CICS® Universal Client Configuration

Configuring CICS Universal Client for Windows NT® for IntranetWare for SAA

CICS® Universal Client Configuration

Configuring CICS Universal Client for Windows NT® for IntranetWare for SAA

Contents

Chapter 1. Overview

In this document we describe how to install and use IntranetWare for SAA with the CICS Universal Client for Windows NT. We cover the installation and configuration of the IntranetWare for SAA gateway and the installation and configuration of the Novell IntranetWare Client for NT on the client workstation. The sample configuration shown in Figure 1 consists of a CICS Universal Client for Windows NT Version 3.1 connecting to a CICS Transaction Server for OS/390 across a network, using IntranetWare for SAA Version 3.0 as a SNA gateway.

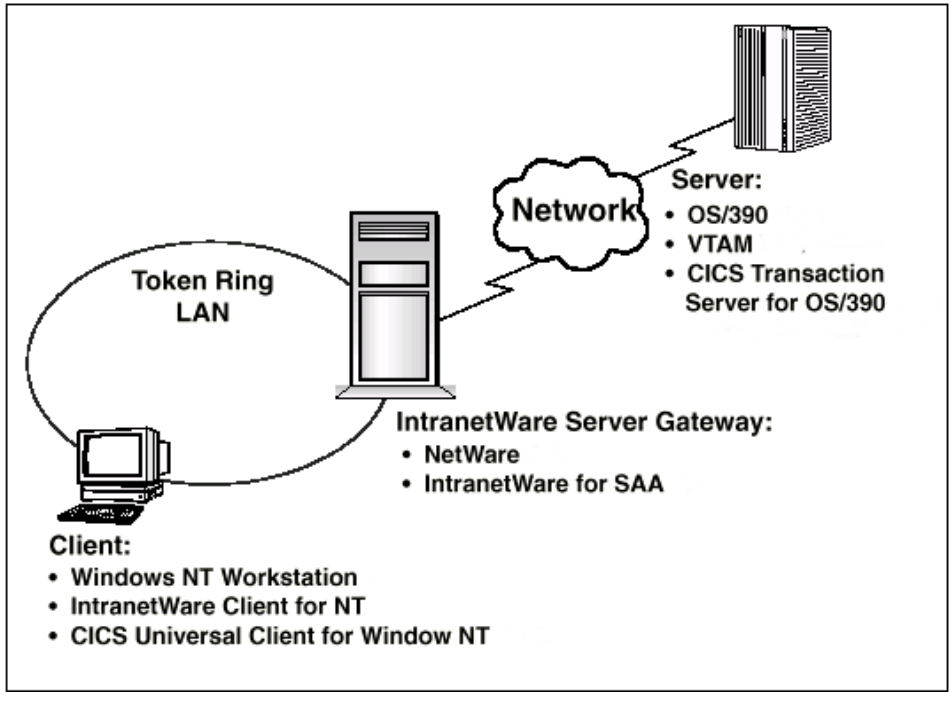

Figure 1. CICS Universal Client for Windows NT connected through IntranetWare for SAA

The information provided in this section does not apply to Novell Netware for SAA Version 2.20 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 Novell NetWare 4.11 network server:

- Novell NetWare Version 4.11 Operating System with Version 6.0 Support pack
- IntranetWare for SAA Version 3.0

We used the following software on the client workstation:

- Windows NT Workstation Version 4.0 (service level 4)
- Novell IntranetWare Client for NT
- 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.)

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

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 definitions for IntranetWare for SAA
  - 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**
- IntranetWare for SAA
  - Network name **1**
  - Local Node ID
    - Block ID.Physical Unit ID **4**
  - Local LU name (Independent LU 6.2) **3**
  - Remote node address **5**
  - Partner LU name **1**.**6**
  - Mode name **7**
- CICS Universal Client for Windows NT
  - Partner LU name **6**
  - Local LU name **3**
  - Mode name **7**

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	IntranetWare for SAA	Client configuration	Example
1	NETID	—	Network name	—	GBIBMIYA
2	PU	—	—	—	IYALR01A
3	LU	Netname	Local LU name	Local LU name	IYALT1A0
4	XID	—	Local Node ID	—	05D 316C3
5	Token Ring destination address	—	Remote node address	—	400045121088
6	APPL	Applid	Partner LU name	Partner LU name	IYCNZCA3
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 on page 10 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.

```
IYALR01A PU ADDR=01,  2
            IDBLK=05D,IDNUM=316C3,  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
*
IYALT1A0 LU LOCADDR=0,DLOGMOD=LU62PS  3
IYALT1A1 LU LOCADDR=0,DLOGMOD=LU62PS
IYALT1A2 LU LOCADDR=0,DLOGMOD=LU62PS
IYALT1A3 LU LOCADDR=0,DLOGMOD=LU62PS
::
```

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

The LU IYALT1A0 **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 on page 11 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 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 on page 12 and Figure 8 on page 12 show the independent LU6.2 connection definitions that we installed on the CICS Transaction Server for OS/390.

Sample configuration

```
OBJECT CHARACTERISTICS                                  CICS RELEASE = 0530
  CEDA View Connection( TLA0 )
   Connection    : TLA0
   Group         : TLA1
   DEscription   :
  CONNECTION IDENTIFIERS
   Netname       : IYALT1A0 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( TLA0 )
 + 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 IntranetWare for SAA you must specify security **ATtachsec = Verify** on your connection definition. It is not necessary to specify SEC=YES as a SIT parameter.

Figure 9 shows the sessions definition required for the sample configuration. You can create the connection and sessions definitions for IntranetWare for SAA by using RDO. The connection and sessions must be defined in the same group, and they must be installed simultaneously. We used Group(TLA1) in our sample configuration.

```
OBJECT CHARACTERISTICS                                    CICS RELEASE = 0530
  CEDA View Sessions( LU62PS )
   Sessions      : LU62PS
   Group         : TLA1
   DEscription   :
  SESSION IDENTIFIERS
   Connection    : TLA0
   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=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

Novell IntranetWare Client for NT

In this section we cover the installation and configuration of the Novell IntranetWare Client for NT on the client workstation.

It is advisable to install the Novell IntranetWare Client for NT on a clean partition so that the networking components are installed at the correct level.

During the installation of the Windows NT Workstation, do not be tempted to try adding the NetWare IPX protocol. This will be added at the correct version level when you install the IntranetWare Client for NT.

To configure Novell IntranetWare Client for Windows NT, follow these steps:

1. Install Windows NT Workstation Version 4.0 with service level 4.
2. Set up the Microsoft Network and select the following components to install:
   - TCP/IP Protocol
   - NetBEUI Protocol

3. Create a Windows NT userid and password with administration and power user authority with the same name as the IntranetWare User Object which you will use when running the CICS Universal Client
4. Install the Novell IntranetWare Client for NT from the supplied CD or from diskettes previously created with the LOAD INSTALL option on the NetWare server.
5. Edit the properties of the Novell IntranetWare Client for Windows NT component, which has now been added to the Settings - Control Panel - Network panel, and add the details shown in Figure 10.

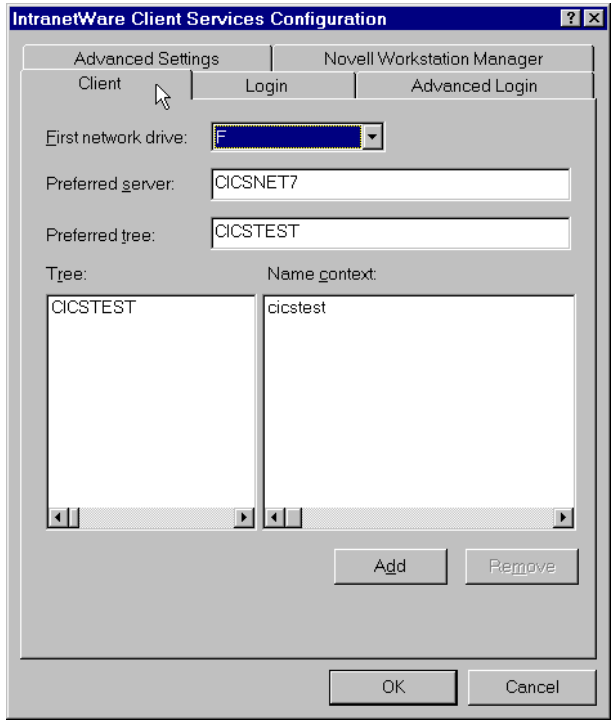

Figure 10. IntranetWare Client Services Configuration panel

6. After rebooting the machine, you should now be able to see your NetWare server on the NetWare Services network and be able to log in to it using your NetWare 4.11 administrator userid and password.

IntranetWare for SAA Version 3.0

Follow the installation procedure to install the IntranetWare for SAA product.

In this section we describe the steps we used to configure IntranetWare for SAA Version 3.0 for our sample configuration.

Figure 11 shows the IntranetWare for SAA Version 3.0 Administrator panel.

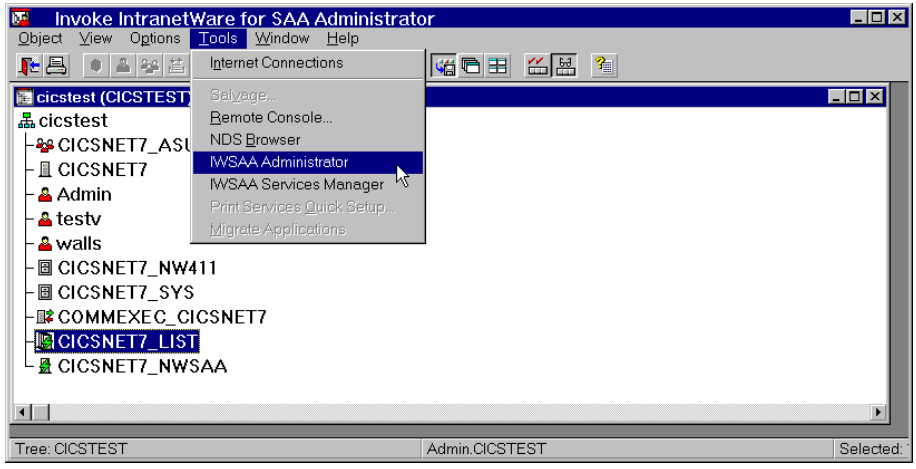

Figure 11. IntranetWare Administrator panel

Select the **IWSAA Administrator** menu option from the Tools pull-down to display the IntranetWare for SAA Server Configuration panel (Figure 12)

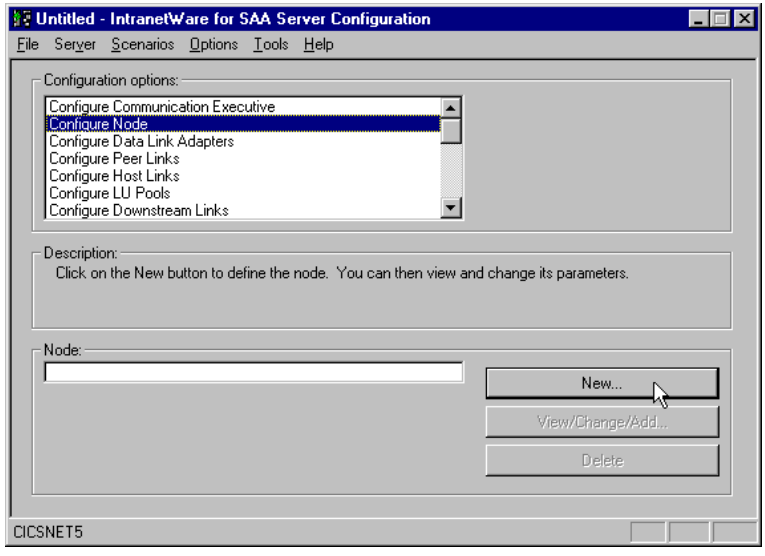

Figure 12. IntranetWare for SAA Server Configuration panel

On the IntranetWare for SAA Server Configuration panel, select **Configure Node** from the Configuration options list box and select the **New...** button to display the Configure the Node panel.

Figure 13 shows the details we entered to configure our node. Enter the Network name **1** for your local SNA network. The value entered for the CP name should be unique to your network. We specified the PU of the IntranetWare for SAA Gateway workstation. The Local Node ID **4** is the XID for the IntranetWare for SAA Gateway workstation.

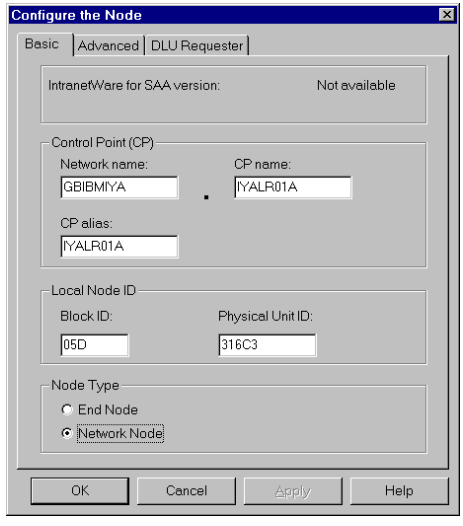

Figure 13. IntranetWare for SAA Configure the Node

Select **OK** to return to the IntranetWare for SAA Server Configuration panel (Figure 12 on page 15).

Now, select **Configure Data Link Adapters** from the Configuration options list box, and **Token Ring** from the Adapters list box. Select **New ...** to create a data link adapter based on the type of adapter for your system. Figure 14 on page 17 shows the values we entered for our sample configuration.

Tip

To find the Adapter name (board name) for your system, run CONFIG from your NetWare Server console.

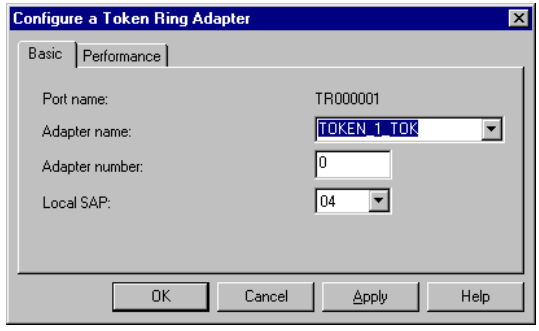

Figure 14. IntranetWare for SAA: Configure a Token Ring Adapter

Select **OK** to return to the IntranetWare for SAA Server Configuration panel (see Figure 12 on page 15).

Now, select **Configure Peer Links** from the Configuration options list box, and Token Ring from the Adapters list box. Select **New ...** to create a peer link.

Figure 15 shows the values we entered to configure a token ring peer Link. In our configuration, the partner node is an immediately adjacent remote node. Therefore, the Remote node address we specified was the MAC address of the adapter belonging to the partner node.

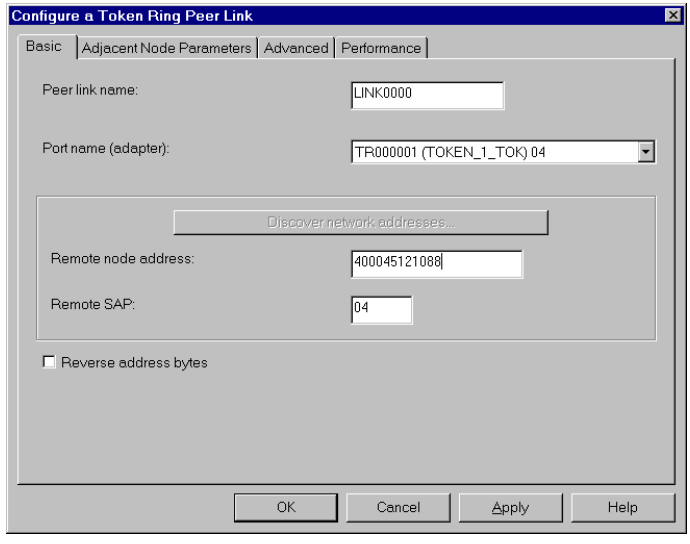

Figure 15. IntranetWare for SAA: Configure a Token Ring Peer Link

Select the **Adjacent Node Parameters** tab. We used the default Adjacent CP type ″Learn″ to allow the system to determine the adjacent node type.

Select **OK** to return to the IntranetWare for SAA Server Configuration panel (see Figure 12 on page 15).

Now, select **Configure Partner LU 6.2** from the Configuration options list box. Select **New ...** to create a partner LU6.2 definition.

Figure 16 shows the Network name **1** and Partner LU name **6** we entered for our partner LU6.2 definition.

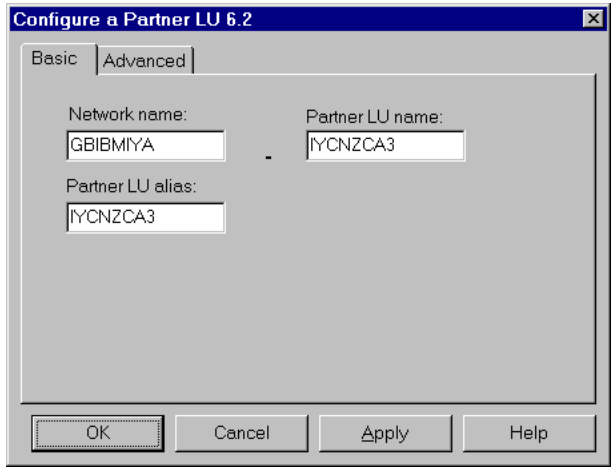

Figure 16. IntranetWare for SAA : Configure a Partner LU6.2 - Basic

Select the **Advanced** tab on the Configure a Partner LU 6.2 panel. and uncheck **Conversation security support** (see Figure 17 on page 19).

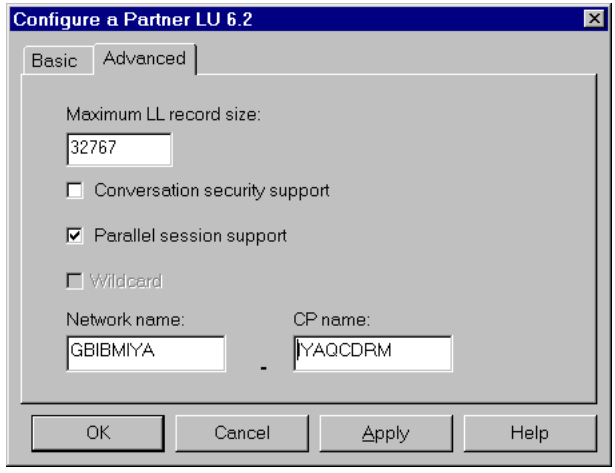

Figure 17. IntranetWare for SAA: Configure a Partner LU6.2 - Advanced

Select **OK** to return to the IntranetWare for SAA Server Configuration panel (Figure 12 on page 15).

Now, select **Configure Modes** from the Configurations option list box. Select **New ...** to create a mode definition. On the Basic panel (see Figure 18 on page 20) enter the Mode name **7** and session values for your configuration.

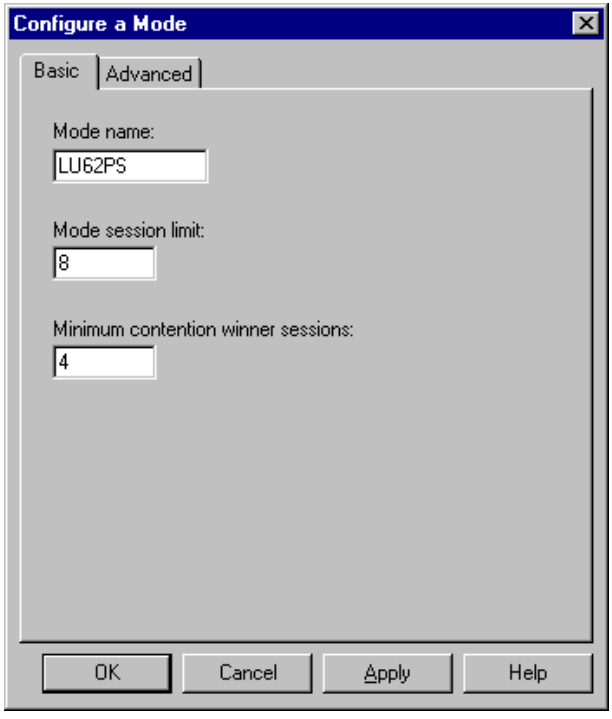

Figure 18. IntranetWare for SAA: Mode Definition - Basic

Figure 19 on page 21 shows the values we entered when selecting the Advanced tab of the Configure a Mode panel.

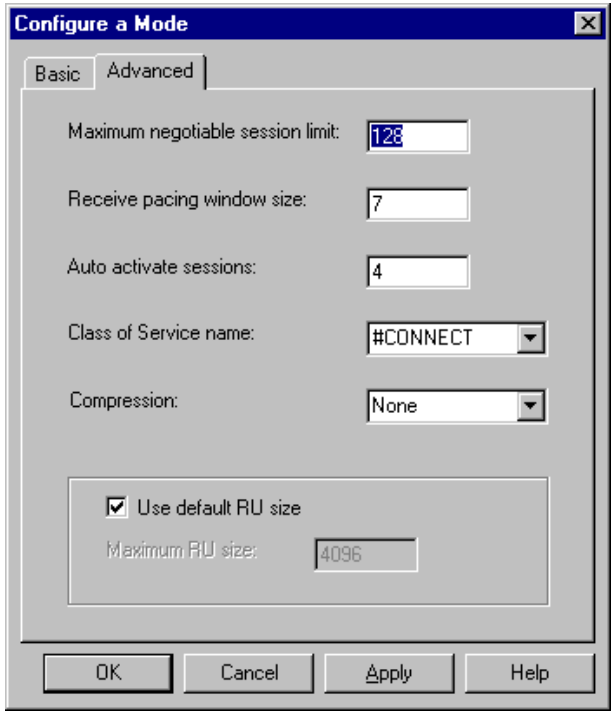

Figure 19. IntranetWare for SAA: Mode Definition - Advanced

Select **OK** to return to the IntranetWare for SAA Server Configuration panel (Figure 12 on page 15).

Now, select **Configure Independent LU 6.2** from the Configuration options list box. Select **New ...** to create an independent LU6.2 definition.

Enter the Local LU name **3** of your client workstation. For simplicity we entered the same value for our Local LU alias name as for our Local LU name (see Figure 20 on page 22).

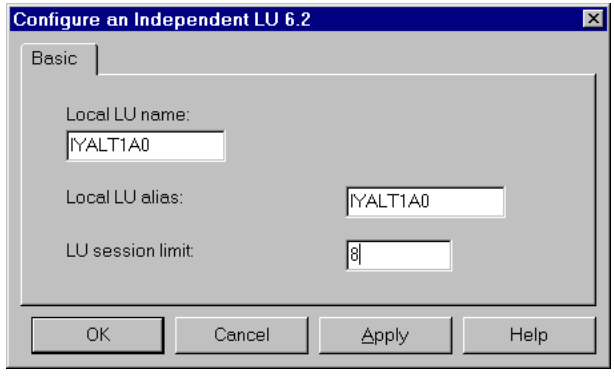

Figure 20. IntranetWare for SAA: Configure an independent LU 6.2

Once you have entered your values, save the IWSAA file. To save the IWSAA file to the NetWare gateway server:

1. On the IntranetWare for SAA Server Configuration panel select the Server pull-down (see Figure 21.

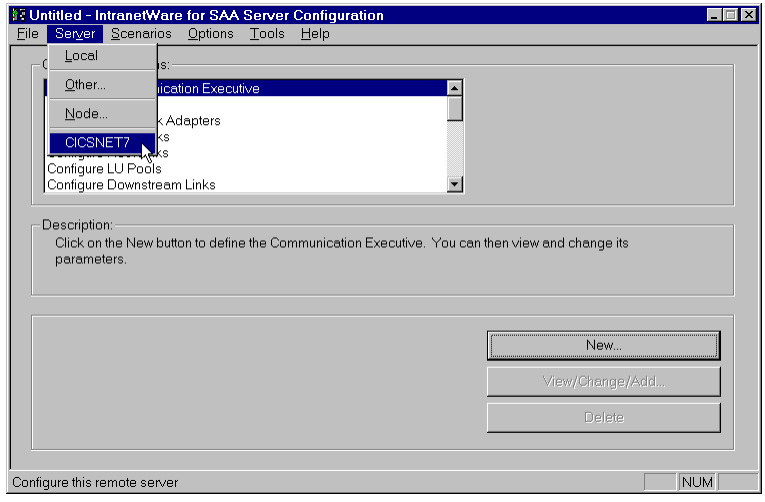

Figure 21. IntranetWare for SAA: Saving your Configuration

2. From the **Server** pull-down, select the name of the remote Netware gateway server. For our sample configuration we used the name CICSNET7.
3. Select the **File** pull-down, then **Save**, to save the configuration for CICSNET7 as a .pcg file.

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 **Client** configuration setting (see Figure 22 on page 24):

Maximum servers
This value specifies the maximum number of servers that can be accessed concurrently from the client. Set this value to 10.

You need to define the following **Server** configuration settings (see Figure 23 on page 25):

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 6
The LU Name of the server as it is known to the APPC configuration at the CICS Universal Client. In our example we used an alias name, IYCNZCA3, see the description of **Use LU Alias names** below.

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.

The Local LU name is the LU name of the gateway machine, not of the client workstation.

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.

LU Alias names enable you to specify the LU alias of the gateway machine, rather than the actual LU name. In our sample configuration we specified the same name for the LU as the LU alias, so no benefit is gained.

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

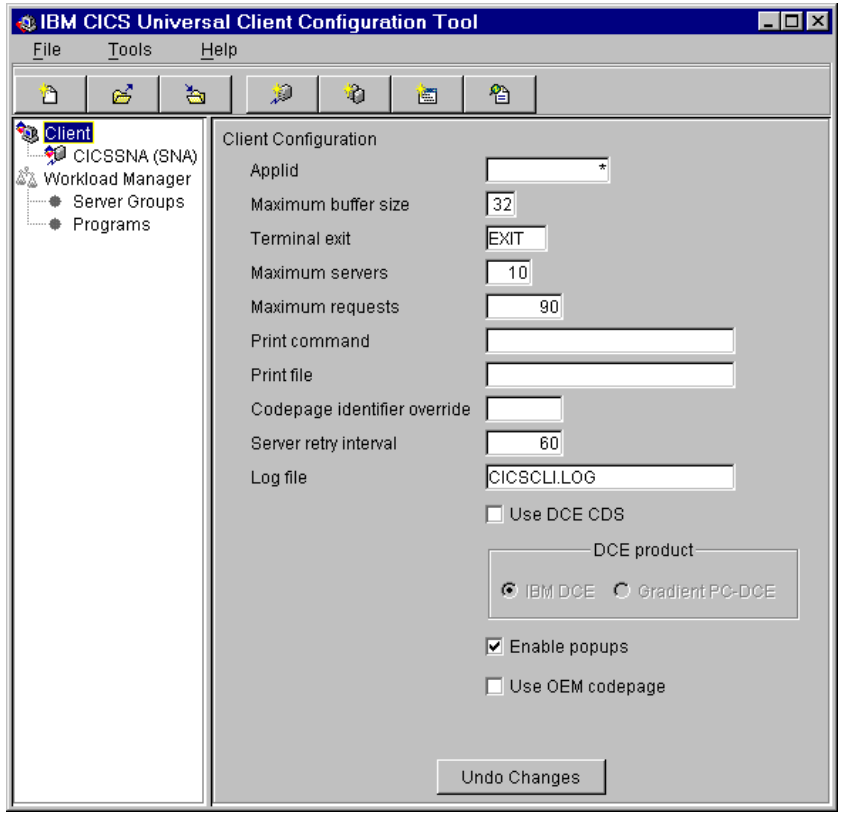

Figure 22. Configuration tool Client settings for IntranetWare for SAA

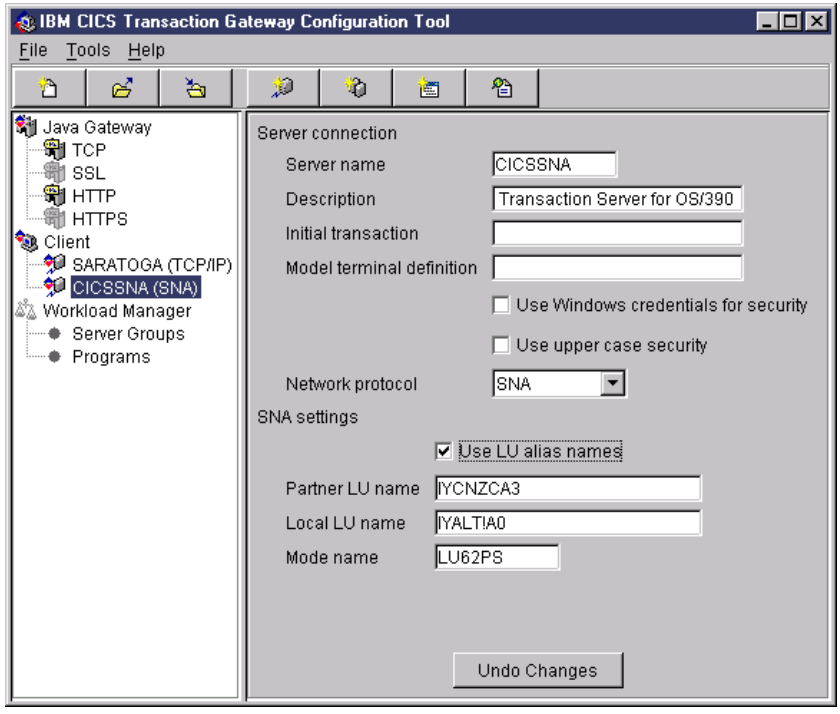

Figure 23. Configuration tool Server settings for IntranetWare for SAA

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

```
SECTION CLIENT = *
    MAXSERVERS=1
    :::
ENDSECTION
    :::
SECTION SERVER = CICSSNA
    DESCRIPTION=Transaction Server for OS/390 via IWSAA30
    UPPERCASESECURITY=N
    PROTOCOL=SNA
    LOCALLUNAME=IYALT1A0          3
    MODENAME=LU62PS               7
    NETNAME=IYCNZCA3              6
    LUALIASNAMES=Y
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:

Follow these steps to test your configuration:

1. Start the CICS Transaction Server for OS/390.
2. Power on the Novell IntranetWare for SAA Gateway workstation and ensure that your node has been updated with your configuration file and you have established a connection with IntranetWare for SAA before proceeding to step 2.
3. Power on the client workstation. Ensure that the network status shows ″Ready.″
4. On the client workstation, log in to Novell Directory Services, using your Netware Administrator user ID and password.
5. On the client workstation, open the NetWare Administrator panel.
6. Select the **Tools** pull-down and double-click on the **IWSAA Services Manager.**
7. Wait for the ″Server is connected″ message to appear
8. From the **Server** pull-down select **Link/Server** Information to display information about your link to CICS for OS/2. The Link status will show ″Disconnected.″
9. On the IntranetWare for SAA Services Manager - Link Information panel, select the **Link** pull-down. Select **Activate**.
10. Ensure that the Link status shows ″Connected″ (see Figure 25 on page 28).

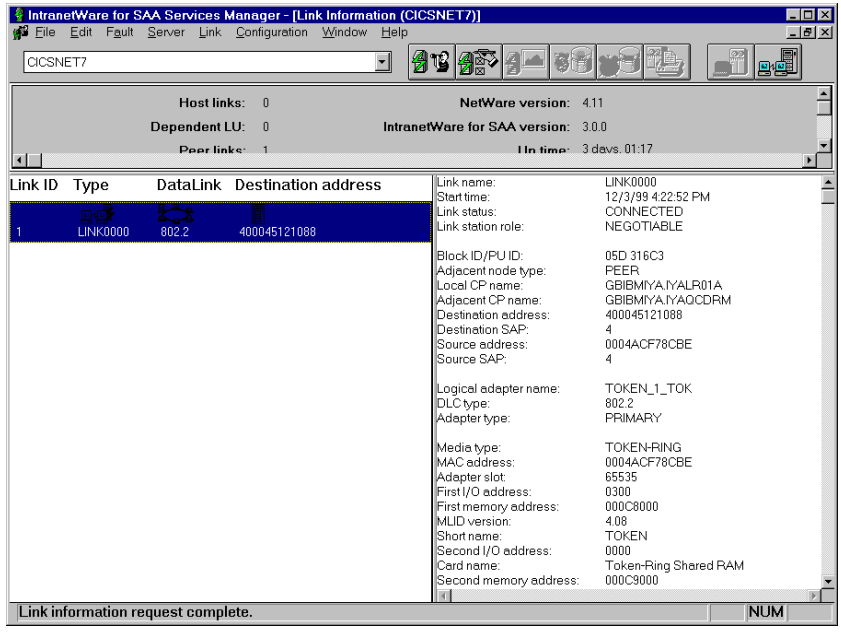

Figure 25. IntranetWare for SAA Services Manager - Link Status: Connected

11. Start the CICS Universal Client for Windows NT using the command `CICSCLI /S=CICSSNA`.
12. On the CICS Universal Client for Windows NT use the `CICSCLI /L` command to check that the status of the connection shows ″Available″.
13. Run an ECI, EPI, or CICSTERM request to confirm that your connection to the server is working.

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 27. 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 26).

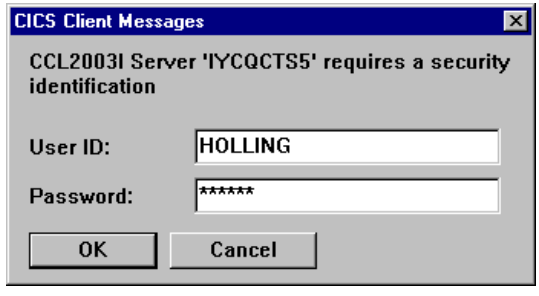

Figure 26. Example of CICS Universal Client security pop-up window

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.

IntranetWare for SAA Version 3.0

The following commands are relevant to IntranetWare for SAA Version 3.0:

MAC address of NetWare Server

To find the MAC address of the NetWare server, run the config command on the NetWare server console.

Token-ring adapter name

To find the name of the token-ring adapter, run the config command on the NetWare server console. The name of the adapter is shown as the Board Name for Frame Type TOKEN-RING.

SNA configuration file

If you want to update the NetWare server SNA configuration file (.pcg), at the Netware server console run the `unload iwsaa` command and then `load iwsaa` to activate the changes. If you want to run a different configuration file, run the `load iwsaa config=`*`filename`*`.pcg` command.

Netware Server console

To view the Netware server console messages, run the `load inetcfg` command and select the **View Configuration** option.

To view the Communication Services Status, run the `csstatus` command at the NetWare server console.

To toggle between the NetWare server console screens, press CTRL-ESC or ALT-ESC.

If you want to view the NetWare server console from the NetWare client workstation, run the RCONSOLE.EXE utility. To exit from this utility, press ALT-F2.

Log and trace utilities

To view the communication services event log (audit), run the `APPNTRC FLUSH` command. This creates an event PD.log in the `\\SYS:\SYSTEM\NWSAA` directory. Use WORDPAD to view the event PD.log.

To run a SNA trace while testing your configuration:

1. From the IntranetWare for SAA Services Manager - Link Information panel, select the **Server** pull-down. Select the **Start Global Trace** option. On the Start Global Trace pop-up window, select **OK** to start the trace.

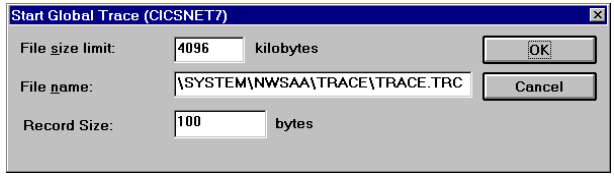

Figure 27. IntranetWare for SAA Services Manager: Global Trace

2. Run your test scenario.
3. To stop the trace, select the **Server** pull-down. Select the **Stop Traces** option. In the Stop Trace pop-up window, select the **Stop Trace** button, then close the panel.
4. Format the trace, using the IWFORMAT utility. This utility resides in the \SYSTEM\NWSAA\TRACE directory. The format of the command is:

   `IWFORMAT` *`trace input filename trace output filename`*

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.