CICS® Universal Client Configuration

Configuring CICS Universal Client for Solaris® for SNA (SunLink SNA/PTP)

CICS® Universal Client Configuration

Configuring CICS Universal Client for Solaris® for SNA (SunLink SNA/PTP)

Contents

Chapter 1. Overview

The sample configuration shown in Figure 1 consists of a CICS Universal Client for Solaris Version 3.1 connecting to CICS Transaction Server for OS/390. Communication is through SNA LU6.2 (APPC) communication, provided by SunLink SNA/PTP Version 9.1 on the client workstation and VTAM on the mainframe server.

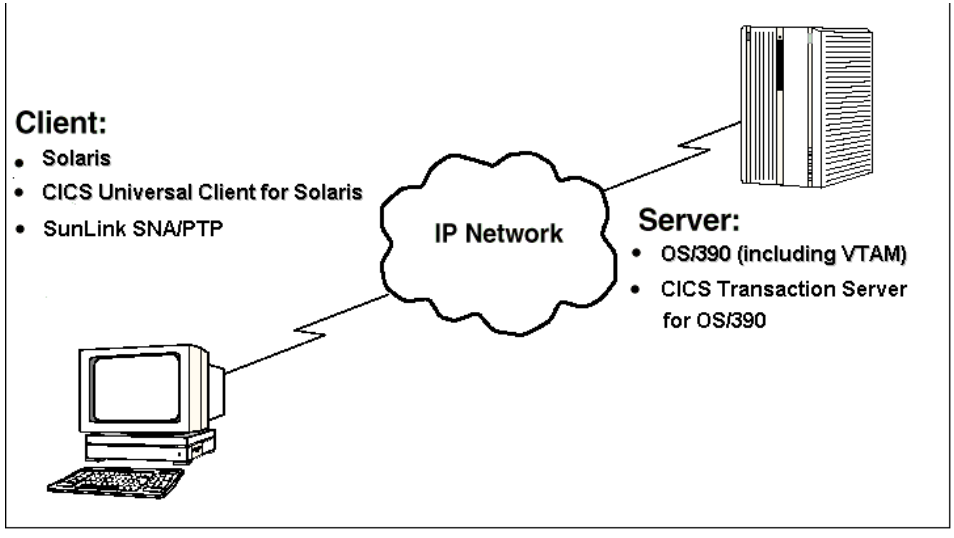

Figure 1. CICS Universal Client for Solaris connected to CICS TS Version 1.3

Although we used the CICS Transaction Server for OS/390 Version 1.3 for the sample configuration, you could use earlier versions of the CICS Transaction Server for OS/390, or CICS/ESA Version 4.1.

We used a token-ring network for this configuration, but you can use other physical links, for example, synchronous data link control (SDLC) or coaxial connections.

In this document we cover the following topics:

Chapter 2. Software checklist

The levels of software we used in the sample configuration are not necessarily the latest levels available. Check the relevant products for levels of compatible software.

We used the following software on the CICS server:

- OS/390 Version 2.6
  - Includes VTAM Version 4.5
- CICS Transaction Server for OS/390 Version 1.3

We used the following software on the client workstation:

- Solaris Version 2.6
- SunLink SNA/PTP Version 9.1, plus the Recommended Patch Cluster for Solaris 2.6
- CICS Universal Client for Solaris Version 3.1
- Java Runtime Environment (JRE) Version 1.1.7 for Solaris (necessary for running the configuration tool and other tools.)

Software checklist

Chapter 3. Definitions checklist

Before you configure the products, we recommend that you acquire definitions for the parameters listed below. Reference keys, for example, **1** are assigned to definitions that must contain the same value in more than one product.

- VTAM
  - NETID **1**
  - PU
  - LU **2**
  - XID
  - APPL **3**
  - LogMode **4**
- CICS Transaction Server for OS/390
  - ISC SIT override
  - APPLID **3**
  - DFHISC group
  - Netname in the LU6.2 connection definition **2**
  - Modename in the LU6.2 sessions definition **4**
- SunLink SNA/PTP
  - Hostname of local machine
  - Local MAC Address
  - Remote MAC Address
  - Partner network ID **1**
  - Partner LU name **3**
  - Local LU name **2**
  - Mode name **4**
- CICS Universal Client for Solaris Version 3.1
  - Partner LU Alias Name
  - Local LU name **2**
  - Mode name **4**

Definitions checklist

Chapter 4. Matching definitions

In the sample configuration a number of definitions must match. Table 1 shows the definitions that must be the same. The Example column shows the values we used in our configuration (see “Chapter 5. Sample configuration” on page 9).

Table 1. Matching Definitions

Ref: Key	VTAM	CICS Transaction Server	SunLink SNA/PTP	Client configuration	Example
1	NETID	—	First part of fully qualified partner LU name	—	GBIBMIYA
2	LU	Netname	LU Name	Local LU name	SC02130I
3	APPL	APPLID	Second part of fully qualified partner LU name	—	IYCQCTS5
4	LogMode	Modename	Mode name	Mode name	LU62PS

Matching definitions

Chapter 5. Sample configuration

In this section we present examples of each of the definitions mentioned in “Chapter 3. Definitions checklist” on page 5. The values highlighted in the figures refer to the Example column of Table 1 on page 7.

VTAM

In this section we present the VTAM definitions required for accessing the server across the network.

NETID

Define the NETID **1** for your network node in the VTAM start command for your VTAM system. Figure 2 shows the NETID we used in our sample configuration.

```
      :::
NETID=GBIBMIYA, 1
      :::
```

Figure 2. VTAM: NETID definition

PU, XID, and LU

Figure 3 shows the VTAM PU, XID, and LU **2** definitions. These are the definitions known to the VTAM system we used in the sample configuration. The XID consists of two parts. The block number, IDBLK, is the first three digits, and the node number, IDNUM, is the last five digits.

```
SC02130 PU ADDR=01,
            IDBLK=05D,IDNUM=02130,
            ANS=CONT,DISCNT=NO,
            IRETRY=NO,ISTATUS=ACTIVE,
            MAXDATA=265,MAXOUT=1,
            MAXPATH=1,
            PUTYPE=2,SECNET=NO,
            MODETAB=POKMODE,DLOGMOD=DYNRMT,
            USSTAB=USSRDYN,LOGAPPL=SCGVAMP,
            PACING=1,VPACING=2
*
SC02130I LU LOCADDR=0,DLOGMOD=LU62PS 2
::
```

Figure 3. VTAM: PU, XID, and LU definitions

The LU SC02030I **2** is an independent LU6.2 definition.

Sample configuration

APPL

Figure 4 shows the VTAM APPL **3** definition for the CICS Transaction Server for OS/390 required for the sample configuration.

```
AP26CICS VBUILD TYPE=APPL 3
*
IYCQCTS5 APPL AUTH=(ACQ,PASS,VPACE),VPACING=0,EAS=29,PARSESS=YES,
              SONSCIP=YES,MODETAB=MTCICS
*
:::
```

Figure 4. VTAM: APPL definition

We used LU6.2 parallel sessions (PARSESS=YES) rather than single sessions.

LogMode

Figure 5 shows the VTAM LogMode **4** definition required for the CICS Universal Client to connect to the CICS Transaction Server for OS/390.

```
LU62PS MODEENT LOGMODE=LU62PS, 4
TYPE=0,           ONLY TYPE RECOGNISED
FMPROF=X'13',     SNA
TSPROF=X'07',     SNA
PRIPROT=X'B0',    PRIMARY PROTOCOL
SECPROT=X'B0',    SECONDARY PROTOCOL
COMPROT=X'79A5',  COMMON PROTOCOL
SSNDPAC=X'00',
SRCVPAC=X'00',
RUSIZES=X'8989',  RUSIZES IN-4096 OUT-4096
PSNDPAC=X'00',
PSERVIC=X'060200000000000000122F00'
```

Figure 5. VTAM: LogMode definition

CICS Transaction Server for OS/390 Version 1.3

In this section we present the definitions required for the CICS Transaction Server for OS/390 Version 1.3.

System Initialization Table parameters

Figure 6 on page 11 shows the SIT parameters required to enable ISC and to define the CICS Transaction Server for OS/390 APPLID **3**.

```
     ::
ISC=YES
APPLID=IYCQCTS5
     ::
```

Figure 6. CICS Transaction Server for OS/390 APPLID definition

DFHISC group

To enable ISC on CICS Transaction Server for OS/390, you must install the DFHISC group. You can use resource definition online (RDO) to install the group, or add the group to your startup list (GRPLIST).

LU6.2 connection

Figure 7 and see Figure 8 on page 12 show the independent LU6.2 connection definitions that we installed on the CICS Transaction Server for OS/390.

```
OBJECT CHARACTERISTICS                                    CICS RELEASE = 0530
  CEDA View Connection( C130 )
   Connection    : C130
   Group         : C130
   DEscription   :
  CONNECTION IDENTIFIERS
   Netname       : SC02130I  2
   INDsys        :
  REMOTE ATTRIBUTES
   REMOTESYSTem  :
   REMOTEName    :
   REMOTESYSNet  :
  CONNECTION PROPERTIES
   ACcessmethod  : Vtam               Vtam ¦ IRc ¦ INdirect ¦ Xm
   PRotocol      : Appc               Appc ¦ Lu61 ¦ Exci
   Conntype      :                    Generic ¦ Specific
   SInglesess    : No                 No ¦ Yes
   DAtastream    : User               User ¦ 3270 ¦ SCs ¦ STrfield ¦ Lms
 + RECordformat  : U                  U ¦ Vb
                                                 SYSID=YCQ5 APPLID=IYCQCTS5

PF 1 HELP 2 COM 3 END            6 CRSR 7 SBH 8 SFH 9 MSG 10 SB 11 SF 12 CNCL
```

Figure 7. CICS Transaction Server for OS/390: SNA Connection definition

```
OBJECT CHARACTERISTICS                                    CICS RELEASE = 0530
  CEDA View Connection( C022 )
 + Queuelimit    : No        No ¦ 0-9999
   Maxqtime      : No        No ¦ 0-9999
  OPERATIONAL PROPERTIES
   AUtoconnect   : Yes       No ¦ Yes ¦ All
   INService     : Yes       Yes ¦ No
  SECURITY
   SEcurityname  :
   ATtachsec     : Verify    Verify Local ¦ Identify ¦ Verify ¦ Persistent
                             ¦ Mixidpe
   BINDPassword  :           PASSWORD NOT SPECIFIED
   BINDSecurity  : No        No ¦ Yes
   Usedfltuser   : Yes       No ¦ Yes
  RECOVERY
   PSrecovery    :           Sysdefault Sysdefault ¦ None
   Xlnaction     :           Keep Keep ¦ Force




                                                  SYSID=YCQ5 APPLID=IYCQCTS5

PF 1 HELP 2 COM 3 END             6 CRSR 7 SBH 8 SFH 9 MSG 10 SB 11 SF 12 CNCL
```

Figure 8. CICS TS Version 1.3: SNA Connection definition (Second Screen)

For SunLink SNA/PTP, you must specify security **ATtachsec : Verify** on your connection definition. It is not necessary to specify SEC=YES as a SIT parameter.

It is recommended that the **Usedfltuser** parameter on the server connection definition is set to Yes if you are using signon capable terminals and to No if you are using signon incapable terminals.

Figure 9 on page 13 shows the sessions definition required for the sample configuration. The LU6.2 connection definition and LU6.2 sessions definition must reside in the same group and be installed simultaneously. We used Group(C130) in our sample configuration.

```
OBJECT CHARACTERISTICS                                    CICS RELEASE = 0530
  CEDA View Sessions( LU62PS )
   Sessions      : LU62PS
   Group         : C022
   DEscription   :
  SESSION IDENTIFIERS
   Connection    : C022
   SESSName      :
   NETnameq      :
   MOdename      : LU62PS
  SESSION PROPERTIES
   Protocol      : Appc                Appc ¦ Lu61 ¦ Exci
   MAximum       : 008 , 004           0-999
   RECEIVEPfx    :
   RECEIVECount  :                     1-999
   SENDPfx       :
   SENDCount     :                     1-999
   SENDSize      : 00256               1-30720
 + RECEIVESize   : 00256               1-30720

                                                  SYSID=YCQ5 APPLID=IYCQCTS5

PF 1 HELP 2 COM 3 END             6 CRSR 7 SBH 8 SFH 9 MSG 10 SB 11 SF 12 CNCL
```

Figure 9. CICS Transaction Server for OS/390: SNA Sessions definition

Setting up SunLink P2P LU6.2 9.1 for CICS Client Solaris SNA driver

This SNA configuration requires a domain nameserver.

You must obtain the licenses for SunLink SNA3270 Gateway and SunLink Client 3270. The request form is:

```
/opt/SUNWste/license_tools/License_Request_For
```

and this can be sent by e-mail to eu-licensing@UK.Sun.COM.

Installing SunLink IBM SNA Gateway

To install:

1. Insert the SunLink IBM SNA Gateway 9.1 CD_ROM. (The VolumeManager should automatically mount it as /cdrom/sunlink_ibm_sna_gateway_9_1.)
2. Change directory to the Product subdirectory.
3. Use the **pkgadd** command to install all the software packages into /opt (the default destination directory).

   ```
   # pkgadd -d .
   ```

After you install SunLink, the programs and configuration files are in SUNW* directories under the /opt directory.

Sample configuration

Set the environment variable:
LM_LICENSE_FILE=/etc/opt/licenses/licenses_combined. Otherwise the sungmi command cannot find the licenses.

Configuring GMAN

1. Change to the SUNWgman directory and run **./sunsetup**
2. Keep the directory names as set.
3. Use the main DNS with domain name, for example, `hursley.ibm.com`
4. Set the SunLink subdomain to your machine name, for example, `newyork`
5. Exit sunsetup.

In the SUNWgman directory, set the contents of named.boot as in the following example:

```
directory .
primary   newyork.hursley.ibm.com       named.db
```

In the same directory, the contents of named.db should start as follows:

```
@  IN  SOA  newyork root.newyork.hursley.ibm.com (
                  . . . . )
```

where newyork is our example machine name.

Configuring SunLink

In this section we describe in detail how to define your values to SunLink for our sample configuration.

Start SunLink by running /opt/SUNWgman/sunsetup and choosing the Start options (4 and 5) to start GMAN and PU21.

Change to the /opt/SUNWgmi directory and start the configuration tool with **./sungmi**. Enter the domain name (in our example, newyork) and root password.

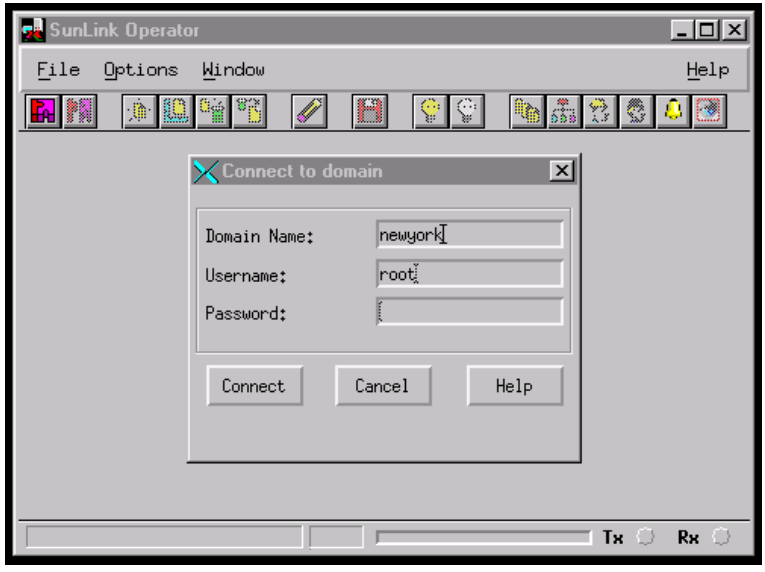

Figure 10. Connect to domain

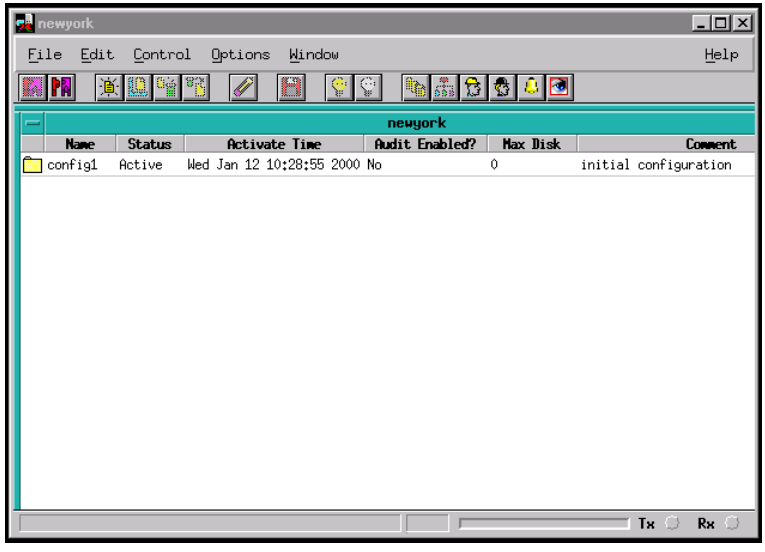

Figure 11. Configuration window

Sample configuration

Now follow the SunLink configuration guide. If operating remotely you may need to right-click and select expand (rather than double-clicking) to open an entry.

1. Create a manager system: Highlight **config1** in the configuration window, (Figure 12), and select **File/Open** to open the configuration. Select **Window/Managers List** and then **Edit/New manager** to display the Create Manager dialog, (Figure 12). Enter the hostname of the machine and select **OK**.

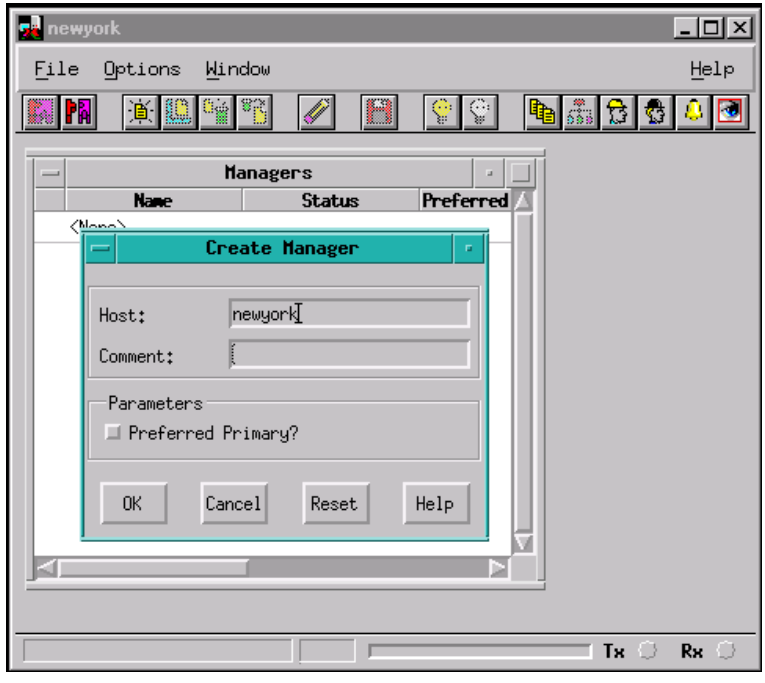

Figure 12. Create a manager system

2. Create system: Open the configuration and select **Systems** in the resource tree. Select **Edit/New/System** to display the Create System dialog, (Figure 13). Enter the hostname of the SNA Server system (this is probably the same machine) and select **OK**.

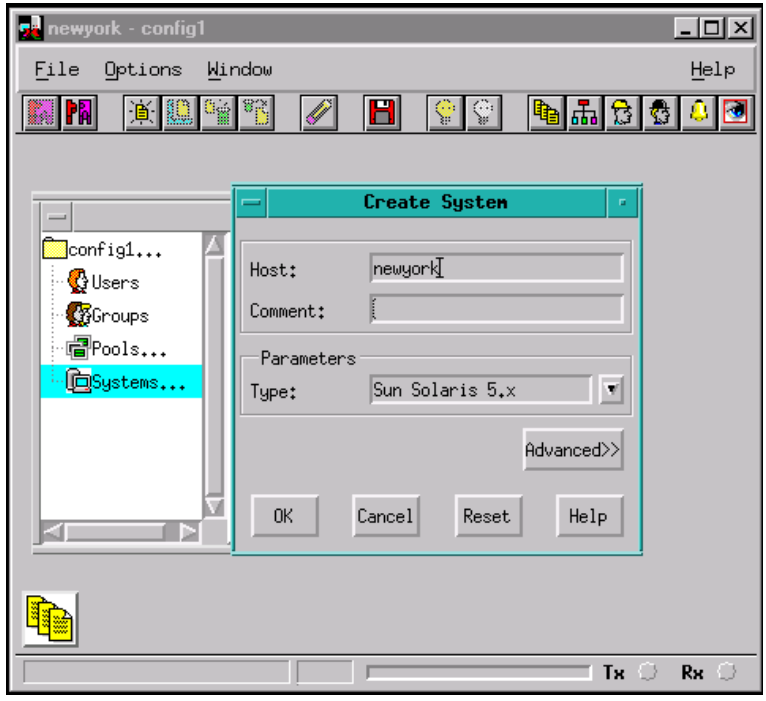

Figure 13. Create system

3. Add PU2.1 Server: Open Systems and the entry for the System just added, and select **PU2.1 Servers** to open the resource. Select **Edit/New/PU2.1 Server** to display the Create PU2.1 Server dialog, (Figure 14). Enter the LU Name **2** and the fully qualified name **1** . **2** and change the Service Name Parameters to brxadmin_pu2 and brxlu62_serv as shown, and select **OK**.

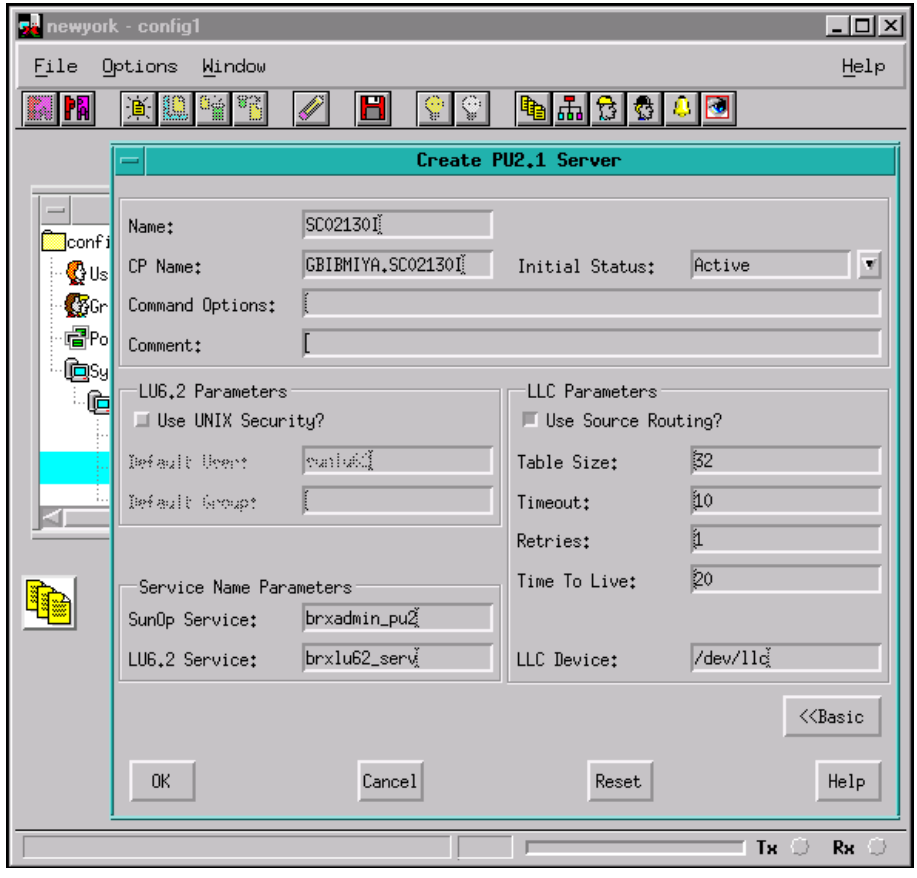

Figure 14. Add PU2.1 Server

4. Add LAN connection: Open PU2.1 Servers in the resource tree and open the PU2.1 server just added. Click on **LAN connections** and select **Edit/New/LAN Connection** to display the Create LAN Connection dialog, (Figure 15). Enter a name and the device as appropriate, enter the MAC address of you local network interface, and change the Token Ring speed (in Advanced) if necessary. Select **OK**.

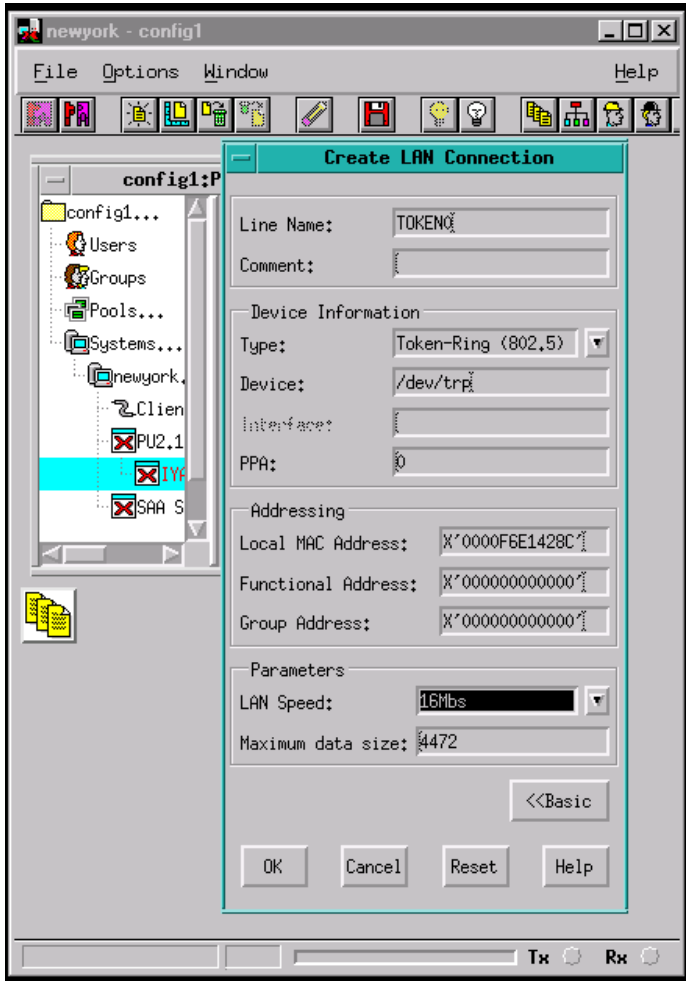

Figure 15. Add LAN connection

5. Add a PU (Advanced DLC configuration): Display the name of the connection just added and select **Edit/New/DLC (PU2)** to display the Create DLC dialog, (Figure 16). Enter the the DLC name, MAC address of the remote SNA host, and select **OK**.

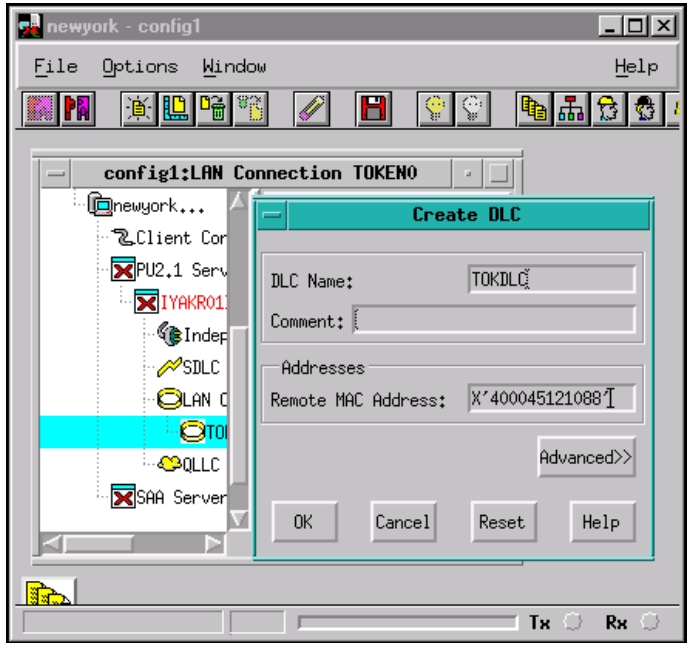

Figure 16. Add a PU

6. Add an independant LU: Open the PU2.1 Servers list, select the entry added above, and select **Edit/New/Independent LU** to display the Create Independent LU dialog, (Figure 17). Enter the local LU name **2** and the fully qualified name **1** . **2** , and change the Session Limit (default 1024) if your license is for fewer connections (for example, 16), and select **OK**.

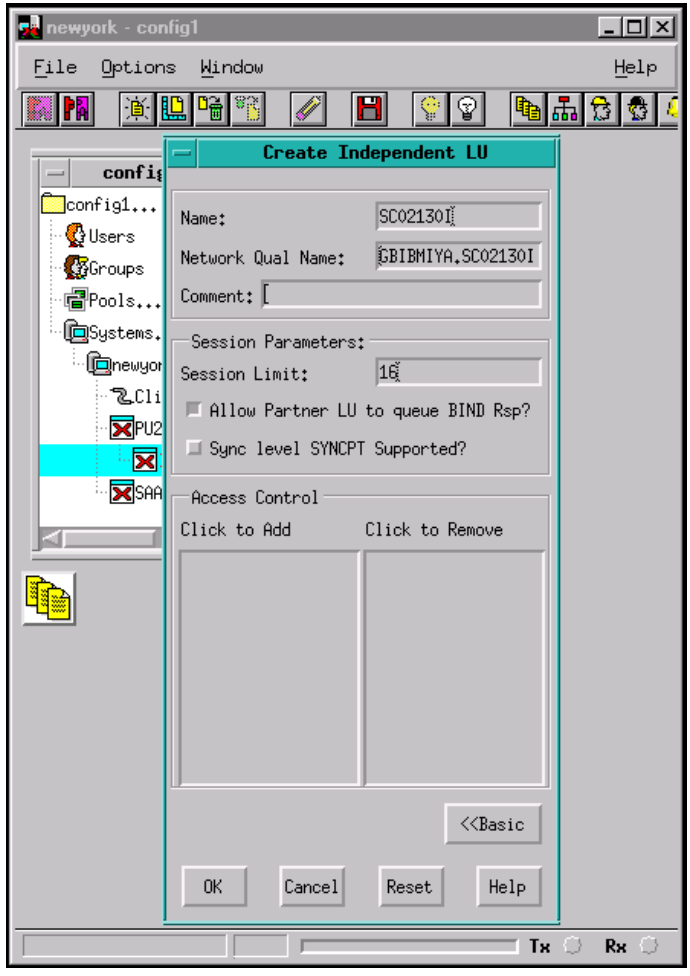

Figure 17. Add an independant LU

7. Configure a partner LU: Open the PU2.1 server as above and select **Edit/New/Partner LU** to display the Create Partner LU dialog, (Figure 18). Enter the Partner LU name **3**, the fully qualified name **1**.**3** and select the Local LU from the list provided, and select **OK**.

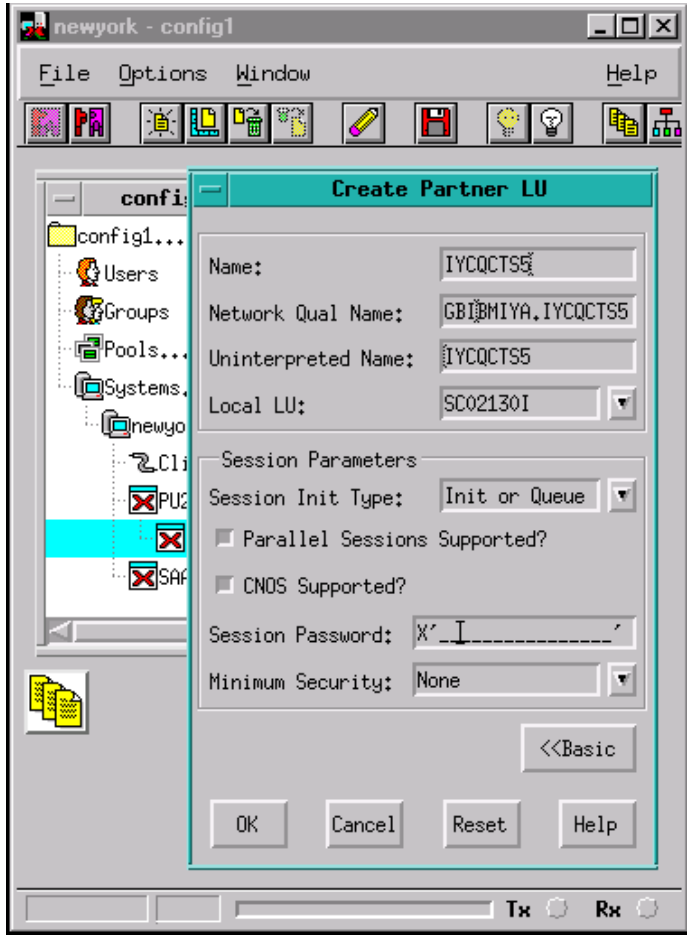

Figure 18. Configure a partner LU

8. Configure the session mode: Open the PU2.1 server name and select the partner LU just added. Select **Edit/New/Mode** to display the Create Mode dialog, (Figure 19). Enter the Mode Name **4** and adjust the Session Limits as appropriate for the remote system. Select **OK**.

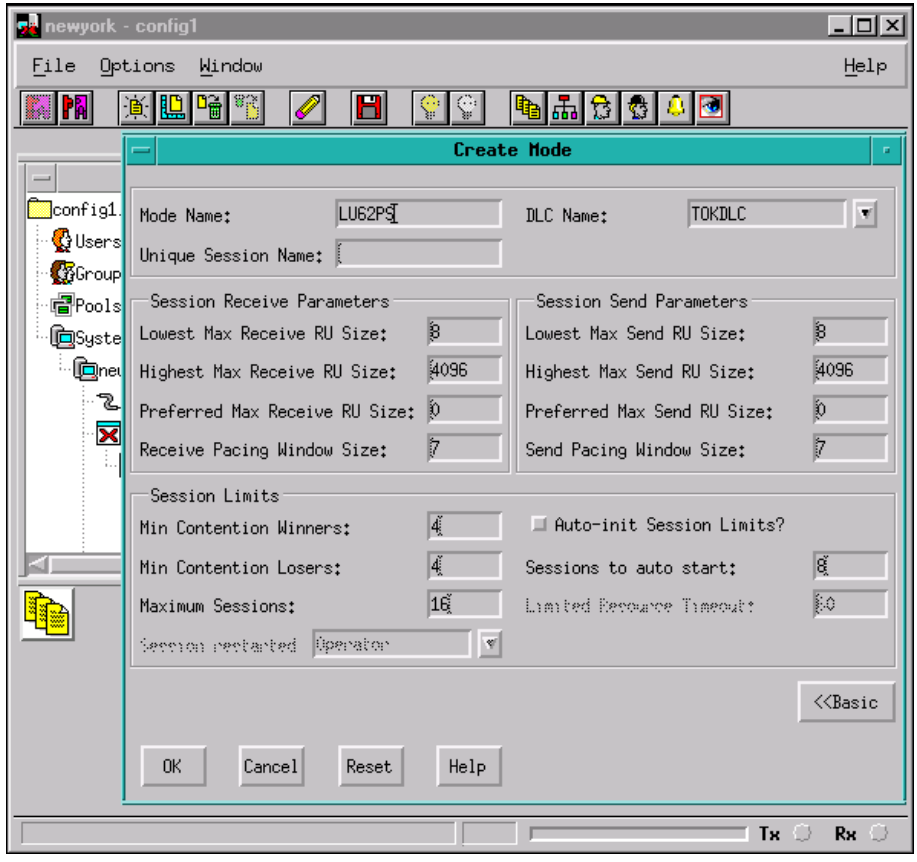

Figure 19. Configure the session mode

9. To enable ATI, configure a transaction program for CRSR. Open the PU2.1 server name and click on **Transaction Programs** to select it. Select **Edit/New/Transaction Program** to display the Create Transaction Program dialog, (Figure 20). Enter the transaction name `CRSR` and the **Command Path** `/usr/.sbin/cclclnt CRSR`. Select **OK**.

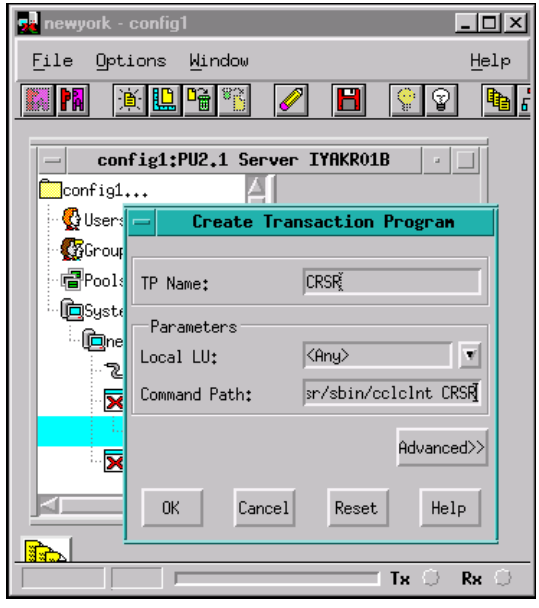

Figure 20. Define the CRSR transaction program

Sample configuration files

The configuration files are stored in /opt/SUNWgman/config1 directory, and for our example, newyork (ILU is SC02030I) would be the following:

- SunNetwork.cfg
- SunSys_newyork.aftp
- SunUser.cfg, which is an empty file
- SunSrv_SC02030I.cfg
- SunSys_newyork.cfg

CICS Universal Client for Solaris

You use the CICS Universal Client's configuration tool to define the settings for SNA communication. The configuration tool generates the CTG.INI file, which is located in the /opt/cicscli/bin subdirectory. The CICS Universal Client uses the CTG.INI file to establish a connection to a CICS server.

For information on using the configuration tool, refer to your *CICS Universal Client Administration* book.

You need to define the following **Server** configuration settings (see Figure 21 on page 26):

Server name
An arbitrary name for a particular CICS server.

Description
An arbitrary description for the CICS server.

Network protocol
The protocol for communication with the CICS server, in this case, SNA.

Partner LU name
The LU Name of the server as it is known to the APPC configuration at the CICS Universal Client. This must be an eight-character alias name; see the description of **Use LU Alias names** below.

Local LU name **2**
The name of a local LU to be used when connecting to the server. The same LU can be used for all server connections.

Mode name **4**
The mode name to be used when connecting to the server.

Use LU alias names
This setting enables the Partner LU name and Local LU name to be specified as alias names instead of real LU names. This means, for

example, that it is possible to switch between servers without stopping the CICS Universal Client. For CICS Universal Client for Solaris, alias names must be used.

The *CICS Universal Client Administration* book and the configuration tool's online help provide descriptions of the configuration settings for CICS Universal Client.

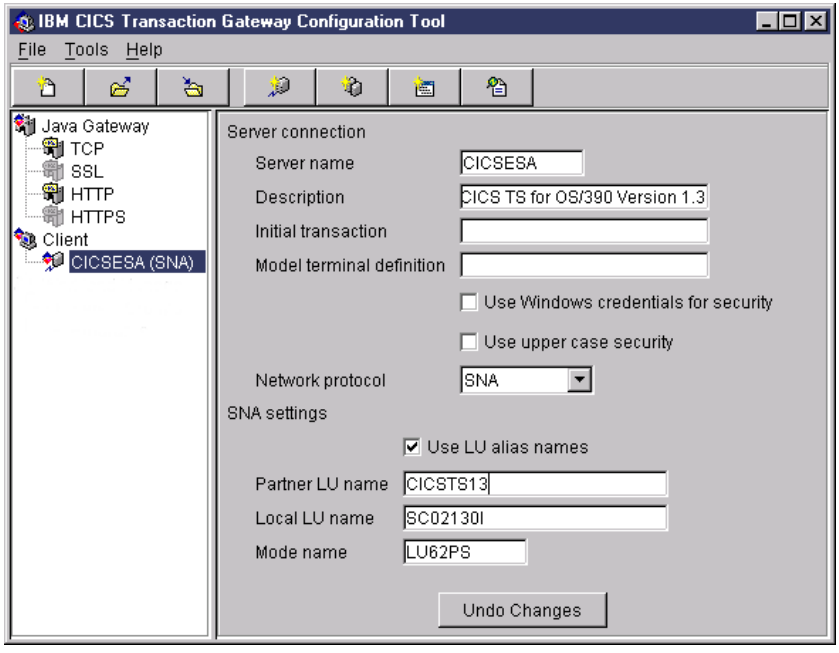

Figure 21. Configuration tool settings for SunLink SNA/PTP

Figure 22 on page 27 shows an excerpt from the resultant CTG.INI file.

```
SECTION CLIENT = *
    :::
ENDSECTION
    :::
SECTION SERVER = CICSESA
    DESCRIPTION=CICS TS for OS/390  V1.3
    UPPERCASESECURITY=N
    PROTOCOL=SNA
    LOCALLUNAME=SCO2130I          2
    MODENAME=LU62PS               4
    NETNAME=CICSTS13
    LUALIASNAMES=Y
ENDSECTION
    :::
SECTION DRIVER = SNA
    DRIVERNAME=CCLIBMSN
ENDSECTION
```

Figure 22. CICS Universal Client: CTG.INI file definitions

Chapter 6. Testing your configuration

After you have installed and configured all relevant products for the sample configuration, we recommend that you:

1. Start the CICS Transaction Server for OS/390.
2. Start the SunLink SNA server.
3. Establish an LU6.2 connection between and CICS Transaction Server for OS/390 Version 1.3. You may find see “Chapter 8. Useful commands and utilities” on page 33 useful when establishing your LU6.2 connection.
4. Start the CICS Universal Client for Solaris Version 3.1, using the `cicscli -s=cicsesa` command. (cicsesa is the name we gave to the server in the client configuration.
5. Check the status of the CICS Universal Client, using the `cicscli -l command`. The connection status to the CICS server should show ″Available.″
6. Issue the `cicsterm -s=cicesa` command to install a terminal on the CICS Transaction Server for OS/390.
7. Run a CICS server transaction, for example, CEMT or CECI.

Testing your configuration

Chapter 7. Security implementation

To provide the necessary security for your CICS regions, CICS Transaction Server for OS/390 uses the MVS SAF to route authorization requests to an External Security Manager, such as RACF, at appropriate points within CICS transaction processing. There are many types of security available, from transaction security to CICS resource security. The CICS Transaction Server for OS/390 provides the following security mechanisms for the APPC environment:

- Bind-time (or session) security prevents an unauthorized connection between CICS regions.
- Link security defines the authority of the remote system to access transactions or resources to which the connection itself is not authorized.
- User security checks that a user is authorized both to attach a transaction and to access all resources the transaction requires.

For CICS Universal Clients connecting to the CICS Transaction Server for OS/390, you may want to consider configuring link security.

Preparing link security for our sample configuration

For link security on incoming ECI, EPI, and CICSTERM requests, CICS Transaction Server for OS/390 needs the following settings in the SECURITY section of the connection definition for the client:

SEcurityname	For example, HOLLING (RACF-authorized TSO ID)
ATtachsec	Verify
Usedfltuser	Yes, for signon incapable terminals; No, for signon incapable terminals, see "Signon capable terminals" on page 32.

In addition, you must specify SEC=YES as a SIT override.

Signon capable terminals

Security checking done in the server for transactions started at a signon capable terminal installed by a Client application does not depend on what is specified by the **ATtachsec** option for the connection representing the Client. Instead security checking depends on whether the user signs on while using the terminal.

If the user does not sign on, the Client installed terminal is associated with the default user defined for the server in the SIT. When a transaction is run, the security checks are carried out against this default user. A check is also done against the userid associated with the connection to see whether the Client itself has authority to access the resource.

When a user does sign on, the terminal is associated with the userid just authenticated. For transactions attempting to access reosurces, security checking is done against the userid associated with the connection and the signed-on user's userid.

It is recommended that the **Usedfltuser** parameter on the server connection definition is set to Yes if using signon capable terminals and to No if using signon incapable terminals.

Running CICS Universal Client applications with link security

To establish a connection between the CICS Universal Client and CICS Transaction Server for OS/390 issue the cicscli -s=*server* command as described in see "Chapter 6. Testing your configuration" on page 29. Link security is initiated when the first ECI, EPI, or CICSTERM request is made on a newly established connection.

Chapter 8. Useful commands and utilities

You will find the commands discussed in this section useful during installation and configuration.

Perform line tracing

For tracing from a remote system, you must include that system in the .rhosts file to allow remote login.

Line tracing for Token Ring (using sunscope) requires a command like the following (which should be run from /opt/SUNWgmi directory):

```
sunscope -e -t -T -d  /dev/trp > /var/cicscli/sunscope.trc
```

where /var/cicscli/sunscope.trc will contain the line trace.

Messages from SunLink

During operation of SunLink 9.1, an internal processing condition message ″Invalid Stray RSP″ is occasionally written to the console. This does not seem to affect its operation.

Establish a connection from the CICS Transaction Server for OS/390

To establish an LU6.2 connection from CICS Transaction Server for OS/390 Version 1.3:

1. From a 3270 terminal emulator connected to your CICS region, enter the CEMT INQ CONN command and locate your connection name.
2. If the connection status shows Rel (for Released), overtype the R with A (for Acquire).
3. Press the Enter key to refresh the connection status. Figure 23 shows the connection acquired for the sample configuration.

```
CEMT INQ CONN(C130)
STATUS: RESULTS - OVERTYPE TO MODIFY
 Con(C130) Net(SC02130I) Ins Acq Vta Appc
```

Figure 23. CICS TS Version 1.3: Connection status

4. The CEMT INQ MODE CONN(C130) command displays the LU6.2 session status for the sample configuration (see Figure 24).

```
CEMT INQ MODE CONN(C130)
STATUS: RESULTS - OVERTYPE TO MODIFY
 Mod(SNASVCMG) Con(C130) Max(002) Ava( 002 ) Act(002)
 Mod(LU62PS  ) Con(C130) Max(008) Ava( 008 ) Act(008)
```

Figure 24. CICS TS Version 1.3: LU6.2 Session status

Appendix. Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, or other countries, or both:

Anynet	CICS
IBM	OS/390
VTAM	

Java, and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, or other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.