.	Enter either a valid HOST ADDRESS or DNS NAME.
"CANNOT HAVE BOTH HOST ADDRESS AND DNS NAME"	Both HOST ADDRESS and DNS NAME have been entered.	Enter either a valid HOST ADDRESS or DNS NAME.
"INVALID MULTIPLEX COUNT OPTIONS=(1-99)"	The MULTIPLEX COUNT entered is not valid.	Enter a valid number for MULTIPLEX COUNT.
"INVALID MAX CONNECTIONS OPTIONS=(1-99)"	The MAX CONNECTIONS entered is not valid.	Enter a valid number for MAX CONNECTIONS.
"TRAN CODE INVALID FOR LMID TYPE (I IMS, T TCP)"	A START TRAN CODE has been entered and the LMID TYPE is not CICS.	Remove the START TRAN CODE or change the LMID TYPE to CICS.
"QUEUE NAME REQUIRED"	The QUEUE NAME has not been entered.	Enter a valid QUEUE NAME.
"CICS DATA INVALID FOR LMID TYPE (I IMS, T TCP)"	CICS DATA has been entered and the LMID TYPE is not CICS.	Remove the CICS DATA or change the LMID TYPE to CICS.
"INVALID PORT NUMBER OPTIONS=(1 -> 65,535)"	The PORT NUMBER entered is not valid.	Enter a valid PORT NUMBER (i.e., 1234).Must not start with a space, null, or underscore and must be within the range (1 -> 65,535)
"ACCOUNT ID REQUIRED"	An ACCOUNT ID is required if you entered a PASSWORD.	Enter an ACCOUNT or erase the PASSWORD.
"PASSWORD REQUIRED"	A PASSWORD is required if you entered an ACCOUNT ID.	Enter a PASWORD or erase the ACCOUNT ID.
"INVALID MAX MSG SIZE OPTIONS=(1 -> 32000)"	The MAX MSG SIZE entered is not valid.	Enter a valid MAX MSG SIZE (i.e., 4096) Must not start with a space, null, or underscore and must be within the range (1 -> 32000)
"INVALID CONNECT RETRY LIMIT"	The CONNECT RETRY LIMIT entered is not valid.	Enter a valid CONNECT RETRY LIMIT (i.e., 10) Must not start with a space, null, or underscore.

Message	Description	Action
"INVALID SELCDE, OPTIONS= (1: INS, 2: UPD, 3: INQ, 4: DEL)	The SELCDE entered is not valid.	Enter a valid SELCDE. See OPTIONS=.
"INVALID SELCDE, OPTIONS= (2: UPD, 3: INQ)	The SELCDE entered is not valid.	Enter a valid SELCDE. See OPTIONS=.
"INVALID SELECTION, OPTIONS=(C2-3, C5, R1-5, S1-5, U2-3, I1-5)"	The SELECTION entered is not valid.	Enter a valid SELECTION. See the list of valid options in the message.
"INVALID SERVICE NAME"	The SERVICE NAME entered is not valid.	Enter a valid SERVICE NAME. (i.e., EMPLSRV) Must not start with a space, null, or underscore.
"INVALID REMOTE SERVICE NAME"	The REMOTE SERVICE NAME entered is not valid.	Enter a valid REMOTE SERVICE NAME (i.e., EMPLSRV) Must not start with a space, null, or underscore
"INVALID LMID TYPE OPTIONS= (C CICS, I IMS, T TCP)"	The LMID TYPE entered is not valid.	Enter a valid LMID TYPE. See Options
"START TRAN CODE REQUIRED FOR LMID TYPE (C CICS)"	No START TRAN CODE has been entered and the LMID TYPE is CICS.	Enter a valid START TRAN CODE
"INVALID TYPE (I INCOMING, O OUTGOING)"	The TYPE entered is not valid.	Enter a valid TYPE.
"INVALID SECURITY FLAG (Y/N)"	The SECURITY FLAG entered is not valid.	Enter a valid SECURITY FLAG (Y or N).
"INVALID SERVICE TIMEOUT(SEC)"	The SERVICE TIMEOUT(SEC) entered is not valid.	Enter a valid SERVICE TIMEOUT(SEC) (i.e. 30). Must not start with a space, null, or underscore.
"INVALID STATUS OPTIONS=(E ENABLE, D DISABLE, A ABORT)"	The STATUS entered is not valid.	Enter a valid STATUS. See OPTIONS=.
"INVALID OPTION= (E ENABLE, D DISABLE)"	The AUTO ENABLE LMID (E|D) option entered is not valid or is empty.	Enter a valid option (E or D).
"NO CHANGE DONE STATUS ENTERED SAME AS ON RECORD"	The STATUS on the record is 'E' and you entered an 'E'. The STATUS on the record is 'D' and you entered a 'D'. The STATUS on the record is 'A' and you entered a 'A'	Enter the appropriate STATUS.

Message	Description	Action
"BEA_REQ_HDR RECORD NOT FOUND"	An error occurred within the Connection CSA.	Contact your system administrator.

A.6 System Error Messages

Message	Description	Action
"BEG/END OF FILE"	The end of file was detected during a browse.	None
"DUPLICATE RECORD"	The record being inserted is already on the file.	Use a different record key.
"FILE NOT OPENED"	The file is not available to CICS.	Contact your system administrator. Check the file status via CEMT.
"DSIDERR"	Refer to the CICS Application Reference Manual.	Contact your system administrator.
"ILLOGIC"	Refer to the CICS Application Reference Manual.	Contact your system administrator.
"INVREQ"	Refer to the CICS Application Reference Manual.	Contact your system administrator.
"IOERR"	Refer to the CICS Application Reference Manual.	Contact your system administrator.
"LENGERR"	Refer to the CICS Application Reference Manual.	Contact your system administrator.
"MAPFAIL"	Refer to the CICS Application Reference Manual.	Contact your system administrator. Check the Mapset status via CEMT.
"NOSPACE"	Refer to the CICS Application Reference Manual.	Contact your system administrator.
"NOTAUTH"	Refer to the CICS Application Reference Manual.	Contact your system administrator.
"PGMIDERR"	Refer to the CICS Application Reference Manual.	Contact your system administrator. Check the Program status via CEMT.
"RECORD NOT FOUND"	The record selected is not in the file.	Verify the data you entered for the record key.
"SYSIDERR"	Refer to the CICS Application Reference Manual.	Contact your system administrator.
"UNKNOWN ERROR"	Refer to the CICS Application Reference Manual.	Contact your system administrator.