



System i
Networking
Telnet

Version 6 Release 1





System i
Networking
Telnet

Version 6 Release 1

Note

Before using this information and the product it supports, read the information in "Notices," on page 103.

This edition applies to version 6, release 1, modification 0 of IBM i5/OS (product number 5761-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

© **Copyright International Business Machines Corporation 1998, 2008.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Telnet.	1
PDF file for Telnet	1
Telnet scenarios	1
Telnet scenario: Telnet server configuration	1
Telnet scenario: Cascaded Telnet sessions	3
System request processing scenarios	5
Using a group job	6
Telnet scenario: Securing Telnet with SSL	8
Configuration details for securing Telnet with SSL	10
Planning for the Telnet server	14
Virtual device descriptions	14
Telnet security	15
Preventing Telnet access	15
Controlling Telnet access	16
Configuring the Telnet server	19
Starting the Telnet server	20
Setting the number of virtual devices	20
Automatically configuring virtual devices	21
Creating your own virtual devices	22
Restricting privileged users to specific devices and limiting sign-on attempts	22
Setting the session keep-alive parameter	23
Assigning devices to subsystems	24
Activating the QSYSWRK subsystem	24
Creating user profiles	25
i5/OS supported emulation types	25
Configuring Telnet server for 5250 full-screen mode	25
Configuring Telnet server for 3270 full-screen mode	25
Supported 3270 terminal types	27
Configuring Telnet server for VTxxx full-screen mode	28
Securing Telnet with SSL	31
Configuring SSL on the Telnet server	31
Removing port restrictions	31
Assigning a certificate to the Telnet server	32
Enabling client authentication for the Telnet server	33
Enabling SSL on the Telnet server	35
SSL initialization and handshake	36
Managing the Telnet server	37
Configuring Telnet printer sessions	37
Requirements for Telnet printer sessions	38
Telnet server print support to System i	38
Access for Windows Telnet client	38
Ending the Telnet server session	39
Ending device manager jobs	39
Using Telnet exit point programs	40
Device initialization exit program	42
Telnet exit point format INIT0100: Required parameter group	42
INIT0100: Format of user description information	44

INIT0100: Format of device description information	44
INIT0100: Format of connection description information	46
Device termination exit program	48
Examples: Telnet exit programs	48
Managing the Telnet client	49
Controlling Telnet server functions from the client	50
5250 Telnet client sessions	51
Starting a Telnet client session	51
3270 Telnet client sessions	52
Starting a 3270 Telnet client session	53
3270 full-screen considerations	54
Using a display station	55
3270 keyboard mapping for Telnet servers	56
VTxxx Telnet client sessions	58
Starting a VTxxx Telnet client session	58
VTxxx full screen considerations	60
VTxxx emulation options	64
VTxxx key values	65
VTxxx national language support	70
VTxxx national mode	71
Numeric keypad	73
Editing keypad	75
VTxxx key values by 5250 function	76
VT220 workstation operating modes	80
VT220 top-row function keys	80
VT100 and VT220 control character keywords	81
Establishing a cascaded Telnet session	82
Moving between cascaded Telnet sessions	83
Ending a Telnet client session	84
Troubleshooting the Telnet problems	84
Determining problems with Telnet	84
Pinging your host server	87
Troubleshooting emulation types	87
Troubleshooting your Telnet SSL server	90
Checking system status	91
Checking for an active SSL listener	92
Checking the Telnet job log	92
SSL return codes	93
TRCTCPAPP service program outputs	95
Materials needed to report Telnet problems	98
Automatically generated diagnostic information	99
Related information for Telnet	100

Appendix. Notices	103
Programming interface information	104
Trademarks	104
Terms and conditions	105

Telnet

Telnet is a protocol that enables you to log onto and use a remote computer as though you were connected directly to it within the local network.

The system (usually a PC) that you are physically in front of is the Telnet client. The Telnet server is the remote computer to which the client is attached. TCP/IP supports both the Telnet client and server.

One of the most important Telnet functions is its ability to negotiate the transmission of data streams between the Telnet client and the server. This type of negotiation makes it possible for either the client or the server to initiate or honor a request.

- | Several different emulation types are available for negotiating requests and converting them to output.
- | For Telnet, the preferred type is 5250 emulation. Telnet also supports 3270 and VTxxx type workstations as well as Request for Comments (RFC) 4777 (TN5250E) printer support modes. This topic introduces
- | Telnet and provides information about administering Telnet on your system.

Note: By using the code examples, you agree to the terms of the “Code license and disclaimer information” on page 101.

PDF file for Telnet

You can view and print a PDF file of this information.

To view or download the PDF version of this document, select [Telnet \(about 1300 KB\)](#).

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF link in your browser.
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe® Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

Related reference

“Related information for Telnet” on page 100

IBM® Redbooks® publications and Web sites contain information that relates to the Telnet topic collection. You can view or print any of the PDF files.

Telnet scenarios

The scenarios provide examples of using Telnet to introduce basic concepts and configuration tasks.

Telnet scenario: Telnet server configuration

The scenario depicts how an administrator configures a Telnet server, including objectives, prerequisites and assumptions, and configuration details.

Situation

Ken Harrison is the administrator for a new i5/OS® environment for the fictitious company Culver Pharmaceuticals.

Objectives

He needs to configure the Telnet server to meet the following specifications:

- Allow up to 100 virtual devices to be created automatically.
- Always display the sign-on window.
- Restrict privileged users to specific devices.
- Limit each user to one device session.

Prerequisites and assumptions

This scenario makes the following assumptions:

- Culver Pharmaceuticals is running the i5/OS operating system.
- TCP/IP is configured.
- Ken has *IOSYSCFG authority.

Configuration details

You can follow the steps to configure your Telnet server in System i® Navigator.

1. Start the Telnet server:
 - a. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
 - b. In the right pane, in the Server Name column, locate **Telnet**.
 - c. Confirm that **Started** appears in the Status column.
 - d. If the server is not running, right-click **Telnet** and click **Start**.
2. Set the number of virtual devices:
 - a. Select *your system* → **Configuration and Service** → **System Values**.
 - b. In the right pane, right-click **Devices** and select **Properties**.
 - c. On the Devices System Values page, enable **Pass-through devices and TELNET** and set the **Maximum number of devices** to 100.
3. Configure Telnet server properties:
 - a. Select *your system* → **Network** → **Servers** → **TCP/IP**.
 - b. In the right pane, right-click **Telnet** and select **Properties**.

Table 1. Telnet properties settings

Click this tab...	And ...
System Sign-On	Select: <ul style="list-style-type: none">• Restrict privileged users to specific devices.• Limit each user to one device session.
Remote Sign-On	Specify the number of sign-on attempts allowed and the action to take if the maximum number of sign-on attempts is reached.
Remote	Select the Always display sign-on option for Use Telnet for remote sign-on .

Table 1. Telnet properties settings (continued)

Click this tab...	And ...
Time-Out	Specify the action to take when jobs reach a time-out. You can also specify how long to give an operation before the job times out. You can specify information for both inactive jobs and disconnected jobs.

Note: These settings apply to all interactive devices and jobs on your system, not just Telnet.

4. Assign devices to subsystems.

At the character-based interface, type:

```
ADDWSE SBS(D(QINTER) WRKSTNTYPE(*ALL)
```

5. Activate the QSYSWRK subsystem:

Check the status of the QSYSWRK subsystem:

- a. In the character-based interface, type WRKSBS (Work with Subsystems).
- b. Verify that the following systems are displayed:
 - QSYSWRK
 - QINTER
 - QSPL

If the QSYSWRK subsystem is not active, complete the following steps:

- a. In the character-based interface, type STRSBS (Start Subsystem).
- b. Type **QSYSWRK** for the Subsystem description and **QSYS** for the Library, then press **Enter**.
- c. Repeat for Subsystem name **QINTER** with Library **QSYS**, and for Subsystem name **QSPL** with Library **QSYS**.

6. Create Telnet user profiles:

- a. Start System i Navigator and expand *your system*.
- b. Right-click **Users and Groups** and select **New User**.
- c. Enter the user name, description, and password.
- d. To specify a job description, click **Jobs** and enter the job description.
- e. Click **OK**.

7. Verify that Telnet is working.

Ken starts a 5250 emulation session and connects to the Telnet server.

Related concepts

“i5/OS supported emulation types” on page 25

The preferred emulation for the system is 5250 emulation. However, the system also supports 3270 and VTxxx emulation.

Related tasks

“Configuring the Telnet server” on page 19

The topic contains information about how to configure your Telnet server for various emulation types.

Telnet scenario: Cascaded Telnet sessions

The scenario demonstrates the ability to start Telnet sessions while you are still in a Telnet session. After you have been connected, you can switch between systems using system request values.

In this scenario, the user establishes Telnet sessions with multiple servers. This is known as a *cascaded Telnet session*. Using this method, you will be able to:

- Establish Telnet sessions between the home office and Chicago.
- Connect to additional Telnet servers without ending the initial session.

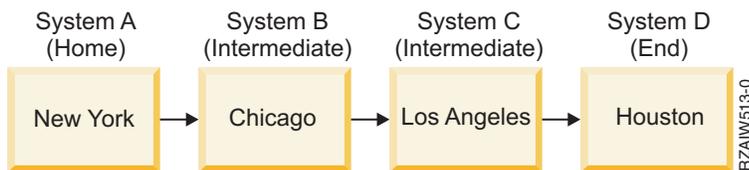
- Move between sessions to return to a job on the New York system.

Situation

Janice Lowe is the director of marketing at Culver Pharmaceuticals. She connects from the office in New York and accesses the main system in Chicago using Telnet. After Janice has established a client session with the Telnet server in Chicago, she realizes that she needs to work with some files from the Los Angeles office.

Objectives

Janice uses the Chicago Telnet client to connect to the Los Angeles Telnet server. While connected to Los Angeles, she decides to establish a session with Houston.



This figure depicts the connections that Janice makes. The system that she starts from in New York is called the home system. From there, she connects to intermediate system B in Chicago, then connects to intermediate system C in Los Angeles, which connects to end system D in Houston.

Prerequisites and assumptions

This scenario makes the following assumptions:

- Telnet server is running on all systems.
- Janice has a sign-on in all systems.
- All systems are running i5/OS V4R5, or later.

Configuration details

Janice completes the following steps to connect to the Telnet servers:

1. From the New York system, type STRTCPTELN CHICAGO.
2. On the Chicago system, type STRTCPTELN LA.
3. On the Los Angeles system, type STRTCPTELN HOUSTON.

After she has connected to the Houston system, she wants to complete a task on the New York (Home) system.

1. Press the **System Request** key.
2. Select option 14 (Transfer to home system). This returns her to the alternate job on the New York system.

After she has completed her work on the New York system, she can return to the Houston system by completing the following tasks:

1. Press the **System Request** key.
2. Select option 15 (Transfer to the end system). This takes her from any intermediate or home system to the end system.

To sign off from all sessions, she uses the SIGNOFF command. This command ends the current session and returns her to the sign-on display of the home system.

Related reference

“Establishing a cascaded Telnet session” on page 82

You can establish another Telnet session while you are in a current Telnet session. After you establish a cascaded session, you can move between the different systems.

“Moving between cascaded Telnet sessions” on page 83

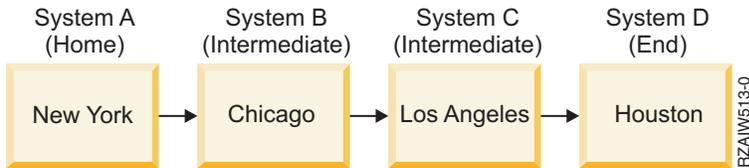
After you start a cascaded Telnet session, press the SysRq key, and press Enter to display the System Request menu.

System request processing scenarios

The scenarios explain how system request processing works with multiple types of systems.

Scenario 1

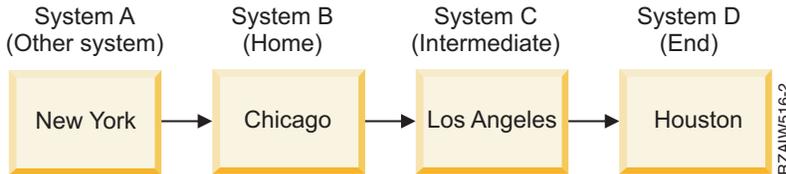
The image depicts the following setup: Home system A in New York connects to intermediate system B in Chicago, which connects to intermediate system C in Los Angeles, which connects to end system D in Houston.



Scenario 2

The New York system uses 3270 or VTxxx Telnet. It is a system other than System i.

The image depicts the following setup: System A in New York connects to home system B in Chicago, which connects to intermediate system C in Los Angeles, which connects to end system D in Houston.

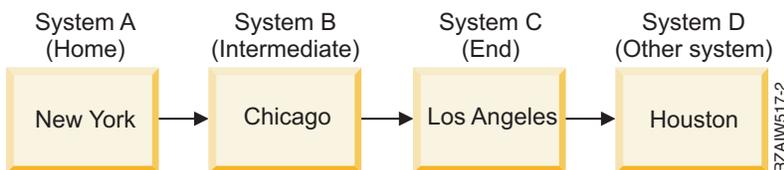


The system request processing works like the first scenario except that Chicago is considered as the home system. All system requests sent to the home system process on the Chicago system.

Scenario 3

The Houston system uses 3270 or VTxxx Telnet. It is a system other than System i.

The image depicts the following setup: Home system A in New York connects to intermediate system B in Chicago, which connects to intermediate system C in Los Angeles, which connects to end system D in Houston.

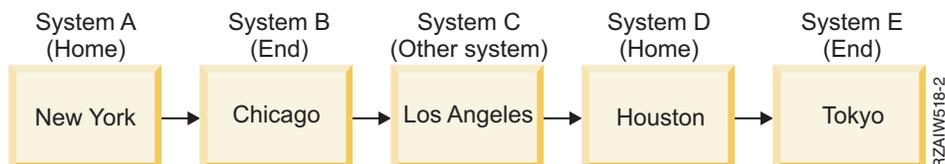


The system request processing works like the first scenario except that Los Angeles is considered as the end system for all system request processing. If you press the System Request key and then press the Enter key, the System Request menu for Los Angeles displays.

Scenario 4

The Los Angeles system uses 3270 or VTxxx Telnet. It is a system other than System i.

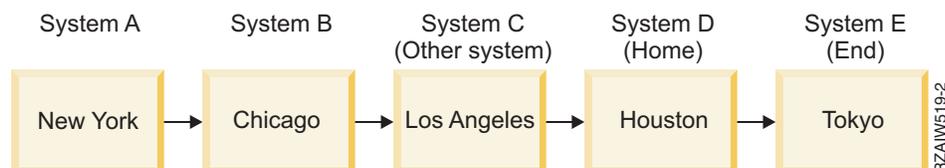
Home system A in New York connects to end system B in Chicago, which connects to system C in Los Angeles, which connects to home system D in Houston, which connects to end system E in Tokyo.



The system request processing works like the first scenario except that the Chicago system is considered as the end system for system request processing. If you press the System Request key and then press the Enter key, the System Request menu for Chicago is displayed.

If you want to send a system request to the Tokyo system, you can map a function key on the Houston system to the System Request key. If you map this function, then the Tokyo system is the end system, and Houston is the home system.

The image depicts the following setup: System A in New York connects to system B in Chicago, which connects to system C in Los Angeles, which connects to home system D in Houston, which connects to end system E in Tokyo.



As an example of this mapping function for a 3270 Telnet server, the default keyboard mapping identifies the System Request key as a 3270 PF11 key. For a 3270 Telnet client, the F11 key is mapped to the 3270 PF11 key. If the Los Angeles system uses the 3270 data stream, then pressing F11 maps the Los Angeles system to the System Request key on the Houston system. The system request transmits to the Tokyo system, and the System Request menu for Tokyo displays.

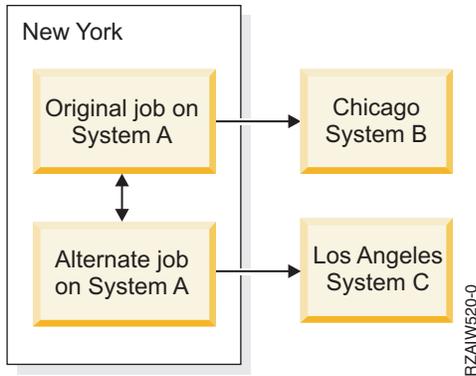
Note: This mapping function is complex especially if you are using the VTxxx data stream and are mapping between block data and character data.

Using a group job

These examples contain information about how to use Telnet, alternate jobs, and group jobs to work with multiple systems.

About this task

You can use Telnet and the alternate job to connect to multiple systems from your home system, consider the following example:



Telnet establishes a session from New York to Chicago. You also want to go to the Los Angeles system and remain connected to the Chicago system. You can start an alternate job on the New York system, using System Request option 11. Use the Telnet command to establish a session to the Los Angeles system. You can get to another system (Houston, for example) by starting another Telnet session from the Chicago system or the Los Angeles system.

An alternative to the alternate job is to use a group job. A group job is one of up to 16 interactive jobs that are associated in a group with the same workstation device and user. To set up a group job, follow these steps:

1. Change the current job to a group job by using the Change Group Attributes (CHGGRPA) command.
CHGGRPA GRPJOB(home)
2. Start a group job for the Chicago system by using the Transfer to Group Job (TFRGRPJOB) command.
TFRGRPJOB GRPJOB(CHICAGO) INLGRPPGM(QCMD)
3. Establish a Telnet session to the Chicago system.
Telnet CHICAGO
4. Return to your home system by pressing the ATTN key. Pressing the ATTN key shows you the Send Telnet Control Functions menu.
5. In the character-based interface for the Send Telnet Control Functions menu, type:
TFRGRPJOB GRPJOB(home)
This returns you to your original job.

Results

You can start other group jobs and Telnet sessions similarly.

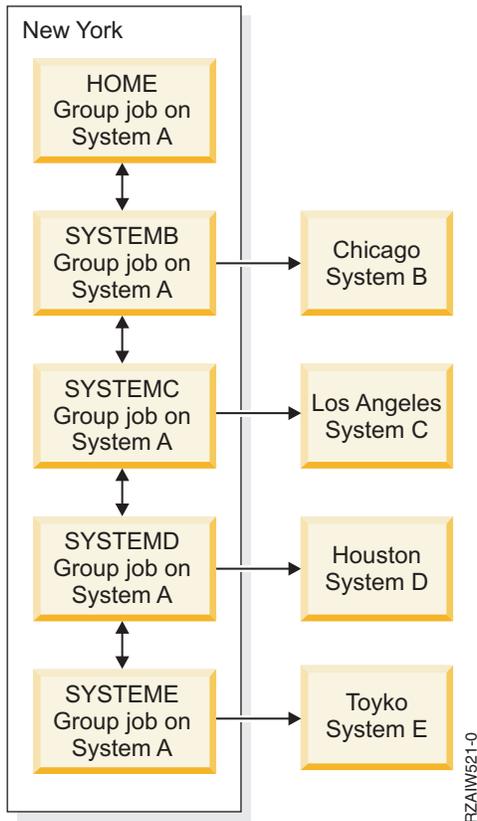
You can use the TFRGRPJOB GRPJOB(*SELECT) command to select the group job you want. For example, if group jobs with the names CHICAGO, LOSANGELES, HOUSTON, and TOKYO start, the TFRGRPJOB GRPJOB(*SELECT) command shows the following display:

```

                                Transfer to Group Job                System: SYS198
Active group job . . . : HOME
Text . . . . . :
Type option, press Enter.
  1=Transfer to group job
-----Suspended Group Jobs-----
Opt  Group Job  Text
-      TOKYO
-      HOUSTON
-      LOSANGELES
-      CHICAGO
Bottom F3=Exit F5=Refresh F6=Start a new group job F12=Cancel

```

You can then use Telnet to establish a session with each system from the appropriate job. The following example shows a group job scenario:



System A in New York contains Home Group job on System A, with bidirectional arrows down a chain connecting to, in order: System B group job on System A, System C group job on System A, System D group job on System A, and System E group job on System A. Each System group job on A has an arrow pointing to the correlating remote system (B, C, D, and E).

When you want to end the group job, use the End Group Job (ENDGRPJOB) command.

To switch to another group job while in a Telnet session:

1. Press the ATTN key.
2. Type TFRGRPJOB in the character-based interface.

Telnet scenario: Securing Telnet with SSL

This configuration example describes how to use Secure Sockets Layer (SSL) to secure Telnet on your system.

Situation

Bob is in the process of creating a home-based brokerage business. He retires from his position as a stockbroker at a major trading firm, and wants to continue to offer brokerage services to a small number of clients from his home. He runs his business on a small system, which he would like to use to provide account access to his clients, through 5250 Telnet sessions. Bob is currently working on a way to allow his clients continuous access to their accounts, so that they can manage their shareholdings. Bob wants his clients to use 5250 Telnet sessions to access their accounts, but he is concerned about the security of his server, as well as the security of his clients' sessions. After researching the Telnet security options, Bob

decides to use Secure Sockets Layer (SSL) to ensure the privacy of data over 5250 Telnet sessions between his server and clients.

Objectives

In this scenario, Bob wants to secure his brokerage clients' 5250 Telnet sessions to their shareholder accounts on his system. Bob wants to enable SSL to protect the privacy of client data as it passes through the Internet. He also wants to enable certificates for client authentication to ensure that his system verifies that only his clients are accessing their accounts. After Bob has configured the Telnet server for SSL and enabled client and server authentication, he can roll out this new account accessibility option to his clients, assuring them that their 5250 Telnet sessions are secure:

- Secure the Telnet server with SSL.
- Enable the Telnet server for client authentication.
- Obtain a private certificate from a local certificate authority (CA) and assign it to the Telnet.

Details

In this scenario, the setup for the brokerage business is as follows:

- The system runs i5/OS V5R4, or later, and provides shareholder account access over 5250 Telnet sessions.
- The Telnet server application is started on the system.
- The Telnet server initializes SSL, and checks the certificate information in the QIBM_QTV_TELNET_SERVER application ID.
- If the Telnet certificate configuration is correct, the Telnet server begins listening on the SSL port for client connections.
- A client initiates a request for access to the Telnet server.
- The Telnet server responds by providing its certificate to the client.
- The client software validates the certificate as an acceptable, trusted source communicating with the server.
- The Telnet server requests a certificate from the client software.
- The client software presents a certificate to the Telnet server.
- The Telnet server validates the certificate, and recognizes the client's right to establish a 5250 session with the server.
- The Telnet server establishes a 5250 session with the client.

Prerequisites and assumptions

This scenario makes the following assumptions:

- The system is running OS/400® V5R2, or i5/OS V5R3, or later.
- TCP/IP is configured.
- Bob has *IOSYSCFG authority.
- Bob addresses the issues in Configuring the Telnet server.
- Bob addresses the issues in SSL prerequisites.
- Bob creates a local certificate authority on his system.

Task steps

There are two sets of tasks that Bob must complete to implement this scenario: one set of tasks allows him to set up his system to use SSL and requires certificates for user authentication; the other set of tasks allows users on Telnet clients to participate in SSL sessions with Bob's Telnet server and to obtain certificates for user authentication.

Bob performs the following task steps to complete this scenario:

Telnet server task steps

To implement this scenario, Bob must perform these tasks on his system:

1. Remove port restrictions. Refer to Removing port restrictions.
2. Create and operate local certificate authority. Refer to Creating and operating local certificate authority.
3. Configure Telnet server to require certificates for client authentication. Refer to Configuring Telnet server to require certificates for client authentication.
4. Enable and start SSL on Telnet server. Refer to Enabling and starting SSL on Telnet server.

Client configuration task steps

To implement this scenario, each user who accesses the Telnet server on Bob's system must perform these tasks:

1. Enable SSL on the Telnet client. Refer to Enabling SSL on the Telnet client.
2. Enable Telnet client to present certificate for authentication. Refer to Enabling Telnet client to present certificate for authentication.

These tasks accomplish both SSL and client authentication by certificates, resulting in SSL-secured access to account information for Bob's clients using 5250 Telnet sessions.

Configuration details for securing Telnet with SSL

Here are the detailed configuration steps for securing Telnet with Secure Sockets Layer (SSL).

Step 1: Removing port restrictions

In releases before V5R1, port restrictions were used because Secure Sockets Layer (SSL) support was not available for Telnet. Now you can specify whether SSL, non-SSL, or both are to start. Therefore, there is no longer a need for port restrictions. If you have defined port restrictions in previous releases, you need to remove the port restrictions in order to use the SSL parameter.

To determine whether you have Telnet port restrictions and remove them so that you can configure the Telnet server to use SSL, follow these steps:

1. To view any current port restrictions, start System i Navigator and expand *your system* → **Network**.
2. Right-click **TCP/IP Configuration** and select **Properties**.
3. Click the **Port Restrictions** tab to see a list of port restriction settings.
4. Select the port restriction that you want to remove.
5. Click **Remove**.
6. Click **OK**.

By default, the setting is to start SSL sessions on port 992 and non-SSL sessions on port 23. The Telnet server uses the service table entry for Telnet to get the non-SSL port and Telnet-SSL to get the SSL port.

Step 2: Creating and operating local certificate authority

To use Digital Certificate Manager (DCM) to create and operate a local certificate authority (CA) on the system, follow these steps:

1. Start DCM.
2. In the navigation frame of DCM, select **Create a Certificate Authority (CA)** to display a series of forms. These forms guide you through the process of creating a Local CA and completing other tasks needed to begin using digital certificates for SSL, object signing, and signature verification.

3. Complete all the forms that are displayed. There is a form for each of the tasks that you need to perform to create and operate a local CA on the system. Completing these forms allows you to:
 - a. Choose how to store the private key for the local CA certificate. This step is included only if you have an IBM 4758-023 PCI Cryptographic Coprocessor installed on your system. If your system does not have a cryptographic coprocessor, DCM automatically stores the certificate and its private key in the Local CA certificate store.
 - b. Provide identifying information for the local CA.
 - c. Install the local CA certificate on your PC or in your browser. This enables software to recognize the local CA and validate certificates that the CA issues.
 - d. Choose the policy data for your local CA.
 - e. Use the new local CA to issue a server or client certificate that applications can use for SSL connections. If you have an IBM 4758-023 PCI Cryptographic Coprocessor installed in the system, this step allows you to select how to store the private key for the server or client certificate. If your system does not have a coprocessor, DCM automatically places the certificate and its private key in the *SYSTEM certificate store. DCM creates the *SYSTEM certificate store as part of this task.
 - f. Select the applications that can use the server or client certificate for SSL connections.

Note: Be sure to select the application ID for the Telnet server (QIBM_QTV_TELNET_SERVER).

- g. Use the new local CA to issue an object signing certificate that applications can use to digitally sign objects. This creates the *OBJECTSIGNING certificate store, which you use to manage object signing certificates.

Note: Although this scenario does not use object signing certificates, be sure to complete this step. If you cancel at this point in the task, the task ends and you need to perform separate tasks to complete your SSL certificate configuration.

- h. Select the applications that you want to trust the local CA.

Note: Be sure to select the application ID for the Telnet server (QIBM_QTV_TELNET_SERVER).

After you have completed the forms for this guided task, you can configure the Telnet Server to require client authentication.

Step 3: Configuring Telnet server to require certificates for client authentication

To activate this support, the system administrator indicates how SSL support is handled. Use the Telnet Properties General panel in System i Navigator to indicate whether SSL, non-SSL, or support for both starts when the Telnet server starts. By default, the SSL and non-SSL support always starts.

The System Administrator has the ability to indicate whether the system requires SSL client authentication for all Telnet sessions. When SSL is active and the system requires client authentication, the presence of a valid client certificate means that the client is trusted.

To configure the Telnet server to require certificates for client authentication, follow these steps:

1. Start DCM.
2. Click **Select a Certificate Store**.
3. Select ***SYSTEM** as the certificate store to open and click **Continue**.
4. Enter the appropriate password for *SYSTEM certificate store and click **Continue**.
5. When the left navigational menu refreshes, select **Manage Applications** to display a list of tasks.
6. Select the **Update application definition** task to display a series of forms.
7. Select **Server** application and click **Continue** to display a list of server applications.

8. From the list of applications, select **i5/OS TCP/IP Telnet Server**.
9. Click **Update Application Definition**.
10. In the table that displays, select **Yes** to require client authentication.
11. Click **Apply**. The **Update Application Definition** page displays with a message to confirm your changes.
12. Click **Done**.

Now that you have configured the Telnet server to require certificates for client authentication, you can enable and start SSL for the Telnet server.

Step 4: Enabling and starting SSL on Telnet server

To enable SSL on the Telnet server, follow these steps:

1. Open System i Navigator.
2. Expand *your system* → **Network** → **Servers** → **TCP/IP**.
3. Right-click **Telnet**.
4. Select **Properties**.
5. Select the **General** tab.
6. Choose one of these options for SSL support:
 - **Secure only**
Select this to allow only SSL sessions with the Telnet server.
 - **Non-secure only**
Select this to an SSL port will not connect.
 - **Both secure and non-secure**
Allows both secure and non-secure sessions with the Telnet server.

To start the Telnet server using System i Navigator, follow these steps:

1. Expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. In the right pane, locate **Telnet** in the Server Name column.
3. Confirm that **Started** appears in the Status column.
4. If the server is not running, right-click **Telnet** and select **Start**.

Step 5: Enabling SSL on the Telnet client

To participate in an SSL session, the Telnet client must be able to recognize and accept the certificate that the Telnet server presents to establish the SSL session. To authenticate the server's certificate, the Telnet client must have a copy of the CA certificate in the i5/OS key database. When the Telnet server uses a certificate from a local CA, the Telnet client must obtain a copy of the local CA certificate and install it in the i5/OS key database.

To add a local CA certificate from the system so that the Telnet client can participate in SSL sessions with Telnet servers that use a certificate from the Local CA, follow these steps:

1. Open System i Navigator.
2. Right-click the name of *your system*.
3. Select **Properties**.
4. Select the **Secure Sockets** tab.
5. Click **Download**. This downloads the i5/OS certificate authority certificate automatically into the certificate key database.

6. You are prompted for your key database password. Unless you have previously changed the password from the default, enter ca400. A confirmation message displays. Click **OK**.

The download button automatically updates the IBM Toolbox for Java™ PC key database.

Step 6: Enabling Telnet client to present certificate for authentication

You have configured SSL for the Telnet server, specified that the server should trust certificates that the present CA issues, and specified that it require certificates for client authentication. Now, users must present a valid and trusted client certificate to the Telnet server for each connection attempt.

Clients need to use the local CA to obtain a certificate for authentication to the Telnet server and import that certificate to the IBM Key Management database before client authentication works.

First, clients must use DCM to obtain a user certificate by following these steps:

1. Start DCM.
2. In the left navigation frame, select **Create Certificate** to display a list of tasks.
3. From the task list, select **User Certificate** and click **Continue**.
4. Complete the **User Certificate** form. Only those fields marked "Required" need to be completed. Click **Continue**.
5. Depending on the browser you use, you are asked to generate a certificate that is loaded into your browser. Follow the directions provided by the browser.
6. When the **Create User Certificate** page browser reloads, click **Install Certificate**. This installs the certificate in the browser.
7. Export the certificate to your PC. You must store the certificate in a password-protected file.

Note: Microsoft® Internet Explorer 5 or Netscape 4.5 are required to use the export and import functions.

Next, you must import the certificate to the IBM Key Management database so that the Telnet client can use it for authenticating the certificate to the IBM key by following these steps:

You must add the import client that creates the client certificate to the PC key database; otherwise, the import operation of the client certificate does not work.

1. Click **Start** → **Programs** → **IBM System i Access for Windows®** → **System i Access for Windows Properties**.
2. Select the **Secure Sockets** tab.
3. Click **IBM Key Management**.
4. You are prompted for your key database password. Unless you have previously changed the password from the default, enter ca400. A confirmation message displays. Click **OK**.
5. From the pull-down menu, select **Personal certificates**.
6. Click **Import**.
7. In the **Import key** display, enter the file name and path for the certificate. Click **OK**.
8. Enter the password for the protected file. This is the same password that you specified when you create a user certificate in DCM. Click **OK**. When the certificate is successfully added to your personal certificates in IBM Key Management, you can use PC5250 emulator or any other Telnet application.

With these steps complete, the Telnet server can establish an SSL session with the Telnet client and the server can authenticate the user to resources based on the certificate that the client presents.

Related tasks

Starting Digital Certificate Manager

“Assigning a certificate to the Telnet server” on page 32

When you enable the Telnet server on your system to use Secure Sockets Layer (SSL), you can establish secure Telnet connections to your system from System i Access for Windows or from any other SSL-enabled Telnet clients, such as a Personal Communications emulator.

Planning for the Telnet server

You can determine the number of virtual devices to associate with the workstations that are connected to your system. This topic also provides security procedures for controlling or preventing access to Telnet.

Before configuring your Telnet server, there are some security and operational features you must consider. You need to know how many virtual devices you want Telnet to automatically configure or whether you want to create your own virtual devices. The number of virtual devices automatically configured affects the number of sign-on attempts allowed. An increased number of sign-on attempts increases the chances of an unauthorized user gaining access to your server. You might also want to consider other security measures, such as having the Telnet server detect lost connections.

Virtual device descriptions

Telnet uses virtual device descriptions to maintain client workstation information for open Telnet sessions. Here are the details about configuring and naming virtual device descriptions.

A *virtual device* workstation attached is a device description that is used to form a connection between a user and a physical workstation attached to a remote system. Virtual devices provide information about your physical device (display or printer) to the programs on the system. The system looks for the attaching client/server protocol to specify a virtual device. If the system cannot find a specified virtual device, it then looks for a designated virtual device in a registered exit program. If the system cannot find a virtual device, it then attempts to match a virtual device description with a device type and model similar to the device on your local system.

Telnet naming conventions for virtual controllers and devices

The Telnet server uses the following conventions for naming automatically created virtual controllers and devices, according to the i5/OS standards:

- For virtual controller, the server uses the name QPACTL *nn* where *nn* is a decimal number of 01 or greater.
- For virtual devices, the server uses the name QPADEV *xxxx*, where *xxxx* is an alphanumeric character from 0001 to zzzzz, excluding vowels.
- For named virtual devices, the server gives the virtual controllers the name of QVIRCD *nnnn*.

Notes:

1. Under the i5/OS naming convention, the virtual controller must have a name of QPACTL *nn*.
2. The virtual device has a name of QPADEV *xxxx*.
3. You must grant the QTCP user profile authority to the user-created virtual devices.
4. You can change the naming conventions for automatically created virtual devices by using the *REGFAC option of QAUTOVRT.

The number of sign-on attempts allowed increases with automatically configured virtual devices. The total amount of sign-on attempts is equal to the number of system sign-on attempts that are allowed, multiplied by the number of virtual devices that can be created. The sign-on system values define the number of sign-on attempts allowed.

The Telnet server reuses available existing virtual devices that were automatically created by selecting virtual devices of the same device type and model. When no more device types and models match but

virtual devices are still available, then the device type and model are changed to match the client device and model negotiated. This is true for both automatically created (QPADEV *xxxx*) virtual devices, and named virtual devices.

If you choose to manually create your own devices, you should establish naming conventions that allow you to easily manage your configuration. You can select whatever device names and controller names that you want, provided that the names conform to the i5/OS object naming rules.

Related concepts

“Creating your own virtual devices” on page 22

You can manually create virtual devices and controllers, with custom names or automatically generated names.

Related tasks

“Setting the number of virtual devices” on page 20

You can enable the Telnet server to automatically configure a set number of virtual devices and controllers using the QAUTOVRT devices system values. You can also limit the number of sign-on attempts allowed.

Related reference

Devices system values: Pass-through devices and Telnet

Telnet security

When you start Telnet across a TCP connection, you need to consider security measures that prevent or allow user access to the system through Telnet.

For example, you should set limits and controls on the number of sign-on attempts, and the number of devices that a user can use to sign on.

Preventing Telnet access

If you do not want anyone to use Telnet to access your system, you should prevent the Telnet server from running. To prevent Telnet access to your system, complete the tasks in this topic.

Preventing Telnet from starting automatically

To prevent Telnet server jobs from starting automatically when you start TCP/IP, follow these steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Right-click **Telnet** and select **Properties**.
3. Clear **Start when TCP/IP starts**.

Preventing access to Telnet ports

To prevent Telnet from starting and to prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for Telnet, follow these steps:

1. In System i Navigator, click *your system* → **Network** → **Servers** → **TCP/IP**.
2. Right-click **TCP/IP Configuration** and select **Properties**.
3. In the TCP/IP Configuration Properties window, click the **Port Restrictions** tab.
4. On the Port Restrictions page, click **Add**.
5. On the Add Port Restriction page, specify the following values:
 - **User name:** Specify a user profile name that is protected on your system. (A protected user profile is a user profile that does not own programs that adopt authority and that does not have a password that is known by other users.) By restricting the port to a specific user, you automatically exclude all other users.
 - **Starting port:** 23 (for non-SSL TELNET) or 992 (for SSL TELNET)

- **Ending port:** 23 (for non-SSL TELNET) or 992 (for SSL TELNET)
- **Protocol:** TCP

Note: These port numbers are specified in the Work with Service Table Entries (WRKSRVTBLE) table under the service names Telnet and Telnet-ssl. They might be mapped to ports other than 23 and 992. Repeat this process for each port that you want to restrict. The Internet Assigned Numbers Authority (IANA) provides information about common port number assignments.

6. Click **OK** to add the restriction.
7. On the Port Restrictions page, click **Add** and repeat the procedure for the User Datagram Protocol (UDP) protocol.
8. Click **OK** to save your port restrictions and to close the TCP/IP Configuration Properties window.
9. The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

Related information

 [Internet Assigned Numbers Authority \(IANA\)](#)

Controlling Telnet access

You should be aware of the security considerations when you want Telnet clients to access your system.

Client authentication

The Telnet server supports client authentication in addition to the SSL server authentication. When enabled, the Telnet server authenticates both server and client certificates when Telnet clients connect to the Telnet SSL port. Telnet clients that do not send a valid client certificate when attempting to connect to the Telnet SSL port, will port fail to establish a display or printer session.

Protecting passwords

Telnet passwords are not encrypted when they are sent between the traditional client and the server. Depending on your connection methods, your system might be vulnerable to password theft through .line sniffing. (Monitoring a line by using electronic equipment is often referred to as sniffing.) Telnet passwords are encrypted, if TN5250E negotiations are used to exchange an encrypted password. In such a case, the sign-on panel can be bypassed and no .clear-text password is sent over the network. Only the password is encrypted with TN5250E; SSL is required to encrypt all traffic.

However, if you use the SSL Telnet server and an SSL-enabled Telnet client, then all transactions, including passwords, are encrypted and protected. The Telnet SSL port is defined in the WRKSRVTBLE entry under .Telnet-ssl that limits the number of sign-on attempts. Although the QMAXSIGN system value applies to Telnet, you might reduce the effectiveness of this system value if you set up your system to configure virtual devices automatically. When the QAUTOVRT system value has a value greater than 0, the unsuccessful Telnet user can reconnect and attach to a newly created virtual device. This can continue until one of the following situations occurs:

- All virtual devices are disabled, and the system has exceeded the limit for creating new virtual devices.
- All user profiles are disabled.
- The hacker succeeds in signing on to your system.

Automatically configuring virtual devices multiplies the number of Telnet attempts that are available.

Note: To make it easier to control virtual devices, you might want to set the QAUTOVRT system value to a value that is greater than 0 for a short period of time. Either use Telnet yourself to force the system to create devices or wait until other users have caused the system to create sufficient virtual devices. Then set the QAUTOVRT system value to 0.

Telnet enhancements provide an option for limiting the number of times a hacker can attempt to enter your system. You can create an exit program that the system calls whenever a client attempts to start a Telnet session. The exit program receives the IP address of the requester. If your program sees a series of requests from the same IP address within a short time span, your program can take action, such as denying further requests from the address and sending a message to the QSYSOPR message queue. Overview of the Telnet exit program capability provides an overview of the Telnet exit program capability.

Note: Alternatively, you can use your Telnet exit program to provide logging. Rather than having your program to make decisions about potential break-in attempts, you can use the logging capability to monitor attempts to start Telnet sessions.

Ending inactive sessions

Telnet sessions are included in the system's QINACTIV processing. The QINACTMSGQ system value defines the action for the interactive Telnet sessions that are inactive when the inactive job time-out interval expires. If the QINACTMSGQ specifies that the job should be disconnected, the session must support the disconnect job function. Otherwise, the job ends rather than be disconnected. Telnet sessions that continue to use device descriptions that are named QPADEVxxxx does not allow users to disconnect from those jobs. Disconnection from these jobs is not allowed because the device description to which a user is reconnected is unpredictable. Disconnecting a job requires the same device description for the user when the job is reconnected.

Limiting sign-on attempts

The number of Telnet sign-on attempts allowed increases if you have virtual devices automatically configured. The device system value in System i Navigator defines the number of virtual devices that Telnet can create.

Use the sign-on system values to define the number of system sign-on attempts allowed. For instructions for setting this value in System i Navigator, refer to "Restricting privileged users to specific devices and limiting sign-on attempts" on page 22.

Restricting powerful user profiles

You can use the QLMTSECOFR system value to restrict users with *ALLOBJ or *SERVICE special authority. The user or QSECOFR must be explicitly authorized to a device to sign on. Thus, you can prevent anyone with *ALLOBJ special authority from using Telnet to access your system by ensuring that QSECOFR does not have authority to any virtual devices. Rather than preventing any Telnet users who have *ALLOBJ special authority, you might restrict powerful Telnet users by location. With the Telnet initiation exit point, you can create an exit program that assigns a specific device description to a session request based on the IP address of the requester.

Controlling function by location

You might want to control which functions you allow or which menu the user sees based on the location where the Telnet request originates. The QDCRDEVD application programming interface (API) provides you with access to the IP address of the requester. Here are some suggestions for using this support:

- You might use the API in an initial program for all users (if Telnet activity is significant in your environment).
- You can set the menu for the user or even switch to a specific user profile based on the IP address of the user who requests sign-on.

- You can use the Telnet exit program to make decisions based on the IP address of the requester. This eliminates the need to define an initial program in every user profile. For example, you can set the initial menu for the user, set the initial program for the user, or specify which user profile the Telnet session will run under.

In addition, with access to the IP address of the user, you can provide dynamic printing to a printer associated with the user's IP address. The QDCRDEVD API also returns IP addresses for printers, as well as for displays. Select the DEVD1100 format for printers, and DEVD0600 for displays.

Controlling automatic sign-on

Telnet supports the capability for a System i Access for Windows user to bypass the Sign On display by sending a user profile name and password with the Telnet session request. The system uses the setting for the QRMTSIGN (Remote sign-on) system value to determine how to handle requests for automatic sign-on. The following table shows the options. These options apply only when the Telnet request includes a user ID and password.

Table 2. QRMTSIGN system setting options

Option	How QRMTSIGN works with Telnet
*REJECT	Telnet sessions that request automatic sign-on are not allowed.
*VERIFY	If the user profile and password combination is valid, the Telnet session starts. ¹
*SAMEPRF	If the user profile and password combination is valid, the Telnet session starts. ¹
*FRCSIGNON	The system ignores the user profile and password. The user sees the Sign-On display.

¹ - A registered Telnet exit program can override the setting of QRMTSIGN by choosing whether to allow automatic sign-on for a requester (probably based on IP address).

This validation occurs before the Telnet exit program runs. The exit program receives an indication that describes whether the validation is successful or unsuccessful. The exit program can still allow or deny the session, regardless of the indicator. The indication has one of the following values:

- Value = 0, Client password/passphrase (or Kerberos ticket) is not validated or none is received.
- Value = 1, Client clear-text password/passphrase is validated
- Value = 2, Client encrypted password/passphrase (or Kerberos ticket) is validated

Enabling anonymous sign-on

You can use the Telnet exit programs to provide .anonymous or .guest Telnet on your system. With your exit program, you can detect the IP address of the requester. If the IP address comes from outside organization, you can assign the Telnet session to a user profile that has limited authority on your system and a specific menu. You can bypass the Sign-On display so the visitor does not have the opportunity to use another more powerful user profile. With this option, the user does not need to provide a user ID and password.

Overview of the Telnet exit program capability

You can register user-written exit programs that run both when a Telnet session starts and when it ends. You can perform the following actions when starting an exit program:

- Use the Client SSL certificate to associate a user profile to the certificate and assign that user profile to the Telnet session, bypassing the Sign-On display.

- Use the system (local) IP address on multi-homed systems to route connections to different subsystems based on the network interface (IP address).
- Allow or deny the session, based on any known criteria, such as the user's IP address, the time of day, and the requested user profile, the device type (such as printer), and so on.
- Assign a specific i5/OS device description for the session. This allows routing of the interactive job to any subsystem set up to receive those devices.
- Assign specific national language values for the session, such as keyboard and character set.
- Assign a specific user profile for the session.
- Automatically sign on the requestor (without displaying a Sign On display).
- Set up audit logging for the session.

Related concepts

“Automatically configuring virtual devices” on page 21

You can enable the Telnet server to automatically configure your virtual devices and controllers using the QAUTOVRT devices system values in System i Navigator.

“Using Telnet exit point programs” on page 40

With the use of exit programs, the experienced programmer can create customized processing during an application. If the Telnet server finds a program registered to one of the exit points for the server, it calls that program using parameters that are defined by the exit point.

Related tasks

Digital Certificate Manager (DCM)

“Setting the session keep-alive parameter” on page 23

You can use the TCP keep-live parameter to set the maximum idle time that the TCP protocol allows before sending a probe to test for an inactive session.

Related reference

System values: Devices overview

System values: Signon overview

Related information

 [Technical Studio: Telnet Exit Programs](#)

Configuring the Telnet server

The topic contains information about how to configure your Telnet server for various emulation types.

About this task

One of the most important Telnet functions is its ability to negotiate options between the client and the server. This type of open negotiation makes it possible for either the client or the server to initiate or to honor a request. Several different emulation types are available to you for negotiating requests and converting them to output. The system can support 3270-type workstations and VTxxx workstations, but the preferred type is 5250 emulation.

To configure your Telnet server for use with one of the other emulation types supported, complete the following children linking tasks that contain task steps.

Results

After you have configured Telnet, you might want to secure Telnet with Secure Sockets Layer (SSL).

Related concepts

“Telnet scenario: Telnet server configuration” on page 1

The scenario depicts how an administrator configures a Telnet server, including objectives, prerequisites and assumptions, and configuration details.

Starting the Telnet server

The active Telnet server has one or more instances of each of these jobs running in the QSYSWRK subsystem: QTVTELNET and QTVDEVICE.

About this task

To start the Telnet server using System i Navigator, follow these steps:

1. Expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. In the right pane, locate **Telnet** in the Server Name column.
3. Confirm that **Started** appears in the Status column.
4. If the server is not running, right-click **Telnet** and select **Start**.

Related concepts

“Ending the Telnet server session” on page 39

By ending a Telnet session, you make the virtual device available to a new Telnet session.

Related tasks

“Activating the QSYSWRK subsystem” on page 24

The system job for a TCP/IP application must start in the QSYSWRK subsystem. The spooling subsystem, QSPL, needs to be active to run printer pass-through sessions.

“Enabling SSL on the Telnet server” on page 35

Follow these steps for understanding how to enable Secure Sockets Layer (SSL) on the Telnet server.

“Checking system status” on page 91

You need to confirm that your Telnet is ready for Secure Sockets Layer (SSL) sessions.

Setting the number of virtual devices

You can enable the Telnet server to automatically configure a set number of virtual devices and controllers using the QAUTOVRT devices system values. You can also limit the number of sign-on attempts allowed.

About this task

You can specify the number of devices that are automatically started and the maximum number of devices that the system automatically configures. The system configures or creates one device at a time, as needed, up to a specified limit.

1. In System i Navigator, select *your system* → **Configuration and Service** → **System Values**.
2. In the right pane, right-click **Devices** and select **Properties**.
3. On the Devices System Values page, enable **Pass-through devices and TELNET** and select an option for the automatic configuration of virtual devices. The options are:
 - **No maximum number of devices** - Allow an unlimited number of devices
 - **Maximum number of devices (1-32 500)** - Specify a value between 1 and 32 500 for the maximum number of devices that can be configured automatically.
 - **Run registered exit program** - Call the program registered for the Virtual Device Selection (QIBM_QPA_DEVSEL) exit point when a virtual device needs to be selected or automatically created.

Related concepts

“Virtual device descriptions” on page 14

Telnet uses virtual device descriptions to maintain client workstation information for open Telnet sessions. Here are the details about configuring and naming virtual device descriptions.

“Automatically configuring virtual devices” on page 21

You can enable the Telnet server to automatically configure your virtual devices and controllers using the QAUTOVRT devices system values in System i Navigator.

Related reference

Devices system values: Pass-through devices and Telnet

Related information

 [Technical Studio: Telnet Exit Programs](#)

Automatically configuring virtual devices

You can enable the Telnet server to automatically configure your virtual devices and controllers using the QAUTOVRT devices system values in System i Navigator.

You can specify the number of devices that are automatically started, and you can specify the maximum number of devices that the system automatically configures. The system configures or creates one device at a time, as needed, up to a specified limit.

When automatically configuring virtual devices with Telnet, the Telnet server does not delete virtual devices and does not delete the devices when the session closes. The server does not delete the devices even if the number of devices attached to the virtual controllers exceeds the maximum number. If the devices already exist on the virtual controller, the Telnet server can use them. The Telnet server modifies the attributes of an existing device to match the client request if that virtual device is requested by name.

If you have never allowed automatic configuration of virtual devices on your system, the Devices System Value Maximum number of devices value is 0. A Telnet connection attempt fails when the number of devices in use exceeds the Maximum number of devices. A device in use has the status active or sign-on display. If you try to sign on, you will receive a message (TCP2504) indicating that the Telnet client session has ended and the connection is closed. In addition, the QTCPIP job on the remote system sends a message (CPF8940) indicating that a virtual device cannot be automatically selected.

If you change the Maximum number of devices to 10, the next Telnet connection attempt causes the Telnet server to create a virtual device. Telnet creates this virtual device because the number of virtual devices on the controller (0) is less than the number specified in the Maximum number of devices (10). Even if you change the specified number to 0 again, the next user attempting a Telnet connection succeeds. When a Telnet connection attempt fails because the system is not able to create a virtual device, the CPF87D7 message is sent to the system operator message queue on the Telnet server.

Notes:

1. The Telnet server does not automatically delete configured virtual devices or named devices, even if the number of devices attached to the virtual controllers exceeds the maximum number of devices.
2. The devices system values specify whether pass-through virtual devices and Telnet full screen virtual devices that are attached to the QPACTL n n controllers are automatically configured. This system value does not affect devices attached to the QVIRCD n n n n controllers, because these are not default system devices. Typically, QPADEV n n n n devices are attached to QPACTL n n controllers while named devices, such as NEWYORK001, are attached to the QVIRCD n n n n controller.

Related concepts

“Controlling Telnet access” on page 16

You should be aware of the security considerations when you want Telnet clients to access your system.

Related tasks

“Setting the number of virtual devices” on page 20

You can enable the Telnet server to automatically configure a set number of virtual devices and controllers using the QAUTOVRT devices system values. You can also limit the number of sign-on attempts allowed.

Related reference

Devices system values: Pass-through devices and Telnet

Creating your own virtual devices

You can manually create virtual devices and controllers, with custom names or automatically generated names.

If you create your own virtual devices and allow your system to automatically select the device name, you must be aware of the following rules:

- The virtual controller has the name QPACTL *nn*, where *nn* is a decimal number 01 or greater.
- The virtual device has the name QPADEV *xxxx*, where *xxxx* is an alphanumeric character from 0001 to zzzz. The virtual device should have a device class of *VRT. The location of the virtual device is under a virtual controller.

If you choose to create your own devices, you should be familiar with the virtual device descriptions naming conventions used by the Telnet server. If you want to select your own device names (using a RFC 4777 client or the Virtual Terminal APIs), then the virtual controller has the name QVIRCD *nnnn*, where *nnnn* is a decimal number 01 or greater.

Related concepts

“Virtual device descriptions” on page 14

Telnet uses virtual device descriptions to maintain client workstation information for open Telnet sessions. Here are the details about configuring and naming virtual device descriptions.

Restricting privileged users to specific devices and limiting sign-on attempts

The sign-on system values are used to both restrict or limit the devices to which a user can sign on and to define the number of system sign-on attempts allowed.

Restricting privileged users to specific devices

The i5/OS licensed program uses the sign-on system values to restrict or limit the devices to which a user can sign on. *All object authority* (*ALLOBJ) allows the user to access any of the resources on the system. *Service special authority* (*SERVICE) allows the user to perform specific service functions on the system. For example, the user with this type of authority will be able to debug a program, and perform display and alter service functions. To set these values using System i Navigator, follow these steps:

1. Select *your system* → **Network** → **Servers** → **TCP/IP**.
2. In the right pane, right-click **Telnet** and select **Properties**.
3. On the Telnet Properties - System Sign-On page, select the following options:
 - **Restrict privileged users to specific devices.** This selection indicates that all users with all object (*ALLOBJ) and service (*SERVICE) special authority need explicit authority to specific workstations.
 - **Limit each user to one device session.** This selection indicates that a user can sign on only at one workstation. This does not prevent the user from using group jobs or making a system request at the workstation. This reduces the likelihood of sharing passwords and leaving devices unattended.

Limiting sign-on attempts

Use the sign-on system values to define the number of system sign-on attempts allowed. The number of Telnet sign-on attempts allowed increases if you have virtual devices automatically configured. To set these values, follow these steps:

1. In System i Navigator, select *your system* → **Network** → **Servers** → **TCP/IP**.
2. In the right pane, right-click **Telnet** and select **Properties**.
3. On the Telnet Properties page, click the **System Sign-On** tab.

4. On the Telnet Properties - System Sign-On page, you can specify the number of sign-on attempts allowed and the action to take if the maximum number of sign-on attempts is reached.
5. Click the **Remote** tab.
6. On the Telnet Properties - Remote Sign-On page, select an option for **Use Telnet for remote sign-on**. The options are:
 - **Always display sign-on** - All remote sign-on sessions are required to go through normal sign-on processing.
 - **Allow sign-on to be bypassed** - The system allows the user to bypass the sign-on panel. The user is still signed on to the system, but the sign-on panel is not displayed.

Note: If Use Pass-through for remote sign-on is enabled, the options are selected automatically based on the settings you specify for Use Pass-through for remote sign-on. Telnet is still available for remote sign-ons if you select Pass-through.

Related concepts

System values: Sign-on overview

Setting the session keep-alive parameter

You can use the TCP keep-live parameter to set the maximum idle time that the TCP protocol allows before sending a probe to test for an inactive session.

About this task

The protocol sends keep-alive requests to the remote client any time the session remains idle for periods longer than the keep-alive value. The idle period is defined by the Session keep-alive timeout parameter in Telnet Properties in System i Navigator, or a parameter in the CHGTELNA command. When a session appears to be inactive (no response is received from the remote client to any keep-alive probe) that session is ended, the virtual device associated with the session is returned to the free pool of virtual devices, and the i5/OS operating system performs the action set in the QDEVRCYACN system value on the interactive job running on the virtual device. This action affects only named virtual devices. For automatically selected virtual devices (QPADEVxxx), the interactive job always ends.

The Telnet server defines the keep-alive setting to 600 seconds by default.

This setting takes effect at server startup. In addition to the session keep-alive timeout parameter, you might also want to review the Timeout interval settings in the Inactive Jobs System Values in System i Navigator. This Timeout parameter limits the amount of time that any interactive job is allowed to be idle before the i5/OS operating system performs the action set in the QINACTMSGQ system value on the interactive job. In the case of Telnet-connected interactive jobs, an action of *DSCJOB is honored for only named virtual devices. For automatically selected virtual devices (QPADEVxxx), an action of *DSCJOB causes the interactive job to be ended.

To set the keep-alive parameter for Telnet in System i Navigator, follow these steps:

1. In System i Navigator, select *your system* → **Network** → **Servers** → **TCP/IP**.
2. In the right pane, right-click **Telnet** and select **Properties**.
3. On the Telnet Properties page, click the **Time-Out** tab.
4. On the Telnet Properties - Time-Out page, specify the action to take when jobs reach a time-out. You can also specify how long to give an operation before the job times out. You can specify information for both inactive jobs and disconnected jobs.

Related concepts

“Controlling Telnet access” on page 16

You should be aware of the security considerations when you want Telnet clients to access your system.

Related reference

System values: Jobs overview

Assigning devices to subsystems

Before a user can sign on to the system, the workstation must be defined to a subsystem. The workstation is the virtual display device that is selected or automatically created by the Telnet server.

The workstation name or the workstation type should be specified in the subsystem description on the system. Use the Display Subsystem Description (DSPSBSD) command to see the workstation entries defined to the subsystem.

You can use the following command to add all workstation types to a subsystem that is named QINTER:

```
ADDWSE SBSB(QINTER) WRKSTNTYPE(*ALL)
```

Printer devices are always routed to the QSPL spooling subsystem.

The Add Workstation Entry (ADDWSE) command can be done when the subsystem is active. However, the changes might or might not take effect immediately. You might need to stop and restart the subsystem.

Activating the QSYSWRK subsystem

The system job for a TCP/IP application must start in the QSYSWRK subsystem. The spooling subsystem, QSPL, needs to be active to run printer pass-through sessions.

About this task

To check the status of the QSYSWRK subsystem, complete the following steps:

1. In the character-based interface, type WRKSBS (Work with active subsystems).
2. Verify that the following systems are displayed:
 - QSYSWRK
 - QINTER
 - QSPL

Results

If the QSYSWRK subsystem is not active, complete the following steps:

1. In the character-based interface, type STRSBS (Start subsystem).
2. Type QSYSWRK for the Subsystem description and QSYS for the Library, then press Enter.
3. Repeat for Subsystem name QINTER with Library QSYS and for Subsystem name QSPL and Library QSYS.

If you do not know which subsystem to use for interactive jobs, type WRKSBSD *ALL in the character-based interface. The Work Station Type entries show you which device is allocated to a subsystem.

What to do next:

Create user profiles

Related tasks

“Starting the Telnet server” on page 20

The active Telnet server has one or more instances of each of these jobs running in the QSYSWRK subsystem: QTVTELNET and QTVDEVICE.

Creating user profiles

On the Telnet server, you can create Telnet user profiles using System i Navigator.

About this task

To create Telnet user profiles, complete the following steps:

1. Start System i Navigator and expand *your system*.
2. Right-click **Users and Groups** and select **New User**.
3. Enter the user name, description, and password.
4. To specify a job description, click **Jobs** and enter the job description.
5. Click **OK**.

i5/OS supported emulation types

The preferred emulation for the system is 5250 emulation. However, the system also supports 3270 and VTxxx emulation.

Select the emulation type you want to configure your Telnet server to use.

Related concepts

“Telnet scenario: Telnet server configuration” on page 1

The scenario depicts how an administrator configures a Telnet server, including objectives, prerequisites and assumptions, and configuration details.

Configuring Telnet server for 5250 full-screen mode

The 5250 full-screen mode enables Telnet client users to sign on and run 5250 full-screen applications.

About this task

You need to complete these steps before establishing your Telnet client session:

1. Start the Telnet server on the remote system (the system that you want to connect to using Telnet).
2. Set the System i platform to automatically configure virtual controllers and devices. Verify that the QTVTELNET and QTVDEVICE jobs in the QSYSWRK subsystem are active by completing the following steps:
 - a. Start System i Navigator and expand *your system* → **Work Management**.
 - b. Right-click **Subsystems** and click **Open**.
 - c. Verify that the subsystem is active.
3. Check the QAUTOVRT system value. It should equal the maximum number of users that are signed on, using automatically configured virtual devices, at any one time. QAUTOVRT supports numeric values of 0 through 32 500, and a special value of *NOMAX.

Configuring Telnet server for 3270 full-screen mode

Telnet client users can sign on and run 5250 full-screen applications using 3270 full-screen mode.

The system negotiates 3270 full-screen support with any Telnet client application that supports 3270 full-screen applications, rather than 5250 full-screen applications. An example of a system that negotiates 3270 full-screen support is the IBM System z[®] family.

Telnet 5250 (TN5250) delivers the data stream between the two systems as EBCDIC. Because the 3270 data streams are translated into 5250 data streams, the workstation devices operate as a remote 5251 display to the system and application programs.

After you have completed the general configuration of the Telnet server, there are a few additional steps to enable system support for 3270 full-screen mode. Full-screen mode is a block mode as opposed to a line mode. Line mode is when data transmits one line at a time, whereas block or full-screen mode transmits the whole screen at one time.

Complete the following tasks to configure the Telnet server for 3270 full-screen mode:

1. Check the QKBDTYPE system value. Refer to “Checking the QKBDTYPE system value”
2. Set the default keyboard mapping. Refer to “Setting the default keyboard mapping”
3. Change a keyboard map. Refer to “Changing a keyboard map”
4. Change message queue. Refer to “Changing message queue” on page 27

Checking the QKBDTYPE system value

When the Telnet server automatically creates virtual display devices, it uses the QKBDTYPE system value to determine the keyboard type for the virtual device.

If the initial creation of the virtual device fails by using the QKBDTYPE system value, the Telnet server uses the keyboard value USB to try to create the device. If the second attempt to create the virtual display device fails using the value of USB, then a message (CPF87D7) is sent to the system operator message queue. This message indicates that the system cannot automatically select the virtual device.

Setting the default keyboard mapping

A 3270 display station connected to a System i model using Telnet appears to be a 5251 display station to a System i platform. The 3270 display station keyboard has a 5251-equivalent keyboard map associated with it. The 5251-equivalent keyboard map allows the 3270 display station keyboard to complete 5251-equivalent functions on the system.

When a Telnet client system user first signs on in 3270 full-screen mode, the system automatically assigns the default keyboard map to the user’s 3277, 3278, or 3279 keyboard. Avoid this by including a user-defined keyboard map in the user’s profile sign-on procedure. This supplies the mapping needed for the 3270 keyboards to do most of the same functions as their 5250-equivalent keyboards do.

Displaying a keyboard map

You can use the Display Keyboard Map (DSPKBDMAP) command to see the current keyboard mapping. Another method is to use option 6 (Display 3270 keyboard map) on the Configure TCP/IP Telnet menu, while your terminal is in 3270 emulation mode.

Changing a keyboard map

Use the Change Keyboard Map (CHGKBDMAP) command if you want to make minor changes to the default keyboard map. This command is available from the Configure TCP/IP Telnet menu as option 7 (Change 3270 keyboard map).

If you want to set a new keyboard map, use the Set Keyboard Map (SETKBDMAP) command. This command is option 7 (Change 3270 keyboard map) on the Configure TCP/IP Telnet menu. The key assignments that you specify are in effect until you use these commands again to specify new key assignments or until you sign off.

Note: The difference between CHGKBDMAP and SETKBDMAP is that, with SETKBDMAP, the system applies the defaults and then the changes in the SETKBDMAP are applied. With CHGKBDMAP, the system applies defaults plus any changes that you have previously made during this session, and then the changes in the CHGKBDMAP are applied.

Changing message queue

A message queue is like a mail box for messages. The system has several message queues that hold messages that provide helpful information when finding and reporting problems. When your workstation message queue is in break mode, messages appear on the 3270 device exactly as they appear on the 5250 display. To receive messages in break mode, you must specify *BREAK on the change message queue (CHGMSGQ) command. When your workstation is not in break mode, you receive the following message: A message has arrived on a message queue.

To retrieve this message and continue using the workstation, follow these steps:

1. Press the function key assigned to the help function, or the function key that is assigned to the error reset function.
2. Enter the Display Message (DSPMSG) command or the function key that is assigned to the system request function followed by option 4 (Display Message) to view the waiting message.
3. Set the workstation message queue to break mode to see the messages as they arrive.

Resetting the display's input-inhibited light

When using a System i model from a 5250-type terminal, pressing certain keys in certain situations causes input to be inhibited. When this occurs, the 5250 terminal displays an input-inhibited light.

Two asterisks shown in the lower-right corner of the display indicate the input-inhibited light. When the keyboard is inhibited, any keys mapped to the i5/OS function keys are ignored.

To reset the keyboard, press the Enter key, or press the key mapped to the Reset key.

Related concepts

“3270 Telnet client sessions” on page 52

The 3270 emulation type allows you to access a remote system that has a Telnet server application.

“3270 keyboard mapping for Telnet servers” on page 56

The topic contains information about keyboard mapping for support of 3270 emulation.

Related reference

“Supported 3270 terminal types”

The topic describes the capabilities of the 3270 devices that Telnet supports. Make sure that your Telnet client 3270 is negotiating one of the supported 3270 terminal types.

Supported 3270 terminal types:

The topic describes the capabilities of the 3270 devices that Telnet supports. Make sure that your Telnet client 3270 is negotiating one of the supported 3270 terminal types.

The following table shows the supported terminal types.

Table 3. Full-screen workstation mappings

Device type	Device capabilities
3277	This display station supports generic 3270 data streams. Extended attributes, such as underlining, blinking, reverse image, or color are not supported.

Table 3. Full-screen workstation mappings (continued)

Device type	Device capabilities
3278	<p>This station supports extended attributes, such as blinking, reverse image, and underlining if requested by the i5/OS Data Description Specifications (DDS) keywords.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Extended attributes are not supported by some client implementations of Telnet 3270 full-screen mode (TN3270). 2. Double-byte character set (DBCS) terminals type are terminals that negotiate a 3278-2-E terminal type are supported.
3279	<p>This display station supports color attributes and the extended data stream attributes sent for a 3278 device. The color attributes are determined (in the same manner as a 5292 Full Color Display) by interpreting the DDS attributes as blinking, high intensity, or the DDS color keywords.</p>

Related concepts

“Configuring Telnet server for 3270 full-screen mode” on page 25

Telnet client users can sign on and run 5250 full-screen applications using 3270 full-screen mode.

Configuring Telnet server for VTxxx full-screen mode

VTxxx server support enables Telnet client users to log on and run 5250 full-screen applications, even though VTxxx full-screen support is negotiated.

The Telnet client application must be able to negotiate VTxxx terminal support. When VTxxx full-screen mode is negotiated, the Telnet server is responsible for mapping 5250 functions to VTxxx keys and vice versa.

Although the Telnet server supports VTxxx clients, this is not the preferred mode to use because the VTxxx terminal is a character-mode device. The i5/OS operating system is a block-mode system. Most Telnet implementations support a TN3270 or TN5250 client that should be used when connecting to a Telnet server.

In general, when a key on a VTxxx terminal is pressed, the hexadecimal code associated with that key immediately transmits to the Telnet server. The Telnet server must process that keystroke and then echo that character back to the VTxxx terminal where it is displayed. This results in a large amount of overhead associated with each keystroke. In contrast, the 5250 and 3270 block mode devices buffer all keystrokes at the client system until an attention identifier (AID) key is pressed. When an AID key is pressed, the client sends the buffered input to the server for processing. The block-mode devices result in less overhead per keystroke and generally provide better performance than a character-mode device, such as the VTxxx terminal.

VTxxx delivers the data between the two systems as ASCII.

After you have completed the general configuration of the Telnet server, you need to complete a few additional steps to enable server support for VTxxx full-screen mode.

Full-screen mode is a block mode as opposed to a line mode. Line mode is when data transmits one line at a time, while block or full-screen mode transmits the whole screen at one time.

Complete the following tasks to configure the server for VTxxx full-screen mode:

1. "Checking the QKBDTYPE system value"
2. "Setting the default keyboard map"
3. "Setting the default network virtual terminal type"
4. "Setting the ASCII/EBCDIC mapping tables" on page 30

Checking the QKBDTYPE system value

When the Telnet server automatically creates virtual display devices, it uses the QKBDTYPE system value to determine the keyboard type for the virtual device.

If the initial creation of the virtual device fails using the QKBDTYPE system value, the Telnet server tries to create the device again, using a keyboard type value of USB. If the second attempt to create the keyboard type fails, then the system sends a message (CPF87D7) to the QTCPIP job log. This message indicates that the system cannot automatically create the virtual device. The system also sends the message to the system operator message queue.

Setting the default keyboard map

When a Telnet session negotiates in VTxxx full-screen mode, the system uses a default keyboard map. To display the default keyboard map for VTxxx, use the Display VT Keyboard Map (DSPVTMAP) command. To change the VTxxx keyboard map, use the Change VT Keyboard Map (CHGVMTMAP) command or the Set VT Keyboard Map (SETVTMAP) command.

The numeric keypad table shows the keys on the auxiliary keypad that normally transmit the codes for the numerals, decimal point, minus sign and comma.

The editing keypad table shows the keys that transmit codes for the editing keypad keys.

Because the VTxxx keyboard does not have the same keys as a 5250 keyboard, a keyboard mapping must exist between the VTxxx keys and the i5/OS functions. The system assigns a default keyboard mapping when a VTxxx session is first established. In some cases, there can be more than one key or key sequence that maps to a particular i5/OS function. In these cases, you can use any of the defined keys to call the required i5/OS function.

Notes:

1. Each control character is a 1-byte value generated from a VTxxx keyboard by holding down the CTRL key while pressing one of the alphabetic keys. Both shifted and unshifted control characters generate the same hexadecimal values.
2. The escape sequences are multiple byte codes that are generated by pressing the Esc key followed by the characters that make up the required sequence.
3. The system ignores the case of all alphabetic characters in an escape sequence. You can type alphabetic characters in escape sequences in either uppercase or lowercase.
4. The system F1-F12 functions are mapped to the Esc key followed by one of the keys in the top row of a VTxxx keyboard. The Esc key followed by a shifted key plus one of the keys in the top row of a VTxxx keyboard maps the F13-F24 functions.
5. Some Telnet VTxxx client systems use Ctrl-S and Ctrl-Q for flow control purposes. This is generally referred to as XON/XOFF flow control. If you are using a client system that has XON/XOFF enabled, you should not use the values *CTLS and *CTLQ in your keyboard mapping.

Setting the default network virtual terminal type

The default network virtual terminal type parameter specifies the mode to use when the Telnet server is not able to negotiate one of the supported terminal types.

To set the value of the default network virtual terminal to either *VT100 for VT100/VT220 mode, or *NVT for ASCII line mode, complete the following steps:

1. Start System i Navigator and expand *your system* → **Network** → **Servers** → **TCP/IP**.
2. Right-click **TELNET** and select **Properties**.
3. Click the **General** tab and select the appropriate value next to **Default network virtual terminal**.
4. Click **OK**.

Setting the ASCII/EBCDIC mapping tables

The Telnet server uses default ASCII-to-EBCDIC and EBCDIC-to-ASCII mapping tables based on the coded character set identifier (CCSID) parameter in the TCP/IP Telnet attributes. The default is to use the DEC multinational character set (*MULTINAT). Other 7-bit and 8-bit ASCII CCSIDs, and any of the 7-bit DEC national replacement character sets are also acceptable to use.

Note: For VT220 8-bit mode, the mapping tables are not available. In this mode, the system uses the DEC replacement character sets. For the VT220 7-bit mode, you can use either the mapping tables or the DEC replacement character sets.

There are three ways to change the default. You can change the CCSID parameter, specify different values for the VTxxx outgoing (TBLVTOU) and incoming tables(TBLVTIN), or change the default tables for the current session.

- To change the values for the tables, complete the following steps:
 1. Start System i Navigator and expand *your system* → **Network** → **Servers** → **TCP/IP**.
 2. Right-click **TELNET** and select **Properties**.
 3. Click the **Mappings** tab.
 4. Select the **Use specified mapping tables** check box and click **Tables**.
 5. Select the **Use outgoing mapping table** and **Use incoming mapping table** check boxes to change the CCSID parameter.
 6. Click **OK**.
 7. Click **OK**.
- To change the default tables for the current session, use the Set VT Mapping Tables (SETVTTBL) command.

Another way to access this command is to use option 2 on the CHGTCPTELN command.

Related concepts

“VTxxx Telnet client sessions” on page 58

VTxxx Telnet client sessions provide information about using this emulation type to sign on and use applications on a remote system that has a Telnet server application. This section also provides more information about VTxxx emulation.

Related reference

“Numeric keypad” on page 73

Here are the keys on the auxiliary keypad that normally transmit the codes for numerals, decimal points, minus signs, and commas.

“Editing keypad” on page 75

The table shows the keys that transmit codes for the editing keypad key.

“VTxxx emulation options” on page 64

When using VTxxx full-screen mode with your Telnet server, there are a few optional procedures that you can do to personalize the emulation type. You can display the current keyboard map and then decide whether you want to change it. You can also change the control characters when using VT220 full-screen mode.

“VTxxx key values by 5250 function” on page 76
The table describes the VTxxx key values by 5250 function.

Securing Telnet with SSL

With the Secure Sockets Layer (SSL) protocol, you can establish secure connections between the Telnet server application and Telnet clients that provide authentication of one or both endpoints of the communication session. SSL also provides privacy and integrity of the data that client and server applications exchange.

Related concepts

Secure Sockets Layer (SSL)

Related tasks

“Troubleshooting your Telnet SSL server” on page 90

Here are the detailed steps for troubleshooting your Secure Sockets Layer (SSL) server including system SSL return codes and a list of common SSL problems.

Configuring SSL on the Telnet server

The most important factor to consider when enabling SSL on the Telnet server is the sensitivity of the information that is involved in client sessions. If the information is sensitive, or private, then securing the Telnet server with SSL is recommended.

About this task

To configure SSL on the Telnet server, follow these steps:

1. Install the following software to support Telnet SSL and to manage digital certificates:
 - IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1)
 - Digital Certificate Manager
 - IBM HTTP Server for i5/OS (5761-DG1)
 - IBM Developer Kit for Java (5761-JV1)
2. Ensure that you have removed port restrictions and allowed SSL to start.
3. Assign a certificate to the Telnet server.
4. Enable client authentication for the Telnet server (optional step).
5. Enable SSL on the Telnet server.
6. Start the Telnet server.

Related concepts

“SSL initialization and handshake” on page 36

Here are the details about the interactions between Telnet servers, clients, and Secure Sockets Layer (SSL).

Related tasks

“Troubleshooting your Telnet SSL server” on page 90

Here are the detailed steps for troubleshooting your Secure Sockets Layer (SSL) server including system SSL return codes and a list of common SSL problems.

“Checking system status” on page 91

You need to confirm that your Telnet is ready for Secure Sockets Layer (SSL) sessions.

Removing port restrictions:

In releases before V5R1, port restrictions were used because Secure Sockets Layer (SSL) support was not available for Telnet. Now you can specify whether SSL, non-SSL, or both are to start. Therefore, there is no longer a need for port restrictions.

About this task

If you defined port restrictions in previous releases, you need to remove the port restrictions in order to use the SSL parameter. In order to remove port restrictions, follow these steps:

1. To list the port restrictions, complete the following steps:
 - a. Start System i Navigator and expand *your system* → **Network**.
 - b. Right-click **TCP/IP Configuration** and select **Properties**.
 - c. Click the **Port Restrictions** tab.
2. To remove the Port Restriction, continue to complete the following steps:
 - a. Select the Port Restriction that you want to remove.
 - b. Click **Remove**.
 - c. Click **OK**.

Results

By default, the setting is to start SSL on port 992 and non-SSL on port 23. The Telnet server uses the service table entry for Telnet to get the non-SSL port and Telnet-SSL to get the SSL port.

Related tasks

“Assigning a certificate to the Telnet server”

When you enable the Telnet server on your system to use Secure Sockets Layer (SSL), you can establish secure Telnet connections to your system from System i Access for Windows or from any other SSL-enabled Telnet clients, such as a Personal Communications emulator.

Assigning a certificate to the Telnet server:

When you enable the Telnet server on your system to use Secure Sockets Layer (SSL), you can establish secure Telnet connections to your system from System i Access for Windows or from any other SSL-enabled Telnet clients, such as a Personal Communications emulator.

About this task

Before you can configure the Telnet server to use SSL, you must install the prerequisite programs and set up digital certificates on your system.

1. Start IBM Digital Certificate Manager (DCM).

Note: If you have questions about how to complete a specific form while using DCM, select the question mark (?) at the top of the page to access the online help.

2. In the navigation frame, click **Select a Certificate Store** and select either ***OBJECTSIGNING** or ***SYSTEM** as the certificate store to open.
3. Enter the password for the certificate store and click **Continue**.
4. After the navigation frame refreshes, select **Manage Certificates** to display a list of tasks.
5. From the list of tasks, select **Assign certificate** to display a list of certificates for the current certificate store.
6. Select a certificate from the list and click **Assign to Applications** to display a list of application definitions for the current certificate store.
7. Select Telnet from the list and click **Continue**. A page displays with either a confirmation message for your assignment selection or an error message if a problem occurred.

Results

Note: The System i Access for Windows clients key database must contain a copy of any required certificate authority (CA) certificate. In this case, a CA certificate must exist in the key database for

the certificate that you assign to the Telnet server application. The key database comes preconfigured with copies of CA certificates from almost all well-known public CAs. If you choose to assign a certificate to the Telnet server that a local CA issues, however, then you must add a copy of the local CA certificate to the client key database. To learn how to add a copy of a local CA certificate, see Step 5: Enabling SSL on the Telnet client in the Telnet scenario: Secure Telnet with SSL - Configuration Details topic.

The Telnet server supports client authentication as an optional component in SSL configuration. Client authentication occurs when the server verifies the identity of the client by authenticating the client certificate passed up to the server application.

What to do next:

Enable client authentication for the Telnet server (optional step) or Enable SSL on the Telnet server.

Related concepts

Planning SSL

“Configuration details for securing Telnet with SSL” on page 10

Here are the detailed configuration steps for securing Telnet with Secure Sockets Layer (SSL).

Related tasks

“Removing port restrictions” on page 31

In releases before V5R1, port restrictions were used because Secure Sockets Layer (SSL) support was not available for Telnet. Now you can specify whether SSL, non-SSL, or both are to start. Therefore, there is no longer a need for port restrictions.

Setting up certificates for the first time

Starting Digital Certificate Manager

“Enabling client authentication for the Telnet server”

The Telnet server supports the authentication of Telnet client certificates. This means that during the Secure Sockets Layer (SSL) handshake, not only can the server generate a server certificate for the client, but also can optionally check for a valid client certificate, depending on how Digital Certificate Manager (DCM) is configured.

“Enabling SSL on the Telnet server” on page 35

Follow these steps for understanding how to enable Secure Sockets Layer (SSL) on the Telnet server.

“Checking system status” on page 91

You need to confirm that your Telnet is ready for Secure Sockets Layer (SSL) sessions.

Enabling client authentication for the Telnet server:

The Telnet server supports the authentication of Telnet client certificates. This means that during the Secure Sockets Layer (SSL) handshake, not only can the server generate a server certificate for the client, but also can optionally check for a valid client certificate, depending on how Digital Certificate Manager (DCM) is configured.

About this task

The DCM allows you to configure whether SSL Client Certificates are required for Telnet sessions.

To activate this support, the system administrator indicates how SSL support is handled. Use the Telnet Properties General panel in System i Navigator to indicate whether SSL, non-SSL, or support for both will start when the Telnet server starts. By default, the SSL and non-SSL support always starts.

The system administrator has the ability to indicate whether the system requires SSL client authentication for all Telnet sessions. When SSL is active and the system requires client authentication, the presence of a valid client certificate means that the client is trusted.

The system applies any negotiated RFC 4777 variables, and the Telnet user exits variables after the satisfaction of SSL controls.

To update the application specifications in IBM DCM and enable client authentication for the Telnet server, follow these steps:

1. Start IBM DCM. If you need to obtain or create certificates, or otherwise set up or change your certificate system, do so now.
2. Click **Select a Certificate Store**.
3. Select ***SYSTEM**. Click **Continue**.
4. Enter the appropriate password for *SYSTEM certificate store. Click **Continue**.
5. When the left navigational menu reloads, expand **Manage Applications**.
6. Click **Update application definition**.
7. On the next panel, select **Server** application. Click **Continue**.
8. Select **i5/OS TCP/IP Telnet Server**.
9. Click **Update Application Definition**.
10. In the table that displays, select **Yes** to require client authentication.
11. Click **Apply**.
12. DCM reloads to the Update Application Definition page with a confirmation message. When DCM reloads is finished reloading and updating the application definition for the Telnet server, click **Done**.

Related tasks

“Assigning a certificate to the Telnet server” on page 32

When you enable the Telnet server on your system to use Secure Sockets Layer (SSL), you can establish secure Telnet connections to your system from System i Access for Windows or from any other SSL-enabled Telnet clients, such as a Personal Communications emulator.

Starting Digital Certificate Manager

“Enabling SSL on the Telnet server” on page 35

Follow these steps for understanding how to enable Secure Sockets Layer (SSL) on the Telnet server.

Related information

 [Configuring DCM](#)

Example: Enabling client authentication for a PC5250 session:

After you have configured Secure Sockets Layer (SSL) for the Telnet server and specified to use client authentication, users are required to provide a valid and trusted client certificate to the Telnet server for each connection attempt.

Clients need to create a user certificate and import that certificate to the IBM Key Management database before client authentication works.

Creating a user certificate in DCM

1. Start IBM Digital Certificate Manager (DCM). If you need to obtain or create certificates, or otherwise set up or change your certificate system, do so now.
2. Expand **Create Certificate**.
3. Select **User Certificate**. Click **Continue**.
4. Complete the User Certificate form. Only those fields marked “Required” need to be completed. Click **Continue**.
5. Depending on the browser you use, you will be asked to generate a certificate that is loaded into your browser. Follow the directions provided by the browser.

6. When the Create User Certificate page reloads, click **Install Certificate**. This installs the certificate in the browser.
7. Export the certificate to your system. You must store the certificate in a password-protected file.

Note: Microsoft Internet Explorer 5 or Netscape 4.5 are required to use the export and import functions.

Importing the certificate to the IBM Key Management

1. Click **Start** → **Programs** → **IBM System i Access for Windows** → **System i Access for Windows Properties**.
2. Select the **Secure Sockets** tab.
3. Click **IBM Key Management**.
4. You are prompted for your key database password. Unless you have previously changed the password from the default, enter ca400. A confirmation message is displayed. Click **OK**.
5. From the pull-down menu, select **Personal certificates**.
6. Click **Import**.
7. In the Import key display, enter the file name and path for the certificate. Click **OK**.
8. Enter the password for the protected file. This is the same password that you created in Step 7 of Create a user certificate in DCM. Click **OK**. When the certificate has been successfully added to your personal certificates in IBM Key Management, you can use the PC5250 emulator or any other Telnet application.

Starting a PC5250 emulator session from System i Navigator

1. Open System i Navigator.
2. Right-click the name of your system that you have set up for client authentication for Telnet.
3. Select **Display emulator**.
4. Select the Communication menu, then select **Configure**.
5. Click **Properties**.
6. In the Connection dialog, select the **Use Secure Sockets Layer (SSL)**.
7. If you have more than one client certificate, select either **Select certificate when connecting** or **Use default** to determine which client certificate to use.
8. Click **OK**.
9. Click **OK**.

Related tasks

Starting Digital Certificate Manager

Configuring DCM

Related information

 [Configuring DCM](#)

Enabling SSL on the Telnet server:

Follow these steps for understanding how to enable Secure Sockets Layer (SSL) on the Telnet server.

1. Open System i Navigator.
2. Expand *your system* → **Network** → **Servers** → **TCP/IP**.
3. Right-click **Telnet**.
4. Select **Properties**.
5. Select the **General** tab.
6. Choose one of these options for SSL support:

- **Secure only**
Select this to allow only SSL sessions with the Telnet server.
- **Non-secure only**
Select this to prohibit secure sessions with the Telnet server. Attempts to connect to an SSL port will not connect.
- **Both secure and non-secure**
Select this to allow both secure and non-secure sessions with the Telnet server.

Related tasks

“Assigning a certificate to the Telnet server” on page 32

When you enable the Telnet server on your system to use Secure Sockets Layer (SSL), you can establish secure Telnet connections to your system from System i Access for Windows or from any other SSL-enabled Telnet clients, such as a Personal Communications emulator.

“Enabling client authentication for the Telnet server” on page 33

The Telnet server supports the authentication of Telnet client certificates. This means that during the Secure Sockets Layer (SSL) handshake, not only can the server generate a server certificate for the client, but also can optionally check for a valid client certificate, depending on how Digital Certificate Manager (DCM) is configured.

“Starting the Telnet server” on page 20

The active Telnet server has one or more instances of each of these jobs running in the QSYSWRK subsystem: QTVTELNET and QTVDEVICE.

SSL initialization and handshake

Here are the details about the interactions between Telnet servers, clients, and Secure Sockets Layer (SSL).

What happens during SSL initialization?

The Telnet server attempts to initialize SSL every time the server is started. During initialization, the Telnet server checks the certificate information in the QIBM_QTV_TELNET_SERVER application. You can tell that the SSL initialization is successful when more than one active QTVTELNET job appears in the QSYSWRK subsystem. Of course, if the number of server jobs to start field in the Telnet properties General page is set to 1, you see only one active QTVTELNET job.

The Telnet server does not initialize SSL when you have a restricted telnet-ssl port. The Telnet server sends the TCP2550 message Access to port 992 is restricted to the QTVTELNET job log and to the QSYSOPR message queue.

When a certificate is incorrect or expired, initialization fails and the Telnet server sends message CPDBC nn to the QTVTELNET job log.

Even if no certificate or an expired certificate is in the QIBM_QTV_TELNET_SERVER application, the Telnet server successfully initializes SSL. However, the SSL handshake fails when the client tries to connect to the Telnet server. The Telnet server sends message CPDBC nn to the QTVTELNET job log.

What happens during SSL re-initialization?

When the certificate in the QIBM_QTV_TELNET_SERVER application changes, the Telnet server re-initializes SSL if a DCM change occurs. This means that you can restore an expired certificate or add or remove user certificates and Telnet picks up changes automatically. The process is the same as SSL initialization. New Telnet SSL client sessions use the new certificate. Telnet SSL client sessions that are already established use the original certificate. After the Telnet server is ended and started again, all Telnet SSL client sessions use the new certificate.

If the SSL re-initialization fails, established SSL sessions use the original certificate that was initialized when the server started and new sessions are blocked from connecting. The next time you start the Telnet

server, SSL initialization fails, although there will still be an active SSL listener. However, no new SSL connections will be successful until a change in the DCM forces Telnet server to re-initialize successfully.

What happens during SSL handshake?

An SSL handshake occurs when the Telnet SSL client connects to TCP port 992 and attempts an SSL negotiation with the server. While the client is connecting to the server, it displays status numbers or messages on the status bar of the open window.

If the SSL handshake fails, the Telnet session is not established. For example, a sign-on screen does not appear in the Telnet SSL client window. Consult the user guide or online help for your Telnet SSL client for information about specific status numbers or messages. The Telnet server sends message CPDBC *nn* to the QTVTELNET job log.

Related tasks

“Configuring SSL on the Telnet server” on page 31

The most important factor to consider when enabling SSL on the Telnet server is the sensitivity of the information that is involved in client sessions. If the information is sensitive, or private, then securing the Telnet server with SSL is recommended.

“Checking the Telnet job log” on page 92

When Secure Sockets Layer (SSL) initialization and handshake fails, the Telnet server sends CPDBC *nn* diagnostic messages to the QTVTELNET job.

Managing the Telnet server

You should be aware of how to work with your Telnet server and how to use exit programs to control user access.

The Telnet server allows a TCP/IP user on a remote Telnet client to sign on to and run applications on the System i platform. The Telnet server support negotiates the transmission of data with the remote Telnet client application for various operating modes.

The Telnet server and client applications negotiate these operating modes. The functions available to you depend on the terminal type that is negotiated.

With minimal changes to the system values, the Telnet server can support Telnet connections when TCP/IP starts. For all operating modes except ASCII line mode, the system automatically sends the sign-on display when a Telnet connection is made. For ASCII line mode, a customer application that displays data must be active.

Configuring Telnet printer sessions

The topic contains instructions for attaching to printers on the system from remote locations on the network.

About this task

You must create a 3812 or 5553 virtual printer device to use Telnet printer emulation. Such a device is needed to generate the printer data streams sent for the printer session. Printers used with Telnet printing can be attached to the PC or attached to the same network as the PC. Telnet printer sessions negotiate with a remote Telnet client on a system that supports Telnet printer emulation.

Telnet printer sessions deliver the printer data stream between the two systems as either EBCDIC or ASCII depending on the preferences of the requesting client.

Telnet printer sessions are active immediately after Telnet initialization. Printing functions do not require user profiles and passwords. However, if your security requires it, you can use Telnet exit point programs to block printer sessions from starting.

When using Telnet printer sessions, all print data is spooled to a printer writer queue for printing. You cannot print directly to a print device. When using the printer file commands to create printer file (CRTPRTF), change printer file (CHGPRTF), and overwrite printer file (OVRPRTF), you must use the default SPOOL (*YES) parameter. Also, Telnet sets the printer writer or output queue to the same name as the printer.

To set up your Telnet printer sessions, follow these steps:

1. Check to make sure that the TCP stack is active. If not, issue the STRTCP command to start the TCP stack.
2. Start the Telnet server. Refer to Starting the Telnet server.
3. Set the number of virtual devices. Refer to Setting the number of virtual devices.
4. Set the Telnet session keep-alive parameter. Refer to Setting the Telnet session keep-alive parameter.
5. Create virtual controllers and devices. Refer to Creating virtual controllers and devices.
6. Activate the QSPL subsystem. Refer to Activating the QSPL subsystem.
7. Test the setup with a test printer file.
8. Print a file through a Telnet printer session.

Results

Note: The QSYSWRK subsystem starts when the TCP stack starts.

Requirements for Telnet printer sessions

If you intend to use Telnet printer sessions, check with your Telnet client vendor to see if they support the printer session function.

These clients support the printer session function:

- IBM System i Access for Windows
- Personal Communications
- IBM Host OnDemand

Telnet printer sessions support these generic EBCDIC printers:

- IBM-3812-1 for single-byte character set (SBCS)
- IBM-5553-B01 for double-byte character set (DBCS)

You can specify either of the generic device types by requesting the Host Print Transform (HPT) function and selecting the specific manufacturing type. If you are using System i Access for Windows, you can use the Printer Definition Table (PDT) or the Graphical Device Interface (GDI) to define specific hardware. The system sends the printer data stream in ASCII.

System API enhancement

The System API Retrieve Device Description (QDCRDEVD) provides the IP address of the Telnet client. There are several fields for display (*DSP) and print (*PRT) devices: Network protocol, Network protocol address, and IP address in dotted decimal form. These fields supply sockets level information to your application about the client's TCP/IP connection.

Telnet server print support to System i Access for Windows Telnet client:

The IBM System i Access for Windows client provides both display emulation, 5250 full-screen Telnet client, and printer emulation.

About this task

Select one of the following to start a printer session:

1. **System i Access for Windows** → **Emulators** → **Start or Configure Session** from the program start menu.
2. Select the name of a System i model to connect to.
3. Use the **Workstation ID** field to specifically request a virtual device name. You can leave the field blank and the Telnet server automatically select a compatible virtual device (QPADEVxxxx) and return the name on the printer control panel.
4. For type of emulation:
 - a. Select a printer.
 - b. Click the **Setup** box to start the PC5250 printer emulation setup dialog.

From the setup dialog, you can configure things such as font, the message queue, and the HPT host function. The HPT host functions include transforming print data to ASCII on the i5/OS operating system. Selecting host print transform (HPT) enables other configuration items, such as printer model and media tray selection options. There is also an option to automatically reconnect, and an option to override the default Telnet port number (23).

Results

To end the session, click **Communication** → **Disconnect from the menu bar**.

Ending the Telnet server session

By ending a Telnet session, you make the virtual device available to a new Telnet session.

When you are connected to a system, signing off does not necessarily end your Telnet server session. The virtual display or printer device is still active and cannot be used by another Telnet session. To end the session, you must enter a key or sequence of keys to put the Telnet client into a local command mode. You can then type the command to end the session. Use one of the following key sequences to end a Telnet server session.

- From the i5/OS operating system, press the **Attention** key and then select option 99 (End TELNET session - QUIT).
- From most other operation systems, log off.

If you do not know what key or key sequence causes the client to enter command mode, consult either your system administrator or your Telnet client documentation.

You can also use the end connection (ENDCNN) parameter of the SIGNOFF command to sign off the system and end the Telnet connection. For example, SIGNOFF ENDCNN(*YES) returns you to the client system (if you only have one Telnet session established). If you have more than one Telnet session established, the command returns you to the previous system.

Related tasks

“Starting the Telnet server” on page 20

The active Telnet server has one or more instances of each of these jobs running in the QSYSWRK subsystem: QTVTELNET and QTVDEVICE.

Ending device manager jobs

Sometimes it is necessary to end and restart the device manager jobs; for example, when applying a program temporary fix (PTF) to the program. This topic provides instructions for ending and restarting device manager jobs.

About this task

Start and stop Telnet ends the Telnet server jobs, but not the device manager jobs. This is because the nature of the device manager jobs requires that they be running all the time, or at least until the next restart of the system. In order to make the device manager jobs cycle, you have to do special steps 2 and 3. Then, the next time you start Telnet, it will see that there are no device manager jobs running and will start them. Complete the following steps to end device manager jobs:

1. End active Telnet server jobs by completing the following steps:
 - a. Start System i Navigator and expand *your system* → **Network** → **Servers** → **TCP/IP**.
 - b. Right-click **Telnet** and select **Stop**.
2. Find all active Telnet device manager jobs by completing the following steps:
 - a. Start System i Navigator and expand *your system* → **Work Management**.
 - b. Select **Active Jobs**.
 - c. Look for QTVDEVICE.
3. End all jobs found in step 2 by right-clicking and selecting **Delete/End**. You must wait for all jobs to exit before doing the next step.
4. Start Telnet server and device manager jobs on the Delete/End panel.

Any Telnet virtual devices that are still in the process of ending when all device manager jobs have ended might become inaccessible until your next restart.

Using Telnet exit point programs

With the use of exit programs, the experienced programmer can create customized processing during an application. If the Telnet server finds a program registered to one of the exit points for the server, it calls that program using parameters that are defined by the exit point.

An *exit point* is a specific point in the Telnet program where control might pass to an exit program. An *exit program* is a program to which the exit point passes control.

For each exit point, there is an associated programming interface, called an **exit point interface**. The exit point uses this interface to pass information between the Telnet application and the exit program. Each exit point has a unique name. Each exit point interface has an exit point format name that defines how information is passed between the Telnet application and the customer-written exit program.

Different exit points can share the same exit point interface. When this is the case, multiple exit points can call a single exit program.

Exit point performance

The Telnet server response time for your initial session request includes any time that it takes for the server to call, process, and return the QIBM_QTG_DEVINIT exit program. If your exit program is doing significant processing, the performance impact might result in a longer wait before your session is established. If you want to modify the default 60 second timeout value for user exit programs, you can use the ADDEXITPGM command to add user data that is read as the timeout value. In the following example, the PGMDTA parameter overrides the default 60 second timeout to 10 seconds:

```
ADDEXITPGM EXITPNT(QIBM_QTG_DEVINIT) FORMAT(INIT0100)
PGMNBR(1) PGM(USEREXIT/DEVINIT2) REPLACE(*YES)
CRTEXITPNT(*NO) PGMDTA(*JOB *CALC 10)
```

After the Telnet program is established by way of a sign-on window or other System i model, there is no effect on performance. When this occurs, the exit program is no longer in the Telnet path. Established Telnet sessions experience no delays due to the QIBM_QTG_DEVINIT exit program.

There is no user-visible performance impact that is associated with disconnecting the session. Disconnecting means that you end your terminal emulation session, not that you sign off and return to the sign-on panel. If you disconnect, then the QIBM_QTG_DEVTERM exit program is called, which performs the disconnect processing for your session. Users can not see this because it occurs after the connection is broken.

Work management

You can solve key work management problems by using a Telnet exit program. These problems include the capability to request device descriptions other than QPADEVxxxx, opening up the door for work management control of interactive virtual workstation jobs, and routing those jobs to specific subsystems.

Subsystem routing and device name selection

Users can take advantage of better Telnet virtual device names and configure their interactive subsystems to subdivide the work. This is done by using the Add Work Station Entry (ADDWSE) command. This command allows you to specify which devices a subsystem should or should not allocate a particular name of virtual terminal devices.

The following command has QINTER allocate all QPADEV* workstations, which means that all such devices route to the QINTER subsystem:

```
ADDWSE SBS(DQINTER) WRKSTN(QPADEV*) AT(*SIGNON)
```

The following command has QINTER not allocating all QPADEV* workstations, which means that these devices can be allocated to a different subsystem:

```
ADDWSE SBS(DQINTER) WRKSTN(QPADEV*) AT(*ENTER)
```

Users can develop their own device naming conventions to subdivide the work. For example, one kind of subdivision is to route certain devices to national language support (NLS) related subsystems in two locations.

Example

The two users are in Chicago and New York. The users are assigned to subsystems CHICAGO or NEWYORK, according to their geographic location. The characteristics of this example include:

- The IP addresses for Chicago start with 1.2.3.*.
- The IP addresses for New York start with 2.3.4.*.
- In order for all of the Chicago Telnet sessions to run in the CHICAGO subsystem the user exit program is employed. The exit program creates a virtual device name that starts with 'CHICAGO' for all Telnet connections from 1.2.3. The user exit program also creates a virtual device name that starts with 'NEWYORK' for all connections from 2.3.4.
- The user exit program assigns the virtual device name 'CHICAGO01' for an IP address of 1.2.3.47. The program assigns a virtual device name of 'NEWYORK01' for an IP address from 2.3.4.48. The program attaches a variable part ('01', '02', etc.) to a root name of 'CHICAGO' and checks to see if the device is not already in use before assigning it to the current user.

To ensure that virtual devices CHICAGO01 goes into subsystem Chicago and NEWYORK01 goes into subsystem New York, set up the workstations entries as follows:

Note: By using the code examples, you agree to the terms of the Code license and disclaimer information.

```
ADDWSE SBS(DQINTER) WRKSTN(CHICAGO*) AT(*ENTER)
ADDWSE SBS(DQINTER) WRKSTN(NEWYORK*) AT(*ENTER)
ADDWSE SBS(DCHICAGO) WRKSTN(CHICAGO*) AT(*SIGNON)
ADDWSE SBS(DNEWYORK) WRKSTN(NEWYORK*) AT(*SIGNON)
```

Related concepts

“Controlling Telnet access” on page 16

You should be aware of the security considerations when you want Telnet clients to access your system.

Device initialization exit program

The Telnet server application includes exit points that allow you to connect Telnet’s sign-on and termination logic. You can use the Work with Registration Information (WRKREGINF) or Add Exit Program (ADDEXITPGM) commands to associate your custom exit program to an exit point.

If the Telnet server finds a program registered to one of the exit points for the server, it calls that program using parameters defined by the exit point. These parameters include things like IP address, user name, and virtual device name. Your custom exit program then processes the information. For example, logs a message and returns control to the Telnet server. On return, your exit program tells the system whether to accept or reject this client and any optional user or password overrides.

Each exit point has a name and an exit point interface. The exit point interface is a list of input and output parameters the Telnet server exchanges with your exit program. There are two exit points for the Telnet server:

- QIBM_QTG_DEVINIT
- QIBM_QTG_DEVTERM

Table 4. Required parameter group

No.	Exit point interface	Input or output?	Parameters
1	User description information	I/O	Char(*)
2	Device description information	I/O	Char(*)
3	Connection description information	Input	Char(*)
4	Environment options	Input	Char(*)
5	Length of environment options	Input	Binary(4)
6	Allow connection	Output	Char(1)
7	Allow autosign-on	Output	Char(1)

QSYSINC Member Name: ETGDEVEX
Exit Point Name: QIBM_QTG_DEVINIT
Exit Point Format Name: INIT0100

The Telnet server optionally provides for selecting or setting the device name to be used over the Telnet session, and allows for a Telnet client to bypass traditional device initialization. Administrators might control these new features through the use of a new exit program, which optionally starts just after client session establishment. Several parameters are supplied to the exit program to be used in the decision process, and the exit program can set or change various parameters before returning to the Telnet server. You can optionally register a second exit program to start just before session termination. You can use this second exit program for session auditing or virtual device management.

Telnet exit point format INIT0100: Required parameter group:

Here are the detailed descriptions of the required parameter group.

User description information

I/O; CHAR(*)

Information about the user that the system uses as part of the auto-signon process.

Device description information

I/O; CHAR(*)

Information that the system uses to create or change the device that it uses for this Telnet session.

Connection description information

I/O; CHAR(*)

Information about the client connection that the exit program can use.

Environment options

INPUT; CHAR(*)

An array containing all the RFC 4777 environment options negotiated by the client. These are in the exact format that they were in when received from the client and specified by RFC 4777. The array in general consists of 1 or more pairs of environment variable names and associated values. The RFC specifies that each variable name is always be preceded by either an X'01' or X'03' depending on whether it is an RFC 4777 defined VAR, or an application specific defined USERVAR. If a value is associated with a VAR (or USERVAR), that value will appear next in the array preceded by the RFC 1572 defined VALUE character - X'01'. This sequence of VAR/VALUE pairs is repeated up to a maximum of 1024 total bytes of negotiation data.

RFC 4777 and the more general Telnet negotiation RFCs also allow for control characters to appear within the VAR/USERVAR variable names or their associated values. This is allowed through the use of the ESC character X'02' and rules that apply when the ESC character itself or Telnet IAC control characters must appear in the negotiation sequence. Refer to RFC 1572 for a more complete description of control character escaping rules.

While the environment options buffer shows negotiations by the client, including passwords, Telnet always overlays any clear-text or encrypted password values in the buffer to avoid security exposures.

Length of environment options

The length of the environment options referenced in the preceding paragraph is typically 1024 bytes. Because option negotiations are of undefined length, any negotiations that exceed the length specified might be truncated to fit in the environment options buffer.

Allow connection

OUTPUT; CHAR(1)

Applies to all devices and indicates to the Telnet server whether all devices should allow the client to connect to the Telnet server. If the device type is display and you have enabled auto-signon, then this client might also bypass the sign-on display on the system. The Valid values are as follows:

- 0 Reject the request from the client
- 1 Accept the request from the client

Allow auto-signon

OUTPUT; CHAR(1)

Applies to DISPLAY device types, and indicates to the Telnet server whether the auto-signon operation should be allowed to proceed for this particular client. This parameter applies to display device types. If auto-signon is allowed, then this client can bypass the sign-on device on the system. The Valid values are as follows:

- 0 Reject the application request from the client. The system ignores the User profile, Current library, Program to call, Initial menu, and Device name output parameters.
- 1 Accept the application request from the client. The system may consider the User profile, Current library, Program to call, Initial menu, and Device name output parameters valid if the exit program returns them.

INIT0100: Format of user description information:

The auto-signon process uses the information about the user.

The following table shows the format of the user description information:

Table 5. Format of user description information

Offset dec	Offset hex	Type	Field
0	0	INT(4)	Length of user description information
4	4	CHAR(10)	User profile
14	E	CHAR(10)	Current library
24	18	CHAR(10)	Program to call
34	22	CHAR(10)	Initial Menu

User description information field descriptions

Current library

The name of the library that is to be made the current library if you enable the auto-signon flag. This parameter is optional, but if you supply it, you must make certain to left-align it and pad it with blanks. The value is as follows:

library name

The name of the library that you would like the system to designate as the current library.

Initial menu

The name of the initial menu to display if you have enabled the auto-signon flag. Valid value is as follows:

menu name

The name of a menu to display.

Length of user description information

The length of the user description information structure.

Program to call

The name of a program that the system calls if you have enabled the auto-signon flag. This parameter is optional, but if you supply it you must left-aligned it and pad it with blanks. The value is as follows:

program name

The name of a program that the system will start.

User profile

The user profile that the system uses for the sign-on procedure if you have enabled the auto-signon flag. The system requires this parameter, and you must left-aligned it and pad it with blanks.

INIT0100: Format of device description information:

Here are the outlines about formats for creating or changing the device used for a Telnet session.

The following table shows the format of the device description information, which describes the characteristics of the device to be associated with this session.

Table 6. Format of the device description information

Offset dec	Offset hex	Type	Field
0	0	CHAR(10)	Device name
10	A	CHAR(8)	Device format
18	12	CHAR(2)	Reserved
20	14	BINARY(4)	Offset to device attributes structure
24	18	BINARY(4)	Length of device attributes structure
28	1C	CHAR(*)	Device attributes structure

Device description information field descriptions

Device name

The specific virtual device to be associated with this Telnet session. For DISPLAY devices, if the QAUTOVRT auto-create device system value allows for it, the device is auto-created by the system if it does not already exist, and varied on. For PRINT devices, the system auto-creates the device if it does not already exist. If the exit program supplies no value, the Telnet server returns to the default of using the traditional Telnet virtual device selection methods. This should be a valid DISPLAY or PRINT device description name and must adhere to standard i5/OS object-naming conventions.

Device format

The specific virtual device type that is associated with this Telnet session. Currently only display devices that the system supports.

DSPD0100

The device is a display. The system returns display attributes.

Reserved

Reserved for future use.

Offset to device attributes structure

The offset from the start of the device description information to the start of the device attributes structure.

Length of device attributes structure

The length in the user space of the device attributes structure.

INIT0100: Format of display device description information (DSPD0100)

The following table shows the format of the display device description information, which describes the characteristics of the device to be associated with this session.

Table 7. Format of display device description information (DSPD0100)

Offset dec	Offset hex	Type	Field
0	0	CHAR(3)	Keyboard identifier
3	3	CHAR(1)	Reserved
4	4	BINARY(4)	Code page
8	8	BINARY(4)	Character set

DSPD0100 field descriptions

Character set

The character set that the system uses for this interactive job. You can find valid values in national language support (NLS). This field is identical to the Character set parameter of the Open Virtual Terminal Path (QTVOPNVT) API.

Code page

The code page that the system uses for this interactive job. You can find valid values in NLS. This field is identical to the Code page parameter of the Open Virtual Terminal Path (QTVOPNVT) API.

Keyboard identifier

The 3-character keyboard identifier that the system uses for this interactive job. The keyboard identifier implicitly specifies the code page and character set to be used, unless it is overridden as part of the Code page and Character set parameters. You can find valid identifiers in NLS. This field is identical to the keyboard Language type parameter of the Open Virtual Terminal Path (QTVOPNVT) API.

Reserved

Reserved for future use.

Related reference

Open Virtual Terminal Path QTVOPNVT API

INIT0100: Format of connection description information:

This topic contains information about the client connection that the exit program can use.

The following table shows the format of the connection description information, which describes client and connection information for this session.

Table 8. Format of connection description information

Offset dec	Offset hex	Type	Field
0	0	INT(4)	Length of connection description information
4	4	CHAR(20)	Client internet address
24	18	CHAR(1)	Client password validated
25	19	CHAR(12)	Workstation type
39	27	CHAR(1)	Secure socket layer connection
40	28	CHAR(20)	Server (local) internet address
60	3C	CHAR(1)	Client authentication level
61	3D	CHAR(3)	Reserved
64	40	INT(4)	Client certificate valid rc
68	44	INT(4)	Offset to client certificate
72	48	INT(4)	Client certificate length

Connection description information field descriptions

Length of connection description information

The length of the connection description structure.

Client internet address

The IP address (or type structure) of the requesting client, which is always provided to the exit program. The layout of the new fields is as follows:

Table 9. Client IP address layout

Name	Size	Description
sin_len	CHAR(1)	Size of the sockaddr_in structure
sin_family	CHAR(1)	Family or protocol. IP (Version 4) is hex 02
sin_port	CHAR(2)	16-bit unsigned port number
sin_addr	CHAR(16)	4-byte unsigned

Client password validated

Whether Telnet validated the clients' encrypted password (if one was received). The system sets this value if TN5250E Clients send the encrypted password for validation. The password is checked using service functions calls. This allows the exit program to guarantee secure client sign-on process.

- Value = 0, Client password/passphrase (or Kerberos ticket) was not validated or none was received.
- Value = 1, Client clear-text password/passphrase was validated.
- Value = 2, Client encrypted password/passphrase (or Kerberos ticket) was validated.

Workstation type

The workstation type requested by the client, which is one of the Internet Specifications listed in the Workstation and printer mappings table.

Secure Sockets Layer

Whether the connection is a Secure Sockets Layer (SSL) connection:

- 0 Connection is not using SSL.
- 1 Connection is using SSL.

Server internet address

The IP address (or type structure) of the host (local) network interface, which is always provided to the exit point program. The layout of the new fields is as follows.

Table 10. Client IP address layout

Name	Size	Description
sin_len	CHAR(1)	Size of the sockaddr_in structure
sin_family	CHAR(1)	Protocol family IP is hex 02, IPX is hex 06
sin_port	CHAR(2)	16-bit unsigned port number
sin_addr	CHAR(16)	4-byte unsigned network address

Client authentication level

Whether client SSL certificates are required in order to connect to the system.

- 0 No client certificate is required.
- 1 A valid client certificate is required.

Client certificate valid return code

The return code received during the SSL handshake operation when validating the client certificate.

Offset to client certificate

The offset from the start of the Connection structure to the first byte of the client certificate.

Client certificate length

The length of the client certificate that is received. If no certificate is received, then the length is 0.

Related concepts

“Troubleshooting emulation types” on page 87

When developing a Telnet client, it is important that you negotiate the correct emulation workstation type. The functions allowed vary with the workstation type. The following guide helps you understand the workstation type and the function capabilities of that workstation.

Device termination exit program

The QIBM_QTG_DEVTERM exit point occurs when a Telnet client ends the Telnet session. This allows you to log session termination information and to perform device reset or cleanup operations.

The following table shows the parameters for the QIBM_QTG_DEVTERM exit point.

1	Device name	Input	Char(10)
---	-------------	-------	----------

QSYSINC Member Name: NONE
Exit Point Name: QIBM_QTG_DEVTERM
Exit Point Format Name: TERM0100

The Telnet server optionally provides for the stopping of the device, session auditing activities, and virtual device management related to the device associated with the ended Telnet session.

Required parameter group

Device name

Input; CHAR(10) The specific virtual device that is associated with this Telnet session.

Examples: Telnet exit programs

Example programs might help you use Telnet exit points on your system.

The downloadable example programs contain the following resources:

- **Example Create Telnet exit program CL utility code (TELCRT)**
Use this code example to create, install, or register Telnet exit programs. It is written in i5/OS Command Language (CL) programming language.
- **Example Delete Telnet exit program CL utility code (TELDLT)**
Use this code example to uninstall and delete Telnet exit programs from your system. It is written in the CL programming language.
- **The basic example Telnet initialization exit program (DEVINIT1)**
The basic Telnet initialization exit program (DEVINIT1) lets you screen Telnet clients. You decide who is allowed to connect to your Telnet server and who is not. This example is basic because it is not designed to take advantage of the many other functions available to Telnet exit programs. The advanced Telnet exit program is designed to take advantage of those functions.
It is suggested that you start with the basic Telnet initialization exit program until you understand how it works, and then migrate to the advanced Telnet initialization exit program if you require Virtual Device mapping or other advanced functions.
- **The advanced example Telnet initialization exit program (DEVINIT2)**
The advanced Telnet initialization (logon) exit program uses the access lists MAP and DISALLOW. By using the MAP list instead of the simpler ALLOW list, the advanced initialization program exploits more of the exit point interface than the basic version. It allows you to set or override Telnet session settings which is a function you normally see in Client Access environments. Here are some examples of the kinds of session settings:

- Select a particular Virtual Terminal device for this session
- Bypass the sign-on panel
- Set up national language support (NLS)
- **Example Telnet termination exit program (DEVTERM)**
DEVTERM QCSRC is a simple logging program that logs a disconnect message.
This is a companion program to both DEVINIT1 QCSRC and DEVINIT2 QCSRC. The termination messages it logs can be matched with the initialization messages to determine Telnet session duration.

Telnet exit program sample files

There are two file formats available for download: ZIP and SAVF. Both formats contain the same files.

The .zip files are in a format that is compatible with PCs. Select the .zip file to download the program and information files to your PC, unzip them, and then transfer them to your system. You need to rename most of files after you save them on your system.

A .savf file is an i5/OS save file. Download it to your PC, and then transfer it to your system. You can create a temporary library on your system and transfer the save file to that. Unpack the save file in the temporary library and follow the instructions in the readme file.

Click the link for the file format you want, and then click **Save**.

Note: By using the code examples, you agree to the terms of the “Code license and disclaimer information” on page 101.

- telnet.zip (924 KB)
- telnet.savf (5.45 MB)

Managing the Telnet client

You can start a Telnet client session using different emulation types. This topic also explains how to establish a cascaded Telnet session.

The Telnet client enables a TCP/IP user to sign on and use applications on a remote system by using a Telnet server application. Telnet allows you to log on to the remote computer and use it as if you were connected directly to it. You can run programs, change configurations, or do just almost anything else you can do.

Telnet makes your computer act like a mainframe computer’s workstation. In other words, when using Telnet, your computer (the client) pretends to be, or emulates, a terminal directly attached to the remote computer (the Telnet server).

The Telnet client also supports Request for Comments (RFC) 4777. RFC 4777 clients get more control over the Telnet server virtual device on the System i platform through several new parameters on the STRTCPTELN (TELNET) command. The new parameters are:

- Remote virtual display (RMTVRTDSP)
- Remote user (RMTUSER)
- Remote password (RMTPWD) (including support for new 128-byte passwords if the Telnet Server supports them)
- Remote password encryption (RMTPWENC) (including DES7 and SHA1 encryption)
- Remote initial program (RMTINLPGM)
- Remote initial menu (RMTINLMNU)
- Remote current library (RMTCURLIB)

- Remote keyboard type (RMTKBDTYPE)
- Remote character set (RMTCHRSET)
- Remote code page (RMTCODPAG)

Controlling Telnet server functions from the client

You can use the Telnet client to control workstation processing on the Telnet server when you are in a client session.

Both the i5/OS name and the TCP/IP name are listed for each of the command functions.

To select which server functions that you want to control, you need to access the Telnet Control Functions menu. To get to this menu, press the **Attention** key on your 5250 keyboard.

The following list provides you with a brief description of each Telnet client control function:

- **Interrupting a process on the system Interrupt process or IP:** This function cancels, interrupts, or suspends a process that has started on the server. For example, you can use IP when a process appears to be in a permanent loop, or if you have started a process by accident.
- **Querying connection status when the system becomes inactive Query connection status or AYT:** This function provides a message from the server that lets you know that the system is still running. You can use this control function when the system is unexpectedly inactive for a long period of time.
- **Discarding remote output before it reaches your workstation Discard remote output data or AO:** This function allows a process that is generating output to run to completion without sending the output to your workstation. This function removes already produced system-system output that has not yet displayed on your workstation.
- **Clearing the data path between your system and the server Clear the data path or SYNCH:** This function discards all characters (except Telnet commands) between your system and the server. You can use this function when the network's flow control mechanisms cause other functions, such as IP or AO, to be buffered.
- **Ending the Telnet session End Telnet session or QUIT:** This function ends the Telnet session and closes the TCP/IP connection to the system (remote system). You can request this function any time during the Telnet session, but you should sign off the remote system before selecting this function. If you do not sign off, you remain signed on to the system because the Telnet protocol does not provide an end session sequence.
- **Using the Attention key to remote host option ATTN key to remote host:** Press the Attention key to display the Telnet Control Functions menu.

Notes:

1. This option only applies to 5250 mode.
2. If you are running VTxxx mode (VT100 or VT220), then there are two additional selections on this menu:
 - For VT100 sessions, option 6 (Change VT100 Primary Keyboard Map) and option 7 (Change VT100 Alternate Keyboard Map).
 - For VT220 session, option 8 (Change VT220 Primary Keyboard Map) and option 9 (Change VT220 Alternate Keyboard Map).

Related concepts

“Starting a Telnet client session” on page 51

You should know the name or Internet address of the remote system with which you want to start the Telnet session.

“Starting a 3270 Telnet client session” on page 53

When you start a Telnet client session using 3270 emulation, the remote system application controls your display station. You receive the same displays and enter data the same way as you do for other 3270 devices locally attached to the remote system.

“Starting a VTxxx Telnet client session” on page 58

You can start a Telnet client session using VTxxx emulation. You need to start the Telnet server on the remote system (the system that you want to connect to using Telnet).

5250 Telnet client sessions

You can use this emulation type to sign on and use applications on a remote system that has a Telnet server application.

Telnet 5250 client support allows users to sign on to other systems and access full-screen 5250 applications. 5250 full-screen support can only be negotiated with a Telnet server application running on an i5/OS operating system or a system that supports the Telnet 5250 server. Negotiating 525x work station support with the remote Telnet server application activates 5250 full-screen support.

Starting a Telnet client session

You should know the name or Internet address of the remote system with which you want to start the Telnet session.

To start a Telnet session with a remote system, follow these steps:

1. Start System i Navigator and expand *your system* → **Network**.
2. Right-click **TCP/IP Configuration** and click **Host Table** to display the Internet addresses and host names.
 1. Type the STRTCPTELN (Start TCP/IP TELNET) command, or type TELNET at the command line and press Enter.
 2. Type the name of the remote system. If you want to use optional parameters, press F10; otherwise, press Enter.
If you typed *INTERNETADR for the **Remote system** field, the server prompts you for the **Internet address** field.
3. Type the Internet address of the remote system. If you want to use optional parameters, press F10; otherwise, press Enter. The display shows optional parameter values and the Internet address information.
4. To use the default parameter values, press Enter.
5. When starting a 5250 full-screen mode session, the following optional parameters are also applicable:
 - Timeout wait for host (INZWAIT)
 - Keyboard language type (KBDTYPE)
 - Port number of the remote host server application (PORT)
 - Remote Virtual Display (RMTVRTDSP)
 - Remote User (RMTUSER)
 - Remote password (RMTPWD)
 - Remote password encryption (RMTPWDENC)
 - Remote initial program (RMTINLPGM)
 - Remote initial menu (RMTINLMNU)
 - Remote Current library (RMTCURLIB)
 - Remote Keyboard Type (RMTKBDTYPE)
 - Remote character set (RMTCHRSET)
 - Remote code page (RMTCODPAG)

The next display is the signon display for the remote system.

Notes:

1. The sign-on display is shown only if none of the Autosignon parameters is entered on the STRTCPTELN command (RMTUSER, RMTPWD, RMTPWDENC) or if there is an error when these parameters are entered. If these values are entered correctly, no sign-on display is shown. The user is automatically signed on, and whatever initial panel is defined for the user is shown.
2. In addition, the following conditions are also true:
 - If the STRTCPTELN command provides the correct RMTUSER, RMTPWD, and RMTPWDENC parameters, and a correct RMTINLPGM parameter is also provided, then the user is signed on. Also, the provided initial program runs.
 - However, if the RMTINLPGM parameter is not valid, the user is signed on, but the message job ended abnormally is displayed. The same actions are true for the RMTINLMNU parameter.
3. For the RMTCURLIB parameter, a correct value results in the user being signed on. Also, any initial program or menu, or both, as defined either in the users profile or on the STRTCPTELN command, runs. In addition the current library is set to the parameter value. If an invalid RMTCURLIB parameter value is provided, then a signon panel is displayed with a message stating that the current library value is invalid.
4. Also, for all of the preceding items, if the RMTKBDTYPE or RMTCHRSET or RMTCODPAG parameters are provided with valid values, they have taken effect for the successful automatic signon attempts. They do not take effect for the invalid signon attempts.

Note: If the system does not find or configure a SOCKS server, or if errors occur using the SOCKS server, then a direct connection is established.

TN5250 screen size

Telnet 5250 full-screen mode supports the following screen sizes:

- 1920-character (24 x 80) on all 5250 display stations.
- 3564-character (27 x 132) on all 3180 Model 2; 3197 Models D1, D2, W1, W2, and 3477 Models FA, FC, FD, FE, FG, FW.

Related reference

“Controlling Telnet server functions from the client” on page 50

You can use the Telnet client to control workstation processing on the Telnet server when you are in a client session.

“Establishing a cascaded Telnet session” on page 82

You can establish another Telnet session while you are in a current Telnet session. After you establish a cascaded session, you can move between the different systems.

3270 Telnet client sessions

The 3270 emulation type allows you to access a remote system that has a Telnet server application.

Because the 3270 data streams are translated into 5250 data streams, the workstation devices operate as a remote 5251 display to the System i platform and application programs.

Note: By using the code examples, you agree to the terms of the “Code license and disclaimer information” on page 101.

Related concepts

“Configuring Telnet server for 3270 full-screen mode” on page 25

Telnet client users can sign on and run 5250 full-screen applications using 3270 full-screen mode.

Starting a 3270 Telnet client session

When you start a Telnet client session using 3270 emulation, the remote system application controls your display station. You receive the same displays and enter data the same way as you do for other 3270 devices locally attached to the remote system.

When the Telnet client negotiates 327x workstation support with the remote Telnet server application, the system activates the 3270 full-screen mode. Telnet client negotiates 3270 full-screen support with any Telnet server application that supports 3270 full-screen (rather than 5250) applications.

You need to start the Telnet server on the remote system (the system that you want to connect to using Telnet).

You should know the name or Internet address of the remote system with which you want to start the Telnet session. To display the Internet addresses and host names, complete the following steps:

1. Start System i Navigator and expand *your system* → **Network**.
2. Right-click **TCP/IP Configuration** and click **Host Table** to display the Internet addresses and host names.
 1. Type the STRTCPTELN (Start TCP/IP TELNET) command, or type TELNET at the command line and press Enter.
 2. Type the name of the remote system. If you want to use the optional parameters, press F10; otherwise, press Enter.

If you type *INTNETADR for the **Remote system** name and press Enter, the server prompts you for the **Internet address** field.
 3. Type the Internet address of the remote system. To use the optional parameters, press F10; otherwise, press Enter. The display shows optional parameter values and the Internet address information.
 4. To use the default parameter values, press Enter. The connection to the Telnet server starts.
 5. During a 3270 full-screen mode session, the following optional parameters are also applicable:
 - Timeout wait for host (INZWAIT)
 - Keyboard language type (KBDTYPE)
 - Page up (roll down) key (PAGEUP)
 - Page down (roll up) key (PAGEDOWN)
 - Cursor select key (CSRSLT)
 - Outgoing 3270 translation table (TBL3270OUT)
 - Incoming 3270 translation table (TBL3270IN)
 - Numeric lock keyboard (NUMLCK)
 - Change how nulls are handled (NULLS)
 - Port number of the remote host server application (PORT)

The next display is the signon display for the remote system.

Related concepts

“3270 keyboard mapping for Telnet servers” on page 56

The topic contains information about keyboard mapping for support of 3270 emulation.

“3270 full-screen considerations” on page 54

You should be aware of the 3270 screen size, cursor select key, error messages, and null characters when using 3270 emulation.

Related reference

“Controlling Telnet server functions from the client” on page 50

You can use the Telnet client to control workstation processing on the Telnet server when you are in a client session.

3270 full-screen considerations

You should be aware of the 3270 screen size, cursor select key, error messages, and null characters when using 3270 emulation.

When using 3270 full-screen mode for your Telnet client, you should be aware of the following considerations:

- 3270 screen size
- The 3270 cursor select key
- 3270 error messages
- 3270 null characters

TN3270 screen size

Telnet 3270 full-screen mode requirements:

- If the negotiated 3270 device type requires 1920 characters, the Telnet client code runs with any 5250 device type as the client terminal.
- If the negotiated 3270 device type requires 3564 characters, the Telnet client code requires a 3180 Model; 3197 Model D1, D2, W1, W2; 3477 Model FA, FC, FD, FE, FG; FW 5250 device type as the client terminal.
- There is a 27x132 display when a 3180 Model 2; 3197 Mode D1, D2, W1, W2; 3477 Model FA, FC, FD, FE, FG; FW device type is negotiated. In previous releases, a data area was needed to get this support.
- To get a 24x80 display, execute the command `CRTDTAARA DTAARA(libname/QTVNO32785) TYPE(*CHAR) VALUE('1')`.

TN3270 Cursor Select key

The existing Cursor Select key is disabled if you choose to emulate the Cursor Select key. Specifying one of the following parameters for the `STRTCPTELN` command emulates the Cursor Select key:

Table 11. Parameters to emulate the cursor select key

Parameter	Value
Page Up (Roll Down) key	*CSRSLT
Page Down (Roll Up) key	*CSRSLT
Cursor Select key	*F-key (specify a function key *F1 to *F24)

TN3270 messages

When you are using Telnet 3270 full-screen mode, several types of error messages might display.

- Key entry errors appear as flashing 4-digit numbers on the lower left corner of the display. Press the Help key or F1 (Help) to obtain more information about the message. See the System Operation book if you cannot correct the error.
- System messages include Telnet messages and are issued from the system.
- For information about messages that are sent from the remote system, see the remote system documentation.

TN3270 - Handling null characters

When a 3270 display station sends a data stream, all null characters are removed. Specify one of the following values for the `handle nulls (NULLS)` parameter on the `STRTCPTELN` command:

***REMOVE**

Removes beginning and embedded null characters

***BLANK**

Changes beginning and embedded null characters to blanks. This is the default value. Trailing null characters are always removed for both values. This is the default value. For example, assume the data consists of the following code (0 indicates a null) :

```
0x0yz000
```

The data stream sent from a 5250 display station that runs Telnet 3270 full-screen with the default *BLANK contains the following code:

```
bxbyz
```

The data stream sent from a 3270 display station or from a 5250 display station running a Telnet 3270 full-screen session when the value *REMOVE is specified would contain the following code:

```
xyz
```

The value *REMOVE is valid for the following devices:

- Any locally attached display
- Displays attached to a remote 5394 controller
- Personal computer displays using the workstation function

Related concepts

“Starting a 3270 Telnet client session” on page 53

When you start a Telnet client session using 3270 emulation, the remote system application controls your display station. You receive the same displays and enter data the same way as you do for other 3270 devices locally attached to the remote system.

Using a display station

Here are keyboard and display differences when using a display station during a Telnet 3270 full-screen session. Other special considerations for Telnet 3270 mode include the number of input fields, error messages, and ending a session.

Specifying keyboard and character sets

The keyboard language type you specify for your workstation, using the keyboard language type parameter on the STRTCPTELN command, must be the same as the keyboard language type parameter of the remotely attached workstation. If you specify a keyboard language type that does not match, some of the characters do not display as expected.

5250 and 3270 keyboards

The placement and function of keys are different on the 5250 keyboard (3196G, 3180 Model 2, or 5291) than on the 3278 keyboard.

Note: For the Telnet client operating in a 3270 full-screen mode, the 3270 Clear function sets to the key sequence Shift-Cmd-Backspace by default.

The System Operation for New Users book provides keyboard differences for the following keyboards

- IBM-enhanced keyboard
- 122-key typewriter keyboard
- 5250 keyboard
- Personal computer or personal computer IBM AT computer-style keyboard
- Personal computer or personal computer AT 5250 style keyboard

- IBM-enhanced personal computer keyboard

Personal computer keyboards

If your personal computer uses the System i Access for Windows Workstation Function (WSF), you can display the layout of your 5250 keyboard using the Work Station Function Keys (WSFKEYS) command. You can alter the style using the Configure Work Station Function (CFGWSF) command. These commands are discussed in the 'Client Access/400 for DOS with Extended Memory Setup' book. If your personal computer does not use the workstation function, refer to the appropriate documentation for your emulator (for example, OS/2[®] CM/2) to view or change the keyboard style.

TN3270-Minus sign

If you specified the value *YES for the numeric lock keyboard parameter of the STRTCPTELN command, if you are using a data entry keyboard, and if the cursor is located in a numeric-only field, then complete these tasks to display a 5250 minus sign:

1. Press the Num (Numeric) key.
2. Press the minus sign (-) key.

To display a 3278 minus sign, press the minus sign key.

TN3270-Page down and page up

If the 3270 application has a display that does not allow all the input data fields to be viewed, use the 5250 Page Down and Page Up keys to enter data when the maximum number of input fields on the display is exceeded.

You can also assign PF and PA functions to the page keys by specifying their use on the STRTCPTELN command.

The cursor always appears as an underline on both 5250 and 3270 displays.

3270 keyboard mapping for Telnet servers

The topic contains information about keyboard mapping for support of 3270 emulation.

The following table shows the default PF key assignments to perform the various 5250 functions. You can use the Display Keyboard Map (DSPKBDMAP) command to see the current keyboard mapping. Or you can use option 6 (Display 3270 keyboard map) on the Configure TCP/IP Telnet Menu, while your terminal is in 3270 emulation mode.

Table 12. Default PF key assignments

5250 function key	Default 3270 keys to select function
Help	PF1
3270 Help	PF2
Clear	PF3
Print	PF4
Display Embedded Attributes	PF5
Test Request	PF6
Roll Down	PF7
Roll Up	PF8
Error Reset	PF10 or Enter
Sys Req	PF11

Table 12. Default PF key assignments (continued)

5250 function key	Default 3270 keys to select function
Record Backspace	PF12
F1 through F12	Press PA1, then one of the following: PF1 through PF12
F13 through F24	Press PA2, then one of the following: PF1 through PF12 or PF13 through PF24 (if present)
Field Exit	Erase EOF, then Field Tab
Attention	For 3277 use Test Request, then PA1. For 3278/3279 use ATTN key

The following example control language (CL) program sets the keyboard map for a 327x-type workstation that is using Telnet to go to a System i platform. This program maps the i5/OS function keys to their equivalent function keys on the 327x workstation. If you attempt to run a CHGKBDMAP command from a workstation not in 3270 emulation mode, you will receive the CPF8701 message. By monitoring the message, the rest of the program goes unused in these circumstances.

Note: By using the code examples, you agree to the terms of the “Code license and disclaimer information” on page 101.

```
PGM
MONMSG      MSGID(CPF8701 CPF0000)
CHGKBDMAP  PF1(*F1) PF2(*F2) PF3(*F3) PF4(*F4) PF5(*F5)
           PF6(*F6) PF7(*DOWN) PF8(*UP) PF9(*F9)
           PF10(*F10) PF11(*F11) PF12(*F12)
           PA1PF1(*HELP) PA1PF2(*HLP3270)
           PA1PF3(*CLEAR) PA1PF4(*PRINT)
           PA1PF5(*DSPATR) PA1PF6(*TEST) PA1PF7(*F7)
           PA1PF8(*F8) PA1PF9(*ATTN) PA1PF10(*RESET)
           PA1PF11(*SYSREQ) PA1PF12(*BCKSPC)
ENDPGM
```

By storing this CL source as part of the QCLSRC file in library TCPLIB as member CHGKBD, you can create the CL program Change Keyboard Map (CHGKBD) into the TCPLIB library by using the following CL command:

```
CRTCLPGM PGM(TCPLIB/CHGKBD) SRCFILE(TCPLIB/QCLSRC)
TEXT('Change the keyboard mapping for 327x terminals')
```

The CHGKBD program can then be called by anyone using Telnet to a System i platform. It can also be called automatically at sign-on time by specifying the CHGKBD program for the Initial program parameter on the Change User Profile (CHGUSRPRF) command, or the CHGKBD program can be called by the profile’s initial program.

PA1 and PA2 keys on a PC keyboard

The PA1 and PA2 keys do not appear on a PC keyboard. A keyboard map in your 3270 emulator provides the function of these 3270 keys on a PC keyboard.

The default 3270 Telnet keyboard map uses these keys. Therefore, it is important that you know where these keys are on the keyboard before starting a 3270 Telnet session. This is especially important if you are planning to start a session without changing the keyboard mapping. You should refer to your emulator documentation for the keys or keystrokes required to provide these functions.

There are some 5250 key sequences for which there is no supported 3270 key sequence and, therefore, it is not possible to set these keyboard commands on a 3270. These key sequences are as follows:

- Field Plus
- Field Minus
- Erase all input fields

The 5250 Field Exit Key function is performed on a 3270 keyboard, using the Erase EOF key and then the tab key.

Special circumstances

When using Telnet 3270 full-screen mode from the 3270 terminal and before the default mapping for the terminal is changed, the keys PF1 to PF12 might be emulated by the key sequence PA1 PF x . Therefore, instructions like Press PF3 or Press PF4 should read: Press PA1 PF3 and Press PA1 PF4, before creating a new keyboard map.

Depending on the installation of the Telnet client for the host (for example, a virtual machine (VM) Telnet client), when pressing PA1, the user might get the instruction TELNET command: at the bottom line of the display. If the system displays this instruction, type PA1, press the Enter key, move the cursor to the command line; and press the required PF key.

Note: The *Host Command Facility (HCF)* is a feature available on System/370™, 43xx, and 30xx host systems. This feature enables a user on the host system to use applications on a System i platform. If you use HCF to connect to a System i platform and then use Telnet to sign on to another System i platform from that platform, you are in a 3270 full-screen mode session. The keyboard maps twice, once for the initial HCF session and once for the Telnet session. To use your PF keys the way you normally would, you must change the keyboard mapping on both platforms. Make sure that you use the same keyboard mapping on each platform.

Related concepts

“Starting a 3270 Telnet client session” on page 53

When you start a Telnet client session using 3270 emulation, the remote system application controls your display station. You receive the same displays and enter data the same way as you do for other 3270 devices locally attached to the remote system.

“Configuring Telnet server for 3270 full-screen mode” on page 25

Telnet client users can sign on and run 5250 full-screen applications using 3270 full-screen mode.

VTxxx Telnet client sessions

VTxxx Telnet client sessions provide information about using this emulation type to sign on and use applications on a remote system that has a Telnet server application. This section also provides more information about VTxxx emulation.

Telnet VTxxx support enables users to sign on to platforms other than the System i platform as if they were on a VTxxx terminal locally attached to the system. Vtxxx client support allows users to sign on to any remote system in a TCP/IP network that supports the Vtxxx byte stream. As a Telnet user, you should be aware of the physical and operational differences between VTxxx and 5250 sessions.

Related concepts

“Configuring Telnet server for VTxxx full-screen mode” on page 28

VTxxx server support enables Telnet client users to log on and run 5250 full-screen applications, even though VTxxx full-screen support is negotiated.

Starting a VTxxx Telnet client session

You can start a Telnet client session using VTxxx emulation. You need to start the Telnet server on the remote system (the system that you want to connect to using Telnet).

You should know the name or Internet address of the remote system with which you want to start the Telnet session.

To start a VTxxx Telnet session to the remote system, follow these steps:

1. Start System i Navigator and expand *your system* → **Network**.
2. Right-click **TCP/IP Configuration** and click **Host Table** to display the Internet addresses and host names.
3. Type the STRTCPTELN (Start TCP/IP TELNET) command, or type TELNET at the command line and press Enter.
4. Type the name of the remote system, or type *INTNETADR if you prefer to use the Internet address. If you want to see the optional parameters, press F10; otherwise, press Enter.
If you typed *INTNETADR for the **Remote system** field, the system prompts you for the **Internet address** field.
5. Type the Internet address of the remote system. To use the optional parameters, press F10; otherwise, press Enter. The display shows optional parameter values and the Internet address information.
6. To use the default parameter values, press Enter.
7. During a VTxxx full-screen mode session, the following optional parameters are also applicable:
 - Incoming ASCII translation table (TBLVTIN)
 - Outgoing ASCII translation table (TBLVTOUT)
 - Special table out (TBLVTDRWO)
 - Special table in (TBLVTDRWI)
 - Options selected (VTOPT)
 - Display character attributes (DSPCHRATTR)
 - Page scroll feature (PAGE_SCROLL)
 - Answer back feature (ANSWERBACK)
 - Tab Stops (TABSTOP)
 - Timeout wait for host (INZWAIT)
 - Coded character set identifier (CCSID)
 - ASCII operating mode (ASCOPRMOD)-- applies to initializing a VT220 session only (has no effect on negotiations)
 - Port number of the remote host server application (PORT)
 - Control Characters (CTLCHAR)

Note: Unexpected characters might appear due to the incorrect configuration of the remote system. If this happens, verify that the workstation-type value is an appropriate value for a VTxxx full-screen mode workstation. You can also use the set term command to change the full-screen mode of the connection.

The next display is the sign-on display for the remote system.

Related concepts

“VTxxx full screen considerations” on page 60

As with any emulation type, you should be aware of certain considerations before using the VTxxx full-screen mode with your Telnet Server. These considerations include security concerns as well as possible error conditions and indicator lights. You can understand how to use VTxxx full-screen mode better if you become familiar with these considerations.

Related reference

“Controlling Telnet server functions from the client” on page 50

You can use the Telnet client to control workstation processing on the Telnet server when you are in a client session.

“VTxxx key values” on page 65

VTxxx key values provide keyboard mapping for support of VTxxx emulation. The client session support for both the VT100 and VT220 modes provides a primary and alternate keyboard map.

“VTxxx national mode” on page 71

VTxxx national mode supports the national replacement character set, which is a group of 7-bit character sets.

VTxxx full screen considerations

As with any emulation type, you should be aware of certain considerations before using the VTxxx full-screen mode with your Telnet Server. These considerations include security concerns as well as possible error conditions and indicator lights. You can understand how to use VTxxx full-screen mode better if you become familiar with these considerations.

In addition to security concerns, there are many other concerns to consider before using VTxxx full-screen mode with your Telnet server. When using VTxxx full-screen mode, you should be aware of the following concerns:

- “Security considerations for VTxxx full-screen mode”
- “Telnet and SNA 5250 pass-through considerations for VTxxx full-screen mode”
- “System request processing for VTxxx sessions”
- “Error conditions on 5250 keyboard” on page 61
- “Displaying stations and VTxxx support” on page 61
- “Operational differences between VTxxx and 5250 terminals.” on page 61
- “Keyboard characteristics” on page 62
- “Screen characteristics” on page 63
- “VTxxx screen size” on page 63
- “VTxxx character attributes” on page 63

Security considerations for VTxxx full-screen mode

The number of sign-on attempts allowed increases if Telnet automatically configures virtual devices. The number of sign-on attempts is equal to the number of system sign-on attempts allowed multiplied by the number of virtual devices possible.

The QMAXSIGN system value defines the number of system sign-on attempts allowed. The QAUTOVRT system value defines the number of virtual devices Telnet can create.

Telnet and SNA 5250 pass-through considerations for VTxxx full-screen mode

The System i platform supports 5250 pass-through. 5250 pass-through is similar to Telnet, but runs on a Systems Network Architecture (SNA) protocol network rather than an IP network. 5250 pass-through uses virtual displays to direct output to the physical devices just as Telnet does. In 5250 pass-through, the system automatically creates virtual devices in the same way as it does for Telnet. Therefore, the devices system value controls the number of automatically configured virtual devices for both 5250 pass-through and Telnet.

System request processing for VTxxx sessions

The system request processing for the VTxxx sessions is slightly different than that for a normal 5250 workstation.

When the System Request key is pressed on a 5250 workstation, a system request command line appears at the bottom of the is shown. If you press the Enter key, the System Request menu appears.

For VTxxx sessions when you call the system request function, the System Request menu displays immediately.

Error conditions on 5250 keyboard

Certain error conditions cause a 5250 keyboard to lock and an error code to display on the message line. An example of such a condition is typing when the cursor is not in an input field. For VTxxx sessions, these errors cause a bell to sound on the VTxxx workstation and the keyboard to remain unlocked.

Certain i5/OS applications also lock the 5250 keyboard and turn on the 5250 input-inhibited light. The user must press the Error Reset key before the keyboard unlocks. For VTxxx sessions, the locking of the 5250 keyboard causes a bell to sound on the VTxxx terminal whenever a key is pressed. To unlock the keyboard, the VTxxx key that is mapped to the Error Reset key must be pressed. In the default VTxxx keyboard map, the CTL-R key maps to the Error Reset key.

Displaying stations and VTxxx support

When the system negotiates VTxxx support, the Telnet server transmits screens that are a maximum of 24 rows by 80 columns. The VTxxx client system sees these screens in much the same way as they appear on a 5251 Model 11 workstation. However, there are some differences.

A 5251 workstation has indicator lights on the right side that indicate: System Available, Message Waiting, Keyboard Shift, Insert Mode, and Input-Inhibited.

The VTxxx server support emulates the System Available light by putting an asterisk in column 80 of row 9. For Message Waiting, Insert Mode, and Input-Inhibited lights, the asterisk appears in column 80 of rows 11, 13, or 15. When an asterisk appears, the asterisk overwrites the character that was previously displayed at that screen location. By default, the VTxxx server does not display the indicator lights. You can enable or disable these indicators by typing the key sequence that is mapped to the toggle indicator lights function. The default key sequence for this function is ESC-T.

Notes:

- When using a VTxxx client to attach to the Telnet server, note that the Insert Mode and the Input-Inhibited lights might not always display as described above. 5250 supports the attachment as a local function while the VTxxx has no such facility. The System Available and Message Waiting indicators, however, display correctly.
- A 5251 display supports a screen attribute known as a column separator. The column separator is a vertical line displayed between characters. This line does not take up a character space. The VTxxx does not support such an attribute. If an i5/OS application generates a screen that uses the column separator attribute, that screen is displayed on the VTxxx client system with the column separator mapped to the VTxxx underline attribute.

Operational differences between VTxxx and 5250 terminals.

As a Telnet user, you should be aware of physical and operational differences between VTxxx and 5250 terminals.

The 5250 is a block mode terminal. Data typed on a 5250 is accumulated in a buffer and only sent to the System i platform when an AID (attention identifier) key is pressed. An AID key on a 5250 keyboard is a key that initiates a function. The following list shows the AID keys on a 5250 keyboard:

- Clear
- Command Function 1 through 24
- Enter/Rec Adv
- Help

- Print
- Record Backspace Function
- Roll Down (Page Up)
- Roll Up (Page Down)

VTxxx terminals operate in a character mode. Characters transmit immediately to the host when a key is pressed.

Another difference is the way the data arrives on the display. The system writes data to a VTxxx terminal one character at a time, and you see the data arrive as streams of characters. With the 5250, the system writes data in blocks, and all or part of the display changes at once.

Keyboard characteristics

You should avoid using the 5250 cursor movement keys. Instead, you should use the function keys associated with the *CSRUP, *CSRDOWN, *CSRRIGHT, and *CSRLEFT keywords. By default these are keys F13, F14, F15, and F16. If you use the 5250 cursor movement keys, the VTxxx application you are using might not function as expected. This is because the results of using these keys do not transmit to the remote system until an attention identifier (AID) key is pressed.

For example, using Telnet to the System p[®] system and obtaining VT220 emulation, the System Management Interface Tool (SMIT) command provides a menu driven interface to AIX[®]. Here the function keys associated with *CSRxx keywords perform as you would expect the cursor movement keys to do. However, the 5250 cursor movement keys, while physically moving the cursor down the screen and correctly selecting the SMIT option, do not cause the selected option to be highlighted. The highlighting in reverse image remains with the first option on the SMIT menu, regardless of the key position.

Typing a control character on a keyboard is different from typing a control character on an actual VTxxx terminal. On a VTxxx terminal, press and hold down the control key while pressing the character associated with the control function.

When using the Telnet support, the equivalent is achieved by typing a 2-character control indicator followed by pressing the function key associated with the Send without Carriage Return (*SENDWOCR) default function (the F11 key). For example, if the default keyboard map and the default STRTCPTELN command parameters are in effect, the VTxxx Control-C function can be entered by typing &C followed by pressing the F11 key. <F12> can also enter this function, using the default keyboard map. In case you are using an application where <F12> is remapped, this example is included, and illustrates the principle of the *SENDWOCR key.

Use the CTLCHAR parameter of the STRTCPTELN command to select the character used to indicate a control character. The default is &. The &C characters must be the last characters typed before pressing the *SENDWOCR function key or the &C is not interpreted as a control character. A control character only transmits when the *SENDWOCR function key is pressed. You can assign frequently used VTxxx control characters to a function key. The following is a descriptive example of the Ctrl-C command. When using a Telnet client to connect to a System p system, the system typically negotiates VT220 emulation. The Ctrl-C sequence is an important one in AIX to end long running commands, such as PING. It is important that you know how to do this before issuing any System p commands. By default the sequence is &C<F11>. Note that you need to enter these keys quickly, and it might take several attempts before the System p task accepts the input.

If you do not want to display the typed characters, press the function key that is associated with the *HIDE function (F6 on the default keyboard map). Use this function when typing a password.

If you want the characters that have been typed to be sent to the remote system for processing without pressing the Enter key, you should press the function key associated with the *SENDWOCR function (F11 on the default keyboard map).

It is often useful to be able to recall previously entered commands. On the System i platform, F9 often provides this function. On AIX, this can be activated by typing the command set -o vi and pressing Enter. After this, you can start retrieving commands with the sequence Esc-K. To perform this sequence using the default keyboard map while in VTxxx emulation, you should use the sequence <F5>k<F11>. The Esc character starts the command retrieval. Then use the letter k to retrieve further commands. While operating in this mode, the commands H for right, L for left, X for delete, I for insert, and R for replace apply. The sequence<F5>i<F11> switches this function off.

Screen characteristics

The character in the position just before the cursor position is always be blank. The actual character saves internally and shows when the display refreshes with the cursor in a different position.

A VTxxx application that uses row 1, column 1 of the display does not work the same when using Telnet client support. Most 5250-type display stations do not allow input to row 1, column 1. If the VTxxx application positions the cursor at row 1, column 1, the system puts the cursor at row 1, column 2 automatically.

Due to architectural differences, the system ignores certain unsupported commands or sequences. An example is downstream loadable character sets.

VTxxx screen size

Telnet VTxxx full-screen mode supports the following screen sizes:

- On 3180 display stations:
 - 24 x 80 VTxxx screens should display as 24 x 80.
 - 24 x 132 VTxxx screens should display as 24 x 132.
- On 5250 display stations:
 - 24 x 80 VTxxx screens should display as 24 x 80.
 - 24 x 132 screens require the function key assigned to *SHIFTDSP (F10 on the default keyboard map) to move the information about the screen right or left.

VTxxx character attributes

A VTxxx terminal supports the following attributes:

- Blink
- Bold
- Reverse image
- Underline
- Any combination of the above

The 5250 data stream supports the previous attributes so that a 5250 display station can represent all of the VTxxx attributes. However, there are some limitations:

- The 5250 data stream can only support three of the character attributes at the same time. The underline, blink, and reverse image attributes display when the remote system selects all the VTxxx attributes at the same time. A 5250 display station cannot display the combination of underline, bold, and reverse image. Underline and reverse image displays when a VTxxx application selects this combination.

- The attribute byte takes up a space on the 5250 display stations that do not support extended attributes. Attributes do not take up space on a VTxxx terminal. This means that if you select character attributes, you do not see all of the data shown on the 5250 display. When receiving VTxxx data that is to display with character attributes, the 5250-attribute byte overlays the position before the data. The character that was displayed there is lost. If a character is to display in row 1, column 1 with the attributes set, that character is not displayed. You can choose not to have the character attributes displayed by specifying DSPCHRATTR(*NO) on the STRTCPTELN command. This allows you to see all of the data on the display without attributes.

Note: This restriction is not applicable for displays that support extended attributes such as the 3477 display.

VT100 keyboard indicator

A VT100 terminal has an L1 indicator that can be programmed for different applications. This indicator is not emulated by the Telnet support.

Related concepts

“Starting a VTxxx Telnet client session” on page 58

You can start a Telnet client session using VTxxx emulation. You need to start the Telnet server on the remote system (the system that you want to connect to using Telnet).

“Determining problems with Telnet” on page 84

You need diagnostic information to troubleshoot Telnet, including a flow chart for system problem analysis, and you need a list of materials when reporting Telnet problems.

VTxxx emulation options

When using VTxxx full-screen mode with your Telnet server, there are a few optional procedures that you can do to personalize the emulation type. You can display the current keyboard map and then decide whether you want to change it. You can also change the control characters when using VT220 full-screen mode.

Displaying a VTxxx keyboard map

To display the current keyboard map, use the Display VT Keyboard Map (DSPVTMAP) command. This command has no parameters. You are shown the VTxxx keys that are mapped to the i5/OS functions.

The DSPVTMAP command is only valid when called from within a Telnet server session operating in VTxxx full-screen mode.

Type DSPVTMAP to see the following display, and then press the Page Down key to see the additional displays. You can display the VT keyboard map using option 3 from the Configure TCP/IP Telnet menu.

Setting a VTxxx keyboard map

To change the default keyboard map, use the Set VT Keyboard Map (SETVTMAP) command. This command is also available by using option 5 (Set VT keyboard map) from the Configure TCP/IP Telnet menu. The shipped default keyboard map specified, restores after running the command without any user-specified parameters. You can specify up to four of the defined special values for each parameter. A special value cannot be used to specify more than one i5/OS function.

Changing a VTxxx keyboard map

Like SETVTMAP, the Change VT Keyboard Map (CHGVTMAP) command allows you to customize keyboard mapping when you are connected to a Telnet server in VTxxx mode. Whereas the parameters for the CHGVTMAP command default to the currently set values. Except for this distinction, the two commands are identical.

VTxxx automatic wrap

The VTxxx server requires the VTxxx client to have the automatic wrap (autowrap) option turned on. When autowrap is on, a character written to column 80 of the VTxxx causes the cursor to move to column 1 of the next line. Refer to your VTxxx client documentation for details of how to set on this option.

VT220 control characters

When VT220 8-bit emulation is negotiated, the range of characters X'80' through X'9F' are protected as C1 control characters as architecturally defined in the DEC VT220 Programmer Reference Manual. This might result in the system interpreting succeeding characters in a data stream as data in relation to these characters. If the system negotiates VT220 7-bit or VT100, then the full range of characters from X'80' through X'F' is available for character translation. Interpret X'80' through X'9F' as C1 control characters in VT220 8-bit control mode only.

This has particular relevance to National Language Support (NLS), as several non-English languages use these values for language-specific characters. In these cases, the VT220 8-bit emulation might not function as anticipated.

Related concepts

“Configuring Telnet server for VTxxx full-screen mode” on page 28

VTxxx server support enables Telnet client users to log on and run 5250 full-screen applications, even though VTxxx full-screen support is negotiated.

Related reference

“VTxxx key values”

VTxxx key values provide keyboard mapping for support of VTxxx emulation. The client session support for both the VT100 and VT220 modes provides a primary and alternate keyboard map.

VTxxx key values

VTxxx key values provide keyboard mapping for support of VTxxx emulation. The client session support for both the VT100 and VT220 modes provides a primary and alternate keyboard map.

To accommodate the additional keypad capabilities of the VT220 mode, you can save your keyboard map. By using the F6 key from the Change VTxxx Keyboard Map display, you can save all changes to these keyboard maps for later sessions. The data saves in the user profile, and will automatically apply the next time Telnet VTxxx emulation is activated.

The keyboard option that you select from the Send Telnet Control Functions menu determines which keyboard map you use. Figures 2 through 9 show the VTxxx functions that correspond to the 5250 AID key. The following list gives the option number and the corresponding figures:

- Figure Figure 1 on page 66 and Figure 2 on page 66 show option 6 (Change VT100 Primary Keyboard Map).
- Figure 3 on page 67 and Figure 4 on page 67 show option 7 (Change VT100 Alternate Keyboard Map).
- Figure 5 on page 68 and Figure 6 on page 68 show option 8 (Change VT220 Primary Keyboard Map).
- Figure 7 on page 69 and Figure 8 on page 69 show option 9 (Change VT220 Alternate Keyboard Map).

The level of support negotiated between the System i platform and the Telnet server determines which options display on the Send Telnet Control Functions menu. The menu displays options 6 and 7 if the VT100 full-screen mode support negotiates initially. The menu displays options 8 and 9 if the VT220 full-screen mode support negotiates initially.

Note: There are no differences in the default values of the VT100 primary and alternate keyboard maps.

The following figures show the default keyboard mappings. You can change any of the values. If you press the Enter key, your changes are saved for the current session only. If you press F6 (Save), your changes are saved permanently and are in effect the next time you start a VTxxx Telnet session.

```
Change VT100 Primary Keyboard Map
Type changes, press Enter:
5250 key          VT100 function
Function Key 1 . . . *PF1
Function Key 2 . . . *PF2
Function Key 3 . . . *PF3
Function Key 4 . . . *PF4
Function Key 5 . . . *ESC
Function Key 6 . . . *HIDE
Function Key 7 . . . *TAB
Function Key 8 . . . *CTLA
Function Key 9 . . . *CTLB
Function Key 10 . . *SHIFTDSP
Function Key 11 . . *SENDWOCR
Function Key 12 . . *CTLC
Function Key 13 . . *CSRUP
Function Key 14 . . *CSRDOWN
Function Key 15 . . *CSRRIGHT
Function Key 16 . . *CSRLEFT

More...

F3=Exit  F6=Save  F12=Cancel
```

Figure 1. Change VT100 primary keyboard map (Display 1)

```
Change VT100 Primary Keyboard Map
Type changes, press Enter:
5250 key          VT100 function
Function Key 17 . . *CTLD
Function Key 18 . . *CTLE
Function Key 19 . . *CTLF
Function Key 20 . . *CTLG
Function Key 21 . . *CTLH
Function Key 22 . . *CTLI
Function Key 23 . . *CTLJ
Function Key 24 . . *CTLK
Rollup key . . . . *CTLL
Rolldown key . . . *CTLM

Bottom

F3=Exit  F6=Save  F12=Cancel
```

Figure 2. Change VT100 primary keyboard map (Display 2)

```

Change VT100 Alternate Keyboard Map
Type changes, press Enter:
5250 key          VT100 function
Function Key 1 . . . *PF1
Function Key 2 . . . *PF2
Function Key 3 . . . *PF3
Function Key 4 . . . *PF4
Function Key 5 . . . *ESC
Function Key 6 . . . *HIDE
Function Key 7 . . . *TAB
Function Key 8 . . . *CTLA
Function Key 9 . . . *CTLB
Function Key 10 . . *SHIFTDSP
Function Key 11 . . *SENDWOCR
Function Key 12 . . *CTLC
Function Key 13 . . *CSRUP
Function Key 14 . . *CSRDOWN
Function Key 15 . . *CSRRIGHT
Function Key 16 . . *CSRLEFT

More...

F3=Exit  F6=Save  F12=Cancel

```

Figure 3. Change VT100 alternate keyboard map (Display 1)

```

Change VT100 Alternate Keyboard Map
Type changes, press Enter:
5250 key          VT100 function
Function Key 17 . . *CTLD
Function Key 18 . . *CTLE
Function Key 19 . . *CTLF
Function Key 20 . . *CTLG
Function Key 21 . . *CTLH
Function Key 22 . . *CTLI
Function Key 23 . . *CTLJ
Function Key 24 . . *CTLK
Rollup key . . . . *CTLL
Rolldown key . . . *CTLM

Bott

F3=Exit  F6=Save  F12=Cancel

```

Figure 4. Change VT100 alternate keyboard map (Display 2)

You can switch between the primary and alternate keyboard maps during a VTxxx session using the function key assigned to the *KEYPRI and *KEYALT keywords. You can assign these keywords to any of the available 5250 function keys. It is recommended that you assign *KEYPRI to the Page Up 5250 function key and *KEYALT to the Page Down 5250 function key for both primary and alternate keyboard maps.

Change VT220 Primary Keyboard Map

Type changes, press Enter:

5250 key	VT220 function
Function Key 1 . . .	*PF1
Function Key 2 . . .	*PF2
Function Key 3 . . .	*PF3
Function Key 4 . . .	*PF4
Function Key 5 . . .	*ESC
Function Key 6 . . .	*HIDE
Function Key 7 . . .	*TAB
Function Key 8 . . .	*CTLA
Function Key 9 . . .	*CTLB
Function Key 10 . . .	*SHIFTDSP
Function Key 11 . . .	*SENDWOCR
Function Key 12 . . .	*CTLC
Function Key 13 . . .	*CSRUP
Function Key 14 . . .	*CSRDOWN
Function Key 15 . . .	*CSRRIGHT
Function Key 16 . . .	*CSRLEFT

More...

F3=Exit F6=Save F12=Cancel

Figure 5. Change VT220 primary keyboard map (Display 1)

Change VT220 Primary Keyboard Map

Type changes, press Enter:

5250 key	VT220 function
Function Key 17 . . .	*CTLD
Function Key 18 . . .	*CTLE
Function Key 19 . . .	*CTLF
Function Key 20 . . .	*CTLG
Function Key 21 . . .	*CTLH
Function Key 22 . . .	*CTLI
Function Key 23 . . .	*CTLJ
Function Key 24 . . .	*CTLK
Page up (rolldown) . . .	*KEYPRI
Page down (rollup) . . .	*KEYALT

Bottom

F3=Exit F6=Save F12=Cancel

Figure 6. Change VT220 primary keyboard map (Display 2)

```

Change VT220 Alternate Keyboard Map
Type changes, press Enter:
5250 key          VT220 function
Function Key 1 . . . *PF1
Function Key 2 . . . *PF2
Function Key 3 . . . *PF3
Function Key 4 . . . *PF4
Function Key 5 . . . *ESC
Function Key 6 . . . *HIDE
Function Key 7 . . . *TAB
Function Key 8 . . . *CTLA
Function Key 9 . . . *CTLB
Function Key 10 . . *SHIFTDSP
Function Key 11 . . *SENDWOCR
Function Key 12 . . *CTLC
Function Key 13 . . *CSRUP
Function Key 14 . . *CSRDOWN
Function Key 15 . . *CSRRIGHT
Function Key 16 . . *CSRLEFT

More...

F3=Exit  F6=Save  F12=Cancel

```

Figure 7. Change VT220 alternate keyboard map (Display 1)

```

Change VT220 Alternate Keyboard Map
Type changes, press Enter:
5250 key          VT220 function
Function Key 17 . . *CTLD
Function Key 18 . . *FINDKEY
Function Key 19 . . *INSERTKEY
Function Key 20 . . *REMOVEKEY
Function Key 21 . . *SELECTKEY
Function Key 22 . . *PREVSCN
Function Key 23 . . *NEXTSCN
Function Key 24 . . *CTLK
Rollup key . . . . *KEYPRI
Rolldown key . . . . *KEYALT

Bottom

F3=Exit  F6=Save  F12=Cancel

```

Figure 8. Change VT220 alternate keyboard map (Display 2)

You can enter several types of VTxxx information to change the keyboard map. Here are some examples:

Character data: You can assign a character string to a function key. For example, assume that you are on a System i model and are using Telnet to establish a connection with System p system. To assign the character string set term=vt100 to the following function key:

```
Function Key 24 .. *CTLK
```

From the system you can type:

```
Function Key 24 . . 'set term=vt100'
```

This allows you to press a function key rather than always having to type that character string.

When you press the function key during a VTxxx session, the character string assigned to that function key transmits to the remote system with the carriage return, line feed characters added. If you type data before pressing the function key, the system adds the character string to the data that you type. This

allows you to assign a frequently used command string to a function key. The character data that you type maps from EBCDIC to ASCII, before transmission to the remote system.

Control key keywords: You can assign a VTxxx control keystroke to a function key using a defined keyword. For example, if you wanted to assign a different VTxxx control keystroke to the following function key:

```
Function Key 24 . . *CTLK
```

You can type:

```
Function Key 24 . . *CTLZ
```

When you press the function key, the new control character assigned to the function key transmits to the remote system. If you type data before pressing the function key, the control character adds to the typed data and transmits to the remote system.

Hexadecimal data: You can assign a hexadecimal string to a function key. When you press the function key, the hexadecimal data transmits to the remote system. The carriage return, and line feed characters are not added to hexadecimal data. If you type data before pressing the function key, the hexadecimal data adds to the typed data and transmits to the remote system. This allows you to type a character that is not on the 5250 keyboard (for example, square brackets). To assign a hexadecimal string, type X followed by a quoted string of hexadecimal characters, for example, X'1A1A'. The hexadecimal data does not map before transmission to the remote system.

Local i5/OS control functions: You can assign a keyword to be handled locally within the Telnet client session. These assignments or mappings might not result in the ASCII data stream traffic transmitting to the remote Telnet server session. These local control functions are *HIDE, *SHIFTDSP, *KEYPRI, and *KEYALT. The send without carriage return (*SENDWOCR) function is also a local function, but in this case, the ASCII data streams transmit to the remote Telnet server session.

Related concepts

“Starting a VTxxx Telnet client session” on page 58

You can start a Telnet client session using VTxxx emulation. You need to start the Telnet server on the remote system (the system that you want to connect to using Telnet).

Related reference

“VTxxx emulation options” on page 64

When using VTxxx full-screen mode with your Telnet server, there are a few optional procedures that you can do to personalize the emulation type. You can display the current keyboard map and then decide whether you want to change it. You can also change the control characters when using VT220 full-screen mode.

VTxxx national language support:

VTxxx national language support (NLS) provides alternative methods of selecting character mapping between the client and systems with VTxxx emulation.

These methods are:

- Coded character set identifier (CCSID)
- Multinational mode
- National mode

If none of these modes is suitable, you might set up and specify your own user-defined mapping tables.

Note: VTxxx support is limited to a subset of single-byte character set (SBCS) languages. A list of the supported languages is found later in this topic. Any of these supported single-byte language

translation tables can be modified to map any single-byte language that is preferred, then identified in the appropriate parameter for starting Client Telnet.

Mode selection is done with the CCSID parameter of the Start TCP/IP Telnet (STRTCPTELN) command. The incoming ASCII/EBCDIC table (TBLVTIN) and outgoing EBCDIC/ASCII table (TBLVTOUT) parameters of this command allow the specification of user-defined mapping tables. If these are not required, the default value of *CCSID allows for character mapping by using the mode specified in the CCSID parameter.

VTxxx multinational mode

The multinational mode supports the DEC multinational character set, which is an 8-bit character set that contains most characters used in the major European languages. The ASCII character set is included in the DEC multinational character set. The DEC multinational character set is used by default.

VTxxx national mode:

VTxxx national mode supports the national replacement character set, which is a group of 7-bit character sets.

Only one character set from the group is available for use at any one time. VT220 also supports the standard 7-bit ASCII character set as part of the national mode. The VT220 terminal supports the following national languages in 7-bit ASCII character sets:

- British
- Danish
- Dutch
- Finnish
- French
- French/Canadian
- German
- Italian
- Norwegian
- Spanish
- Swedish
- Swiss
- U.S. English

To use a national mode, the system requires mapping tables to map incoming ASCII data into Extended Binary Coded Decimal Interchange Code (EBCDIC) and outgoing EBCDIC data into ASCII when operating in VTxxx full-screen mode.

Use the coded character set identifier (CCSID) parameter on the Telnet command to select a national mode, that is an NLS mapping table.

Entering a numeric value that represents a registered CCSID value in the range 1 to 65 553 is one way to identify the appropriate mapping table. The AS/400® International Application Development V4R2  book contains details of registered CCSIDs.

The NLS mapping tables are built dynamically to a remote system the first time Telnet is used, and are based on DEC national replacement character sets. Because the character sets are 7-bit based, they can contain only the unique characters from one region. Because the DEC multinational character set is 8-bit based, it allows for the inclusion of the unique characters from a group of countries.

Identifying table objects

You can identify the table objects (*TBL) using the Work with Object command: WRKOBJ OBJ(QUSRSYS/Q*) OBJTYPE(*TBL)

All of the system table objects are in the QUSRSYS library.

The table objects are named *Qxxxyyyzzz*, where *xxx* is the FROM code page, *yyy* is the TO character set, and *zzz* is the TO code page.

Here are the guidelines for the outgoing (EBCDIC-to-ASCII) table:

- The FROM code page ID is taken from the code page ID in QCHRID of message description CPX8416 (use WRKMSGD CPX8416 to display), 37 in the following figure from a US English-based system.
- The TO character set and code page are derived from the CCSID parameter used with the Telnet command.

Here are the guidelines for the incoming (ASCII-to-EBCDIC) table:

- The FROM code page ID is derived from the CCSID parameter used with the Telnet command.
- The TO character set and code page are taken from the character set ID and code page ID in QCHRID of message description CPX8416 (use WRKMSGD CPX8416 to display), 697 and 37 in the following figure from a US English-based system.

```

System: SYSNAM01
Message ID . . . . . : CPX8416
Message file . . . . . : QCPFMMSG
Library . . . . . : QSYS

Message . . . . . :
QCHRID      697 37      QCURSYM      $ QDATFMT      MDY QDATSEP /
QDECFTM     QLEAPADJ  0 QCCSID 37      QTIMSEP      : QLANGID ENU
QCNTRYID    US QIGCCDEFNT *NONE
  
```

Figure 9. Example CPX8416 message

CCSID	Character set actual ID	Character set table ID	Code page actual ID	Code page actual ID
MULTINAT	1290	A05	1100	A5U
BRITISH	1291	A06	1101	A5V
1292	A07	1102	A5W	
1293	A08	1103	A5X	
289	289	1104	A5Y	
1192	A8E	1020	A3M	
265	265	1011	A3D	
293	293	1012	A3E	
1297	BAB	1107	A52	
1195	A8H	1023	A3P	
1296	BAA	1106	A51	
1193	A8F	1021	A3N	

For example, on a British system with a QCHRID of 697 285 (character set 697 code page 285) in message CPX8416 that uses Telnet with CCSID(*BRITISH), the tables will have the following names:

- Outgoing (EBCDIC-to-ASCII) Q285A06A5V
- Incoming (ASCII-to-EBCDIC) QA5V697285

User-Defined mapping tables (ASCII Mode)

Where the multinational or NLS mapping tables do not meet the requirements of a user, user-defined character mapping tables can be created and used.

You also have the ability to specify user-defined mapping tables using the outgoing ASCII-to-EBCDIC table (TBLVTOUT) and incoming ASCII-to-EBCDIC table (TBLVTIN) parameters of the STRTCPTLN command. You can specify a user-defined mapping table for either the outgoing mapping table or the incoming mapping table, and then use the system default value for the other.

Related concepts

“Starting a VTxxx Telnet client session” on page 58

You can start a Telnet client session using VTxxx emulation. You need to start the Telnet server on the remote system (the system that you want to connect to using Telnet).

Numeric keypad:

Here are the keys on the auxiliary keypad that normally transmit the codes for numerals, decimal points, minus signs, and commas.

Table 13. Keys on the auxiliary keypad

Keyword	Mode	Hex character transmitted	Control character description
*NUM0	VT52 mode	X'30' or X'1B3F70 ¹	Numeric keypad 0 key
*NUM0	VT100 or VT220 7-bit mode	X'30' or X'1B4F70 ¹	Numeric keypad 0 key
*NUM0	VT220 8-bit mode	X'30' or X'8F70 ²	Numeric keypad 0 key
*NUM1	VT52 mode	X'31' or X'1B3F71 ¹	Numeric keypad 1 key
*NUM1	VT100 or VT220 7-bit mode	X'31' or X'1B4F71 ¹	Numeric keypad 1 key
*NUM1	VT220 8-bit mode	X'31' or X'8F71 ²	Numeric keypad 1 key
*NUM2	VT52 mode	X'32' or X'1B3F72 ¹	Numeric keypad 2 key
*NUM2	VT100 or VT220 7-bit mode	X'32' or X'1B4F72 ¹	Numeric keypad 2 key
*NUM2	VT220 8-bit mode	X'32' or X'8F72 ²	Numeric keypad 2 key
*NUM3	VT52 mode	X'33' or X'1B3F73 ¹	Numeric keypad 3 key
*NUM3	VT100 or VT220 7-bit mode	X'33' or X'1B4F73 ¹	Numeric keypad 3 key
*NUM3	VT220 8-bit mode	X'33' or X'8F73 ²	Numeric keypad 3 key
*NUM4	VT52 mode	X'34' or X'1B3F74 ¹	Numeric keypad 4 key
*NUM4	VT100 or VT220 7-bit mode	X'34' or X'1B4F74 ¹	Numeric keypad 4 key
*NUM4	VT220 8-bit mode	X'34' or X'8F74 ²	Numeric keypad 4 key
*NUM5	VT52 mode	X'35' or X'1B3F75 ¹	Numeric keypad 5 key
*NUM5	VT100 or VT220 7-bit mode	X'35' or X'1B4F75 ¹	Numeric keypad 5 key
*NUM5	VT220 8-bit mode	X'35' or X'8F75 ²	Numeric keypad 5 key
*NUM6	VT52 mode	X'36' or X'1B3F76 ¹	Numeric keypad 6 key
*NUM6	VT100 or VT220 7-bit mode	X'36' or X'1B4F76 ¹	Numeric keypad 6 key
*NUM6	VT220 8-bit mode	X'36' or X'8F76 ²	Numeric keypad 6 key
*NUM7	VT52 mode	X'37' or X'1B3F77 ¹	Numeric keypad 7 key

Table 13. Keys on the auxiliary keypad (continued)

Keyword	Mode	Hex character transmitted	Control character description
*NUM7	VT100 or VT220 7-bit mode	X'37' or X'1B4F77 ¹	Numeric keypad 7 key
*NUM7	VT220 8-bit mode	X'37' or X'8F77 ²	Numeric keypad 7 key
*NUM8	VT52 mode	X'38' or X'1B3F78 ¹	Numeric keypad 8 key
*NUM8	VT100 or VT220 7-bit mode	X'38' or X'1B4F78 ¹	Numeric keypad 8 key
*NUM8	VT220 8-bit mode	X'38' or X'8F78 ²	Numeric keypad 8 key
*NUM9	VT52 mode	X'39' or X'1B3F79 ¹	Numeric keypad 9 key
*NUM9	VT100 or VT220 7-bit mode	X'39' or X'1B4F79 ¹	Numeric keypad 9 key
*NUM9	VT220 8-bit mode	X'39' or X'8F79 ²	Numeric keypad 9 key
*NUMMINUS	VT52 mode	X'2D' or X'1B3F6D ¹	Numeric keypad minus key
*NUMMINUS	VT100 or VT220 7-bit mode	X'2D' or X'1B4F6D ¹	Numeric keypad minus key
*NUMMINUS	VT220 8-bit mode	X'2D' or X'8F6D ²	Numeric keypad minus key
*NUMCOMMA	VT52 mode	X'2C' or X'1B3F6C ¹	Numeric keypad comma key
*NUMCOMMA	VT100 or VT220 7-bit mode	X'2C' or X'1B4F6C ¹	Numeric keypad comma key
*NUMCOMMA	VT220 8-bit mode	X'2C' or X'8F6C ²	Numeric keypad comma key
*NUMPERIOD	VT52 mode	X'2E' or X'1B3F6E ¹	Numeric keypad period key
*NUMPERIOD	VT100 or VT220 7-bit mode	X'2E' or X'1B4F6E ¹	Numeric keypad period key
*NUMPERIOD	VT220 8-bit mode	X'2E' or X'8F6E ²	Numeric keypad period key
*PF1	VT52 mode	X'1B50'	Numeric keypad PF1 key
*PF1	VT100 or VT220 7-bit mode	X'1B4F50'	Numeric keypad PF1 key
*PF1	VT220 8-bit mode	X'8F50 ²	Numeric keypad PF1 key
*PF2	VT52 mode	X'1B51'	Numeric keypad PF2 key
*PF2	VT100 or VT220 7-bit mode	X'1B4F51'	Numeric keypad PF2 key
*PF2	VT220 8-bit mode	X'8F51 ²	Numeric keypad PF2 key
*PF3	VT52 mode	X'1B52'	Numeric keypad PF3 key
*PF3	VT100 or VT220 7-bit mode	X'1B4F52'	Numeric keypad PF3 key
*PF3	VT220 8-bit mode	X'8F52 ²	Numeric keypad PF3 key
*PF4	VT52 mode	X'1B53'	Numeric keypad PF4 key
*PF4	VT100 or VT220 7-bit mode	X'1B4F53'	Numeric keypad PF4 key
*PF4	VT220 8-bit mode	X'8F53 ²	Numeric keypad PF4 key

¹ A single-character is transmitted when in keypad numeric mode; a 3-character sequence is sent when in keypad application mode.

² This sequence is a shortened version of the 7-bit sequence. It is either presented when you are operating in 8-bit mode, which can be called by the remote VT220 host or server, or you can specify it on the ASCOPRMOD parameter of the Start TCP/IP TELNET (STRCTPTELN) command.

Related concepts

“Configuring Telnet server for VTxxx full-screen mode” on page 28

VTxxx server support enables Telnet client users to log on and run 5250 full-screen applications, even though VTxxx full-screen support is negotiated.

Editing keypad:

The table shows the keys that transmit codes for the editing keypad key.

Table 14. Keys that transmit codes for the editing keypad keys

Keyword	Mode	Hexadecimal character transmitted	Control character description
*CSRUP	VT52 mode	X'1B41'	Cursor-up key
*CSRUP	VT100 or VT220 7-bit Cursor Key Mode Reset	X'1B5B41'	Cursor-up key
*CSRUP	VT220 8-bit Cursor Key Mode Reset	X'9B41'	Cursor-up key
*CSRUP	VT100 or VT220 7-bit Cursor Key Mode Set	X'1B4F41'	Cursor-up key
*CSRUP	VT220 8-bit Cursor Key Mode Set	X'8F41'	Cursor-up key
*CSRDOWN	VT52 mode	X'1B42'	Cursor-down key
*CSRDOWN	VT100 or VT220 7-bit Cursor Key Mode Reset	X'1B5B42'	Cursor-down key
*CSRDOWN	VT220 8-bit mode Cursor Key Mode Reset	X'9B42'	Cursor-down key
*CSRDOWN	VT100 or VT220 7-bit Cursor Key Mode Set	X'1B4F42'	Cursor-down key
*CSRDOWN	VT220 8-bit mode Cursor Key Mode Set	X'8F42'	Cursor-down key
*CSRRIGHT	VT52 mode	X'1B43'	Cursor-right key
*CSRRIGHT	VT100 or VT220 7-bit Cursor Key Mode Reset	X'1B5B43'	Cursor-right key
*CSRRIGHT	VT220 8-bit Cursor Key Mode Reset	X'9B43'	Cursor-right key
*CSRRIGHT	VT100 or VT220 7-bit Cursor Key Mode Set	X'1B4F43'	Cursor-right key
*CSRRIGHT	VT220 8-bit Cursor Key Mode Set	X'8F43'	Cursor-right Key
*CSRLEFT	VT52 mode	X'1B44'	Cursor-left key
*CSRLEFT	VT100 or VT220 7-bit Cursor Key Mode Reset	X'1B5B44'	Cursor-left key
*CSRLEFT	VT220 8-bit Cursor Key Mode Reset	X'9B44'	Cursor-left key
*CSRLEFT	VT100 or VT220 7-bit Cursor Key Mode Set	X'1B4F44'	Cursor-left key
*CSRLEFT	VT220 8-bit Cursor Key Mode Set	X'8F44'	Cursor-left key
*FINDKEY	VT220 7-bit mode	X'1B5B317E'	Editing keypad Find key
*FINDKEY	VT220 8-bit mode	X'9B317E' ¹	Editing keypad Find key

Table 14. Keys that transmit codes for the editing keypad keys (continued)

Keyword	Mode	Hexadecimal character transmitted	Control character description
*INSERTKEY	VT220 7-bit mode	X'1B5B327E'	Editing keypad Insert Here key
*INSERTKEY	VT220 8-bit mode	X'9B327E' ¹	Editing keypad Insert Here key
*REMOVEKEY	VT220 7-bit mode	X'1B5B337E'	Editing keypad Remove key
*REMOVEKEY	VT220 8-bit mode	X'9B337E' ¹	Editing keypad Remove key
*SELECTKEY	VT220 7-bit mode	X'1B5B347E'	Editing keypad Select key
*SELECTKEY	VT220 8-bit mode	X'9B347E' ¹	Editing keypad Select key
*PREVSCN	VT220 7-bit mode	X'1B5B357E'	Editing keypad Prev Screen key
*PREVSCN	VT220 8-bit mode	X'9B357E' ¹	Editing keypad Prev Screen key
*NEXTSCN	VT220 7-bit mode	X'1B5B367E'	Editing keypad Next Screen key
*NEXTSCN	VT220 8-bit mode	X'9B367E' ¹	Editing keypad Next Screen key

Note: This sequence is a shortened version of the 7-bit sequence. It is only presented when you are operating in 8-bit mode, which can be called by the remote VT220 host or server, or you can specify it on the ASCOPRMOD parameter of the Start TCP/IP TELNET (STRTCPTLN) command.

Related concepts

“Configuring Telnet server for VTxxx full-screen mode” on page 28

VTxxx server support enables Telnet client users to log on and run 5250 full-screen applications, even though VTxxx full-screen support is negotiated.

VTxxx key values by 5250 function:

The table describes the VTxxx key values by 5250 function.

Table 15. VTxxx key values by 5250 function

Default 5250 function	Special value	VTxxx keys	Hexadecimal value ¹
Attention	*CTLA	<CTRL-A>	X'01'
Attention	*ESCA	<ESC><A>	X'1B41'
Backspace	*BACKSPC	<Backspace or CTRL-H>	X'08'
Clear Screen	*ESCC	<ESC><C>	X'1B43'
Cursor Down	*CSRDOWN	<Down Arrow>	X'1B5B42'
Cursor Left	*CSRLEFT	<Left Arrow>	X'1B5B44'
Cursor Right	*CSRRIGHT	<Right Arrow>	X'1B5B43'
Cursor Up	*CSRUP	<Up Arrow>	X'1B5B41'
Delete	*DLT	<Delete>	X'7F'
Delete	*RMV	<Remove>	X'1B5B337E' ²
Delete	*RMV	<Remove>	X'9B337E' ³

Table 15. VTxxx key values by 5250 function (continued)

Default 5250 function	Special value	VTxxx keys	Hexadecimal value ¹
Duplicate	*ESCD	<ESC><D>	X'1B44'
Enter	*RETURN	<Return or CTRL-M>	X'0D'
Erase Input	*CTLE	<CTRL-E>	X'05'
Error Reset	*CTLR	<CTRL-R>	X'12'
Error Reset	*ESCR	<ESC><R>	X'1B52'
Field Advance	*TAB	<TAB or CTRL-I>	X'09'
Field Backspace	*ESCTAB	<ESC><Tab or CTRL-I>	X'1B09'
Field Exit	*CTLK	<CTRL-K>	X'0B'
Field Exit	*CTLX	<CTRL-X>	X'18'
Field Exit	*ESCX	<ESC><X>	X'1B58'
Field Minus	*ESCM	<ESC><M>	X'1B4D'
Help	*CTLQST	<CTRL-Question Mark>	X'1F'
Help	*ESCH	<ESC><H>	X'1B48'
Home	*CTLO	<CTRL-O>	X'0F'
Insert	*ESCI	<ESC><I>	X'1B49'
Insert	*ESCDLT	<ESC><Delete>	X'1B7F'
Insert	*INS	<Insert Here>	X'1B5B327E ²
Insert	*INS	<Insert Here>	X'9B327E ³
New Line	*ESCLF	<ESC> <Line Feed or CTRL-J>	X'1B0A'
Page Down (Roll Up)	*CTLD	<CTRL-D>	X'04'
Page Down (Roll Up)	*CTLF	<CTRL-F>	X'06'
Page Down (Roll Up)	*NXTSCR	<Next Screen>	X'1B5B367E ²
Page Down (Roll Up)	*NXTSCR	<Next Screen>	X'9B367E ³
Page Up (Roll Down)	*CTLB	<CTRL-B>	X'02'
Page Up (Roll Down)	*CTLU	<CTRL-U>	X'15'
Page Up (Roll Down)	*PRVSCR	<Prev Screen>	X'1B5B357E ²
Page Up (Roll Down)	*PRVSCR	<Prev Screen>	X'9B357E ³
Print	*CTLP	<CTRL-P>	X'10'
Print	*ESCP	ESC	X'1B50'
Redraw Screen	*CTLL	<CTRL-L>	X'0C'
Redraw Screen	*ESCL	<ESC><L>	X'1B4C'
System Request	*CTLC	<CTRL-C>	X'03'
System Request	*ESCS	<ESC><S>	X'1B53'
Test Request	*CTLT	<CTRL-T>	X'14'
Toggle Indicator Lights	*ESCT	<ESC><T>	X'1B54'
F1	*ESC1	<ESC><1>	X'1B31'
F1	*F1	<F1> ⁵	X'1B5B31317E ²
F1	*F1	<F1> ⁵	X'9B31317E ³
F1	*PF1	<PF1>	X'1B4F50 ²

Table 15. VTxxx key values by 5250 function (continued)

Default 5250 function	Special value	VTxxx keys	Hexadecimal value ¹
F1	*PF1	<PF1>	X'8F50 ³
F2	*ESC2	<ESC><2>	X'1B32'
F2	*F2	<F2> ⁵	X'1B5B31327E ²
F2	*F2	<F2> ⁵	X'9B31327E ³
F2	*PF2	<PF2>	X'1B4F51 ²
F2	*PF2	<PF2>	X'8F51 ³
F3	*ESC3	<ESC><3>	X'1B33'
F3	*F3	<F3> ⁵	X'1B5B31337E ²
F3	*F3	<F3> ⁵	X'9B31337E ³
F3	*PF3	<PF3>	X'1B4F52 ²
F3	*PF3	<PF3>	X'8F52 ³
F4	*ESC4	<ESC><4>	X'1B34'
F4	*F4	<F4> ⁵	X'1B5B31347E ²
F4	*F4	<F4> ⁵	X'9B31347E ³
F4	*PF4	<PF4>	X'1B4F53 ²
F4	*PF4	<PF4>	X'8F53 ³
F5	*ESC5	<ESC><5>	X'1B35'
F5	*F5	<F5> ⁵	X'1B5B31357E ²
F5	*F5	<F5> ⁵	X'9B31357E ³
F6	*ESC6	<ESC><6>	X'1B36'
F6	*F6	<F6>	X'1B5B31377E ²
F6	*F6	<F6>	X'9B31377E ³
F7	*ESC7	<ESC><7>	X'1B37'
F7	*F7	<F7>	X'1B5B31387E ²
F7	*F7	<F7>	X'9B31387E ³
F8	*ESC8	<ESC><8>	X'1B38'
F8	*F8	<F8>	X'1B5B31397E ²
F8	*F8	<F8>	X'9B31397E ³
F9	*ESC9	<ESC><9>	X'1B39'
F9	*F9	<F9>	X'1B5B32307E ²
F9	*F9	<F9>	X'9B32307E ³
F10	*ESC0	<ESC><0>	X'1B30'
F10	*F10	<F10>	X'1B5B32317E ²
F10	*F10	<F10>	X'9B32317E ³
F11	*ESCMINUS	<ESC><Minus>	X'1B2D'
F11	*F11	<F11>	X'1B5B32337E ²
F11	*F11	<F11>	X'9B32337E ³
F12	*ESCEQ	<ESC><Equal>	X'1B3D'
F12	*F12	<F12>	X'1B5B32347E ²
F12	*F12	<F12>	X'9B32347E ³

Table 15. VTxxx key values by 5250 function (continued)

Default 5250 function	Special value	VTxxx keys	Hexadecimal value ¹
F13	*ESCEXCL	<ESC><Exclamation>	X'1B21'
F13	*F13	<F13>	X'1B5B32357E ²
F13	*F13	<F13>	X'9B32357E ³
F14	*ESCAT	<ESC><At sign>	X'1B40'
F14	*F14	<F14>	X'1B5B32367E ²
F14	*F14	<F14>	X'9B32367E ³
F15	*ESCPOUND	<ESC><Pound>	X'1B23'
F15	*F15	<F15>	X'1B5B32387E ²
F15	*F15	<F15>	X'9B32387E ³
F16	*ESCDOLLAR	<ESC><Dollar>	X'1B24'
F16	*F16	<F16>	X'1B5B32397E ²
F16	*F16	<F16>	X'9B32397E ³
F17	*ESCPCT	<ESC><Percent>	X'1B25'
F17	*F17	<F17>	X'1B5B33317E ²
F17	*F17	<F17>	X'9B33317E ³
F18	*ESCCFX	<ESC><Circumflex Accent>	X'1B5E ¹
F18	*F18	<F18>	X'1B5B33327E ²
F18	*F18	<F18>	X'9B33327E ³
F19	*ESCAMP	<ESC><Ampersand>	X'1B26'
F19	*F19	<F19>	X'1B5B33337E ²
F19	*F19	<F19>	X'9B33337E ³
F20	*ESCAST	<ESC><Asterisk>	X'1B2A'
F20	*F20	<F20>	X'1B5B33347E ²
F20	*F20	<F20>	X'9B33347E ³
F21	*ESCLPAR	<ESC><Left Parenthesis>	X'1B50'
F22	*ESCRPAR	<ESC><Right Parenthesis>	X'1B51'
F23	*ESCUS	<ESC><Underscore>	X'1B5F'
F24	*ESCPLUS	<ESC><Plus>	X'1B2B'
See note 4	*FIND	<Find>	X'1B5B317E'
See note 4	*FIND	<Find>	X'9B317E'
See note 4	*SELECT	<Select>	X'1B5B347E'
See note 4	*SELECT	<Select>	X'9B347E'

Notes:

- ¹ - Unless otherwise identified, the hexadecimal value is in the VT100 mode.
- ² - VT220 7-bit control mode.
- ³ - There is no 5250 function key that maps to this VT key.

⁴ - The keys F1 through F5 are not available on a VT220 terminal. However, many VT220 emulators send these hexadecimal values when the F1 through F5 keys are pressed.

Related concepts

“Configuring Telnet server for VTxxx full-screen mode” on page 28

VTxxx server support enables Telnet client users to log on and run 5250 full-screen applications, even though VTxxx full-screen support is negotiated.

VT220 workstation operating modes:

Several operating modes are supported while the system negotiates the VT220 workstation type.

These operating modes are as follows:

- VT200 mode with 7-bit controls is the default mode and uses the standard ANSI functions. This mode provides the full range of VT220 capabilities in an 8-bit communications environment with 7-bit controls. This mode supports the DEC multinational character set or national replacement character (NRC) sets, depending on the character set mode selected.
- VT200 mode with 8-bit controls uses the standard ANSI functions and provides the full range of VT220 capabilities in an 8-bit communications environment with 8-bit controls. This mode supports the DEC multinational character set or NRC sets, depending on the character set mode selected.
- VT100 mode uses standard ANSI functions. This mode restricts the use of the keyboard to VT100 keys. All data has a 7-bit restriction, and only ASCII, NRC, or special graphics characters generate.
- VT52 mode uses DEC private functions (not ANSI). This mode restricts the use of the keyboard to VT52 keys.

If VT220 mode is negotiated, an initial operating mode for the Telnet client is selected using the ASCII operating mode (ASCOPRMODE) parameter of the start TCP/IP Telnet (STRTCPTLN) or TELNET command.

VT220 top-row function keys:

The table describes the keys that transmit the codes for function keys on the top row of the VT220 keyboard in 7-bit mode.

Table 16. VT220 top-row function keys

Keyword	Hexadecimal character transmitted
*F6	X'1B5B31377E'
*F7	X'1B5B31387E'
*F8	X'1B5B31397E'
*F9	X'1B5B32307E'
*F10	X'1B5B32317E'
*F11	X'1B5B32337E'
*F12	X'1B5B32347E'
*F13	X'1B5B32357E'
*F14	X'1B5B32367E'
*F15 or *HELP	X'1B5B32387E'
*F16 or *DO	X'1B5B32397E'
*F17	X'1B5B33317E'
*F18	X'1B5B33327E'
*F19	X'1B5B33337E'

Table 16. VT220 top-row function keys (continued)

Keyword	Hexadecimal character transmitted
*F20	X'1B5B33347E'

This table describes the keys that transmit the codes for function keys on the top row of the VT220 keyboard in 8-bit mode.

Table 17. VT220 top-row function keys in 8-bit mode

Keyword	Hexadecimal character transmitted
*F6	X'9B31377E'
*F7	X'9B31387E'
*F8	X'9B31397E'
*F9	X'9B32307E'
*F10	X'9B32317E'
*F11	X'9B32337E'
*F12	X'9B32347E'
*F13	X'9B32357E'
*F14	X'9B32367E'
*F15 or *HELP	X'9B32387E'
*F16 or *DO	X'9B32397E'
*F17	X'9B33317E'
*F18	X'9B33327E'
*F19	X'9B33337E'
*F20	X'9B33347E'

VT100 and VT220 control character keywords:

The VT100 and VT220 control character keywords are listed in the table.

Table 18. VT100 and VT220 control character keywords

Control character description	Key+CTRL	Keyword	Hexadecimal character transmitted
Null	Spacebar	*NUL	X'00'
Start of heading	A	*SOH,*CTLA	X'01'
Start of text	B	*STX,*CTLB	X'02'
End of text	C	*ETX,*CTLC	X'03'
End of transmission	D	*EOT,*CTLD	X'04'
Enquire	E	*ENQ,*CTLE	X'05'
Acknowledge	F	*ACK,*CTLF	X'06'
Bell	G	*BEL,*CTLG	X'07'
Back Space	H	*BS,*CTLH	X'08'
Horizontal tabulation	I	*HT,*CTLI	X'09'
Line feed	J	*LF,*CTLJ	X'0A'
Vertical tab	K	*VT,*CTLK	X'0B'

Table 18. VT100 and VT220 control character keywords (continued)

Control character description	Key+CTRL	Keyword	Hexadecimal character transmitted
Form feed	L	*FF,*CTLL	X'0C'
Carriage return	M	*CR,*CTLM	X'0D'
Shift out	N	*SO,*CTLN	X'0E'
Shift in	O	*SI,*CTLO	X'0F'
Data link escape	P	*DLE,*CTLP	X'10'
Device control 1	Q	*DC1,*CTLQ	X'11'
Device control 2	R	*DC2,*CTLR	X'12'
Device control 3	S	*DC3,*CTLS	X'13'
Device control 4	T	*DC4,*CTLT	X'14'
Negative acknowledgement	U	*NAK,*CTLU	X'15'
Synchronous idle	V	*SYN,*CTLV	X'16'
End of transmission block	W	*ETB,*CTLW	X'17'
Cancel previous word or character	X	*CAN,*CTLX	X'18'
End of medium	Y	*EM,*CTLY	X'19'
Substitute	Z	*SUB,*CTLZ	X'1A'
Escape	[*ESC	X'1B'
File separator	\	*FS	X'1C'
Group separator]	*GS	X'1D'
Record separator	&eqv.	*RS	X'1E'
Unit separator	?	*US	X'1F'
Delete		*DEL	X'7F'

Establishing a cascaded Telnet session

You can establish another Telnet session while you are in a current Telnet session. After you establish a cascaded session, you can move between the different systems.

The home system is the first client system that you use. The end system is the last Telnet server system that you access. The system that you pass through to get from the home system to the end system is an intermediate system.

Starting a cascaded session

To start your cascaded session, sign on to the home system, then follow the steps to establish a client session. Repeat the steps for each system you want to connect to.

Returning to the system

The SIGNOFF command ends the session and returns you to the sign-on display of the system. When you are signed on to the system, the SIGNOFF command ends the current server job and returns you to the sign-on display of the system.

You can use the end connection (ENDCNN) parameter of the SIGNOFF command to sign off the system and end the TELNET connection. For example, `signoff endcnn(*yes)` returns you to your original session on the client system, or the previous session if you have more than one TELNET session established.

Notes:

1. There is no limit the number of systems to which you can establish a Telnet session.
2. The home system intercepts System Request options 13 and 14 if entered on the System Request input line. This function might be helpful if you establish a Telnet session with a system to which you cannot sign on. In this case, you can end a session to that system completing the following steps:
 - Press the System Request key.
 - Type 13 (Start system request at home system) on the System Request input line.
 - Type 2 (End previous request) on the System Request menu.

Related concepts

“Telnet scenario: Cascaded Telnet sessions” on page 3

The scenario demonstrates the ability to start Telnet sessions while you are still in a Telnet session. After you have been connected, you can switch between systems using system request values.

“Starting a Telnet client session” on page 51

You should know the name or Internet address of the remote system with which you want to start the Telnet session.

Moving between cascaded Telnet sessions

After you start a cascaded Telnet session, press the SysRq key, and press Enter to display the System Request menu.

The System Request menu provides you with the following options.

System Request option	Action	Description
10	Starting a system request at a client system	Displays the System Request menu on the previous client system
11	Transferring to the client system	Transfers you to an alternative job on the previous client system
13	Starting a system request at the home system	Takes you from an intermediate or end system to the System Request menu of the home system
14	Transferring to the home system	Takes you from an intermediate or end system to the alternative job on the home system
15	Transferring to the end system	Takes you from an intermediate or home system to the end system

To bypass the System Request menu, press the SysRq key and type 10 on the command line. This shortcut is applicable between System i platforms only.

For non-IBM Telnet clients

You might drop a cascaded Telnet session when you try to use System Request options 10, 11, 13, or 14. For options 10 and 11, the client PC is the previous system. For options 13 and 14, the client PC is the home system.

Your Telnet client is compatible, if it passes these two tests:

- You return to the home system after using options 13 or 14.
- You do not drop a session when using options 10 or 11 from the home system.

For incompatible clients, follow these steps instead of using System Request options 10, 11, 13, or 14:

1. Use System Request option 11 to move backward from system to another system until you reach the home system. The home system is the first system to which your Telnet client connected at the beginning of the session.
2. From the home system, use System Request option 1 to move forward from one system to another system.

Related concepts

“Telnet scenario: Cascaded Telnet sessions” on page 3

The scenario demonstrates the ability to start Telnet sessions while you are still in a Telnet session. After you have been connected, you can switch between systems using system request values.

Ending a Telnet client session

When you are connected to a System i platform, signing off does not necessarily end your Telnet server session. To end the session, you must enter a key or sequence of keys to put the Telnet client into a local command mode. You can then type the command to end the session.

- From the i5/OS operating system, press the Attention key and then select option 99 (End TELNET session - QUIT).
- From most other systems, log off.

If you do not know what key or key sequence causes the client to enter command mode, consult either your system administrator or your Telnet client documentation.

You can also use the end connection (ENDCNN) parameter of the SIGNOFF command to sign off the system and end the Telnet connection. For example, SIGNOFF ENDCNN(*YES) returns you to the client system (if you only have one Telnet session established). Or, if you have more than one Telnet session established, the command returns you to the previous system.

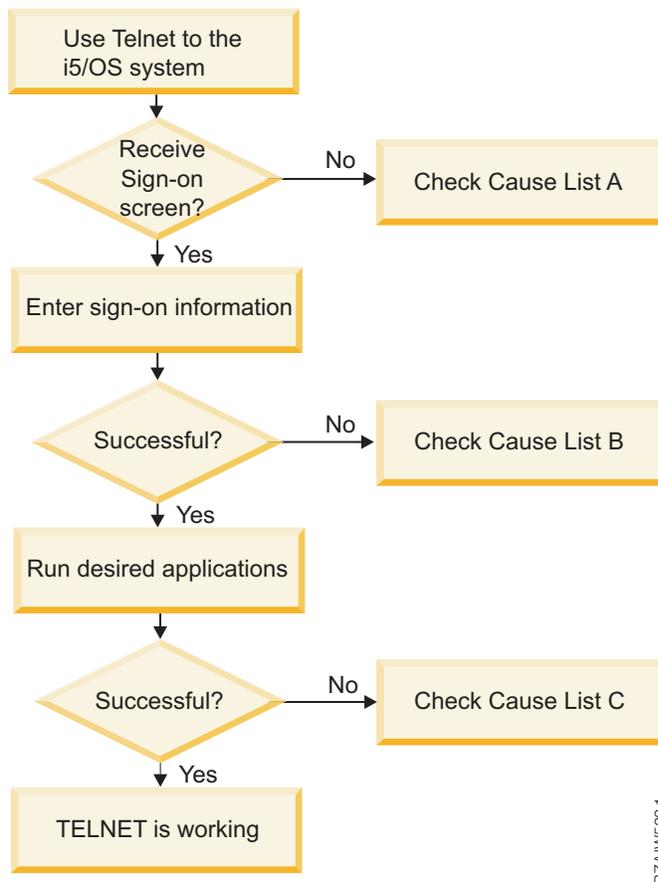
Troubleshooting the Telnet problems

This topic contains information about troubleshooting and correcting problems with Telnet.

Determining problems with Telnet

You need diagnostic information to troubleshoot Telnet, including a flow chart for system problem analysis, and you need a list of materials when reporting Telnet problems.

Use this flow chart after using the flow chart for general TCP/IP problems. If a problem is detected when using the Telnet server, use the flow chart to identify the cause. The cause lists that follow the flow chart might help identify potential problems.



Cause list A

1. Verify that the Telnet server jobs are active and that Telnet service is assigned to a valid nonrestricted port.
 - a. To verify that the QTVTELNET and QTVDEVICE jobs are active in the QSYSWRK subsystem, complete the following steps:
 - 1) Start System i Navigator and expand *your system* → **Work Management**.
 - 2) Right-click **Active Jobs**, and look to see if QTVTELNET and QTVDEVICE are active. If they are, continue with step 1c.
 - b. If these jobs are not active, complete the following steps to start these jobs:
 - 1) Start System i Navigator and expand *your system* → **Network** → **Servers** → **TCP/IP**.
 - 2) Right-click **Telnet** and select **Start**.
 - c. To verify that Telnet service is assigned to a valid port, complete the following steps:
 - 1) Start System i Navigator and expand *your system* → **Network** → **Servers** → **TCP/IP**.
 - 2) Right-click **Connections** and select **Open**.
 - 3) Look for Telnet.
 - d. For printers, insure that subsystem QSPL is active.
 - e. Check for port restrictions by going to menu CFGTCP and selecting option 4 (Work with TCP/IP port restrictions).
2. Verify that the devices system value on the system is properly set to allow the Telnet server to automatically create virtual devices.
3. Verify that the network connection between the system and the Telnet client is active by using the Ping function in System i Navigator. If the connection is not active, see your network administrator.

4. Verify that the virtual devices on the system that are used by Telnet are defined to a subsystem under which the interactive Telnet jobs should run.
 - a. To see which workstation entries are defined to a subsystem, complete the following steps:
 - 1) Start System i Navigator and expand *your system* → **Work Management**.
 - 2) Right-click **Subsystems** and select **Open**.
 - b. Use the Add Work Station Entry (ADDWSE) command to define work stations to a subsystem. For example, you could use the following command to allow all work station types to run under the QINTER subsystem:


```
ADDWSE SBS(D(QINTER) WRKSTNTYPE(*ALL)
```
5. Verify that the interactive subsystem (QINTER) is active. Telnet connections is not complete if the interactive subsystem is not active. In this situation, the system does not write error messages to the QTVTELNET job log or the QTVDEVICE job log to show you the problem.

To verify that the subsystem is active, complete the following steps:

 - a. Start System i Navigator and expand *your system* → **Work Management**.
 - b. Right-click **Subsystems** and select **Open**.
 - c. Verify that the subsystem is active.
6. If you are operating in VTxxx full-screen mode, verify that your local VTxxx client configuration specifies autowrap. When autowrap is on, the system will automatically wrap lines at column 80.
7. Check for a Telnet exit program registered to exit point QIBM_QTG_DEVINIT, format INIT0100, using the work with registration information (WRKREGINF) command. If there is a registered user exit program, check the Telnet server job log with job name QTVDEVICE for any errors related to that program. If errors exist, correct the errors in the exit program or remove the exit program with the remove exit program (RMVEXITPGM) command.
8. Ensure that your client is attempting to use the correct port to connect to Telnet.

To determine the port that Telnet service is assigned to, complete the following steps:

 - a. Start System i Navigator and expand *your system* → **Network** → **Servers** → **TCP/IP**.
 - b. Right-click **Connections** and select **Open**.
 - c. Look for Telnet.
9. Use the CFGTCP command to verify that the port your client is attempting to connect on is not restricted. Also look in the QTVTELNET job log for messages that indicate that the port that you are trying to use is restricted.
10. When attempting to connect using SSL Telnet, make sure that you have installed the Digital Certificate Manager (DCM). This is in addition to the above items listed. Also, ensure that a valid, unexpired certificate is assigned to the Telnet server (QIBM_QTV_TELNET_SERVER).

Cause list B

1. Verify your authority to the virtual display device. If you receive message CPF1110 when attempting to sign on the System i platform, you are not authorized to the virtual display device. When the Telnet server creates virtual devices, the QCRTAUT system value is used to determine the authority granted to user *PUBLIC. This system value should be *CHANGE to allow any user to sign on using Telnet.
2. Verify that the QLMTSECOFR system value is correct if you are the security officer or have *SECOFR authority.

Cause list C

1. Verify your word processing choice. If you experience problems when using the Work with Folders (WRKFLR) command, you might need to change your configuration so that the Office Adapted Editor is used instead of the Standard Editor. To do this, have your system administrator change your word-processing choice in the environment information associated with your office user ID.

2. If you are operating in VTxxx full-screen mode, verify that your local VTxxx client configuration specifies autowrap. When autowrap is on, the system will automatically wrap lines at column 80.
3. If characters do not display properly for your VTxxx session, verify that the correct mapping tables are in use for your session.
4. If your VTxxx client beeps every time you press a key, your keyboard might be locked.
5. Check the QTVTELNET job log and the QTVDEVICE job log for error messages on the system.

Related concepts

System values: Devices overview

“VTxxx full screen considerations” on page 60

As with any emulation type, you should be aware of certain considerations before using the VTxxx full-screen mode with your Telnet Server. These considerations include security concerns as well as possible error conditions and indicator lights. You can understand how to use VTxxx full-screen mode better if you become familiar with these considerations.

Description: Telnet problem analysis flow chart

Follow these steps to determine which cause list to use:

1. Telnet to the i5/OS operating system.
2. Did you receive a sign-on screen? If Yes, continue. If No, see Cause List A.
3. Enter sign-on information.
4. Is sign-on successful? If Yes, continue. If No, see Cause List B.
5. Run the required applications.
6. Are applications successful? If Yes, continue. If No, see Cause List C.
7. Telnet is working.

Pinging your host server

You can use the Ping function in System i Navigator to test your TCP/IP connection.

About this task

To ping your system, complete the following steps:

1. Start System i Navigator and expand *your system* → **Network**.
2. Right-click **TCP/IP Configuration** and select **Utilities**.
3. Click **Ping** to display the **Ping** dialog box.
4. Type your host name in the **Ping** box (for example, companyname.com).
5. Click **Ping Now**.

Results

Messages display in the **Results** box to tell you the status of your connection.

Related tasks

“Checking system status” on page 91

You need to confirm that your Telnet is ready for Secure Sockets Layer (SSL) sessions.

Troubleshooting emulation types

When developing a Telnet client, it is important that you negotiate the correct emulation workstation type. The functions allowed vary with the workstation type. The following guide helps you understand the workstation type and the function capabilities of that workstation.

Workstation type negotiations and mappings

The Workstation and printer mappings table shows a list of virtual display stations that the server uses to match the physical display stations of the client system.

If you are not sure what emulation package you are running, you need to determine what your virtual display device is. You can use the Work with Job (WRKJOB) command to find out what it is. The job name is displayed at the top. This is the name of the virtual display device associated with your job. By default, the naming convention is QPADEVxxxx, where xxxx are alphanumeric characters.

To determine the device type, type:

```
WRKCFGSTS *DEV QPADEVxxxx
```

You can work with your device description. Type an 8 (Work with description) next to the name of the device. The system displays the device type. You can then determine from the device type whether you are running in full-screen mode for 3270, 5250, VT100, or VT220.

Table 19. Workstation and printer mappings

Supported workstation and (model)	Equivalent type and (model)	Internet specification	Description
5251 (11)		IBM-5251-11	24 X 80 monochrome display
5291 (1)	5291 (2)	IBM-5291-1	24 X 80 monochrome display
5292 (2)		IBM-5292-2	24 X 80 color graphics display; this workstation type is also emulated by a graphic workstation function.
3196 (A1)	3196 (A1) 3196(B1) 3196 (B2) 3476 (EA)	IBM-3196-A1	24 X 80 monochrome display; this workstation type is also emulated by a monochrome workstation function.
3486 (BA)		IBM-3486-BA	24 X 80 monochrome display
3487(HA) ²	3487 (HG) ² 3487 (HW) ²	IBM-3487-HA	24 X 80 monochrome display; this workstation type is also emulated by a monochrome workstation function.
3487 (HC) ²		IBM-3487-HC	24 X 80 color display; this workstation type is also emulated by a color workstation function.
3179 (2)	3197 (C1) 3197 (C2) 3476 (EC)5292 (1)	IBM-3179-2	24 X 80 color display; this workstation type is also emulated by a color workstation function.
3180 (2)	3197 (D1) 3197 (D2) 3197 (W1) 3197 (W2)	IBM-3180-2	27 X 132 monochrome display

Table 19. Workstation and printer mappings (continued)

Supported workstation and (model)	Equivalent type and (model)	Internet specification	Description
5555 (B01)	5555 (E01)	IBM-5555-B01	24 X 80 double-byte character set (DBCS) monochrome display; this workstation type is emulated by a workstation function that supports DBCS display.
5555 (C01) I	5555 (F01)	IBM-5555-C01	24 x 80 DBCS color display; this workstation type is emulated by a workstation function that supports DBCS display.
5555 (G01)		IBM-5555-G01	24 X 80 double-byte character set (DBCS) monochrome, graphics display; this workstation type is emulated by a workstation function that supports DBCS display.
5555 (G02)		IBM-5555-G02	24 x 80 DBCS color graphics display; this workstation type is emulated by a workstation function that supports DBCS display.
3477 (FC)		IBM-3477-FC	27 X 132 wide-screen color display
3477 (FG)	3477 (FA) 3477 (FD) 3477 (FW)3477 (FE)	IBM-3477-FG	27 X 132 wide-screen monochrome display
3277 (0) ³	3277 (DHCF)	IBM-3277-2	24 X 80 monochrome display
3277 (0) ^{3,4}	3278 (DHCF)	IBM-3278-2	24 X 80 monochrome display
3278 (0) ³		IBM-3278-2-E ⁵	24 x 80 monochrome display
3278 (0) ³		IBM-3278-3	24 x 80 monochrome display
3278 (0) ³		IBM-3278-4	24 x 80 monochrome display
3278 (0) ³		IBM-3278-5	24 x 80 monochrome display
3279 (0) ³	3279 (DHCF)	IBM-3279-2 IBM-3279-2-E ⁵	24 X 80 monochrome display
3279 (0) ³		IBM-3279-3	24 x 80 color display
3812 (1)		IBM-3812-1	3812 printer (SBCS)
5553 (B01)		IBM-5553-B01	5553 printer (DBCS)

Table 19. Workstation and printer mappings (continued)

Supported workstation and (model)	Equivalent type and (model)	Internet specification	Description
VT100 (*ASCII) ⁶		DEC-VT100 VT100(7) VT102 DEC-VT102 DEC-VT200 DEC-VT220 VT200(7) VT220(7)	24 x 80 monochrome ASCII display

Considerations:

¹ All 5250 workstations, except 5555 (B01) and 5555 (C01), can operate as 5251-11 workstations.

² This workstation can be configured to be either 24 x 80 or 27 x 132. You must determine the mode of the workstation before setting the workstation type parameter value.

³ The system supports only 24 X 80 screens in remote 327x workstations. Remote 3277 (both distributed host command facility (DHCF) and regular) workstations are mapped to IBM-3277-2. Remote 3278 workstations are mapped to IBM-3278-2. Remote 3279 workstations are mapped to IBM-3279-2.

⁴ Some Telnet 3270 full-screen (TN3270) or 3278-2 emulator packages do not support write-structured fields correctly. Because of this, 3278-2 type devices are mapped to 3277-2 devices by the Telnet server implementation to allow the system to work with those TN3270 implementations.

⁵ The extended attributes highlighting is supported. Underline, blink, and reverse video are included. 3270 DBCS processing is also supported.

⁶ The VT100 virtual device supports VT220 devices.

⁷ VT100, VT200, and VT220 are not official terminal type names. However, some implementations negotiate using these names as the terminal type value.

Related reference

“INIT0100: Format of connection description information” on page 46

This topic contains information about the client connection that the exit program can use.

Troubleshooting your Telnet SSL server

Here are the detailed steps for troubleshooting your Secure Sockets Layer (SSL) server including system SSL return codes and a list of common SSL problems.

About this task

To identify problems with your Telnet SSL server, follow these steps:

1. Check your system status to verify that the proper software has been installed and that the servers are started.
2. Ping your host server to check that TCP/IP is started and the network is OK.
3. Check that the Telnet server is started.
4. Check for an active SSL listener by using the NETSTAT *CNN command.
5. Check the Telnet job log to find the SSL return code.
6. Look up the SSL problems and return codes for suggestions to solve the problem.

Results

Incorrect digital certificates can cause many problems with SSL. Digital Certificate Manager (DCM) lets you change your certificate authority (CA) or system certificates. To confirm that you have a valid system certificate, read how to start Digital Certificate Manager (DCM) and then view the system certificate.

Related concepts

“Securing Telnet with SSL” on page 31

With the Secure Sockets Layer (SSL) protocol, you can establish secure connections between the Telnet server application and Telnet clients that provide authentication of one or both endpoints of the communication session. SSL also provides privacy and integrity of the data that client and server applications exchange.

DCM concepts

Starting Digital Certificate Manager

Related tasks

“Configuring SSL on the Telnet server” on page 31

The most important factor to consider when enabling SSL on the Telnet server is the sensitivity of the information that is involved in client sessions. If the information is sensitive, or private, then securing the Telnet server with SSL is recommended.

Checking system status

You need to confirm that your Telnet is ready for Secure Sockets Layer (SSL) sessions.

1. Verify that you have the appropriate software installed to support Telnet SSL and to manage certificates:
 - IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1)
 - Digital Certificate Manager
 - IBM HTTP Server for i5/OS (5761-DG1)
 - IBM Developer Kit for Java (5761-JV1)
2. Verify that you have a secure Telnet server by associating a certificate with the Telnet server application QIBM_QTV_TELNET_SERVER.
3. Ping your host system to verify that your TCP/IP connection and network status.
4. Determine whether the Telnet server is started.
5. Determine whether the Telnet server is configured to allow SSL connections.

Related tasks

“Assigning a certificate to the Telnet server” on page 32

When you enable the Telnet server on your system to use Secure Sockets Layer (SSL), you can establish secure Telnet connections to your system from System i Access for Windows or from any other SSL-enabled Telnet clients, such as a Personal Communications emulator.

“Pinging your host server” on page 87

You can use the Ping function in System i Navigator to test your TCP/IP connection.

“Starting the Telnet server” on page 20

The active Telnet server has one or more instances of each of these jobs running in the QSYSWRK subsystem: QTVTELNET and QTVDEVICE.

“Configuring SSL on the Telnet server” on page 31

The most important factor to consider when enabling SSL on the Telnet server is the sensitivity of the information that is involved in client sessions. If the information is sensitive, or private, then securing the Telnet server with SSL is recommended.

Related reference

“SSL return codes” on page 93

The topic lists the system Secure Sockets Layer (SSL) return codes for the most common problems that might occur during SSL initialization or SSL handshake.

Checking for an active SSL listener

Use this procedure to check for an active Secure Sockets Layer (SSL) listener. The Telnet server must be active and ready to receive connection attempts.

About this task

To check for an active SSL listener, follow these steps:

1. In the character-based interface, type `NETSTAT *CNN` to show the Work with TCP/IP Connection Status display.
2. In the **Local Port** column, find the `telnet-` label for `telnet-ssl`. You can see only `telnet-` because the field is not long enough on the display.
 - Use the F22 key to display the entire Local Port field.
 - Use the F14 key to see the port numbers. The `telnet-ssl` entry is port 992.

Results

SSL initialization fails if you do not find `telnet-ssl` in the Local Port column. For fixing the problem, check the SSL diagnostic messages in the QTVTELNET job log running in the QSYSWRK subsystem. Only one QTVTELNET job will be running after an SSL initialization failure.

Related tasks

“Checking the Telnet job log”

When Secure Sockets Layer (SSL) initialization and handshake fails, the Telnet server sends CPDBC *mm* diagnostic messages to the QTVTELNET job.

Checking the Telnet job log

When Secure Sockets Layer (SSL) initialization and handshake fails, the Telnet server sends CPDBC *mm* diagnostic messages to the QTVTELNET job.

About this task

To check the Telnet server job log, follow these steps:

1. In System i Navigator, expand *your system* → **Network** → **TCP/IP Configuration** → **IPv4**.
2. Click **Connections**.
3. Right-click the IP address of the client workstation that is failing and select **Jobs**. Note the job name.
4. Expand **Job Management** → **Server Jobs**.
5. Right-click **QTVTELNET** in the Job name column.
6. Select **Job Log**.
7. Look for the CPDBC *mm* message in the Message ID column.

Results

Here are some things to remember about the Telnet server jobs:

- Only one QTVTELNET job starts when the SSL listener fails to initialize.
- QTVDEVICE and QTVTELNET jobs start when the Telnet server starts after the system restarts.
- The same number of QTVTELNET and QTVDEVICE jobs start when the Telnet server starts an SSL listener.
- The ENDTCPSVR *TELNET or ENDTCP command ends QTVTELNET jobs.
- When the QSYSWRK subsystem ends, the QTVDEVICE jobs end.

Related concepts

“SSL initialization and handshake” on page 36

Here are the details about the interactions between Telnet servers, clients, and Secure Sockets Layer (SSL).

Related tasks

“Checking for an active SSL listener” on page 92

Use this procedure to check for an active Secure Sockets Layer (SSL) listener. The Telnet server must be active and ready to receive connection attempts.

SSL return codes

The topic lists the system Secure Sockets Layer (SSL) return codes for the most common problems that might occur during SSL initialization or SSL handshake.

You need to do these steps before using the following return code tables:

- You need to find the SSL return code in the QTVTELNET job log.
- In some cases, you need to work with the Digital Certificate Manager (DCM) configuration to correct problems with certificate authority (CA) certificates or system certificates.
- When you copy the CA certificate information for your Telnet SSL client, remember to include the lines containing the words BEGIN CERTIFICATE and END CERTIFICATE.

Table 20. Common return codes

Return code	Description
-2	<p>No system certificate is available for SSL processing. The Telnet server successfully initializes SSL, but the SSL handshake fails. There is no signon panel in the SSL Telnet client window. The QIBM_QTV_TELNET_SERVER application does not have an assigned system certificate.</p> <p>View the system certificate and check that the value Yes shows in the Certificate assigned column. If the value is No, create a system certificate for the QIBM_QTV_TELNET_SERVER application.</p>
-4	<p>The CA certificate or system certificate is bad. The system certificate is not private or trusted. The Private Key and Trusted fields on the server certificate are not correct. The Telnet SSL client window has no signon panel.</p> <p>Add CA information in your Telnet SSL client. If you are using System i Access for Windows as your Telnet SSL client, see Manage public Internet certificates for SSL communication sessions. Otherwise, see Obtain a copy of the private CA certificate for instructions.</p>
-16	<p>The peer system is not recognized. This problem is the most common problem when a Telnet SSL client first attempts to establish an SSL session. The Telnet SSL client window has no sign-on panel.</p> <p>Add CA certificate information to your Telnet SSL client.</p>
-18	<p>The system certificate is self-signed and server is using it as a CA certificate. The system certificate assigned to the QIBM_QTV_TELNET_SERVER application must be trusted, signed by a certificate authority, and used within the valid time period. You need to create a CA certificate and associate it with the system certificate. The Telnet server does not initialize SSL if the system certificate is incorrect.</p> <p>Create a CA certificate and associate it with the system certificate.</p>
-23	<p>The system certificate is not signed by a trusted certificate authority. The system certificate assigned to the QIBM_QTV_TELNET_SERVER application must be trusted, signed by a certificate authority, and used within the valid time period.</p> <p>Change the CA certificate to Trusted. For instructions, see Manage applications in DCM.</p>

Table 20. Common return codes (continued)

Return code	Description
-24	The valid time period of the CA certificate has expired. You are using an out-of-date certificate. The Telnet SSL client window has no sign-on panel. Renew the CA certificate that was used to build the system certificate.
-93	SSL is not available for use. Telnet SSL clients cannot connect to a host because there is no active SSL listener. Install software requirements to support Telnet SSL and to manage certificates. For instructions, see Check system status.

Other SSL return codes

For the SSL return codes in the following table, use DCM to verify that the digital certificates meet these requirements:

- The CA certificate is valid and has not expired.
- The Telnet server application QIBM_QTV_TELNET_SERVER has a value of Yes in the Certificate Assigned column.
- A certificate authority signs the system certificate.
- The system certificate is trusted.
- The system certificate is used within the timeframe stated on the certificate.

Table 21. Other SSL return codes

Return code	Description
-1	No ciphers are available or specified
-6	i5/OS operating system does not support the certificate type
-10	An error occurred in SSL processing. In the job log, check the CPExxxx message where xxxx is the sockets error value
-11	SSL received a badly formatted message
-12	A bad message authentication code was received
-13	Operation is not supported by SSL
-14	The certificate signature is not valid
-15	The certificate is bad
-17	Permission was denied to access object
-20	Unable to allocate storage required for SSL processing
-21	SSL detected a bad state in the SSL session
-22	The socket used by the SSL connection has been closed
-25	The date in the certificate is in a bad format
-26	The key length is bad for export
-90	Not a key ring file
-91	The password in the key database has expired
-92	Certificate is not valid or is rejected by the exit program
-94	SSL_Init() was not previously invoked for the job
-95	There is no key ring for SSL initialization
-96	SSL is not enabled

Table 21. Other SSL return codes (continued)

Return code	Description
-97	The specified cipher suite is not valid
-98	The SSL session ended
-99	An unknown or unexpected error occurred during SSL processing
-1010	Double encryption is not allowed when using AC2 and IP-SEC

Related tasks

Configuring DCM

Managing the certificate assignment for an application

Managing public Internet certificates for SSL communications sessions

Creating and operating a local CA

Managing applications in DCM

“Checking system status” on page 91

You need to confirm that your Telnet is ready for Secure Sockets Layer (SSL) sessions.

Related reference

Obtaining a copy of the private CA certificate

TRCTCPAPP service program outputs

You can run a Virtual Terminal Manager (VTM) component trace with the user data field set to Telnet.

For the trace TCP/IP application (TRCTCPAPP) command, the listing of the VTM component trace shows up as a spooled file, called VTMTRACE with the user data field set to TELNET. The system places this file in the default output queue of the profile that runs the TRCTCPAPP *TELNET *OFF call. At the same time, all server job flight recorders are dumped to spooled files called QTOCTTRC with user data set to QTVnnnnnn.

Here is an example of what you see in your interactive job log when you perform a TRCTCPAPP *OFF call.

```

Command Entry                               SYSNAM03
Request level: 1
All previous commands and messages:
> trctcpapp *telnet *off
Spooled printer file 1 opened for output.
Trace data for application TELNET formatted: Spooled VTMTRACE user data 'TELNET'
Trace data for application TELNET formatted: Spooled QTOCTTRC user data 'TV017231'
Trace data for application TELNET formatted: Spooled QTOCTTRC user data 'TV017230'
Trace data for application TELNET formatted: Spooled QTOCTTRC user data 'TV017229'
Trace data for application TELNET formatted: Spooled QTOCTTRC user data 'TV017232'
Trace data for application TELNET formatted: Spooled QTOCTTRC user data 'TV017233'
Trace data for application TELNET formatted: Spooled QTOCTTRC user data 'TV017234'
More...
Type command, press Enter.
====>
F3=ExitF4=Prompt F9=Retrieve F10=Exclude detailed messages
F11=Display full F12=Cancel F13=Information Assistant F24=More keys

```

Here is an example of what you see in your default output queue.

Work with All Spooled Files

Type options, press Enter.

1=Send 2=Change 3=Hold 4=Delete 5=Display 6=Release 7=Messages
8=Attributes 9=Work with printing status

Opt File	User	Queue	Device or User Data	Sts	Total Pages	Page
VTMTRACE	JEFF	JEFFSOUTQ	TELNET	HLD	46	1
QTOCTTRC	JEFF	JEFFSOUTQ	TV017231	HLD	4	1
QTOCTTRC	JEFF	JEFFSOUTQ	TV017231	HLD	2	1
QTOCTTRC	JEFF	JEFFSOUTQ	TV017231	HLD	2	1
QTOCTTRC	JEFF	JEFFSOUTQ	TV017231	HLD	2	1
QTOCTTRC	JEFF	JEFFSOUTQ	TV017231	HLD	2	1

Parameters for options 1, 2, 3 or command

==>

F3=Exit F10=View 4 F11=View 2 F12=Cancel F22=Printers F24=More keys

Only one file that is called VTMTRACE that is created. If SSL Telnet mode is operational on the server, you may have one or more QTOCTTRC files.

Here is an example of a QTOCTTRC file. This spooled file is a Telnet server job (QTVTELNET) as opposed to a QTVDEVICE job.

```

                                Display Spooled File
File . . . . . : TV017231                               Page/Line  1/6
Control . . . . .           Columns                    1 - 78
Find . . . . .
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...
5769TC1 V4R4M0 990521 TRCTCPAPP Output SysName Date-12/11/98 Time-14:08:32 Page-
TRCTCPAPP Attributes
  Application.....: Telnet Server
  Buffer size (KB).....: 0
                        (Default of 0 means 16MB buffer)
  Trace full action.....: *WRAP
  Job id.....: 017231/QTCP /QTVTELNET
  Start date/time.....: Fri Dec 11 13:50:33 1998
  End date/time.....: Fri Dec 11 14:08:34 1998
  Trace buffer wrapped.....: No
Telnet Server Attributes
  AutoStart server.....: 'Y'
  Number servers.....: 2
  Session keep alive timeout..: 0
  Default NVT type.....: >*VT100<
  Outgoing EBCDIC/ASCII table.: >*CCSID <
  Incoming ASCII/EBCDIC table.: >*CCSID <
  Coded character set id.....: 84542
  Attributes version id.....: >V4R4M0 <
Trace common buffer structure:
  80000000 00000000 161A8753 14001074 | .....g.....| Byte 16
  80000000 00000000 161A8753 14FFFFE4 | .....g....U| Byte 48
  80000000 00000000 161A8753 14005820 | .....g.....| Byte 80
  00FF0000 00000084 F0F1F7F2 F3F1D8E3 | ..0....d017231QT| Byte 112
  C3D74040 40404040 D8E3E5E3 C5D3D5C5 | CP QTVTELNE| Byte 144
  E340C699 8940C485 8340F1F1 40F1F37A | T Fri Dec 11 13:| Byte 176
  F5F07AF3 F340F1F9 F9F8D8E3 E5F0F1F7 | 50:33 1998QTV017| Byte 208
  F2F3F140 |231 | Byte 228
Flight Records:
qvtvtnet: Job: QTVTELNET/QTCP/017231
(C) Copyright IBM Corporation, 1999
Licensed Material - Program Property of IBM.
Refer to Copyright Instructions Form No. G120-2083
ProdId: 5769-SS1 Rel: V4R4M0 Vers: V4R4M0 PTR: P3684767
qvtvtnet: Program QTVTELNET dated 04 December 1998 running
qvtvtnet: Source file: qvtvtnet.plc
qvtvtnet: Last modified: Wed Dec 9 11:57:40 1998
qvtvtnet: Last compiled at 12:00:10 on Dec 9 1998
qvtvtnet: Arguments passed: 1
qvtvtnet: Time Started: Fri Dec 11 13:50:34 1998
qvtvtnet: sigaction() for SIGUSR1 is EndClientSession()
qvtvtnet: Set Telnet Server job identity for OpNav
qvtvtnet: Need to setup SSL_Init_Application()
qvtvtnet: SSL_Init_Application() successful
qvtvtnet: Find Telnet Server control block
qvtvtnet: Lock Telnet Server control block
qvtvtnet: Open driver to stream
qvtvtnet: First Telnet Server Job...

F3=Exit   F12=Cancel  F19=Left  F20=Right  F24=More keys

```

Here is an example of another QTOCTTRC file. This is a device manager spooled file, as opposed to the QTVTELNET server job.

```

                                Display Spooled File
File . . . . . :      TV017230                Page/Line  1/6
Control . . . . . :                               Columns    1 - 78
Find . . . . . :
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...
TRCTCPAPP Attributes
  Application.....: Telnet Server
  Buffer size (KB).....: 0
                        (Default of 0 means 16MB buffer)
  Trace full action.....: *WRAP
  Job id.....: 017230/QTCP /QTVDEVICE
  Start date/time.....: Fri Dec 11 13:50:33 1998
  End date/time.....: Fri Dec 11 14:08:39 1998
  Trace buffer wrapped.....: No
Telnet Server Attributes
  AutoStart server.....: Y
  Number servers.....: 2
  Session keep alive timeout..: 0
  Default NVT type.....: >*VT100<
  Outgoing EBCDIC/ASCII table.: >*CCSID <
5769TC1 V4R4M0 990521 TRCTCPAPP Output SysName Date-12/11/98 Time-14:08:32 Page-
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...
  Incoming ASCII/EBCDIC table.: >*CCSID <
  Coded character set id.....: 84542
  Attributes version id.....: >V4R4M0 <
Trace_common buffer structure:
  80000000 00000000 3DA86C25 5F001074 | .....y...| Byte 16
  80000000 00000000 3DA86C25 5FFFFFFE4 | .....y..U| Byte 48
  80000000 00000000 3DA86C25 5F002F64 | .....y...| Byte 80
  00FFF000 00000084 F0F1F7F2 F3F0D8E3 | ..0....d017230QT| Byte 112
  C3D74040 40404040 D8E3E5C4 C5E5C9C3 | CP QTVDEVIC| Byte 144
  C540C699 8940C485 8340F1F1 40F1F37A | E Fri Dec 11 13:| Byte 176
  F5F07AF3 F340F1F9 F9F8D8E3 E5F0F1F7 | 50:33 1998QTV017| Byte 208
  F2F3F040 |230 | Byte 228
Flight Records:
qvtvncsh: >>>> entry
(C) Copyright IBM Corporation, 1999.
Licensed Material - Program Property of IBM.
Refer to Copyright Instructions Form No. G120-2083
ProdId: 5769-SS1 Release: V4R4M0 Version: V4R4M0 PTR: P3684767
qvtvncsh: Program QTVTNCSSH dated 04 December 1998 running
qvtvncsh: iActiveLogLevel: 0
qvtvncsh: Source file: qvtvncsh.c
qvtvncsh: Last modified: Wed Dec 9 11:48:33 1998
qvtvncsh: Last compiled at 11:59:42 on Dec 9 1998
qvtvncsh: SignalHandler() registered with signal()
qvtvncsh: Arguments passed: 4
qvtvncsh: argc: 4
qvtvncsh: argv[0]: >QSYS/QTVTNCSSH<
qvtvncsh: argv[1]: ><
qvtvncsh: argv[2]: >1p<
qvtvncsh: argv[3]: >s<
SignalHandler: >>>> entry
SignalHandler: Caught signal SIGSEGV

F3=Exit   F12=Cancel  F19=Left   F20=Right  F24=More keys

```

Related concepts

“Materials needed to report Telnet problems”

You might need to provide your service representative with this information when you report a Telnet problem.

Materials needed to report Telnet problems

You might need to provide your service representative with this information when you report a Telnet problem.

- Telnet Server job logs:

- QTVTELNET job log
- QTVDEVICE job log
- Some details on the problem scenario. For example:
 - The type of remote host you are using to Telnet from or to, such as System i, System z, or System p. This is particularly useful if you are doing cascaded Telnet functions.
 - The type of client attempting to connect to the Telnet server, such as IBM Personal Communications and System i Access for Windows.
- The job log of the interactive job running Telnet client (when Telnet client is under investigation).
- The trace job (TRCJOB) output of the failing interactive job (especially important if running Telnet client).

Note: Use TRCJOB *ON to start this trace. The result is a QPSRVTRC spooled file in the interactive job.

- A communications trace of the failure, formatted for both ASCII and EBCDIC, which contains TCP/IP data only. Your service representative can direct you to include broadcast messages in this trace. In addition, you might need to filter this trace on a specific IP address if you have a large amount of traffic on your network, and know the IP address of the failing client.
- Any licensed internal code (LIC) logs with major code 0700 and minor code 005x from the time of failure. In addition, there might be some major code 0701, and minor code 005x informational LIC logs that might be useful but not necessarily critical.
- A Virtual Terminal Manager (VTM) LIC component trace. You can gather this trace using the trace TCP/IP application TRCTCPAPP command, or through the start system service tools (STRSST) command. For full details on using the trace TCP/IP application (TRCTCPAPP) command, see the TRCTCPAPP command description.

You will have performance impacts when you run the VTM LIC trace. Some examples of using this command are:

- To trace all VTM activity:


```
TRCTCPAPP APP(*TELNET) SET(*ON)
```
- To trace the activity on a specific device, when you know the device name:


```
TRCTCPAPP APP(*TELNET) SET(*ON) DEVD(devicename)
```
- To trace the activity on a specific device, when you know the IP address of the client:


```
TRCTCPAPP APP(*TELNET) SET(*ON) RMTNETADR(*INET'www.xxx.yyy.zzz')
```
- To turn the trace off and spooled file output:


```
TRCTCPAPP APP(*TELNET) SET(*OFF)
```

Note: You should receive specific details of which trace parameters to use for your problem from your service representative before running this command. This ensures that you gather the correct information for your problem.

Related concepts

“TRCTCPAPP service program outputs” on page 95

You can run a Virtual Terminal Manager (VTM) component trace with the user data field set to Telnet.

Automatically generated diagnostic information

Some Telnet server errors automatically generate diagnostic information. This topic describes how to retrieve that information.

There might be some automatically generated diagnostic information produced when certain errors occur within the Telnet server. There are times when your service representative will require this diagnostic information to properly analyze a Telnet server problem.

If any Telnet or device manager job fails with a first failure data capture (FFDC) error, you will see the spooled files under the WRKSPLF QTCP profile. When a job fails with an FFDC error, each failing job will automatically have two dumps. One is a dump made by calling DSPJOB *PRINT, and DSPJOBLOG *PRINT makes the other. In this way, you get both the job log and job run attributes dumped and have the output from user data group together with a job number identifier. Then you can match up with any VTM component trace output.

You can see a total of four spooled files; two for the QTVTELNET job and two for the QTVDEVICE job. When the system encounters an FFDC error, these spooled files automatically generate. For an example, see the following figure:

```

Work with All Spooled Files

Type options, press Enter.
  1=Send 2=Change  3=Hold   4=Delete  5=Display  6=Release  7=Messages
  8=Attributes          9=Work with printing status

Opt  File           User      Queue           Device or
      QPJOBLOG      QTCP     QEZJOBLOG      TV016868   HLD   4
      QPDSPJOB      QTCP     QPRINT         TV016868   HLD   7
      QPJOBLOG      QTCP     QEZJOBLOG      TV016955   HLD   3
      QPDSPJOB      QTCP     QPRINT         TV016955   HLD   7
      QPJOBLOG      QTCP     QEZJOBLOG      TV017231   HLD   3
      QPJOBLOG      QTCP     QEZJOBLOG      TV017232   HLD   3
      QPDSPJOB      QTCP     QPRINT         TV017232   HLD   7
      QPDSPJOB      QTCP     QPRINT         TV017231   HLD   7

Parameters for options 1, 2, 3 or command
===>
F3=Exit  F10=View 4  F11=View 2  F12=Cancel  F22=Printers  F24=More keys

```

Related information for Telnet

IBM Redbooks publications and Web sites contain information that relates to the Telnet topic collection. You can view or print any of the PDF files.

IBM Redbooks

V4 TCP/IP for AS/400 : More Cool Things Than Ever  (about 10 035 KB)

This publication provides extensive information about TCP/IP, including sample scenarios that demonstrate common solutions with example configurations.

Web sites

- **Internet Assigned Numbers Authority (IANA)**  (www.iana.org)
Find information about common port number assignments.

- **The Internet Engineering Task Force (IETF)**  (www.ietf.org)

Read Request for Comments (RFC), such as RFC 4777 5250 Telnet Enhancements .

Related reference

“PDF file for Telnet” on page 1
You can view and print a PDF file of this information.

Code license and disclaimer information

IBM grants you a nonexclusive copyright license to use all programming code examples from which you can generate similar function tailored to your own specific needs.

SUBJECT TO ANY STATUTORY WARRANTIES WHICH CANNOT BE EXCLUDED, IBM, ITS PROGRAM DEVELOPERS AND SUPPLIERS MAKE NO WARRANTIES OR CONDITIONS EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, REGARDING THE PROGRAM OR TECHNICAL SUPPORT, IF ANY.

UNDER NO CIRCUMSTANCES IS IBM, ITS PROGRAM DEVELOPERS OR SUPPLIERS LIABLE FOR ANY OF THE FOLLOWING, EVEN IF INFORMED OF THEIR POSSIBILITY:

1. LOSS OF, OR DAMAGE TO, DATA;
2. DIRECT, SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES, OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES; OR
3. LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF DIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, SO SOME OR ALL OF THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU.

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

- | The licensed program described in this document and all licensed material available for it are provided
- | by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement,
- | IBM License Agreement for Machine Code, or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

| **Programming interface information**

This Telnet publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM i5/OS.

| **Trademarks**

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

AIX
AS/400
i5/OS
IBM
IBM (logo)
OS/2
OS/400
Redbooks
System i
System p
System z
System/370

- | Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks
- | of Adobe Systems Incorporated in the United States, and/or other countries.

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 are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.



Printed in USA