CICS® Universal Client Configuration

IBM

Configuring CICS Universal Client for Windows NT® for TCP62

CICS® Universal Client Configuration

Configuring CICS Universal Client for Windows NT® for TCP62

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. Communication is through TCP62 provided with the CICS Universal Client for Windows NT on the client workstation and AnyNet® provided with VTAM on the mainframe server.
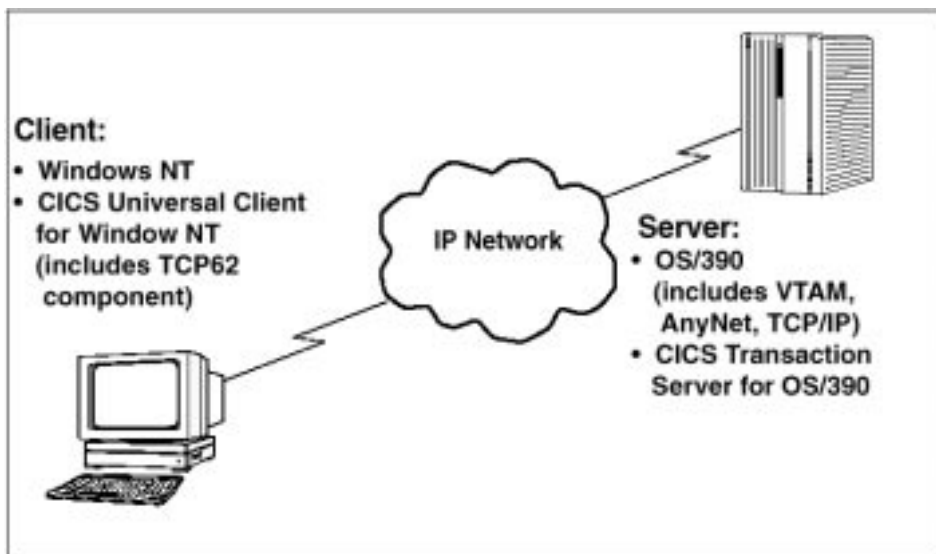
Figure 1. CICS Universal Client for Windows NT to CICS TS through TCP62

To understand how TCP62 works, refer to the *CICS Universal Client Administration* book for your platform, and to *Revealed! CICS Transaction Gateway with More CICS Clients Unmasked.*

The TCP62 component is provided with the CICS Universal Client for Windows NT so you do not have to configure TCP62 on the client workstation.

For the sample configuration we chose to autoinstall an LU6.2 parallel connection rather than define a static definition. Combined with the ability to dynamically create VTAM logical units (LUs) and control points (CPs), autoinstall is advantageous as it enables you to use the same CTG.INI configuration file for all workstations without having to define multiple entries in VTAM and CICS.

Overview

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
- "Chapter 5. Sample configuration" on page 9 of:
  - OS/390
  - VTAM
  - AnyNet
  - CICS Transaction Server for OS/390 Version 1.3
  - CICS Universal Client for Windows NT Version 3.1
  - TCP/IP HOSTS file on workstation
- "Chapter 6. Testing your configuration" on page 19
- "Chapter 7. Security implementation" on page 21
- "Chapter 8. Useful commands and utilities" on page 25

Chapter 2. Software checklist

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

We used the following software on the CICS server:

- OS/390 Version 2.6
  - Includes VTAM Version 4.5
    - Includes AnyNet feature
  - Includes IBM TCP/IP for OS/390
- 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)
- CICS Universal Client for Windows NT Version 3.1
  - Includes TCP62 component
- 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.

- OS/390
  - TCP/IP address and hostname
- AnyNet
  - TCP Major Node
  - DNSUFX **1**
  - Port
- VTAM
  - NETID **2**
  - APPL **3**
  - LogMode **4**
- CICS Transaction Server for OS/390
  - ISC System Initialization Table (SIT) override
  - Applid **3**
  - DFHISC group
  - Modename in the LU6.2 sessions autoinstall template CBPS **4**
- CICS Universal Client for Windows NT
  - Fully qualified CP name or template
  - IP address mask for CP name (optional)
  - Anynet domain name suffix **1**
  - Partner LU name **2** . **3**
  - Local LU name or template
  - IP address mask for LU name template (optional)
  - Mode name **4**
- TCP/IP HOSTS file on client workstation
  - IP_address NetName.NetWork.DomainNameSuffix **3** . **2** . **1**

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: CICS Universal Client for Windows NT: TCP62

Ref: Key	VTAM	CICS Transaction Server	Client configuration	TCP/IP HOSTS File	Example
1	DNSUFX	—	Anynet domain name suffix	DomainNameSuffix	hursley.ibm.com
2	NETID	—	Partner LU name	Network	GBIBMIYA
3	APPL	Applid	Partner LU name	NetName	IYCQCTS5
4	LOGMODE	Modename	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.

OS/390 TCP/IP

The TCP/IP address and hostname are defined to the OS/390 TCP/IP in the PROFILE.TCPIP and TCPIP.DATA data sets. For the sample configuration, 9.20.101.6 is the TCP/IP address of our OS/390 system, and winmvs26 is our TCP/IP hostname. Refer to *IBM TCP/IP MVS: Customization and Administration Guide Version 3.2* for more information about configuring TCP/IP on OS/390.

AnyNet

In this section we present the AnyNet definitions for the server.

TCP Major Node

Figure 2 shows the TCP Major Node definition used in our configuration. The TCP Major Node defines the AnyNet interface between TCP/IP and VTAM. This definition specifies the domain name suffix, DNSUFX **1**, and the TCP protocol port number that VTAM uses to support SNA sessions over an IP network. All nodes that establish SNA sessions over an IP network must use the same port number. The default value is 397 and has been registered with the Internet Activities Board (IAB).

Refer to *VTAM AnyNet Guide to SNA over TCP/IP* for more information about AnyNet.

```
ANYTCP    VBUILD TYPE=TCP,                          X
                 CONTIMER=25,                        X
                 DGTIMER=40,                         X
                 DNSUFX=HURSLEY.IBM.COM,             X  1
                 EXTIMER=5,                          X
                 IATIMER=60,                         X
                 PORT=397,                           X
                 TCB=10,                             X
                 TCPIPJOB=TCPIP
ANY1GRP   GROUP ISTATUS=ACTIVE
ANY1LINE  LINE  ISTATUS=ACTIVE
ANY1PU    PU    ISTATUS=ACTIVE
```

Figure 2. AnyNet: TCP Major Node definition

Sample configuration

CDRSC definitions

The CDRSC defines the remote client and instructs VTAM to route any session requests through the TCP/IP physical unit (PU). In our sample configuration we dynamically generated CDRSC definitions through a key and template defined in the client configuration, (see "Dynamic CP name generation" on page 16). Therefore you do not have to define a CDRSC major node.

VTAM

In this section we present the VTAM definitions for the server.

DYNLU

To dynamically allocate CDRSC definitions, specify DYNLU=YES as a startup option for VTAM. This parameter saves you the need to define multiple static CDRSC definitions within VTAM. The CDRSC names are dynamically generated from the **CP name** and **IP address mask for CP name** client configuration settings, along with the IP address of the client machine. See "Dynamic CP name generation" on page 16 for more details.

NETID

You specify the NETID **2** for VTAM in your VTAM start procedure. For the sample configuration, specify NETID=GBIBMIYA.

APPL

Figure 3 shows the VTAM APPL **3** definition required for the sample configuration. Because TCP62 supports only LU6.2 parallel sessions, specify PARSESS=YES.

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

Figure 3. VTAM: APPL definition

LogMode

Figure 4 on page 11 shows the LogMode **4** required for the LU6.2 parallel sessions.

```
LU62PS   MODEENT LOGMODE=LU62PS,
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'0602000000000000000122F00'
```

Figure 4. VTAM: LogMode definition for LU6.2 parallel sessions

CICS Transaction Server for OS/390

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

System Initialization Table parameters

Figure 5 shows the SIT parameters to enable intersystem communication (ISC) and to define the CICS region APPLID.

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

Figure 5. CICS Transaction Server SIT definitions: ISC and APPLID

Autoinstall of LU6.2 connection

The autoinstall control program, DFHZATDY, is used in conjunction with the APPC autoinstall template for parallel sessions secondary (CBPS) to dynamically create an LU6.2 connection. The same program also automatically releases and uninstalls the connection once all sessions are released. By default, the CPBS sessions definition, found in group DFHAI62, uses a blank modename. As groups that start with DFH should not be altered, we copied this group as AXHAI62, altered the CBPS definition to have a modename of LU62PS **4** , and changed the MAXIMUM sessions option to Max(8,1). The second value in the number of sessions specifies that the CICS server is to have one contention winner only. This value is for CNOS (change number of sessions) purposes and to enable START requests to be initiated by the server to the client. A value of 1 is recommended to ensure that START requests are shipped serially from the server to the client and thereby avoid committing all available sessions to START requests.

Sample configuration

Figure 6 shows our altered APPC autoinstall template for parallel sessions.

```
 CEDA  View Sessions( CBPS    )
  Sessions      : CBPS
  Group         : AXHAI62
  DEscription   : APPC Autoinstall template for parallel session
 SESSION IDENTIFIERS
  Connection    : CBPS
  SESSName      :
  NETnameq      :
  MOdename      : LU62PS
 SESSION PROPERTIES
  Protocol      : Appc            Appc ! Lu61 ! Exci
  MAximum       : 008 , 001       0-999
  RECEIVEPfx    :
  RECEIVECount  :                 1-999
  SENDPfx       :
  SENDCount     :                 1-999
  SENDSize      : 04096           1-30720
  RECEIVESize   : 04096           1-30720
      ::
```

Figure 6. APPC autoinstall template CBPS for parallel sessions

To activate autoinstall control program DFHZATDY, you can issue the CICS
CEMT command shown in Figure 7.

```
CEMT SET AUTOINSTALL PROGRAM(DFHZATDY)

STATUS:  RESULTS - OVERTYPE TO MODIFY
  Aut Max( 100 ) Progr( DFHZATDY ) Cur(000)    Ena      NORMAL
```

Figure 7. Results of CEMT SET AUTOINSTALL PROGRAM(DFHZATDY)

Alternatively you can add a SIT override to your CICS JCL (see Figure 8).

```
    ::

AIEXIT=DFHZATDY

    ::
```

Figure 8. CICS Transaction Server SIT definition: AIEXIT

CICS Universal Client for Windows NT Version 3.1

You use the CICS Universal Client's configuration tool to define the settings
for TCP62 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 11 on page 15 and Figure 12 on page 17).

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, TCP62.

Partner LU name `2`.`3`
> The LU Name of the server as it is known to the APPC configuration at the CICS Universal Client. This must be a qualified 17-character name, as in our example, GBIBMIYA.IYCQCTS5.

Local LU name or template
> The name of a local LU to be used when connecting to the server. You can enter a real LU name or a template for the name of a local LU to be used when connecting to the CICS server.
>
> If you enter a template, you must fill in the **IP address mask for LU name template** field.
>
> See "Dynamic LU name generation" on page 16 for more information.

IP address mask for LU name template
> An IP address mask in most-significant-byte-first order. This must be a hexadecimal number, as in our example FFFFFF80.

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

The settings on the **Common TCP62 settings** tab are as follows:

Fully qualified CP name or template
> A fully-qualified CP name, or a template for the fully-qualified CP name, of the node to be started.
>
> If you enter a template, as in our sample configuration, you must fill in the **IP address mask for CP name (optional)** field.
>
> See "Dynamic CP name generation" on page 16 for more information.

IP address mask for CP name
> An IP address mask in most-significant-byte-first order. This must be a hexadecimal number, as in our example FFFF8080.

Sample configuration

Anynet domain name suffix **1**

The AnyNet domain name suffix. This parameter is used with the partner (Partner LU name) to determine the IP address of the host associated with that LU.

On the **Advanced TCP62 settings** tab you can leave the settings with their default values.

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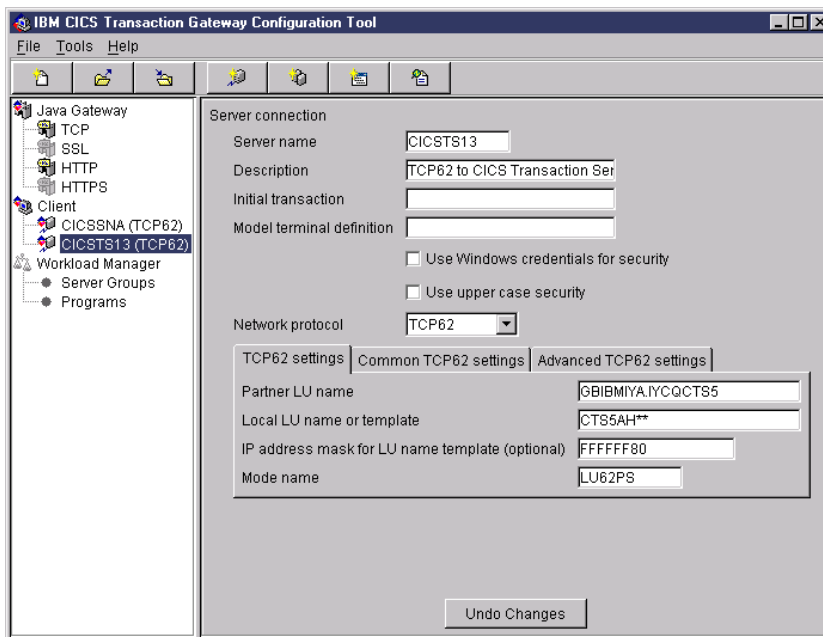

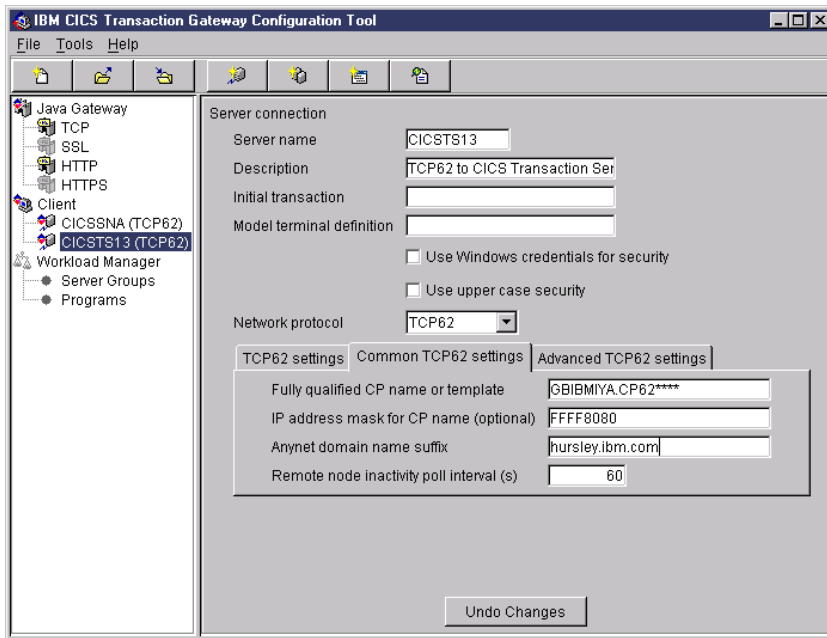*Figure 9. TCP62 settings in configuration tool*

Figure 10. Common TCP62 settings in configuration tool

Figure 11 shows an excerpt from the resultant CTG.INI file.

```
SECTION CLIENT = *
    CPNAME=GBIBMIYA.CP62****
    CPIPADDRESSMASK=FFFF8080
    DOMAINNAMESUFFIX=hursley.ibm.com              1
    :::
ENDSECTION
    :::
SECTION SERVER = CICSTS13
    DESCRIPTION=TCP62 to CICS Transaction Server
    :::
    LOCALLUNAME=CTS5AH**
    LUIPADDRESSMASK=FFFFFF80
    SNAMAXRUSIZE=1024
    SNASESSIONLIMIT=8
    MODENAME=LU62PS                              4
    SNAPACINGSIZE=8
    NETNAME=GBIBMIYA.IYCQCTS5                    2 . 3
    PROTOCOL=TCP62
ENDSECTION
    :::
SECTION DRIVER = TCP62
    DRIVERNAME=CCLTCP62
ENDSECTION
```

Figure 11. CICS Universal Client CTG.INI file definitions

Sample configuration

The *CICS Universal Client Administration* book for your platform provides definitions of the parameters in the CTG.INI file.

Dynamic LU name generation

With dynamic name generation for the Local LU name, you can use the same CTG.INI file on all client machines because different Local LU names are generated on the basis of the IP address of the client machine. Therefore you do not have to define multiple LUs within VTAM.

In our configuration, the Local LU name of CTS5AH** indicates that a name must be dynamically generated to replace the two template replacement characters, that is, asterisks (*). Using the Local LU name, IP Address Mask, and the workstation IP address, the algorithm creates a Local LU name of CTS5AH38. If several hundred clients will be using dynamic LU name generation to connect to the server, you should have more template replacement characters in your Local LU name, for example, CTS5****.

Dynamic CP name generation

You can dynamically generate CP names with an algorithm similar to that for dynamic LU name generation (see "Dynamic LU name generation"). Using the CP name, IP address mask for the CP name, and the workstation IP address, a CP is dynamically generated within VTAM. Therefore you do not have to define multiple CPs to VTAM. In our configuration the CP name of GBIBMIYA.CP62**** indicates that a name must be dynamically generated to replace the four template replacement characters, that is, asterisks (*). If several hundred clients will be using dynamic CP name generation, you should have more template replacement characters in your CP name, for example, GBIBMIYA.CP******. The NETID **2** must not contain any template replacement characters.

TCP/IP HOSTS file

In this section we present the definition required for the TCP/IP HOSTS file. The definition maps the IP address of the OS/390 system to the generated IP name. The IP name is generated by concatenating the NetName **3**, the Network name **2**, and the DomainNameSuffix **1**.

Figure 12 on page 17 shows the TCP/IP HOSTS file definition we used for our configuration. Note the order of the parameters. The IP address of the OS/390 system is first. After one or more spaces, the NetName **3** precedes the Network **2** name, which in turn precedes the DomainNameSuffix **1**.

```
OS/390                      Generated
IP address                  IP name

9.20.101.6      IYCQCTS5.GBIBMIYA.hursley.ibm.com

                NetName  Network  DomainNameSuffix
                  3        2           1
```

Figure 12. TCP/IP HOSTS file definition

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. Check that autoinstall control program DFHZATDY is available (see "Autoinstall of LU6.2 connection" on page 11).
3. Start the CICS Universal Client for Windows NT using the `CICSCLI /S=CICSTS13` command. (CICSTS13 is the name of server in the client configuration, see Figure 11 on page 15.)
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=CICSTS13` command to install a terminal on the CICS Transaction Server for OS/390.
6. Run a CICS server transaction, for example, CEMT or CECI.

In the sample configuration, the CTG.INI definition dynamically creates an LU with netname CTS5AH38, and sample autoinstall control program DFHZATDY dynamically creates a connection name of AH38 by using the last characters of the netname. The CICS server CEMT command displays the netname and connection dynamically created and CBPS, the autoinstall template for parallel sessions (see Figure 13).

```
CEMT INQ CONNECTION

STATUS:  RESULTS - OVERTYPE TO MODIFY
 Con(AH38) Net(CTS5AH38)     Ins Acq Vta Appc
 Con(CBPS) Net(TMPLATE1)     Ins Rel Vta Appc
```

Figure 13. CICS TS Version 1.3: display of dynamically generated connection

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 19. 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 14).
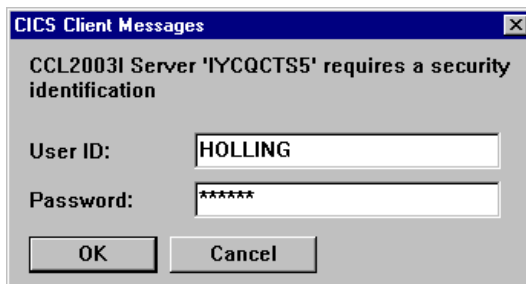

Figure 14. Example of CICS Universal Client security pop-up window

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.

Security implementation

Chapter 8. Useful commands and utilities

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

TSO VTAM commands from SDSF

The following commands are entered from system display and search facility (SDSF) on TSO:

Display TCPIP status

The display command, `d tcpip`, indicates whether TCP/IP is active (see Figure 15).

```
D TCPIP
EZAOP50I TCPIP STATUS REPORT 931
COUNT   TCPIP NAME   VERSION   STATUS
-----   ----------   -------   -------------------------------
    1   TCPIP        CS V2R5   ACTIVE
*** END TCPIP STATUS REPORT ***
EZAOP41I 'DISPLAY TCPIP' COMMAND COMPLETED SUCCESSFULLY
```

Figure 15. SDSF: Display TCPIP status

Display AnyNet PU state

The display command, `d net,id=any1pu,e`, shows the state of the AnyNet PU (see Figure 16 on page 26). For AnyNet to work, the status must be ACTIV. The following parameters are also of interest: CP NETID **2** shows the network name, DYNAMIC LU=YES confirms that dynamic LU generation is enabled, MAJNOD shows the TCP Major Node, and LOGICAL UNITS: indicates that our dynamically generated LU, CTS5AH38, is active.

Useful commands and utilities

```
D NET,ID=ANY1PU,E
IST097I DISPLAY ACCEPTED
IST075I NAME = ANY1PU, TYPE = PU_T2.1 341
IST486I STATUS= ACTIV--L--, DESIRED STATE= ACTIV
IST1043I CP NAME = ***NA***, CP NETID = GBIBMIYA, DYNAMIC LU = YES
IST1589I XNETALS = NO
IST081I LINE NAME = ANY1LINE, LINE GROUP = ANY1GRP, MAJNOD = AP26ANYN
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST355I LOGICAL UNITS:
IST080I CTS5AH38 ACT/S----Y
IST314I END
```

Figure 16. SDSF: Display AnyNet PU state

Display TCP Major Node

The display command, d net,id=ap26anyn,e, shows the current state of the TCP Major Node (see Figure 17). The status should be ACTIV. The other parameters of interest are DNSUFX, showing the domain name suffix **1**, and the OS/390 TCP PORT.

```
D NET,ID=AP26ANYN,E
IST097I DISPLAY ACCEPTED
IST075I NAME = AP26ANYN, TYPE = TCP/IP MAJOR NODE 824
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1342I DNSUFX = HURSLEY.IBM.COM
IST1692I TCB = 10  TCP PORT =   397
IST1400I DGTIMER  =   40  EXTIMER =     5
IST1406I CONTIMER =   25  IATIMER =    60
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST170I LINES:
IST232I ANY1LINE ACTIV
IST314I END
```

Figure 17. SDSF: Display TCP Major Node

Display VTAM STATS information

The display command, d net,stats,type=vtam, shows whether AnyNet SNA over TCP/IP is installed and the number of TCP Major Nodes defined to this VTAM (see Figure 18 on page 27).

```
D NET,STATS,TYPE=VTAM
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = STATS,TYPE=VTAM 781
IST1349I COMPONENT ID IS 5695-11701-411
IST1345I    ID      VALUE       DESCRIPTION
  ::
IST1227I   130         YES = ANYNET/MVS SNA OVER TCP/IP INSTALLED
IST1227I   127           1 = TCP/IP MAJOR NODES
IST1227I   128          10 = MAXIMUM TCB VALUE FOR TCP/IP MAJOR NODES
IST1227I   129           3 = TCP/IP LU-LU SESSIONS
  ::
IST314I END
```

Figure 18. SDSF: Display VTAM STATS information

Display active session status information

The display command, d net,sessions,lu1=CTS5AH38,list=all, shows the active sessions between the client and server (see Figure 19).

```
D NET,SESSIONS,LU1=CTS5AH38,LIST=ALL
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = SESSIONS 636
IST873I       PLU           SLU              SID        STATUS
IST874I GBIBMIYA.IYCQCTS5 GBIBMIYA.CTS5AH38 F337539C85506917 ACTIV/SV
IST874I GBIBMIYA.CTS5AH38 GBIBMIYA.IYCQCTS5 DA17EACE855E1757 ACTIV
IST874I GBIBMIYA.CTS5AH38 GBIBMIYA.IYCQCTS5 DA17EACE855E1756 ACTIV/SV
IST924I -------------------------------------------------------------
IST878I NUMBER OF PENDING SESSIONS =         0
IST924I -------------------------------------------------------------
IST878I NUMBER OF ACTIVE  SESSIONS =         3
IST924I -------------------------------------------------------------
IST878I NUMBER OF QUEUED  SESSIONS =         0
IST924I -------------------------------------------------------------
IST878I NUMBER OF TOTAL   SESSIONS =         3
IST314I END
```

Figure 19. SDSF: display active session status information

Display session information

The display command, d net,sessions,sid=DA17EACE855E1757, shows information for the session in Figure 19. Figure 20 on page 28 shows this particular session to be ACTIV. Other parameters of interest are LOGMODE 4 showing LU6.2 user modename LU62PS, and the LOCAL TCP/IP ADDRESS and port number and REMOTE TCP/IP ADDRESS and port number of OS/390 and the client workstation, respectively.

Useful commands and utilities

```
D NET,SESSIONS,SID=DA17EACE855E1757
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = SESSIONS 124
IST879I PLU/OLU REAL = GBIBMIYA.CTS5AH38 ALIAS = ***NA***
IST879I SLU/DLU REAL = GBIBMIYA.IYCQCTS5 ALIAS = ***NA***
IST880I SETUP STATUS = ACTIV
IST875I ALSNAME TOWARDS PLU = ANY1PU
IST933I LOGMODE=LU62PS  , COS=*BLANK*
IST1165I LOCAL TCP/IP ADDRESS = 9.20.101.6..397
IST1165I REMOTE TCP/IP ADDRESS = 9.1.150.232..1240
  ::
IIST314I END
```

Figure 20. SDSF: Display session information

Display version of VTAM running

The SDSF command, d net,vtamopts, displays the version of VTAM running on OS/390.

SDSF Vary command

It may be necessary to activate nodes that are currently inactive. The vary commands are similar to the display commands. For example, to vary the TCP Major Node active in our sample configuration, you would issue this SDSF command: v net,act,id=ap26anyn .

TCP/IP Commands

The following commands are entered from a command prompt:

Ping utility

To verify the TCP/IP communication between the client and the server, use the ping utility. You can specify either the IP address or IP name. Figure 21 shows the messages returned from the ping utility when the IP name is specified.

```
ping IYCQCTS5.GBIBMIYA.hursley.ibm.com

Pinging IYCQCTS5.GBIBMIYA.hursley.ibm.com [9.20.101.6] with 32 bytes of data:

Reply from 9.20.101.6: bytes=32 time=190ms TTL=52
Reply from 9.20.101.6: bytes=32 time=191ms TTL=52
Reply from 9.20.101.6: bytes=32 time=190ms TTL=52
Reply from 9.20.101.6: bytes=32 time=201ms TTL=52
```

Figure 21. TCP/IP: Messages Returned from Ping Utility

Tracert utility

The tracert utility traces the TCP/IP path to the requested destination. It is useful for determining whether there is a problem with one of the

intermediate nodes. Figure 22 shows the TCP/IP route from the workstation to the CICS Transaction Server for OS/390 Version 1.3 used in our configuration.

```
tracert IYCQCTS5.GBIBMIYA.hursley.ibm.com

Tracing route to IYCQCTS5.GBIBMIYA.hursley.ibm.com [9.20.101.6]
over a maximum of 30 hops:

  1    <10 ms   <10 ms   <10 ms  vulture-150.almaden.ibm.com [9.1.150.254]
  2    <10 ms    10 ms   <10 ms  cisco.almaden.ibm.com [9.1.24.253]
  3    <10 ms    10 ms   <10 ms  sjalm-t3.almaden.ibm.com [9.1.1.11]
  4    <10 ms    10 ms    10 ms  9.32.221.25
  5     10 ms   <10 ms   <10 ms  9.32.221.20
  6     60 ms    70 ms    81 ms  199.4.213.121
  7    120 ms   130 ms   130 ms  9.32.1.166
  8    200 ms   191 ms   190 ms  portsmouth5.mpn.ibm.com [9.32.184.82]
  9    200 ms   231 ms   200 ms  9.31.253.29
 10    190 ms   200 ms   190 ms  9.31.232.118
 11    200 ms   201 ms   190 ms  hurroute1.hursley.ibm.com [9.20.61.2]
 12    200 ms   191 ms   200 ms  hurmss-01.hursley.ibm.com [9.20.26.218]
 13    200 ms   191 ms   200 ms  IYCQCTS5.GBIBMIYA.hursley.ibm.com [9.20.101.6]

Trace complete.
```

Figure 22. TCP/IP: messages returned from Tracert utility

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.

IBM ®