CICS® Universal Client Configuration

Configuring CICS Universal Client for Windows NT® for eNetwork Personal Communications

CICS® Universal Client Configuration

IBM

Configuring CICS Universal Client for Windows NT® for eNetwork Personal Communications

Contents

© Copyright IBM Corp. 1994, 1999

Chapter 1. Overview

The sample configuration shown in Figure 1 consists of a CICS Universal Client for Windows NT Version 3.1 connecting to CICS Transaction Server for OS/390 Version 1.3 across a network using IBM eNetwork Personal Communications Version 4.3.

Communication is through SNA LU6.2 communication provided by eNetwork Personal Communications on the client workstation, and VTAM on the mainframe server.

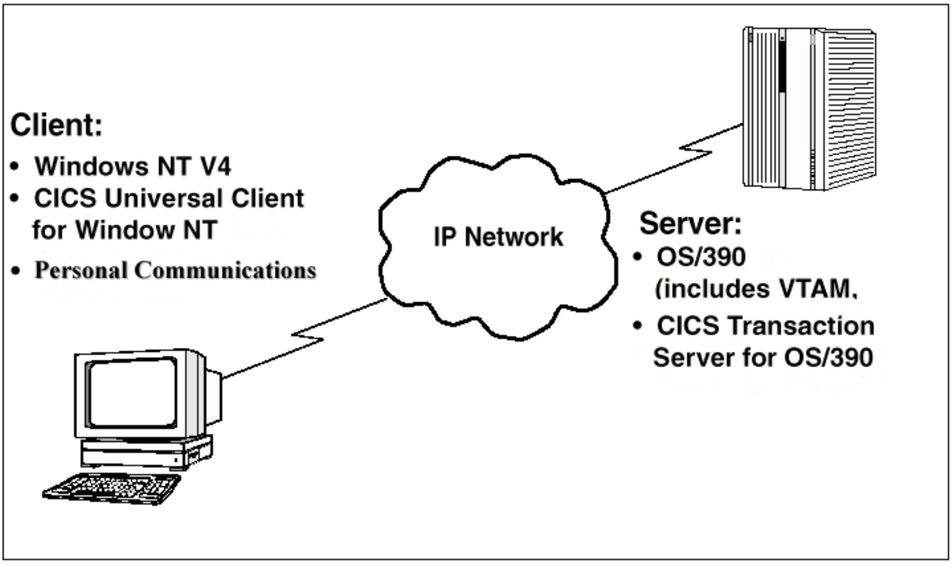

Client:
• Windows NT V4
• CICS Universal Client for Window NT
• Personal Communications
IP Network
Server:
• OS/390 (includes VTAM,
• CICS Transaction Server for OS/390

Figure 1. CICS Universal Client for Windows NT connected through eNetwork Personal Communications

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.

In this document we cover the following topics:

- “Chapter 2. Software checklist” on page 3
- “Chapter 3. Definitions checklist” on page 5
- “Chapter 4. Matching definitions” on page 7

© Copyright IBM Corp. 1994, 1999

- “Chapter 5. Sample configuration” on page 9
- “Chapter 6. Testing your configuration” on page 23
- “Chapter 7. Security implementation” on page 25
- “Chapter 8. Useful commands and utilities” on page 29

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

We used the following software on the client workstation:

- Windows NT Workstation Version 4.0 (service level 4)
- eNetwork Personal Communications Version 4.3
- CICS Universal Client for Windows NT Version 3.1
- Java Runtime Environment (JRE) Version 1.1.8 for Windows NT (necessary for running the configuration tool and other tools.)

© Copyright IBM Corp. 1994, 1999

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 2
  - LU 3
  - XID 4
  - Token Ring destination address 5
  - APPL 6
  - LogMode 7
- CICS Transaction Server for OS/390
  - Netname 3
  - Applid 6
  - Modename 7
- eNetwork Personal Communications
  - A fully qualified CP name, consisting of:
    - A qualified network name 1 .control point name 2
  - Partner LU name 1 . 6
  - CP Alias 2
  - Local Node ID 4
  - Destination address 5
  - Local LU Name 3
  - Mode Name 7
- CICS Universal Client for Windows NT Version 3.1
  - Partner LU name, which can be either of:
    - A qualified network name Network 1 .Partner LUName 6
    - An alias name 6 .
  - Local LU name 3
  - Mode name 7

© Copyright IBM Corp. 1994, 1999

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**	**eNetwork Personal Communications**	**Client configuration**	**Example**
1	NETID	—	First part of Partner LU name	Partner LU name	GBIBMIYA
2	PU	—	CP Alias	—	IYALR01E
3	LU	Netname	Local LU name	Local LU name	IYALT1E0
4	XID	—	Local Node ID	—	05D 316C7
5	Token Ring destination address	—	Destination address	—	400045121088
6	APPL	Applid	Second part of Partner LU name	Partner LU name	IYCNZCA3
7	LogMode	Modename	Mode name	Mode name	LU62PS

© Copyright IBM Corp. 1994, 1999

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 2, XID 4, and LU 3 definitions for our Client gateway. These are the definitions for the Client gateway 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.

```
IYALR01E PU ADDR=01,  2
            IDBLK=05D,IDNUM=316C7,  4
            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
*
IYALT1E0 LU LOCADDR=0,DLOGMOD=LU62PS  3
::
```

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

© Copyright IBM Corp. 1994, 1999

The LU IYALT1E0 3 is an independent LU6.2 definition.

APPL

Figure 4 shows the VTAM APPL 6 definition for the CICS Transaction Server for OS/390 required for the sample configuration.

```
AP23CICS VBUILD TYPE=APPL 6
*
IYCNZCA3 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 7 definition required for the CICS Universal Client to connect to the CICS Transaction Server for OS/390.

```
LU62PS MODEENT LOGMODE=LU62PS, 7
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 CICS Transaction Server for OS/390 definitions required for the sample configuration shown in Figure 1 on page 1.

System Initialization Table parameters

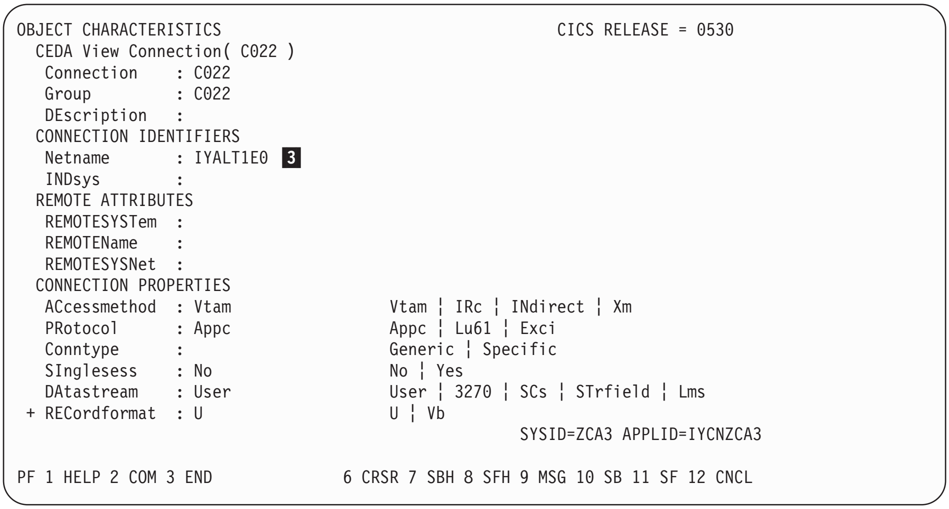
Figure 6 on page 11 shows the SIT parameters required to enable ISC and to define the CICS Transaction Server for OS/390 APPLID 6 .

```
     ::
ISC=YES
APPLID=IYCNZCA3
     ::
```

Figure 6. CICS TS Version 1.3: APPLID definition

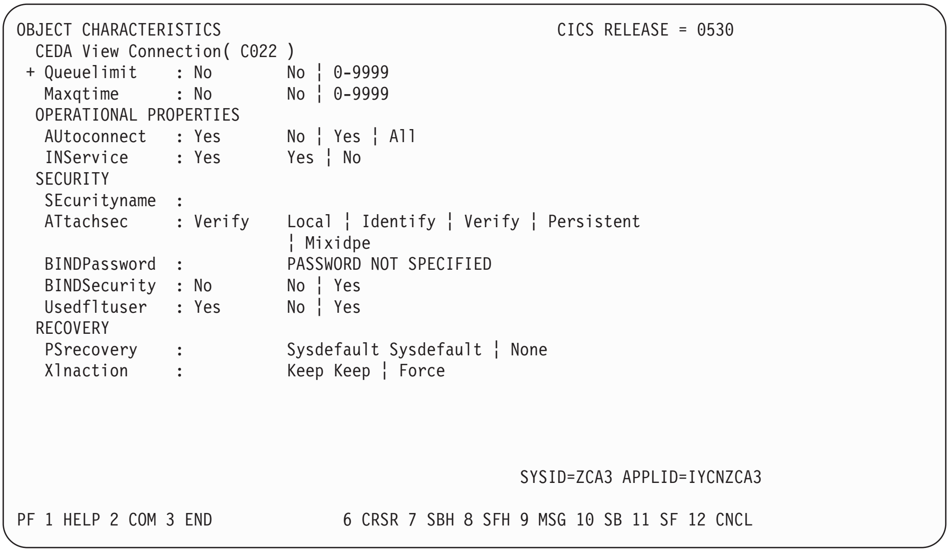
LU6.2 Connection and Sessions

Figure 7 and 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( C022 )
   Connection    : C022
   Group         : C022
   DEscription   :
  CONNECTION IDENTIFIERS
   Netname       : IYALT1E0  3
   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=ZCA3 APPLID=IYCNZCA3

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

Figure 7. CICS TS Version 1.3: SNA Connection definition (first screen)

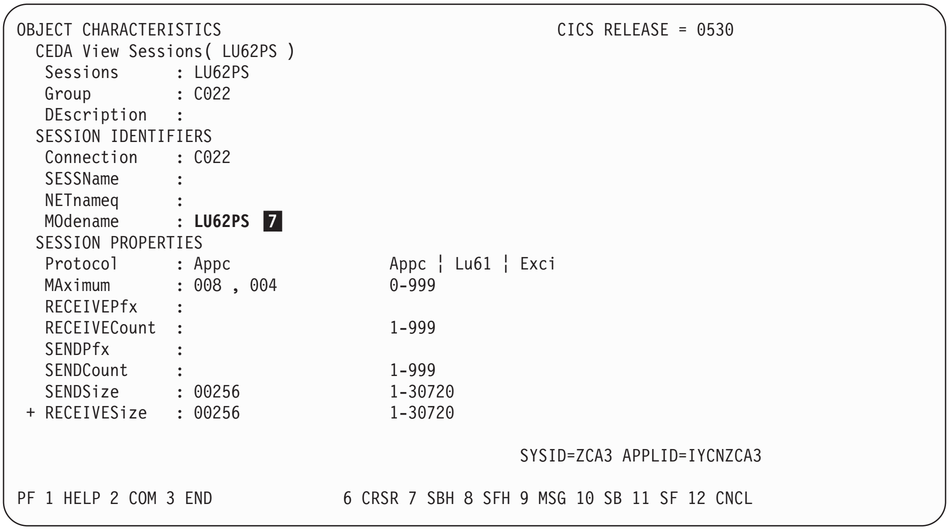


```
OBJECT CHARACTERISTICS                                    CICS RELEASE = 0530
  CEDA View Connection( C022 )
 + Queuelimit    : No        No ¦ 0-9999
   Maxqtime      : No        No ¦ 0-9999
  OPERATIONAL PROPERTIES
   AUtoconnect   : Yes       No ¦ Yes ¦ All
   INService     : Yes       Yes ¦ No
  SECURITY
   SEcurityname  :
   ATtachsec     : Verify    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=ZCA3 APPLID=IYCNZCA3

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 eNetwork Personal Communications, you must specify security **ATtachsec = Verify** on your connection definition. It is not necessary to specify SEC=YES as a SIT parameter.

Figure 9 on page 13 shows the sessions definition required for the sample configuration. You can create the connection and sessions definitions for eNetwork Personal Communications by using RDO. The connection and sessions must be defined in the same group, and they must be installed simultaneously. We used Group(C022) in our sample configuration.



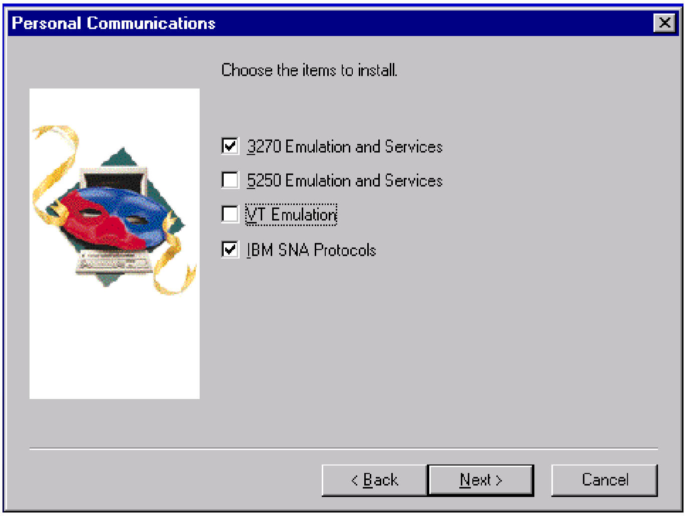
```
OBJECT CHARACTERISTICS                                      CICS RELEASE = 0530
  CEDA View Sessions( LU62PS )
   Sessions      : LU62PS
   Group         : C022
   DEscription   :
  SESSION IDENTIFIERS
   Connection    : C022
   SESSName      :
   NETnameq      :
   MOdename      : LU62PS  7
  SESSION 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=ZCA3 APPLID=IYCNZCA3

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

Figure 9. CICS TS Version 1.3: Sessions definition

Configuring eNetwork Personal Communications

In this section we describe the steps we used to install and set up eNetwork Personal Communications in our sample configuration.

To install eNetwork Personal Communications, run the setup program and follow the instructions on the panels. When you reach the panel shown in Figure 10 on page 14, select **3270 Emulation and Services** and **IBM SNA Protocols**.



Personal Communications

Choose the items to install.

☑ 3270 Emulation and Services

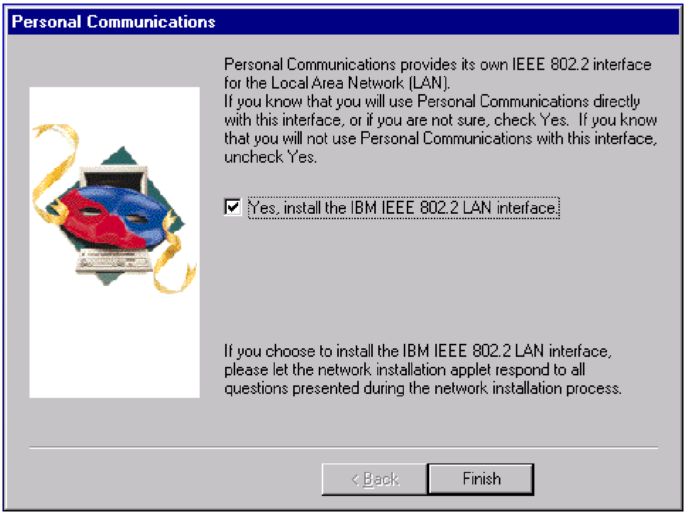
□ 5250 Emulation and Services

□ VT Emulation

☑ IBM SNA Protocols

Figure 10. eNetwork Personal Communications: Installation Items

When you reach the panel shown in Figure 11, select **Yes, install the IEEE 802.2 LAN Interface** and then **Finish** to complete the installation.



Personal Communications

Personal Communications provides its own IEEE 802.2 interface for the Local Area Network (LAN).
If you know that you will use Personal Communications directly with this interface, or if you are not sure, check Yes. If you know that you will not use Personal Communications with this interface, uncheck Yes.

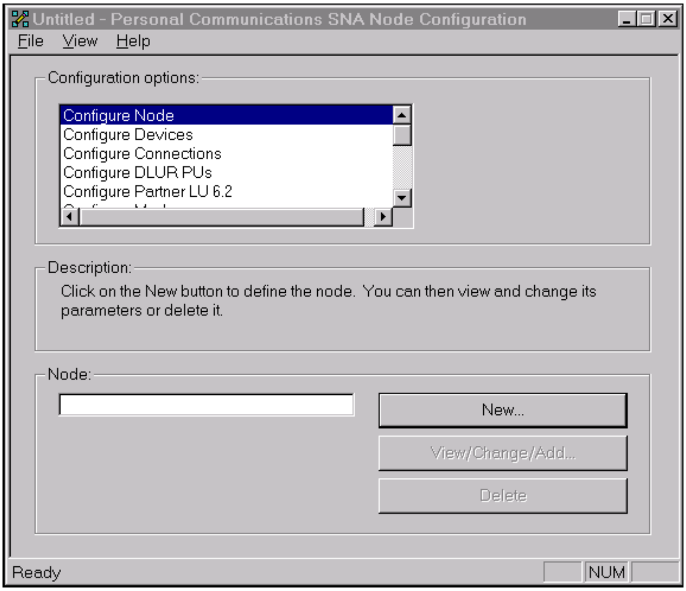
☑ Yes, install the IBM IEEE 802.2 LAN interface.

If you choose to install the IBM IEEE 802.2 LAN interface, please let the network installation applet respond to all questions presented during the network installation process.

Figure 11. eNetwork Personal Communications: Final Installation panel

To configure eNetwork Personal Communications:

1. In the IBM eNetwork Personal Communications folder, select **SNA Node Configuration**. The Node Configuration panel is displayed, see Figure 12.

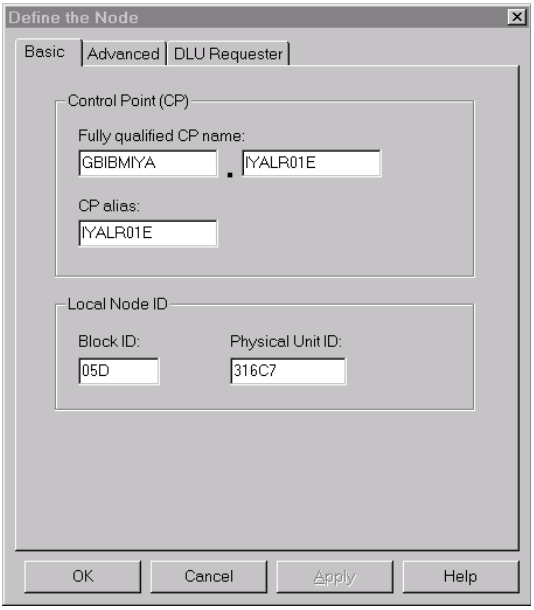


Click on the New button to define the node. You can then view and change its parameters or delete it.

Figure 12. eNetwork Personal Communications: Node Configuration panel

From this panel you select each of the required configuration options.

2. On the Node Configuration panel, select **Configure Node** to display the Define the Node panel, see Figure 13 on page 16, Enter the fully qualified control point name 1 . 2 , the CP alias 2 , and Local Node ID 4 .



Control Point (CP)

Fully qualified CP name: GBIBMIYA . IYALR01E

CP alias: IYALR01E

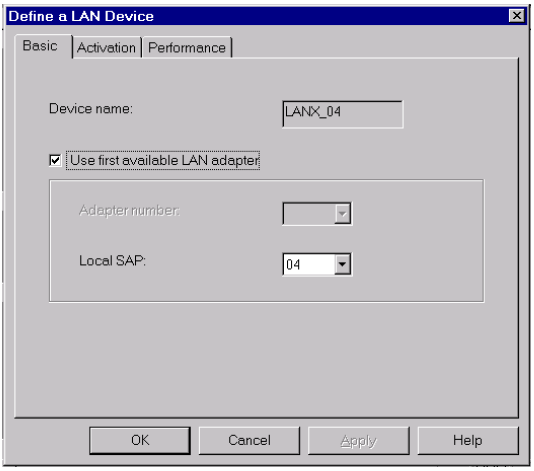
Local Node ID

Block ID: 05D

Physical Unit ID: 316C7

Figure 13. eNetwork Personal Communications: Define the Node

3. On the Node Configuration panel, select **Configure Devices** to display the Define a LAN Device panel, see Figure 14. Select **OK** to accept the defaults on the panel.



Device name: LANX_04

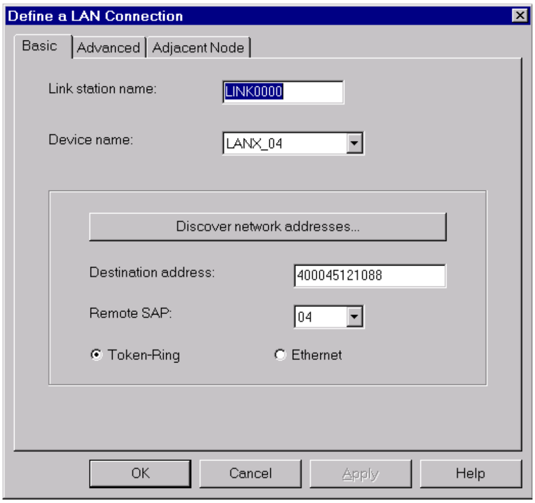
☑ Use first available LAN adapter

Adapter number:

Local SAP: 04

Figure 14. eNetwork Personal Communications: Define a LAN Device

4. On the Node Configuration panel, select **Configure Connections** to display the Define a Lan Connection panel, see Figure 15. Fill in the panel including the Destination Address **5**.



Link station name: LINK0000

Device name: LANX_04

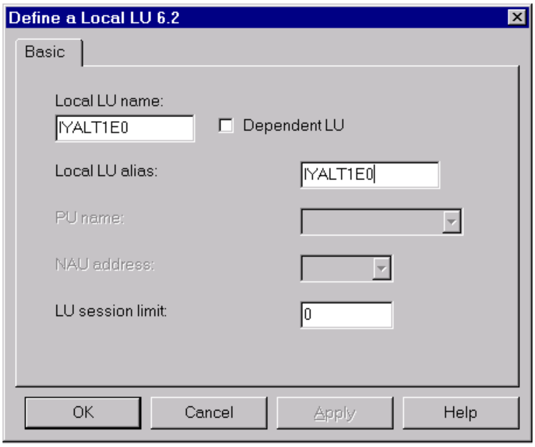
Destination address: 400045121088

Remote SAP: 04

● Token-Ring ○ Ethernet

Figure 15. eNetwork Personal Communications: Define a LAN Connection

5. On the Node Configuration panel, select **Configure Local LU 6.2** to display the Define a Local LU 6.2 panel, see Figure 16. Enter the Local LU Name, which is the same as the Local LU Alias **3** Also, make sure that **Dependent LU** is not checked.



Local LU name: IYALT1E0

□ Dependent LU

Local LU alias: IYALT1E0

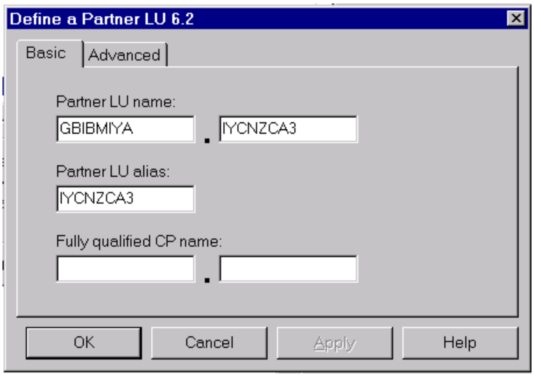
PU name:

NAU address:

LU session limit: 0

Figure 16. eNetwork Personal Communications: Define a Local LU 6.2

6. On the Node Configuration panel, select **Configure Partner LU6.2** to display the Define a Partner LU 6.2 panel, see Figure 17. Enter the Partner LU Name **1** . **6** and the Partner LU Alias **6** .



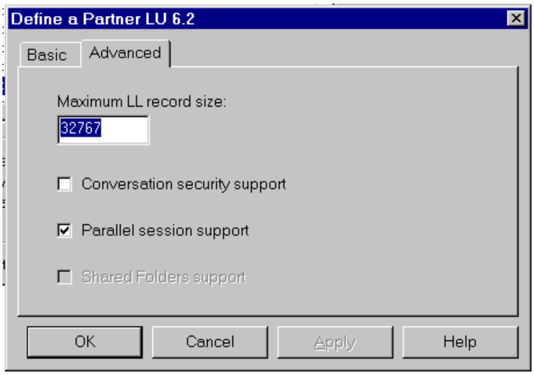
Partner LU name: GBIBMIYA . IYCNZCA3

Partner LU alias: IYCNZCA3

Fully qualified CP name: .

Figure 17. eNetwork Personal Communications: Define a Partner LU 6.2 (Basic)

7. Now select the **Advanced** tab, and uncheck **Conversation security support**, see Figure 18.



Maximum LL record size: 32767

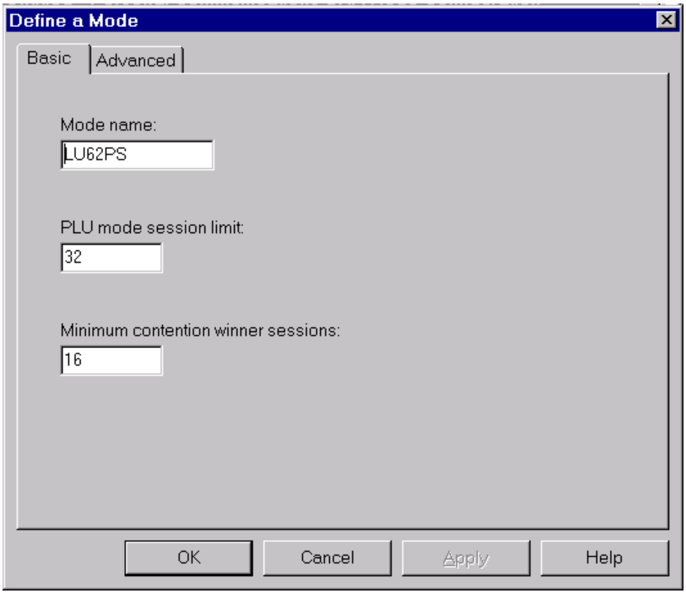
☐ Conversation security support

☑ Parallel session support

☐ Shared Folders support

Figure 18. eNetwork Personal Communications: Define a Partner LU 6.2 (Advanced)

8. On the Node Configuration panel, select **Configure Modes** to display the Define a Mode panel, see Figure 19 on page 19. Enter the Mode name **7** , and select **OK** to accept the default values for the other fields.



Define a Mode

Basic | Advanced

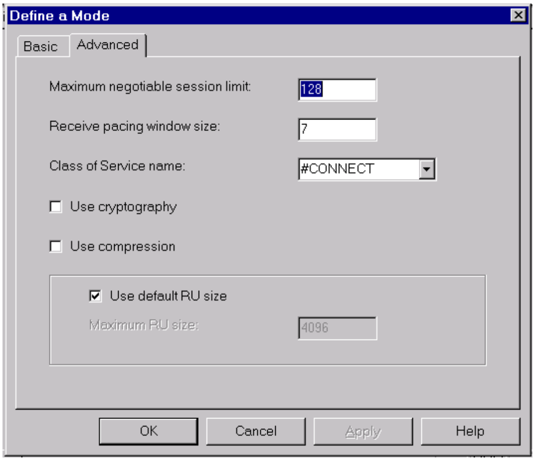
Mode name: LU62PS

PLU mode session limit: 32

Minimum contention winner sessions: 16

Figure 19. eNetwork Personal Communications: Define a Mode (Basic)

9. Now select the **Advanced** tab, and fill in the panel as shown in Figure 20.



Define a Mode

Basic | Advanced

Maximum negotiable session limit: 128

Receive pacing window size: 7

Class of Service name: #CONNECT

☐ Use cryptography

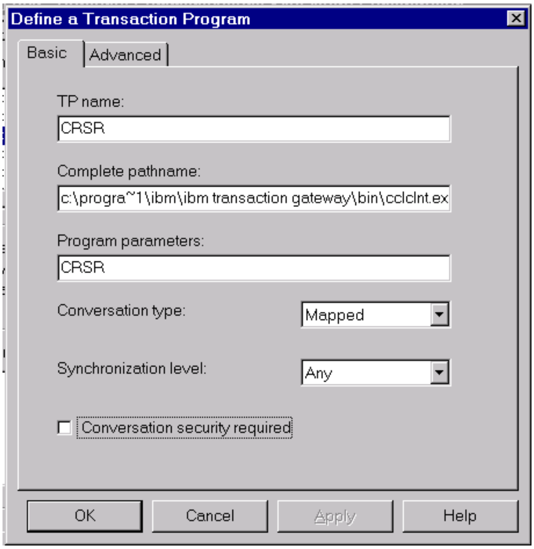
☐ Use compression

☑ Use default RU size

Maximum RU size: 4096

Figure 20. eNetwork Personal Communications: Define a Mode (Advanced)

10. To enable Automatic Transaction Initiation (ATI) against CICS Universal Client terminals, you must define the transaction program CRSR. On the Node Configuration panel, select **Configure Transaction Programs**, and fill in the diaplayed panel as shown in Figure 21 on page 20.



TP name: CRSR

Complete pathname: c:\progra~1\ibm\ibm transaction gateway\bin\cclclnt.ex

Program parameters: CRSR

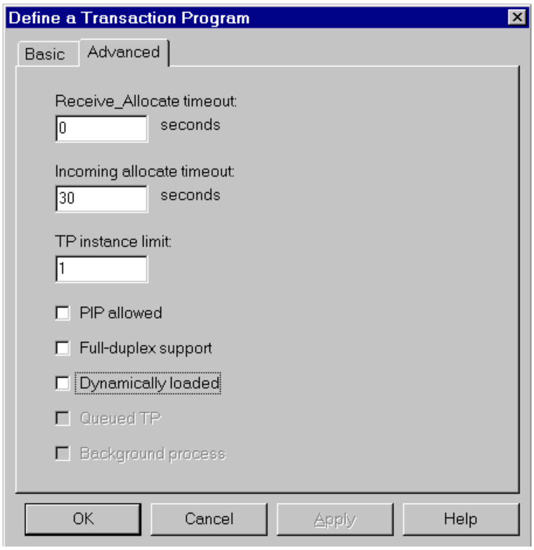
Conversation type: Mapped

Synchronization level: Any

☐ Conversation security required

Figure 21. eNetwork Personal Communications: Define a Transaction Program (Basic)

11. Now select the **Advanced** tab, and fill in the panel as shown in Figure 22.



Receive_Allocate timeout: 0 seconds

Incoming allocate timeout: 30 seconds

TP instance limit: 1

☐ PIP allowed

☐ Full-duplex support

☐ Dynamically loaded

☐ Queued TP

☐ Background process

Figure 22. eNetwork Personal Communications: Define a Transaction Program (Advanced)

12. On the Node Configuration panel, select **File** and **Save** your configuration. The default file type is *.ACG and the default directory is the \private subdirectory of your eNetwork Personal Communications directory.

Configuring CICS Universal Client for Windows NT

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 \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 23 on page 22):

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.

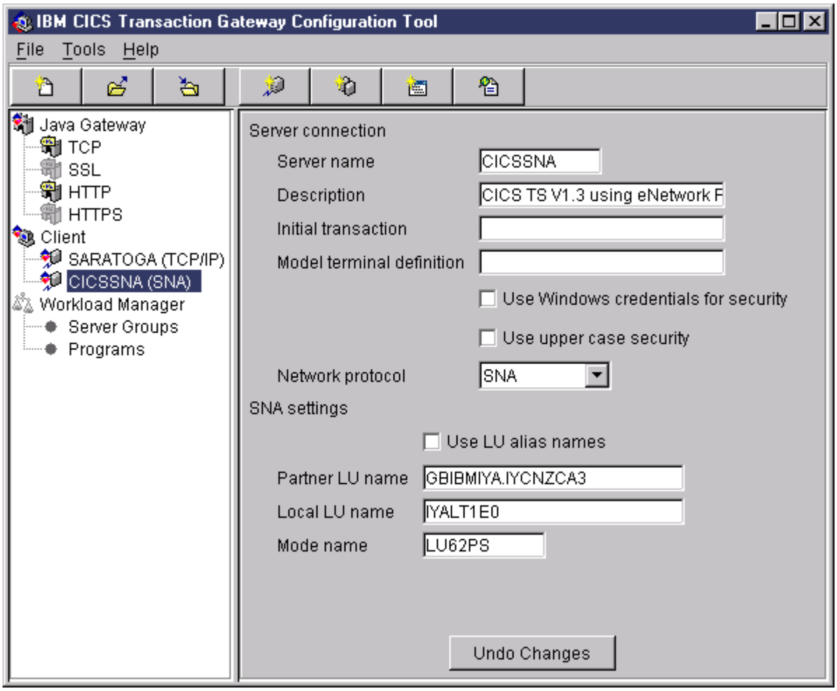
Partner LU name 1 . 6
The LU Name of the server as it is known to the APPC configuration at the CICS Universal Client. This can be a qualified 17-character name as in our example, GBIBMIYA.IYCNZCA3, or an alias name (as long as **Use LU Alias names** is selected).

Local LU name 3
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 7
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. The default is that LU alias names are not used.

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



Server connection

Server name: CICSSNA

Description: CICS TS V1.3 using eNetwork F

Initial transaction:

Model terminal definition:

□ Use Windows credentials for security

□ Use upper case security

Network protocol: SNA

SNA settings

□ Use LU alias names

Partner LU name: GBIBMIYA.IYCNZCA3

Local LU name: IYALT1E0

Mode name: LU62PS

Figure 23. Configuration tool settings for eNetwork Personal Communications

Figure 24 shows an excerpt from the resultant CTG.INI file.

```
SECTION CLIENT = *
    :::
ENDSECTION
    :::
SECTION SERVER = CICSSNA
    DESCRIPTION=CICS TS V1.3 using eNetwork Personal Communications
    UPPERCASESECURITY=N
    USENPI=N
    PROTOCOL=SNA
    LOCALLUNAME=IYALT1E0          3
    MODENAME=LU62PS               7
    NETNAME=GBIBMIYA.IYCNZCA3     1 . 6
    LUALIASNAMES=N
ENDSECTION
    :::
SECTION DRIVER = SNA
    DRIVERNAME=CCLWNTSN
ENDSECTION
```

Figure 24. 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 eNetwork Personal Communications.
3. Start the CICS Universal Client for Windows NT Version 3.1 on the client workstation, using the `CICSCLI /S=CICSSNA` command. CICSSNA is the name of the server in the client configuration (see Figure 24 on page 22).
4. Check the status of the CICS Universal Client, using the `CICSCLI /L` command. The connection status to the CICS server should show ″Available.″
5. Issue the `CICSTERM /S=CICSSNA` command to install a terminal on the CICS Transaction Server for OS/390
6. If a CICS Universal Client security pop-up appears, enter a valid RACF user ID and password.
7. Run a CICS server transaction, for example, CEMT or CECI.
8. Problems? If the following error appears in the CICS Universal Client error log, CICSCLI.LOG, during connection to eNetwork Personal Communications:

   ```
   CCL4668 SNA node not started, APPC return code X'001B'
   ```

   it is likely that there is a conflict between eNetwork Personal Communications Server and another SNA product installed, Ensure that you have no other SNA products or components of other SNA products or components installed, for example Microsost SNA Server Client, or IBM Communications Server for Windows NT Client.

   You can also check the eNetwork Personal Communications Administrative and PD Aids Log Viewer for error messages.

© Copyright IBM Corp. 1994, 1999

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	= HOLLING (RACF-authorized TSO ID)
ATtachsec	= Verify
Usedfltuser	= Yes for signon incapable terminals; = No for signon incapable terminals, see "Signon capable terminals".

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.

© Copyright IBM Corp. 1994, 1999

Security implementation

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.

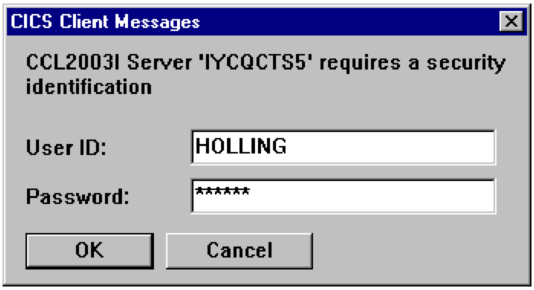
When a user does sign on, the terminal is associated with the userid just authenticated. For transactions attempting to access reosources, security checking is done against the userid associated with the connection and the signed-on user’s userid.

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 23. Link security is initiated when the first ECI, EPI, or CICSTERM request is made on a newly established connection.

If you have not provided a userid and password, CICS Universal Client may request that you enter a valid userid and password in a security pop-up window (see Figure 25).



CCL2003I Server 'IYCQCTS5' requires a security identification

User ID: HOLLING

Password: ******

Figure 25. Example of CICS Universal Client security pop-up window

For more information about the circumstances under which security pop-ups are displayed, see the *CICS Universal Client Administration* book.

To prevent the security pop-up window from appearing you can:

- Specify the CICSCLI /C /U /P options to assign a userid and password to each request sent to the server specified by the /C option.
- Pass the userid and password in the ECI parameter block.

- Specify the CICSCLI /N option to suppress all pop-ups. In this case a security error is returned to the ECI, EPI, or CICSTERM request.
- Ensure that **Enable popups** is not selected in the client configuration.
- Set a default userid and password using the ESI function **CICS_SetDefaultSecurity**.
- Use the Network Provider Interface (NPI), which allows you to sign on to a CICS server using the same user ID and password that you use to log on to Windows NT. In this case, you must enable the **Use NPI security** configuration setting.

Chapter 8. Useful commands and utilities

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

SNA configuration file and verification utility

The SNA configuration file has a file type of .ACG and is stored in the \private subdirectory of your eNetwork Personal Communications directory by default. When you double-click the file in Windows Explorer, the configuration tool is launched.

You can edit or view the .ACG file with an ASCII text editor, however we recommend that you use the configuration tool. If you do manually edit the SNA configuration file, we strongly suggest that you use the SNA Node Configuration Verification utility before using the file for the first time. For more information, see the *eNetwork Personal Communications: System Management Programming* book.

Using aliases

When configuring a product for the first time, it is wise to use the same name for the alias as the real name. For example, make the LU name and the LU alias names the same.

Once you are sure that the configuration is working, you can change the alias names to more meaningful names.

© Copyright IBM Corp. 1994, 1999

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

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

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.

© Copyright IBM Corp. 1994, 1999

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