CICS® Universal Client Configuration

Configuring CICS Universal Client for Windows NT® for Microsoft SNA Server

CICS® Universal Client Configuration

Configuring CICS Universal Client for Windows NT® for Microsoft SNA Server

Contents

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 Microsoft SNA Server Version 4.0 as a SNA gateway.

Communication is through SNA LU6.2 communication provided by Windows NT Client for SNA Server on the client workstation, Microsoft SNA Server Version 4.0 on the gateway, and VTAM on the mainframe server.

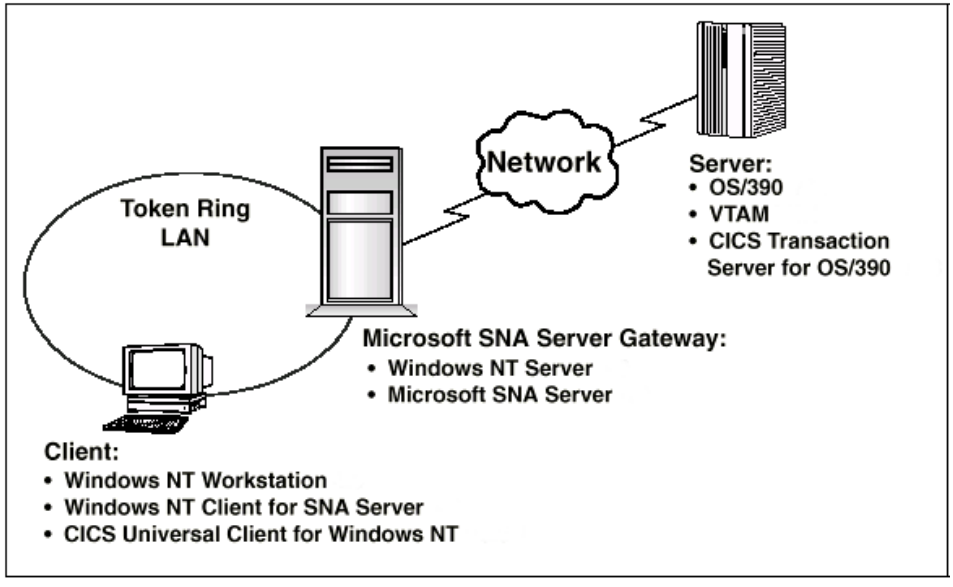

Figure 1. CICS Universal Client for Windows NT connected through MS SNA

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.

The sample configuration information provided in this section does not apply to Microsoft SNA Server 3.0 or earlier versions of the product.

In this document we cover the following topics:

Overview

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 Microsoft SNA server:

- Windows NT Server Version 4.0 (service level 4)
- Microsoft SNA Server Version 4.0 (service level 1)

We used the following software on the client workstation:

- Windows NT Workstation Version 4.0 (service level 4)
- Windows NT Client for SNA Server Version 4.0 (service level 1)
- 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.)

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**
- Microsoft SNA Server
  - Network Name **1**
  - Control Point Name **2**
  - Local Node ID **4**
  - Remote Network Address **5**
  - LU Name **3**
  - Mode Name **7**
- CICS Universal Client for Windows NT
  - Partner LU name, which can be either of:
    - A qualified network name Network **1** .LUName **6**
    - An alias name.
  - Local LU name **3**
  - Mode name **7**

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	Microsoft SNA Server 4.0	Client configuration	Example
1	NETID	—	Network Name	Partner LU name	GBIBMIYA
2	PU	—	Control Point Name	—	SC02234
3	LU	Netname	LU Name	Local LU name	SC02234I
4	XID	—	Local Node ID	—	05D 02234
5	Token Ring destination address	—	Remote Network Address	—	400045121088
6	APPL	APPLID	Remote LU Name	Partner LU name	IYCQCTS5
7	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 **2**, XID **4**, and LU **3** definitions for our Microsoft SNA Server gateway. These are the definitions for the SNA Server 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.

```
SC02234 PU ADDR=01, 2
            IDBLK=05D,IDNUM=02234, 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
*
SC02234I LU LOCADDR=0,DLOGMOD=LU62PS 3
::
```

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

Sample configuration

The LU SC02234I **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.

```
AP26CICS VBUILD TYPE=APPL 6
*
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 **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=IYCQCTS5
     ::
```

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       : SC02234I  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=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 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    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 Microsoft SNA Server, 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 Microsoft SNA Server 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
  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 TS Version 1.3: Sessions definition

Microsoft SNA Server Version 4.0

In this section we describe the steps we used to install and set up the Microsoft SNA Server in our sample configuration. You should install the Microsoft SNA Server on a Windows NT Server Version 4 operating system with Service Level 4.

On the Settings-Control Panel-Add/Remove Programs menu, select **INSTALL** and open `D:\SNA40\I386\SETUP.EXE`.

Follow the installation procedure to install the Microsoft SNA Server product. For details about the installation procedure, refer to your Microsoft SNA Server documentation. When prompted to choose which SNA Server components you want to install, select the **Link services** component.

For our sample configuration we chose the installation options shown in Figure 10 on page 14.

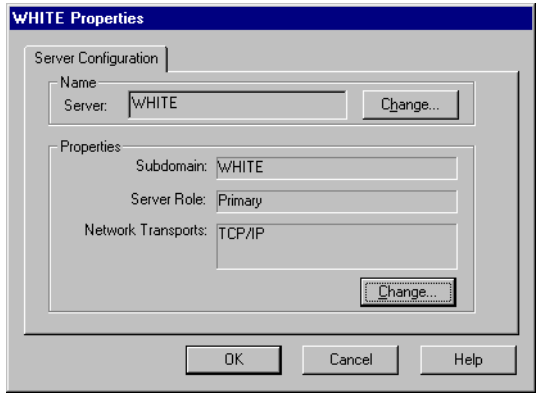

Figure 10. Microsoft SNA Server installation options

Figure 11 shows the Microsoft SNA Server Manager panel we used to set up our sample configuration.

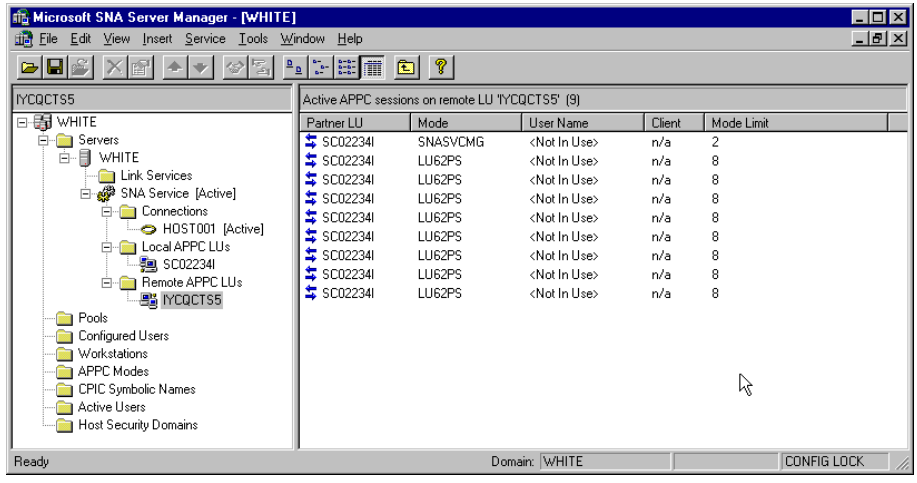

Figure 11. Microsoft SNA Server Manager

To configure the Microsoft SNA Server, follow the steps listed below. To configure each component, you highlight the option on the SNA Server Manager panel with the left mouse button, click the right mouse button, select **New** and then options as appropriate.

1. Right-click the **SNA Service** component, select **New**, then **Link Service**. On the Link Service panel, select **DLC 802.2 Link Service**, and select **OK** on the Properties panel. You will need to install the DLC protocol driver from the Windows NT Server 4.0 installation CD-ROM before you can complete this step.

2. Right-click on **SNA Service** and select **Properties**. On the Properties panel (Figure 12), enter the Network Name **1** and the Control Point Name **2**.

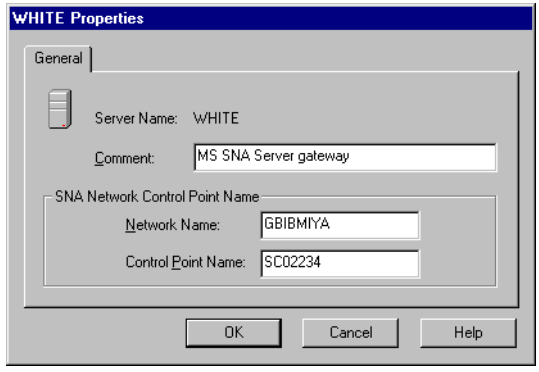

Figure 12. Microsoft SNA Server: Server Properties

3. Right-click on **Connections** (Figure 11 on page 14), select **New**, and then **802.2**. See Figure 13.

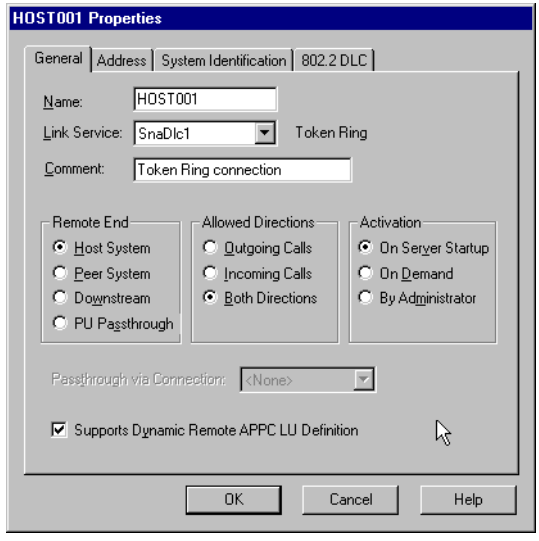

Figure 13. Microsoft SNA Server: Connection Properties

4. On the Connection Properties panel, select the **Address** tab. Enter the Remote Network Address **5** (see Figure 14 on page 16).

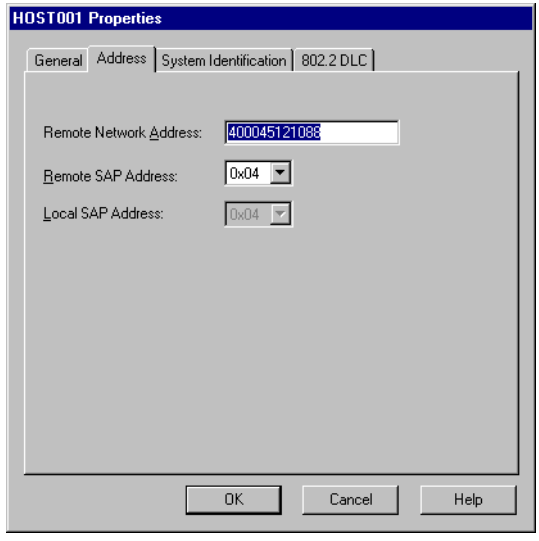

Figure 14. Microsoft SNA Server: Remote Network Address

5. On the Connection Properties panel, select the **System Identification** tab. Enter the Network Name **1**, Control Point Name **2**, and Local Node ID **4** (see Figure 15.

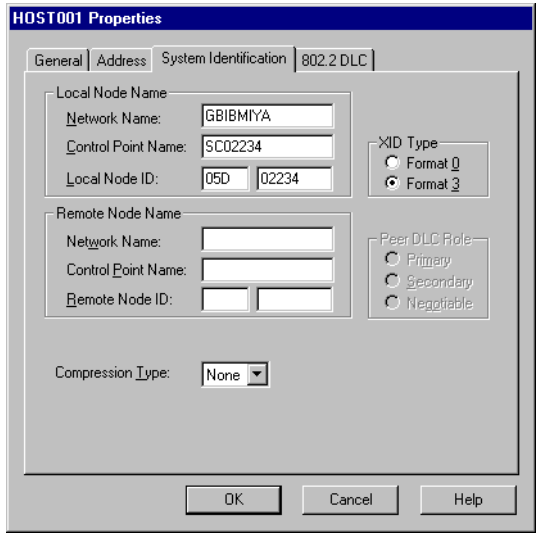

Figure 15. Microsoft SNA Server: Connection Properties - System Identification

6. Right-click on **Local APPC LUs** (Figure 11 on page 14), select **New**, and then **Local LU**. On the Local LU panel specify the Network Name **1**, and the LU Name **3** (see Figure 16).

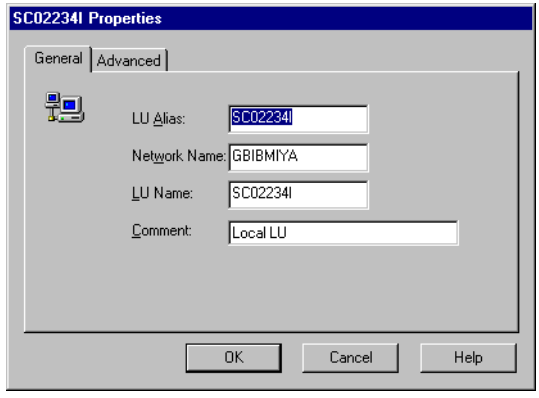

Figure 16. Microsoft SNA Server: Local APPC LU - Properties

7. Right-click on **Remote APPC LUs** (Figure 11 on page 14), select **New**, and then **Remote LU**. On the Remote APPC LU Properties panel specify a Connection name meaningful to the end user, the Network Name **1**, and LU Name **3** (see Figure 17).

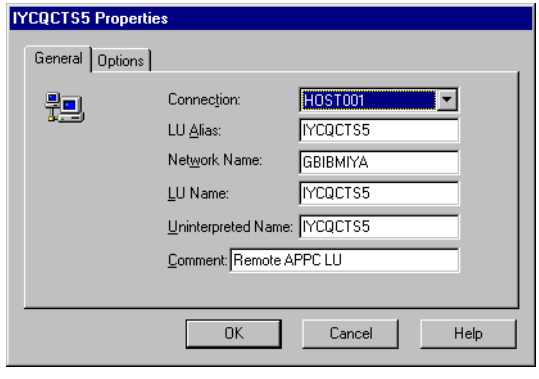

Figure 17. Microsoft SNA Server: Remote APPC LU - Properties

8. Right-click on **APPC Modes** (Figure 11 on page 14), select **New**, and then **Mode Definition**. On the APPC Mode Properties panel specify the ModeName **7** (see Figure 18 on page 18).

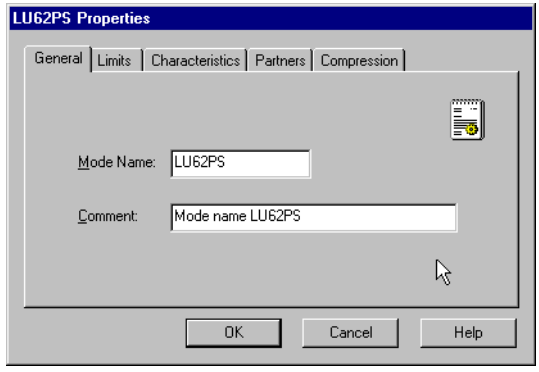

Figure 18. Microsoft SNA Server: APPC Mode Definition

9. On the APPC Mode Properties panel, select the **Limits** tab. Enter session limits for your environment (see Figure 19).

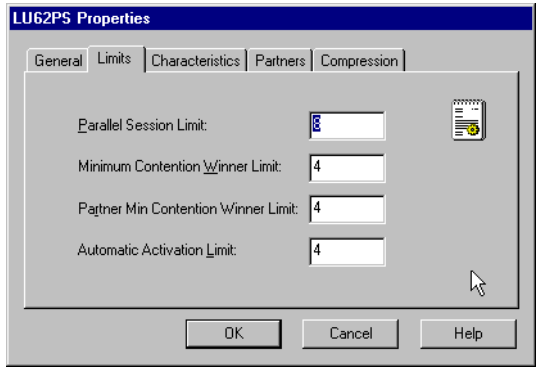

Figure 19. Microsoft SNA Server: APPC Mode Definition - Session Limits

10. Right-click on **APPC Modes** (Figure 11 on page 14), select **New**, and then **Mode Definition**. On the APPC Mode Properties panel specify SNASVCMG (see Figure 20 on page 19).

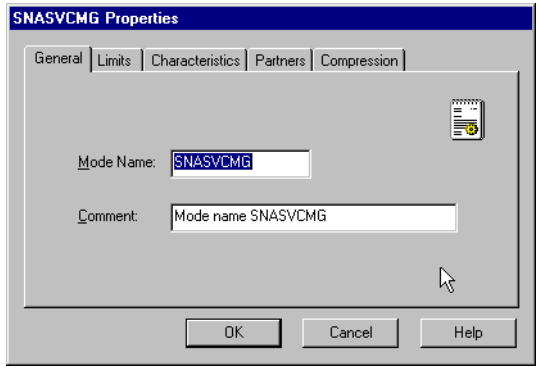

Figure 20. Microsoft SNA Server: APPC Mode Properties - SNASVCMG

11. On the APPC Mode Properties panel, select the **Limits** tab. Enter the session limits shown in Figure 21.

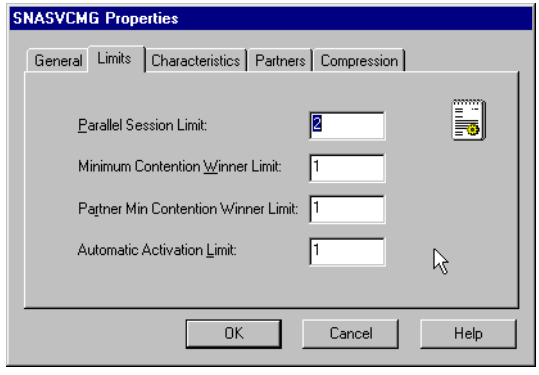

Figure 21. Microsoft SNA Server: APPC Mode Properties - Session Limits

Windows NT Client for SNA Server

Windows NT Client for SNA Server will not work while other SNA products are installed. You must uninstall other SNA products first, including the TCP62 component supplied with the CICS Universal Client for Windows NT.

To configure the Windows NT Client for SNA Server to communicate over TCP/IP to Microsoft SNA Server, follow these steps:

1. Install the Windows NT Client for SNA Server, either from the CD on the client workstation, or by mapping a network drive to the Microsoft SNA Server workstation. We chose the latter option, as recommended by the Microsoft SNA Server documentation.

2. During installation, the Windows NT Client for SNA Server - Select Components panel appears. To install the minimum required code, do not choose any components in this list. Select the **Continue** button to install the base code.
3. During installation, the software detects the communication protocols installed on the client workstation (see Figure 22). Select **TCP/IP** to use TCP/IP communication between the client workstation and the Microsoft SNA Server. Select **Continue** to get to the Client Mode panel.

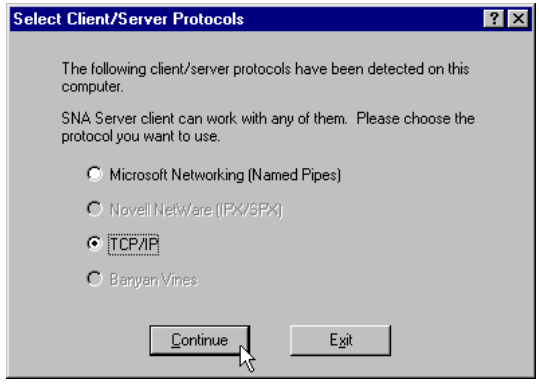

Figure 22. Windows NT Client for SNA Server: Client Configuration

4. The Client Mode panel (see Figure 23) displays a choice of how the client will locate the server. Select the option to locate the server by name. Select **Continue** to get to the Remote Server Names panel.

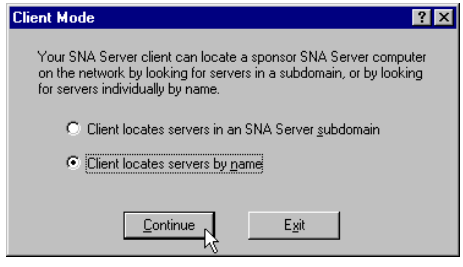

Figure 23. Windows NT Client for SNA Server: Client Mode

5. On the Remote Server Names panel, enter the TCP/IP hostname of the Microsoft SNA Server workstation (see Figure 24 on page 21).

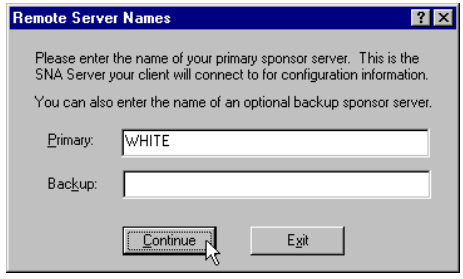

Figure 24. Windows NT Client for SNA Server: Remote Server Names

6. The installation may produce a pop-up to indicate that your workstation is not in the same domain as the Microsoft SNA Server workstation. Enter your user ID and password on the Server Domain Account Information (see Figure 25) window to update the domain account information on the Microsoft SNA Server workstation.

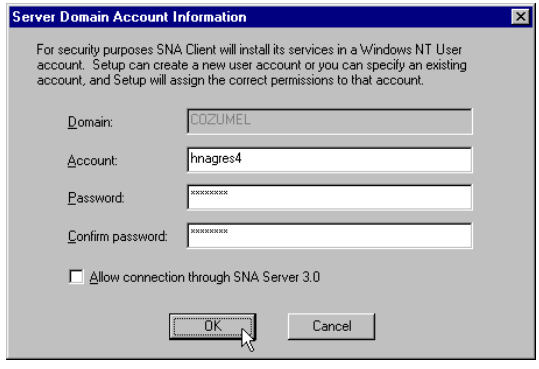

Figure 25. Windows NT Client for SNA Server: Server Domain Account Information

7. Select **OK** to complete the installation.

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 26 on page 23):

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.IYCQCTS5, 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.

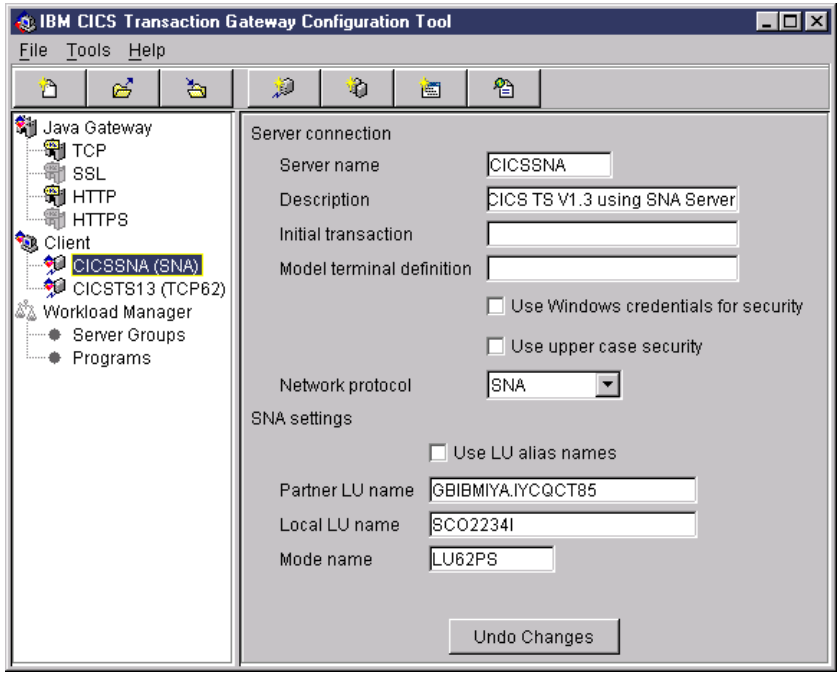

Figure 26. configuration tool settings for SNA Server

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

```
SECTION CLIENT = *
    :::
ENDSECTION
    :::
SECTION SERVER = CICSSNA
    DESCRIPTION=CICS TS V1.3 using SNA Server
    UPPERCASESECURITY=N
    USENPI=N
    PROTOCOL=SNA
    LOCALLUNAME=SCO2234I          3
    MODENAME=LU62PS               7
    NETNAME=GBIBMIYA.IYCQCT85     1 . 6
    LUALIASNAMES=N
ENDSECTION
    :::
SECTION DRIVER = SNA
    DRIVERNAME=CCLWNTSN
ENDSECTION
```

Figure 27. CICS Universal Client: CTG.INI file definitions

CRSR transaction program

CRSR is required if the CICS server supports terminal emulation. It is used to perform automatic transaction initiation (ATI) against the CICS client terminal.

Sample configuration

The CRSR definition is defined to the Microsoft SNA Server through the CCLMSATI utility (see Figure 28). This adds a registry entry for the LU name.

```
C:\Program Files\IBM\CICS Universal Client\bin>cclmsati SC02234I 3
```

Figure 28. CICS Universal Client: CCLMSATI Utility

Refer to the *CICS Universal Client Administration* book for more information.

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 Microsoft SNA Server gateway. The SNA Service status should show "Active".
3. Activate the connection between the Microsoft SNA Server gateway and the CICS Transaction Server for OS/390. You should be able to see the active APPC sessions on the Remote LU.
4. 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 27 on page 23). When the CICS Universal Client is started, it automatically starts the SnaBase service.
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=CICSSNA` command to install a terminal on the CICS Transaction Server for OS/390.
7. If a CICS Universal Client security pop-up appears, enter a valid RACF user ID and password.
8. Run a CICS server transaction, for example, CEMT or CECI.
9. Problems? If the following error appears in the CICS Universal Client error log, CICSCLI.LOG, during connection to the Microsoft SNA Server:

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

   it is likely that there is a conflict between Windows NT Client for SNA Server and another SNA product installed, for example, the TCP62 component. You have to uninstall all other SNA products.

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.

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 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 25. 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 29).

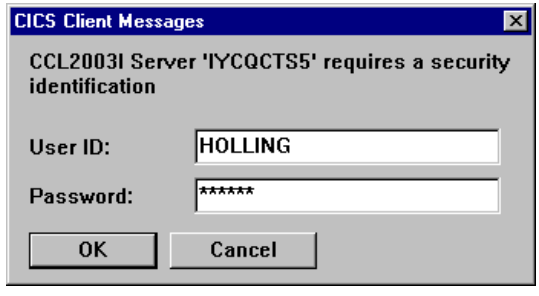

Figure 29. Example of CICS Universal Client security pop-up window

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.

Microsoft SNA Server configuration file

To view the Microsoft SNA Server configuration file, run the command:

```
SNACFG /DISPLAY COM.CFG > com.txt
```

This will pipe the data into the com.txt file. Use the notepad editor to view the com.txt file.

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.

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.

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