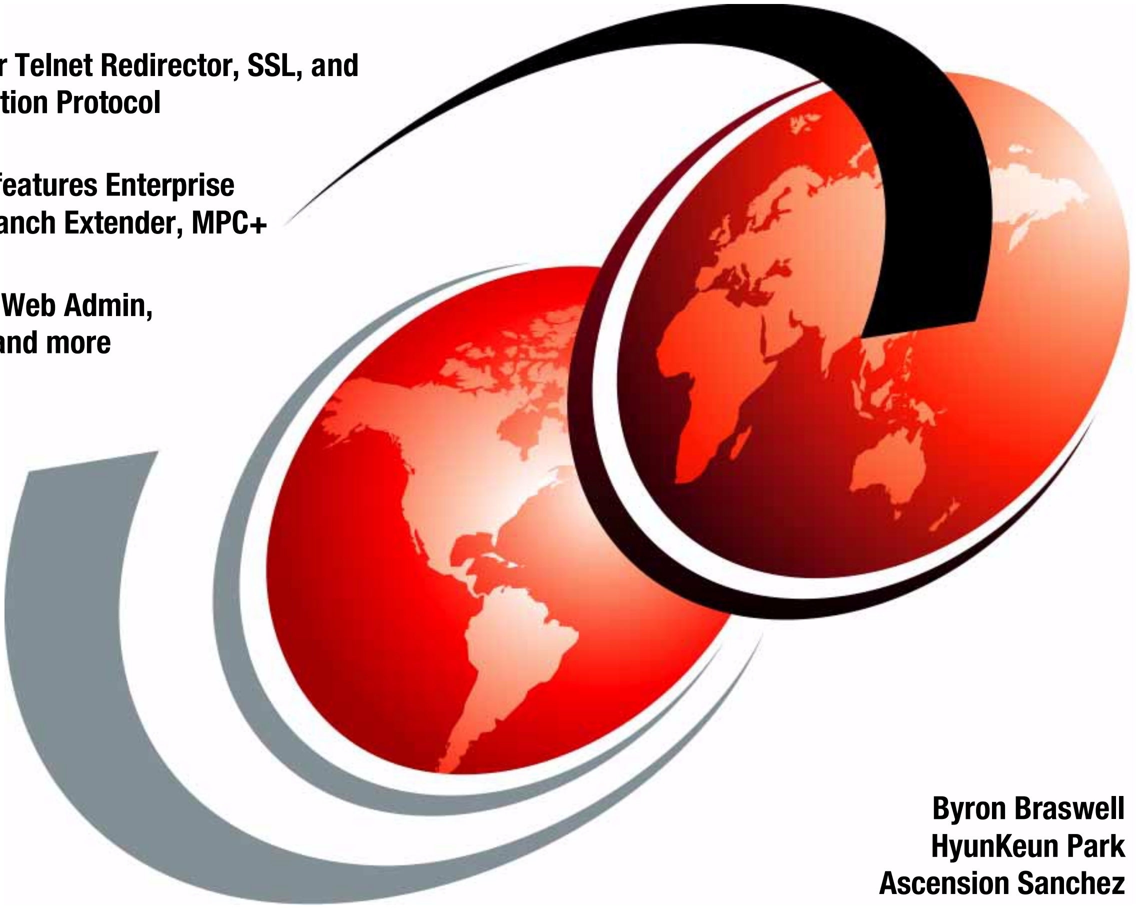
IBM Communications Server for AIX, V6

New Features and Implementation Scenarios

Scenarios for Telnet Redirector, SSL, and Service Location Protocol

Covers SNA features Enterprise Extender, Branch Extender, MPC+

Examples of Web Admin, 64-bit apps and more



Byron Braswell
HyunKeun Park
Ascension Sanchez

Redbooks

ibm.com/redbooks

SG24-5947-00

International Technical Support Organization

IBM Communications Server for AIX, V6 New Features and Implementation Scenarios

July 2000

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix A, “Special notices” on page 225.

First Edition (July 2000)

This edition applies to Version 6.0 of IBM Communications Server for AIX, Program Number 5765-E51 for use with the AIX Operating System.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. HZ8 Building 678
P.O. Box 12195
Research Triangle Park, NC 27709-2195

Contents

Preface

This redbook describes the new functionality included in the latest release of IBM Communications Server for AIX, Version 6. It focuses on the new functions, features and technologies implemented in this product. It helps you plan, install and configure the new functions and features quickly in a wide variety of environments.

Information on the new Service Location Protocol and Secure Sockets Layer support included with the TN3270 Server is presented along with installation and configuration examples. There are also information and configuration scenarios for the new Telnet Redirector function which also includes support for SSL connections.

This redbook also covers the many SNA features and enhancements including Enterprise Extender, Branch Extender and MultiPath Channel Plus (MPC+) support included in this release of CS/AIX. Functional overview and configuration examples are included.

The new Web Administration program, support for 64-bit SNA applications, CS/AIX licensing, and other features and enhancements are also covered.

This redbook does not cover the initial installation of CS/AIX on an AIX system. Nor does it discuss the configuration of CS/AIX features that were available in previous releases of the product (for example, TN3270 server, DLUR, SNA Gateway, ATM, frame relay, and so on). For a discussion of these topics, please see *IBM eNetwork Communications Server for AIX: Understanding and Migrating to Version 5 (Part 1): Configuration and New Features,* SG24-5215.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Raleigh Center.

Byron Braswell is a networking professional at the International Technical Support Organization, Raleigh Center. He writes extensively and teaches IBM classes worldwide in areas of network connectivity. Before joining the ITSO, he worked in IBM Learning Services Development in networking education development.

HyunKeun Park is an IT Specialist in the desktop software server support working for ITS in Korea. He has five years of experience in the networking software field in IBM. His areas of expertise include Communications Server and Personal Communications for OS/2, Windows NT, and AIX.

Ascension Sanchez is an IT support specialist in the AIX Systems Support Center in Basingstoke, England, where she specializes in AIX networking support. She has two years of experience in AIX, both spent working for IBM. Her areas of expertise include problem determination in the AIX base operating system and networking software for AIX. She holds a degree in Electronics and Electrical Engineering from the Universidad Politecnica de Madrid, Spain. Prior to joining IBM she worked as a Research Associate at the University of Birmingham, UK.

Thanks to the following people for their invaluable contributions to this project:

Donna Rutigliano
IBM Host Integration Servers Development, Research Triangle Park, North Carolina

Paul Landay
IBM CS/AIX Test, Research Triangle Park, North Carolina

Margaret Ticknor
IBM ITSO, Raleigh Center

Comments welcome

Your comments are important to us!

We want our Redbooks to be as helpful as possible. Please send us your comments about this or other Redbooks in one of the following ways:

- Fax the evaluation form found in “IBM Redbooks review” on page 237 to the fax number shown on the form.
- Use the online evaluation form found at http://www.redbooks.ibm.com/
- Send your comments in an Internet note to redbook@us.ibm.com

Part 1. Introduction

Chapter 1. Overview

IBM Communications Server for AIX, Version 6 brings the power of personal networking to your workstation. Whether it is for host terminal emulation, client/server and distributed applications, or connectivity across local and wide area networks (LANs and WANs), IBM Communications Server for AIX offers a robust set of communications, networking and systems management features.

In this chapter, we provide an overview of the new features and functions included in CS/AIX V6. For a review and detailed discussion of features and functions included in the previous release of Communications Server for AIX, please see *IBM eNetwork Communications Server for AIX: Understanding and Migrating to Version 5: Part 1 - Configuration and New Features*, SG24-5215.

1.1 Secure Sockets Layer support

CS/AIX provides support for Secure Sockets Layer (SSL) V3 connections between CS/AIX and telnet clients and/or IP hosts. The CS/AIX TN3270E server supports SSL connections to TN3270 clients while the TN Redirector supports SSL connections to Telnet clients and TN servers (3270 and 5250). This security uses SSL Version 3.0 to provide data encryption, server authentication and optional client authentication using signed certificates. The primary goal of the SSL is to provide private and reliable communications between two applications.

By using this SSL protocol, you can establish TCP/IP connections that provide the following security features:

- Message privacy (encryption of data)
- Message integrity (each packet arrives unaltered)
- Authentication (identity of remote nodes can be verified)

1.2 TN Redirector

The CS/AIX TN Redirector feature provides passthrough TCP/IP access to host applications, such as 3270 applications and host printing applications, for TN3270, TN3270E, TN5250 and Virtual Terminal (VT) clients, referred to collectively as Telnet clients. The Telnet user communicates with CS/AIX over a TCP/IP connection and CS/AIX then communicates with the host over another TCP/IP connection.

TN Redirector also supports filters on which client workstations are allowed access to the host. Filtering can be done by fully qualified IP address or host name. The default is to grant access to all clients.

1.3 Service Location Protocol

Service Location Protocol (SLP) is an Internet Engineering Task Force (IETF) proposed standard protocol that is designed to simplify the discovery and use of network resources. It allows SLP-enabled resources (TN3270E servers, for example) to advertise their services. SLP-enabled clients automatically select the most appropriate server based on attributes (such as current load) of the server.

As network IP environments become more dynamic in character, SLP will play a major role in managing available network resources in these environments.

IBM Communications Server for AIX, Version 6 provides TN3270E Server support for SLP. SLP-enabled TN3270 clients can automatically select the least loaded CS/AIX TN3270E server based on server load parameters.

1.4 Enterprise Extender

Enterprise Extender (HPR/IP) provides High Performance Routing (HPR) functionality over IP connections to support SNA applications that are connected over an IP network. It allows you to take advantage of the HPR benefits in an IP-routed network, and participate as a full APPN node in an APPN network.

HPR (which replaces intermediate session routing in APPN), is a routing technique that reduces processing overhead at intermediate nodes, reroutes sessions around failed nodes and links non-disruptively, and regulates traffic flow by predicting and reducing congestion in the network.

HPR’s main components are:

- Rapid Transport Protocol (RTP), which allows a node to be the initiator or terminator of an HPR connection.
- Automatic Network Routing (ANR), which allows a node to act as an intermediary along the path of an HPR connection.

Enterprise Extender in CS/AIX is implemented simply as a communications link. To connect two SNA applications over IP, you define an Enterprise

Extender link, in the same way as for any other link type such as SDLC or Ethernet.

1.5 Branch Extender

Network nodes in an APPN network need to maintain topology information about the location of other nodes in the network and the communications links between them, and to forward this information around the network when the topology changes. As the network grows in size, the amount of stored information and topology-related network traffic can become large and difficult to manage. The Branch Extender feature of APPN has been developed to provide a solution to these problems.

As the name implies, Branch Extender is designed for networks that can be divided into distinct areas such as separate branches of a large organization. It works by separating out branches from the main backbone APPN network (for example, the network in the organization's headquarters).

1.6 MPC+ support

Multipath Channel Plus (MPC+) provides support for High Performance Routing (HPR) connectivity over channel connections to host mainframe computers running VTAM V4R4 or later.

The ESCON adapter card required for MPC+ support enables an AIX system to appear to the host as one or more ESCON control units.

1.7 Web administration

IBM Communications Server for AIX, Version 6 includes a new tool to administer the CS/AIX configuration: the Web Administration program. It allows you to administer CS/AIX from a browser without the need to start an X session or telnet session to the CS/AIX server, and is particularly useful when connecting over slow or unreliable links.

With your Internet browser, you can access your CS/AIX configuration, register new resources, and manage them from around the world.

Administration functions are similar to those provided by the Motif administration program.

1.8 CS/AIX licensing

CS/AIX licensing is based on the number of concurrent users of the product. New functions are provided to record information about the current and peak usage of CS/AIX resources. You can use these functions to help determine whether your usage is within the limits permitted by your license.

1.9 CS/AIX documentation

Product documentation for CS/AIX now includes AIX docsearch indices. This allows a user with a Web browser and connectivity to the CS/AIX server to access and search all CS/AIX softcopy documentation for specific keywords.

1.10 64-bit application support

SNA applications using the CS/AIX APIs can be compiled and linked to run in either 32-bit mode or 64-bit mode. This allows SNA applications to take advantage of 64-bit hardware features such as large file, addressing and memory support.

1.11 Java CPI-C API

CS/AIX includes support to develop and implement Java object-oriented applications using the Common Programming Interface for Communications (CPI-C) API. This is in addition to the current support in CS/AIX for CPI-C API support for applications written in the C language.

CPI-C for Java is an object-oriented version of the x/open standard interface to the IBM SNA LU 6.2 for developing SNA applications. The basic goal of including Java CPI-C is to enable programmers to access classic SNA applications where corporate data is traditionally stored. A programmer familiar with standard CPI-C or APPC, who is also comfortable with object-oriented programming (for example in C++ or Java) will feel comfortable with the Java CPI-C API.

Part 2. Telnet services and enhancements

Chapter 2. Secure Sockets Layer support

This chapter introduces the Secure Sockets Layer (SSL) function of IBM Communications Server for AIX, Version 6. CS/AIX supports secure connections between Telnet clients and a CS/AIX TN3270E server. In addition, the CS/AIX TN Redirector supports both upstream and downstream SSL connections.

CS/AIX Secure Sockets Layer uses SSL Version 3 to provide data encryption and server/client authentication using signed certificates. The primary goal of the SSL protocol is to provide private and reliable communications between two applications. In the following sections, we'll discuss the concept of SSL and the way it securely handles data between a Telnet server and its clients.

2.1 Secure Sockets Layer (SSL) overview

SSL is an industry-standard protocol originally developed by Netscape Communications Corporation. It defines a method of providing a private channel between client and server that ensures privacy of data, authentication of the session partners, and message integrity.

- Privacy requires that the information flowing between client and server cannot be read by anyone else
- Authentication ensures that the partners are actually who they say they are
- Integrity ensures that information sent is not modified in transmission.

To achieve this, SSL uses three cryptographic techniques:

- Symmetric-key encryption
- Public-key encryption
- Hashing functions

We describe each of these techniques below:

2.1.1 Symmetric-key encryption

Symmetric-key encryption uses a single key, which must be known to both client and server, to encrypt and decrypt messages. It is very fast and secure, and for this reason is used for most encryption. However, a limitation of symmetric-key encryption is that the key must be passed between server and client before secure transmission starts.

2.1.2 Public-key encryption

Public-key encryption uses a pair of keys, a public key and a private key. The server's public key is published, and the private key is kept secret. To send a secure message to the server, the client encrypts the message using the server's public key. When the server receives the message, it decrypts the message using its private key. The message is secure because it cannot be decrypted by means of the public key. Public key encryption has a big advantage over the symmetric-key approach in that no secret key needs to be transmitted. However, it requires much more processing power than symmetric-key encryption.

2.1.3 Hashing functions

Hashing functions are used to ensure message integrity. The message sender applies a hashing function to the message to create a message digest, which it sends with the message. The receiver applies the same algorithm to the message and compares the two digests. If they are identical, it proves that the message has not been tampered with during transmission.

SSL uses these techniques to provide its three basic security services:

- Message privacy is achieved through a combination of public-key and symmetric-key encryption. During session setup, a symmetric key is created using information exchanged using public-key encryption. Once the session is initiated, all traffic between client and server is encrypted using symmetric-key encryption and the key negotiated during session setup. In this way, SSL exploits the advantages of both symmetric and public-key encryption to ensure message privacy.
- The message integrity service ensures that messages cannot be changed in transit without detection. SSL uses hash functions to ensure message integrity.
- Mutual authentication is the process whereby the client and the server convince each other of their identities. The client and server identities are encoded in public-key certificates.

2.2 Public-key certificates

Public-key encryption provides a powerful way by which information can be sent across the Internet in encrypted form without the decoding key (the private key) ever having to be transmitted. However, how can you be sure that the owner of the public key is really who it claims to be?

The *public-key certificate* is a means of guaranteeing the integrity of a public key.

Public-key certificates are special files adhering to the X.509 standard and issued by a certifying authority (CA). Being in a standard form, they can be recognized and validated by software, and they are, of course, tamper proof.

A public-key certificate contains the following identifying components:

- The subject’s distinguished name, which consists of the common name, or host name, of the Web site (server) that will use the certificate - for example, rs60030.itso.ral.ibm.com
- The organization name - for example, IBM
- Optionally, an organization unit - for example, ITSO
- Optionally, a city or locality - for example, Raleigh
- Optionally, a state or province - for example, NC
- A country code of at least two characters - for example, US
- The issuer’s distinguished name
- The subject’s public key
- The issuer’s signature
- A validity period
- A serial number

The certificate tells you that the CA confirms that the public key belongs to the organization identified by the distinguished name.

SSL has been implemented in IBM Communications Server for AIX to support establishment of secure sessions between Telnet clients and the TN3270E server and/or TN Redirector.

Clients that support SSL V3 encryption are IBM Personal Communications for Windows 95 and Windows NT Version 4.3 and IBM Host On-Demand Version 2.0 and later. The IETF TN3270 working group has indicated that SSL V3 is the protocol of choice while addressing the security issues between TN clients and servers.

2.3 SSL implementation in CS/AIX

The TN3270E Server and TN Redirector functions of IBM Communications Server for AIX, Version 6 support SSL connections.

To establish an SSL connection, you must do the following:

1. Install SSL support for CS/AIX
2. Enable SSL in the TN3270 server and/or TN Redirector configuration
3. Execute the Key Management utility to manage certificates
4. Decide what type of certificate to use
5. Decide what type of authentication to use

2.3.1 Install SSL support for CS/AIX

Version 4.3.2-ML2 or later of the AIX operating system is required to support CS/AIX SSL configurations.

Secure Sockets Layer support for CS/AIX requires installation of additional filesets that are included with the CS/AIX distribution media. The following filesets are included with CS/AIX for SSL support:

gskit.rte AIX Certificate and SSL Base Runtime. The gskit.rte fileset must be at the 4.0.3.42 level or later.

sna.strong_sec.tnssl Strong security, available in the United States and Canada. Depending on your location, you may or may not have the strong security fileset because it is not available in your country.

If you want to use SSL with TN server or TN Redirector, you must install the AIX Certificate and SSL Base Runtime fileset. If you want to use strong security, and the additional fileset is available, you must install it in addition to the AIX Certificate and SSL Base Runtime fileset.

2.3.2 Enable SSL in TN3270 server/TN Redirector

2.3.2.1 TN3270 server

To configure a secure TN3270 server, proceed as if you were configuring a normal TN3270 server.

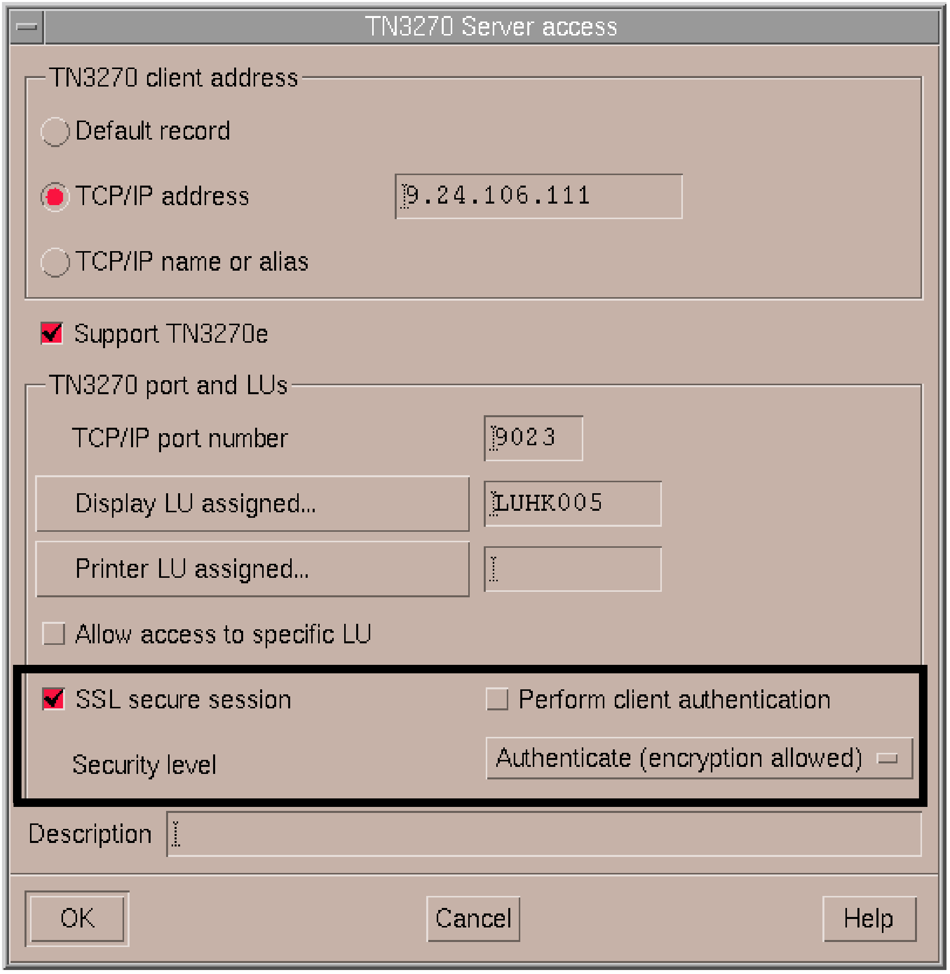
For more information on how to perform the normal TN3270 server configuration, refer to *IBM Communications Server for AIX Administration Guide Version 6*, SC31-8586, or *IBM eNetwork Communications Server for AIX: Understanding and Migrating to Version 5: Part 1 - Configuration and New Features*, SG24-5215.

From the main CS/AIX node panel, select:

Services -> TN Server -> TN Server

Select the **TN3270 server access records** pane and click the **New** button.

A panel similar to the one shown on Figure 1 is displayed. Selecting the **SSL secure session** button will display additional options for configuring SSL communications for clients requiring secure connections.



TN3270 Server access

TN3270 client address

○ Default record

● TCP/IP address 9.24.106.111

○ TCP/IP name or alias

☑ Support TN3270e

TN3270 port and LUs

TCP/IP port number 9023

Display LU assigned... LUHK005

Printer LU assigned...

□ Allow access to specific LU

☑ SSL secure session

□ Perform client authentication

Security level: Authenticate (encryption allowed)

Description

Figure 1. TN3270 Server access window

SSL secure session: Select this option if this session is to use SSL security. You can choose this option only if you have the SSL Runtime Toolkit software installed on the CS/AIX server.

Perform client authentication: Select this option if you want to verify that clients are authorized to establish a secure connection to the TN3270E server. Client Authentication also enables you to use Certificate Revocation List (CRL) support by configuring the location of a Lightweight Directory Access Protocol (LDAP) Server where the CRL is stored. This information is entered in the SSL Client Revocation dialog window. You can choose this option only if you have chosen **SSL secure session**.

Configuring the LDAP server for CRL support is not covered in this document. Please see the documentation for the specific LDAP server being used for the needed configuration information.

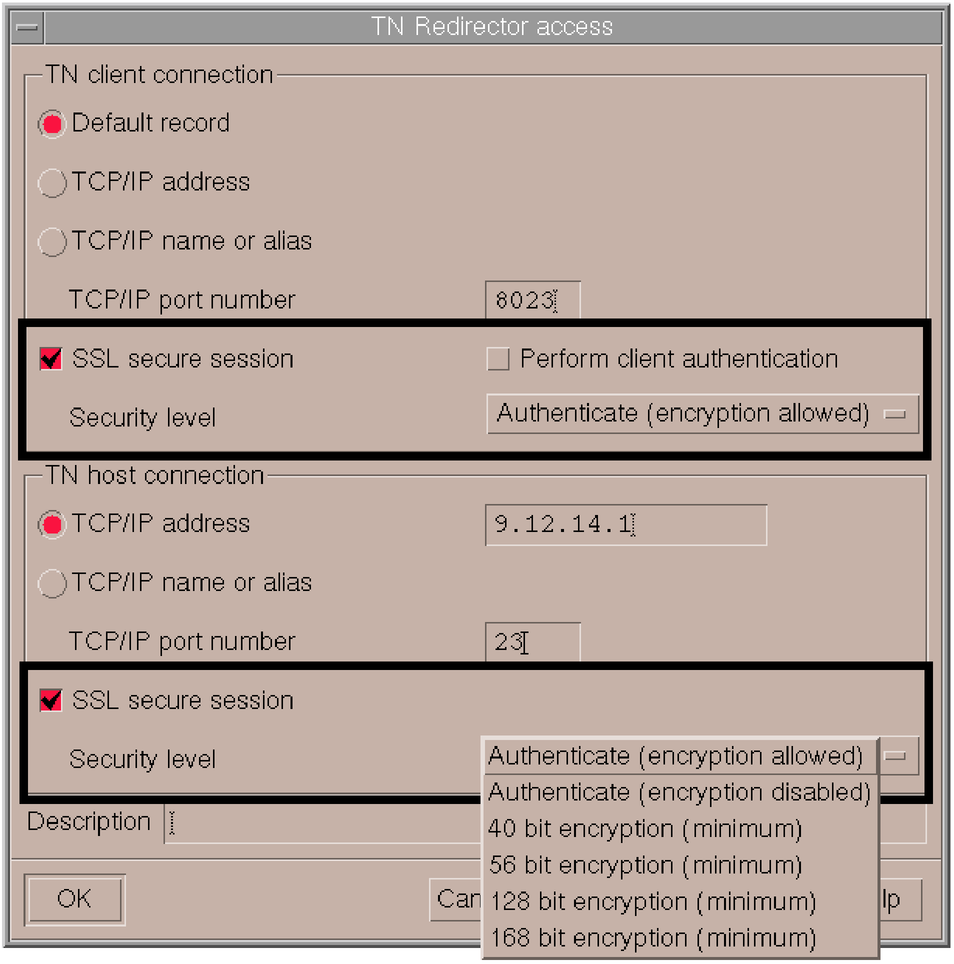
Security Level: This option allows you to specify the security level that clients must use in order to establish a connection to the TN3270E server. You can choose this option only if you have chosen **SSL secure session**. See Figure 2 on page 15 for a display of the available security level options.

2.3.2.2 TN Redirector

To configure a secure TN Redirector, proceed as if you were configuring a normal TN Redirector. See Chapter 3, “TN Redirector” on page 33 for configuration assistance.

- Click **Services -> TN Server -> TN Server.**
- Select the **TN Redirector access records** pane and click on the **New** button.

A panel similar to the one shown in Figure 2 on page 15 is displayed. Note that the **SSL secure session** button is displayed for both the client connection and the host connection. Selecting this button displays additional options for configuring SSL communications.



TN Redirector access

TN client connection

● Default record

○ TCP/IP address

○ TCP/IP name or alias

TCP/IP port number: 8023

☑ SSL secure session □ Perform client authentication

Security level: Authenticate (encryption allowed)

TN host connection

● TCP/IP address: 9.12.14.1

○ TCP/IP name or alias

TCP/IP port number: 23

☑ SSL secure session

Security level: Authenticate (encryption allowed)

Description:

Authenticate (encryption disabled)
40 bit encryption (minimum)
56 bit encryption (minimum)
128 bit encryption (minimum)
168 bit encryption (minimum)
OK
Can
lp

Figure 2. TN Redirector access window

2.3.3 Key Management utility

To make a secure connection between the TN server and clients with SSL V3.0 in IBM Communications Server for AIX, Version 6, you may get a Certificate from a certificate authority (CA), or the IBM Key Management utility allows you to request the server to certify itself.

The IBM Key Management utility allows you to do the following:

- Request certificates from a CA
- Create “self-signed” certificates

- Store, export, and import certificates

All these certificates adhere to the X.509 standard (either V1, 2, or 3).

Use of the IBM Key Management utility is discussed in “Configuring SSL security” on page 19.

2.3.4 Deciding what type of certificates to use

There are three types of certificates available for use when setting up SSL for TN server with CS/AIX. One type of certificate, self-signed, can be generated by the user. The other two types of certificates, well-known and unknown, require the user to request a certificate from a certificate provider. The type of environment the user will be implementing will dictate the type of certificate the user should use. The following is a brief description of each type of certificate that will aid the user in deciding what type of certificate is best for them.

2.3.4.1 Self-signed certificates

Receipt of a certificate from a well-known trusted CA can take up to three weeks. Until you receive the public server certificate(s), you can create a self-signed certificate by using the IBM Key Management database, to enable SSL sessions between clients and the server. A self-signed certificate should be used for controlled testing purposes only. To ensure adequate security for your site, a self-signed certificate should not be used in a production environment.

2.3.4.2 Certificates from a well-known trusted certificate authority

A well-known trusted certificate authority (CA) is one that is widely known and trusted by the user community. Signer (CA root) certificates for well-known trusted CAs are present by default in the IBM Key Management database and will also be present in the key databases of most other SSL-enabled applications. In practical terms, this means that every user will have the public key of each well-known CA and will have their software configured to trust the CA. This allows the user’s software to automatically check the validity on any certificate issued by a well-known CA without further configuration.

Using well-known certificates requires the user to contact a well-known CA provider (for example Verisign or Thawte) and apply for the additional certificate(s) the user needs. Certificates from a well-known CA are adequate for a production environment.

2.3.4.3 Certificates from an unknown CA

A certificate issued by an unknown CA is termed *unknown* because the signer (CA root) certificate is not already present in the IBM Key Management database. This will be the case if the user decides to purchase a certificate from a CA whose signer (CA root) certificate is not already present in the database, or if the user does not want to depend on an outside vendor to provide certificates. The user can purchase software such as IBM Vault Registry to generate certificates for their secure environment. Certificates generated from an unknown CA or generated by IBM Vault Registry software are adequate for a production environment.

2.3.5 Deciding what type of authentication to use

CS/AIX SSL supports data encryption, server authentication, and client authentication. Data encryption ensures that the data flowing between the TN server and your TN3270 emulator is in encrypted form. Server authentication is always performed when SSL is enabled. Client authentication can optionally be performed to provide additional security.

Server authentication and client authentication are explained in the following sections.

2.3.5.1 Server authentication

Server authentication allows a TN3270 client to be sure that the TN server it is connected to is the one it expects. Server authentication requires two pieces: a key pair is required to allow data encryption and decrypting to be carried out and a certificate on the server is required to allow authentication. The certificate and key pair are stored in a key database file and comprise a single record in the database. The database is used by TN server to implement SSL and resides on the CS/AIX server running TN server. The emulator software (for example Personal Communications V4.3) on the client machine also uses a similar database to store the server’s signer (CA root) certificate to implement SSL.

2.3.5.2 Client authentication

Client authentication allows the TN server to verify that the client has a valid, signed certificate. You can use SSL with server authentication alone or enable client authentication that also requires the client to have a certificate for authentication. Client authentication requires three pieces: a key pair is required to allow data encryption and decrypting to be carried out, the server must have a certificate for authentication, and the client must have a certificate for authentication. The certificate(s) and key pair are stored in a key database file and comprise a single record in the database. The database on the CS/AIX server is used by TN server to implement SSL. The emulator software (for example IBM Personal Communications V4.3) on the client machine also uses a similar database to store the necessary certificate(s) to implement SSL.

2.4 Scenario

For this scenario we use the following software:

- IBM Communications Server for AIX, Version 6
- IBM Personal Communications for Windows NT Version 4.3

We will configure an SSL connection between a CS/AIX TN3270E server and a PCOMM TN3270 client. The configuration is shown in Figure 3.

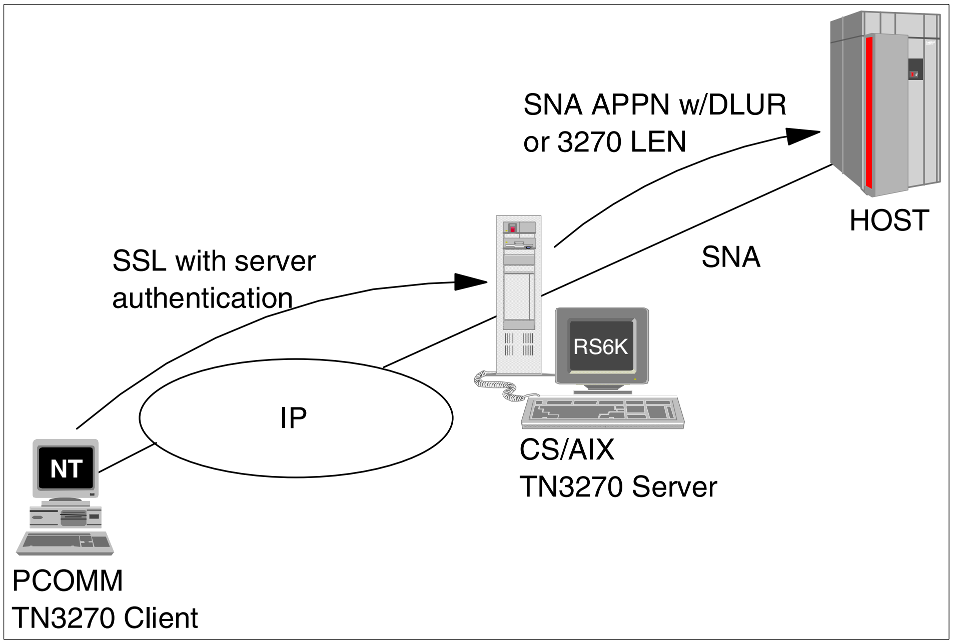


Figure 3. SSL scenario

2.4.1 Enabling SSL for a TN3270 server

As shown previously in Figure 1 on page 13, the normal process of configuring a CS/AIX TN3270 server allows you to specify whether the session will use SSL for a secure connection. For our scenario, we will use only server authentication with 56-bit encryption.

For more information on how to perform the basic TN3270 server configuration, refer to *IBM Communications Server for AIX Administration Guide Version 6*, SC31-8586, or *IBM eNetwork Communications Server for AIX: Understanding and Migrating to Version 5: Part 1 - Configuration and New Features,* SG24-5215.

2.4.2 Configuring SSL security

The key database file on the CS/AIX server is managed by the IBM Key Management utility. Running the executable for it, `snakeyman`, will launch a Java graphical user interface program. Before you can run the utility, you will need to export the JAVA_HOME environment variable with the following command:

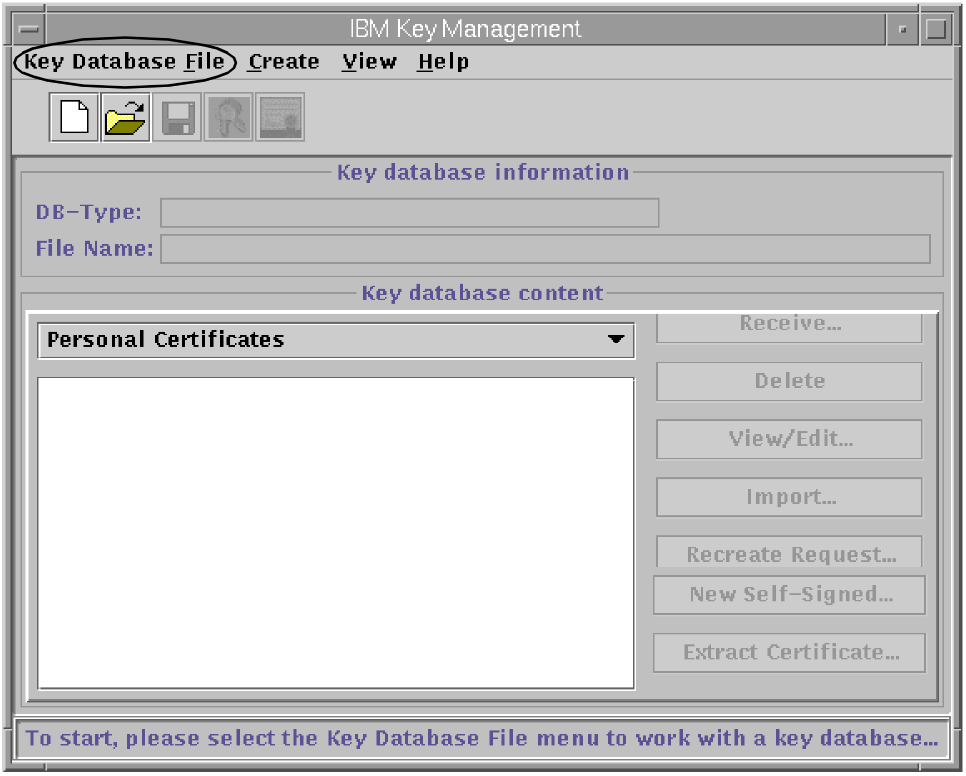
```
export JAVA_HOME=/usr/jdk_base
```

where `/usr/jdk_base` is the directory where Java 1.1.6 or later is installed.

In addition there may be a need to export the DISPLAY environment variable. Once the export(s) have been run, type:

```
snakeyman
```

and the database GUI will open. The IBM Key Management window shown in Figure 4 will be displayed.



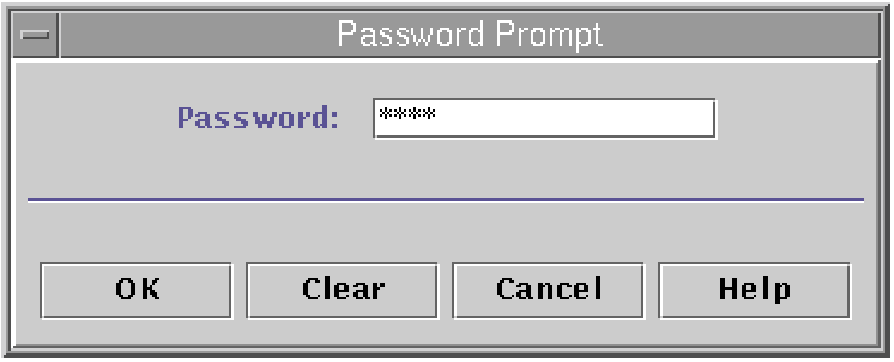
To start, please select the Key Database File menu to work with a key database...

Figure 4. IBM Key Management window

Before using the database, a database file must be selected. Click **Key Database File** on the menu bar.

If **New** is selected, the user must provide a new database name. The key database type must default to the CMS key database file, and the name must be ibmcs.kdb. The required location for this file is in /etc/sna/. Installation of the SSL code automatically creates an ibmcs.kdb file. Therefore, select **New** only if the original ibmcs.kdb file has become corrupt or if you simply want to create a new kdb from scratch.

If **Open** is selected, a list of files from /etc/sna/ will come up. Locate the ibmcs.kdb file, highlight it, and select **OK**. At this point a password prompt will pop up as shown in Figure 5.



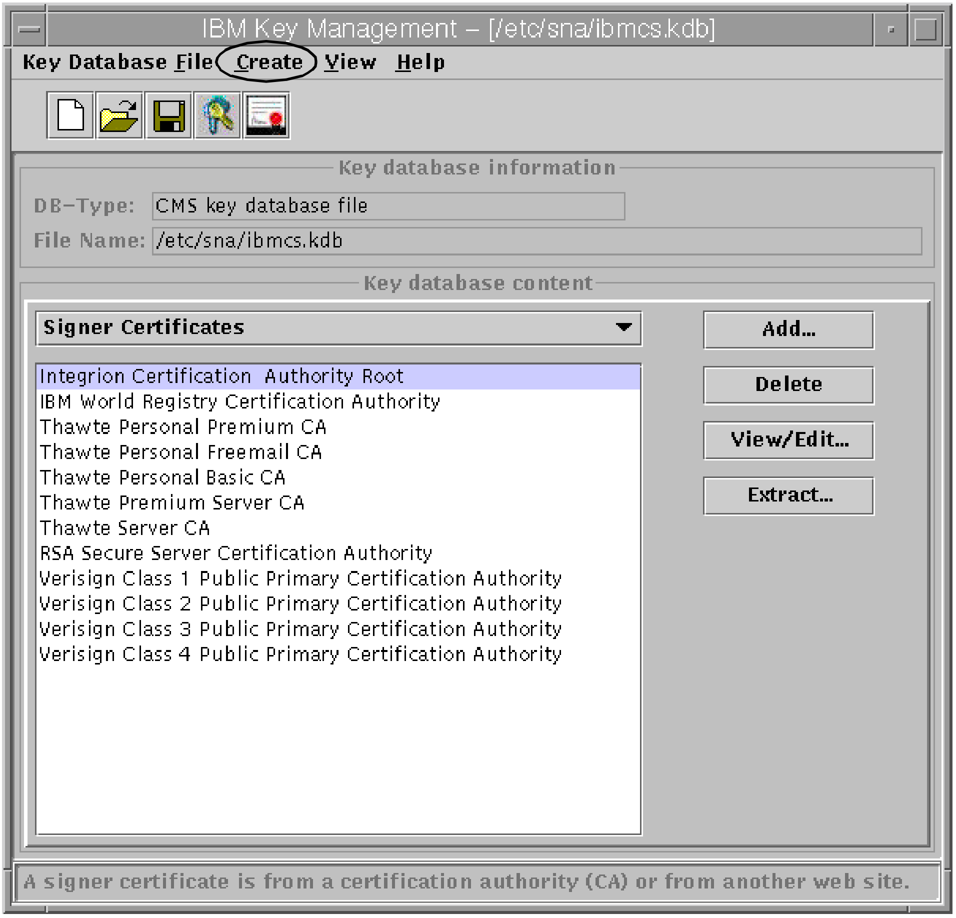
Password: *****

Figure 5. Password Prompt dialog

The password is initially set to `ibmcs`. However, you should change this once you have entered the database. To change the database password, select **Key Database File** on the menu bar of the IBM Key Management panel. Select **Change Password** and enter your new password. When you change the password, be sure to stash it. Otherwise, CS/AIX code will not be able to open the key database.

This password will be used each time you open this key database file, so it is important to remember it.

Select **OK**. The following panel is displayed when the ibmcs.kdb file is opened.



DB-Type: CMS key database file

File Name: /etc/sna/ibmcs.kdb

Signer Certificates

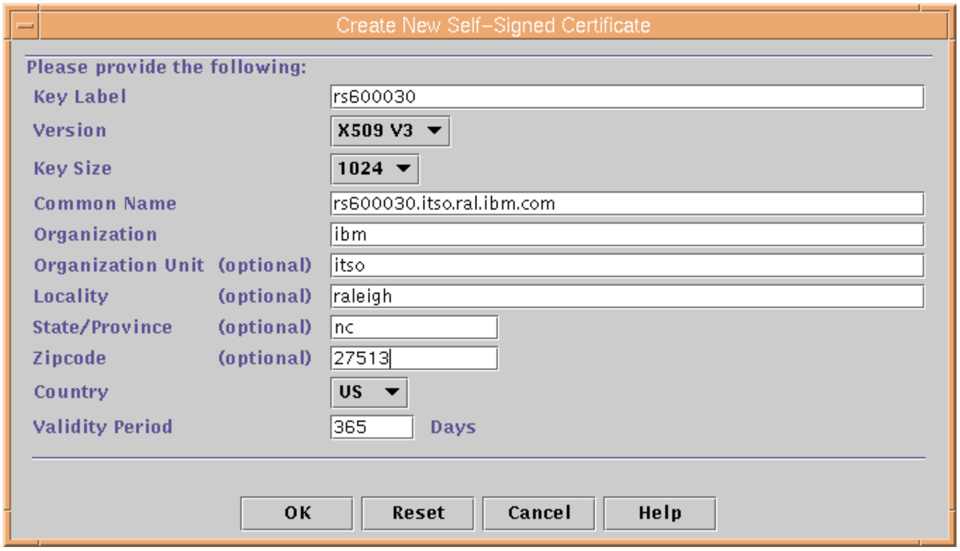
- Integrion Certification Authority Root
- IBM World Registry Certification Authority
- Thawte Personal Premium CA
- Thawte Personal Freemail CA
- Thawte Personal Basic CA
- Thawte Premium Server CA
- Thawte Server CA
- RSA Secure Server Certification Authority
- Verisign Class 1 Public Primary Certification Authority
- Verisign Class 2 Public Primary Certification Authority
- Verisign Class 3 Public Primary Certification Authority
- Verisign Class 4 Public Primary Certification Authority

A signer certificate is from a certification authority (CA) or from another web site.

Figure 6. Key Management window for ibmcs.kdb

This view lists the signer certificates stored from trusted Certificate Authorities. We will create a self-signed certificate for our scenario.

Select **Create -> New Self-signed Certificate**. The panel shown in Figure 7 is displayed.



Create New Self–Signed Certificate

Please provide the following:

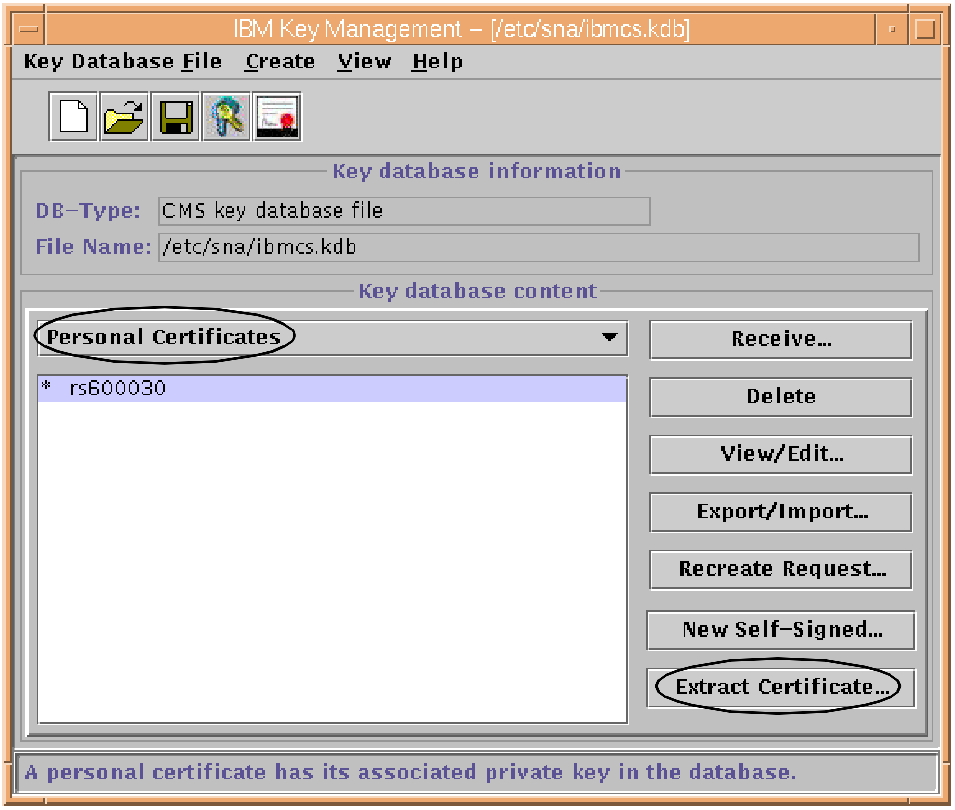
Key Label		rs600030
Version		X509 V3
Key Size		1024
Common Name		rs600030.itso.ral.ibm.com
Organization		ibm
Organization Unit	(optional)	itso
Locality	(optional)	raleigh
State/Province	(optional)	nc
Zipcode	(optional)	27513
Country		US
Validity Period		365 Days

Figure 7. Create New Self-Signed Certificate

Enter the data for your self-signed certificate:

- Enter the key label that is used to identify the key and certificate within the database.
- Select **X509 V3** as the certificate version.
- Enter the TCP/IP host name of the communication server as the common name (for example, rs600030.itso.ral.ibm.com).
- You can enter optional values, organization name, organization unit, city or locality, state or province, ZIP code.
- You must enter a country code.
- Enter the number of days the self-signed certificate is to be valid.
- Select **OK.**

The self-signed certificate is now listed under Personal Certificates as shown on Figure 8.



DB–Type: CMS key database file

File Name: /etc/sna/ibmcs.kdb

* rs600030

A personal certificate has its associated private key in the database.

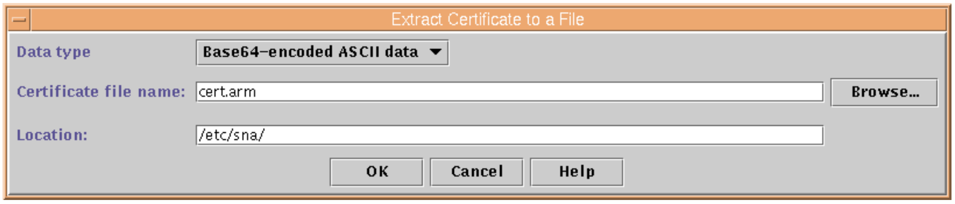
Figure 8. IBM key management - personal certificates

Now that we have created our self-signed certificate (rs600030), it must be distributed to our PCOMM TN3270 client in order for SSL to work. Therefore, our server certificate (which contains the server's public key and other items) must be placed in the client's key ring database. Before the certificate can be sent to the client, it must be extracted out of the CS/AIX server's database.

Select **Personal Certificates** from the drop-down list (already selected on Figure 8).

Highlight your self-signed certificate (rs600030) and select **Extract Certificate.**

The Extract Certificate to a File dialog appears as shown in Figure 9.


Extract Certificate to a File

Data type: Base64-encoded ASCII data

Certificate file name: cert.arm

Location: /etc/sna/

Figure 9. Extract Certificate to a File

In this window:

- Select **Base64-encoded ASCII** data or **Binary DER** as the data type.
- Enter the certificate file name. The file should have a file type of .arm (for example, ibmcs.arm) or .der (for example, ibmcs.der).
- Enter the location (absolute path name) of the certificate.
- Select **OK.**

If the extract was successfully completed, the file is now ready for sharing. Each client authorized to connect to the server using SSL must have this certificate. Consult the client documentation for instructions on storing the self-signed certificate as a CA root certificate in the key database. It is important when using FTP to transfer the certificate in binary mode.

2.4.3 Bringing up certificates using Personal Communications

IBM Personal Communications V4.3 provides three ways of managing certificates. The utilities are in the PCOMM Utilities folder:

- Certificate Wizard: this provides a simple, guided means of adding a certificate to the key database
- Certificate Management: This is a comprehensive tool that lets you create certificate requests, receive certificates, and create and extract self-signed certificates.
- Command-line: a program, PCSGSK, uses a customizable profile to manage certificates.

To begin, select **Start -> Programs -> IBM Personal Communications -> Utilities -> Certificate Management.**

The IBM Key Management window will appear as shown in Figure 10.

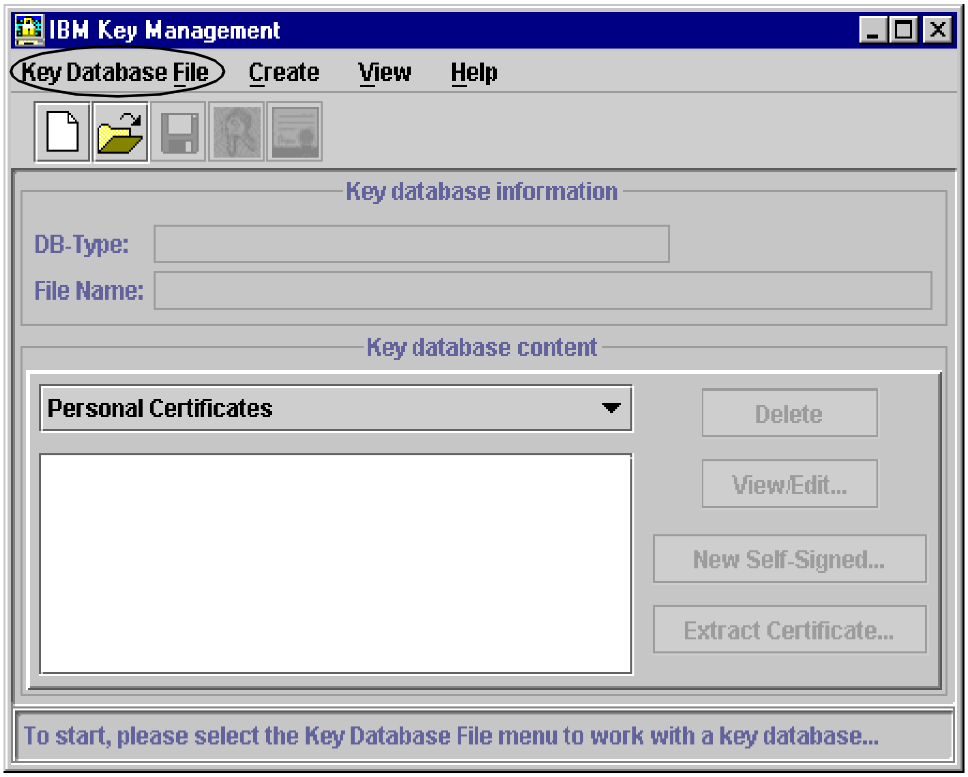
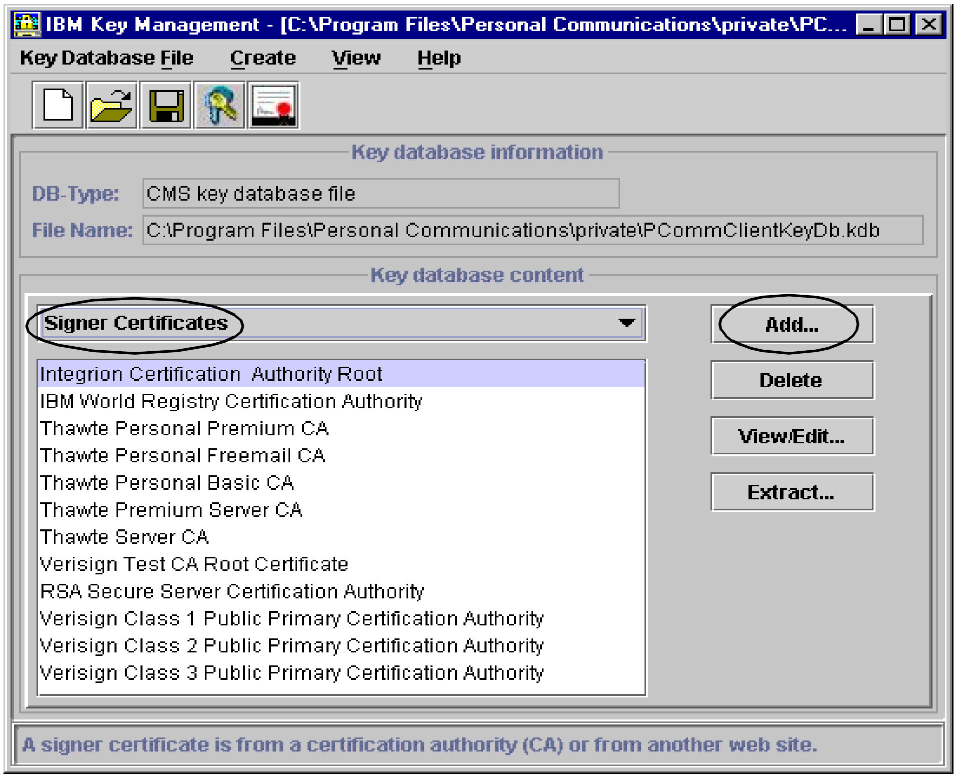


Figure 10. IBM Key Management

In this window:

- Select **Key Database File**.
- Select **Open**.
- Select **PCommClientKeyDb.kdb** file.
- Select **Open**.
- Type the password in the Password entry field and click **OK**.

  Note: PCommClientKeyDb.kdb is a certificate management database that is automatically created when Personal Communications is installed. It is password protected. The default password is `pcomm` and is generated when PCommClientKeyDb.kdb is initially created by Personal communications.
- Select **Signer Certificates** from the drop-down list box. A window similar to that shown in Figure 11 is displayed.



DB-Type: CMS key database file

File Name: C:\Program Files\Personal Communications\private\PCommClientKeyDb.kdb

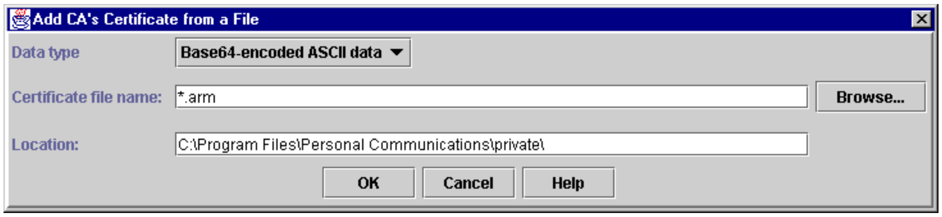
Integrion Certification Authority Root
IBM World Registry Certification Authority
Thawte Personal Premium CA
Thawte Personal Freemail CA
Thawte Personal Basic CA
Thawte Premium Server CA
Thawte Server CA
Verisign Test CA Root Certificate
RSA Secure Server Certification Authority
Verisign Class 1 Public Primary Certification Authority
Verisign Class 2 Public Primary Certification Authority
Verisign Class 3 Public Primary Certification Authority

A signer certificate is from a certification authority (CA) or from another web site.

Figure 11. IBM Key Management - Signer Certificates

- Select **Add**.

The Add CA’s Certificate from a File panel in Figure 12 appears.



Data type: Base64-encoded ASCII data

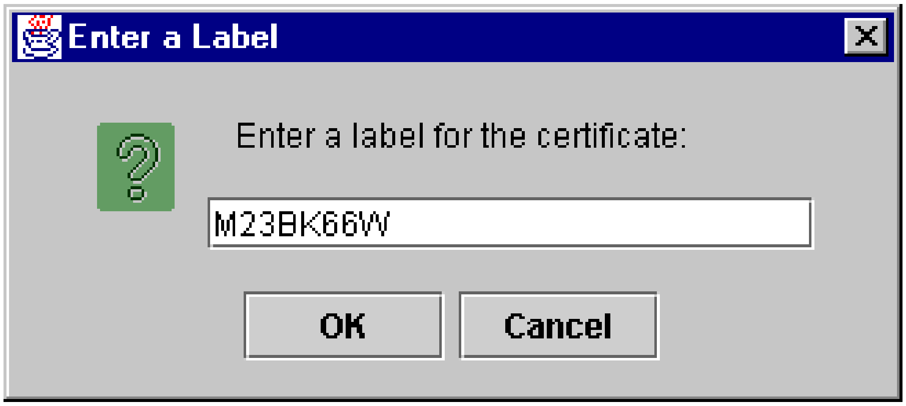
Certificate file name: *.arm

Location: C:\Program Files\Personal Communications\private\

Figure 12. Add CA/s Certificate from a Fle

Select the format dictated by your server administrator from the Data Type list box. Select the certificate file and click **OK**.

- Enter a label for the certificate and click **OK**.



Enter a label for the certificate:

M23BK66W

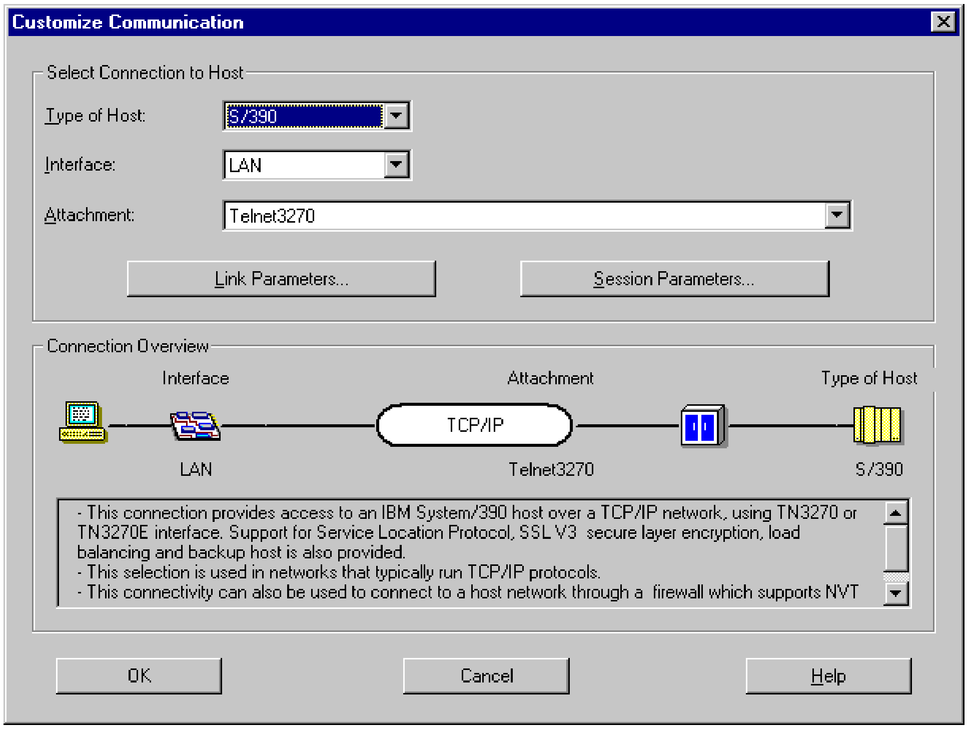
Figure 13. Enter a Label

- Select **View/Edit.**
- Activate the **Set the certificate as a trusted root**, and click **OK**.

2.4.4 Setting up TN3270 connections using PCOMM

When all of the above configuration steps have been completed, you may establish a secure TN3270 session to a host from your client via an SSL-enabled CS/AIX TN3270 server.

- Select **Start -> Programs -> IBM Personal Communications -> Start or Configure Sessions**.
- When the Welcome to the IBM Personal Communications WorkStation Window appears, then select **OK**.
- The Customize Communication window as shown in Figure 14 is displayed.

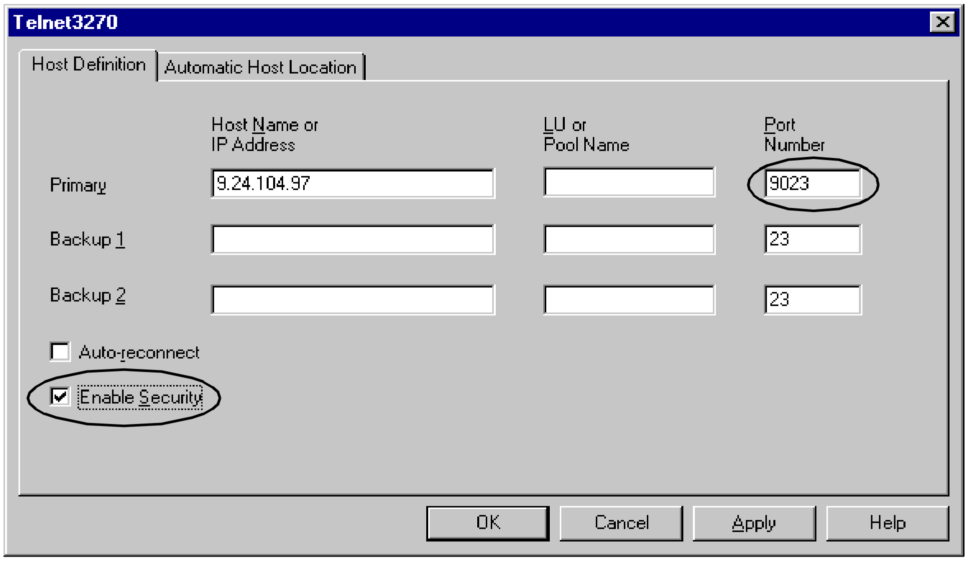


- This connection provides access to an IBM System/390 host over a TCP/IP network, using TN3270 or TN3270E interface. Support for Service Location Protocol, SSL V3 secure layer encryption, load balancing and backup host is also provided.
- This selection is used in networks that typically run TCP/IP protocols.
- This connectivity can also be used to connect to a host network through a firewall which supports NVT

Figure 14. Customize Communication

- Choose the appropriate type of host, interface and attachment values for the desired Telnet host.
- Select **Link Parameters**.

The Telnet3270 window appears as shown in Figure 15.



	Host Name or IP Address	LU or Pool Name	Port Number
Primary	9.24.104.97		9023
Backup 1			23
Backup 2			23

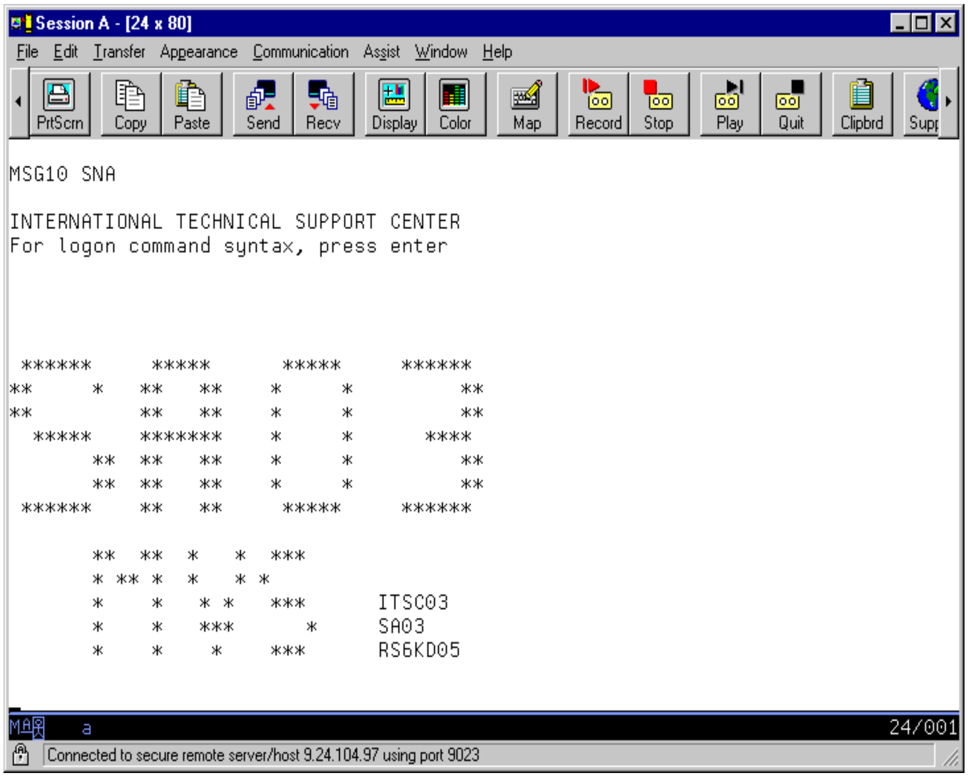
☐ Auto-reconnect

☑ Enable Security

Figure 15. Telnet3270

- Specify the Host Name or IP Address and LU parameters in the Primary field.
- Specify the Port number for Primary. The default Telnet port value of 23 is displayed. However, this must be changed to match the port number defined in the CS/AIX Telnet server.
- Check **Enable Security**.
- Select **Apply**.
- Select **OK**.
- Select **OK**.

TN3270 secure connection is shown in Figure 16.



```
MSG10 SNA

INTERNATIONAL TECHNICAL SUPPORT CENTER
For logon command syntax, press enter




 ******     *****      *****     ******
**     *   **   **    *     *         **
**         **   **    *     *         **
  *****    *******    *     *      ****
       **  **   **    *     *         **
       **  **   **    *     *         **
 ******    **   **     *****     ******

       **  **  *   *  ***
       * ** *  *   * *
       *    *   * *   ***      ITSC03
       *    *   ***      *     SA03
       *    *    *    ***      RS6KD05
```

```
MA      a                                                   24/001
Connected to secure remote server/host 9.24.104.97 using port 9023
```

Figure 16. TN3270 session

When it has connected successfully, you will see a normal session window except that the status bar has a locked padlock in the bottom left-hand corner which tells you that it is connected to a secure server.

Chapter 3. TN Redirector

This chapter describes the functionality of the TN Redirector and how it is configured, and provides two example scenarios that illustrate the use of TN Redirector in its simplest form, without SSL (Secure Sockets Layer).

3.1 Overview

The function of TN Redirector is to allow TN3270, TN3270E, TN5250 and VT programs, collectively known as Telnet clients, to access a host using an intermediate CS/AIX node, instead of accessing the host directly. The clients connect to the CS/AIX node that implements the TN Redirector component using TCP/IP. The TN Redirector then establishes a separate TCP/IP connection to the host.

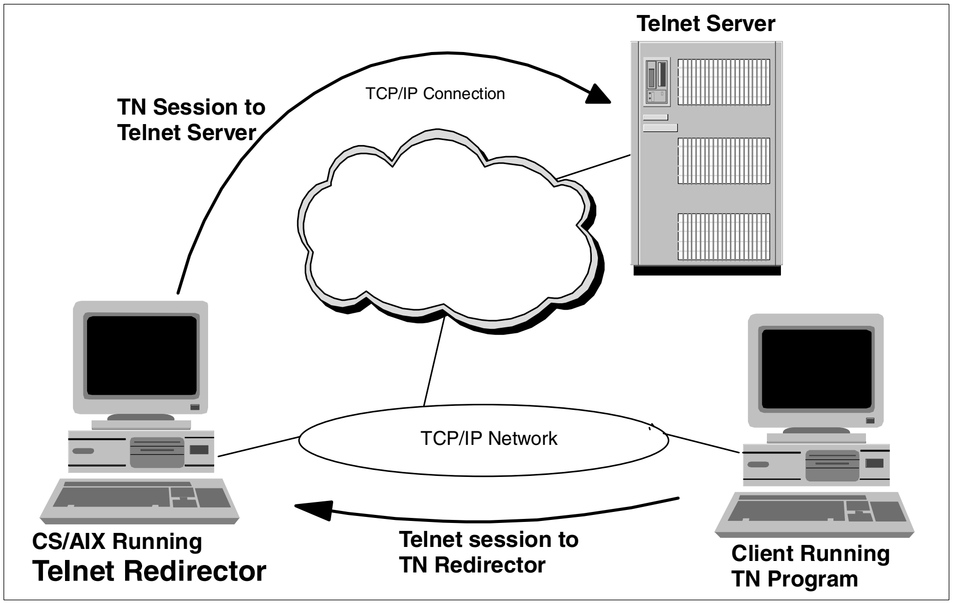


Figure 17. TN Redirector

The TN3270 server component introduced in Communications Server for AIX, Version 5 is still available. It enables communication between TN3270 clients and an SNA host.

There are two main benefits associated with the use of TN Redirector:

1. Having a large number of clients connecting directly to the host system introduces a potential security risk. By using a TN Redirector that passes connections to the host, you can hide the address of the host from the client users.
2. It provides SSL (Secure Sockets Layer) support.

SSL is explained in Chapter 2, “Secure Sockets Layer support” on page 9. It enables encryption and authentication for client and host TCP/IP connections.

To use SSL the GSK Runtime Toolkit component of CS/AIX must be installed and AIX must be at Level 4.3.2-ML2 or above. For software requirements see *IBM Communications Server for AIX, Version 6, Quick Beginnings,* GC31-8583.

3.2 Implementation

TN Redirector support in CS/AIX requires AIX V4.3.2-ML2 or later.

The steps to configure the TN Redirector are:

1. Configure the node
2. Start the node
3. Configure TN Redirector access records

The first two steps are covered in *IBM Communications Server for AIX, Version 6, Quick Beginnings,* GC31-8583.

TN Redirector access records identify which Telnet clients are permitted to access the TN Redirector, the TCP/IP port that the client uses to connect to CS/AIX, the TCP/IP port that CS/AIX uses to connect to the host, the TCP/IP address of the host, and the SSL security settings.

You must create an access record for every TN server/port to which you want an emulator to connect.

Multiple TN Redirector records may be defined to support access to multiple hosts using different ports. They can be implemented using different security requirements for different clients and hosts. As shown in Figure 18 on page 35, Secure Sockets Layer (SSL) can be implemented between the client and the Telnet Redirector and/or between the TN Redirector and the SSL-capable Telnet server such as CS for OS/390, AS/400, or CS/NT.

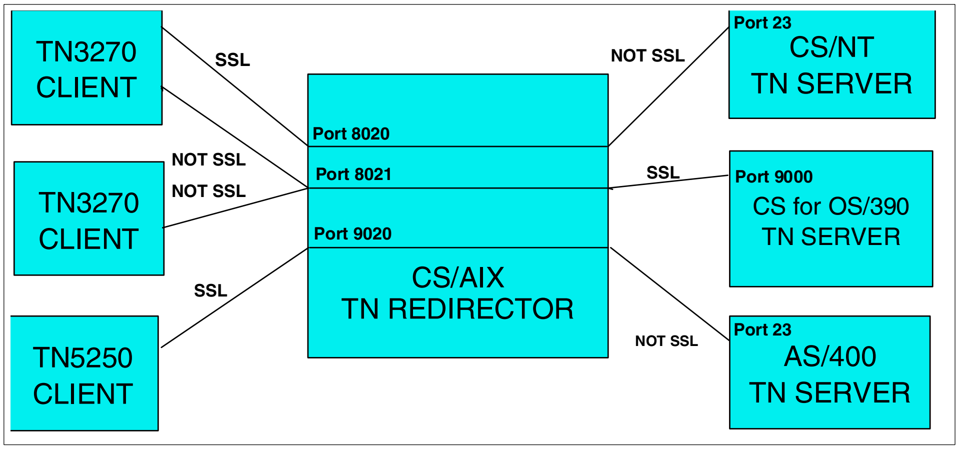


Figure 18. Different ways of Implementing SSL with TN Redirector

3.2.1 Configuring CS/AIX TN Redirector access records

To define a TN Redirector access record perform the following steps:

1. Start the Motif administration program by keying in `xsnaadmin` from the command line. The node window will appear.

2. From the node window, click **Services -> TN Server -> TN Server...**

   The following panel will appear:

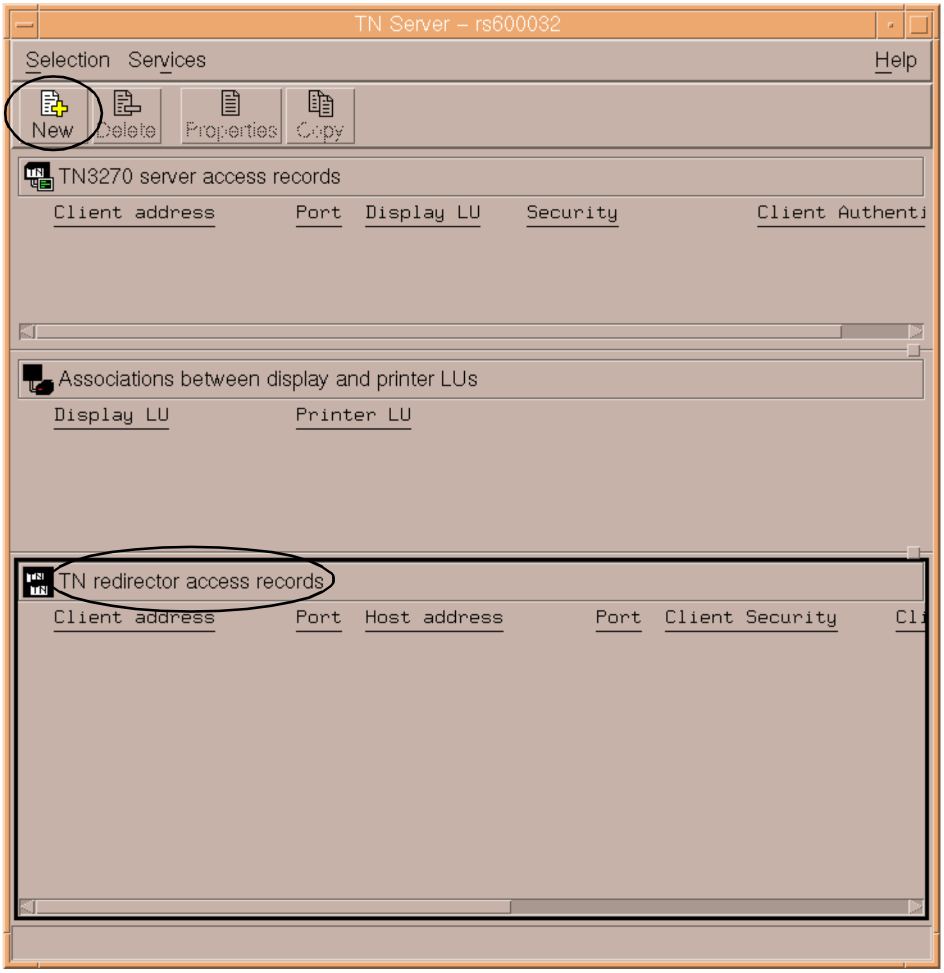
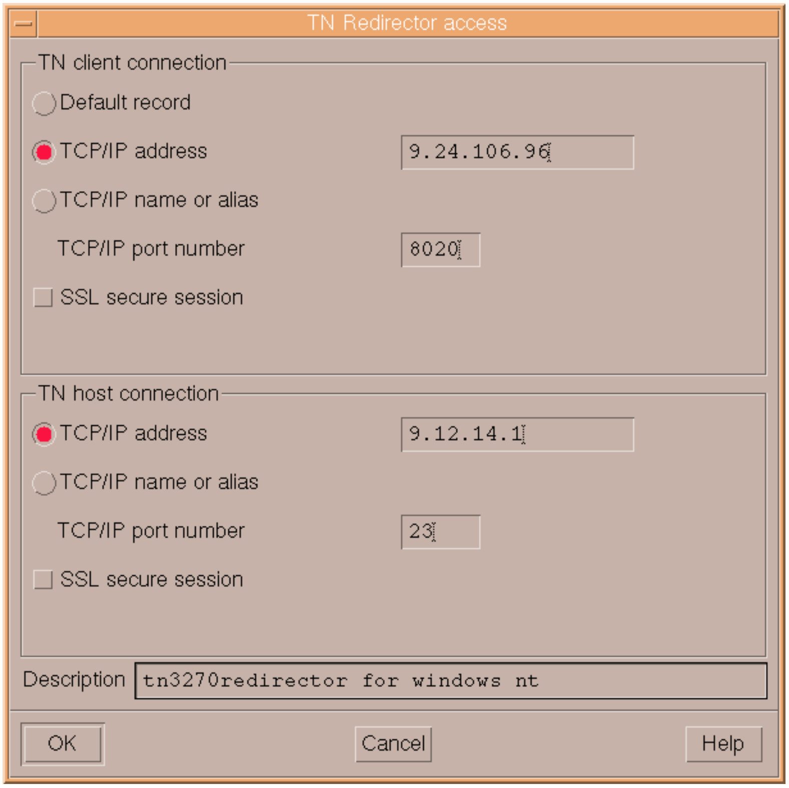


Figure 19. TN server window

3. Select the pane that contains TN Redirector access records and click on the **New** button.

CS/AIX displays the TN Redirector Access dialog window shown in Figure 20.

4. Enter appropriate values in the TN Redirector access configuration dialog and click the **OK** button. The record appears in the TN Redirector pane of the TN Server window.



TN client connection

○ Default record

● TCP/IP address 9.24.106.96

○ TCP/IP name or alias

TCP/IP port number 8020

□ SSL secure session

TN host connection

● TCP/IP address 9.12.14.1

○ TCP/IP name or alias

TCP/IP port number 23

□ SSL secure session

Description tn3270redirector for windows nt

Figure 20. TN Redirector access dialog window

TN Redirector access records consist of two groups of parameters:

1. **TN client connection**

   These fields identify the TN client to which the access record applies.

2. **TN host connection**

   These fields identify the host computer to which the Redirector connects.

3.2.1.1 TN client connection parameters

Default record Select this option to allow access by any Telnet client. All clients will use the same host access parameters.

If only certain clients are permitted:

Telnet client address Enter the TCP/IP address of the client in the standard TCP/IP dotted decimal address format.

TCP/IP name or alias If you know the TCP/IP name of the TN client, you can select this option and enter the name.

TCP/IP port number The TCP/IP port number to which the TN client connects on the TN Redirector.

Note: Use of the port number 23 is likely to clash with the AIX Telnet service. Examine the /etc/services file and use the `netstat -an` command to choose a port number that is not in use by AIX. Specify this port number when you start the TN client.

SSL secure session Select this option if this session is to use SSL to access the TN Redirector. Both the TN client and the TN Redirector access record must be configured to use SSL.

Perform client authentication The client must send a valid certificate identifying it as a valid client authorized to use the TN Redirector. As well as checking that the certificate is valid, the TN Redirector may also need to check the certificate against a certificate revocation list on an external LDAP server, to ensure that the user's authorization has not been revoked. To specify how to access this server, from the TN Server window click **Services -> SSL Client Revocation -> Check Certificate Revocation List**.

Security level Select this option to specify the security level that clients must use in order to establish a connection to the TN Redirector. Possible values are:

- Authenticate Only (only TN Redirector authentication, no encryption),
- 40 bit minimum - at least 40 bits
- 56 bit minimum - at least 56 bits
- 128 bit minimum - at least 128 bits
- 168 bit minimum - at least 168 bits
- Authenticate minimum - any of the above

The session will use the highest security level that both client and TN Redirector can support. If the client cannot support the requested level of security or higher the session will not be started.

Note: Using encryption requires additional software to be installed with CS/AIX. See *IBM Communications Server for AIX, Version 6, Quick Beginnings,* GC31-8583, for more information. Depending on your location, you may not be able to use all the encryption levels listed because the software required to support them is not available in your country.

3.2.1.2 TN host connection parameters

TCP/IP address of host Enter the TCP/IP address of the host in the standard TCP/IP dotted decimal address format.

TCP/IP name or alias If you know the TCP/IP name of the host, you can select this option and enter the name.

TCP/IP port number The TCP/IP port number that the TN Redirector uses to access the host. Port 23 is used by most CS for OS/390, AS/400, and VT hosts for Telnet connections.

SSL secure session Select this option to indicate that the TN Redirector uses SSL to access the host. This option is available only if the host supports SSL.

Security level This option allows you to specify the security level that the host must use in order to establish a connection to the TN Redirector. Possible values are:

- Authenticate only (only server authentication),
- 40 bit minimum - at least 40 bits
- 56 bit minimum - at least 56 bits
- 128 bit minimum - at least 128 bits
- 168 bit minimum - at least 168 bits
- Authenticate minimum - any of the above

The session will use the highest security level that both host and TN Redirector can support. If the host cannot support the requested level of security or higher the session will not be started.

Note: Using encryption requires additional software to be installed with CS/AIX. See *IBM Communications Server for AIX, Version 6, Quick Beginnings,* GC31-8583 for more information. Depending on your location, you may not be able to use all the encryption levels listed because the software required to support them is not available in your country.

3.3 Scenario

For this section we will use the following equipment:

- An RS/6000 running AIX Version 4.3.3 with the latest maintenance level, and IBM Communications Server for AIX, Version 6
- A PC running Windows NT and IBM Personal Communications for Windows NT, Version 4.3 (PCOMM)
- A host running CS for OS/390

- An AS/400 host

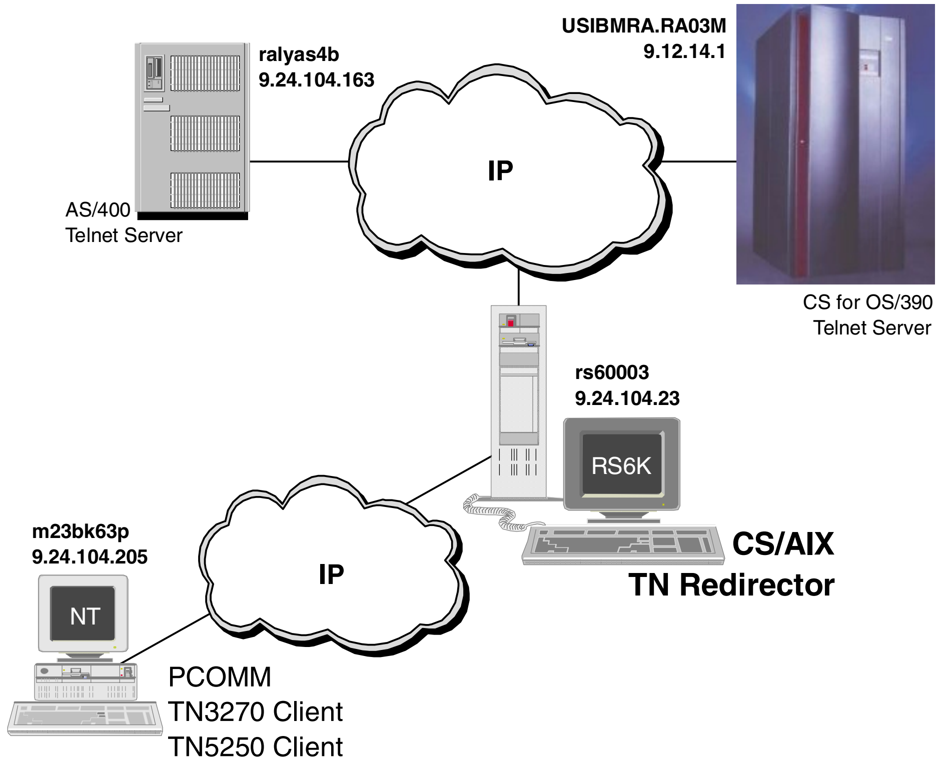


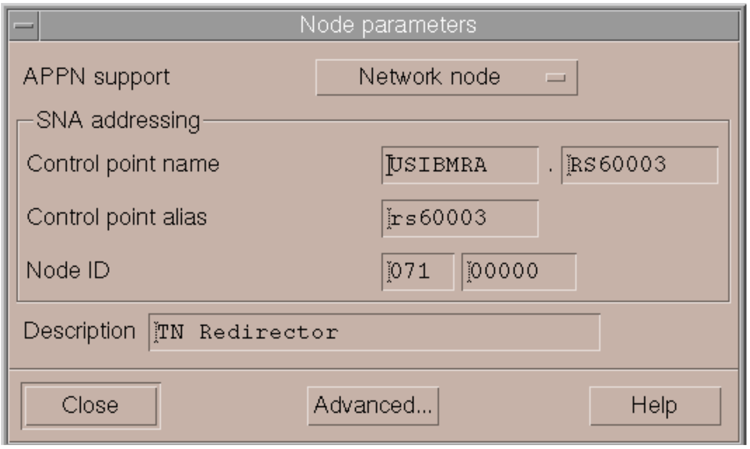
Figure 21. Test scenario

The steps to test the scenario in Figure 21 were as follows:

On the RS/6000:

1. The node was configured as a network node.

   Note: The TN Redirector can be configured in any node type. We chose a network node for our configuration.


Node parameters

APPN support: Network node

SNA addressing

Control point name: USIBMRA . RS60003

Control point alias: rs60003

Node ID: 071 00000

Description: TN Redirector

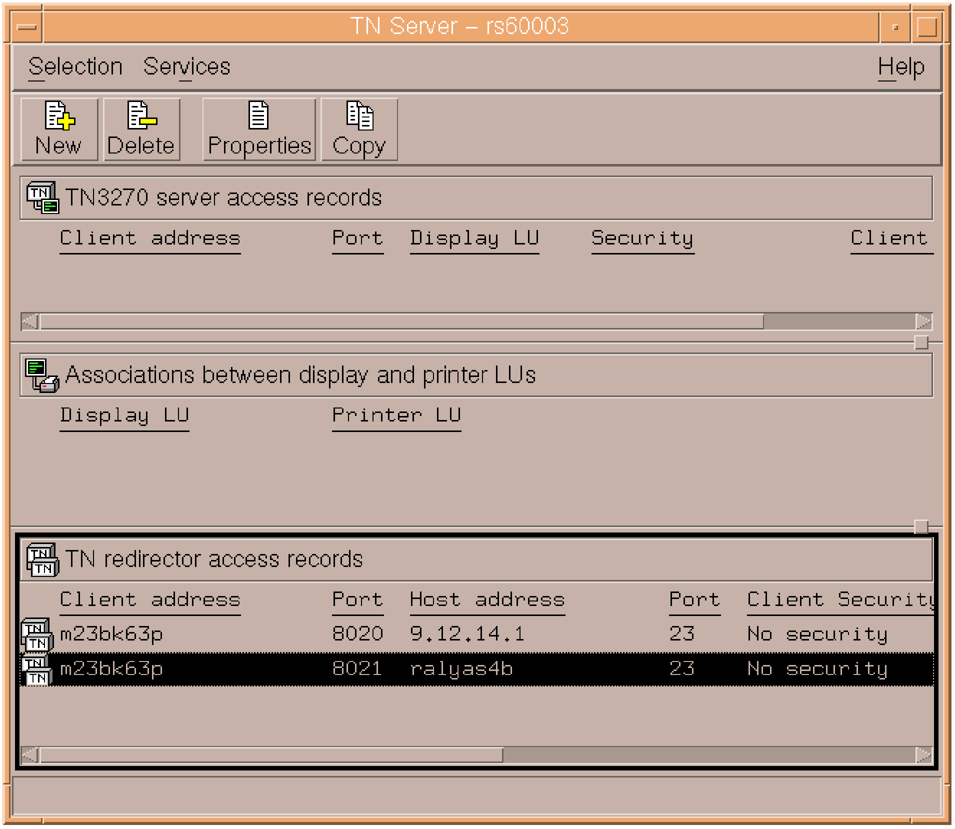
Figure 22. Node configuration

The define_node section of the /etc/sna/sna_node.cfg file looks like the following:

```
[define_node]
cp_alias = rs60003
description = TN Redirector
fqcp_name = USIBMRA.RS60003
node_type = NETWORK_NODE
mode_to_cos_map_supp = YES
mds_supported = YES
node_id = <07100000>
max_locates = 1500
dir_cache_size = 255
max_dir_entries = 0
locate_timeout = 0
reg_with_nn = YES
reg_with_cds = YES
mds_send_alert_q_size = 100
cos_cache_size = 24
tree_cache_size = 40
tree_cache_use_limit = 40
max_tdm_nodes = 0
max_tdm_tgs = 0
max_isr_sessions = 1000
isr_sessions_upper_threshold = 900
isr_sessions_lower_threshold = 800
isr_max_ru_size = 16384
isr_rcv_pac_window = 8
store_endpt_rscvs = NO
```

```
store_isr_rscvs = NO
store_dlur_rscvs = NO
cos_table_version = VERSION_0_COS_TABLES
send_term_self = NO
disable_branch_awareness = NO
cplu_syncpt_support = NO
cplu_attributes = NONE
dlur_support = YES
pu_conc_support = YES
nn_rar = 128
max_ls_exception_events = 0
ms_support = NORMAL
queue_nmvts = YES
ptf_flags = NONE
```

2. The node was started.
3. Two TN Redirector access records were defined. One access record was configured for connection to the CS for OS/390 host and the other for access to the AS/400. The configuration panel is shown in Figure 23 on page 43.


TN Server – rs60003
Selection
Services
Help
New
Delete
Properties
Copy
TN3270 server access records
Associations between display and printer LUs
TN redirector access records

TN3270 server access records

Client address	Port	Display LU	Security	Client

Associations between display and printer LUs

Display LU	Printer LU

TN redirector access records

Client address	Port	Host address	Port	Client Security
m23bk63p	8020	9.12.14.1	23	No security
m23bk63p	8021	ralyas4b	23	No security

Figure 23. TN Redirector access records

Note: TCP/IP names can be used instead of TCP/IP addresses if name resolvers are in use. The TCP/IP port numbers to which the TN client connects to the TN Redirector must be different to access different hosts.

The access records definitions in the /etc/sna/sna_node.cfg file look like:

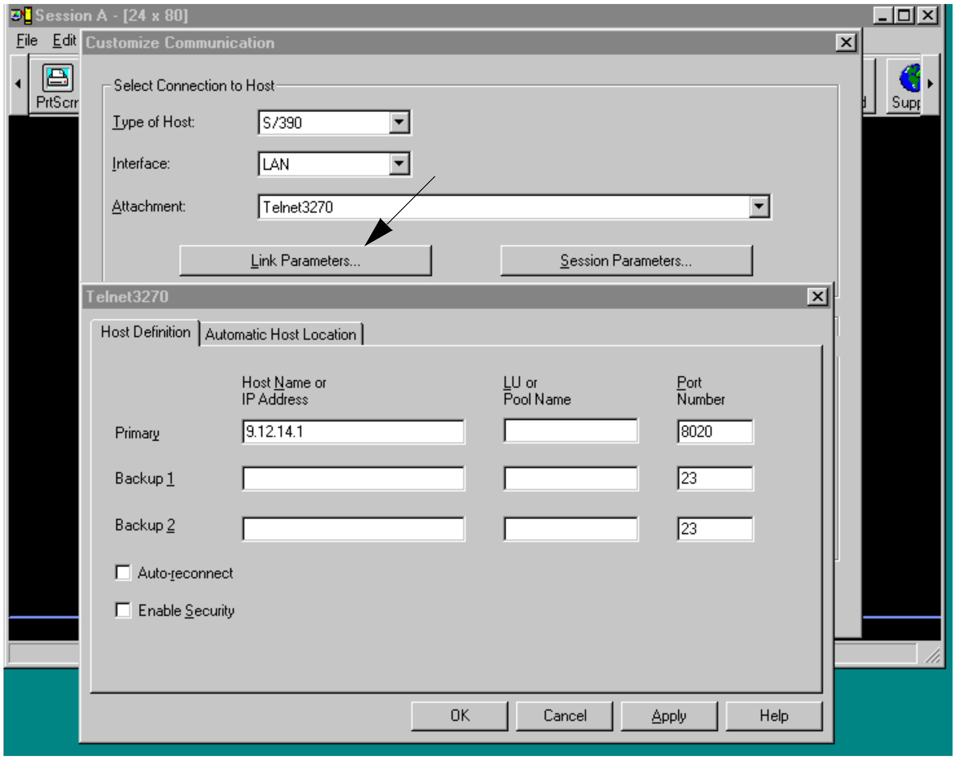
```
 [define_tn_redirect]
default_record = NO
address_format = FULLY_QUALIFIED_NAME
client_address = m23bk63p
client_port = 8020
host_address_format = IP_ADDRESS
host_address = 9.12.14.1
host_port = 23
cli_ssl_enabled = NO
cli_conn_security_level = SSL_AUTHENTICATE_MIN
host_ssl_enabled = NO
```

```
serv_conn_security_level = SSL_AUTHENTICATE_MIN
description = TN3270 session
cli_conn_cert_key_label = ""
serv_conn_cert_key_label = ""

[define_tn_redirect]
default_record = NO
address_format = FULLY_QUALIFIED_NAME
client_address = m23bk63p
client_port = 8021
host_address_format = FULLY_QUALIFIED_NAME
host_address = ralyas4b
host_port = 23
cli_ssl_enabled = NO
cli_conn_security_level = SSL_AUTHENTICATE_MIN
host_ssl_enabled = NO
serv_conn_security_level = SSL_AUTHENTICATE_MIN
description = TN5250 session
cli_conn_cert_key_label = ""
serv_conn_cert_key_label = ""
```

On the PC:

4. Using PCOMM (IBM Personal Communications software for Windows NT) we configured two Telnet sessions, one to the host CS for OS/390 and the other to the AS/400. From the session window click **Communication** -> **Configure** -> **Link Parameters.**

In both cases, Figure 24 on page 45 and Figure 25 on page 46, the Link Parameters consist of the hostname or IP address of the TN Redirector and the port number to which the Telnet client connects to the TN Redirector.



Select Connection to Host

Type of Host: S/390

Interface: LAN

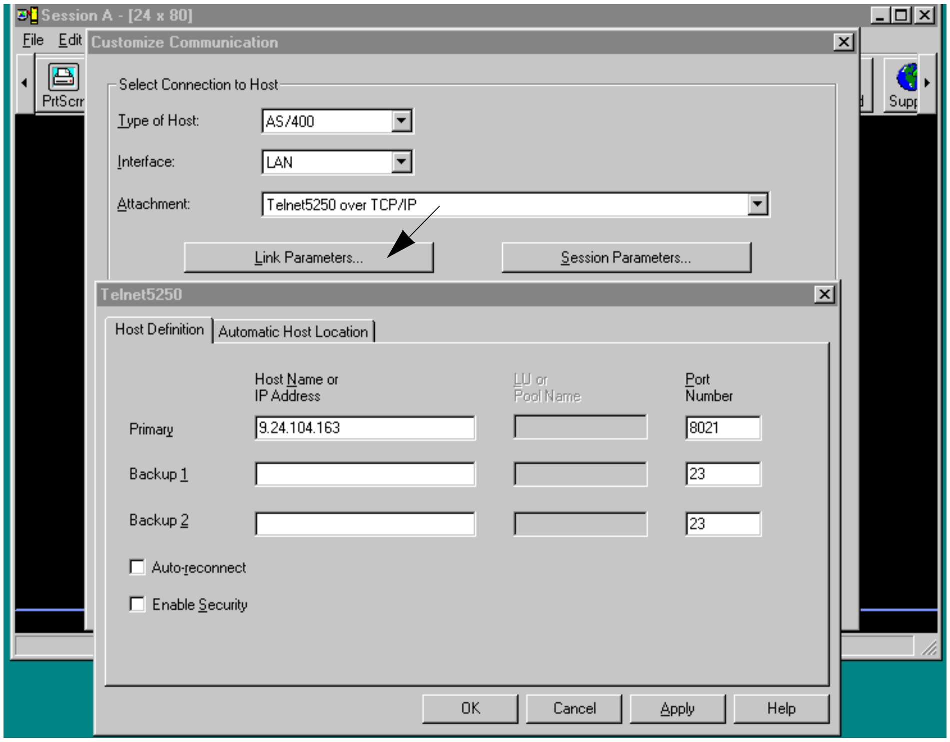
Attachment: Telnet3270

	Host Name or IP Address	LU or Pool Name	Port Number
Primary	9.12.14.1		8020
Backup 1			23
Backup 2			23

□ Auto-reconnect

□ Enable Security

Figure 24. PCOMM Telnet 3270 session



Type of Host: AS/400

Interface: LAN

Attachment: Telnet5250 over TCP/IP

	Host Name or IP Address	LU or Pool Name	Port Number
Primary	9.24.104.163		8021
Backup 1			23
Backup 2			23

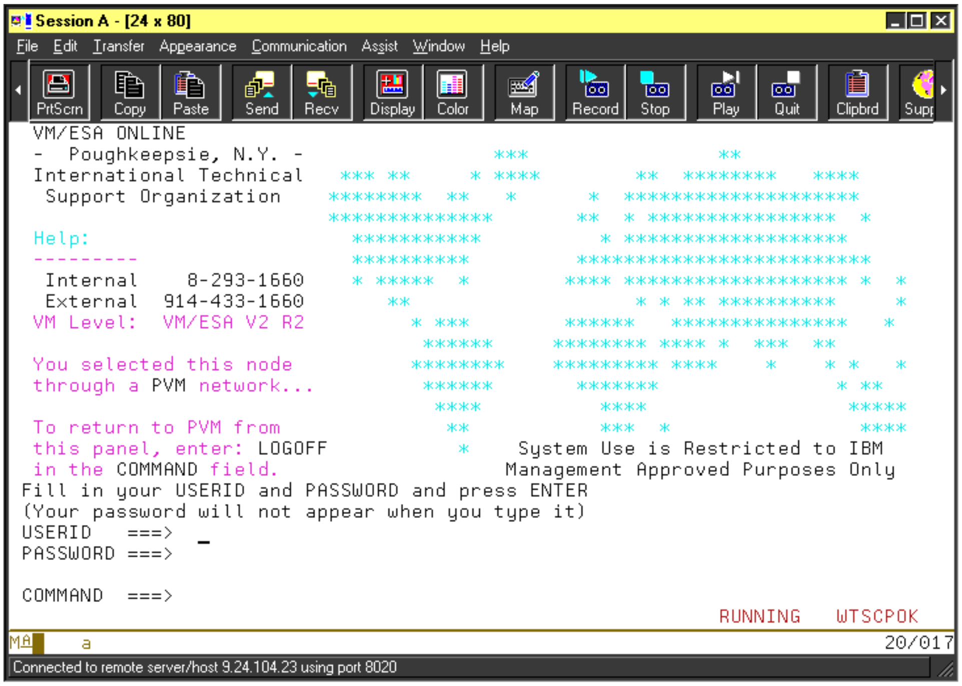
□ Auto-reconnect

□ Enable Security

Figure 25. PCOMM TN5250 session

5. After clicking **OK** the Telnet client connects to the TN Redirector using the specified port. The TN Redirector connects the client to the Telnet servers, CS for OS/390 or AS/400, transparently, and a session can then be started.

   The only IP address known to the client is the address of the TN Redirector.



```
 VM/ESA ONLINE
 -  Poughkeepsie, N.Y. -                ***                **
 International Technical   *** **     * ****        **  *********  ****
  Support Organization    ********* **   *      *  ********************
                          **************       **  * ****************  *
 Help:                      ***********          * *******************
 ----------                 **********         *************************
  Internal    8-293-1660    * *****  *        **** ******************* *  *
  External  914-433-1660       **                   * * ** **********     *
 VM Level:  VM/ESA V2 R2         * ***        ******   ***************   *
                                  ******     ******** **** *  ***  **
 You selected this node          ********    ********* ****    *    * *   *
 through a PVM network...         ******       *******               * **
                                   ****          ****                 *****
 To return to PVM from              **           ***  *                ****
 this panel, enter: LOGOFF           *    System Use is Restricted to IBM
 in the COMMAND field.                   Management Approved Purposes Only
Fill in your USERID and PASSWORD and press ENTER
(Your password will not appear when you type it)
USERID   ===>
PASSWORD ===>

COMMAND  ===>
                                                           RUNNING   WTSCPOK
MA     a                                                              20/017
```

Connected to remote server/host 9.24.104.23 using port 8020

Figure 26. TN session to OS/390 through TN Redirector

TN Redirector is also documented in *IBM Communications Server for AIX, Version 6, Administration Guide,* SC31-8586, and *IBM Communications Server for AIX, Version 6, Quick Beginnings,* GC31-8583.

3.4 TN Redirector and SSL

As mentioned previously, the TN Redirector can use SSL support for authentication and encryption across TCP/IP networks. It allows the use of SSL security checking where necessary: between the Telnet client and the TN Redirector and/or the TN Redirector and the host.

For example:

- If Telnet clients are connecting to CS/AIX over a TCP/IP LAN where security checking is not required, but are redirected to a remote host that requires secure connections, you can use SSL over the TCP/IP connection between CS/AIX and the host. This means that security is checked once for all clients, and individual clients do not have to provide security information. See Figure 27.

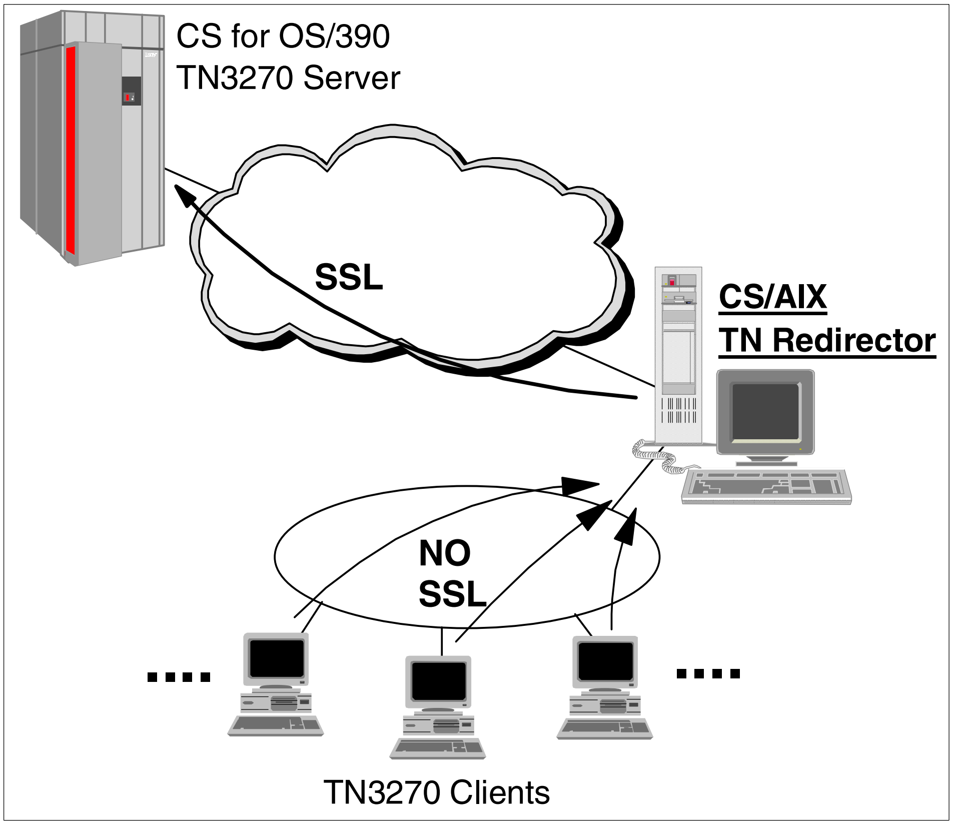


Figure 27. SSL between the TN Redirector and host

- If CS/AIX is installed at the same site as the host, and Telnet clients are connecting in from external sites, you can use SSL over the client connections to CS/AIX without having to install SSL software on the host. After SSL security checking is done on the AIX system, TN Redirector completes the connection to the host. This moves the CPU cost of encryption to the AIX box instead of the host system. See Figure 28.

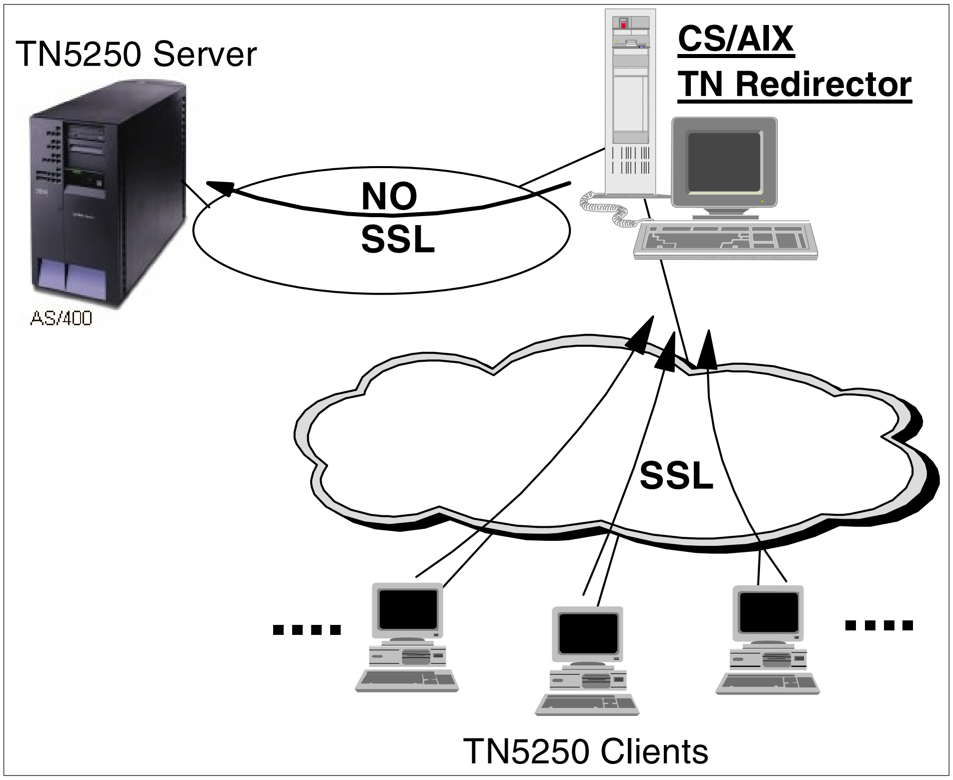


Figure 28. SSL between clients and the TN Redirector

Chapter 4. Service Location Protocol (SLP)

Service Location Protocol (SLP) specifies a method to provide dynamic directory services specifically for finding servers by attributes rather than by name or address. In so doing, SLP provides a standard method of allocating service requests among a set of servers with some level of workload balancing. SLP uses multicast services to locate SLP components and unicast services to communicate between components.

IBM Communication Server for AIX, V6.0 supports SLP providing service location and server load balancing for CS/AIX TN3270 servers. In this chapter, we will discuss the new function of the IBM CS/AIX Service Location Protocol and how to implement it in an Internet network environment.

4.1 Overview

As businesses expand the scope of their network resources by connecting corporate LANs and WANs with TCP/IP-based intranets, TN3270E servers play an increasingly important role in providing mainframe host connectivity to TCP/IP-based clients. Service Location Protocol (SLP) allows corporate in-house “intranet” environments using Internet standards, in conjunction with TN3270E servers and emulators, to provide fast, reliable and cost-effective load-balanced host sessions for end users.

4.1.1 Service location protocol

Service Location Protocol is a new Internet Engineering Task Force (IETF) proposed standard protocol that was designed to simplify the discovery and use of network resources. In a corporate intranet, users need to access services and resources on the network. Often, it is not clear to the users what useful services are available to them. These resources could include TN3270E servers, Web servers, printers, fax machines, file systems, databases, and any other future services that might become available. IBM Communications Server for AIX, Version 6 supports SLP in conjunction with TN3270E servers and clients.

SLP is defined in Request for Comments (RFC) 2165. It is a service-discovery method for TCP/IP-based communications, providing a simple and lightweight protocol for automatic advertisement and maintenance of intranet services and minimizing the use of broadcast and multicast in the network. SLP uses multicast, which targets a group of nodes, unlike broadcast, which targets all nodes. The benefit of multicast is that it sends one packet that all members of the group receive, but that only the intended recipients read. A multicast packet is not isolated to a local segment; routes can forward it to whatever subnets are attached.

Without SLP, users find services by using the name of a network host (a human-readable text string) that is an alias for a network address. Service Location Protocol eliminates the need for a user to know the name of a network host supporting a service. Service Location Protocol allows the user to bind a service description to the network address of the service.

SLP provides a dynamic configuration mechanism for applications in local area networks. It is not a global resolution system for the entire Internet; rather it is intended to serve enterprise networks with shared services. Applications are modeled as clients that need to find servers attached to the enterprise network at a possibly distant location. For cases where there are many different clients and/or services available, the protocol is adapted to make use of nearby directory agents that offer a centralized repository for advertised services.

4.1.2 SLP terminology

SLP defines three types of agents as shown in Figure 29.

- **User agent (UA):**

  Supports service query functions. It acquires/requests service information for user applications. The user agent retrieves service information from the service agent or directory agents.

- **Service agent (SA):**

  Service registration and service advertisement.

- **Directory agent (DA)**:

  Collects service information from service agents to provide a repository of service information in order to centralize it for efficient access by user agents. There can only be one DA present per given host.

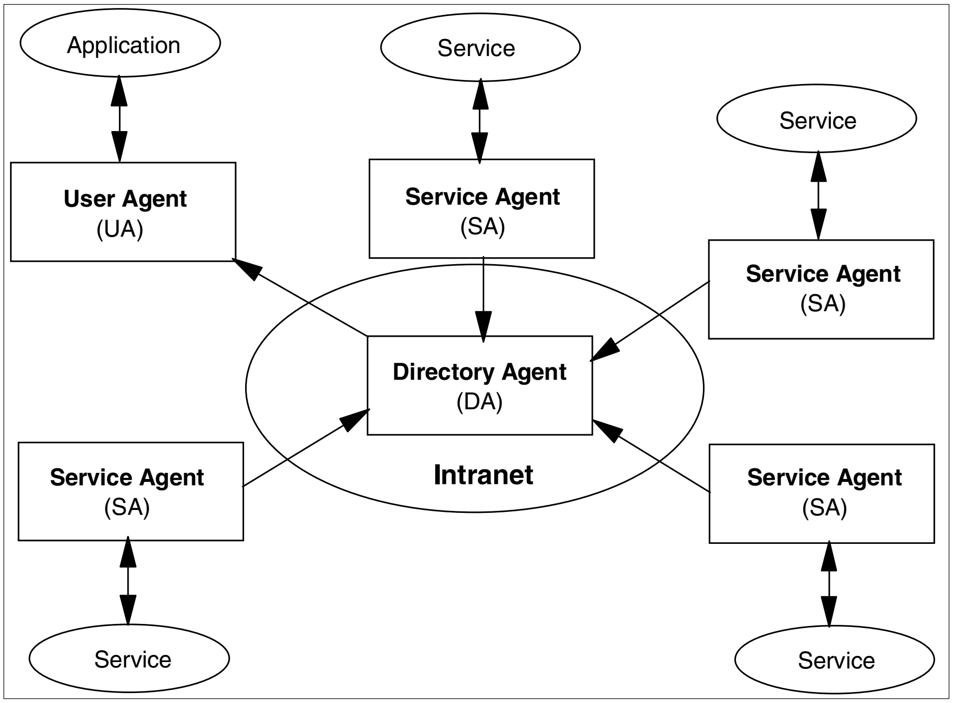


Figure 29. SLP agents

IBM Communications Server for AIX, Version 6 performs the role of a service agent advertising TN3270 server services. IBM Host-On-Demand, IBM Personal Communications and other SLP-enabled TN3270 clients perform the role of user agents. CS/AIX does not provide an SLP directory agent function.

Services are described by the configuration of attributes associated with a type of service. For instance, a CS/AIX configuration providing TN3270 gateway access to an SNA network via the TN3270 protocol would define a service called TN3270 with a set of associated attributes. A TN3270 client would select the appropriate TN3270 attributes group that it needs in a request message to a directory agent, or directly to service agents, and await a reply. CS/AIX V6 includes the SLP service agent. In small installations, there may be no directory agents, and the request message from the TN3270 client would be sent (multicast) directly to the service agents.

A user agent can select an appropriate service by specifying the attributes that it needs in a service request. When service replies are returned (assuming multiple service agents can satisfy the request), they contain a

Uniform Resource Locator (URL) pointing to the service desired, and other information, such as server load, needed by the user agent.

Following is additional terminology used when discussing SLP:

- **Service**

  The service is a process or system (such as TN3270 server, Web server, and so on) providing a function or service to the network. The service itself is accessed using a communication mechanism external to the Service Location Protocol.

- **Service Information**

  A collection of attributes and configuration information associated with a single service. The service agents advertise service information for a collection of service instances.

- **Site Network**

  All the hosts accessible within the agent's multicast radius, which defaults to a value appropriate for reaching all hosts within a site. If the site does not support multicast, the agent's site network is restricted to a single subnet.

- **Scope**

  A collection of services that make up a logical group.

4.1.3 SLP load balancing

Load balancing using SLP dynamically balances user agent sessions by distributing them to the service agent (which supports the desired service) with the smallest load. TN3270 clients that support load balancing have the ability to query participating SLP TN3270E servers and connect to the least loaded service agent (for example, a CS/AIX TN3270 server gateway).

The SLP load balancing weight factor gives the administrator the ability to modify or weight the load balancing measurement for each server. The factor can be different for each server. The measurement can take into account numbers of active sessions, memory constraints and CPU constraints on each server. The weight factor gives the administrator an element of control in this calculation. The weighting factor is useful because:

- In some cases, there are other factors that may have an effect on server load that are not taken into account by the server load algorithm, for example, if the server is not dedicated to SNA gateway traffic only.
- If the server providing TN3270 services must coexist in a network with other TN server implementations using SLP for load balancing, the load

factor can be adjusted to compensate for differences between server machines.

The weight factor allows the administrator to bias the load measurement on that server either away from or towards selecting the server. The factor can be turned on or off as well, causing it to be ignored in load calculations.

As shown in Figure 30, when a TN3270 client requests a session to the host, those servers that support TN3270 services respond with their current load. The least loaded TN3270 server will be chosen by the client to make connection to the host.

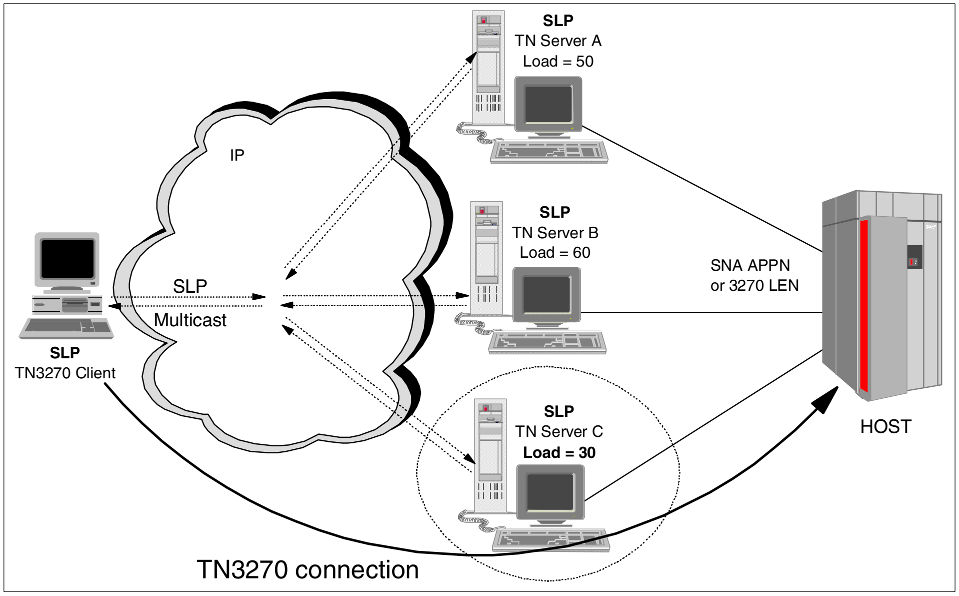


Figure 30. SLP load balancing

Note that both the TN3270 client and TN3270 server must support SLP and the load balancing process.

4.1.4 SLP scope

SLP can reduce overall network traffic by using *scopes* to manage client service requests. A scope is essentially a grouping method used to organize servers into named groups or pools. This is ideal for large networks with a number of gateways or servers.

Scope can be looked at in two different ways:

1. Scope is a *mechanism* in Service Location Protocol that provides the capability to organize a site network along administrative lines. A set of services can be assigned to a given department of an organization, to a certain geographical area, or for a certain purpose.
2. Scope is a *parameter* used to control and manage access by workstations (user agents) to TN3270 servers (service agents) in a network.

Scope values are defined by a network administrator, and may represent departments, regions, or organizations. If desired, different scopes can be assigned for different services provided on the server.

For an example, see Figure 31.

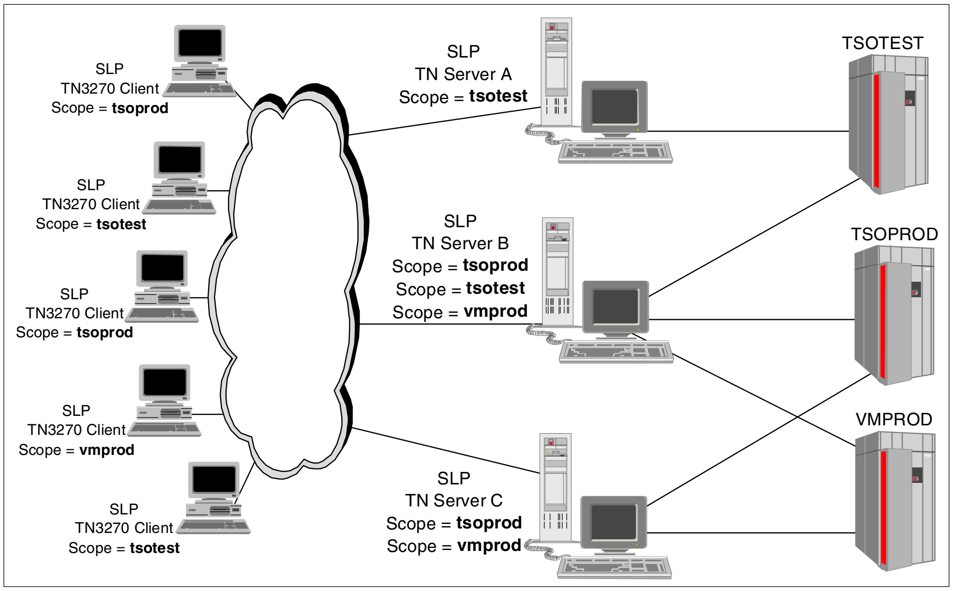


Figure 31. SLP scope example

In the example network shown in Figure 31, CS/AIX Server A has only one scope defined (TSOTEST) and is attached to only one host. However, Server B is attached to three different hosts and advertises three different scopes (TSOPROD, TSOTEST and VMPROD). Server C advertises scopes TSOPROD and VMPROD.

In this configuration, clients using scope TSOPROD will balance between CS/AIX Servers B and C, while clients using other scopes will balance between the servers that can provide that particular class of LU. In addition, specification of scope on the client platform supports the use of wildcards.

For example, a client that specifies a scope of TSO* can select between servers that advertise scopes of TSOTEST and TSOPROD.

4.2 SLP review

The basic operation in Service Location Protocol is that a client attempts to discover the location of a service. In smaller installations, each service will be configured to respond individually to each client. In larger installations, services will register their services with one or more directory agents, and clients will contact the directory agent to fulfill requests for Service Location information.

A large network can be divided and categorized by the use of scopes, so that information about a TN server is advertised only to TN3270 clients and directory agents that have the same scope as the TN server. This allows you to control the range of service searches.

The following describes the operations a user agent would employ to find services on the site's network. The user agent needs no configuration to begin network interaction. The user agent can acquire information to construct predicates that describe the services that match the user's needs. The user agent may build on the information received in earlier network requests to find the service agents advertising service information.

A user agent will operate two ways:

1. If the user agent has already obtained the location of a directory agent, the user agent will unicast a request to it in order to resolve a particular request. The directory agent will unicast a reply to the user agent. The user agent will retry a request to a directory agent until it gets a reply, so if the directory agent cannot service the request it must return an response with zero values, possibly with an error code set.
2. If the user agent does not have knowledge of a directory agent or if there are no directory agents available on the site network, a second mode of discovery may be used. The user agent multicasts a request to the service-specific multicast address, to which the service it wishes to locate will respond. All the service agents that are listening to this multicast address will respond, provided they can satisfy the user agent's request.

A directory agent acts on behalf of many service agents. It acquires information from them and acts as a single point of contact to supply that information to user agents.

The queries that a user agent multicasts to service agents (in an environment without a directory agent) are the same as queries that the user agent might unicast to a directory agent.

4.3 SLP support in CS/AIX

IBM Communications Server for AIX, Version 6 supports SLP service advertisement and load balancing for TN3270 servers.

CS/AIX provides information about the server load by calculating the percentage of available resources. For TN3270(E) sessions, the load percentage is the number of active application connections divided by the total number of LUs available.

Because SLP in CS/AIX provides services that are available for use by any TN3270 client, it operates only if a default TN3270 access record has been defined to allow access by any client. If an access record for a specific named clients is defined and no default records are included, the TN server service will not advertise.

4.3.1 Configuring TN3270 server with SLP

Service Location Protocol support in CS/AIX is configured from the TN Server panel. Using xsnaadmin, from the initial node panel, select **Services -> TN Server -> TN Server.**

On the TN Server panel select **Services -> TN3270 SLP Parameters**.

See Figure 32.

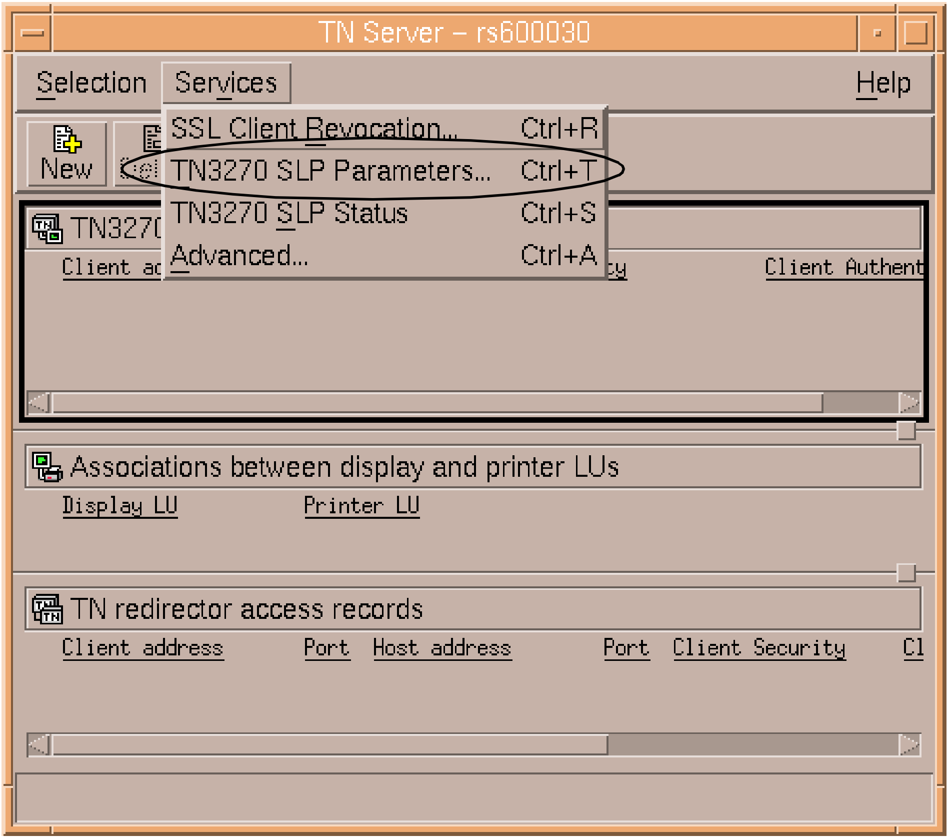
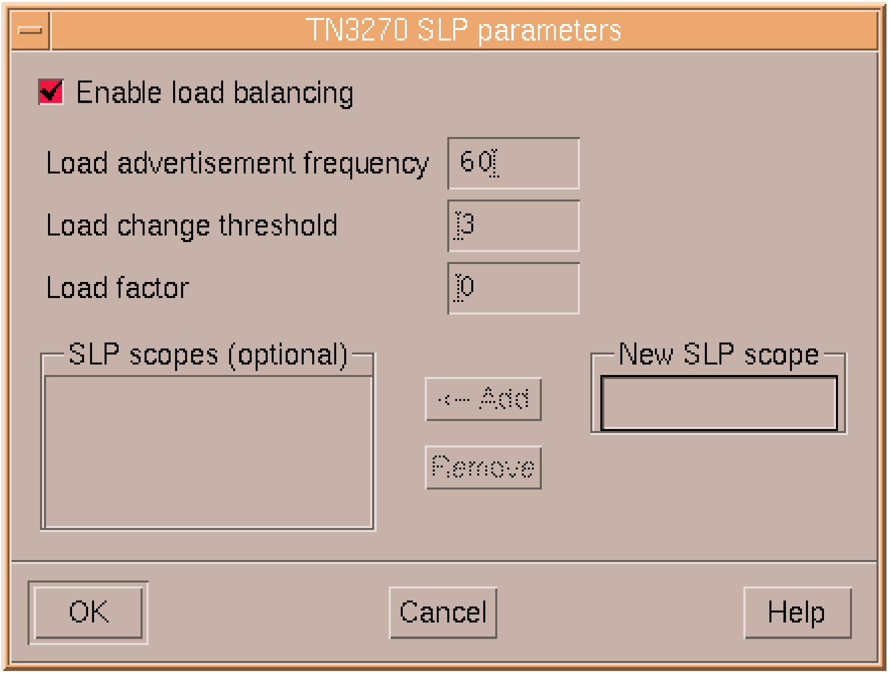


Figure 32. Invoking SLP configuration parameters

This results in the TN3270 SLP Parameters panel being displayed as shown in Figure 33. CS/AIX SLP customization is performed from this panel.



TN3270 SLP parameters

☑ Enable load balancing

Load advertisement frequency: 60

Load change threshold: 3

Load factor: 0

SLP scopes (optional)

New SLP scope

Figure 33. Enable load balancing window

- **Enable load balancing**

  This check box enables SLP load balancing to be started with the TN3270 server.

- **Load advertisement frequency**

  This specifies the frequency, in seconds, with which the TN server load should be determined.

- **Load change threshold**

  This specifies the absolute change in load required to reregister the load.

- **Load factor**

  This allows you to weight the calculated load to compensate for differences such as available memory or processor speed. Specifying a negative number decreases the calculated session load, and specifying a positive number increases the calculated session load. Hence, you can increase the load factor to decrease the number of sessions the server manages (and vice-versa). Enter an integer between -100 and 100.

- **SLP scope**

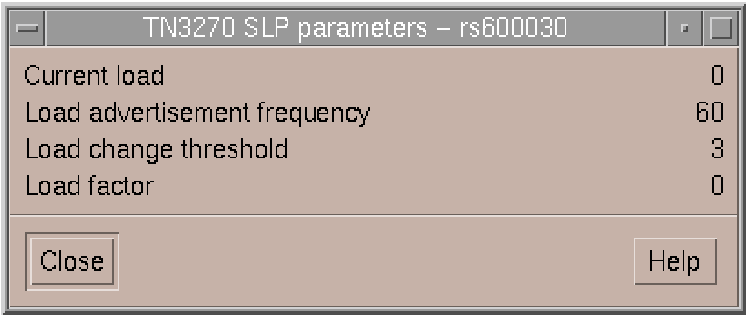
  This specifies an SLP scope to associate with the TN3270 service agent. This is an optional field. The Scope field may be blank (unscoped), or have a specific scope name (scoped). If you enable load balancing, but do not provide a scope name, the server participates in load balancing, but is unscoped. A TN3270 user agent that does not specify a scope value may use an unscoped TN3270 server. A TN3270 user agent may specify a scope using a wildcard character (*). For example, a user agent that specifies a scope of TSO* will receive advertisements from TN3270 servers with scope names that start with TSO (such as TSOTEST and TSOPROD).

  A TN server can support having multiple scopes associated with it. CS/AIX can define up to 10 scopes. A specific scope name will typically be associated with the host resources available via that TN Server.

4.3.2 Monitoring SLP

Once the TN3270 server configuration is complete with parameters required for SLP load balancing, and TN3270 clients begin connecting, the current SLP load may be monitored. From the TN Server panel shown in Figure 32 on page 59, select **TN3270 SLP Status** from the Services pull-down menu.

The current SLP load and configuration parameters are displayed as shown in Figure 34. The current load is calculated based on the Load factor (see Figure 33) and the current number of TN3270 client sessions divided by the total number of LUs available.


TN3270 SLP parameters – rs600030

Current load	0
Load advertisement frequency	60
Load change threshold	3
Load factor	0

Figure 34. SLP status window

The current load is the advertised load for any TN3270 access record that doesn’t restrict the LUs available to the client. If the TN3270 access record only allows access to specific LUs, that advertised load may differ from the value shown here.

Note: When there are multiple SLP TN3270 service agents available to satisfy SLP user agent requests, special consideration should be taken to coordinate the *load advertisement frequency* values in all the service agents (see Figure 33 on page 60). If one of the service agents is configured with a load advertisement frequency that is much higher than the others (it does *not* recalculate its load as often as the other agents), and client login activity is high, that service agent could accept an unduly larger proportion of the login requests than the other service agents. This is because the other service agents adjust their load more often and may reflect a higher load when responding to a user agent request. The service agent with the higher load advertisement frequency continues to advertise a lower load value even though it has accepted many more login requests than the other service agents.

4.4 Scenario

Figure 35 shows a sample network that we will use to step through configuration of SLP support on CS/AIX.

Three RS/6000 machines running IBM Communications Server for AIX, Version 6 are configured with SLP-enabled TN3270 servers. A scope named *slp* will be used to group the servers. LUs will be defined on each machine to support sessions from the TN3270 gateway to the host. At the same time, clients will use an SLP-enabled 3270 emulator (PCOMM for Windows NT V4.3) to connect to the host through the scoped TN3270 servers. From a client's point of view, there is no need to define any TN3270 server's IP address (or alias) or port number to which clients try to connect.

We will also review the change in server load as clients log in to the host.

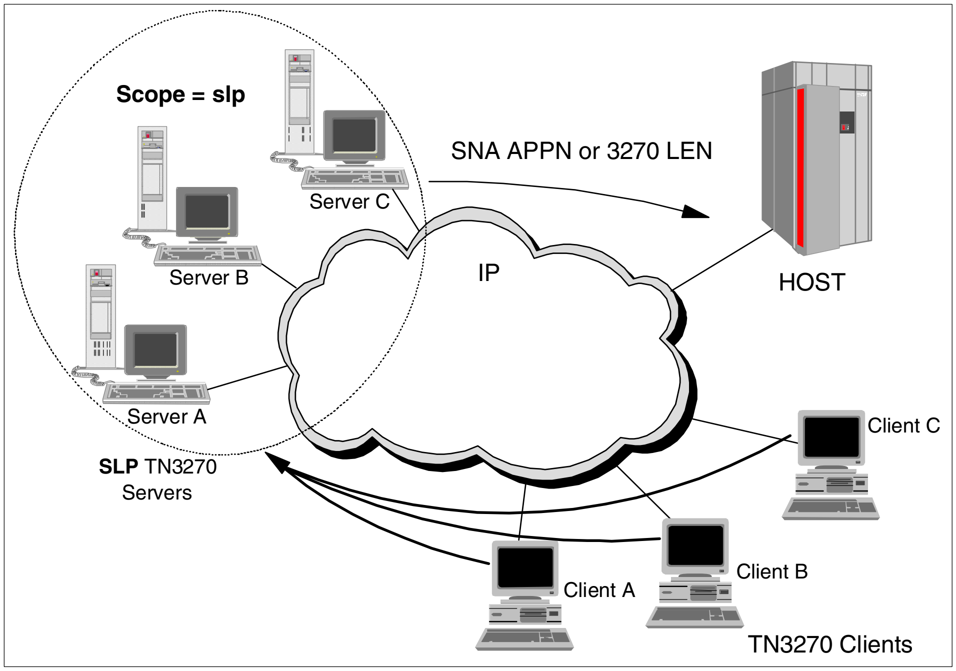
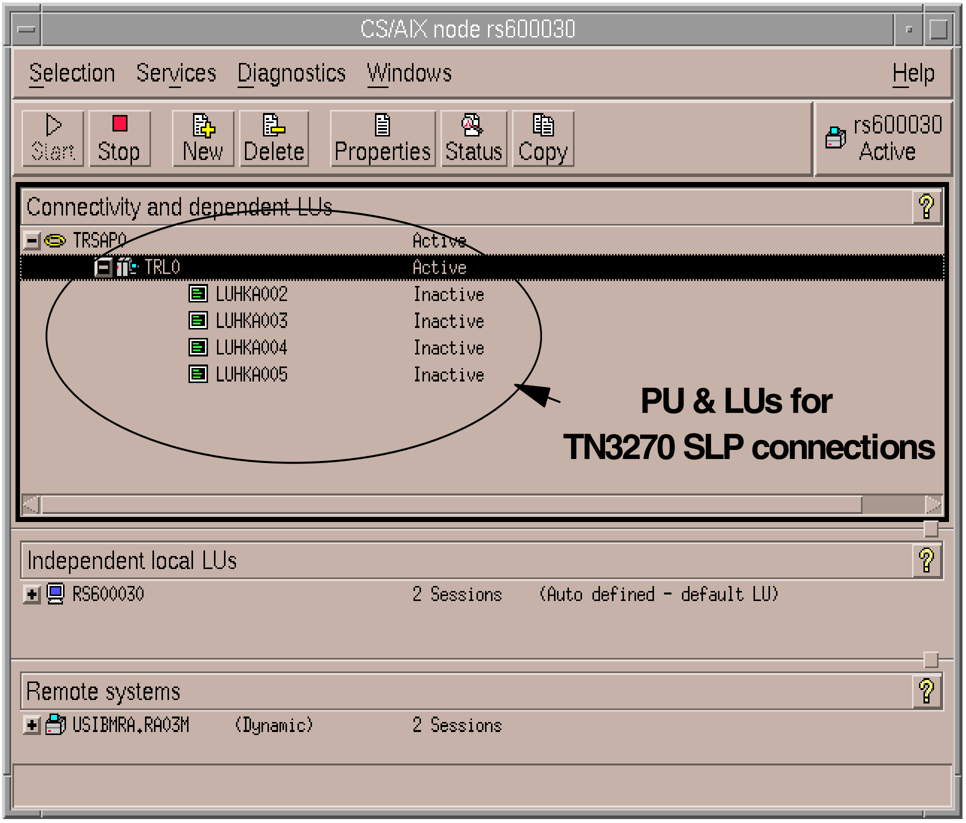


Figure 35. SLP connection scenario

4.4.1 Configuring TN3270 SLP servers

On each CS/AIX server, the node must be configured, followed by definitions for port(s), link(s) and LU(s). The LUs will be used by the TN3270 gateway to satisfy session requests to the host. The following panels show the configuration for Server A. Similar definitions for Servers B and C are also required.

Figure 36 shows the node configuration for Server A.



```
TRSAP0                                  Active
      TRL0                              Active
            LUHKA002                    Inactive
            LUHKA003                    Inactive
            LUHKA004                    Inactive
            LUHKA005                    Inactive
```

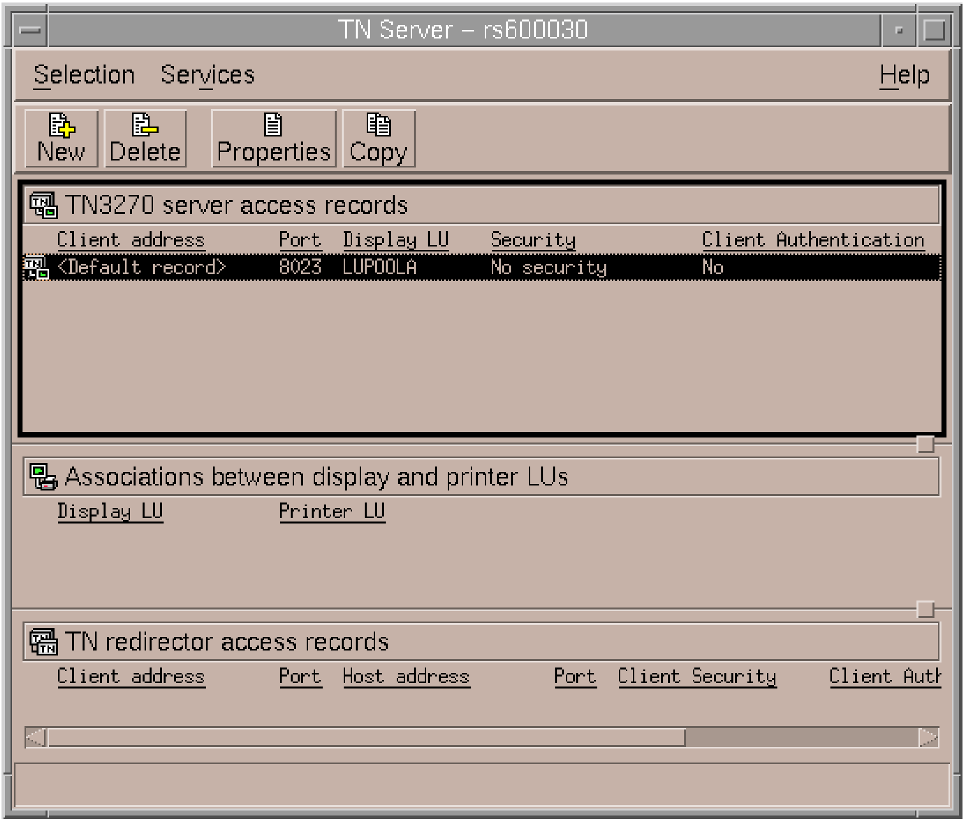
```
RS600030                                2 Sessions    (Auto defined - default LU)
```

```
USIBMRA.RA03M     (Dynamic)             2 Sessions
```

PU & LUs for
TN3270 SLP connections

Figure 36. PU and LU definition for SLP TN3270 Server A

Once the node and required port, link and LUs have been defined, the TN3270 server must be configured. See Figure 37.



TN3270 server access records

Client address	Port	Display LU	Security	Client Authentication
<Default record>	8023	LUPOOLA	No security	No

Associations between display and printer LUs

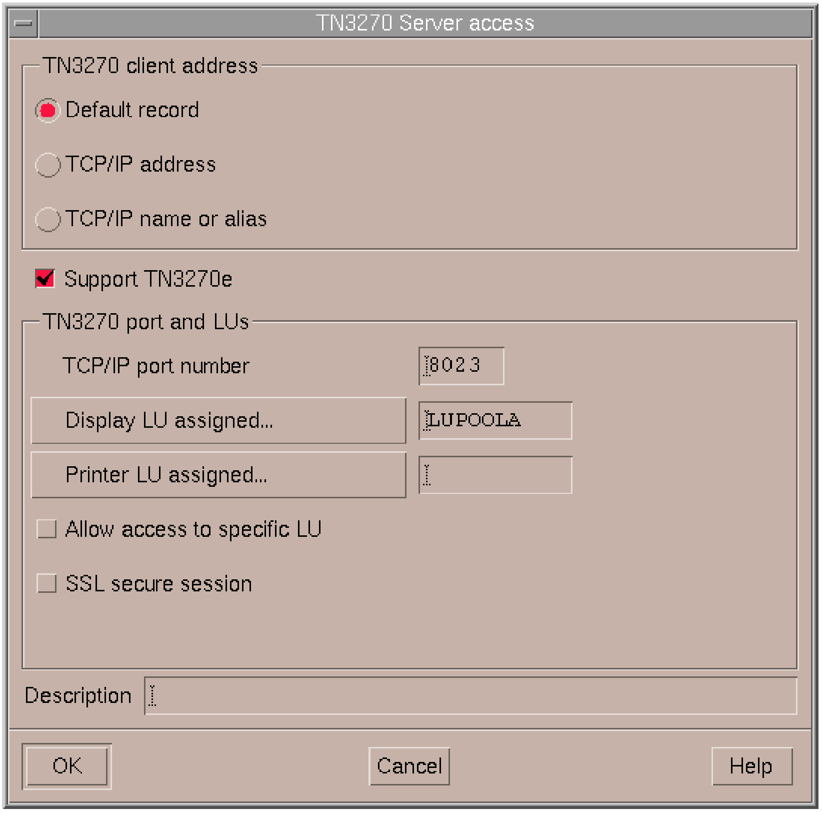
Display LU	Printer LU

TN redirector access records

Client address	Port	Host address	Port	Client Security	Client Auth

Figure 37. TN3270 Server A configuration

On TN3270 Server A, we define a default access record that allows clients to make connections to the host through this server using port 8023 and LUs in LUPOOLA. However, as mentioned previously, SLP TN3270 clients will not require a server port number. The default access record configuration is shown in Figure 38.



TN3270 Server access

TN3270 client address

● Default record

○ TCP/IP address

○ TCP/IP name or alias

☑ Support TN3270e

TN3270 port and LUs

TCP/IP port number: 8023

Display LU assigned...: LUPOOLA

Printer LU assigned...:

□ Allow access to specific LU

□ SSL secure session

Description:

Figure 38. TN3270 Server A default access record

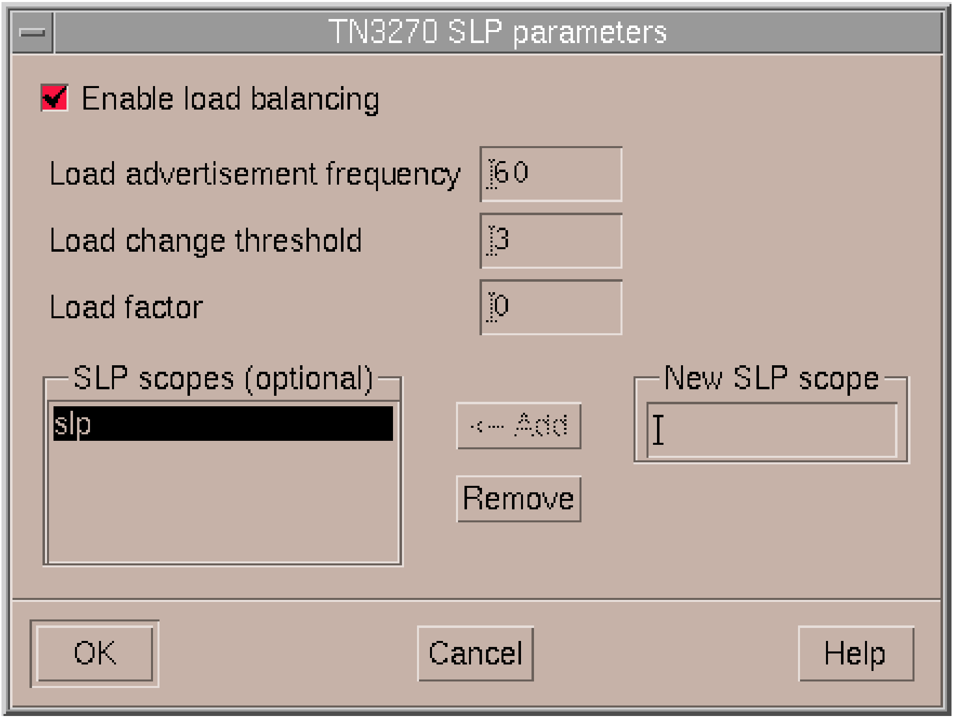
Remember that SLP load balancing only works for default TN3270 server access records. Access records that define a specific client IP address or name do not participate in SLP.

SLP support must now be configured on Server A. From the TN3270 Server panel shown in Figure 37, we select **Services** -> **TN3270 SLP Parameters** from the menu bar.

On the TN3270 SLP Parameters panel shown in Figure 39, check **Enable load balancing** and enter values needed.

Enter the scope name `slp` into the New SLP scope field and add it to SLP scopes.

Select **OK**.



TN3270 SLP parameters

☑ Enable load balancing

Load advertisement frequency 60

Load change threshold 3

Load factor 0

SLP scopes (optional): slp

New SLP scope

Figure 39. SLP enable load balancing window

Coordination with your network administrator is required to ensure the proper SLP scope name is defined in Servers B and C. In addition, the values chosen for load advertisement frequency, Load change threshold and Load factor must be agreed to for all servers participating in this SLP network.

Note: Resources required to support TN3270 server definitions such as LU name, LU pool name, and port number do not need to be the same as those in other servers.

Configuration of SLP TN3270 server support is now complete in Server A. Similar definitions must be made in Servers B and C.

Next, we define a TN3270 client to use SLP.

4.4.2 Configuring TN3270 SLP clients

An SLP-enabled TN3270 emulator is required to request a service or application running on the host. For this scenario, we will configure a TN3270 client session using Personal Communications for Windows NT V4.3.

When not using SLP, a TN3270 emulator session is configured by adding the TN3270 server host name or IP address and port number. However, when configuring an SLP TN3270 agent, much less configuration is required.

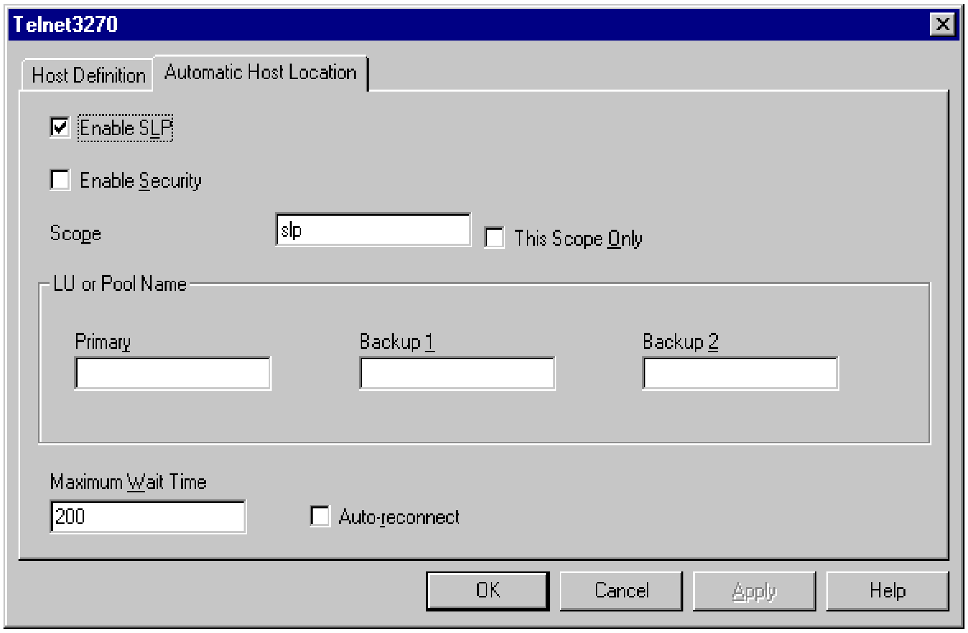
Select **Start -> IBM Personal Communications -> Start or Configure Session.**

Select **OK** when the Welcome window appears.

The Customize Communications window will appear. Select Telnet3270 for Attachment. Then select **Link Parameters**.

The Telnet3270 window is displayed.

Go to the second tab, Automatic Host Location, leaving Host Definition blank. Figure 40 displays the completed panel.



Telnet3270

☑ Enable SLP

☐ Enable Security

Scope: slp ☐ This Scope Only

LU or Pool Name

Primary:

Backup 1:

Backup 2:

Maximum Wait Time: 200

☐ Auto-reconnect

Figure 40. SLP configuration window of client

Check **Enable SLP**.

For our scenario, we will enable a scope named `slp`. Enter the scope name into **Scope**, and select **OK**.

An “*” (wildcard character) in the Scope field means that this SLP TN3270 client user agent is unscoped, indicating that any SLP TN3270 server that advertises is acceptable to the client. Another example of using a wildcard in a scope name is to have one CS/AIX server use scope name SLP1 and a second CS/AIX server use scope name SLP2. A client then may code a scope of `slp*` indicating that an advertisement from any TN3270 server with a scope starting with slp is acceptable.

If a server is not found for the specified scope, or if the scope is not defined on any server, SLP returns an unscoped server (if one is available), unless you check **This-Scope-Only**. If you check **This-Scope-Only** and no server is found within the specified scope, the session will not connect.

If you want your session to use SSL security in addition to SLP load balancing, check **Enable Security** and follow the steps required to support security. Remember that the servers must also support SSL for secure sessions to be established. For more information, refer to Chapter 2, “Secure Sockets Layer support” on page 9.

Notice that you may also select a specific LU or Pool Name. If you have multiple default TN3270 access records defined in your CS/AIX TN3270 service agents, each with their own LU pool or specific LU, you may specify that pool name or LU here to ensure you are connected to the correct LU. The TN3270 server port number is not required.

4.4.3 Connecting to TN3270 SLP servers

In this scenario, as mentioned in beginning part of this section, there are three TN3270 SLP servers and three clients that request TN3270 sessions to servers. Client session requests are balanced between the three servers that are available with their scope definition.

4.4.3.1 First session request from Client A

Client A begins by requesting a host session. See Figure 41.

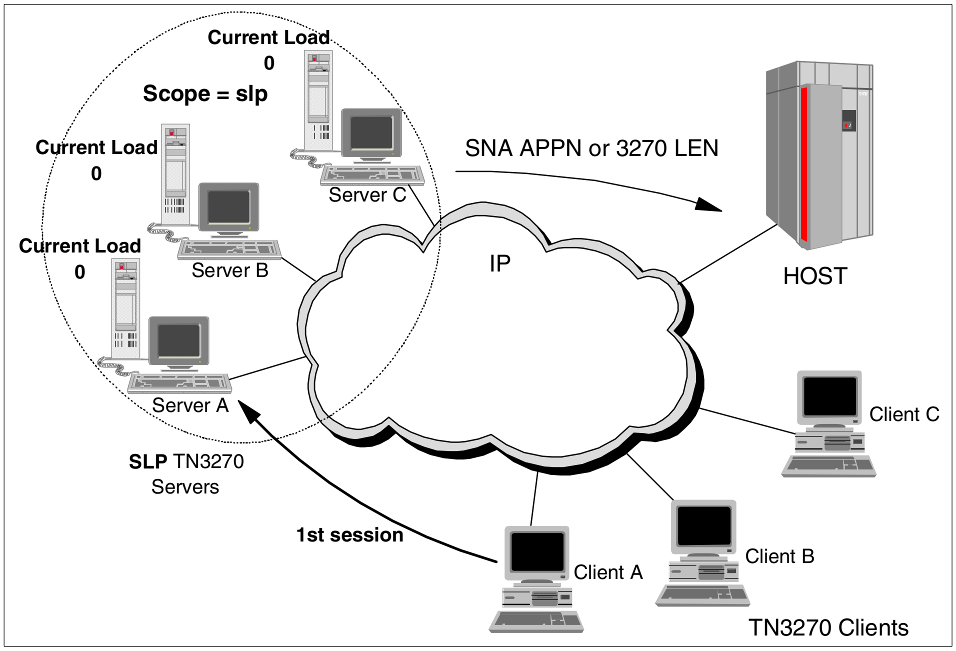
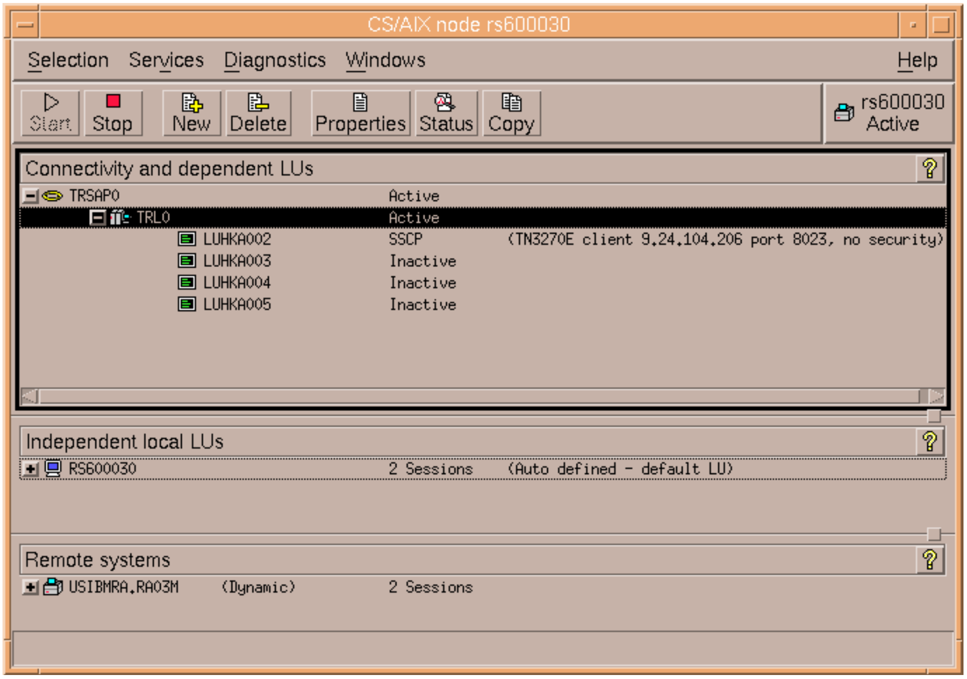


Figure 41. First TN3270 SLP session connection

Assuming that the SLP selection process chooses Server A to complete the connection, you can see and confirm it from Server A's node resource window. It displays the client IP address and related connection information, as shown in Figure 42.



Connectivity and dependent LUs

```
TRSAP0                              Active
     TRL0                           Active
          LUHKA002                  SSCP        (TN3270E client 9.24.104.206 port 8023, no security)
          LUHKA003                  Inactive
          LUHKA004                  Inactive
          LUHKA005                  Inactive
```

Independent local LUs

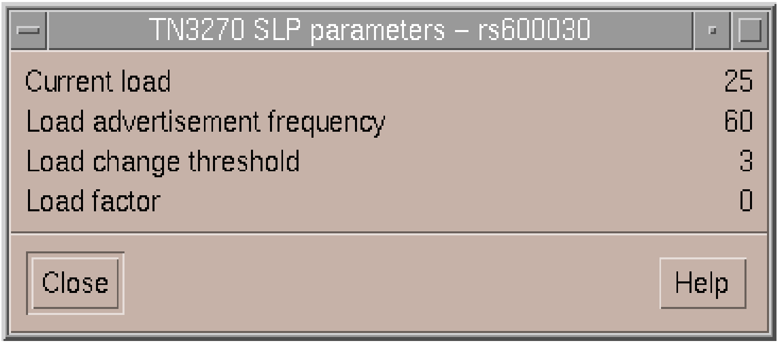
```
RS600030                            2 Sessions     (Auto defined - default LU)
```

Remote systems

```
USIBMRA.RA03M        (Dynamic)      2 Sessions
```

Figure 42. CS/AIX resource window of Server A

At the same time, you can monitor the load of Server A’s resources from the TN3270 SLP parameters window, as shown in Figure 43.



Current load	25
Load advertisement frequency	60
Load change threshold	3
Load factor	0

Figure 43. TN3270 SLP parameters window of Server A

TN3270 Server A has only four LUs available for 3270 display sessions, and one LU is being used for Client A. Thus, the current load of TN3270 SLP Server A is 25, as you can see above. The current load displayed in the

TN3270 SLP parameters window can be changed by adjusting the load factor value.

4.4.3.2 Second session request from Client B

When Client B requests a session with the host, SLP load balancing picks from either Server B or C to complete the session, since Server A has a higher calculated load. In our scenario, Server B is chosen.

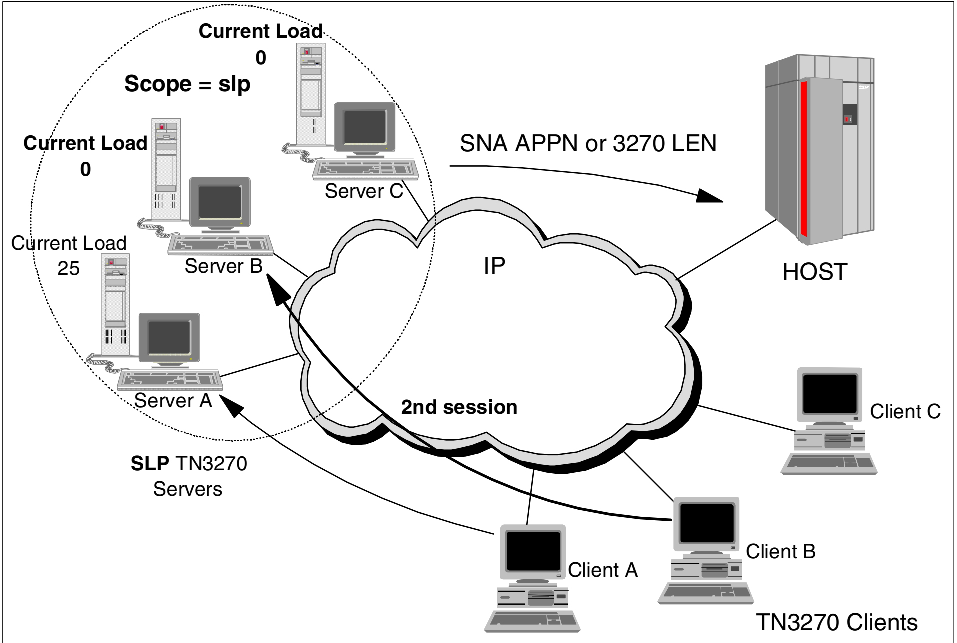
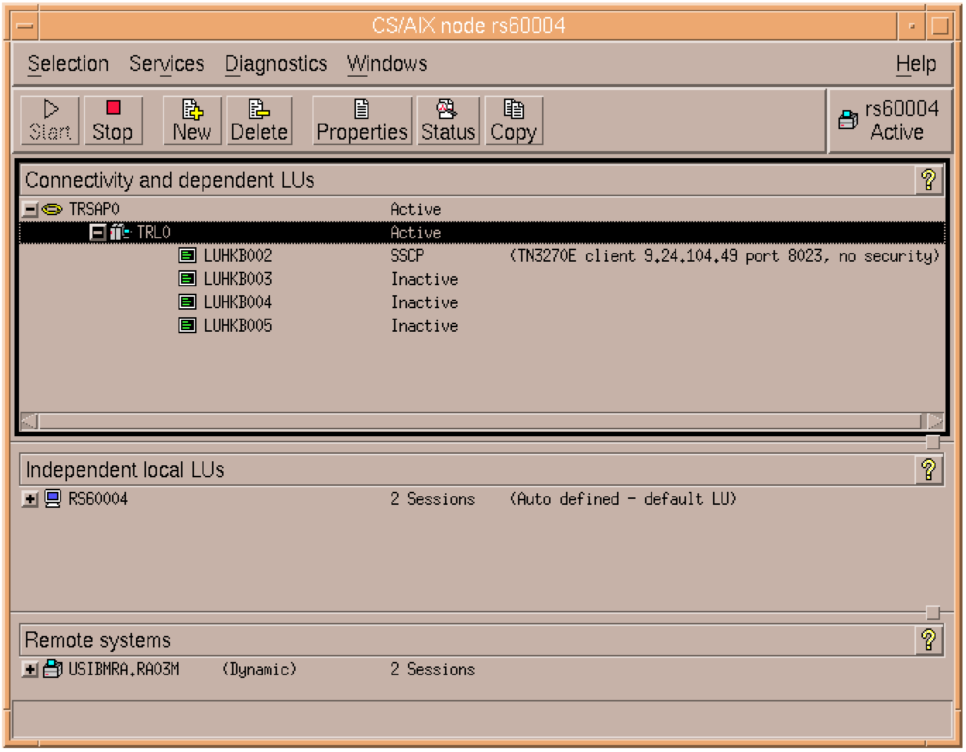


Figure 44. Second TN3270 SLP session connection

You can confirm it from the CS/AIX resource window of Server B as shown in Figure 45.



Connectivity and dependent LUs

```
TRSAP0                              Active
     TRL0                           Active
          LUHKB002                  SSCP      (TN3270E client 9.24.104.49 port 8023, no security)
          LUHKB003                  Inactive
          LUHKB004                  Inactive
          LUHKB005                  Inactive
```

Independent local LUs

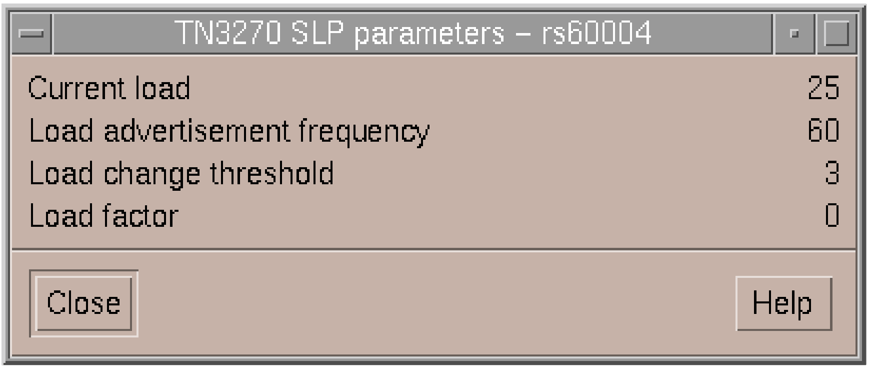
```
RS60004                             2 Sessions     (Auto defined - default LU)
```

Remote systems

```
USIBMRA.RA03M       (Dynamic)       2 Sessions
```

Figure 45. CS/AIX resource window of Server B

TN3270 SLP Server B now has a current load of 25 as shown in Figure 46.



Current load	25
Load advertisement frequency	60
Load change threshold	3
Load factor	0

Figure 46. TN3270 SLP parameters window of Server B

4.4.3.3 Third session request from Client B

Now, a third session is received from client C. The current load on Servers A and B is 25. So SLP load balancing sends the third session request to server C which has no current load.

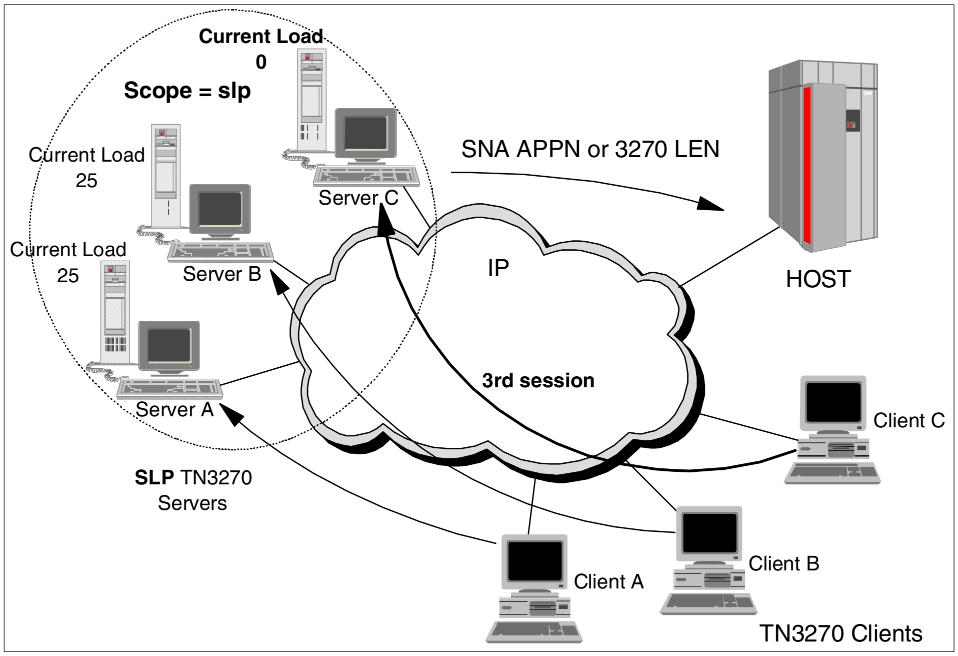
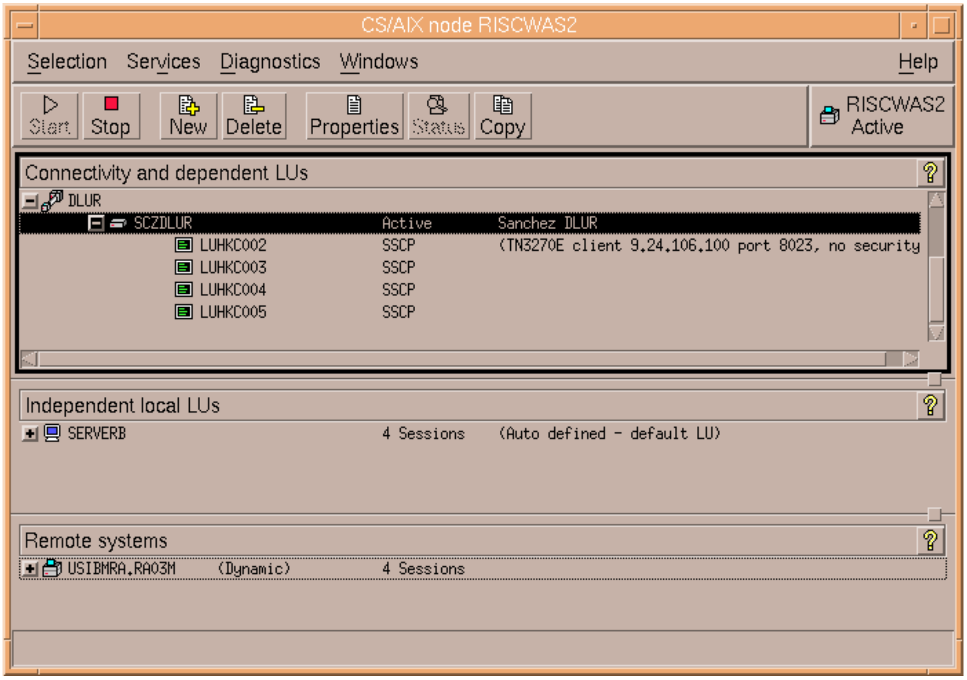


Figure 47. Third TN3270 SLP session connection

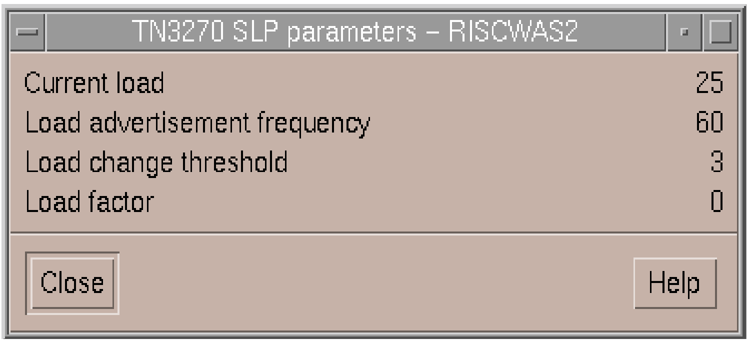
Figure 48 shows the third session is being serviced by Server C.



```
DLUR
    SCZDLUR                          Active       Sanchez DLUR
            LUHKC002                 SSCP         (TN3270E client 9.24.106.100 port 8023, no security
            LUHKC003                 SSCP
            LUHKC004                 SSCP
            LUHKC005                 SSCP

SERVERB                              4 Sessions   (Auto defined - default LU)

USIBMRA.RA03M        (Dynamic)       4 Sessions
```

Figure 48. CS/AIX resource window of server C for third session

And also, server C has a current load of 25, as shown in Figure 49.



```
Current load                      25
Load advertisement frequency      60
Load change threshold              3
Load factor                        0
```

Figure 49. TN3270 SLP parameters window of Server A

Chapter 5. TN3270 inactivity timeout

CS/AIX allows an inactivity timeout value to be defined for LU types 0-3. This timeout value will automatically deactivate a session if the LU user supports inactivity timeout. The TN3270 server feature in IBM Communications Server for AIX, Version 6 has been enhanced to support this inactivity timeout capability.

5.1 Overview

The `timeout=` parameter on the [define_lu_0_to_3] stanza allows an LU to be disconnected from its current user. The *CS/AIX Administration Command Reference V6*, SC31-8587, says this about the timeout parameter:

> Timeout for the LU specified in seconds. If the timeout is set to a nonzero value and the user of the LU supports session inactivity timeouts, then the LU is deactivated after the PLU-SLU session is left inactive for the specified period and one of the following conditions exist:
>
> - The session passes over a limited resource link.
> - Another application requests to use the LU before the session is used again.
>
> If the timeout is set to 0 (zero), the LU is not deactivated.

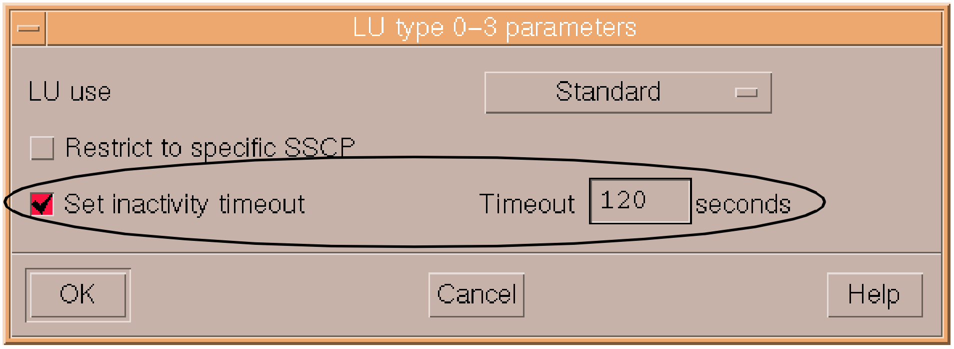
The *user of the LU* is a component of CS/AIX such as the Gateway function or an external application such as HCON. In CS/AIX V5, the TN3270(E) server component did not support this timeout, but in CS/AIX V6 it does.

The first condition listed is: if the session passes over a limited resource link. An example of this would be a SDLC switched link which is paid for by connect-time (for example, a long-distance phone call). In this case disconnecting an idle LU would allow the link to disconnect, saving connect-time charges.

The second condition listed is if another application requests to use the LU before the session is used again. An example of this would be a token-ring link with 255 LUs in a pool, but more than 255 potential users. In this case, disconnecting an idle LU would allow it to be used by someone else (another TN3270 client).

5.2 Implementation

The timeout parameter can be set on the SMIT menu or with the `snaadmin` command or in xsnaadmin by selecting **Services -> 3270 -> New 3270 display LU -> Advanced -> Set inactivity timeout.**



LU type 0–3 parameters

LU use: Standard

□ Restrict to specific SSCP

☑ Set inactivity timeout   Timeout 120 seconds

Figure 50. Set inactivity timeout

Different timeout values can be used for different LUs, even on the same link. For example, you may want to define LUs used by managers with a timeout value of zero (no timeout), while the LUs used by developers have a large timeout, and the LUs used by casual users have a small timeout.

For the TN3270E server the users could be segregated by using different pools.

The actual value for the timeout may be as much as two times the configured value depending on when the original user of the LU connected relative to when the timer was set.

Part 3. SNA networking

Chapter 6. Enterprise Extender

This chapter describes the functionality of Enterprise Extender (EE), gives an overview of High-Performance Routing (HPR), and discusses the implementation of Enterprise Extender in CS/AIX. An example scenario illustrates the use of HPR over IP to support SNA applications.

Enterprise Extender is also referred to as High Performance Routing over IP (HPR/IP). Throughout this chapter, Enterprise Extender will be referred to as EE and HPR/IP.

6.1 Overview

Enterprise Extender (or HPR/IP) provides High-Performance Routing (HPR) functionality over IP connections to support SNA applications connected over an IP network.

SNA applications are designed to use SNA protocols to communicate over SNA networks with other SNA applications. When installed in a TCP/IP network using Enterprise Extender, SNA applications continue to communicate. The Enterprise Extender function provides a mechanism for transporting SNA protocols over an IP network using the UDP protocol. Unlike AnyNet, Enterprise Extender provides APPN High-Performance Routing functionality, giving applications the benefits of both APPN and IP connectivity.

Enterprise Extender in CS/AIX is implemented simply as a new communications link. To connect two SNA applications over IP, you define an Enterprise Extender link in the same way as for any other link type such as SDLC or Ethernet. This new DLC allows you to take advantage of APPN/HPR functions in the IP environment.

Note that Enterprise Extender (HPR/IP) links support independent LU6.2 sessions. Dependent LUs are supported using DLUR over the EE link.

An example of a node configured with one explicit HPR/IP link to a NN is shown in Figure 51 on page 82.

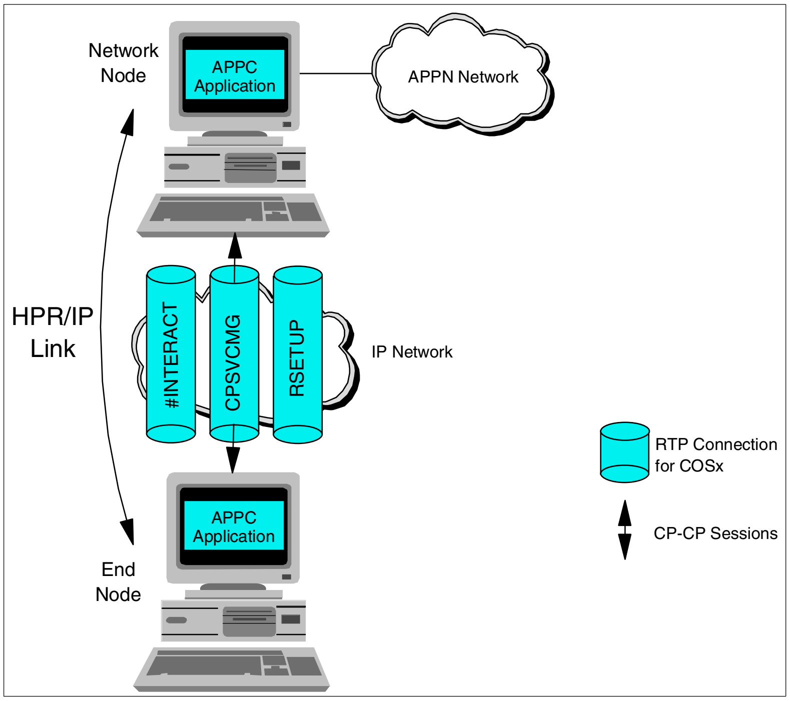


Figure 51. EE link with several RTP connections and CP-CP sessions

Enterprise Extender (HPR/IP) allows you:

1. To use IP between the origin node and the destination node of an Enterprise Extender link to transport SNA data (something that AnyNet APPC over IP also can do).
2. To participate as a full APPN node in an APPN network (something that AnyNet APPC over IP can't).
3. To benefit from the advantages of HPR in an IP-routed network.

6.2 An HPR overview

High-Performance Routing (HPR) is an extension to APPN. It's first aim is to improve data routing performance by reducing the overhead that takes place at all intermediate nodes of an APPN-session (session-level error check, flow control, segmentation and reassembly). It does so by letting these functions take place only at the begin- and end-points of the HPR-session. By doing so it reduces storage and processing requirements on intermediate nodes in the route and reduces the latency (the time it takes for data to reach its destination) of the network. While in APPN, all NNs over which a session traverses play an equally important role in error checking and recovery, in HPR the begin- and end-node are the only nodes responsible for this checking, flow control and, if necessary, reassembly and segmentation. This means that CPU and memory needs of intermediate nodes are less, but that CPU and memory needs of the end-nodes is more. In a 1-hop (2 node) HPR environment, you get none of the advantages but you pay all the costs of HPR, which means throughput is likely to be less than non-HPR.

A second aim of HPR is to allow for non-disruptive path switch if a link or node in the path becomes unavailable. While in APPN a session has to follow a route which has been determined at the session setup, in an HPR network, the LU-LU sessions flow within RTP connections (which can be thought of as pipes) which makes the underlying route (succession of NNs) invisible.

HPR's main components by which these aims can be accomplished are:

- Rapid Transport Protocol (RTP)
- Automatic Network Routing (ANR)
- Adaptive Rate-Based (ARB) flow/congestion control. ARB is actually part of RTP.

6.2.1 Rapid Transport Protocol (RTP)

Rapid Transport Protocol (RTP) is a connection-oriented, full-duplex protocol designed to transport SNA session traffic in high-speed networks. RTP provides reliability (error recovery via selective retransmission), in-order delivery (a first-in-first-out service provided by resequencing data that arrives out of order), message segmentation and reassembly, ARB flow congestion control and automatic path-switching without disrupting sessions. Because RTP provides these functions on an end-to-end basis, it eliminates the need for these functions to be implemented on the link level along the path of the connection. The result is improved overall performance for HPR.

The physical path used by the RTP connection satisfies the Class Of Service (COS) associated with the sessions routed over it. Traffic from many sessions requesting the same COS can be routed over a single RTP connection. RTP connections are used to:

- Transport CP-CP session traffic
- Transport LU-LU session traffic
- Carry route setup requests required to establish LU-LU sessions over a series of RTP connections

An example of an RTP connection is shown in Figure 52.

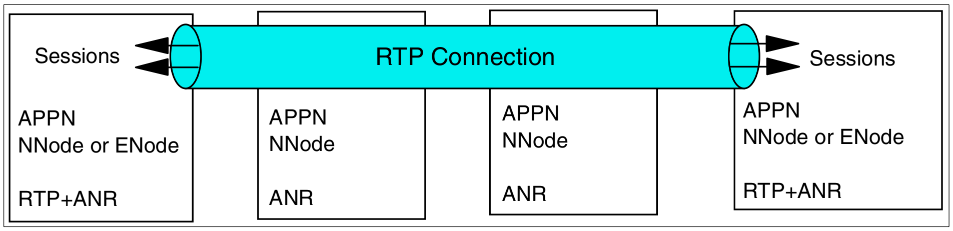


Figure 52. An RTP connection in an HPR subnet within an APPN network

The requirements for a node to act as a beginning or ending node of an RTP connection are:

1. That it is an APPN end or network node
2. That it has the RTP functions implemented

The requirements for a node to be an intermediate node over which such a connection runs are:

1. That it is an APPN network node
2. That it has the ANR functions implemented

An RTP connection has the following features:

- It transports data at very high speeds by using lower-level intermediate routing (ANR) and by minimizing the number of flows over the links for error recovery and flow control. These functions are performed at the session endpoints rather than at each hop along the path. For more information on ANR, see “Automatic Network Routing (ANR)” on page 86.
- It can be switched automatically to reroute data around a failed node or link without disrupting the LU-LU sessions. This is called non-disruptive path switch because LU-LU sessions survive link failures. A non-disruptive path switch within the HPR portion of the network automatically occurs in an HPR subnet to bypass link and node failures if an acceptable alternate path is available. However, all the nodes on both the failed path and the new path must be HPR-capable. This function does not operate within or across a basic APPN subnet. Figure 53 illustrates a non-disruptive path switch.

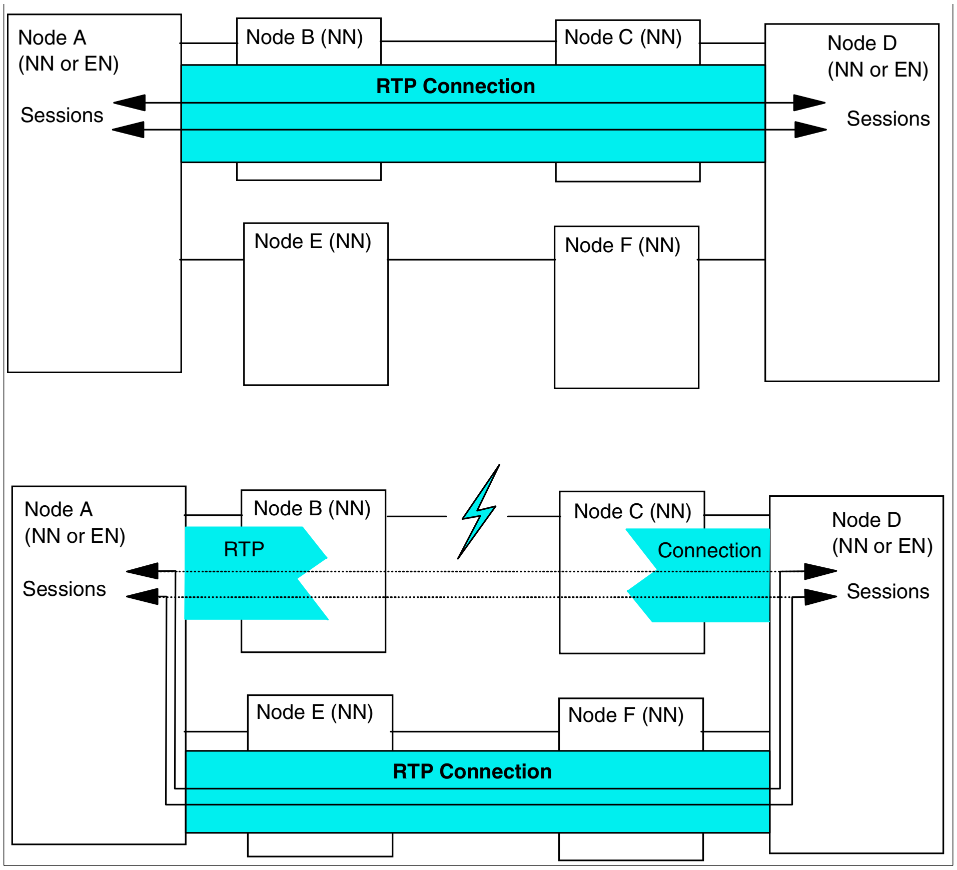


Figure 53. Non-disruptive path switch

- It provides transport of data in a reliable manner. RTP guarantees delivery of all data and performs the necessary end-to-end error recovery. HPR uses selective retransmission, which eliminates the need for error recovery at each hop. Selective retransmission transmits only packets that were lost, rather than retransmitting the lost packet and all the following packets.
- It provides rate-based flow/congestion control. HPR uses the adaptive rate-based (ARB) flow/congestion algorithm. This eliminates the need for flow control at each hop.
- It performs segmentation and reassembly. RTP performs the necessary segmenting and reassembly of messages based on the minimum link BTU size on the path between the two endpoints of the RTP connection.

6.2.1.1 Automatic Network Routing (ANR)

Automatic Network Routing (ANR) is a low-level routing mechanism that minimizes cycles and storage requirements for routing packets through intermediate nodes. ANR represents significant increases in routing speed over basic APPN. ANR provides point-to-point transport between any two endpoints in the network. Intermediate nodes are not aware of SNA sessions or RTP connections passing through the node. ANR is designed for high-performance switching, since no intermediate node storage for routing tables is required and no precommitted buffers are necessary.

The originator of the packet explicitly defines in the routing field of the packet's network layer header the exact path on which the packet is to flow through the network; thus, ANR is a special implementation of a source-routing protocol. Each Network Layer Packet (NLP) is routed through the network as a self-contained unit and is independent of all other packets. There is no table lookup or processing necessary at transit nodes.

Figure 54 illustrates automatic network routing.

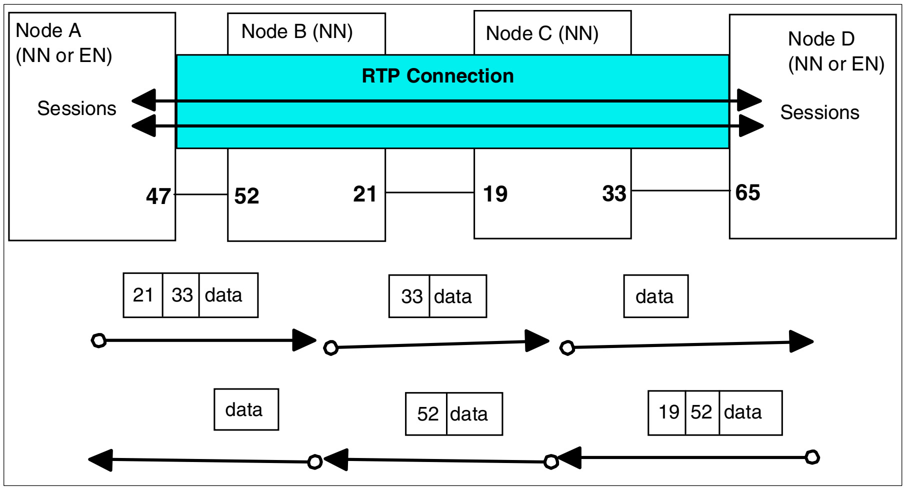


Figure 54. Automatic network routing

The routing information is carried in the NLP as a sequence of ANR labels. The processing of the label is designed to be simple and very efficient. Each node examines the label at the beginning of the ANR string. The ANR node strips the first label from the ANR string and forwards the NLP to the next hop. When a packet is forwarded across a transmission link, the first label in the routing field always indicates the physical link to be used by the next node.

Each transmission link connecting two nodes or subnodes is assigned two ANR labels, one at each end. When the transmission link is activated, each node assigns an ANR label for the outbound direction. For example, in Figure 54 on page 86, Node A assigns the label 47 for the direction from Node A to Node B and Node B assigns label 52 for the direction from Node B to Node A.

In contrast to the RTP-capable nodes where the RTP connection ends or begins, an intermediate ANR-capable NN doesn't do any route setup, session level error recovery or flow control.

In contrast to the FID2 transmission units used for APPN, the NLPs aren't segmented in the intermediate ANR-capable NNs, thanks to the information the origin RTP node collected during the setup of the RTP connection (smallest maximum packet size).

6.2.1.2 Adaptive Rate-Based flow/congestion control (ARB)

The Adaptive Rate-Based (ARB) flow/congestion control algorithm is designed to make efficient use of network resources by providing a congestion avoidance and control mechanism. The basic approach used in this algorithm is to regulate the input traffic in the face of changing network conditions. When the algorithm detects that the network is approaching congestion and the path becomes saturated, resulting in increased delays and decreased throughput, it reduces the input traffic rate until these indications go away. When the network is sensed to have enough capacity to handle the offered load, the algorithm allows more traffic to enter the network without exceeding the rate the receiver can handle. ARB prevents unnecessary retransmissions, minimizes response time, and improves throughput efficiency. ARB also fosters network stability and consistent, predictable performance.

The ARB algorithm is based on information exchanged between the two endpoints of a connection. This information reflects the state of both the receiver and of the network. The sender, based on information from the receiver, regulates the input traffic accordingly. The rate-based algorithm is applied independently in each direction. ARB *smooths* the sending of the available input to accommodate the target rate. The smoothing gives networks better characteristics than if the input is sent in a burst.

ARB is based on controlling the rate at which data may be sent rather than controlling a window of data that may be sent at any rate. Figure 55 on page 88 illustrates the difference between basic APPN and HPR in the way session-level pacing is handled.

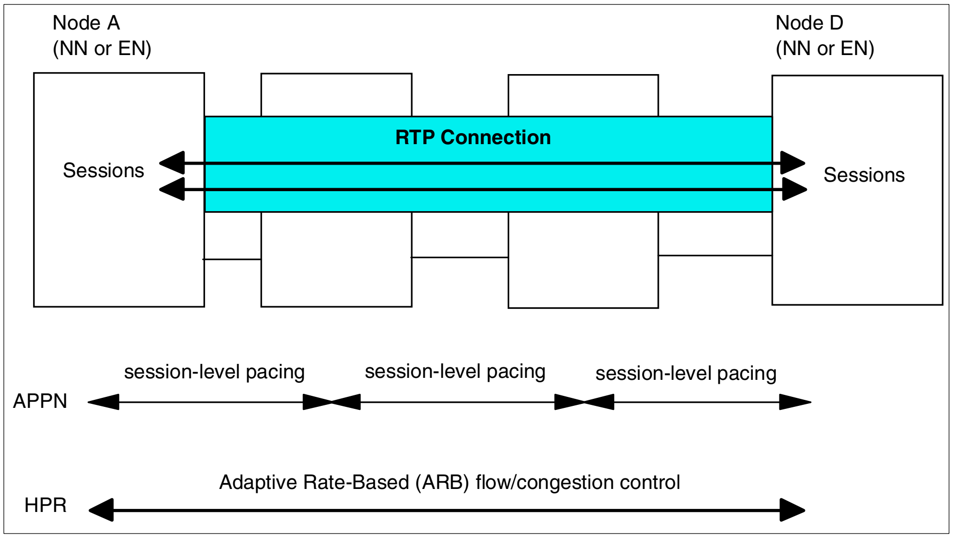


Figure 55. APPN/HPR session-level pacing

The feedback information consists mainly of the minimum of two rates: one is the rate at which the receiver accepts arriving data from the network, and the other is the rate at which the receiver delivers data to the end user. The former indicates the state of the path in the network and is used by the sender to regulate the input traffic load to avoid overloading the path and therefore causing congestion. The latter is used by the sender to avoid overloading the receiver and thus results in end-to-end flow control. Based on the rate information received, the sender can determine when congestion is about to develop in the network and take appropriate actions to avoid it. If congestion does occur, the sender takes drastic measures to bring the network back to normal.

There are two levels of ARB flow control support:

Base ARB (ARB1) This is the original ARB algorithm defined by HPR. The Base ARB design makes some assumptions about the types of networks in which Base ARB is used. In particular, the design assumes that the networks are SNA networks and have relatively stable traffic patterns and applications demands. It also assumes that all traffic on the network is using the same flow control algorithm. Some of these assumptions may no longer be valid in today's networks. Characteristics of Base ARB:

- Slow, linear ramp-up speed.

- Rate fairness is limited if some connections have very large burst sizes.
- Insufficient clock resolution for high speed links (T3 and above).
- Over-reaction to data loss.

Responsive Mode ARB (ARB2) Responsive Mode ARB provides better performance and stability in networks with variable characteristics. Responsive Mode ARB is designed to work nearly as well as Base ARB in environments for which Base ARB was designed, and to work better than Base ARB in environments such as the multiprotocol network, which is currently the most significant environment for HPR and in which different types of traffic using different flow control algorithms share some of the same physical resources. Characteristics of Responsive Mode ARB:

- Faster, exponential ramp-up speed at start-up (congestion conditions permitting).
- Short transmissions get high priority.
- Sustained transmissions get fair bandwidth allocation.
- Much less sensitive to packet loss.
- More intelligent reaction to changing network conditions.
- Compete fairly with other protocols such as TCP.

IBM Communications Server for AIX, Version 6 supports both ARB1 and ARB2. It will use ARB1 when the remote node is not ARB2-capable.

6.3 Implementation

As mentioned in “Overview” on page 81, Enterprise Extender in CS/AIX is implemented simply as a communications link.

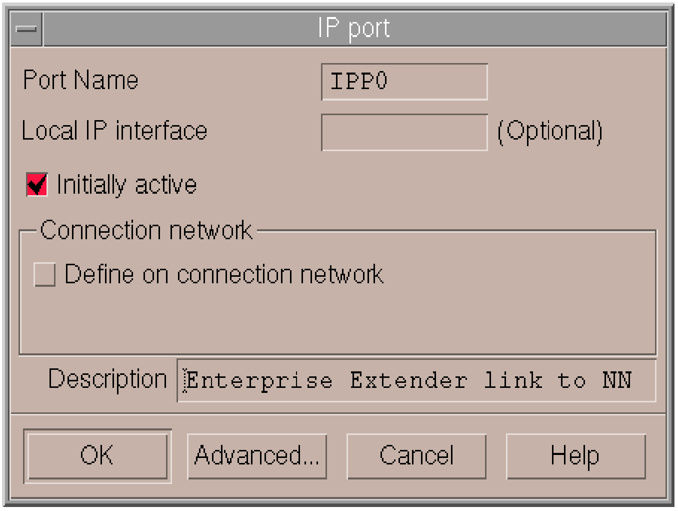
To configure the Enterprise Extender link, perform the following steps from the **Node** window:

1. Configure the port

   a. From the main window select: **Services** -> **Connectivity** -> **New port.**

   b. Select the **Enterprise Extender (HPR/IP)** link protocol.

   c. When you click the **OK** button, CS/AIX displays the IP port dialog window.



Port Name: IPP0

Local IP interface: (Optional)

☑ Initially active

Connection network

□ Define on connection network

Description: Enterprise Extender link to NN

Figure 56. IP port dialog

You need the following information:

SNA Port Name This is a name for you to identify the IP port. This name can be up to eight characters.

Local IP interface The identifier for the TCP/IP network interface to be used for the HPR/IP link. For example, *tr0*. If no value is provided, CS/AIX defaults this parameter to the primary TCP/IP network interface. If you have multiple TCP/IP network interfaces, supply the interface you want to use for the HPR/IP link (such as tr0, en0).

Initially active If you select this option, the IP port is activated automatically when the node is started.

Define on connection network Select this option if you want to use the port to access the LAN as a connection network.

Advanced parameters In most cases you can use the default settings for these parameters, so you do not need to alter the settings in the advanced dialog.

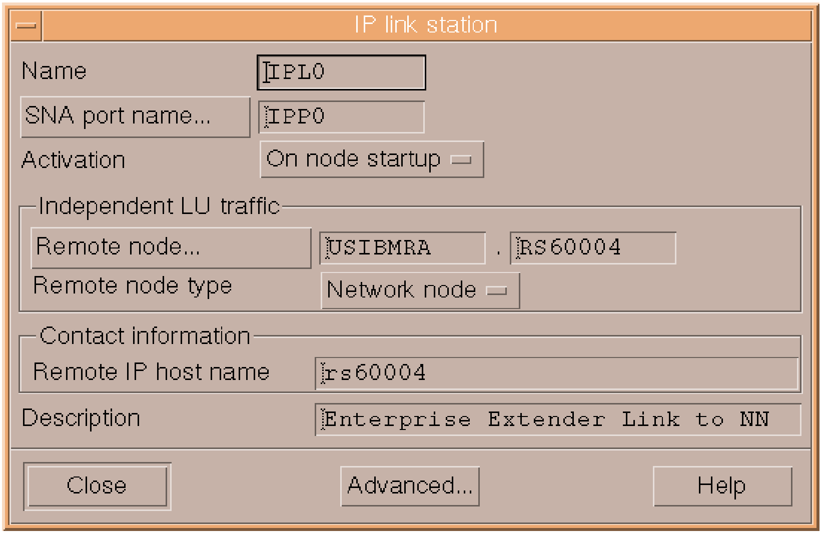
d. Click the **OK** button and the port will appear in the Connectivity pane of the Node window.

2. Define a link station on the port:

   a. In the Connectivity pane of the Node window select the port to which the link station is being added.

   b. Click the **New** button in the button bar.

   c. Click the **OK** button and enter appropriate values in the fields of the Enterprise Extender (HPR/IP) Link Station Configuration dialog shown in Figure 57.



Name: IPL0
SNA port name...: IPP0
Activation: On node startup

Independent LU traffic
Remote node...: USIBMRA . RS60004
Remote node type: Network node

Contact information
Remote IP host name: rs60004

Description: Enterprise Extender Link to NN

Figure 57. IP link station dialog box

You need the following information:

Link station name This is a name to identify the link station locally. It can be up to eight characters.

SNA port name By default CS/AIX enters the name of the port selected in the connectivity pane.

Activation method This indicates how and when the link station is to be activated. The possible values are by administrator, on node startup, or on demand.

Remote node CP NETNAME.CPNAME. Optional. Can be used as a validity check to make sure the link goes to the expected node.

Remote node type Network node, end node, or discover.

Remote IP host name To configure a selective link station enter the IP hostname or dotted-decimal IP address of the remote station.

Advanced parameters In most cases you can use the default settings for these parameters, so you do not need to alter the settings in the advanced dialog.

d. Click the **OK** button and the link station will appear beneath the port to which it belongs in the Connectivity pane of the Node window.

Note that Enterprise Extender links support only independent LU traffic. That means that if dependent LUs must be supported, DLUR must be configured on the CS/AIX node.

6.4 Scenario

For this section we used the following equipment:

- Two RS/6000s running AIX Version 4.3.3.0 with the latest maintenance level, and *Communications Server for AIX, Version 6*
- A PC running Windows NT and IBM Personal Communications for Windows NT*,* Version 4.3 (PCOMM)
- A host running CS for OS/390

We used DLUR to show that Enterprise Extender provides a mechanism for transporting SNA protocols over the IP network.

DLUR is an APPN feature that allows dependent LU sessions without a direct connection to a host. The Dependent LU Requester (DLUR) communicates with a Dependent LU Server (DLUS) over an APPN network. DLUR must be available on the node where the LUs are located but DLUR is not required on any intermediate nodes in the session route.

By using HPR/IP links, the session route between DLUR and DLUS will take place in an IP network but taking advantage of APPN features such as HPR. Sessions between DLUR and DLUS will be routed over an RTP connection.

The following configuration steps are required for this scenario:

1. Configure EE support on the rs60003 machine including DLUR
2. Configure EE support on the rs60004 machine
3. Activate CS/AIX resources on both nodes

4. Configure EE support in VTAM and TCP/IP on the host
5. Test the EE connections using PCOMM

The test scenario is shown in Figure 58. Refer to this figure when reviewing the following configuration steps.

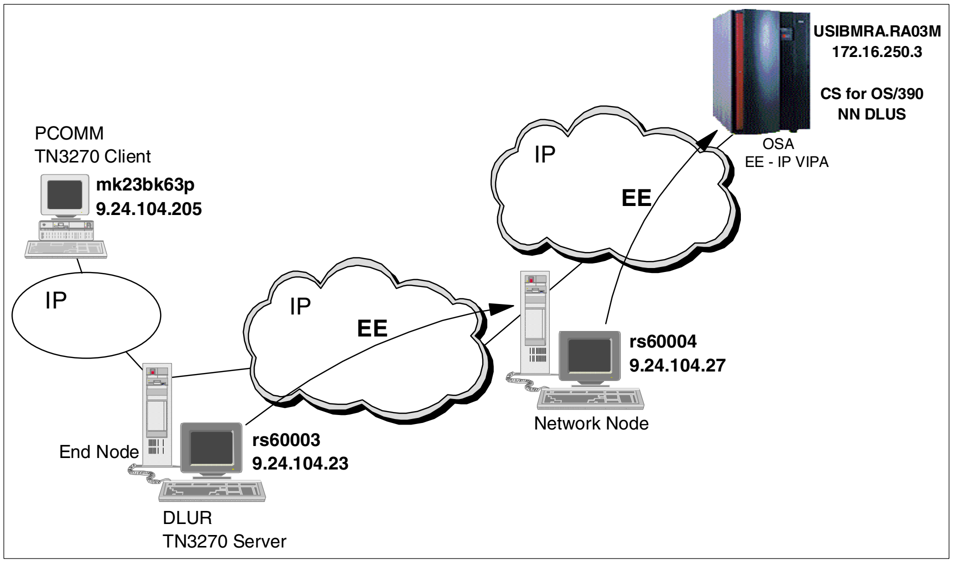
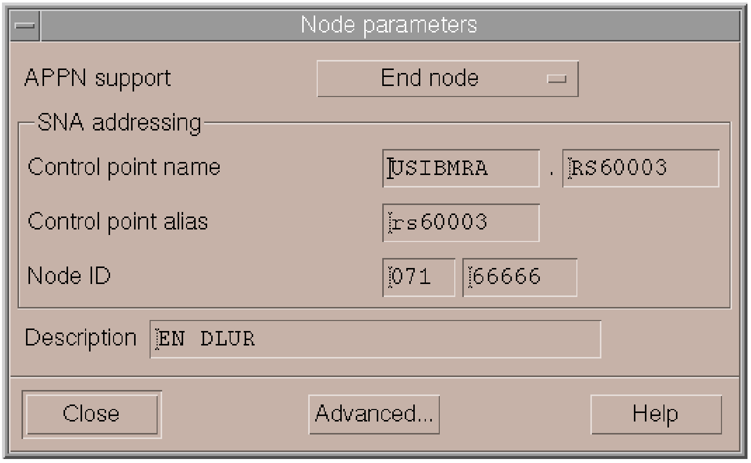


Figure 58. Test scenario

6.4.1 Configure the rs60003 machine

On the rs60003 machine:

1. Configure the node as an End Node, as shown in Figure 59.


Node parameters

APPN support: End node

SNA addressing

Control point name: USIBMRA . RS60003

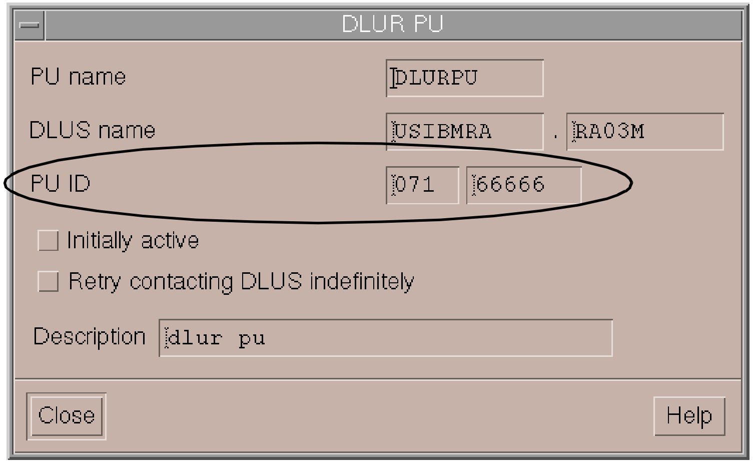
Control point alias: rs60003

Node ID: 071 66666

Description: EN DLUR

Figure 59. Configuration of rs60003 EN

2. Define a DLUR PU. Click **Services** -> **Connectivity** -> **New DLUR PU.**


DLUR PU

PU name: DLURPU

DLUS name: USIBMRA . RA03M

PU ID: 071 66666

□ Initially active

□ Retry contacting DLUS indefinitely

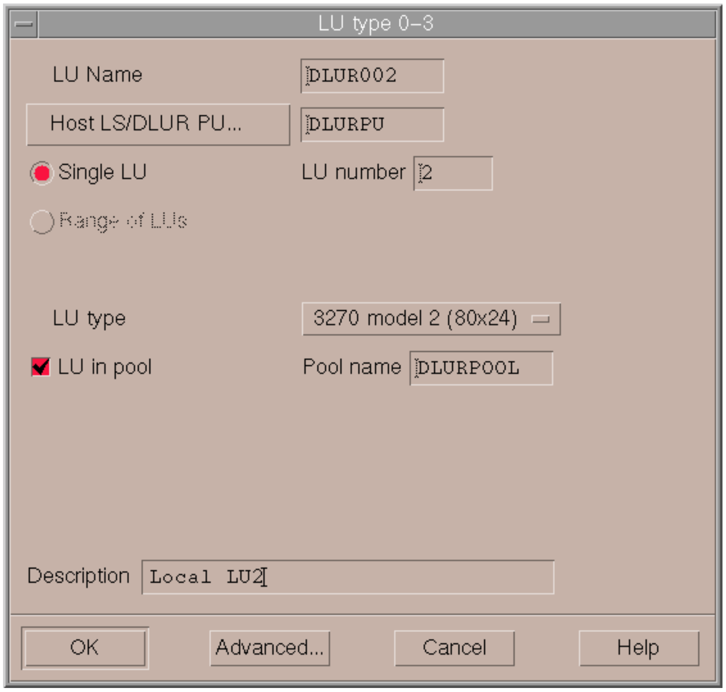
Description: dlur pu

Figure 60. Definition of DLUR PU

The DLUR PU ID that you enter here must match the ID by which the PU is defined within the VTAM configuration.

For assistance configuring the DLUR PU refer to *IBM Communications Server for AIX Quick Beginnings, Version 6,* GC31-8583 and *IBM Communications Server for AIX Administration Guide, Version 6,* SC31-8586.

3. Define the Dependent LUs



LU type 0–3

LU Name: DLUR002

Host LS/DLUR PU...: DLURPU

● Single LU — LU number: 2

○ Range of LUs

LU type: 3270 model 2 (80x24)

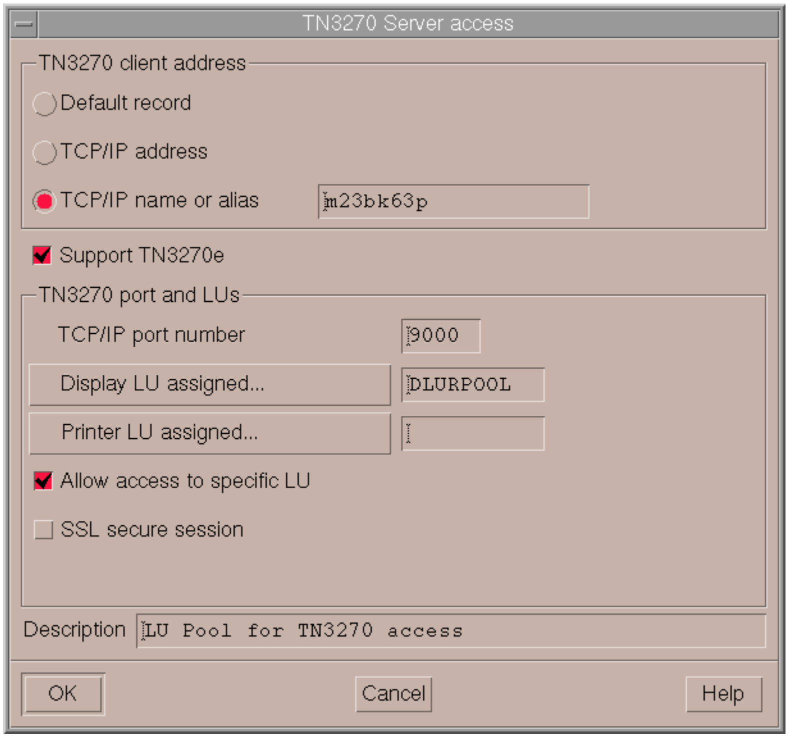
☑ LU in pool — Pool name: DLURPOOL

Description: Local LU2

Figure 61. Definition of dependent LUs

For assistance configuring Dependent LUs refer to *IBM Communications Server for AIX Quick Beginnings, Version 6,* SC31-8583 and *IBM Communications Server for AIX Administration Guide, Version 6,* SC31-8586.

4. Configure the TN3270 server access records. Click **Services** -> **TN Server** -> **TN Server...**



TN3270 Server access

TN3270 client address

○ Default record

○ TCP/IP address

● TCP/IP name or alias: m23bk63p

☑ Support TN3270e

TN3270 port and LUs

TCP/IP port number: 9000

Display LU assigned...: DLURPOOL

Printer LU assigned...:

☑ Allow access to specific LU

□ SSL secure session

Description: LU Pool for TN3270 access

Figure 62. TN3270 server access

The LU Pool assigned for access by the TN3270 client contains the dependent LUs defined to DLUR. Port 9000 was chosen as the TN Server port.

For more information on TN3270 refer to *IBM Communications Server for AIX Quick Beginnings, Version 6,* GC31-8583 and *IBM Communications Server for AIX Administration Guide, Version 6,* SC31-8586.

5. Configure HPR/IP connectivity to the rs60004 NN as shown in Figure 56 on page 90 and Figure 57 on page 91.

   The definition of the port adds the following define_ip_dlc and define_ip_port sections to the /etc/sna/sna_node.cfg file:

   ```
    [define_ip_dlc]
   dlc_name = IP0
   description = ""
   initially_active = NO
   udp_port_llc = 12000
   udp_port_network = 12001
   ```

```
udp_port_high = 12002
udp_port_medium = 12003
udp_port_low = 12004
ip_precedence_llc = 6
ip_precedence_network = 6
ip_precedence_high = 4
ip_precedence_medium = 2
ip_precedence_low = 1

[define_ip_port]
port_name = IPP0
description = HPR/IP Port
determined_ip_address = 9.24.104.23
lsap_address = 0x04
dlc_name = IP0
initially_active = YES
max_rcv_btu_size = 1500
tot_link_act_lim = 4096
inb_link_act_lim = 0
out_link_act_lim = 0
act_xid_exchange_limit = 9
nonact_xid_exchange_limit = 5
max_ifrm_rcvd = 7
target_pacing_count = 7
max_send_btu_size = 1500
implicit_cp_cp_sess_support = YES
implicit_limited_resource = NO
implicit_deact_timer = 30
implicit_uplink_to_en = NO
effect_cap = 3993600
connect_cost = 0
byte_cost = 0
security = SEC_NONSECURE
prop_delay = PROP_DELAY_LAN
user_def_parm_1 = 128
user_def_parm_2 = 128
user_def_parm_3 = 128
local_ip_interface = ""
react_timer = 30
react_timer_retry = 65535
ack_timeout = 2000
max_retry = 10
liveness_timeout = 2000
short_hold_mode = NO
```

Note: When you use Motif Administration to define a port for a particular link protocol, CS/AIX automatically defines a DLC for the port if a DLC of that type has not already been defined. For command-line configuration, you must define the port and DLC using different commands.

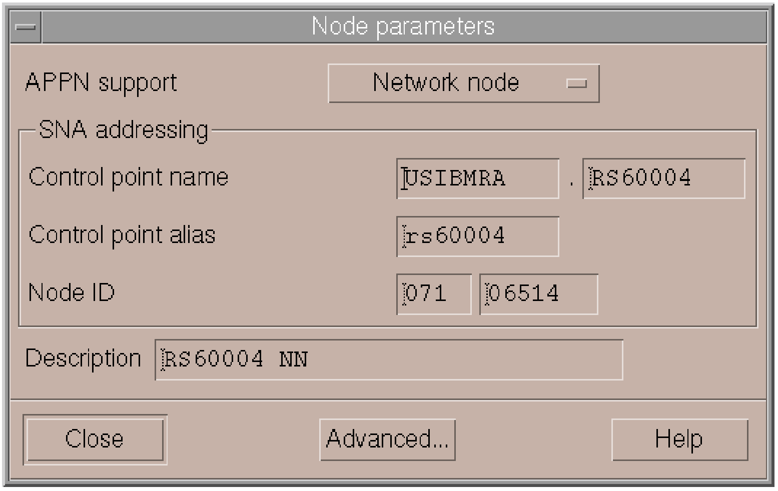
The define_ip_ls section in the /etc/sna/sna_node.cfg file looks like this:

```
[define_ip_ls]
ls_name = IPL0
description = EE Link to NN rs60004
port_name = IPP0
adj_cp_name = USIBMRA.RS60004
adj_cp_type = NETWORK_NODE
max_send_btu_size = 1500
ls_attributes = SNA
cp_cp_sess_support = YES
default_nn_server = YES
lsap_address = 0x04
determined_ip_address = 9.24.104.27
auto_act_supp = NO
tg_number = 0
limited_resource = NO
disable_remote_act = NO
link_deact_timer = 30
use_default_tg_chars = YES
effect_cap = 3993600
connect_cost = 0
byte_cost = 0
security = SEC_NONSECURE
prop_delay = PROP_DELAY_LAN
user_def_parm_1 = 128
user_def_parm_2 = 128
user_def_parm_3 = 128
target_pacing_count = 7
max_ifrm_rcvd = 0
branch_link_type = NONE
adj_brnn_cp_support = ALLOWED
initially_active = YES
restart_on_normal_deact = NO
react_timer = 30
react_timer_retry = 65535
remote_ip_host = rs60004
ack_timeout = 2000
max_retry = 10
liveness_timeout = 2000
short_hold_mode = NO
```

In the previous two listing examples from the /etc/sna/sna_node.cfg file, the determined_ip_address is recalculated from the local_ip_interface field every time a define_ip_port verb is issued or when the node is started.

6.4.2 Configure the rs60004 machine

1. Configure the node as a network node as shown in Figure 63.



Node parameters

APPN support: Network node

SNA addressing

Control point name: USIBMRA . RS60004

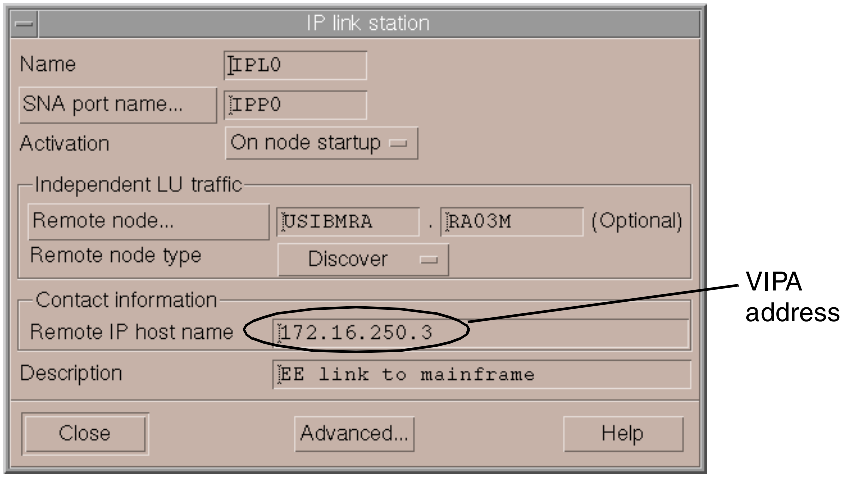
Control point alias: rs60004

Node ID: 071 06514

Description: RS60004 NN

Figure 63. Configuration of rs60004 NN

2. Configure an HPR/IP port. Note that since there is only one physical attachment to the token-ring LAN, only one port definition is required, even though we will define two HPR/IP links on this port.
3. Configure two HPR/IP links: one to the host USIBMRA.RA03M, and one to the DLUR node, rs60003. Figure 64 shows the link definition to host USIBMRA.RA03M.



IP link station

Name: IPL0

SNA port name...: IPP0

Activation: On node startup

Independent LU traffic

Remote node...: USIBMRA . RA03M (Optional)

Remote node type: Discover

Contact information

Remote IP host name: 172.16.250.3

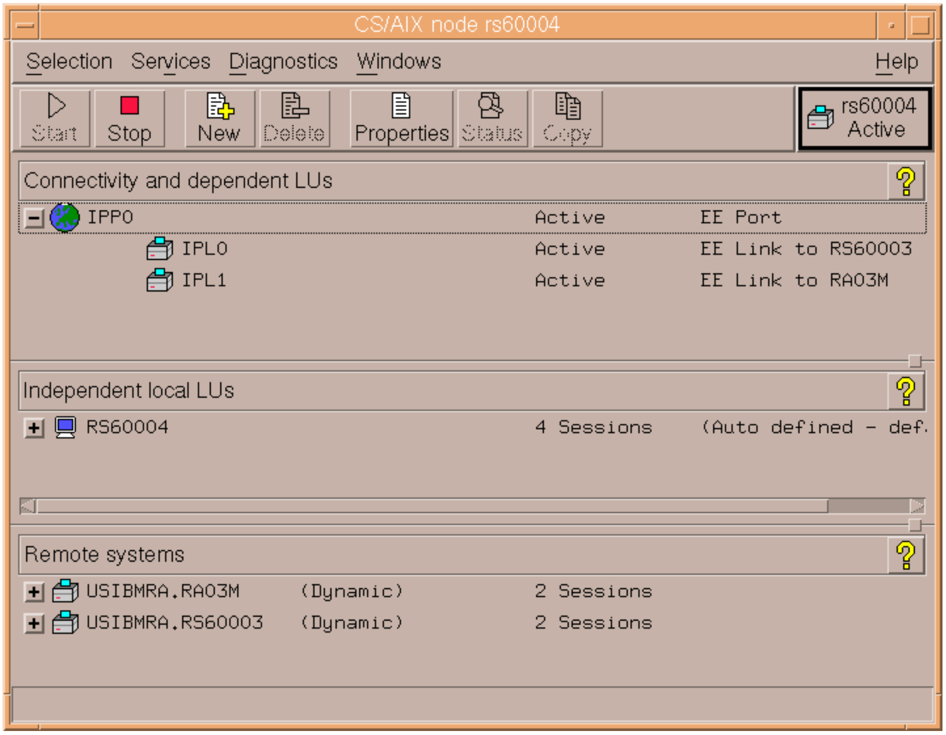
Description: EE link to mainframe

VIPA address

Figure 64. Link station dialog box for link to USIBMRA.RA03M

Note that the IP address used to define the remote VTAM host must be a VIPA address for the host. VIPA is discussed in more detail in “TCP/IP profile” on page 102.

Figure 65 shows that link IPL0 defines the link to the host while link IPL1 defines the link to rs60003.



```
Connectivity and dependent LUs
IPP0                                  Active     EE Port
    IPL0                              Active     EE Link to RS60003
    IPL1                              Active     EE Link to RA03M

Independent local LUs
RS60004                               4 Sessions   (Auto defined - def.

Remote systems
USIBMRA.RA03M      (Dynamic)          2 Sessions
USIBMRA.RS60003    (Dynamic)          2 Sessions
```

Figure 65. HPR/IP link definitions on host RS60004

6.4.3 Activate CS/AIX resources on both nodes

On both rs60003 and rs60004, activate the EE links. The EE link on rs60004 that connects to the host will not become active until the required VTAM EE definitions have been completed there.

6.4.4 Configure VTAM and TCP/IP on the host

There are four places on the host that will require configuration for EE link support:

1. Additional definitions in the TCP/IP profile (“TCP/IP profile” on page 102)
2. Additional parameters in the VTAM ATCSTRxx startup member (“VTAM ATCSTRxx” on page 102)
3. VTAM switched major node (“VTAM switched major node” on page 103)
4. VTAM XCA major node (“VTAM XCA major node” on page 104)

6.4.4.1 TCP/IP profile

Definition statements are required in the TCP/IP profile to define VTAM-to-TCP/IP communication within the host. These statements are shown in Figure 66.

```
IPCONFIG  SOURCEVIPA 1
;
; *********************************************************
;      Enterprise Extender Device
; *********************************************************
 DEVICE IUTSAMEH MPCPTP 2
 LINK   IUTSAMEH MPCPTP  IUTSAMEH
 START  IUTSAMEH
;
; *********************************************************
;      Virtual IP Address Definition
; *********************************************************
  DEVICE VIPA3A   VIRTUAL     0 3
  LINK   VIPA3A   VIRTUAL     0     VIPA3A
;
HOME 4
   172.16.250.3     VIPA3A      ; 1st VIPA Link 5
   172.16.250.254   IUTSAMEH    ; EE
```

Figure 66. TCP/IP profile data for VTAM EE

Defining the `IPCONFIG SOURCEVIPA` (1) parameter results in TCP/IP including the host VIPA address (virtual IP address) as the source IP address for all outbound datagrams. Note that VIPA is required for VTAM support of Enterprise Extender.

A series of `DEVICE`, `LINK` and `START` statements (2) is required to define a multipath channel point-to-point device (MPCPTP) for VTAM-to-TCP/IP communication. The `DEVICE` statement uses the reserved TRLE (Transport Resource List Entry) name, IUTSAMEH, for the Enterprise Extender connection to VTAM on this host. When defining an EE connection on a host, the device name must be IUTSAMEH. VTAM activates the IUTSAMEH TRLE automatically. The `LINK` statement contains a link name, MPCPTP, and the reserved device name IUTSAMEH. The `START` statement starts the device. This link must be active before VTAM can establish any EE connections. The VIPA definitions (3) and `HOME` (4) statement are used by VTAM when it is represented as an EE node. This address (5) may also be defined in the VTAM START options if there is more than one VIPA address defined to TCP/IP.

6.4.4.2 VTAM ATCSTRxx

Changes may be required to the VTAM ATCSTRxx start list. See Figure 67.

```
..........
HOSTPU=ISTPUS03,
HOSTSA=03,
HPR=RTP,
NETID=USIBMRA,
NODETYPE=NN,
SSCPID=03,
SSCPNAME=RA03M,
IPADDR=172.16.250.3,
..........
..........
```

Figure 67. VTAM ATCSTRxx start options for RA03M

The IPADDR parameter in ATCSTRxx specifies the VIPA address of the local TCP/IP stack. If you have only one VIPA address defined in your TCP/IP stack, then this parameter is not required. If multiple VIPA addresses are defined in TCP/IP, use IPADDR to specify which VIPA address you want other EE nodes to use in order to communicate with this VTAM host. If IPADDR is not specified, it will default to the first VIPA address in the local TCP/IP stack's HOME list. See **5** on Figure 66 on page 102.

6.4.4.3 VTAM switched major node

VTAM uses a switched major node to define an adjacent APPN node attached via an EE HPR/IP connection. See Figure 68.

```
RA3R6EES VBUILD TYPE=SWNET
PRS60004 PU     CONNTYPE=APPN,
                CPCP=YES,
                CPNAME=RS60004,
                HPR=YES,
                ISTATUS=ACTIVE,
                LUGROUP=RS6KLU1,
                LUSEED=RS6KD##,
                PUTYPE=2
PTS60004 PATH   GRPNM=R6EEGRP,
                IPADDR=9.24.104.27,
                SAPADDR=8,
                IPRESOLV=90
```

Figure 68. VTAM switched major node for rs6004 EE connection

We define all the required APPN parameters, such as CPCP, CPNAME and HPR, on the PU statement.

The PATH statement following the PU statement is used to define a path to the physical unit (rs60004) defined by this switched major node. The IPADDR keyword specifies the IP address for rs60004 used for dial-out connections.

The GRPNM keyword on the PATH statement ties to the XCA major node discussed next. In our example, GRPNM=R6EEGRP matches the name on the XCA GROUP statement. See Figure 69.

6.4.4.4 VTAM XCA major node

A VTAM external communications adapter (XCA) major node defines VTAM’s connection to a shared access transport facility (SATF) such as:

- Local area networks (LANs)
- Asynchronous transfer mode (ATM) networks
- Enterprise Extender (EE) networks

Figure 69 shows the XCA major node coding required to define a connection to our EE sample network.

For EE connections, MEDIUM=HPRIP must be coded on the PORT statement.

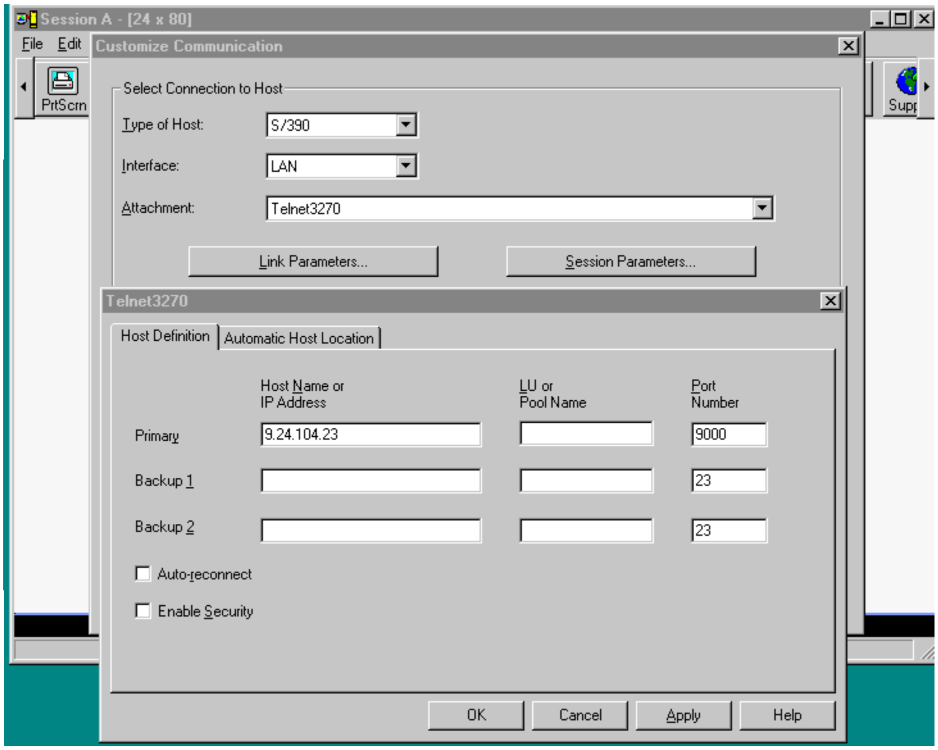
The name on the GROUP statement (R6EEGRP) is referenced by the GRPNM parameter on the PATH statement in the associated switched major node.

```
RA3R6EE  VBUILD TYPE=XCA
R6EEPORT PORT  MEDIUM=HPRIP,
               IPPORT=12000,
               SAPADDR=4
R6EEGRP  GROUP DIAL=YES
R6EELN1  LINE  CALL=INOUT
R6EEPU1  PU
R6EELN2  LINE  CALL=INOUT
R6EEPU2  PU
R6EELN3  LINE  CALL=INOUT
R6EEPU3  PU
R6EELN4  LINE  CALL=INOUT
R6EEPU4  PU
```

Figure 69. VTAM XCA major node for rs60004 EE connection

6.4.5 Test the connection

On our test machine, we started a TN3270 session to the host using IBM Personal Communications for Windows NT (PCOMM).



Select Connection to Host

Type of Host: S/390

Interface: LAN

Attachment: Telnet3270

	Host Name or IP Address	LU or Pool Name	Port Number
Primary	9.24.104.23		9000
Backup 1			23
Backup 2			23

□ Auto-reconnect

□ Enable Security

Figure 70. PCOMM TN3270 session configuration

The PCOMM configuration panels displayed in Figure 70 show that we defined a TN3270 client session to connect to the CS/AIX TN3270 server running on rs60003 at 9.24.104.23. The TN3270 server was configured to use DLUR dependent LUs to complete the connection to DLUS running on the host.

6.5 Verifying the HPR/IP connection

To show the establishment of the RTP connection, we enabled logging in the RS/6000 machine, node rs60003. From the main window select **Diagnostics** -> **Logging** -> **Log audit messages** -> **succint**.

The audit file sna.aud is created in /var/sna/sna.aud.

The sequence of events were as follows:

1. With SNA resources active in rs60004 (port and link stations) we started the node rs60003. From the audit file:

```
============ Log file initialized 10:49:50 EDT  28 Apr 2000 ============
10:49:50 EDT  28 Apr 2000 4097-32(1-1) A (rs60003) PID 13164 (snacfgdae)
Configuration file /etc/sna/sna_domn.cfg updated.
New revision level = 6
10:49:52 EDT  28 Apr 2000 512-252(0-10) A (rs60003)
Node started.
CP name (Alias)     = USIBMRA.RS60003   (rs60003 )
Node type           = 03
Node info           = CS/AIX 6.0.0
10:49:53 EDT  28 Apr 2000 4097-72(1-1) A (rs60003) PID 13164 (snacfgdae)
Held Alert Handler successfully initialized.
Held Alert File is /var/sna/heldalrt.dat
```

2. The IP port and IP link station were configured to activate automatically on node startup.

```
10:49:53 EDT  28 Apr 2000 512-117(0-10) A (rs60003)
DLC started.
DLC name            = IP0
10:49:53 EDT  28 Apr 2000 4099-18(221-1) A (rs60003) PID 15602
(snadaemon)
New Stream created between /dev/snahprip and /dev/sna_v5router (Stream
identifier 0x700cde00).
10:49:53 EDT  28 Apr 2000 16432-5(0-10) A (rs60003)
G-SNA DLC created.
10:49:53 EDT  28 Apr 2000 512-117(0-10) A (rs60003)
DLC started.
DLC name            = $GSNA$
10:49:53 EDT  28 Apr 2000 4099-18(221-1) A (rs60003) PID 15602
(snadaemon)
New Stream created between /dev/snahprip and /dev/sna_v5router (Stream
identifier 0x700cd600).
10:49:53 EDT  28 Apr 2000 512-119(0-10) A (rs60003)
Port started.
DLC name            = IP0
Port name           = IPP0
10:49:53 EDT  28 Apr 2000 512-119(0-10) A (rs60003)
Port started.
DLC name            = $GSNA$
Port name           = $GSNA$
10:49:53 EDT  28 Apr 2000 4099-18(221-1) A (rs60003) PID 15602
(snadaemon)
New Stream created between /dev/snahprip and /dev/sna_v5router (Stream
identifier 0x700c9000).
10:49:53 EDT  28 Apr 2000 1-9(1-10) A (rs60003)
The Node’s configuration has been successfully loaded.
```

```
10:49:53 EDT  28 Apr 2000 512-115(0-10) A (rs60003)
HPR-capable link station started.
Port name                 = IPP0
LS name                   = IPL0
Adjacent CP name          = USIBMRA.RS60004
Adjacent CP type          = 02
TG number                 = 21
Last TG number            = 0
ANR Label                 = 90FF
Link level error recovery = 00
Adjacent RTP support      = 01
```

The above information is a result of the XID3 negotiation during the link activation.

3. After the link setup, both nodes set up the CP-CP sessions (two sessions). And because the link is an HPR/IP link, the CP-CP sessions flow over an RTP connection with COS CPSVCMG. Notice that both sessions use the same RTP connection.

```
10:49:53 EDT  28 Apr 2000 512-726(0-10) A (rs60003)
Adjacent CP contacted.
Adjacent CP name = USIBMRA.RS60004
10:49:53 EDT  28 Apr 2000 512-660(0-10) A (rs60003)
RTP Connection has been established.
Connection name  = @R000001
Partner name     = RS60004
COS name         = CPSVCMG
Local TCID       = 0000000001000000
Remote TCID      = 0000000004000000
10:49:53 EDT  28 Apr 2000 512-307(0-10) A (rs60003)
LU6.2 session activated.
Local LU (Alias)   = USIBMRA.RS60003   (rs60003 )
Partner LU (Alias) = USIBMRA.RS60004   (@I000001)
Mode name          = CPSVCMG
Session identifier = F25FB4F4803F407A
Session polarity   = 02
Session type       = 01
LS name            = @R000001
LFSID              = 02000000
10:49:53 EDT  28 Apr 2000 512-307(0-10) A (rs60003)
LU6.2 session activated.
Local LU (Alias)   = USIBMRA.RS60003   (rs60003 )
Partner LU (Alias) = USIBMRA.RS60004   (@I000001)
Mode name          = CPSVCMG
Session identifier = F25FB3F4803F18C9
Session polarity   = 03
Session type       = 02
```

```
LS name            = @R000001
LFSID              = 02000001
10:49:53 EDT  28 Apr 2000 512-727(1-10) A (rs60003)
CP-CP sessions established.
Adjacent CP name = USIBMRA.RS60004
1015 compliant   = 3
Topology awareness of CP-CP sessions support = 01
CP Capabilities :
000C12C1 00000000 E2844000
```

The above message indicates that the BIND for the CP-CP session has started and the CP capabilities have been exchanged.

4. The DLURPU was activated. Information about the best possible HPR route for the sessions that will follow is collected by the Route_Setup command:

```
10:50:00 EDT  28 Apr 2000 512-660(0-10) A (rs60003)
RTP Connection has been established.
Connection name  = @R000003
Partner name     = RS60004
COS name         = RSETUP
Local TCID       = 0000000003000000
Remote TCID      = 0000000005000000
```

5. Next, the RTP connections used to carry the CP-CP sessions between the DLUR and the DLUS (mode CPSVRMGR) are started.

```
10:50:00 EDT  28 Apr 2000 512-660(0-10) A (rs60003)
RTP Connection has been established.
Connection name  = @R000002
Partner name     = RA03M
COS name         = SNASVCMG
Local TCID       = 0000000002000000
Remote TCID      = 31818CC10000016C
10:50:00 EDT  28 Apr 2000 512-307(0-10) A (rs60003)
LU6.2 session activated.
Local LU (Alias)   = USIBMRA.RS60003   (rs60003 )
Partner LU (Alias) = USIBMRA.RA03M     (@I000002)
Mode name          = CPSVRMGR
Session identifier = F25FB4F4803F407D
Session polarity   = 02
Session type       = 01
LS name            = @R000002
LFSID              = 02000000
10:50:00 EDT  28 Apr 2000 512-660(0-10) A (rs60003)
RTP Connection has been established.
Connection name  = @R000004
Partner name     = RA03M
```

```
COS name         = SNASVCMG
Local TCID       = 0000000004000000
Remote TCID      = 31818CC300000195
10:50:00 EDT  28 Apr 2000 512-307(0-10) A (rs60003)
LU6.2 session activated.
Local LU (Alias)   = USIBMRA.RS60003   (rs60003 )
Partner LU (Alias) = USIBMRA.RA03M     (@I000002)
Mode name          = CPSVRMGR
Session identifier = C7335B7CB30EA363
Session polarity   = 03
Session type       = 02
LS name            = @R000004
LFSID              = 02000001
```

6. The SSCP-PU and SSCP-LU sessions between DLUS and DLUR get established; see Figure 71 on page 110.

```
10:50:00 EDT  28 Apr 2000 512-592(0-10) A (rs60003)
A pipe to a DLUS has activated
DLUS name                    = USIBMRA.RA03M
DLUS persistent pipe support = 02
Persistent pipe active       = 00
10:50:00 EDT  28 Apr 2000 512-740(0-10) A (rs60003)
A PU-SSCP session has been activated.
PU name = DLURPU
10:50:00 EDT  28 Apr 2000 512-560(0-10) A (rs60003)
An LU-SSCP session has been activated for LU type 0, 1, 2, or 3.
PU name                = DLURPU
NAU address            = 02
LU name                = DLUR002
10:50:00 EDT  28 Apr 2000 512-560(0-10) A (rs60003)
An LU-SSCP session has been activated for LU type 0, 1, 2, or 3.
PU name                = DLURPU
NAU address            = 03
LU name                = DLUR003
10:50:00 EDT  28 Apr 2000 512-560(0-10) A (rs60003)
An LU-SSCP session has been activated for LU type 0, 1, 2, or 3.
PU name                = DLURPU
NAU address            = 04
LU name                = DLUR004
```

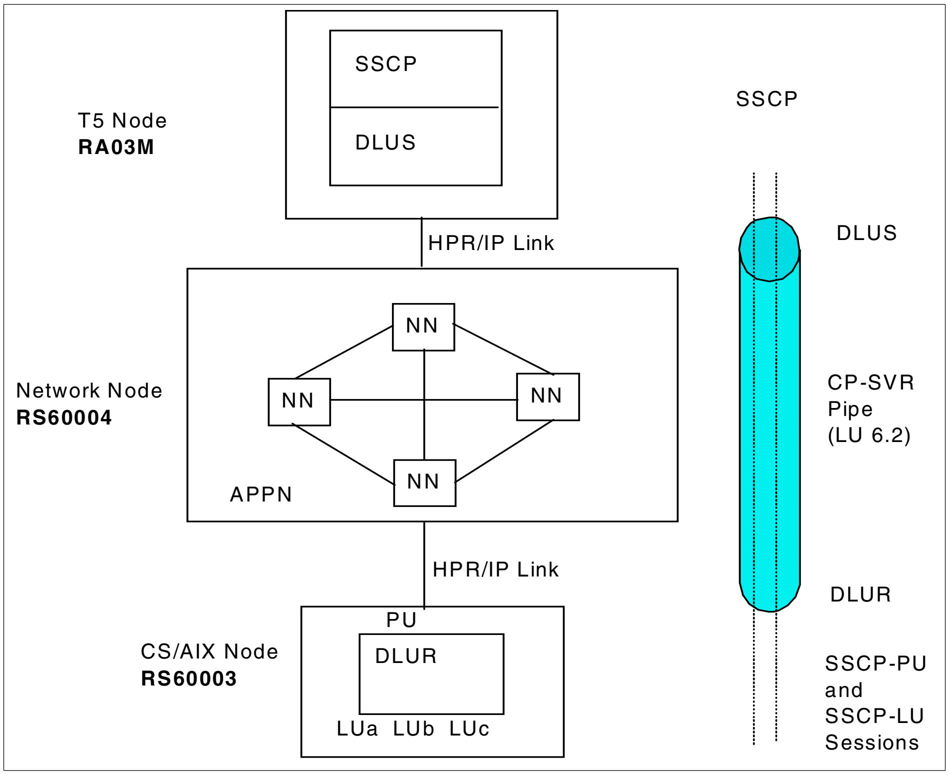
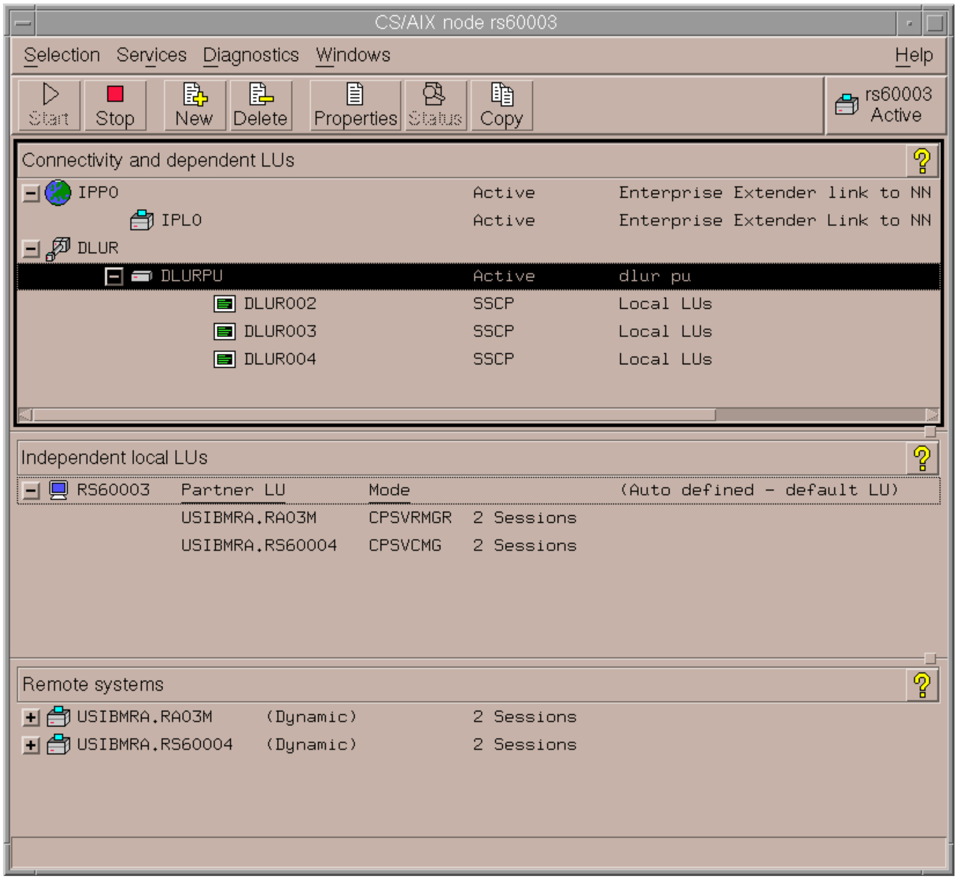


Figure 71. DLUR

A GUI representation of the above situation can be found in Figure 72 on page 111.



```
Connectivity and dependent LUs
IPP0                           Active     Enterprise Extender link to NN
        IPL0                   Active     Enterprise Extender Link to NN
DLUR
        DLURPU                 Active     dlur pu
                DLUR002        SSCP       Local LUs
                DLUR003        SSCP       Local LUs
                DLUR004        SSCP       Local LUs

Independent local LUs
RS60003    Partner LU         Mode                 (Auto defined - default LU)
           USIBMRA.RA03M      CPSVRMGR   2 Sessions
           USIBMRA.RS60004    CPSVCMG    2 Sessions

Remote systems
USIBMRA.RA03M      (Dynamic)         2 Sessions
USIBMRA.RS60004    (Dynamic)         2 Sessions
```

Figure 72. SNA window on rs60003 after activation of DLUR and HPR/IP link to NN

7. Finally a TN3270 session was started from the client. The session uses an available LU in the pool.

```
10:50:19 EDT  28 Apr 2000 4102-50(0-1) A (rs60003) PID 16324
(snatnsrvr_mt)
Client 2 opened to port 9000 using socket 25
Client address = 9.24.104.205
10:50:19 EDT  28 Apr 2000 4102-54(0-1) A (rs60003) PID 16324
(snatnsrvr_mt)
Client 9.24.104.205:1122[2]: assigned LU DLUR002 .
```

8. The SNA APPC application <`aping`> was also used to show Enterprise Extender functionality over IP connections.

   Using `aping usibmra.rs60004` from rs60003 logged the following information:

```
10:50:37 EDT  28 Apr 2000 8195-6(0-1) A (rs60003) PID 21726 (aping)
Unknown CPI-C symbolic destination name (4150494e47442020) specified.
10:50:37 EDT  28 Apr 2000 8193-8(213-1) A (rs60003) PID 21726 (aping)
APPC invoking TP started.
TP ID   = 0000000001000000
TP name =
c3d7c9c36dc4c5c6c1e4d3e36de3d7d5c1d4c54040404040404040404040404040404040404
04040404040404040404040404040404040404040404040404040404040
10:50:37 EDT  28 Apr 2000 8195-0(0-1) A (rs60003) PID 21726 (aping)
New TP instance started for CPI-C.  TP id = 00000000
10:50:37 EDT  28 Apr 2000 512-660(0-10) A (rs60003)
RTP Connection has been established.
Connection name  = @R000005
Partner name     = RS60004
COS name         = SNASVCMG
Local TCID       = 0000000005000000
Remote TCID      = 0000000008000000
10:50:37 EDT  28 Apr 2000 512-307(0-10) A (rs60003)
LU6.2 session activated.
Local LU (Alias)   = USIBMRA.RS60003   (rs60003 )
Partner LU (Alias) = USIBMRA.RS60004   (@I000001)
Mode name          = SNASVCMG
Session identifier = F25FB4F4803F4080
Session polarity   = 02
Session type       = 01
LS name            = @R000005
LFSID              = 02000000
10:50:37 EDT  28 Apr 2000 512-32(0-10) A (rs60003)
Session limits changed.
Local LU (Alias)             = USIBMRA.RS60003   (rs60003 )
Partner LU (Alias)           = USIBMRA.RS60004   (@I000001)
Mode name                    = #INTER
New session limit            = 8
Min. contention winner limit = 4
Min. contention loser limit  = 4
Termination count            = 0
10:50:37 EDT  28 Apr 2000 512-660(0-10) A (rs60003)
RTP Connection has been established.
Connection name  = @R000006
Partner name     = RS60004
COS name         = #INTER
Local TCID       = 0000000006000000
Remote TCID      = 0000000009000000
10:50:37 EDT  28 Apr 2000 512-307(0-10) A (rs60003)
LU6.2 session activated.
Local LU (Alias)   = USIBMRA.RS60003   (rs60003 )
Partner LU (Alias) = USIBMRA.RS60004   (@I000001)
```

```
Mode name          = #INTER
Session identifier = F25FB4F4803F4082
Session polarity   = 02
Session type       = 01
LS name            = @R000006
LFSID              = 02000000
10:50:37 EDT  28 Apr 2000 8195-2(0-1) A (rs60003) PID 21726 (aping)
New CPI-C conversation started. CPI-C conversation ID = 0100000100000000
10:50:38 EDT  28 Apr 2000 8195-3(0-1) A (rs60003) PID 21726 (aping)
CPI-C conversation deallocated. CPI-C conversation ID = 0100000100000000
```

Note: The RTP connection with COS SNASVCMG is established to perform a CNOS (Change Number of Sessions) for mode #INTER, after which the RTP connection that carries the actual #INTER session (aping session) is started.

Chapter 7. Branch Extender

This chapter describes the functionality of Branch Extender and how it is configured, and an example scenario illustrates the use of Branch Extender in combination with HPR.

7.1 Overview

As the name implies, Branch Extender is designed for networks that can be divided into distinct areas, such as separate branches of a large organization. It works by separating out branch offices from the main APPN WAN backbone network, for example, the organization's headquarters network.

Each branch contains a node of the type called branch network node (BrNN), which combines the functions of an APPN network node and an APPN end node.

To the backbone network, the BrNN appears as an end node, connected to its network node server (NNS) in the backbone network. Because the BrNN appears as an end node, it does not receive topology information from the backbone network (topology information is transmitted only between network nodes).

The BrNN registers all resources in the branch with its NNS as though they were located on the BrNN itself.This means that the nodes in the backbone network can locate resources in the branch without having to be aware of the separate nodes in the branch, thus reducing the amount of topology information that must be stored. While a BrNN knows the topology of its local branch, it knows nothing of the uplink topology.

To the branch network, the BrNN appears as a network node, acting as the NNS for end nodes in the branch. Each node in the branch sees the rest of the network as being connected through its NNS, in the same way as for a standard NNS. When the BrNN can't resolve a request for network services locally, it refers the request to its NNS, which connects to other NNs using normal CP-CP sessions. This can be thought of as default routing. That is why a BrNN's uplink to its NNS may be called the "default routing link".

For directory services purposes, the BrNN appears to own all branch resources. For route selection purposes, the BrNN appears to be the origin or destination of all sessions involving branch LUs.

The Branch Extender feature of APPN is illustrated in Figure 73 and Figure 74.

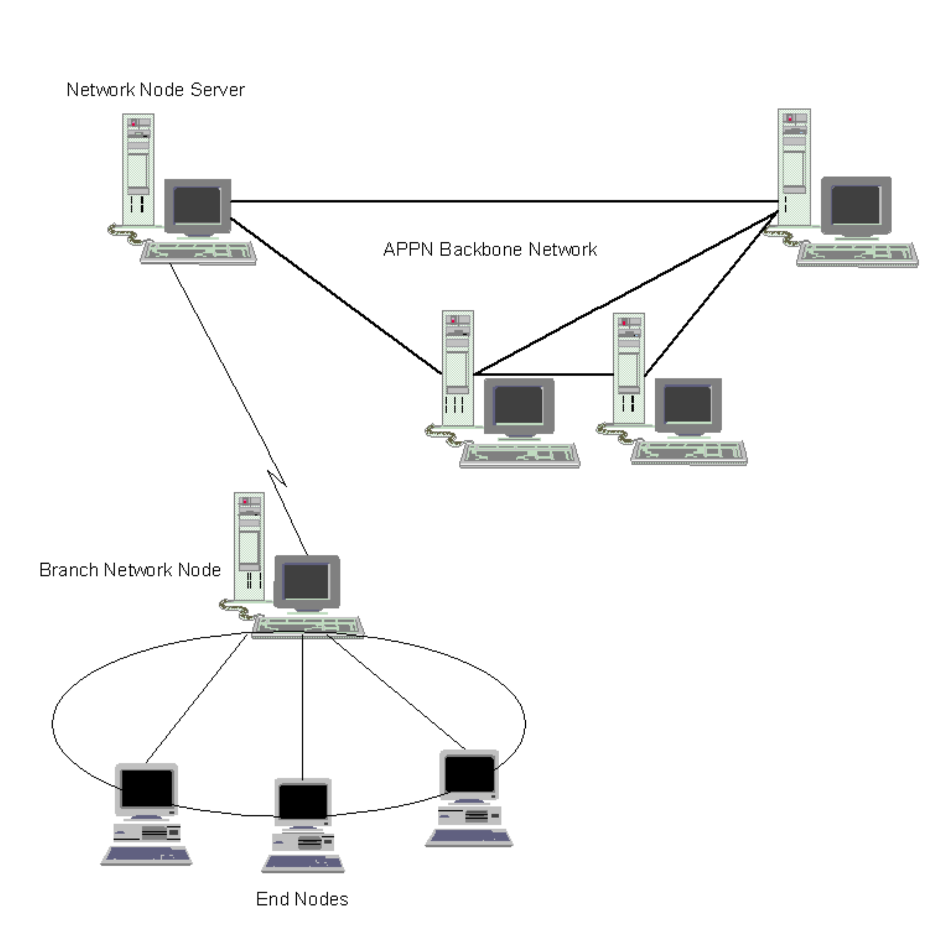


Figure 73. Sample “branched” network 1

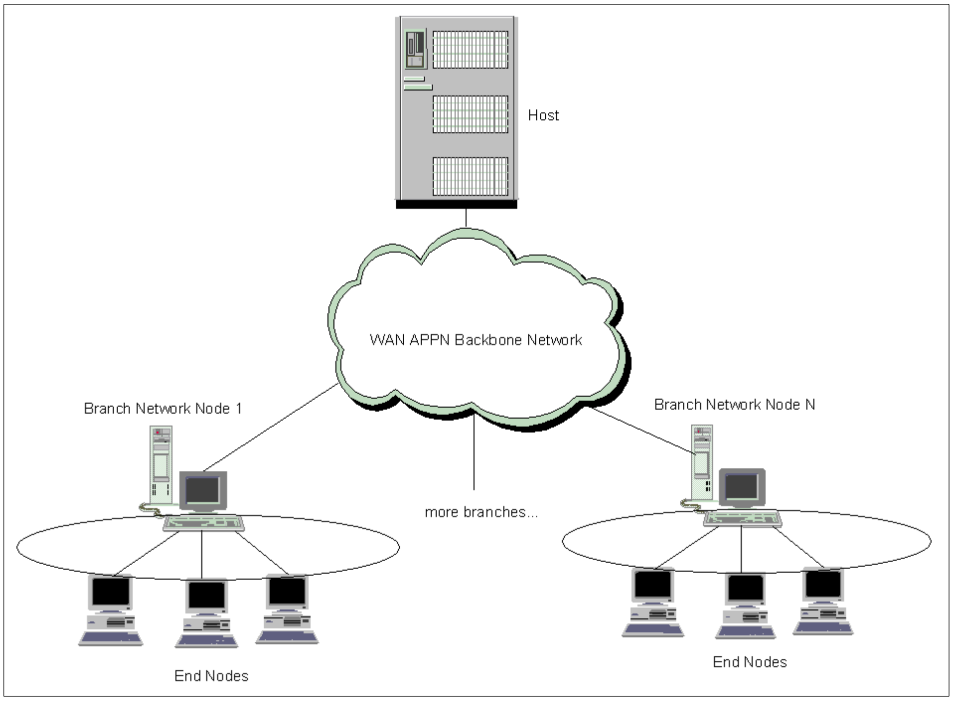


Figure 74. Sample "branched" network 2

Large enterprise networks can benefit greatly from advanced HPR functions such as automatic resource discovery and route selection. However, the price of dynamic network operation is the need to advertise the network topology or search the network for resources. Prior to Branch Extender, any HPR node that routed data between other systems (for example, CS/AIX connecting a branch office to a host) was required to be a network node, and thus to send and receive network control messages. In a small network, the overhead of these network control messages is insignificant. But in a large network made up of hundreds to thousands of relatively slow lines, even small overhead may be unacceptable. See 7.2, "Topology databases" on page 118. IBM introduced Branch Extender to enable such enterprises to gain the benefits of HPR throughout their entire network without these concerns. It can support end-to-end HPR connections all the way from computers in the branch to a host system (this provides maximum flexibility in rerouting connections around failed network components). The Branch Extender itself can also be the endpoint of reroutable HPR connections and extend HPR reliability to 3270 sessions.

Technically, a Branch Extender poses as a network node with DLUR support to computers or 3270 terminals in its local branch. At the same time it poses as an end node to computers in the WAN. By impersonating an end node, a Branch Extender gains the following advantages:

- It does not receive topology data or directory broadcasts from the wide area network. Instead, it lets a network node in the WAN choose routes for computers in the branch. A Branch Extender relays data between the branch and the WAN and enables HPR traffic to flow to computers in the branch.
- It can register all the branch's resources to a directory server in the APPN backbone network so that no manual definitions are needed there. Network efficiency is improved by notifying the central directory server of each resource's location, to greatly reduce or even eliminate broadcast searches in the WAN.

Branch Extender also allows direct, peer-to-peer communication between branches connected to the same APPN connection network (CN). Though a connection network configuration is not required, Branch Extender provides substantial benefit when the uplink and downlink networks are CNs, for example a branch CN such as token-ring, Ethernet or FDDI connected via a BrNN to a WAN CN such as ATM.

7.2 Topology databases

APPN networks consist of a backbone structure of network nodes interconnected by TGs, known as intermediate-routing TGs, and TGs connecting end nodes to adjacent network nodes, virtual routing nodes, or other end nodes, known as endpoint TGs.

Information about the backbone structure of the APPN network is kept within the network topology database, which resides on every APPN network node. Information about endpoint TGs is contained within local topology databases, which reside on every APPN node or LEN end node.

The primary use of local and network topology databases is to enable route calculation when an LU residing in one APPN node wishes to establish a session with an LU residing in another APPN node. The topology databases enable topology and routing services in the network node (NN) server to determine all possible routes between the nodes. The local topology database contributes the end node's TG, while the network topology database supplies the information on network nodes and the TGs between them.

7.2.1 Local topology database

The local topology database contains information on all of the transmission groups (TGs) attached to the node. Every APPN node maintains a local topology database. An APPN end node uses the information in its local topology database to send local TG information to its network node server in locate requests and replies. In a network node, the local topology database includes information about the attached end nodes. In HPR networks, the APPN end node's TG information (carried in TG vectors) indicates whether the nodes are HPR-capable.

The local topology database is created and maintained by the end node Topology Database Manager (TDM). It is not saved across reboots and is rebuilt when the node initializes. Entries in the local topology database are created automatically when configuration services informs TDM about newly activated or changed TGs. The operator updates the local topology database through configuration services. The local topology database is searched by TDM when it receives a query from route selection services or from session services.

7.2.2 Network topology database

Network nodes in an APPN network need to maintain topology information about the location of other nodes in the network and the communications links between them, and to forward this information around the network when the topology changes. The information is maintained in a database called the network topology database. As the network grows in size, the amount of stored information and topology-related network traffic can become large and difficult to manage. Topology database size is a function of the number of NNs and links, as well as the frequency of link state changes.

Every APPN network node maintains a network topology database in addition to its local topology database. The network topology database does not include information on APPN end nodes, LEN end nodes, or the transmission groups attached to them. It includes information only on network nodes in the APPN network and the transmission groups interconnecting them.

Network nodes in an APPN network send one another topology database updates (TDUs) over CP-CP sessions whenever a resource (network node or a TG between network nodes) is activated or deactivated, or its characteristics change. Only the current changes are included in the TDU. Every network node receives the TDU containing the current change, so each has the same view of the network. The network topology database is used by the network node to select routes for sessions that originate at the LUs in it and at the end nodes that it serves. Unlike the directory database, which is distributed among network nodes, the network topology database is fully replicated on all APPN network nodes. APPN protocols for the distribution of network topology information ensure that every network node is provided with a complete view of the network backbone topology.

Note: Although the TGs connecting a network node to attached end nodes are not included in the network topology database, the network node, nevertheless, knows of those TGs through its local topology database. This information is kept locally only and not sent to adjacent network nodes.

The network topology database is created and maintained by TDM and saved across reboots by the safe-store of network topology database function. In a CS/AIX network node, the network topology database is saved in the file /var/sna/topology.dat.

7.3 Supported configurations

The following sections describe Branch Extender components and capacities.

7.3.1 Links

The number and type of links over which a BrNN provides network node services to its branch are unrestricted. Although a typical BrNN branch is a single LAN, a BrNN's supported network may consist of any combination of one or more local area network(s), including standard Ethernet, 802.3 Ethernet, token-ring, FDDI, ATM LAN Emulation, one or more wide area network link(s), including SDLC, X.25, frame relay using emulated token-ring.

The number and type of links over which a BrNN supports receiving network node services from an uplink NNS are unrestricted, but a BrNN acts as an EN on uplinks and, as a result, never has more than one NNS at a time.

The same physical medium may support BrNN uplinks and downlinks simultaneously, as long as the medium supports simultaneous multiple logical connections. Example of logical addressing are SDLC multipoint stations addresses, IEEE 802.2 Logical Link Control type 2 connections identified by unique SSAP/DSAP pairs, and X.25 Virtual Circuits.

A BrNN will typically have many downlinks and only a few uplinks.

7.3.2 Nodes

In a BrNN-served branch, the only active NNs allowed are BrNN(s). All other nodes in the branch are ENs or LEN ENs, and use a BrNN as their server.

Two types of BrNN-BrNN connectivity are supported:

1. Cascaded BrNNs. The upper BrNN defines the link as a downlink and assumes an NN role. The lower BrNN defines it as an uplink and assumes an EN role. The lower BrNN, in turn, may be the NNS for resources on its own downlinks.
2. Parallel (peer) BrNNs. Both BrNNs configure the link between them as an uplink, and appear as ENs to each other. Each BrNN typically has at least one uplink to the WAN. In this configuration, the BrNN-served downlinks are disjoint, but a given EN can establish CP-CP sessions and register its resources with either BrNN. The BrNN with which an EN currently has CP-CP sessions is its NNS; only this BrNN replies positively to a Locate request for that EN's resources.

By definition, a BrNN maintains CP-CP sessions with no more than one node outside its branch network - its current network node server. A BrNN is allowed to have different NN servers from time to time, but only one at a time. If its NNS fails, the BrNN automatically switches to another available NNS, which can be another BrNN. If a link to a preferred NNS becomes operational, the CP-CP sessions to the current NNS can be manually deactivated in order to activate CP-CP sessions with the preferred NNS.

All DLUR support in a BrNN-served local branch is provided by the BrNN. No DLUR support may be provided by any node downstream of a BrNN. If BrNNs are cascaded, only the highest BrNN can be a DLUR.

7.3.3 LU-LU sessions

LU-LU sessions between two ENs in the same branch are managed and connected without the intervention of NNs across the WAN. However, a BrNN relies on its server for default routing to connect LU-LU sessions between LUs in different branches. A BrNN does not try to get complete topology data. It only retains the topology of its local branch. When that information is insufficient, the BrNN sends a Locate to its NNS asking for assistance in locating the resource and calculating the route to get there from the BrNN.

To keep these dual faces, although it's really an NN, a BrNN emulates an EN to its NNS by setting EN parameters in XID and CP-CP capabilities. (The BrNN determines if the link is downlink or uplink before sending an XID).

Since a BrNN appears to be an EN, it is isolated from the WAN. The NNS does not bother to send it TDUs, giving the BrNN no chance to learn about central directory servers or other NNs or their TGs.

By default, the BrNN sends a Locate only to its current NNS, since that is the only NN with which it ever has CP-CP sessions.

A BrNN is an NN inside and shows an NN image to its branch ENs. Branch ENs don’t need to know that their NNS is actually a BrNN.

7.4 Implementation

The APPN Branch Extender function is implemented by the APPN Branch Network Node, so its implementation involves configuring a CS/AIX node as a branch network node:

To implement Branch Extender, configure the node as follows:

1. Define the node

   a. From the Node window select **Services** -> **Configure Node Parameters**.

   CS/AIX displays the Node Parameters dialog.

   APPN support To provide session routing services to other nodes in a branch network that are not part of the main APPN backbone network, configure the node as a branch network node.

   Control Point Name Fully qualified control point name for the local node.

   Control Point Alias Local alias for the default local LU. Supply this value if the default local LU is used by independent LU 6.2 LUs.

   Node ID Identifier for the PU on the local node. Supply a value only if the node will be used for dependent traffic using the default (control point) LU.

   b. Click on the **OK** button to define the node. When you define the node, CS/AIX automatically defines a default LU with the same name as the control point. That LU can act as the default local LU for the node.

2. Define connectivity

   a. To define the port, click **Services** -> **Connectivity** -> **New Port**.

   Choose the correct type of port and click **OK.**

   Each port is associated with a specific link protocol and therefore the port dialog depends on the port type. For an Enterprise Extender (HPR/IP) port, for example, the parameters are:

Port name The locally known name of the port.

Local IP Interface The identifier for the TCP/IP network interface to be used for the HPR/IP link. For example, *tr0*. If no value is provided, CS/AIX defaults this parameter to the primary TCP/IP network interface.

Initially Active Whether to activate the port automatically when the node is started. This setting enables link stations that use the port to be activated in response to requests from adjacent nodes or on demand by the local node. (Activating the port does not activate any link stations; link stations are activated separately).

b. Define the link station to the end node within the branch. Click **Services** -> **Connectivity** -> **New Link Station.**

Select **End Node** for the Remote Node Type and **downlink** for Branch Link Type. Fill in the parameters to create the link station. The link dialog depends on the link type. Common Link Station Parameters are:

Name A name to identify the link station locally.

Port Name The port that is to be used to access the adjacent node.

Activation Method used to activate the link station. Specify one of the following methods: By administrator, On node Startup, or On Demand.

LU traffic The type of LU traffic to flow over the link: Any, Independent Only or Dependent Only. This parameter is not used for an Enterprise Extender (HPR/IP) or MPC+ link, because this link type supports only independent traffic.

Remote IP host name You need to provide addressing information for contacting the adjacent node. If you do not supply an address for the remote node, the link station acts as a nonselective link station, accepting incoming calls from any remote node. For an Enterprise Extender (HPR/IP) link, enter the remote host name of the destination node for this link. This can be specified as a dotted-decimal IP address, as a name, or as an alias. If you specify a name or alias, the AIX system must be able to resolve this to a fully qualified name.

c. Define the link station to the network node within the main APPN WAN backbone network. Click **Services** -> **Connectivity** -> **New Link Station.**

   Fill in the parameters to create the link station. Select **Network Node** for the Remote Node Type and **uplink** for Branch Link Type.

For more information on node and connectivity definitions refer to *IBM Communications Server for AIX, Version 6, Quick Beginnings*, GC31-8583 and *IBM Communicatons Server for AIX, Version 6, Administration Guide*, SC31-8586.

7.5 Scenario

In this section we will use the following equipment: three RS/6000s running AIX Version 4.3.3, Communications Server for AIX, Version 6 and a host running CS for OS/390.

Two of the RS/6000s will be configured as Branch Extender Nodes, and the third will be configured as an end node, as shown in Figure 75.

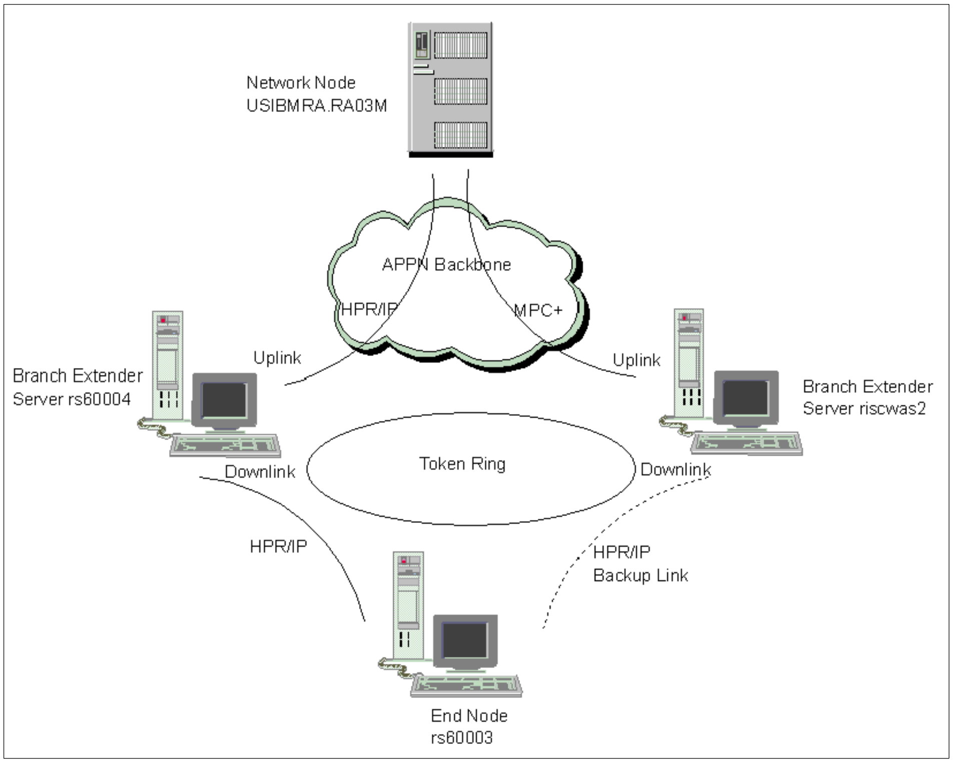


Figure 75. Branch Extender test scenario

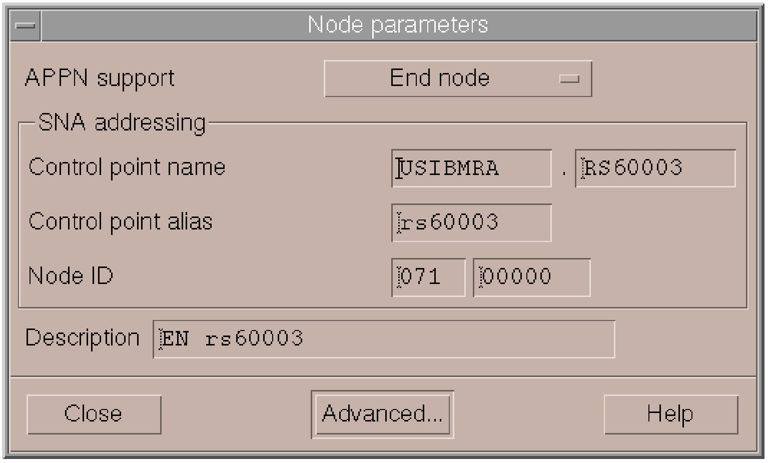
This scenario could correspond to a large branch with several workstations, such as rs60003, running APPC applications. Just bear in mind that you can’t define a DLUR in a node which is connected through a downlink TG to a Branch Extender.

Both servers, rs60004 and riscwas2, can provide NN services for the downstream EN, rs60003. We chose to configure server rs60004 as being the preferred NN server for workstation rs60003 and we configured a backup link from rs60003 to server riscwas2. In case of failure of the LAN adapter, or crash of server rs60004, the HPR link between rs60003 and its preferred NN will go down and rs60003 shall automatically try to set up a link to server riscwas2 (which can also provide NN services).

The configuration steps were as follows:

1. Configure nodes rs60003, rs60004 and riscwas2.

We defined nodes rs60004 and riscwas2 as Branch Extender Nodes and node rs60003 as an end node (see Figure 76, Figure 77 and Figure 78). Note that the CP name for node riscwas2 is USIBMRA.SERVERB.



APPN support: End node

SNA addressing

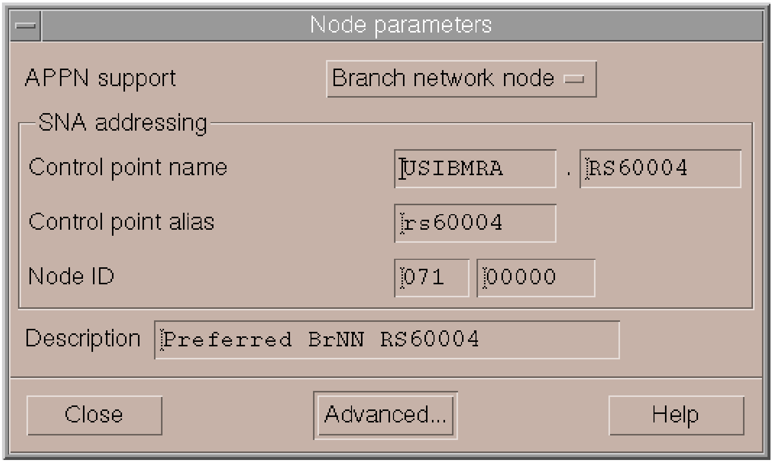
Control point name: USIBMRA . RS60003

Control point alias: rs60003

Node ID: 071 00000

Description: EN rs60003

Figure 76. Node rs60003



APPN support: Branch network node

SNA addressing

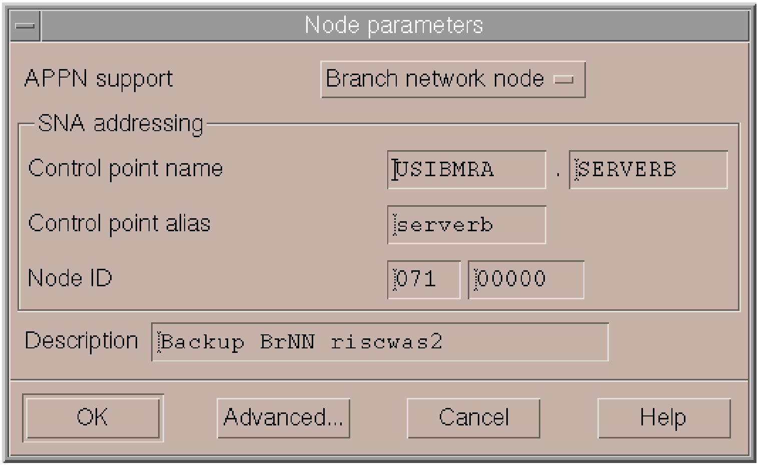
Control point name: USIBMRA . RS60004

Control point alias: rs60004

Node ID: 071 00000

Description: Preferred BrNN RS60004

Figure 77. Node rs60004



Node parameters

APPN support: Branch network node

SNA addressing

Control point name: USIBMRA . SERVERB

Control point alias: serverb

Node ID: 071 00000

Description: Backup BrNN riscwas2

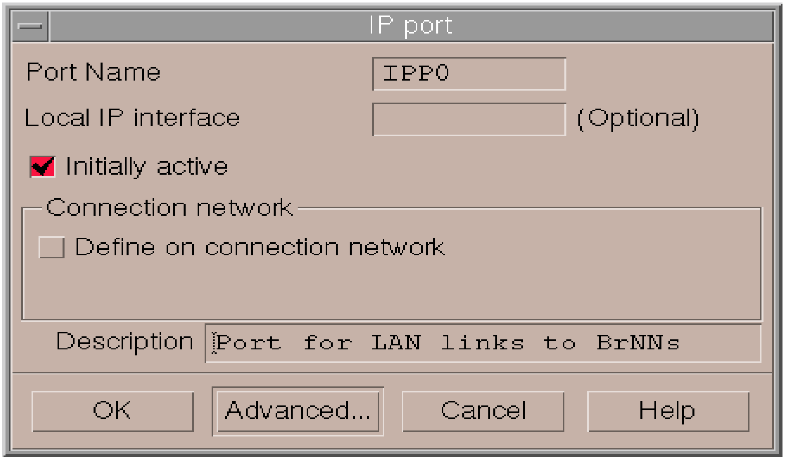
Figure 78. Node riscwas2

After clicking the **OK** button, the SNA Node Configuration utility adds the define_node section to the configuration file (/etc/sna/sna_node.cfg). The keyword parameters which change for the different nodes are marked below (in the order of rs60003, rs60004 and riscwas2).

```
[define_node]
cp_alias =    rs60003          rs60004                serverb
description = EN rs60003       Preferred BrNN RS60004 Backup BrNNriscwas2
fqcp_name =   USIBMRA.RS60003  USIBMRA.RS60004        USIBMRA.SERVERB
node_type =   END NODE         BRANCH_NETWORK_NODE    BRANCH_NETWORK_NODE
mode_to_cos_map_supp = YES
mds_supported = YES
node_id = <07100000>
max_locates = 1500
dir_cache_size = 255
max_dir_entries = 0
locate_timeout = 0
reg_with_nn = YES
reg_with_cds = YES
mds_send_alert_q_size = 100
cos_cache_size = 24
tree_cache_size = 40
tree_cache_use_limit = 40
max_tdm_nodes = 0
max_tdm_tgs = 0
max_isr_sessions = 1000
isr_sessions_upper_threshold = 900
```

```
isr_sessions_lower_threshold = 800
isr_max_ru_size = 16384
isr_rcv_pac_window = 8
store_endpt_rscvs = NO
store_isr_rscvs = NO
store_dlur_rscvs = NO
cos_table_version = VERSION_0_COS_TABLES
send_term_self = NO
disable_branch_awareness = NO
cplu_syncpt_support = NO
cplu_attributes = NONE
dlur_support = YES
pu_conc_support = YES
nn_rar = 128
max_ls_exception_events = 0
ms_support = NORMAL
queue_nmvts = YES
ptf_flags = NONE
```

2. Create the LAN and WAN ports on nodes rs60003, rs60004 and riscwas2. All the nodes will use the Enterprise Extender (HPR/IP) type of port (rs60004 and riscwas2 will use the same port for down and uplink connections). The HPR/IP port dialog for rs60003 is shown in Figure 79. It is the same for nodes rs60004 and riscwas2.



IP port

Port Name: IPP0

Local IP interface: (Optional)

☑ Initially active

Connection network

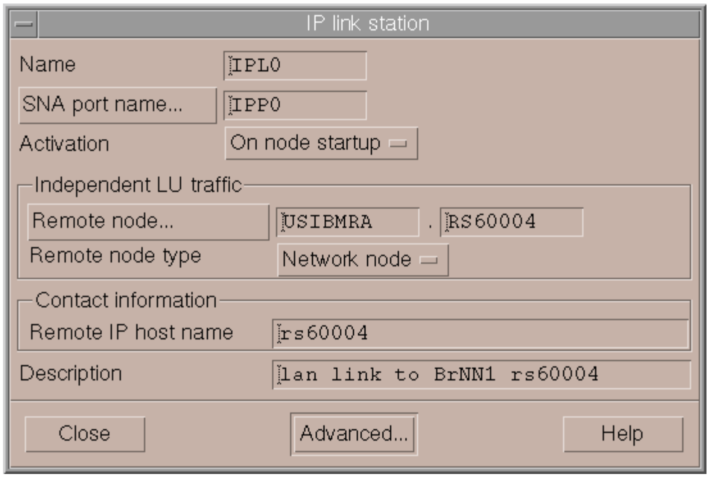
☐ Define on connection network

Description: Port for LAN links to BrNNs

Figure 79. HPR/IP port definition in node rs60003

The Advanced Settings for branch network nodes rs60004 and riscwas2 presents the IP port parameter **Implicit Links to End Nodes -> Downlink.** This parameter specifies whether implicit links to end nodes should be treated as uplinks or downlinks.

3. Create the LAN Link from rs60003 to branch network node servers rs60004 and riscwas2 (see Figure 80 and Figure 81).



IP link station

Name: IPL0

SNA port name...: IPP0

Activation: On node startup

Independent LU traffic

Remote node...: USIBMRA . RS60004

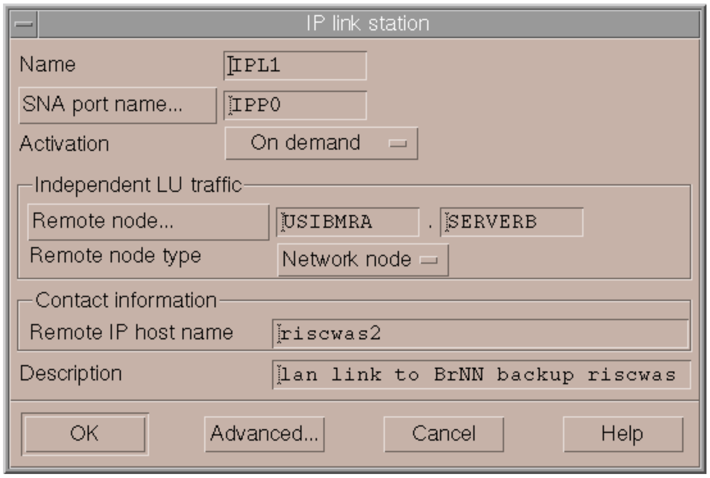
Remote node type: Network node

Contact information

Remote IP host name: rs60004

Description: lan link to BrNN1 rs60004

Figure 80. LAN link from rs60003 to preferred BrNN server rs60004



IP link station

Name: IPL1

SNA port name...: IPP0

Activation: On demand

Independent LU traffic

Remote node...: USIBMRA . SERVERB

Remote node type: Network node

Contact information

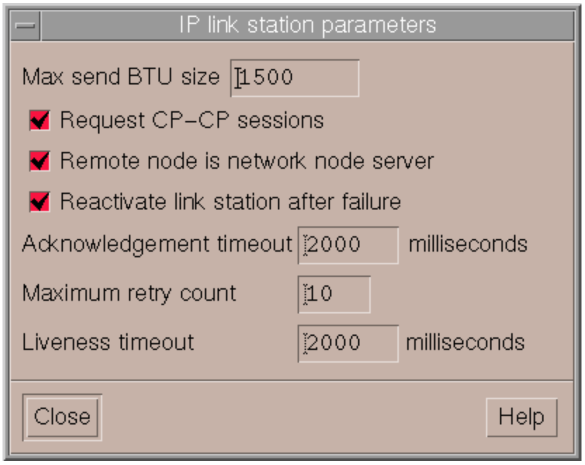
Remote IP host name: riscwas2

Description: lan link to BrNN backup riscwas

Figure 81. LAN link from rs60003 to backup BrNN server riscwas2

The only difference between the two link stations definitions is the **Activation** method. For the preferred server we use activation on node startup (the link station is started automatically when the node starts up) whereas we choose activation on demand for the backup server (the link station is started automatically when required to provide connectivity for an application).

The Advanced Settings for both link stations are as shown in Figure 82.



IP link station parameters

Max send BTU size 1500

☑ Request CP-CP sessions

☑ Remote node is network node server

☑ Reactivate link station after failure

Acknowledgement timeout 2000 milliseconds

Maximum retry count 10

Liveness timeout 2000 milliseconds

Figure 82. IP link station advanced parameters from rs60003 to BrNN servers rs60004 and riscwas2

The link station definitions on rs60003 for the links to rs60004 and riscwas2 are shown below. The keyword parameters that change for rs60004 and riscwas2 have been highlighted.

```
[define_ip_ls]
ls_name =         IPL0                     IPL1
description =     lan link to BrNN1 rs60004  lan link to BrNN backup riscwas2
port_name = IPP0
adj_cp_name =     USIBMRA.RS60004          USIBMRA.SERVERB
adj_cp_type = NETWORK_NODE
max_send_btu_size = 1500
ls_attributes = SNA
cp_cp_sess_support = YES
default_nn_server = YES
lsap_address = 0x04
determined_ip_address = 9.24.104.27         9.24.104.233
auto_act_supp =    NO                      YES (On Demand)
tg_number =       0                        1
limited_resource = NO                       NO SESSIONS
disable_remote_act = NO
link_deact_timer = 30
use_default_tg_chars = YES
effect_cap = 3993600
connect_cost = 0
byte_cost = 0
security = SEC_NONSECURE
```

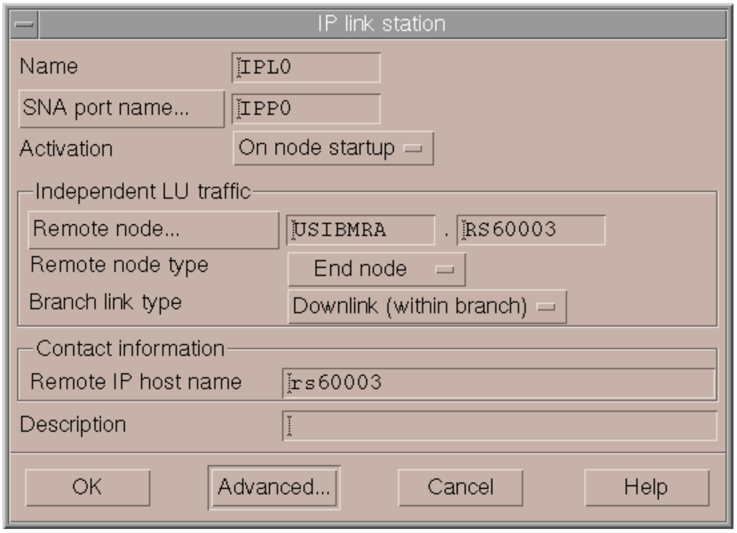
```
prop_delay = PROP_DELAY_LAN
user_def_parm_1 = 128
user_def_parm_2 = 128
user_def_parm_3 = 128
target_pacing_count = 7
max_ifrm_rcvd = 0
branch_link_type = NONE
adj_brnn_cp_support = ALLOWED
initially_active =   YES                   NO
restart_on_normal_deact = NO
react_timer = 30
react_timer_retry = 65535
remote_ip_host =     rs60004               riscwas2
ack_timeout = 2000
max_retry = 10
liveness_timeout = 2000
short_hold_mode = NO
```

Note: For an end node, the parameter default_nn_server specifies whether this is a link supporting CP-CP sessions to a network node that can act as the local node's network node server. When the local node has no CP-CP sessions to a network node server and needs to establish them, it checks this parameter on its defined link stations to find a suitable link station to activate. This enables you to specify which adjacent NNs are suitable to act as the NN server. Possible values are:

- YES: This link supports CP-CP sessions to a network node that can act as the local node's NN server; the local node can automatically activate this link if it needs to contact an NN server. The cp_cp_sess_support parameter must be set to YES.
- NO: This link does not support CP-CP sessions to a network node that can act as the local node's NN server; the local node cannot automatically activate this link if it needs to contact an NN server.

If the local node is not an end node, this parameter is ignored.

4. Create the LAN links from the server nodes rs60004 and riscwas2 to the end node rs60003. The configuration parameters are the same for both nodes; see Figure 83 and Figure 84.



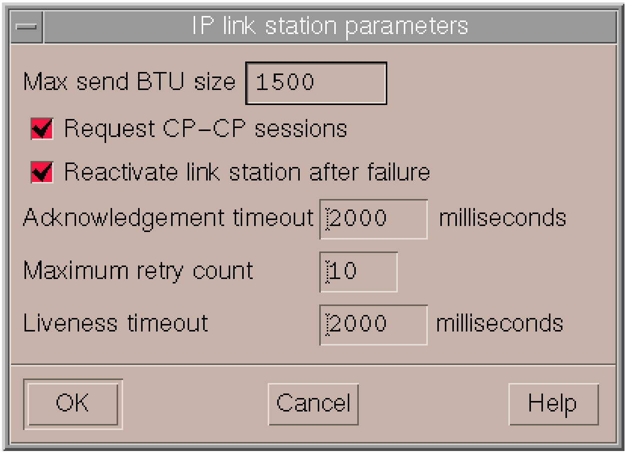
Name: IPL0
SNA port name...: IPP0
Activation: On node startup

Independent LU traffic
Remote node...: USIBMRA . RS60003
Remote node type: End node
Branch link type: Downlink (within branch)

Contact information
Remote IP host name: rs60003

Description:

Figure 83. LAN HPR/IP link station definition from BrNN servers rs60004 and riscwas2 to rs60003



Max send BTU size: 1500
☑ Request CP–CP sessions
☑ Reactivate link station after failure
Acknowledgement timeout: 2000 milliseconds
Maximum retry count: 10
Liveness timeout: 2000 milliseconds

Figure 84. LAN HPR/IP link station definition, advanced parameters, from BrNN servers rs60004 and riscwas2 to rs60003

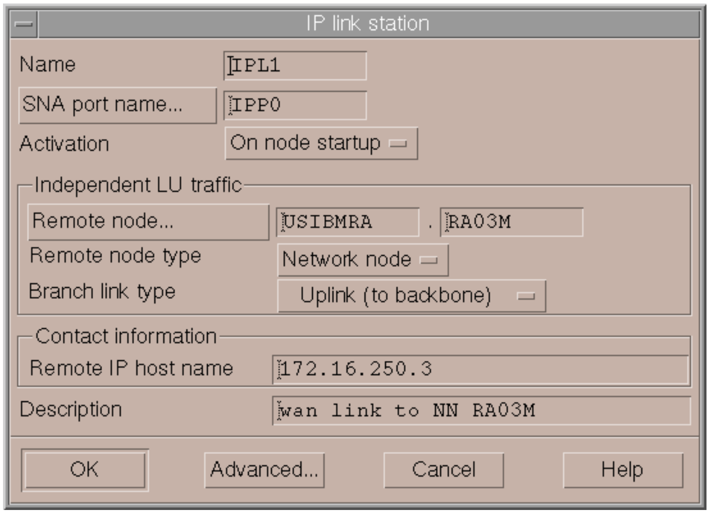
Note: Instead of configuring the link stations explicitly, we could have used dynamically created link stations (implicit links). If a remote node attempts to connect to the local node, but no link station is defined that matches the address specified on the incoming call, CS/AIX can define one implicitly if a suitable port has been defined on the local node. This dynamically created link station appears in the connectivity section of the Node window for the duration of the connection.

The define_ip_ls section in the configuration file /etc/sna/sna_node.cfg is the same for rs60004 and riscwas2. It looks like:

```
[define_ip_ls]
ls_name = IPL0
description = ““
port_name = IPP0
adj_cp_name = USIBMRA.RS60003
adj_cp_type = END_NODE
max_send_btu_size = 1500
ls_attributes = SNA
cp_cp_sess_support = YES
default_nn_server = NO
lsap_address = 0x04
determined_ip_address = 9.24.104.23
auto_act_supp = NO
tg_number = 0
limited_resource = NO
disable_remote_act = NO
link_deact_timer = 30
use_default_tg_chars = YES
effect_cap = 3993600
connect_cost = 0
byte_cost = 0
security = SEC_NONSECURE
prop_delay = PROP_DELAY_LAN
user_def_parm_1 = 128
user_def_parm_2 = 128
user_def_parm_3 = 128
target_pacing_count = 7
max_ifrm_rcvd = 0
branch_link_type = DOWNLINK
adj_brnn_cp_support = ALLOWED
initially_active = YES
restart_on_normal_deact = NO
react_timer = 30
react_timer_retry = 65535
remote_ip_host = rs60003
ack_timeout = 2000
max_retry = 10
liveness_timeout = 2000
short_hold_mode = NO
```

5. Create the WAN links from BrNN servers rs60004 and riscwas2 to the preferred NN in the WAN APPN Network. We used HPR/IP links in both

cases. The HPR/IP link dialog for rs60004 is shown in Figure 85. It is the same for node riscwas2.



Name: IPL1
SNA port name...: IPP0
Activation: On node startup

Independent LU traffic
Remote node...: USIBMRA . RA03M
Remote node type: Network node
Branch link type: Uplink (to backbone)

Contact information
Remote IP host name: 172.16.250.3

Description: wan link to NN RA03M

Figure 85. WAN HPR/IP link from BrNN rs60004 to preferred NN in the backbone APPN network

In both cases CP-CP sessions with the remote network node are enabled (Advanced Parameters).

The define_ip_ls section in the configuration file /etc/sna/sna_node.cfg, which is the same for rs60004 and riscwas2, looks like:

```
[define_ip_ls]
ls_name = IPL1
description = UpLink to NN RA03M
port_name = IPP0
adj_cp_name = USIBMRA.RA03M
adj_cp_type = NETWORK_NODE
max_send_btu_size = 1500
ls_attributes = SNA
cp_cp_sess_support = YES
default_nn_server = NO
lsap_address = 0x04
determined_ip_address = 172.16.250.3
auto_act_supp = NO
tg_number = 0
limited_resource = NO
disable_remote_act = NO
link_deact_timer = 30
use_default_tg_chars = YES
```

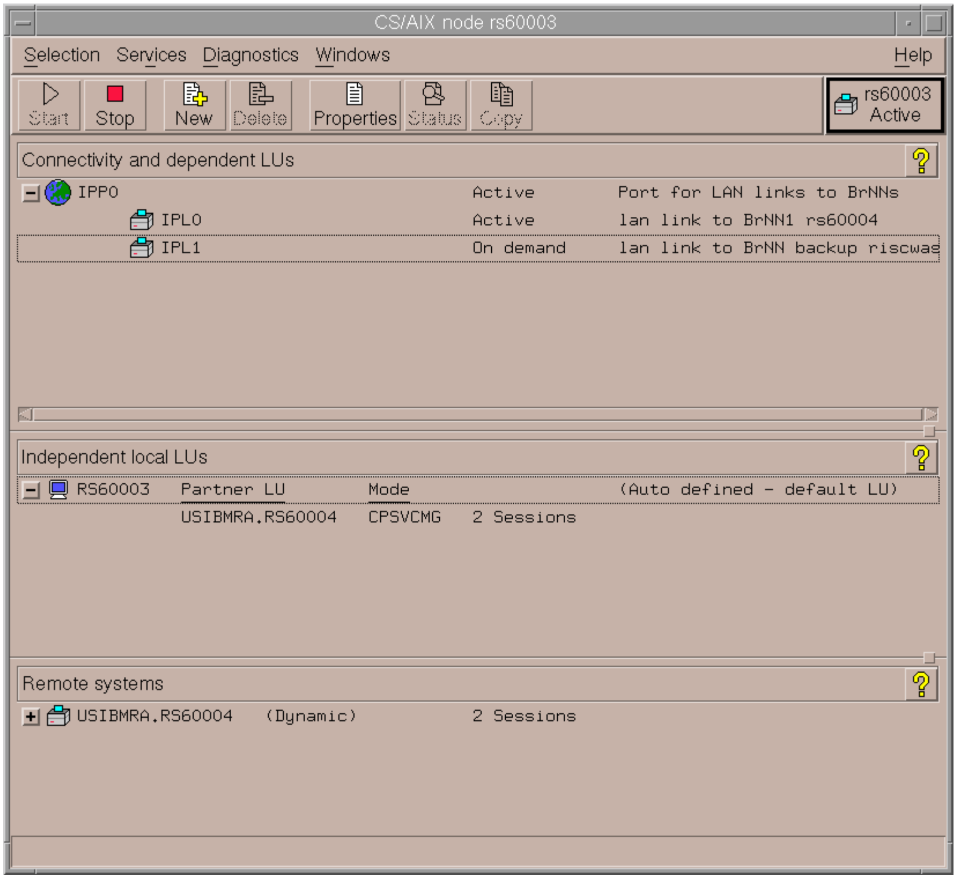
```
effect_cap = 3993600
connect_cost = 0
byte_cost = 0
security = SEC_NONSECURE
prop_delay = PROP_DELAY_LAN
user_def_parm_1 = 128
user_def_parm_2 = 128
user_def_parm_3 = 128
target_pacing_count = 7
max_ifrm_rcvd = 0
branch_link_type = UPLINK
adj_brnn_cp_support = ALLOWED
initially_active = YES
restart_on_normal_deact = NO
react_timer = 30
react_timer_retry = 65535
remote_ip_host = 172.16.250.3
ack_timeout = 2000
max_retry = 10
liveness_timeout = 2000
short_hold_mode = NO
```

7.5.1 Testing the connections

In this section we will test connectivity from rs60003 to the NN in the main backbone APPN network using the SNA APPC application <aping**>**. The connection will take place through the preferred BrNN rs60004. Then we will stop SNA services in the BrNN rs60004 to test the backup link from rs60003 to riscwas2. After stopping SNA services in rs60004, riscwas2 is identified as the branch network node server by rs60003. The connectivity to the main APPN backbone network will remain but this time through BrNN riscwas2. HPR will allow for non-disruptive path-switches through BrNN riscwas2 in case of failure of the LAN adapter or a crash of BrNN rs60004.

The sequence of events were as follows:

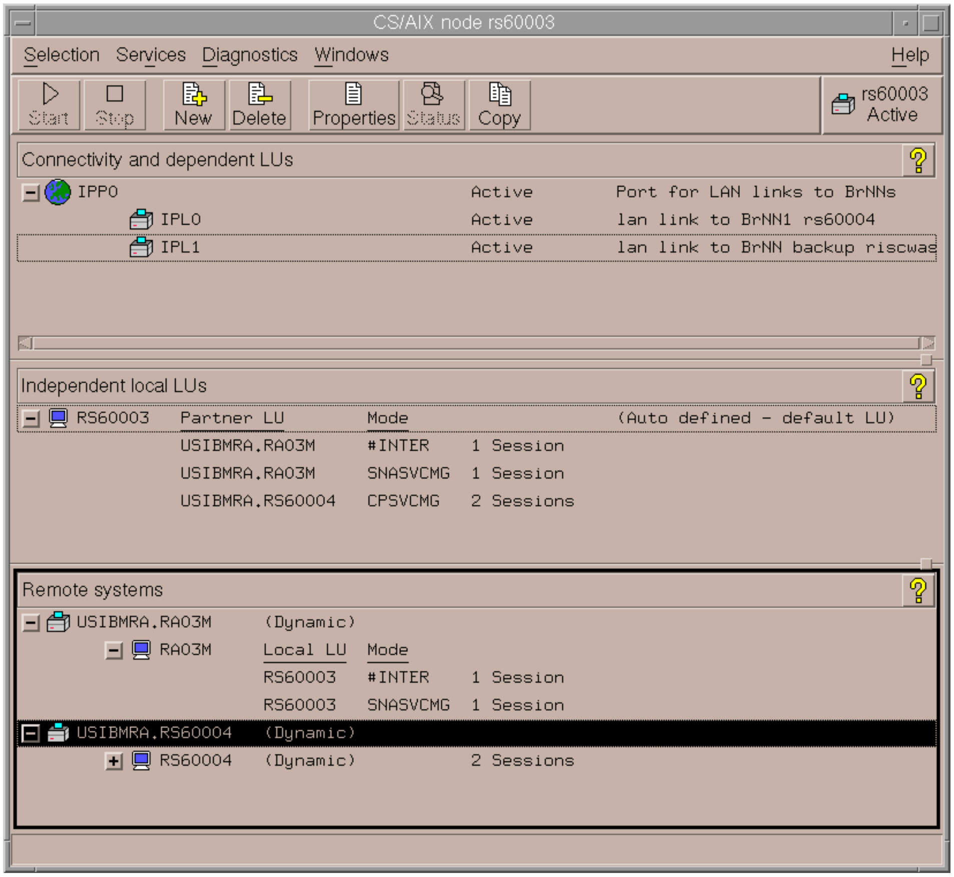
1. With SNA resources active in Branch Extender network nodes rs60004 and riscwas2, we started the end node rs60003. In Figure 86 we can see that the end node rs60003 has set up CP-CP sessions with the preferred BrNN rs60004.



```
Connectivity and dependent LUs
IPP0                                   Active       Port for LAN links to BrNNs
        IPL0                           Active       lan link to BrNN1 rs60004
        IPL1                           On demand    lan link to BrNN backup riscwas

Independent local LUs
RS60003     Partner LU       Mode                   (Auto defined - default LU)
            USIBMRA.RS60004  CPSVCMG  2 Sessions

Remote systems
USIBMRA.RS60004   (Dynamic)           2 Sessions
```

Figure 86. rs60003 node window after activation

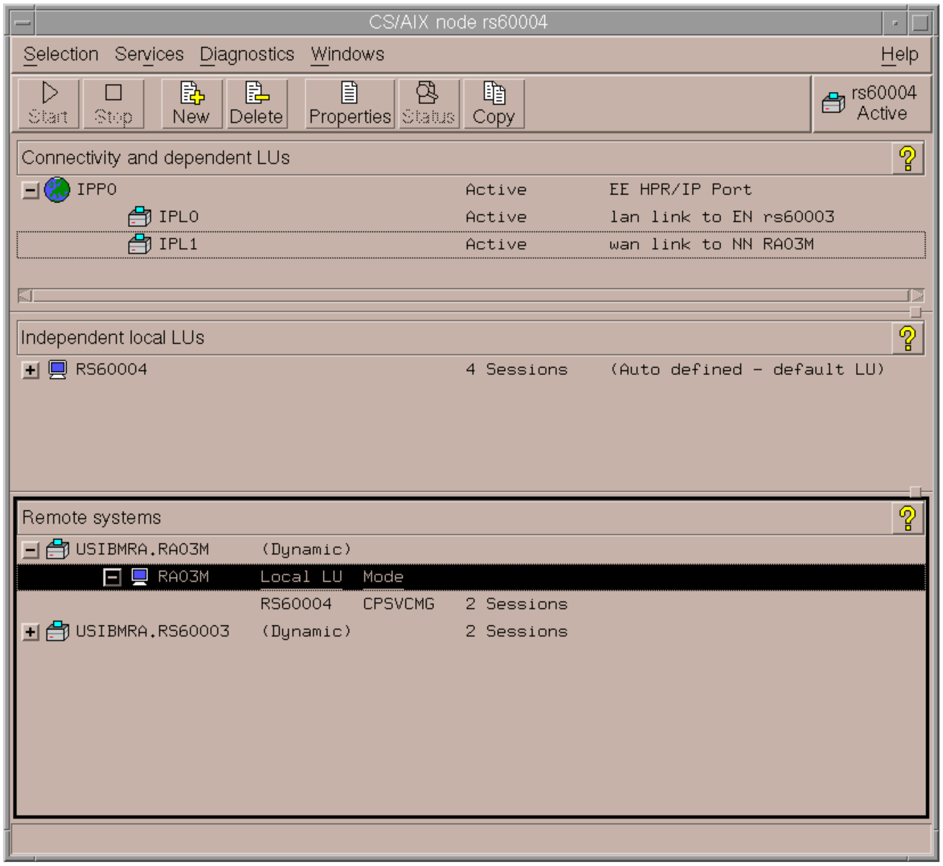
2. We tested connectivity from the end node rs60003 to the main APPN backbone network using the SNA APPC application <`aping`>. Figure 87 on page 137 shows the establishment of the RTP connections between rs60003 and the network node in the main APPN backbone network. The RTP connection with COS SNASVCMG is established to perform a CNOS (Change Number of Sessions) for mode #INTER, after which the RTP connection that carries the actual #INTER session (aping session) is started.



```
Connectivity and dependent LUs
[-] IPPO                                    Active     Port for LAN links to BrNNs
        IPL0                                Active     lan link to BrNN1 rs60004
        IPL1                                Active     lan link to BrNN backup riscwas

Independent local LUs
[-] RS60003      Partner LU        Mode                  (Auto defined - default LU)
                 USIBMRA.RA03M     #INTER     1 Session
                 USIBMRA.RA03M     SNASVCMG   1 Session
                 USIBMRA.RS60004   CPSVCMG    2 Sessions

Remote systems
[-] USIBMRA.RA03M      (Dynamic)
    [-] RA03M          Local LU    Mode
                       RS60003     #INTER     1 Session
                       RS60003     SNASVCMG   1 Session
[-] USIBMRA.RS60004    (Dynamic)
    [+] RS60004        (Dynamic)              2 Sessions
```

Figure 87. rs60003 node window after aping of NN in the main backbone APPN network

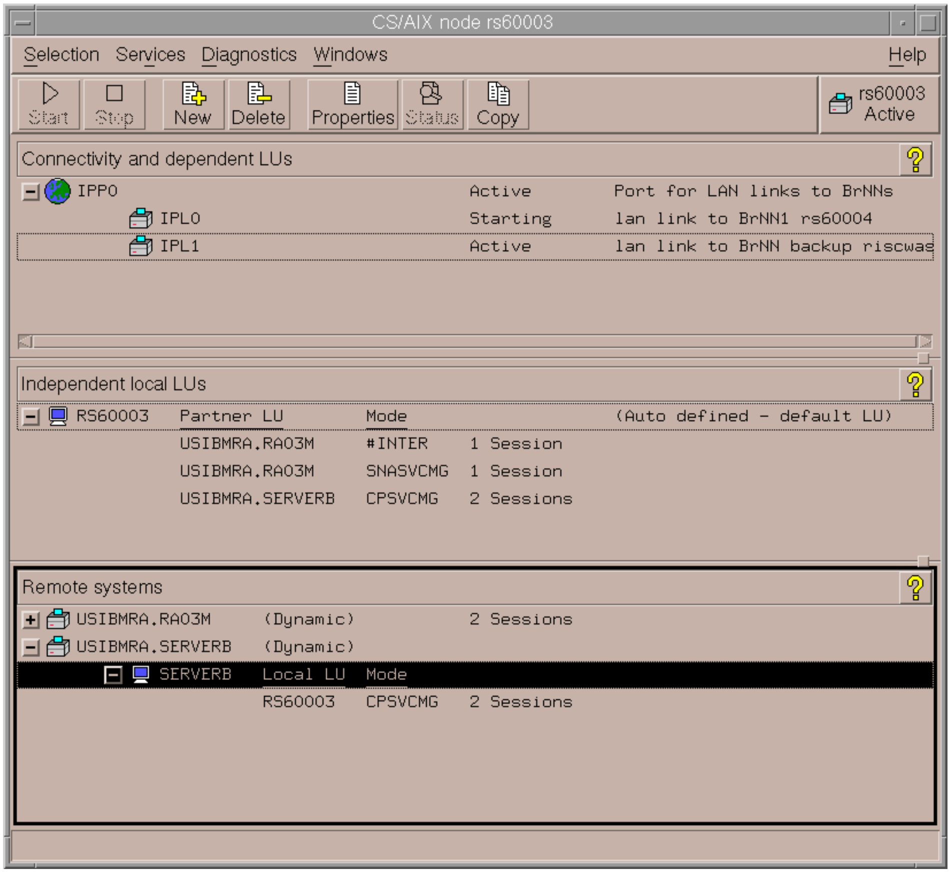
Figure 88 on page 138 shows that the BrNN rs60004 has set up CP-CP sessions with the preferred NN in the main APPN backbone network (usibmra.ra03m).



```
Connectivity and dependent LUs
⊟ IPP0                              Active       EE HPR/IP Port
        IPL0                        Active       lan link to EN rs60003
        IPL1                        Active       wan link to NN RA03M

Independent local LUs
⊞ RS60004                           4 Sessions   (Auto defined - default LU)

Remote systems
⊟ USIBMRA.RA03M     (Dynamic)
      ⊟ RA03M       Local LU  Mode
                    RS60004   CPSVCMG   2 Sessions
⊞ USIBMRA.RS60003   (Dynamic)           2 Sessions
```

Figure 88. rs60004 node window after EN established a ping session with a node in the APPN backbone network

3. Next, we stopped SNA services in the preferred BrNN rs60004. Figure 89 on page 139 shows how the end node rs60003 automatically sets up CP-CP sessions with the backup BrNN riscwas2, which shall become its NN.



CS/AIX node rs60003
Selection Services Diagnostics Windows Help
Start Stop New Delete Properties Status Copy
rs60003 Active

Connectivity and dependent LUs

```
IPP0                                   Active      Port for LAN links to BrNNs
      IPL0                             Starting    lan link to BrNN1 rs60004
      IPL1                             Active      lan link to BrNN backup riscwas
```

Independent local LUs

```
RS60003    Partner LU        Mode                      (Auto defined - default LU)
           USIBMRA.RA03M     #INTER     1 Session
           USIBMRA.RA03M     SNASVCMG   1 Session
           USIBMRA.SERVERB   CPSVCMG    2 Sessions
```

Remote systems

```
USIBMRA.RA03M       (Dynamic)            2 Sessions
USIBMRA.SERVERB     (Dynamic)
      SERVERB      Local LU   Mode
                   RS60003    CPSVCMG    2 Sessions
```

Figure 89. rs60003 node window after stopping SNA services in the preferred BrNN rs60004

Because all the nodes are HPR capable, LU-LU sessions already established between the node rs60003 and the main APPN backbone network will get rerouted automatically around the alternative path, riscwas2.

Chapter 8. MPC+ support

MultiPath Channel Plus (MPC+) is an enhancement to MultiPath Channel (MPC) protocol support introduced in VTAM V4R3 and Communications Server for AIX, V4.2. MPC+ adds support for high performance routing (HPR) connectivity over channel connections when using VTAM V4R4 or higher. CS/AIX V6 includes support for MPC+ and basic MPC.

Note that MPC+ is referred to as High Performance Data Traffic (HPDT) MPC in some publications.

The basic features and requirements of MPC and MPC+ are as follows:

- Requires an ESCON channel attachment.

  Note: CS/AIX V6 supports both ESCON and Block Multiplexer channel connections.

- Requires MVS VTAM V4R3 or later with APPN enabled.

  Note: MPC+ requires MVS VTAM V4R4 or later.

- MPC+ requires DLUR for dependent LU traffic, while basic MPC requires DLUR or separate link stations for independent and dependent LU traffic.
- Uses separate subchannels for read and write, which reduces control delays.
- Uses SNA frame sizes up to 4 KB, but frames may be blocked together so that up to 60 KB can be sent in a single channel transmission.
- Using MPC+ requires HPR connectivity over channel connections.

The following figure shows a sample MPC+ ESCON configuration.

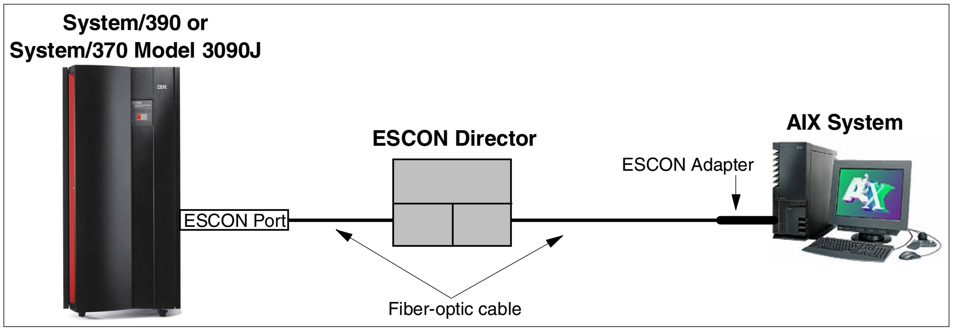


Figure 90. MPC+ ESCON connection through a single ESCON Director

The previous figure shows an ESCON director between the host and the AIX system. However, an ESCON director is not required. Up to two ESCON directors may be used to extend the distance between the host and AIX system up to 43 kilometers.

MPC+ links require HPR and support only independent LUs. Therefore, if dependent LU (LU0, 1, 2, 3) support is required over an MPC+ link, DLUR/DLUS must be used.

The overall CS/AIX support for channel connectivity is referred to as the *SNA Channel for AIX* feature. Support for MPC+ connectivity is part of the SNA Channel for AIX feature. See the IBM *Communications Server for AIX Channel Connectivity User's Guide*, SC31-8219 for detailed information on all the channel connectivity options supported by CS/AIX V6.

8.1 Hardware requirements

The SNA Channel for AIX feature of CS/AIX V6 supports both Micro Channel Architecture (MCA) ESCON and Peripheral Component Interconnect (PCI) ESCON adapter cards. In this book, we cover only the PCI ESCON adapter configuration.

To install SNA Channel for AIX for the PCI ESCON adapter, you must have the following hardware:

- S/390 ESCON Channel PCI Adapter (Feature 2751)
- ESCON fiber optic cabling and connections
- One of the following RISC System/6000 models:
  - 7017, all models
  - 7025 Models F50 and F80
  - 7026 Models H50, H70, H80 and M80
- One of the following host systems:
  - IBM ES/9000 Model 9021
  - IBM 9672

8.2 Software requirements

To install SNA Channel for AIX for the PCI ESCON adapter, you must have the following software:

- S/390 ESCON Channel PCI Adapter device driver (program number 5765-D49)
- AIX 4.3.2 or later
- IBM Communications Server for AIX, V6 or later
- MVS VTAM V4R3 or higher, with APPN enabled

  Note: For MPC+ support, VTAM V4R4 or later is required.

In addition, CS/AIX includes the following data link control filesets to support SNA channel data link communications:

sna.dlcchannel Contains the SNA Channel for AIX SNA DLC software for CDLC mode channel communications

sna.dlcmpc Contains the SNA Channel for AIX SNA DLC software for MPC mode channel communications

Both of these filesets are included as part of the SNA Channel for AIX feature of CS/AIX.

For MPC+ channel communications, the sna.dlcmpc fileset is required and should be installed when CS/AIX is installed.

8.3 MPC+ configuration

Configuration of MPC+ support for a ESCON PCI adapter involves hardware installation on the AIX system and software definitions on both the MVS host and AIX systems. The software definitions must be closely coordinated between the two systems.

The following figure gives an overview of where software definitions are required. Arrows indicate where definition statements refer to parameters coded on other definition statements within that system.

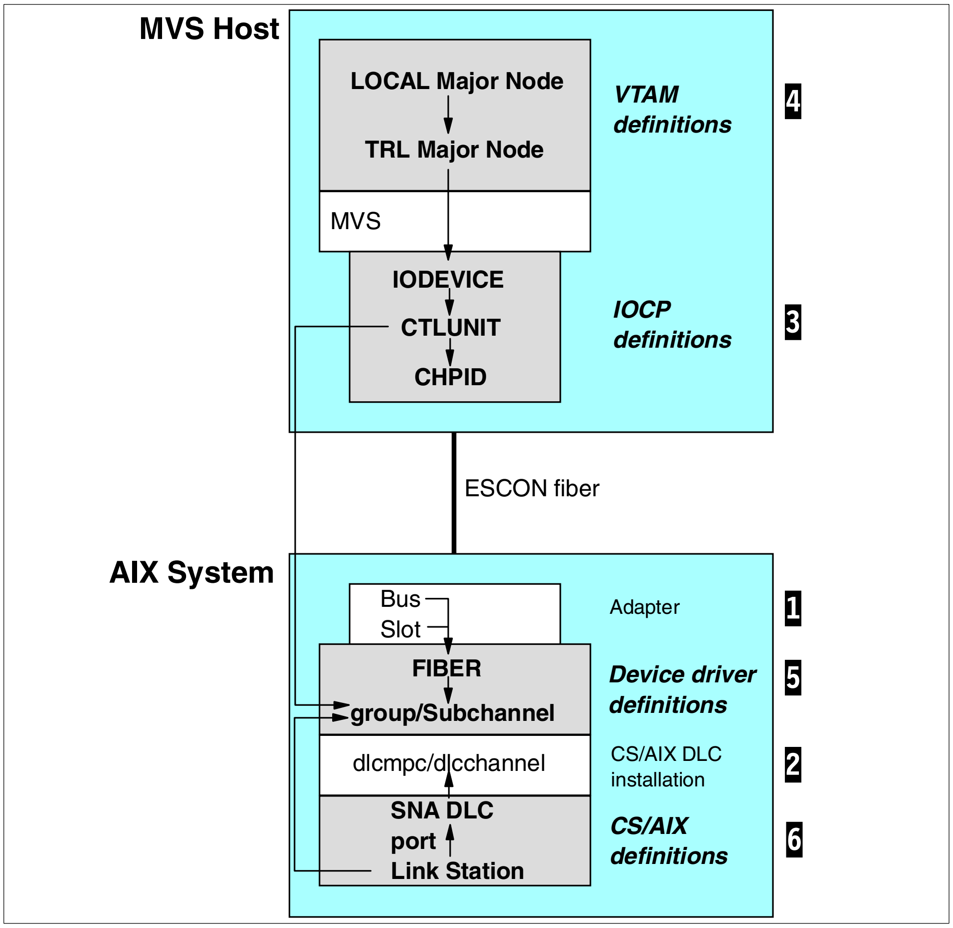


Figure 91. Software definitions for MPC+ support

The following configuration tasks must be performed to enable MPC+ support for CS/AIX. The numbers included in Figure 91 refer to these tasks. These tasks will be covered in more detail in the following sections.

1 Install the communications adapter (and associated software) to support the SNA Channel for AIX feature (see “Install the communications adapter” on page 145)

2 Install the SNA Channel for AIX feature from the CS/AIX distribution media (see “Install the SNA channel for AIX feature” on page 146)

3 Configure the MVS operating system to recognize the AIX system communications adapter (see “Configure the MVS operating system” on page 146)

4 Configure VTAM on the host to communicate with CS/AIX over the MPC+ channel (see "Configure VTAM" on page 148)

5 Configure the communications adapter device driver to the AIX system (see "Configure the communications adapter" on page 150)

6 Configure the channel SNA DLC, port and link station to CS/AIX (see "Configure the adapter to CS/AIX" on page 158)

8.4 Our scenario

The following figure represents the sample configuration we will use to step through and detail the MPC+ ESCON PCI configuration tasks listed above.

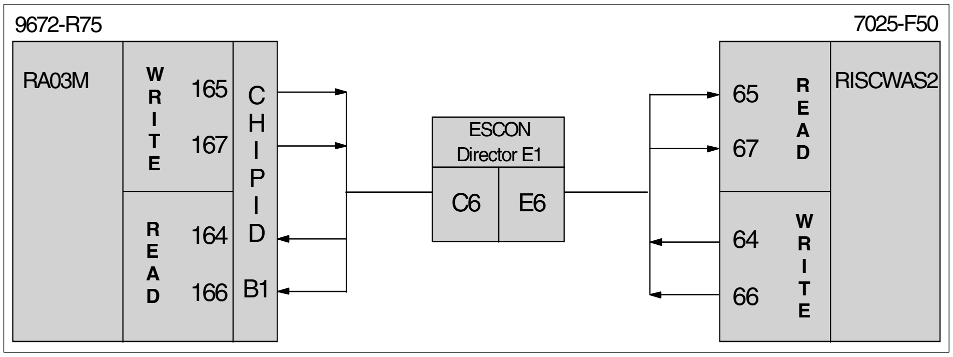


Figure 92. Sample ESCON channel configuration

This figure shows an ESCON connection between a S/390 Model 9672-R75 running OS/390 V2.8 (RA03M) and an RS/6000 Model 7025-F50 running AIX V4.3.3 (RISCWAS2). Two subchannels are used for write operations and two are used for read. The subchannels defined for write on MVS must be defined for read on the RS/6000. Our sample configuration has the ESCON channels routed through an ESCON director. Zero, one or two ESCON directors are supported allowing the RS/6000 machine to be located up to 43 kilometers from the MVS host.

The following sections detail the numbered steps displayed in Figure 91 on page 144.

8.4.1 Install the communications adapter

The S/390 ESCON Channel PCI Adapter is based on the ARTIC960 family of adapters. It is comprised of an ARTIC BASE PCI Adapter, an Application Interface Board and a memory SIMM. See *PCI Adapter Placement*

Reference, SA38-0538 for details on physically installing the adapter in an RS/6000 system.

The ESCON channel adapter optional program product (5765-D49) provides software support for the ESCON PCI adapter. It is installed from CD-ROM using SMIT. You must install both the devices.pci.esconCU and devices.common.IBM.esconCU.mpc filesets for MPC support. Details of the software installation process are included in *S/390 ESCON Channel PCI Adapter: User's Guide and Service Information,* SC23-4232.

8.4.2 Install the SNA channel for AIX feature

As mentioned previously, the SNA Channel for AIX feature is included on the CS/AIX distribution media. The following two filesets make up the SNA Channel for AIX feature:

1. sna.dlcchannel
2. sna.dlcmpc

If these filesets were not automatically installed during the CS/AIX installation, they may be installed using SMIT. Enter the following command from the AIX command line:

```
smit install_selectable_all
```

See *IBM Communications Server for AIX Channel Connectivity User's Guide*, SC31-8219 for more details.

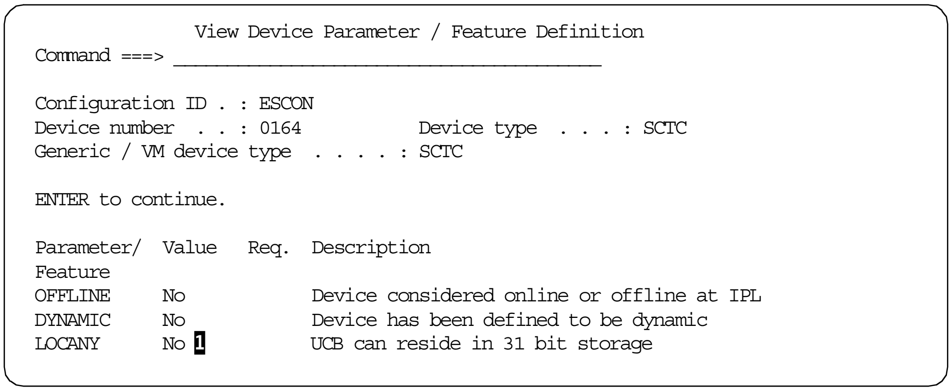
8.4.3 Configure the MVS operating system

Both the host processor hardware definitions and the MVS operating system must be configured to recognize the ESCON PCI adapter and its associated device drivers. There are two steps to perform:

1. Hardware Configuration Definition - HCD gen, which in turn creates the Input/Output Control Program - IOCP gen
2. Operating system I/O gen

8.4.3.1 HCD/IOCP gen

Figure 93 shows the HCD definitions for the ESCON PCI channel at address 164. There are HCD device definitions for each address we used (164-167).



```
                View Device Parameter / Feature Definition
Command ===> ________________________________________

Configuration ID . : ESCON
Device number  . . : 0164          Device type  . . . : SCTC
Generic / VM device type  . . . . : SCTC

ENTER to continue.

Parameter/  Value   Req.  Description
Feature
OFFLINE     No            Device considered online or offline at IPL
DYNAMIC     No            Device has been defined to be dynamic
LOCANY      No 1          UCB can reside in 31 bit storage
```

Figure 93. HCD definitions for ESCON PCI channel connection

Note the LOCANY value at 1 in Figure 93. Even though later releases of MVS support 31-bit UCB addresses, VTAM does not. Therefore, the LOCANY must be specified as `NO` on the DEVICE FEATURES panel in HCD.

8.4.3.2 Operating system I/O gen

Figure 94 shows the IOCP definitions generated from the HCD gen used on our 9672-R75 host system running OS/390 native in an LPAR configuration. It is recommended that the IOCP definitions be used for the MVS I/O gen.

```
         CHPID PATH=((B1)1),TYPE=CNC,SWITCH=E1 2
*
         CNTLUNIT CUNUMBR=160,UNIT=RS6K 3,PATH=(B1)1
               CUADD=1 4,LINK=(E6)5,UNITADD=((60,32)6)
DEV160   IODEVICE UNIT=RS6K 3,ADDRESS=(160,32)7,CUNUMBR=(160)
```

Figure 94. IOCP definitions for ESCON PCI channel connection

1 The fiber to the ESCON director is connected to host CHPID B1.

2 The ESCON director is number E1. If an ESCON director is not used, the `SWITCH` parameter is not required.

3 `UNIT=RS6K` or `UNIT=RS6K-2` is specified for ESCON PCI connections.

4 `CUADD=1` specifies a virtual control unit image on the AIX machine. It must match the `CUADD` parameter on the AIX ESCON subchannel definitions.

5 `LINK=E6` specifies the port on the ESCON director the RS/6000 fiber is connected to. If an ESCON director is not used, the `LINK` parameter is not required. See Figure 92 on page 145 to see where we got E6 from.

6 `UNITADD=((60,32))` specifies a range of subchannel addresses defined with this definition. This `CNTLUNIT` entry defines 32 subchannel addresses starting with 60.

7 The `IODEVICE` macro assigns host addresses to the subchannel range specified in the `CNTLUNIT` macro. Our example uses address 160 for subchannel 60, 161 for subchannel 61, and so on.

An MVS missing interrupt handler entry must be added for each MPC address to prevent reads from timing out on the channel. Figure 95 shows the missing interrupt handler entries required for the addresses used in our example. These entries must be in SYS1.PARMLIB member IECIOSxx.

```
MIH TIME=00:00,DEV=(164-165)
MIH TIME=00:00,DEV=(166-167)
```

Figure 95. MVS missing interrupt handler

See both *IBM Communications Server for AIX Channel Connectivity User's Guide,* SC31-8219, and *AIX V4.3 S/390 ESCON Channel PCI Adapter: User's Guide and Service Information*, SC23-4232 for additional detail on configuring the MVS operating system and hardware to support SNA Channel for AIX.

8.4.4 Configure VTAM

See item 4 in Figure 91 on page 144 to see where we are in the MPC+ configuration process.

Support for MPC+ within the host VTAM environment requires two additional major nodes to be configured:

1. Transport Resource List (TRL) major node
2. Local major node

More information on the coding requirements for VTAM can be found in *OS/390 SecureWay Communications Server SNA Resource Definition Reference*, SC31-8565, and *OS/390 SecureWay Communications Server SNA Network Implementation Guide*, SC31-8563.

8.4.4.1 Transport resource list major node

A TRL major node contains transport resource list elements (TRLE) that describe the connectivity characteristics of an MPC+ connection.

```
RA3R6TRL VBUILD TYPE=TRL
RA3MPCA 1 TRLE  LNCTL=MPC,
               READ=(164,166), 2
               WRITE=(165,167), 3
               MAXBFRU=16, 4
               REPLYTO=3.0,
               MPCLEVEL=HPDT 5
```

Figure 96. Transport resource list definitions for MPC+ channel connection

1 This name must match the TRLE name specified on the PU macro for the connection defined in the local major node (see 1 in Figure 97).

2 The subchannel addresses specified as READ must be the addresses that CS/AIX is writing to (see item 3 in Figure 108 on page 156).

3 The subchannel addresses specified as WRITE must be the addresses that CS/AIX is reading from (see item 2 in Figure 108 on page 156).

4 `MAXBFRU` specifies the number of 4 KB buffer pages VTAM uses to receive data when activating a multipath channel. The same `MAXBFRU` value is used for each of the READ subchannels.

5 `MPCLEVEL` specifies the level of MPC capability to be used for the connection. `MPCLEVEL=HPDT` is required for MPC+. In addition, `HPR=RTP` must be coded in the start list for VTAM.

8.4.4.2 Local major node

A VTAM local major node defines the characteristics of the device (CS/AIX on an RS/6000) at the other end of the MPC+ connection.

```
RA3R6MPC VBUILD TYPE=LOCAL
RA3MPCPU PU    TRLE=RA3MPCA, 1
               CONNTYPE=APPN,
               XID=YES,
               DELAY=0.0,
               CPCP=YES,
               CAPACITY=136M
```

Figure 97. Local major node definitions for MPC+ channel connection

1 The TRLE name specified here must match the TRLE defined in the TRL major node (see 1 in Figure 96).

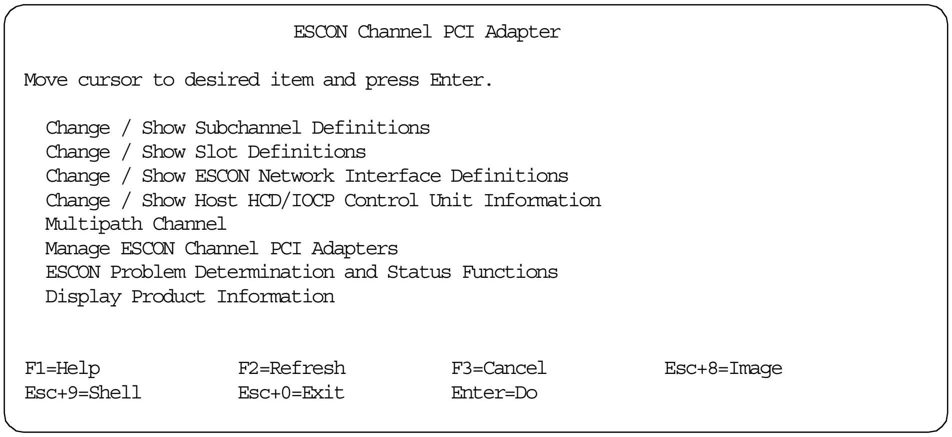
8.4.5 Configure the communications adapter

See item 5 in Figure 91 on page 144 to see where we are in the MPC+ configuration process.

Configuring the ESCON PCI channel adapter to AIX is done using SMIT. The ESCON Channel PCI Adapter menu displayed in Figure 98 is the starting point for configuration and use. It can be reached by navigating through the following SMIT panels. Click **smit -> Devices -> Communication -> ESCON Channel PCI Adapter**

Or, use the fastpath `smit esca_pci`.

This configuration process is covered in more detail in *AIX V4.3 S/390 ESCON PCI Adapter: User's Guide and Service Information*.



```
                           ESCON Channel PCI Adapter

Move cursor to desired item and press Enter.

  Change / Show Subchannel Definitions
  Change / Show Slot Definitions
  Change / Show ESCON Network Interface Definitions
  Change / Show Host HCD/IOCP Control Unit Information
  Multipath Channel
  Manage ESCON Channel PCI Adapters
  ESCON Problem Determination and Status Functions
  Display Product Information


F1=Help             F2=Refresh          F3=Cancel           Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 98. ESCON channel PCI adapter SMIT menu

The following configuration steps are required:

1. Add ESCON subchannel definitions (page 151)
2. Add slot definitions (page 153)
3. Add an MPC group definition (page 155)
4. Make and configure the ESCON PCI adapter (page 157)

Figure 99 shows the SMIT panel flow matching these configuration steps.

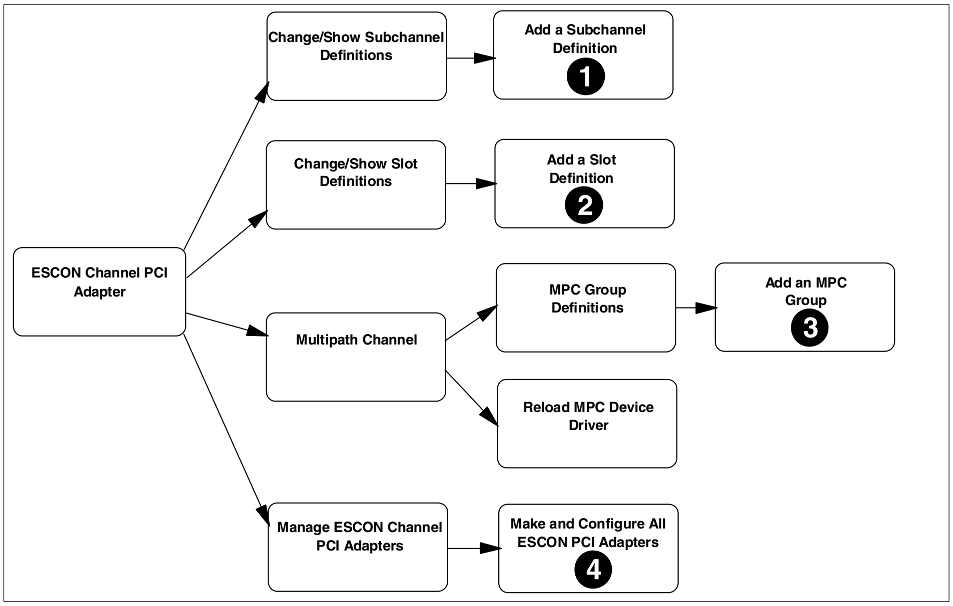
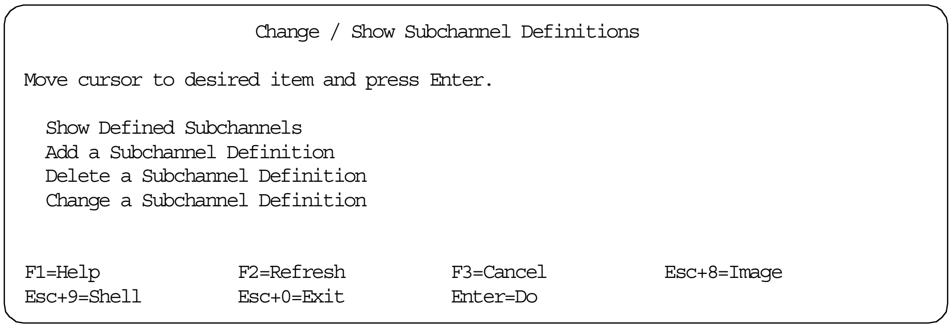

Change/Show Subchannel Definitions
Add a Subchannel Definition
1
Change/Show Slot Definitions
Add a Slot Definition
2
ESCON Channel PCI Adapter
MPC Group Definitions
Add an MPC Group
3
Multipath Channel
Reload MPC Device Driver
Manage ESCON Channel PCI Adapters
Make and Configure All ESCON PCI Adapters
4

Figure 99. SMIT panel flow to configure an ESCON channel PCI adapter

8.4.5.1 Add ESCON subchannel definitions

To add ESCON subchannel definitions, select **Change/Show Subchannel Definitions** from the ESCON Channel PCI Adapter menu. Figure 100 displays this menu.

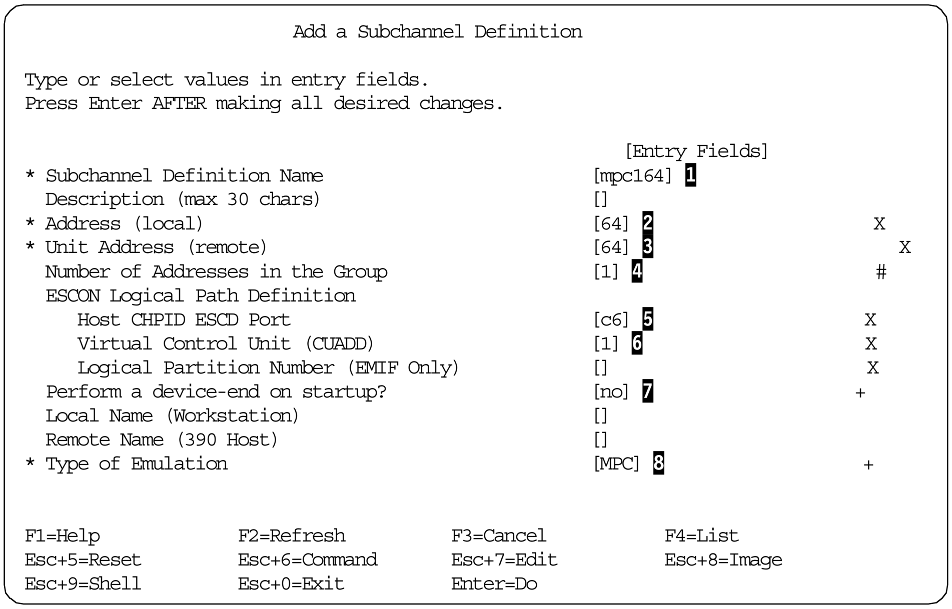


```
                    Change / Show Subchannel Definitions

Move cursor to desired item and press Enter.

  Show Defined Subchannels
  Add a Subchannel Definition
  Delete a Subchannel Definition
  Change a Subchannel Definition


F1=Help             F2=Refresh          F3=Cancel           Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 100. Change/Show Subchannel Definitions

This menu allows you to show, add, delete or change a subchannel definition. On the Change/Show Subchannel Definitions menu, select **Add a Subchannel Definition**.

Figure 101 shows the SMIT menu used to define an ESCON subchannel. The subchannel definitions menu allows you to define the characteristics of a subchannel. This includes the path to the S/390 channel subsystem as well as the type of channel emulation to use.



```
                          Add a Subchannel Definition

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
* Subchannel Definition Name                       [mpc164] 1
  Description (max 30 chars)                       []
* Address (local)                                  [64] 2                 X
* Unit Address (remote)                            [64] 3                   X
  Number of Addresses in the Group                 [1] 4                  #
  ESCON Logical Path Definition
     Host CHPID ESCD Port                          [c6] 5                X
     Virtual Control Unit (CUADD)                  [1] 6                 X
     Logical Partition Number (EMIF Only)          []                    X
  Perform a device-end on startup?                 [no] 7               +
  Local Name (Workstation)                         []
  Remote Name (390 Host)                           []
* Type of Emulation                                [MPC] 8               +


F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 101. Adding an ESCON subchannel

1 Associates this particular subchannel definition with a slot (see Figure 104 on page 154) containing an ESCON channel adapter.

2 Specifies the local address used by CS/AIX to map into the correct subchannels.

3 Specifies the hexadecimal subchannel address defined in the IOCP definition on the S/390 host. The address is taken from the range of addresses specified in the IOCP `UNITADD` parameter. See 6 in Figure 94 on page 147.

4 Defines how many consecutive subchannel addresses are used in this definition. For MPC, this value must be 1.

5 If an ESCON (ESCD) director is being used, this specifies the port number of the ESCD (switch) to which the host channel is attached. Use the port number that has the fiber leading to the S/390 host. See Figure 92 on page 145 to see where we got C6 from.

6 Must match the CUADD parameter in the host HCD/IOCP gen. See 4 in Figure 94 on page 147.

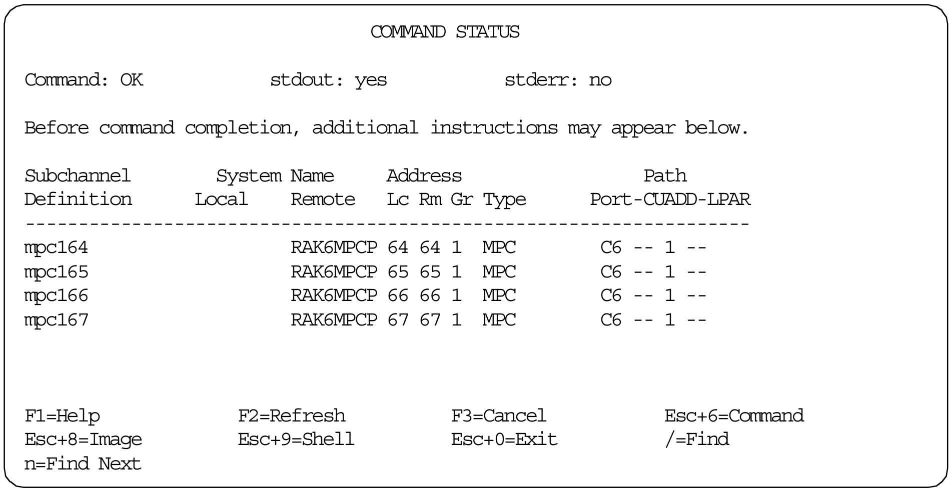
7 Specifies whether a device-end should be issued from the AIX system to the S/390 during startup. Must be NO for MPC subchannels.

8 Defines the device level protocol for the subchannel definition used. Must be MPC.

Figure 101 shows subchannel definitions being added for address 64. The same must also be done for subchannels 65, 66 and 67.

Changes or additions to subchannel definitions will not take effect until a reboot or the adapter has been taken offline and brought back online.

After all our subchannel definitions have been added, selecting **Show Defined Subchannels** (see Figure 100 on page 151) results in the following display.



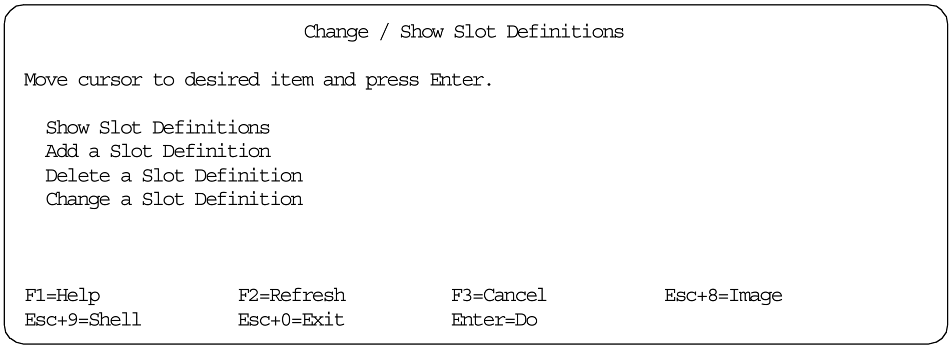
```
                                COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

Subchannel        System Name     Address               Path
Definition      Local    Remote   Lc Rm Gr Type      Port-CUADD-LPAR
--------------------------------------------------------------------
mpc164                   RAK6MPCP 64 64 1  MPC        C6 -- 1 --
mpc165                   RAK6MPCP 65 65 1  MPC        C6 -- 1 --
mpc166                   RAK6MPCP 66 66 1  MPC        C6 -- 1 --
mpc167                   RAK6MPCP 67 67 1  MPC        C6 -- 1 --



F1=Help             F2=Refresh          F3=Cancel           Esc+6=Command
Esc+8=Image         Esc+9=Shell         Esc+0=Exit          /=Find
n=Find Next
```

Figure 102. Show defined subchannels output

8.4.5.2 Add slot definitions

A PCI ESCON channel adapter is identified to AIX by the PCI slot into which it is installed. The Add a Slot Definition menu identifies which previously defined subchannel definitions are assigned to a specific ESCON channel adapter.

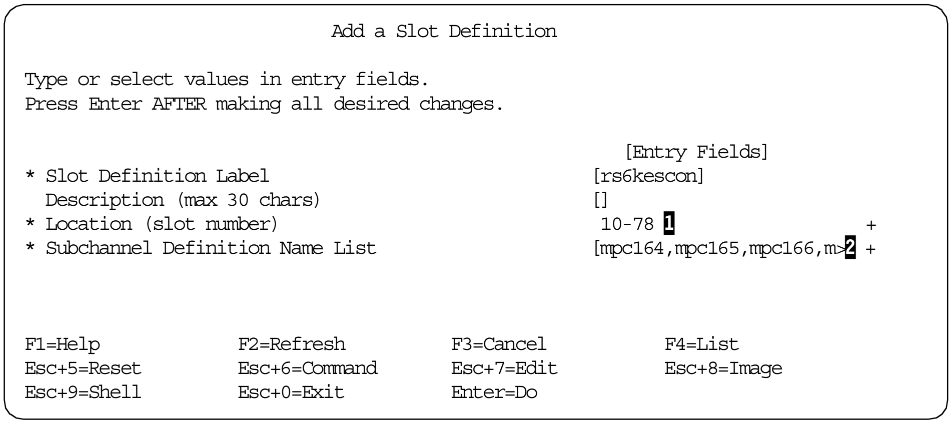
From the ESCON Channel PCI Adapter menu shown in Figure 98 on page 150, select **Change/Show Slot Definitions**. The following menu is displayed.



```
                        Change / Show Slot Definitions

Move cursor to desired item and press Enter.

  Show Slot Definitions
  Add a Slot Definition
  Delete a Slot Definition
  Change a Slot Definition



F1=Help             F2=Refresh          F3=Cancel           Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 103. Managing slots

From this menu, selecting **Add a Slot Definition** results in the following menu being displayed.



```
                          Add a Slot Definition

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
* Slot Definition Label                            [rs6kescon]
  Description (max 30 chars)                       []
* Location (slot number)                            10-78 1             +
* Subchannel Definition Name List                  [mpc164,mpc165,mpc166,m>2 +



F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

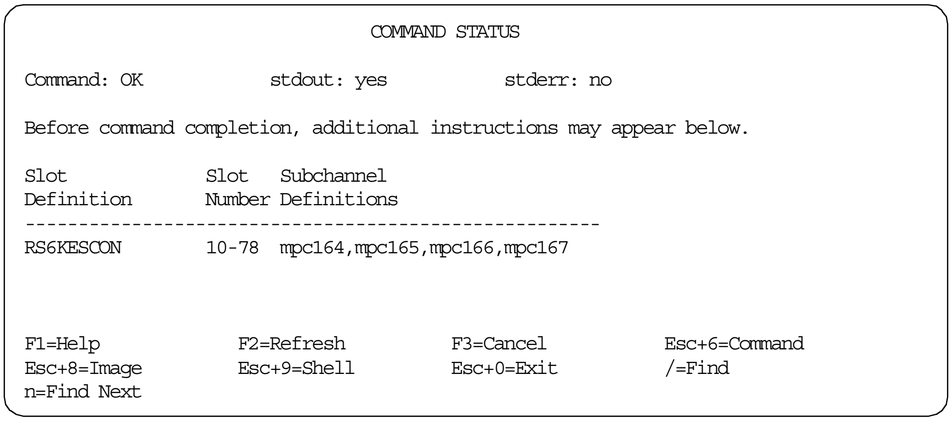
Figure 104. Adding an ESCON slot definition

1 Specify a 4-digit slot number. A list of valid PCI slots containing an ESCON channel adapter(s) can be retrieved using F4.

2 Specifies a list of subchannel definitions used by the ESCON channel adapter. The subchannel names specified here were defined previously in Figure 101 on page 152.

Changes or additions to slot definitions will not take effect until a reboot or the adapter has been taken offline and brought back online.

After our slot definition has been added, selecting **Show Slot Definitions** (see Figure 103 on page 154) results in the following display.



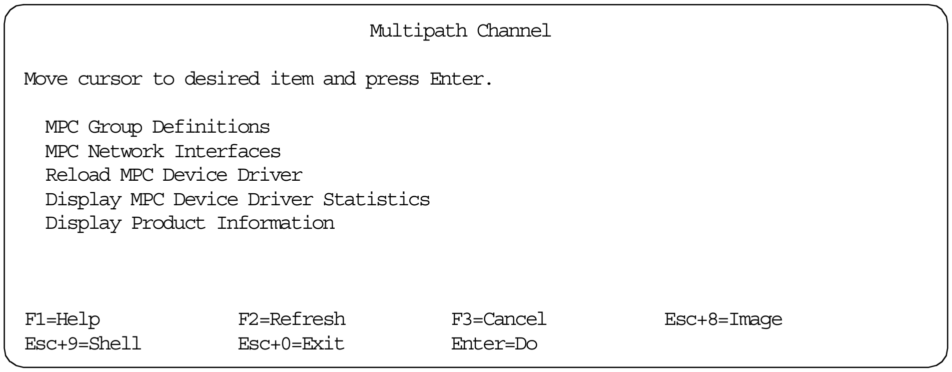
```
                                 COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

Slot             Slot   Subchannel
Definition       Number Definitions
-----------------------------------------------------
RS6KESCON        10-78  mpc164,mpc165,mpc166,mpc167



F1=Help             F2=Refresh          F3=Cancel           Esc+6=Command
Esc+8=Image         Esc+9=Shell         Esc+0=Exit          /=Find
n=Find Next
```

Figure 105. Show defined slots output

8.4.5.3 Add an MPC group definition

An MPC group definition is where you define which subchannels are READ and which are WRITE.

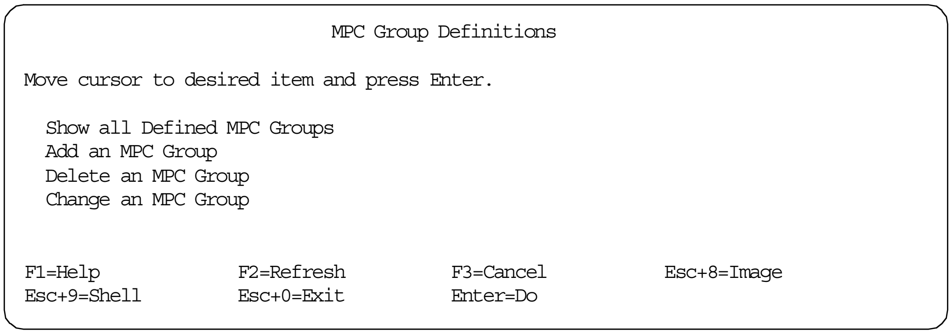
From the ESCON Channel PCI Adapter menu shown in Figure 98 on page 150, select **Multipath Channel**. The following menu is displayed.



```
                                Multipath Channel

Move cursor to desired item and press Enter.

  MPC Group Definitions
  MPC Network Interfaces
  Reload MPC Device Driver
  Display MPC Device Driver Statistics
  Display Product Information



F1=Help             F2=Refresh          F3=Cancel           Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 106. Multipath Channel menu

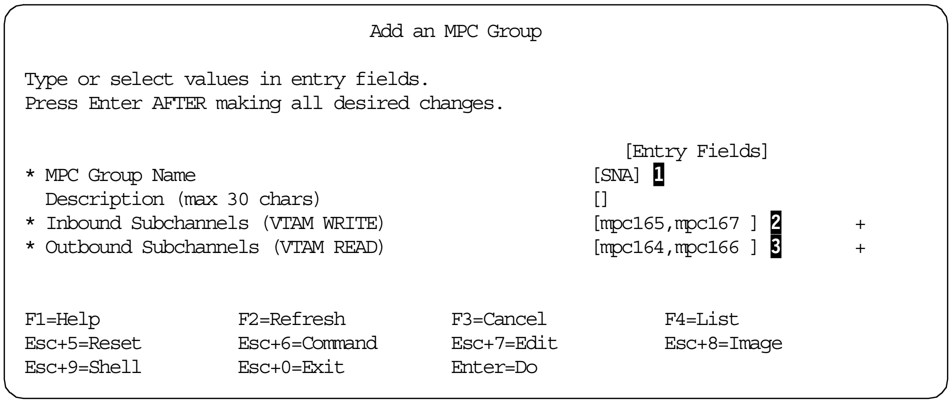
From this menu, select **MPC Group Definitions**. This will display the following menu.



```
                              MPC Group Definitions

Move cursor to desired item and press Enter.

  Show all Defined MPC Groups
  Add an MPC Group
  Delete an MPC Group
  Change an MPC Group


F1=Help             F2=Refresh          F3=Cancel           Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 107. MPC Group Definitions menu

This menu allows complete control of MPC group definitions. Select **Add an MPC Group** to define a new group. The following menu is displayed.



```
                                  Add an MPC Group

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                        [Entry Fields]
* MPC Group Name                                     [SNA] 1
  Description (max 30 chars)                         []
* Inbound Subchannels (VTAM WRITE)                   [mpc165,mpc167 ] 2      +
* Outbound Subchannels (VTAM READ)                   [mpc164,mpc166 ] 3      +


F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 108. Adding an MPC group

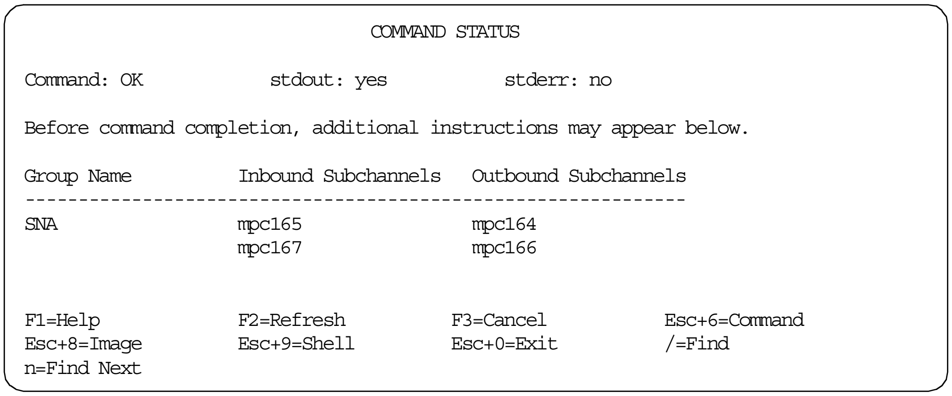
1 Specifies the MPC group name. This name is used when configuring an MPC+ channel link station to CS/AIX. See Figure 116 on page 162.

2 Lists the subchannel names that are used for reading by CS/AIX. They must be defined as WRITE in the host VTAM TRLE major node.

3 Lists the subchannel names that are used for writing by CS/AIX. They must be defined as READ in the host VTAM TRLE major node.

Whenever MPC group definitions have been added, deleted or changed, the MPC device driver must be reloaded before the changes will take effect. See **Reload MPC Device Driver** in Figure 106 on page 155.

After the MPC Group has been added, selecting **Show all Defined MPC Groups** (see Figure 107 on page 156) results in the following display.



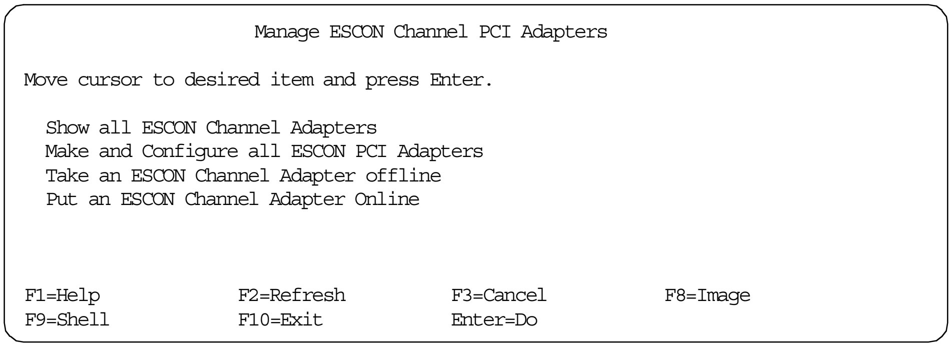
```
                                COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

Group Name           Inbound Subchannels   Outbound Subchannels
--------------------------------------------------------------
SNA                  mpc165                mpc164
                     mpc167                mpc166


F1=Help              F2=Refresh           F3=Cancel           Esc+6=Command
Esc+8=Image          Esc+9=Shell          Esc+0=Exit          /=Find
n=Find Next
```

Figure 109. Show defined MPC groups output

8.4.5.4 Make and configure the ESCON PCI adapter

When an ESCON channel adapter is initially installed and configured, it is controlled by the standard ARTIC-based device driver. The Make and Configure All ESCON PCI Adapters process will unconfigure the ARTIC device driver and reconfigure the ESCON device driver.

From the ESCON Channel PCI Adapter menu shown in Figure 98 on page 150, select **Manage ESCON Channel PCI Adapters**. The following menu is displayed.



```
                      Manage ESCON Channel PCI Adapters

Move cursor to desired item and press Enter.

  Show all ESCON Channel Adapters
  Make and Configure all ESCON PCI Adapters
  Take an ESCON Channel Adapter offline
  Put an ESCON Channel Adapter Online



F1=Help              F2=Refresh           F3=Cancel           F8=Image
F9=Shell             F10=Exit             Enter=Do
```

Figure 110. Managing ESCON channel PCI adapters

From this menu, select **Make and Configure All ESCON Adapters**. This will reconfigure the adapter for ESCON support.

8.4.6 Configure the adapter to CS/AIX

See item 6 in Figure 91 on page 144 to check where we are in the MPC+ configuration process.

For CS/AIX to use the ESCON PCI channel, three definitions must be added to the CS/AIX configuration:

1. DLC
2. Port
3. Link station

The SMIT interface, the Motif interface, the `snaadmin` command line, or the Web Administration interface may be used to create these definitions. When using the Motif interface, the DLC is defined automatically when the port is defined. We will use the Motif interface for this scenario.

8.4.6.1 Add a port definition to CS/AIX

Using `xsnaadmin`, click **Services -> Connectivity -> New Port.**

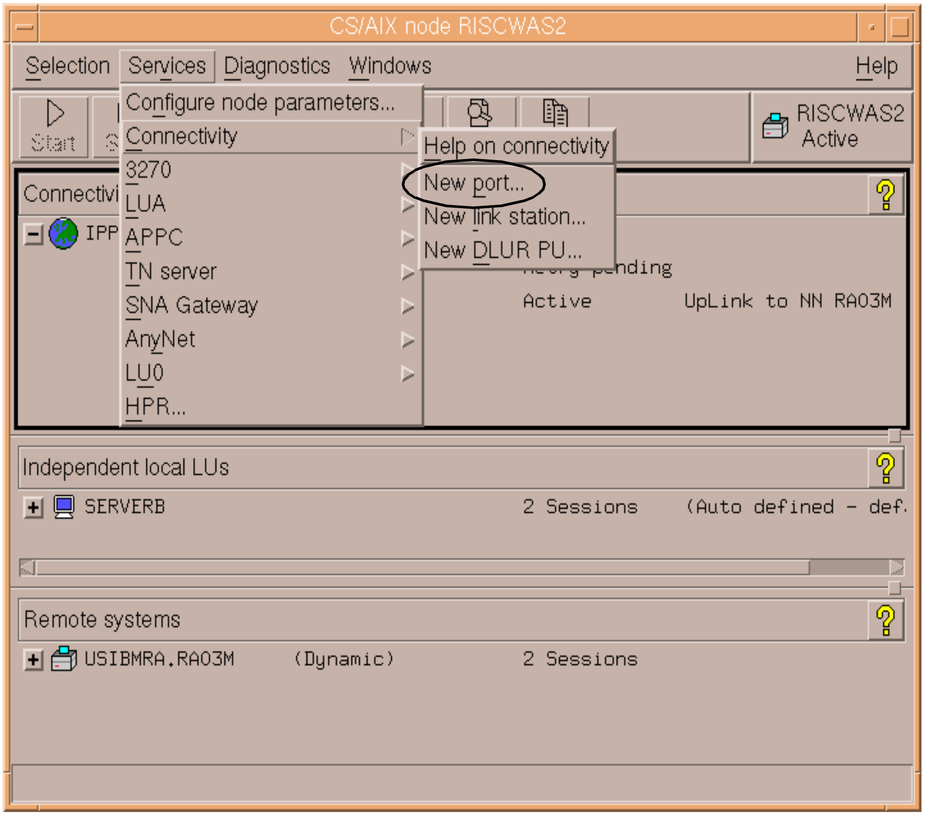


Figure 111. Adding a port to CS/AIX

Select **IBM ESCON Channel card using MPC+** from the selection list as shown in Figure 112.

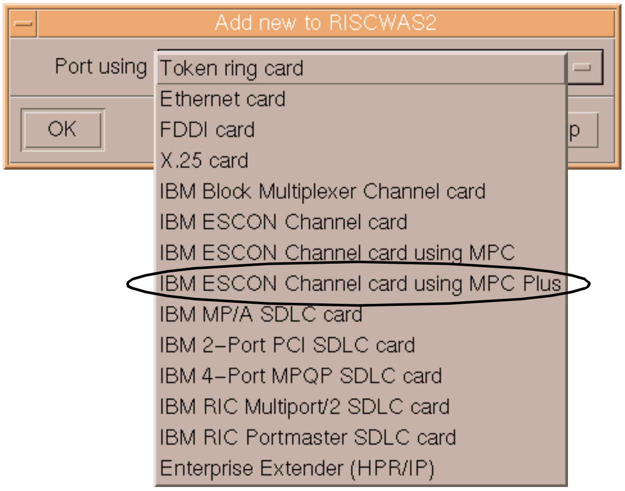
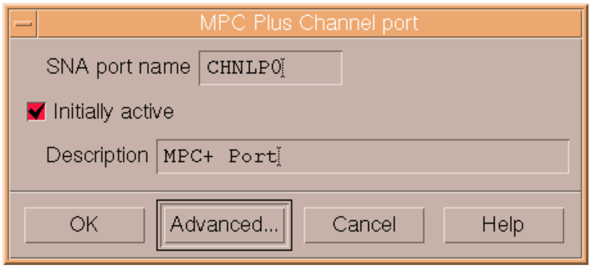

Add new to RISCWAS2
Port using
Token ring card
Ethernet card
FDDI card
X.25 card
IBM Block Multiplexer Channel card
IBM ESCON Channel card
IBM ESCON Channel card using MPC
IBM ESCON Channel card using MPC Plus
IBM MP/A SDLC card
IBM 2−Port PCI SDLC card
IBM 4−Port MPQP SDLC card
IBM RIC Multiport/2 SDLC card
IBM RIC Portmaster SDLC card
Enterprise Extender (HPR/IP)
OK
p

Figure 112. Adding a new MPC+ port definition

This results in the following MPC+ panel being displayed.



SNA port name CHNLP0

☑ Initially active

Description MPC+ Port

Figure 113. MPC+ port characteristics

Modify the SNA port name and description as you see fit.

Defining MPC+ support in our CS/AIX node results in the following additions being made to the CS/AIX node configuration file (/etc/sna/sna_node.cfg).

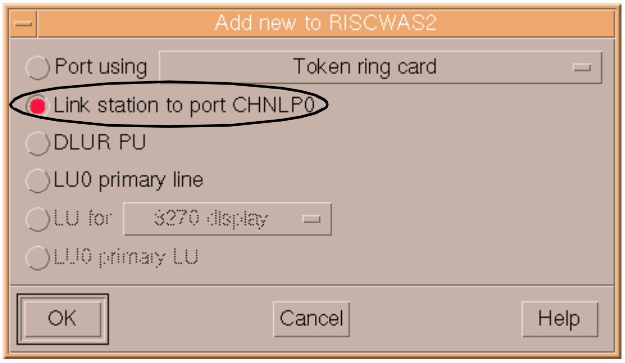
```
T
[define_mpc_plus_dlc]
dlc_name = CHNL0
description = ""
initially_active = YES
.
.
[define_mpc_plus_port]
port_name = CHNLP0
description = MPC+ Port
dlc_name = CHNL0
initially_active = YES
max_rcv_btu_size = 4096
tot_link_act_lim = 64
inb_link_act_lim = 0
out_link_act_lim = 0
act_xid_exchange_limit = 9
nonact_xid_exchange_limit = 5
max_ifrm_rcvd = 7
target_pacing_count = 7
max_send_btu_size = 4096
effect_cap = 78643200
connect_cost = 0
byte_cost = 0
security = SEC_NONSECURE
prop_delay = PROP_DELAY_MINIMUM
user_def_parm_1 = 128
user_def_parm_2 = 128
user_def_parm_3 = 128
.
.
```

Figure 114. MPC+ DLC and port definitions

As can be seen in Figure 114, when we defined the MPC+ port, `xsnaadmin` automatically defined the required MPC+ DLC entries in /etc/sna/sna_node.cfg.

8.4.6.2 Add a link station definition

Use `xsnaadmin` to highlight the MPC+ port just added. Click **New** from the button list. A panel similar to the one shown in Figure 115 will be displayed.



Add new to RISCWAS2

○ Port using Token ring card

● Link station to port CHNLP0

○ DLUR PU

○ LU0 primary line

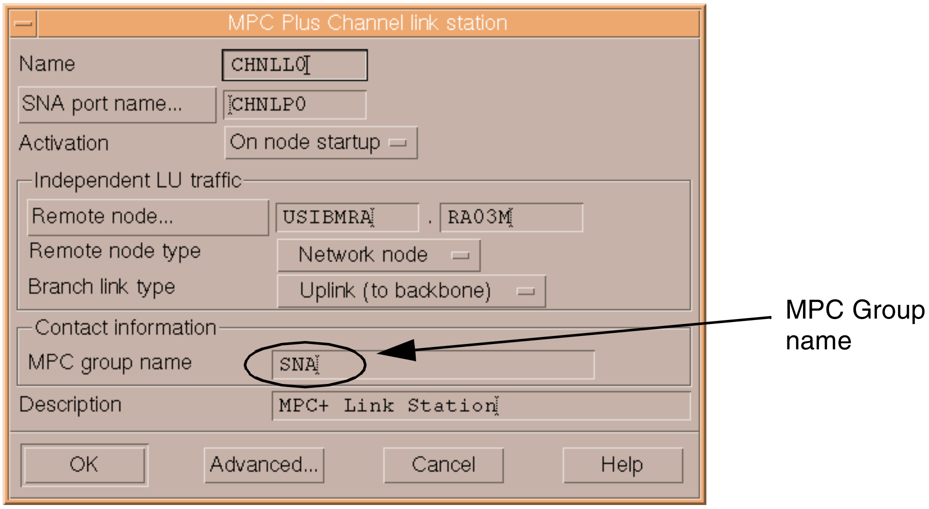
○ LU for 3270 display

○ LU0 primary LU

Figure 115. Adding a link station to the MPC+ port

Note that the entry to add a new link station to the MPC+ port is automatically selected. Click **OK**.

The following link station panel will be displayed.



MPC Plus Channel link station

Name: CHNLL0

SNA port name...: CHNLP0

Activation: On node startup

Independent LU traffic

Remote node...: USIBMRA . RA03M

Remote node type: Network node

Branch link type: Uplink (to backbone)

Contact information

MPC group name: SNA

Description: MPC+ Link Station

Figure 116. Configuring the MPC+ link station

Note that only independent LU traffic is supported over an MPC+ channel. Dependent LU traffic is supported only over a DLUR-DLUS LU 6.2 session.

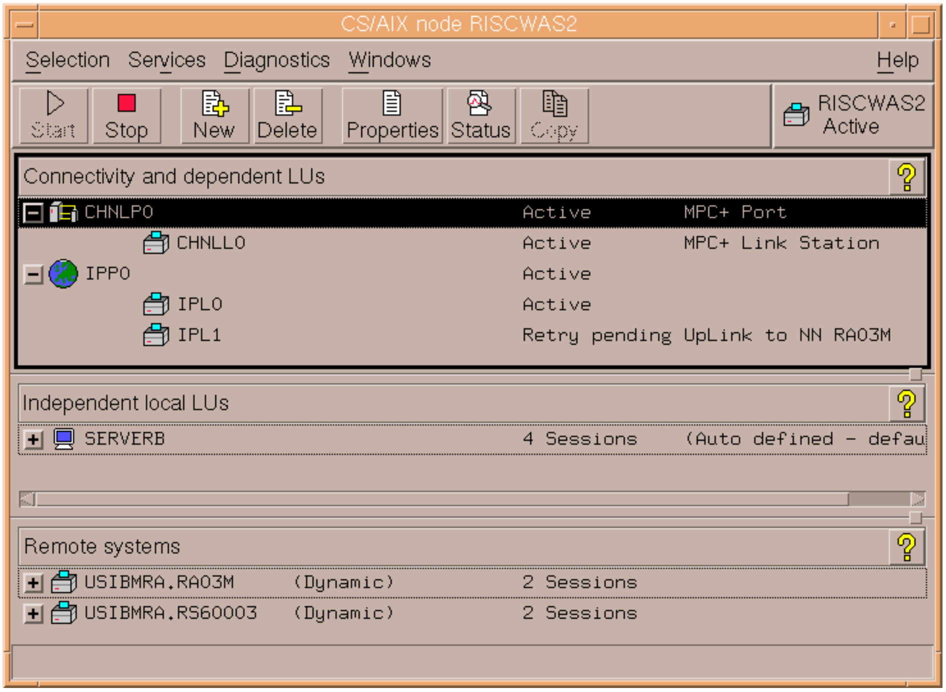
The MPC group name must be the name defined on the Add an MPC Group SMIT menu shown in Figure 108 on page 156.

The following entries were created in /etc/sna/sna_node.cfg when we defined the MPC+ link station.

```
[define_mpc_plus_ls]
ls_name = CHNLL0
description = MPC+ Link Station
port_name = CHNLP0
mpc_group_name = SNA
adj_cp_name = USIBMRA.RA03M
adj_cp_type = NETWORK_NODE
local_node_id = <00000000>
adj_node_id = <00000000>
max_send_btu_size = 4096
ls_attributes = SNA
cp_cp_sess_support = YES
default_nn_server = NO
auto_act_supp = NO
tg_number = 0
limited_resource = NO
disable_remote_act = NO
link_deact_timer = 30
use_default_tg_chars = YES
effect_cap = 78643200
connect_cost = 0
byte_cost = 0
security = SEC_NONSECURE
prop_delay = PROP_DELAY_MINIMUM
user_def_parm_1 = 128
user_def_parm_2 = 128
user_def_parm_3 = 128
target_pacing_count = 7
max_ifrm_rcvd = 0
branch_link_type = UPLINK
adj_brnn_cp_support = ALLOWED
need_vrfy_fixup = NO
initially_active = YES
restart_on_normal_deact = NO
react_timer = 1
react_timer_retry = 65535
```

Figure 117. MPC+ link station definition

Figure 118 shows the xsnaadmin node panel which displays the results of our MPC+ port and link station definitions.



```
Connectivity and dependent LUs
CHNLP0                                     Active          MPC+ Port
        CHNLL0                             Active          MPC+ Link Station
IPP0                                       Active
        IPL0                               Active
        IPL1                               Retry pending UpLink to NN RA03M

Independent local LUs
SERVERB                                    4 Sessions      (Auto defined - defau

Remote systems
USIBMRA.RA03M         (Dynamic)            2 Sessions
USIBMRA.RS60003       (Dynamic)            2 Sessions
```

Figure 118. Active MPC+ port and link station

Chapter 9. DDDLU enhancement

DDDLU is an acronym for Dynamic Definition of Dependent LUs. It is sometimes referred to as Self-Defining Dependent LUs (SDDLU). This feature allows dependent LU definitions to be dynamically created on the host by VTAM when they are needed.

If the host VTAM is DDDLU capable, it will send information to CS/AIX when the link station activates to indicate that the host supports DDDLU. When a host LU is needed, CS/AIX sends in a Reply Product Set ID (PSID) Network Management Vector Transport (NMVT) with the required information VTAM needs to dynamically define the dependent LU.

Dependent LU definitions must still be defined on the CS/AIX node. There are no configuration changes in CS/AIX when connecting to DDDLU capable hosts.

Support for DDDLU hosts was first introduced in CS/AIX V5.

IBM Communications Server for AIX, Version 6 introduces DDDLU power-off support.

9.1 DDDLU power-off feature

The new DDDLU power-off feature allows CS/AIX V6 to send an NMVT power-off message to the host when an LU or application ends. This allows the host (or an application at the host end) to delete the dynamically created LU from its tables.

This feature affects LU types 0-3 only. The NMVT power-off message is sent when an application terminates its use of an LU if the following are true:

- The host supports DDDLU.
- CS/AIX V6 is configured to send the NMVT power-off message.

Using DDDLU without the power-off feature requires no special definitions on the CS/AIX side. The link station and all dependent LUs still must be defined.

However, sending the NMVT power-off message requires configuration changes. Sending the NMVT power-off message is configurable on a per-PU basis. The default is to not send the NMVT power-off message.

The NMVT power-off message support must be configured using the `snaadmin` command line interface or a node operator facility (NOF) API program. The other CS/AIX configuration tools (SMIT, Motif administration program, Web administration program) do not expose the power-off option.

The following snaadmin commands support specification of the DDDLU power-off parameter:

define_internal_pu	defines a PU on the local node that is served by DLUR
define_channel_ls	defines or modifies a channel link station
define_mpc_ls	defines or modifies an MPC link station
define_qllc_ls	defines or modifies an QLLC link station
define_sdlc_ls	defines or modifies an SDLC link station.
define_tr_ls	defines or modifies a token-ring link station.
define_ethernet_ls	defines or modifies an Ethernet link station.
define_fddi_ls	defines or modifies an FDDI link station.

The parameter on each of these commands that controls the DDDLU power-off support is:

```
dddlu_offline_supported = NO,YES (NO)
```

This parameter specifies whether the local PU should send NMVT power-off messages to the host. If the host system supports DDDLU, CS/AIX sends NMVT power-off to the host when it has finished using a dynamically defined LU. The default is NO.

DDDLU Documentation

IBM Communications Server for AIX Administration Command Reference, Version 6, SC31-8587, documents the use of these commands and parameters. However, the *Administration Command Reference* publication shipped with CS/AIX describes the incorrect DDDLU power-off parameter. It states that the DDDLU power-off parameter is:

```
pu_can_send_dddlu_offline
```

This is incorrect. The correct parameter is:

```
dddlu_offline_supported
```

To modify the value for the dddlu_offline_supported parameter without resetting other parameter values, issue snaadmin -c define_* and specify the resource name to be changed. For example:

```
snaadmin -c define_tr_ls, ls_name=TRL0, dddlu_offline_supported=YES
```

Part 4. Administration

Chapter 10. Web Administration program

In this chapter, we will review the range of tools provided with CS/AIX that may be used to configure and administer the system. We will then go into more detail on using the new Web Administration program to configure and manage a CS/AIX system.

10.1 Overview

CS/AIX includes the following administration tools:

- Motif administration program
- SMIT
- Command-line administration program
- Web Administration program
- Service point command facility
- Node Operator Facility (NOF) API

10.1.1 Motif administration program

The easiest way to define and modify the CS/AIX configuration is to use the Motif administration program (xsnaadmin). All the CS/AIX panels you have seen up to now in this book are from the Motif administration program. This program provides a graphical user interface from which you can view and manage CS/AIX resources.

The Motif administration program can be used to manage both node resources and domain resources. For each type of communications (such as 3270 or APPC), the program guides you in setting up the configuration of the required resources.

The Motif administration program includes help panels that provide overview information for SNA and CS/AIX, reference information for CS/AIX dialog, and guidance for performing specific tasks.

Before starting the Motif administration program, make sure the CS/AIX software is enabled on the local node. The Motif administration program will not automatically start CS/AIX. Enable the CS/AIX software by issuing the command:

```
sna start
```

To start the Motif Administration program in the background, issue the following command:

```
xsnaadmin &
```

The Motif administration program initially presents the Node window, which displays resource information for the local node. If you have not yet configured the node, the program prompts you to do so and leads you through the steps required to configure it.

Note: The Motif administration program enables you to set up all required parameters for standard CS/AIX configurations. For advanced parameters, the Motif administration program supplies default values. You need to supply only the essential configuration information, which enables you to set up SNA communications quickly and easily.

The main advantage to using the Motif administration program to manage your system is that it provides context-sensitive guidance for node configuration and management. The panels and data entry fields displayed are dynamically presented and modified based on data entered and field selections made on the current and previous panels.

10.1.2 SMIT administration program

SMIT provides a menu-based interface to configure and manage CS/AIX resources. It can be used either from a Motif interface or from an ASCII terminal.

SMIT provides the same administration functions as the Motif administration program, including help panels for each SMIT panel. Before you can use SMIT to administer CS/AIX, the CS/AIX software must be enabled on the local node. If you attempt to use SMIT to configure a CS/AIX system without first enabling the software, it is enabled for you.

Note that unlike the Motif administration program, the SMIT dialogs are not dynamic and context-sensitive.

10.1.3 Command-line administration program

The command-line administration program, snaadmin, enables you to issue commands to configure and manage individual CS/AIX resources. You can use snaadmin either directly from the AIX command prompt or from within a shell script.

Commands can be issued to the CS/AIX node to manage the node’s resources, or to the domain configuration file to manage domain resources.

The snaadmin command-line administration program can be used for all possible CS/AIX configuration parameters, while xsnaadmin, SMIT, and the Web Administration program only expose the most common subset of parameters.

You can get help for command-line administration by using any of the following commands:

snaadmin -h provides basic help for command-line administration and usage information for command-line help.

snaadmin -h -d provides a list of commands that can be supplied to the snaadmin program.

snaadmin -h *command* provides help for the named command.

snaadmin -h -d *command* provides detailed help for the named command, including a list of the configuration parameters that can be specified with the command.

Refer to the *Communications Server for AIX Administration Command Reference*, SC31-8587, for more information.

10.1.4 Network operator facility API

The CS/AIX NOF application program interface allows you to write your own application programs to administer CS/AIX.

All the CS/AIX administration tools use the NOF API.

The CS/AIX NOF API provides access to a standard set of commands, called NOF verbs, that can be used to administer the CS/AIX system from within an application program. These verbs enable you to define and delete resources, specify CS/AIX parameters such as diagnostics levels and file names, start and stop defined resources, and query the definition or current status of resources.

The NOF verbs provide the same functions as commands issued to the command-line administration program snaadmin, or as records in a CS/AIX configuration file. For example, the NOF verb DEFINE_LOCAL_LU is equivalent both to a `define_local_lu` command issued to the snaadmin program, and to a define_local_lu record in a configuration file; all three of them perform the same function, which is to specify the parameters of a CS/AIX local APPC LU.

10.1.5 Service point command facility

The service point command facility is one of the functions provided by the CS/AIX remote command facility (RCF). The RCF operates in conjunction with the NetView program at a host computer enabling a NetView operator to issue commands from the host NetView program to the CS/AIX computer.

The service point command facility (SPCF) enables a NetView operator to issue CS/AIX administration commands from NetView using the same syntax as the command-line administration program, snaadmin.

10.1.6 Web Administration program

The Web Administration program provides CS/AIX configuration capabilities similar to those found using SMIT, while using a display panel interface similar to the Motif administration program. It allows you to administer CS/AIX from your Web browser without the need to start an X session or Telnet session to the CS/AIX server, and is particularly useful when connecting over slow or unreliable links.

The Web Administration program provides a subset of the functions provided by the Motif administration program. It is not context-sensitive to user input, unlike the Motif administration program.

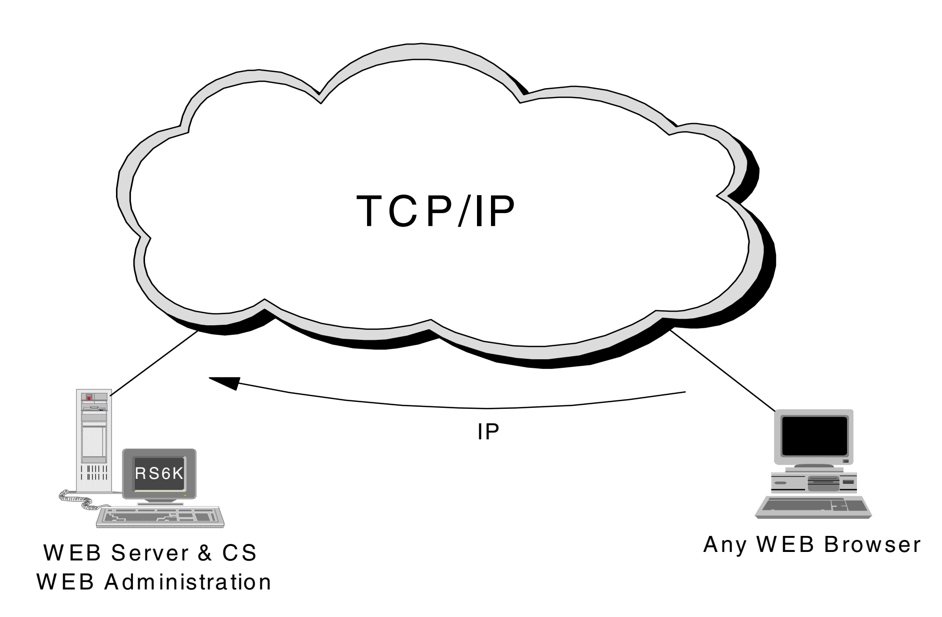


Figure 119. Web Administration

The Web Administration program requires a Web server to be running on the same AIX system as CS/AIX. The Web server must support Java 1.1 servlets.

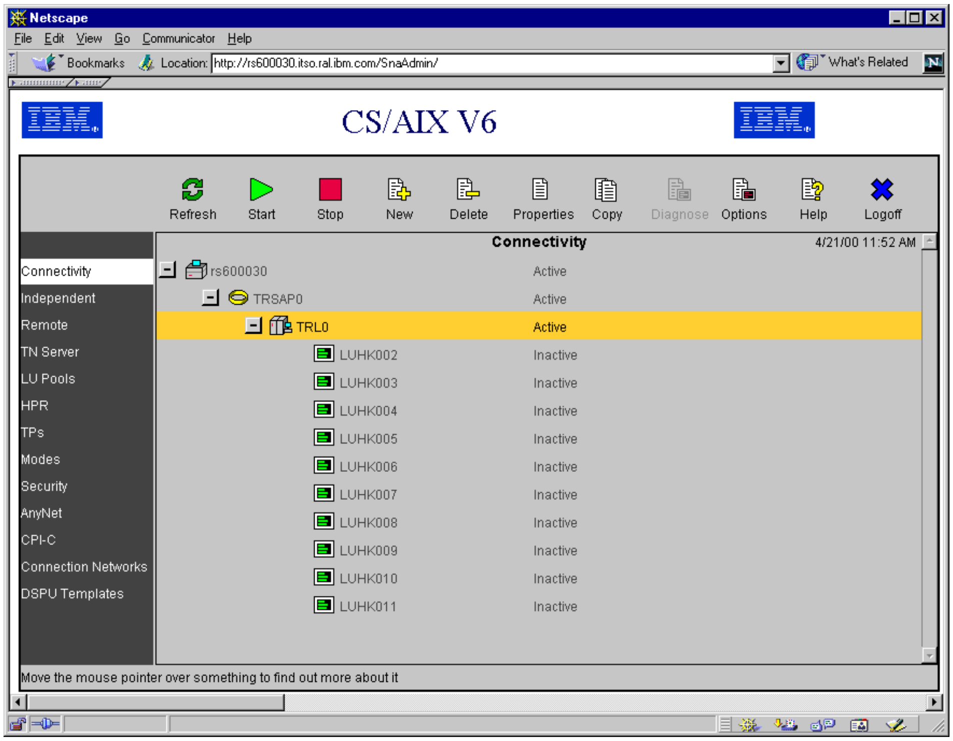
To use the Web Administration program, load the following URL in your browser:

```
http://server_name/SnaAdmin/
```

Replace `server_name` with the TCP/IP host name of the CS/AIX server.

The program displays a logon panel where you enter the AIX user ID and password that you use to log on to the AIX system when performing other CS/AIX administration functions.

Once you have logged on, the program displays a panel similar to the Motif administration program. Figure 120 shows the main window from the client's browser through the Web Administration program.



Location: http://rs600030.itso.ral.ibm.com/SnaAdmin/

Connectivity 4/21/00 11:52 AM

rs600030	Active
TRSAP0	Active
TRL0	Active
LUHK002	Inactive
LUHK003	Inactive
LUHK004	Inactive
LUHK005	Inactive
LUHK006	Inactive
LUHK007	Inactive
LUHK008	Inactive
LUHK009	Inactive
LUHK010	Inactive
LUHK011	Inactive

Move the mouse pointer over something to find out more about it

Figure 120. Web Administration main window

You can also use the Web Administration program to manage the CS/AIX system while it is active. The administration program enables you to make and apply changes to the configuration while CS/AIX is active. You can add, modify, and remove resources (in most cases, even when the node and its resources are active), and use the modified configuration immediately for continued operation.

The Web Administration program enables you to set up all required parameters for standard CS/AIX configurations. For advanced parameters, the program supplies default values. You need to supply only the essential configuration information, which enables you to set up SNA communications quickly and easily.

Note that the other CS/AIX administration tools (command-line configuration and NOF application programs) provide access to a wider range of configuration parameters and options than those shown in the Web Administration program. In most cases, however, you can perform all needed configuration from this program because it exposes the key fields needed to configure and hides the fields that most users should not need to modify.

The default values supplied by the Web Administration program may differ from those supplied by command-line configuration because the Web program can choose values based on the context of the configuration task being performed. Similarly, the default values supplied by the Web Administration program may differ from those supplied by the Motif administration program because the Motif program can choose values based on other choices you have already made *in the same dialog*.

10.2 Web Administration program implementation

In this section, we discuss configuring the Web Administration program (Web Admin) connection to the Web server, and Web Administration program usage.

The Web admin component of CS/AIX is contained in the sna.wa fileset on the product distribution media. It can be installed when CS/AIX is installed, or at a later time.

10.2.1 Supported Web servers

The following Web servers are supported by CS/AIX Web Administration.

- IBM HTTP Server V1.3.6 for AIX (with WebSphere Application Server 2.03)
- Apache Server (with Jserv support)

- Netscape Enterprise Server V3.01 and V3.51 for AIX (V3.51 is recommended)
- Lotus Domino Go Server

10.2.2 Configuring a Web server for Web Administration

If one of the following Web servers is installed on the AIX system before the Web admin program is installed, the required links between the Web server and the CS/AIX Web admin program will be created during installation.

- IBM HTTP Server
- Netscape Enterprise Server
- Lotus Domino Go Server

If you install one of the listed Web servers after installing the Web admin program, you need to set up links between Web admin directories and the Web server's directories so that the Web server can find the required files. Use the following command to create these links.

```
/usr/bin/snawebconfig
```

To undo Web admin changes to all your Web servers, run the command:

```
/usr/bin/snawebunconfig
```

If you are using the Web Administration program with a Web server that is not automatically configured by the `/usr/bin/snawebconfig` command, you need to set up links between CS/AIX directories and the Web server's directories so that the Web server can find the required files. Use the `ln` command to create these links.

1. The Web server's *servlets* directory must be linked to /usr/lib/sna/WebAdmin/Server.
2. The subdirectory SnaAdmin in the Web server's *public HTML* directory must be linked to /usr/lib/sna/WebAdmin/Client.

10.2.3 Invoking the Web Administration program

Before starting the Web Administration program, ensure the following:

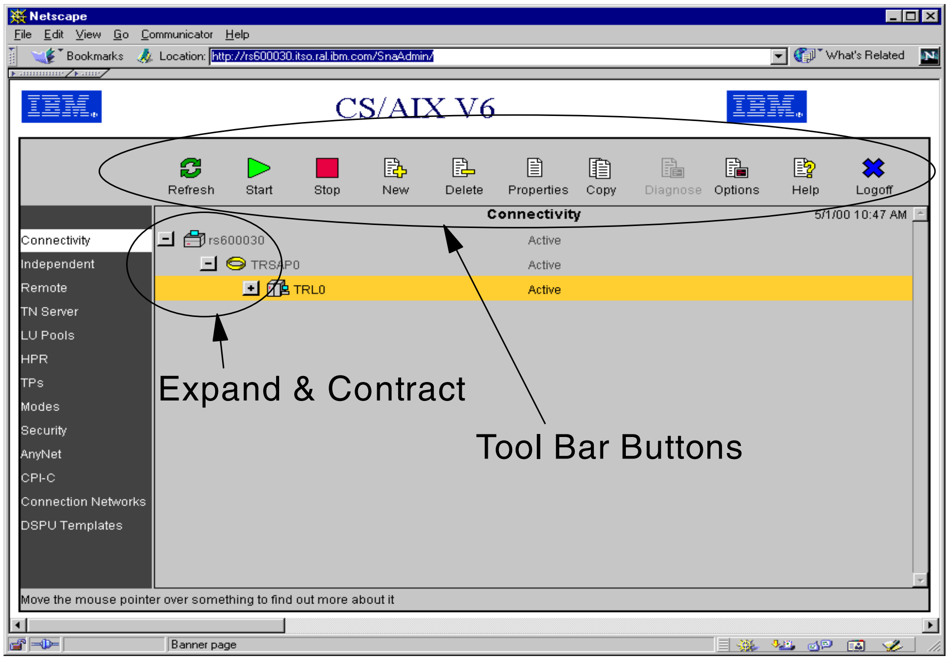
- The CS/AIX software is enabled.
- The Web server software is running on the CS/AIX server.

To use the Web Administration program, load the following URL in your browser:

```
http://server_name/SnaAdmin/
```

Replace `server_name` with the TCP/IP host name of the CS/AIX server.

The Web Administration logon procedure is displayed. After successful logon, the Web Administration main window is displayed. See Figure 121.



rs600030 Active
TRSAP0 Active
TRL0 Active

Move the mouse pointer over something to find out more about it

Figure 121. Web Administration buttons

10.2.4 Using the Web Administration program

As shown in Figure 121, there are several buttons in Web Administration program used for managing resources of CS/AIX. In this section, we cover the tools and the action they perform.

When the main window first appears, the display is contracted so that the node's connectivity resources are not shown.

You can click the **Expand** button ⊞ next to the node to show its connectivity resources.

You can click the **Contract** button ⊟ to hide them.

For each item listed, resources that belong to that item are nested within the information for that item. For example, link stations are grouped under the port to which they belong.

10.2.4.1 Resource windows

The left side toolbar in the main window allows you to access different CS/AIX resources: connectivity, independent LUs, TPs, security resources, and so on. Click an entry in the toolbar to view and manage each type of resource.

You can expand and contract the display in each window in the same way as for the connectivity resources.

10.2.4.2 Tool bar buttons

Tool bar buttons at the top of the Web Administration program window make it easy to perform common functions.

All buttons appear in the tool bars of each resource window. If a button’s operation is not valid for the currently selected item (or an operation requires an item to be selected, but none is), the button is displayed in gray, and the function cannot be selected (the button cannot be pressed).

The following buttons can appear on resource windows:

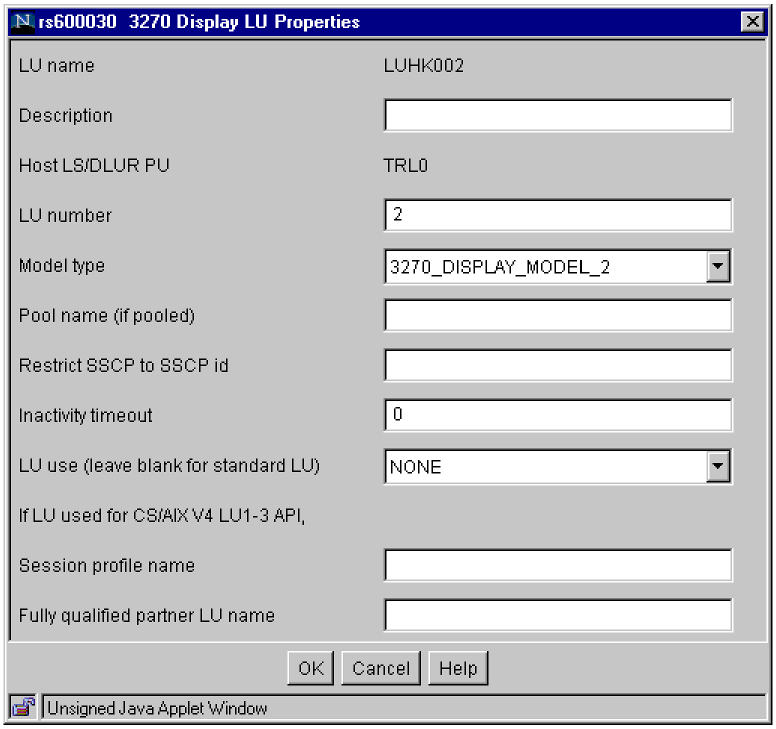
Table 1. Tool bar buttons

Button	Description
🔄	Click the **Refresh** button to update the Web Administration program’s display to match the latest information available in the configuration file. You can also set the program to refresh the information automatically at intervals, using the **Options** button. In addition to setting a refresh timer, you can also set whether Web Administration refreshes automatically, never, or prompts you whenever you change resource windows or issue a potentially configuration-modifying verb.
▶	Click the **Start** button to start the selected item.
🟥	Click the **Stop** button to stop the selected item.
📄➕	Click the **New** button to add a new resource item.
📄➖	Click the **Delete** button to delete the selected item.

Button	Description
📄	Click the **Properties** button to view or modify the selected item’s configuration.
📋	Click the **Copy** button to copy the selected item’s configuration. Pressing this button opens a dialog whose fields duplicate the configuration of the selected item. Complete the dialog’s fields (filling in the new item’s name) to add the new item.
📄	Click the **Diagnose** button to control diagnostics for the node.
📄	Click the **Options** button to set up options that determine how the Web Administration program operates. For example, you can set it up to refresh the display at intervals so that it matches the latest available information in the configuration file, and specify the time interval between refreshes; or you can set it up so that it only refreshes when you explicitly request this by clicking on the **Refresh** button.
❓	Click the **Help** button to display help information on the current resource window.
✖	Click the **Logoff** button to disconnect the program from the CS/AIX server. This allows you to leave the program running but not displaying details of the configuration. The program also disconnects from the server when you close your browser, or when you browse to a new Web page that is not part of the Web Administration program.

10.2.4.3 Resource dialog

When you add a new item or modify an existing one, a resource dialog shows default information for the new item, or the current configuration information for an existing resource. A sample dialog for an LU is shown in Figure 122 on page 179.


rs600030 3270 Display LU Properties
OK
Cancel
Help
Unsigned Java Applet Window

LU name	LUHK002
Description	
Host LS/DLUR PU	TRL0
LU number	2
Model type	3270_DISPLAY_MODEL_2
Pool name (if pooled)	
Restrict SSCP to SSCP id	
Inactivity timeout	0
LU use (leave blank for standard LU)	NONE
If LU used for CS/AIX V4 LU1-3 API,	
Session profile name	
Fully qualified partner LU name	

Figure 122. LU resource dialog

Resource dialogs guide you through the configuration process and supply default values whenever possible. If you do not supply a required value, the program presents a message pop-up that indicates the information you need to provide.

Most dialogs provide a Description field; the information you enter there is displayed on the window where the resource is displayed.

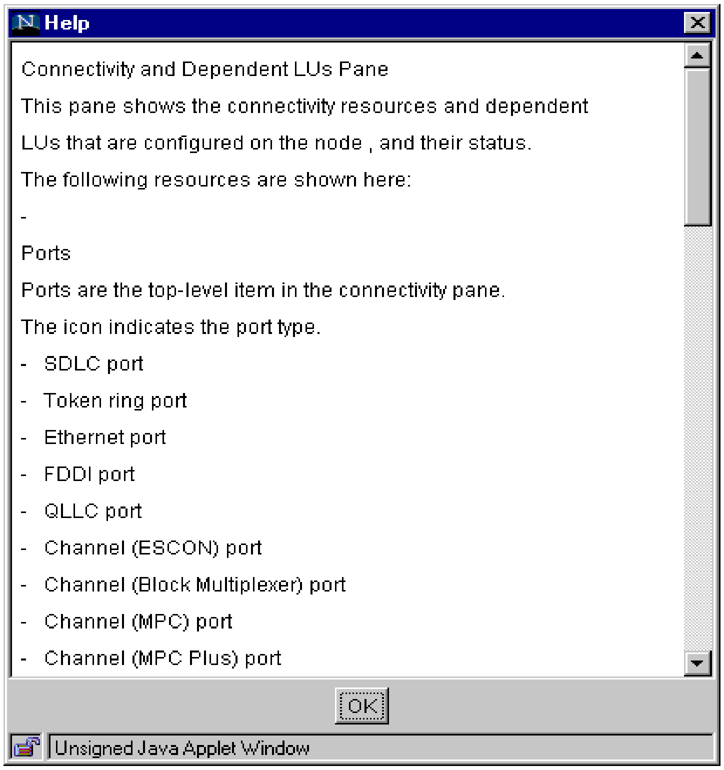
If you are permitted to change the information in a resource dialog (when you are adding a new item or modifying an existing one), the dialog includes OK and Cancel buttons. Click the **OK** button when you are finished, or the **Cancel** button to exit without changing the configuration for the resource.

If you cannot change the information in a resource dialog (for example if the resource's configuration cannot be modified while it is active), the `snaadmin` command issued when you click **OK** will be rejected with an appropriate return code, and an error dialog will be displayed.

For help on the dialog, click the **Help** button.

10.2.4.4 Help windows

The online help for the Web Administration program provides detailed guidance for each configuration window. A typical Help window is shown in Figure 123.



Connectivity and Dependent LUs Pane

This pane shows the connectivity resources and dependent

LUs that are configured on the node , and their status.

The following resources are shown here:

-

Ports

Ports are the top-level item in the connectivity pane.

The icon indicates the port type.

- SDLC port
- Token ring port
- Ethernet port
- FDDI port
- QLLC port
- Channel (ESCON) port
- Channel (Block Multiplexer) port
- Channel (MPC) port
- Channel (MPC Plus) port

Figure 123. Help window

10.3 Scenario

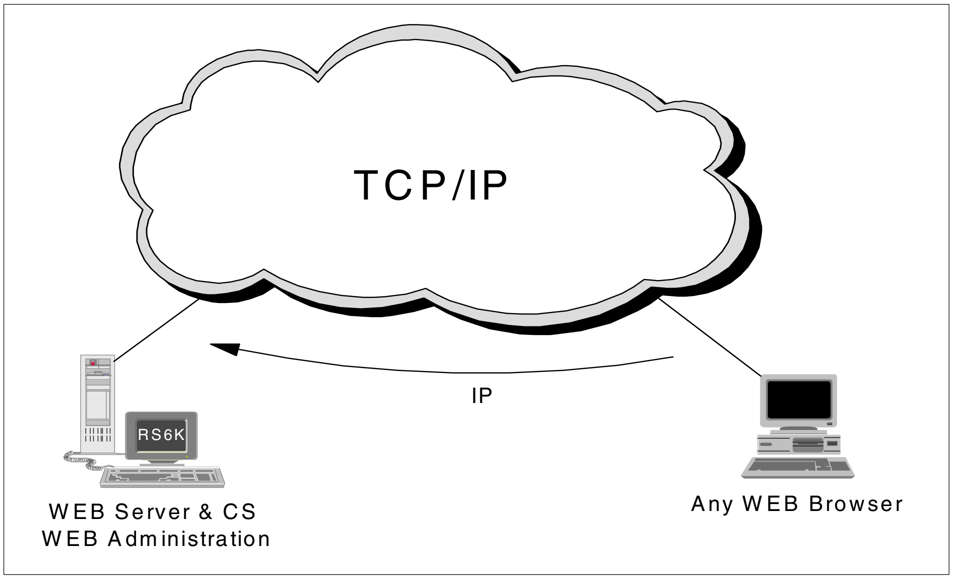
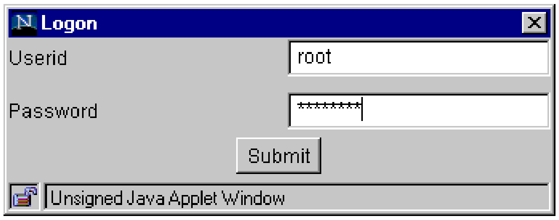


Figure 124. Web Administration scenario

This scenario illustrates the configuration steps of node, port, link station and LUs as a simple example to show how to use the Web Administration program. We will define a token-ring connection to a CS/AIX node.

10.3.1 Node configuration

Enter `http://server_name/SnaAdmin/` in your Web browser to invoke the Web Administration program. The Logon window will appear and prompt you to input your user ID and password as shown in Figure 125.



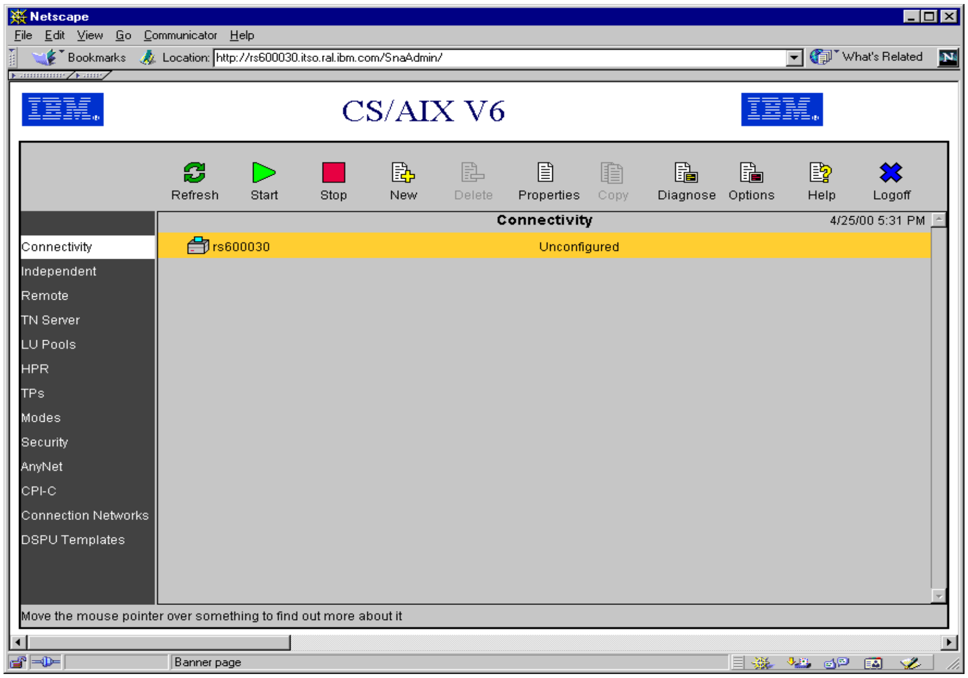
Userid: root

Password: *********

Figure 125. Logon window

The userid/password can be for user root, or a user who belongs to the *system* group.

The Web Administration program initial window is displayed as shown in Figure 126.



Connectivity 4/25/00 5:31 PM

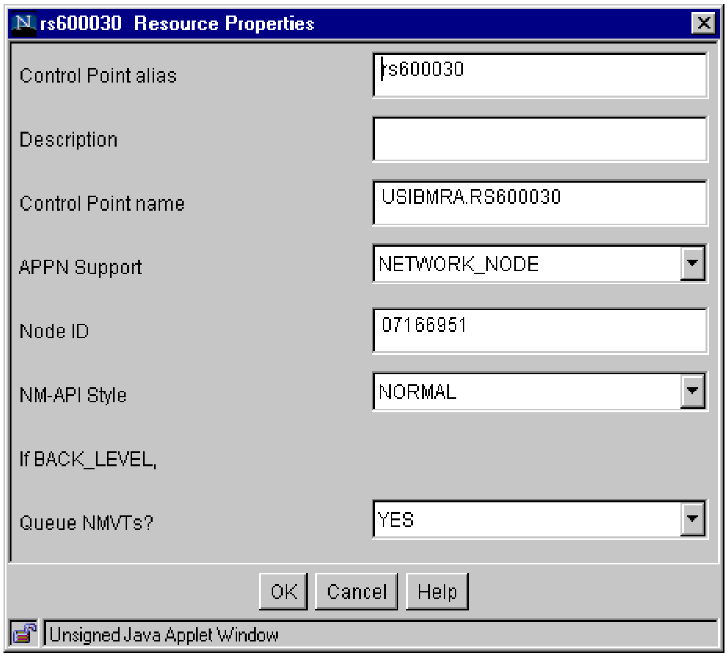
rs600030 Unconfigured

Move the mouse pointer over something to find out more about it

Figure 126. Initial Web Administration window

If no CS/AIX resources are configured, the window shows the node as being Unconfigured.

Double-click the node name (in this example, it is rs600030) or select **Properties** menu in the tool bar to initially configure the node. The rs600030 Resource Properties window will appear as shown in Figure 127.



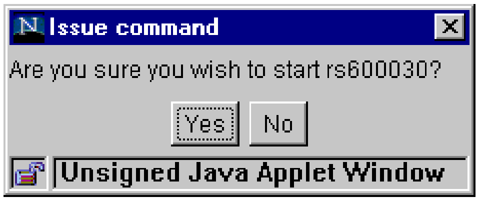
Control Point alias	rs600030
Description	
Control Point name	USIBMRA.RS600030
APPN Support	NETWORK_NODE
Node ID	07166951
NM-API Style	NORMAL
If BACK_LEVEL,	
Queue NMVTs?	YES

Figure 127. Node resource properties

Enter the node configuration values as required. Select **OK**.

The rs600030 node is now defined, but set to Inactive.

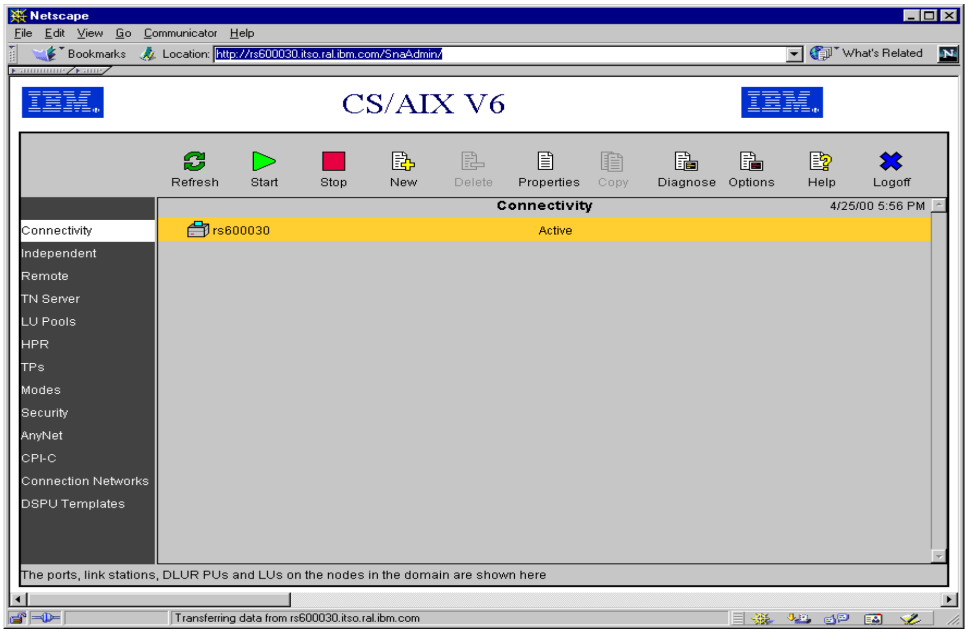
Select the **Start** button in the tool bar.



Are you sure you wish to start rs600030?

Figure 128. Issue command window

The Issue command window as shown in Figure 128 asks you if you are sure you wish to issue the Start command. Select **Yes.** The node rs600030 will be Active as shown in Figure 129.



Connectivity 4/25/00 5:56 PM

rs600030 Active

The ports, link stations, DLUR PUs and LUs on the nodes in the domain are shown here

Transferring data from rs600030.itso.ral.ibm.com

Figure 129. Node configuration

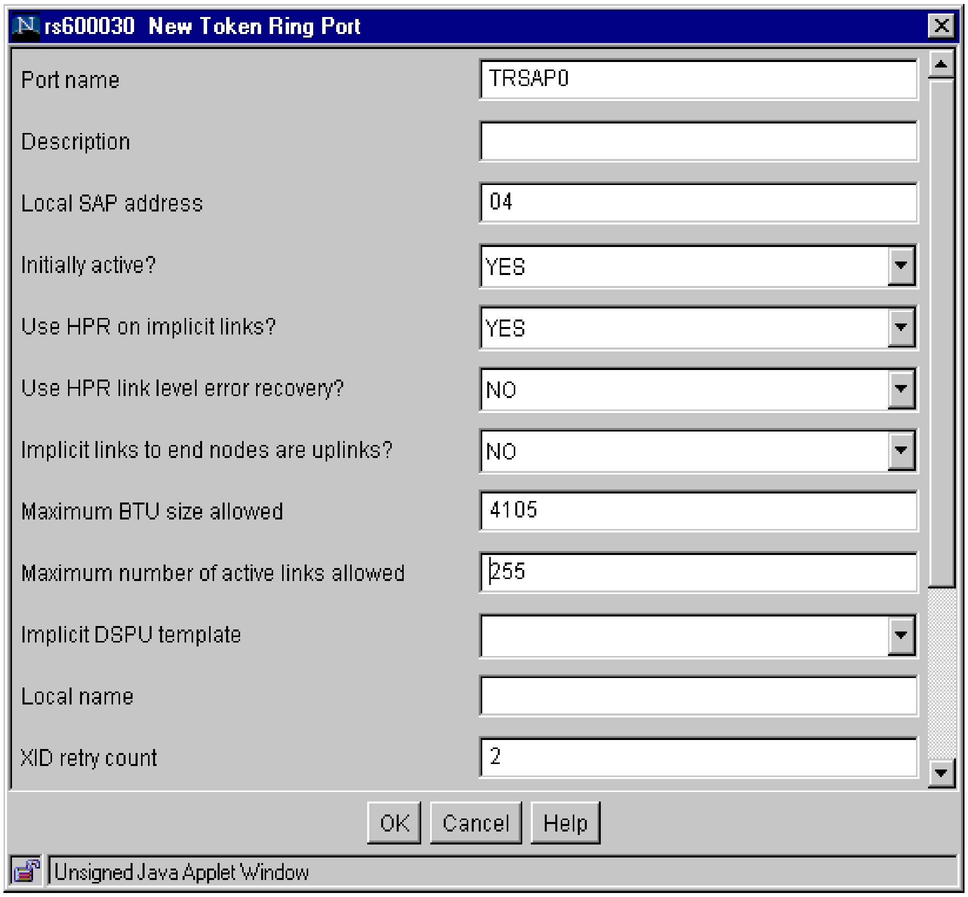
After the node configuration has been completed, you proceed to the next stop: port configuration.

10.3.2 Port configuration

You must first determine which type of port to add to the node just configured. In our example, we will define a token ring port.

Select **New** -> **Port** -> **TR port** in the tool bar.

The rs600030 New Token Ring Port window will be displayed as shown in Figure 130.



rs600030 New Token Ring Port

Port name	TRSAP0
Description	
Local SAP address	04
Initially active?	YES
Use HPR on implicit links?	YES
Use HPR link level error recovery?	NO
Implicit links to end nodes are uplinks?	NO
Maximum BTU size allowed	4105
Maximum number of active links allowed	255
Implicit DSPU template	
Local name	
XID retry count	2

Figure 130. New port configuration

Enter the port definition parameters as required. Note that there is a scroll bar displayed implying that there are additional undisplayed parameters that must be considered for customization. This is similar to the way CS/AIX parameter values are input using SMIT.

Select **OK**.

The node entry now has an expand box next to it. Click the expand box to display the new token-ring port. You may make it active by clicking the port followed by clicking the **Start** button in the tool bar as shown in Figure 131.

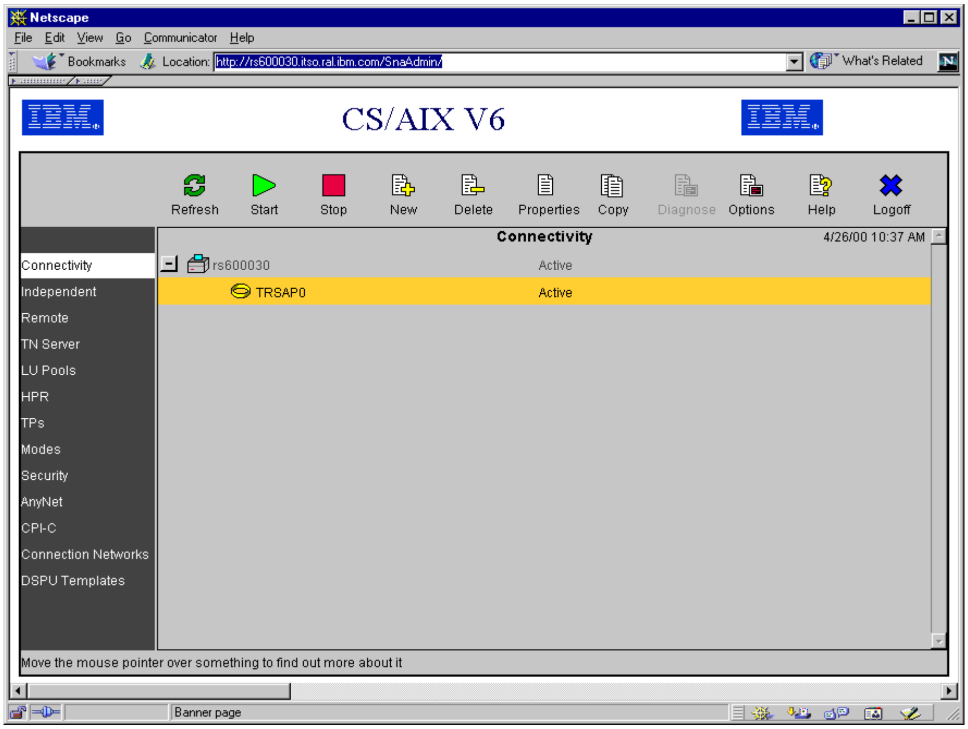


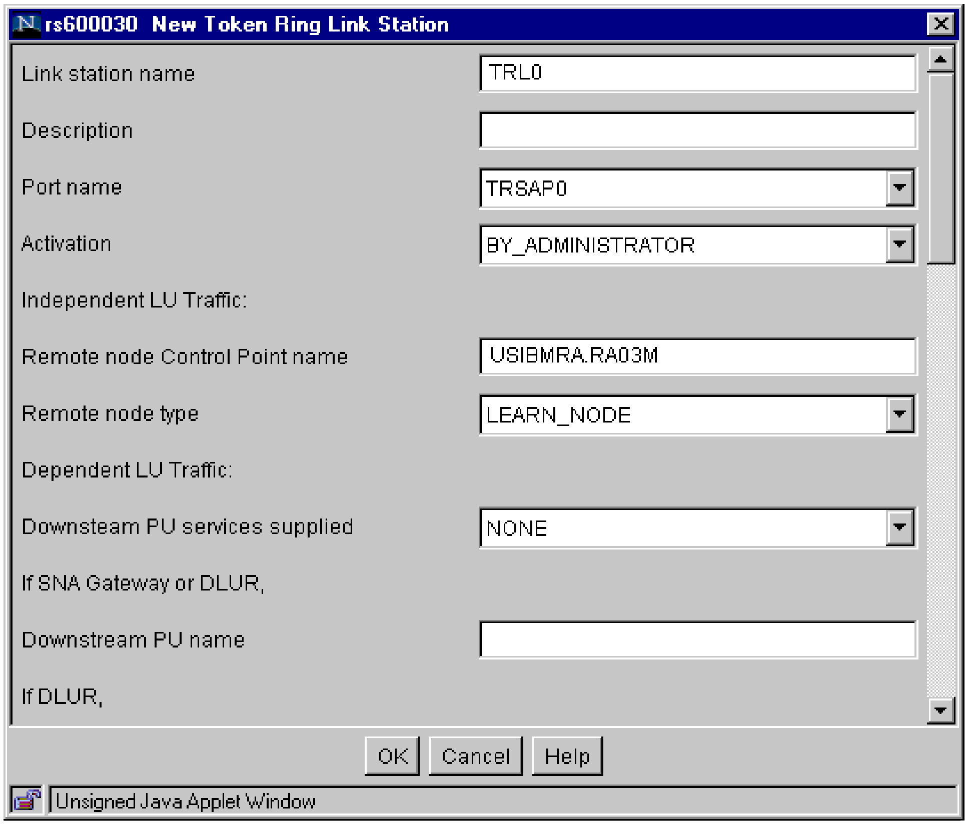
Figure 131. Active port window

10.3.3 Link station configuration

A link station must now be configured on the token-ring port.

Select **New** -> **Link Station** -> **TR Link Station** in the tool bar.

The rs600030 New Token Ring Link Station window will be displayed as shown in Figure 132.


rs600030 New Token Ring Link Station

Link station name	TRL0
Description	
Port name	TRSAP0
Activation	BY_ADMINISTRATOR
Independent LU Traffic:	
Remote node Control Point name	USIBMRA.RA03M
Remote node type	LEARN_NODE
Dependent LU Traffic:	
Downsteam PU services supplied	NONE
If SNA Gateway or DLUR,	
Downstream PU name	
If DLUR,	

OK
Cancel
Help
Unsigned Java Applet Window

Figure 132. New token-ring link station configuration

Enter the appropriate values for your token-ring link station.

You can scroll down to see and enter values for required fields. Then select **OK**.

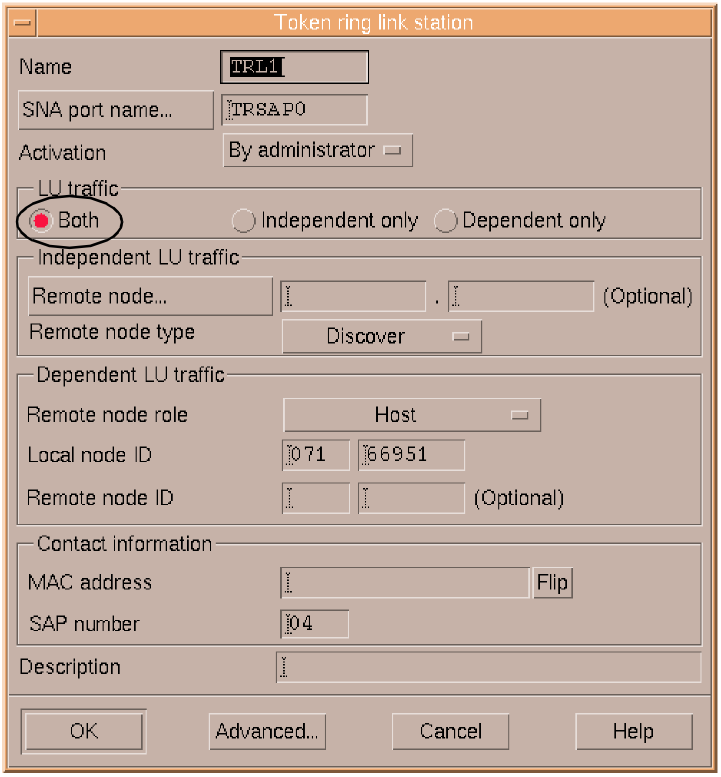
10.3.4 Administration program differences

The addition of a token-ring link station gives us the opportunity to point out a difference in the way the Web Administration program and the Motif administration program work.

A token-ring link station may be configured to support only independent LUs, only dependent LUs, or both.

In configuring a token-ring link station with the Motif administration program, the configuration panel that is displayed depends on which button is selected for LU traffic:

- Both (see Figure 133)
- Independent Only (see Figure 134)
- Dependent Only (see Figure 135)



Token ring link station

Name: TRL1

SNA port name...: TRSAP0

Activation: By administrator

LU traffic: ● Both ○ Independent only ○ Dependent only

Independent LU traffic

Remote node... . (Optional)

Remote node type: Discover

Dependent LU traffic

Remote node role: Host

Local node ID: 071 66951

Remote node ID: (Optional)

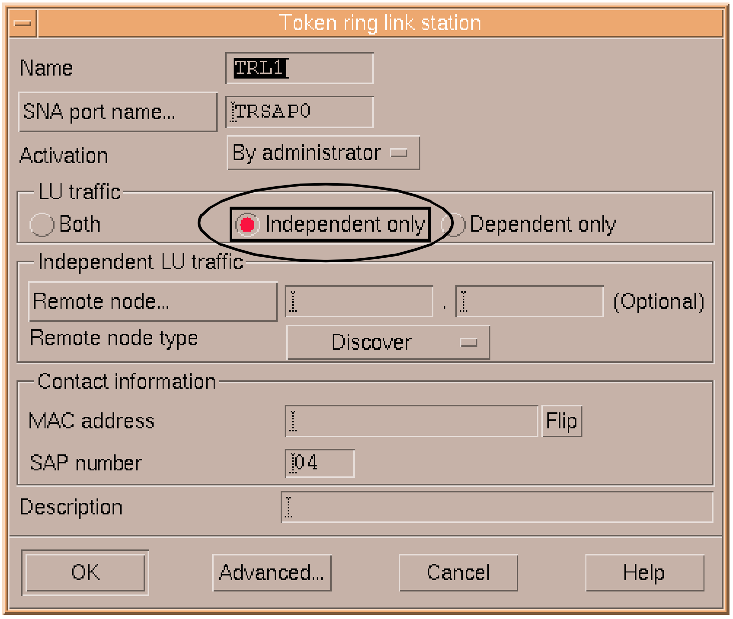
Contact information

MAC address: Flip

SAP number: 04

Description:

Figure 133. Support for both



Token ring link station

Name: TRL1

SNA port name...: TRSAP0

Activation: By administrator

LU traffic

○ Both ● Independent only ○ Dependent only

Independent LU traffic

Remote node... . (Optional)

Remote node type: Discover

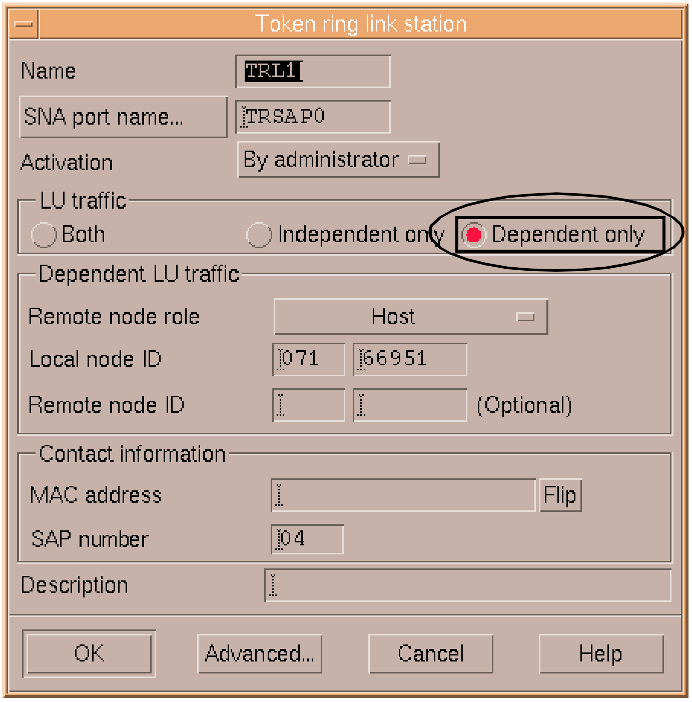
Contact information

MAC address: Flip

SAP number: 04

Description:

Figure 134. Support for independent only



Name: TRL1

SNA port name...: TRSAP0

Activation: By administrator

LU traffic: ○ Both ○ Independent only ● Dependent only

Dependent LU traffic

Remote node role: Host

Local node ID: 071 66951

Remote node ID: (Optional)

Contact information

MAC address:

SAP number: 04

Description:

Figure 135. Support for dependent only

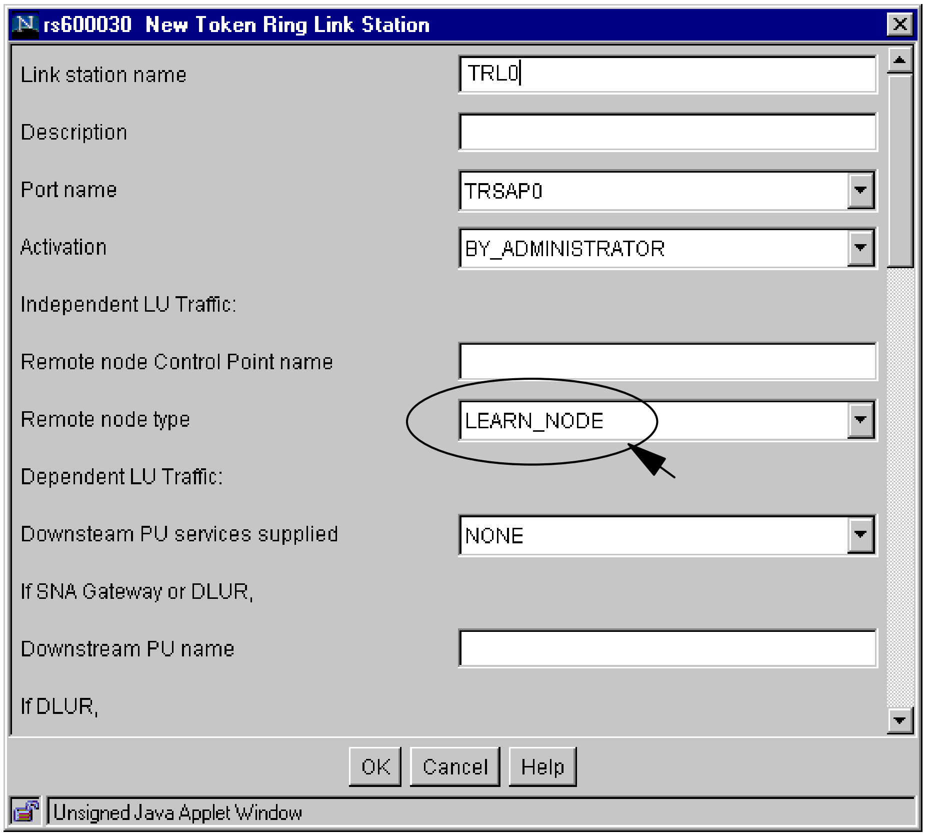
Note that the layout of each of these panels is different and depends on which LU traffic button is selected. This is because the Motif administration program is context-sensitive and can modify the panel being displayed based on selections made on the panel.

The Web Administration program does not dynamically display a different panel based on a selection made on that panel. It displays a fixed list of parameters based on values entered on previous panels.

Therefore, to make a similar selection for LU Traffic of Both, Independent Only or Dependent Only, you must select different values for the parameters displayed in Figure 132 on page 187. An example configuration for each type follows:

- **Both**

  In order to configure a link station as Both (that is, available for both independent LU traffic and dependent LU traffic), the remote node type must be LEARN_NODE as shown in Figure 136.



rs600030 New Token Ring Link Station

Link station name: TRL0

Description:

Port name: TRSAP0

Activation: BY_ADMINISTRATOR

Independent LU Traffic:

Remote node Control Point name:

Remote node type: LEARN_NODE

Dependent LU Traffic:

Downsteam PU services supplied: NONE

If SNA Gateway or DLUR,

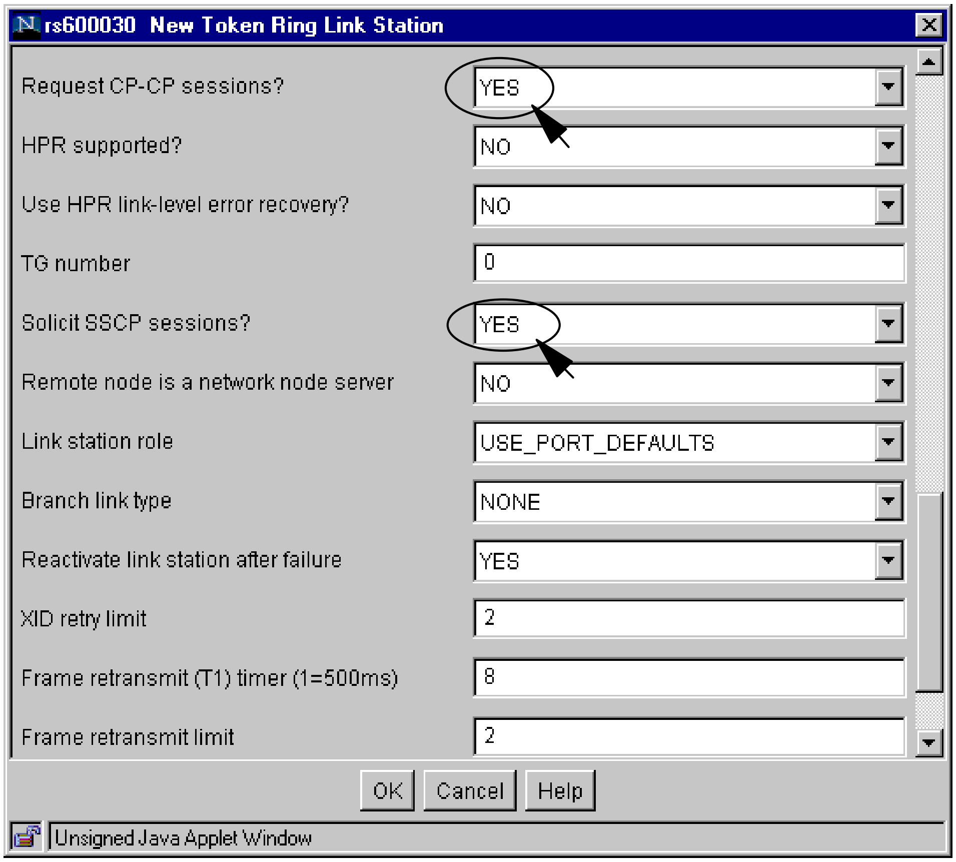
Downstream PU name:

If DLUR,

OK
Cancel
Help
Unsigned Java Applet Window

Figure 136. Remote note type selection for both LU traffic types

In addition, as shown in Figure 137, you must set Request CP-CP sessions and Solicit SSCP sessions to **YES.**



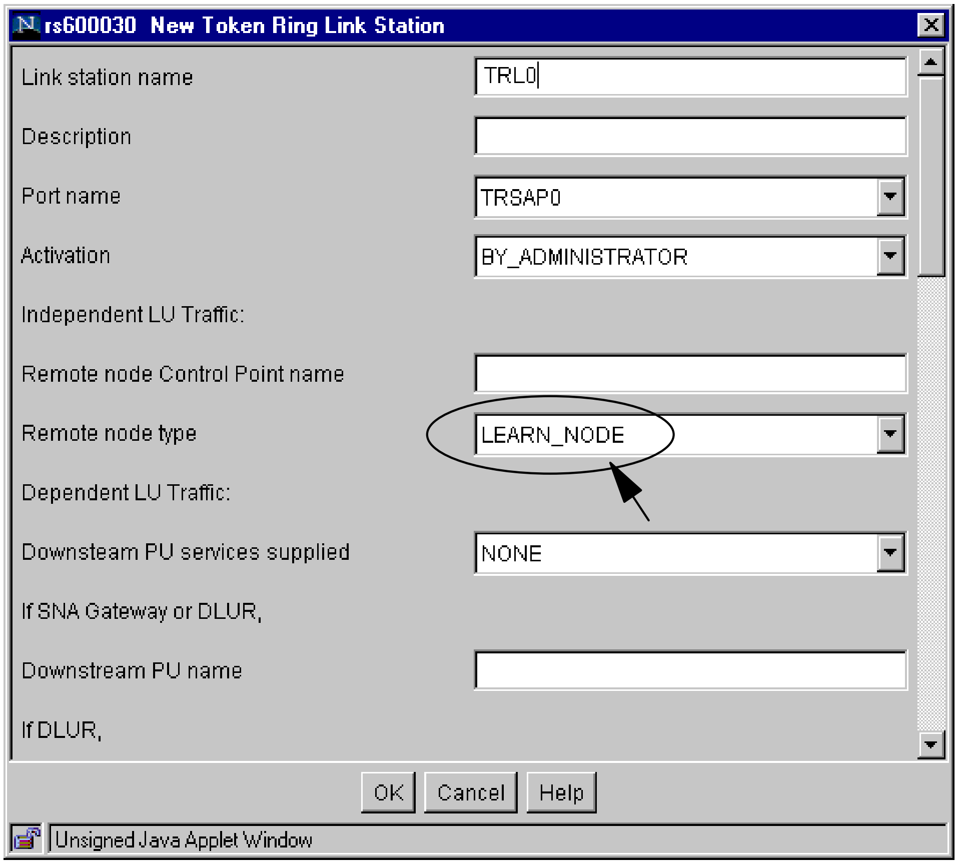
rs600030 New Token Ring Link Station

Request CP-CP sessions?	YES
HPR supported?	NO
Use HPR link-level error recovery?	NO
TG number	0
Solicit SSCP sessions?	YES
Remote node is a network node server	NO
Link station role	USE_PORT_DEFAULTS
Branch link type	NONE
Reactivate link station after failure	YES
XID retry limit	2
Frame retransmit (T1) timer (1=500ms)	8
Frame retransmit limit	2

Figure 137. CP-CP session and SSCP session selection for both LU traffic types

- **Independent Only**

  For independent only LU traffic, the value of the remote node type has to be one of the following: LEARN_NODE, NETWORK_NODE, END_NODE, BACK_LEVEL_LEN_NODE as shown in Figure 138.


rs600030 New Token Ring Link Station

Link station name TRL0

Description

Port name TRSAP0

Activation BY_ADMINISTRATOR

Independent LU Traffic:

Remote node Control Point name

Remote node type LEARN_NODE

Dependent LU Traffic:

Downsteam PU services supplied NONE

If SNA Gateway or DLUR,

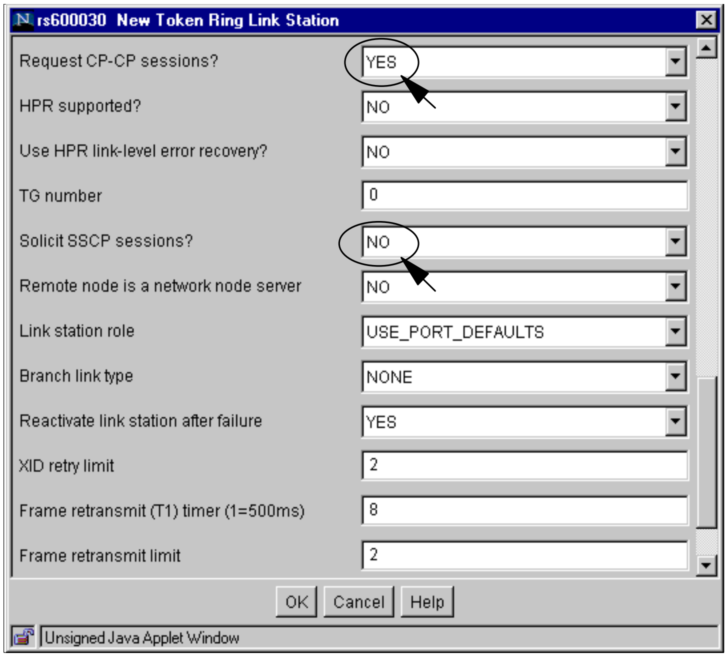
Downstream PU name

If DLUR,

OK
Cancel
Help
Unsigned Java Applet Window

Figure 138. Remote note type selection for independent only LU traffic

In addition, **YES** is required for Request CP-CP sessions, and **NO** for Solicit SSCP sessions as shown in Figure 139.

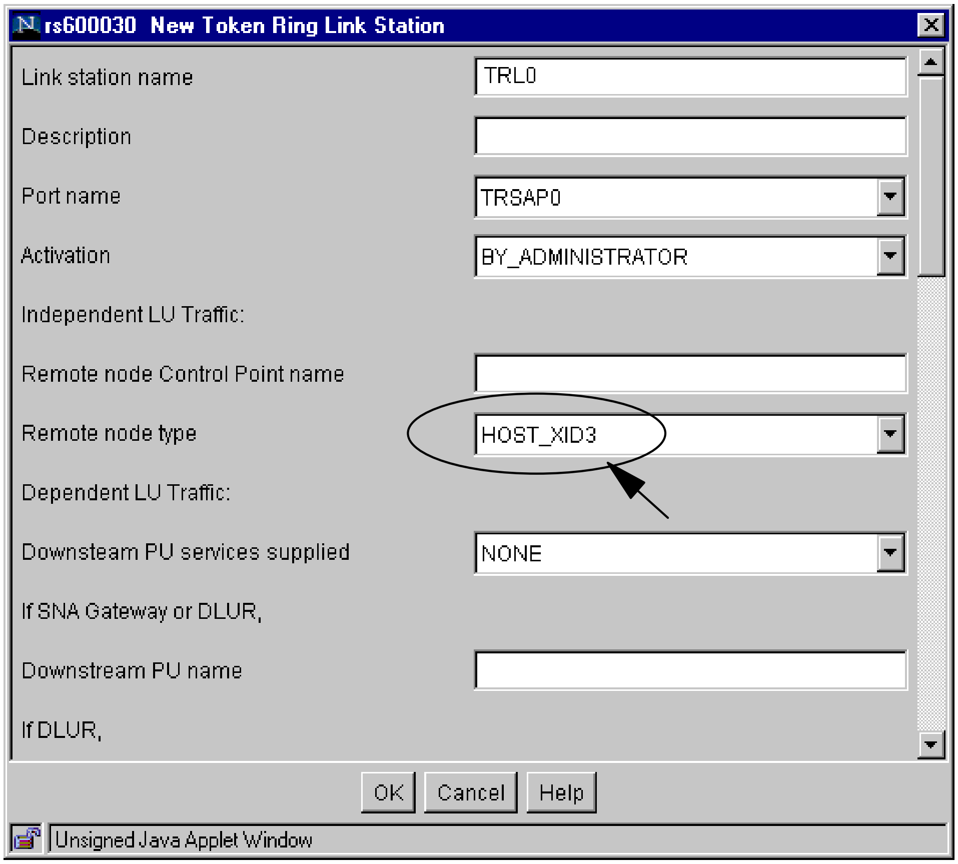

rs600030 New Token Ring Link Station
OK
Cancel
Help
Unsigned Java Applet Window

Request CP-CP sessions?	YES
HPR supported?	NO
Use HPR link-level error recovery?	NO
TG number	0
Solicit SSCP sessions?	NO
Remote node is a network node server	NO
Link station role	USE_PORT_DEFAULTS
Branch link type	NONE
Reactivate link station after failure	YES
XID retry limit	2
Frame retransmit (T1) timer (1=500ms)	8
Frame retransmit limit	2

Figure 139. CP-CP session and SSCP session selection for Independent only LU traffic

- **Dependent Only**

  For dependent only LU traffic, the value of the remote node type is selected one of the following: HOST_XID3, HOST_XID0, DSPU_XID, DSPU_NOXID as shown in Figure 140.

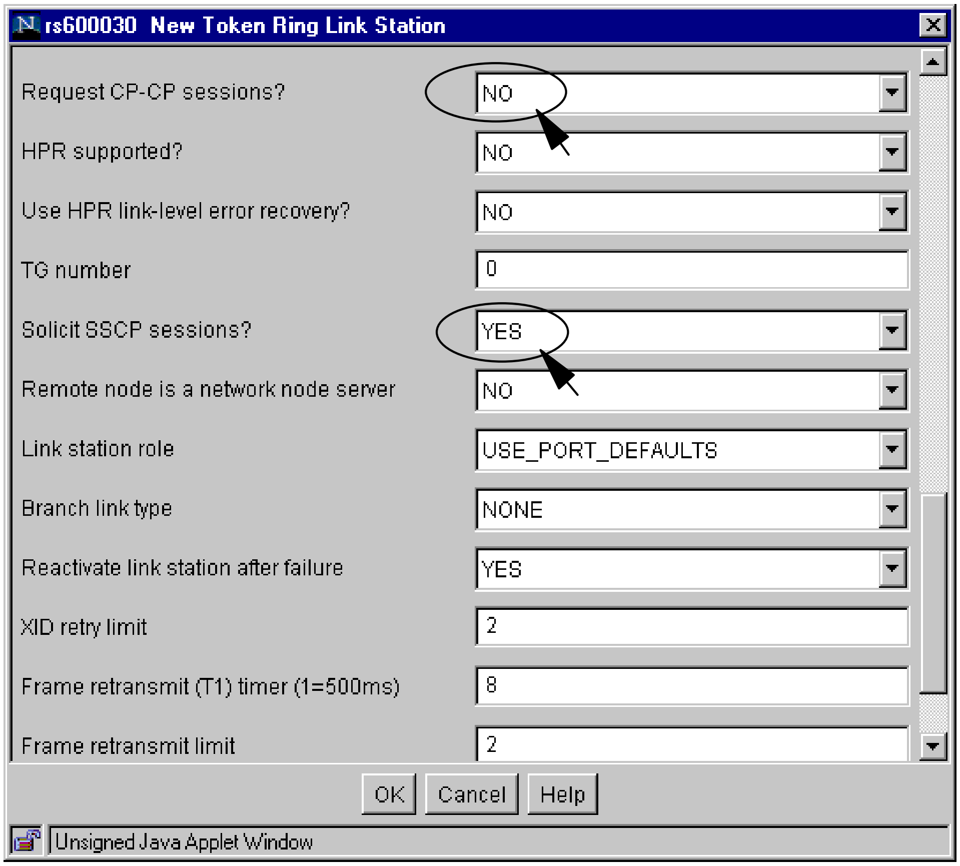


rs600030 New Token Ring Link Station

Link station name	TRL0
Description	
Port name	TRSAP0
Activation	BY_ADMINISTRATOR
Independent LU Traffic:	
Remote node Control Point name	
Remote node type	HOST_XID3
Dependent LU Traffic:	
Downsteam PU services supplied	NONE
If SNA Gateway or DLUR,	
Downstream PU name	
If DLUR,	

Figure 140. Remote note type selection for dependent only LU traffic

Then select **NO** for Request CP-CP sessions, and **YES** for Solicit SSCP sessions as shown in Figure 141.



rs600030 New Token Ring Link Station

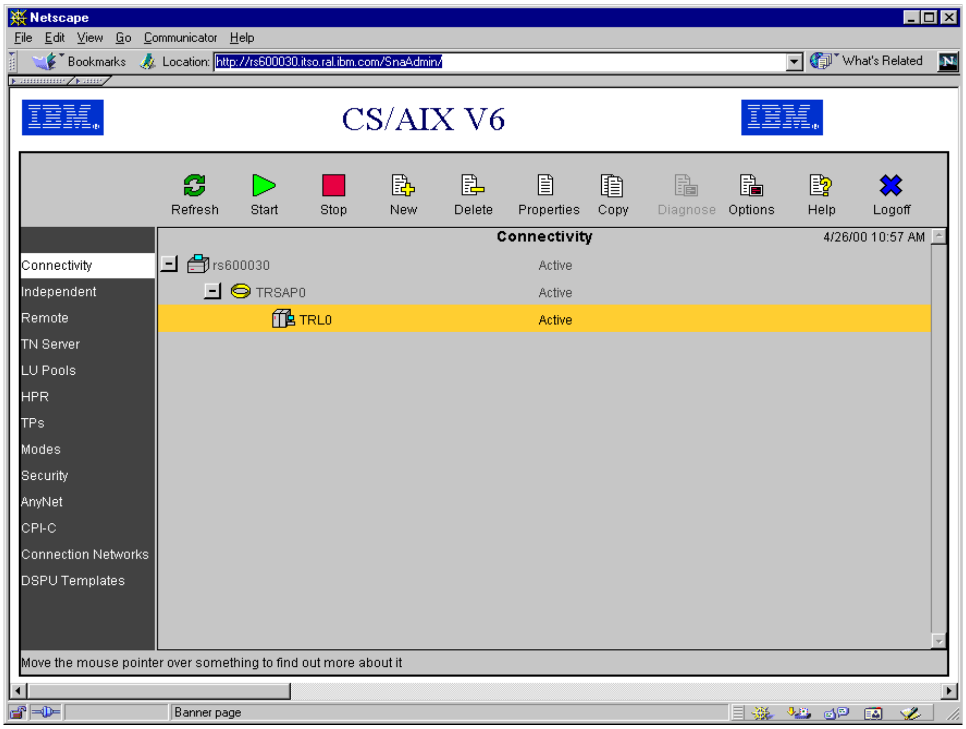
Request CP-CP sessions?	NO
HPR supported?	NO
Use HPR link-level error recovery?	NO
TG number	0
Solicit SSCP sessions?	YES
Remote node is a network node server	NO
Link station role	USE_PORT_DEFAULTS
Branch link type	NONE
Reactivate link station after failure	YES
XID retry limit	2
Frame retransmit (T1) timer (1=500ms)	8
Frame retransmit limit	2

Figure 141. CP-CP session and SSCP session selection for dependent only LU traffic

The result from configuring the link station can be confirmed through the Motif administration program after all of the above parameters are saved.

After you have completed your parameter definitions for the token-ring link station, select **OK**.

The main CS/AIX window shows the link station added below the port configured in the previous section. The link station will be active if you select it and click the **Start** button in the tool bar as shown in Figure 142.



Connectivity 4/26/00 10:57 AM

```
rs600030        Active
  TRSAP0        Active
    TRL0        Active
```

Move the mouse pointer over something to find out more about it

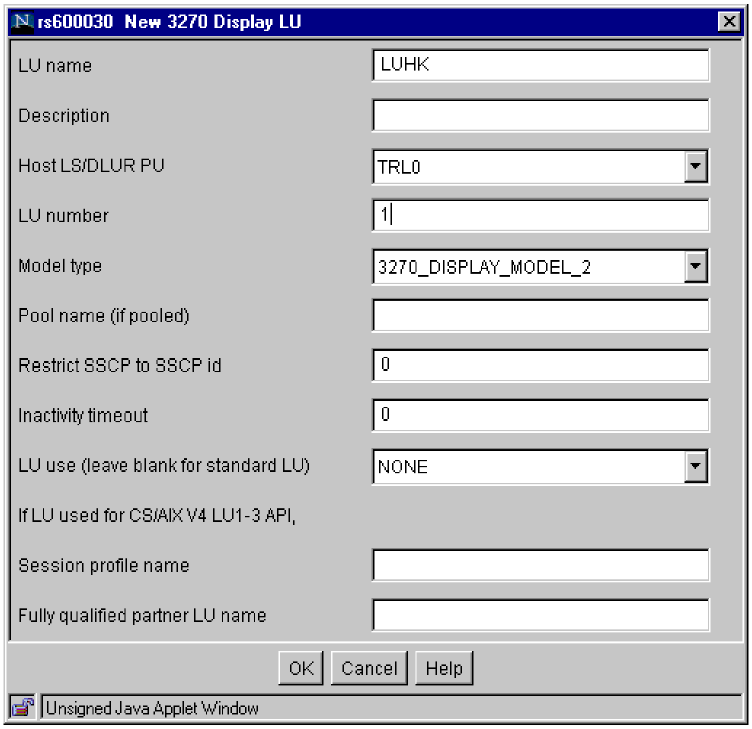
Figure 142. Active link station window

10.3.5 LUs configuration

Depending on your configuration requirements, you may now add LUs to the link station you just configured. In this section, we will add new a 3270 Display LU.

Select **New** -> **LU** -> **3270 Display LU** in the tool bar.

The rs600030 New 3270 Display LU window is displayed as shown in Figure 143.


rs600030 New 3270 Display LU

LU name	LUHK
Description	
Host LS/DLUR PU	TRL0
LU number	1
Model type	3270_DISPLAY_MODEL_2
Pool name (if pooled)	
Restrict SSCP to SSCP id	0
Inactivity timeout	0
LU use (leave blank for standard LU)	NONE
If LU used for CS/AIX V4 LU1-3 API,	
Session profile name	
Fully qualified partner LU name	

Figure 143. New LU configuration

Enter values as required for LUs desired.

Select **OK**.

Chapter 11. CS/AIX licensing

Communications Server for AIX, Version 6 monitors access to users and partner nodes. CS/AIX licensing is based on the number of active concurrent users and links to partner nodes. Current and peak usage is recorded to help determine whether your usage is within the limits permitted by your license.

This chapter covers the CS/AIX licensing and monitoring facilities.

11.1 Overview

IBM Communications Server for AIX, Version 6 includes many functions and features to meet the varying networking connectivity requirements for a broad set of implementation scenarios. In many cases, however, customers may choose to implement only a subset of these features and functions to meet the demands of their networking and connectivity environment. To support this potentially large difference in the level of CS/AIX function that may be required and used in different situations, it is appropriate to apply different licensing requirements based on the level of CS/AIX functions and features that are actually configured and used.

Therefore, CS/AIX license management involves two type of licenses:

- A server license is required for each machine or SP node on which CS/AIX is installed.
- One or more user licenses are required in conjunction with each server license.

Determining the number of server and user licenses required when ordering CS/AIX is covered in the following sections.

CS/AIX does not perform *user license checking*, just *user usage monitoring*. In other words, CS/AIX will not fail to start a session/link/etc; it just keeps track of how many sessions/links/etc have been used.

11.2 Server license

A CS/AIX server license is required for each machine or SP (Scalable-Parallel) node on which any CS/AIX components are installed. For multiprocessor hardware, where a single CS/AIX image is installed and AIX spreads the CS/AIX load across multiple processors, only one CS/AIX server license is required.

CS/AIX uses nodelock licenses to enable or disable the product. Purchase of CS/AIX includes a permanent nodelock license, which is installed automatically into the system's nodelock license file during product installation. The server license is a nodelocked *iforls* key.

Only one CS/AIX server license is required for a machine or SP node regardless of the various functions or features being provided and the number of user licenses that may be required.

11.3 User license

For the purpose of determining CS/AIX user license requirements, a *user* is normally defined as a person. A user license is required for every concurrent user that accesses and uses CS/AIX, either directly or indirectly. In addition, a user license is required for each active link station (may be to a host, adjacent APPN or LEN node, downstream DLUR or SNA gateway client).

Simply stated, a user license is required for each person who is using support provided by CS/AIX, even if they interact with some other intermediate product or application, which in turn uses CS/AIX to access a host. You should obtain user licenses for the maximum number of users who are to be supported concurrently.

The following are considered users:

- Telnet sessions connecting to the TN3270 server component of CS/AIX (for example, PCOMM or HOD TN3270 client sessions), whether or not they use SSL encryption or client/server authentication.
- Telnet sessions connecting to the TN Redirector component of CS/AIX (for example, redirected PCOMM TN3270 or TN5250 client sessions), whether or not they use SSL encryption or client/server authentication.
- APPC and CPI-C applications
- Active SNA LU-LU sessions (LU types 1, 2, or 3 and LU6.2 sessions, excluding those used to control the network) and applications written to the LUA interface.
- Active link stations (link to a host, adjacent APPN or LEN node, downstream DLUR or SNA gateway client).

Following are some sample scenarios that may be used as guidance when calculating the number of user licenses required for a CS/AIX installation.

11.3.1 TN3270 server scenario

A CS/AIX user license is required for each concurrent Telnet user supported, regardless of the number of Telnet emulation sessions they may use or whether SSL is used. You should license the maximum number of TN3270 users who will be logged on.

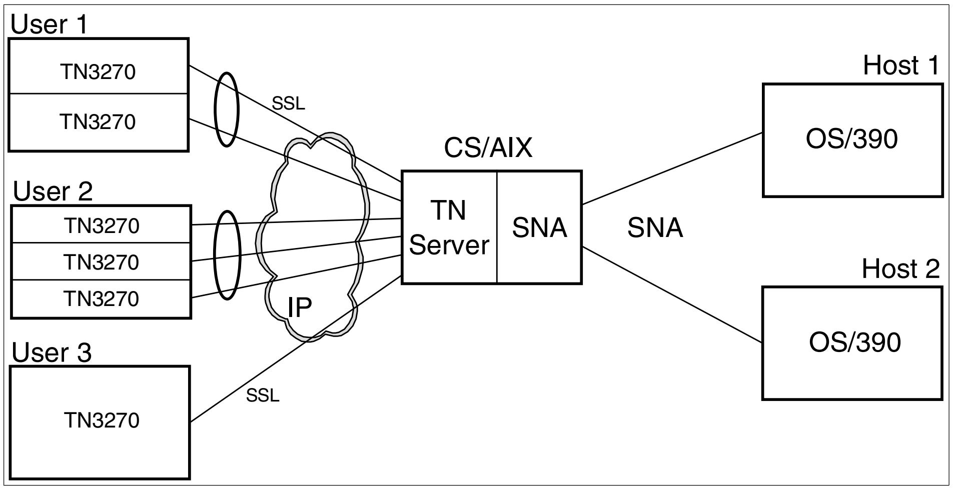


Figure 144. TN server user licenses

The network diagram in Figure 144 shows a sample CS/AIX TN server configuration requiring five user licenses.

CS/AIX cannot tell the difference between multiple TN clients from a single user and multiple TN clients from multiple users going through a proxy or other type of gateway. It is up to the CS/AIX administrator to manage the number of user licenses required. CS/AIX will report the number of TN clients, not the number of users. In the example shown in Figure 144, User 1 has two active TN client sessions with the CS/AIX TN server but requires only a single user license. Likewise, User 2 has three TN client sessions but requires only one user license. And of course, User 3 requires one user license.

Assuming Host 1 and 2 are attached to the CS/AIX system by different links, one user license is required for the link to Host 1, and one user license is required for the link to Host 2.

You should have sufficient user licenses to match the peak number of TN3270 users, in addition to the link stations.

11.3.2 Telnet Redirector scenario

A CS/AIX user license is required for each concurrent redirected Telnet user supported, regardless of the number of Telnet emulation sessions they may use or whether SSL is used.

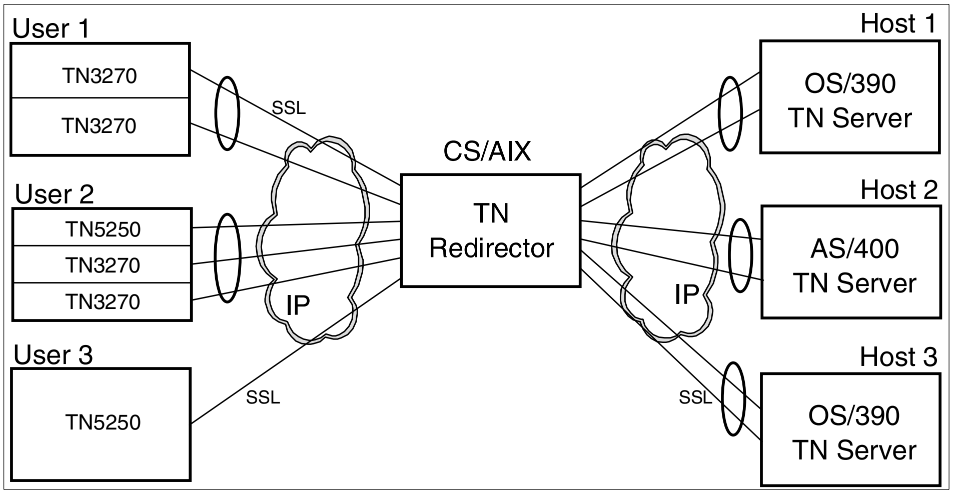


Figure 145. TN Redirector user licenses

The network diagram in Figure 145 shows a sample CS/AIX TN Redirector configuration requiring three user licenses.

As explained in the previous example, CS/AIX cannot tell the difference between multiple TN clients from a single user and multiple TN clients from multiple users going through a proxy or other type of gateway. The CS/AIX administrator must determine that Users 1, 2 and 3 each require a separate user license even though they may be running multiple TN client sessions to the CS/AIX TN Redirector.

Since the TN users and TN hosts connect via TCP/IP, they do not have an associated link station, so no additional licenses are required for link stations.

You should have sufficient user licenses to match the peak number of TN Redirector users.

11.3.3 APPC/CPI-C scenario

Many APPC and CPI-C applications support concurrent users connected to various hosts. A user license is required for each concurrent connected user of each APPC or CPI-C application that uses CS/AIX support. This is required even though the user may be an indirect user and not directly connected to or aware of their use of CS/AIX.

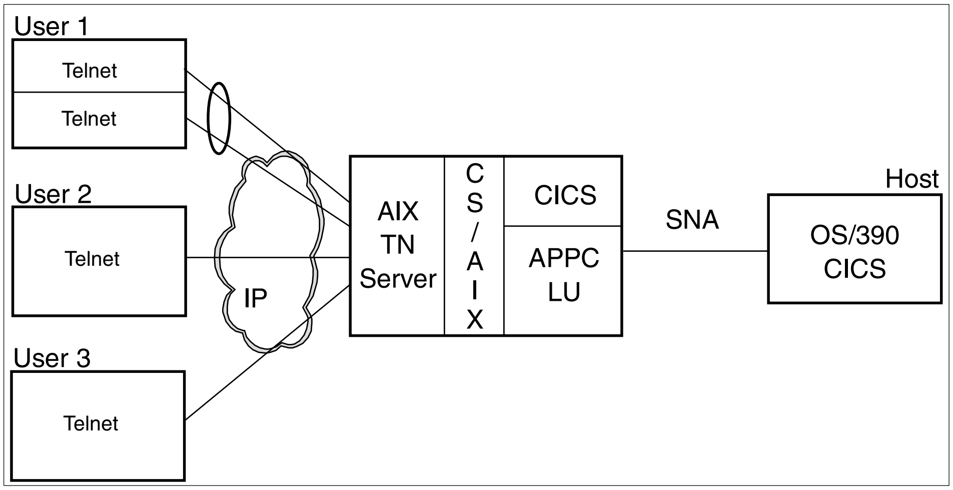


Figure 146. APPC/CPI-C user licenses

In Figure 146, CICS running on the AIX system uses APPC to communicate with CICS running on the host system. Users Telnet into the AIX Telnet server and then log on to the AIX CICS application from the AIX command line.

Each concurrent user requires a separate user license even though the user is not “visible” to CS/AIX. CS/AIX monitors the number of APPC and CPI-C conversations started. In this example, a separate user license is required for Users 1, 2 and 3.

In addition, a user license is required for the link to the OS/390 host.

In summary, this scenario requires four user licenses.

11.3.4 SNA gateway scenario

Each traditional LU1, LU2, LU3 or LUA application requires a user license for each concurrently logged-on user. IBM Personal Communications 3270 emulation is an example of this kind of application. As mentioned in previous scenarios, a user license is required for each user, regardless of the number of emulation sessions they may use.

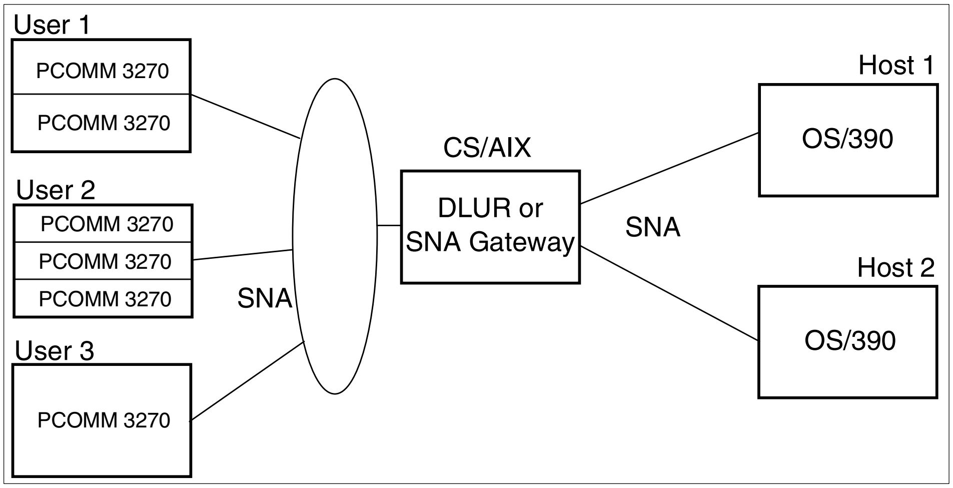


Figure 147. 3270 emulation user licenses

In Figure 147, if the CS/AIX system is adjacent to the host system, an SNA gateway may be used to connect downstream 3270 emulator sessions with host applications. If the CS/AIX system is not adjacent to the host system, then APPN and DLUR are required to complete the connections. Users initiate PCOMM 3270 emulation sessions with the DLUR or SNA Gateway function in CS/AIX. DLUR or SNA Gateway then completes the session to the host.

User 1 has two PCOMM emulator session active to CS/AIX but requires one user license. Similarly, User 2 has three PCOMM 3270 emulator sessions active but requires only one user license. User 3 also requires one user license.

Again, assuming that Host 1 and Host 2 are attached to the CS/AIX system via different links, two user licenses are required for the two data links.

Therefore, this scenario requires five user licenses.

11.3.5 Local dependent LU scenario

Each dependent LU local to the CS/AIX system requires a user license for each concurrently logged-on user. The AIX 3270 Host Connection Program (HCON) is an example of this kind of application. HCON supports SNA 3270 emulation for AIX users. A user license is required for each HCON user.

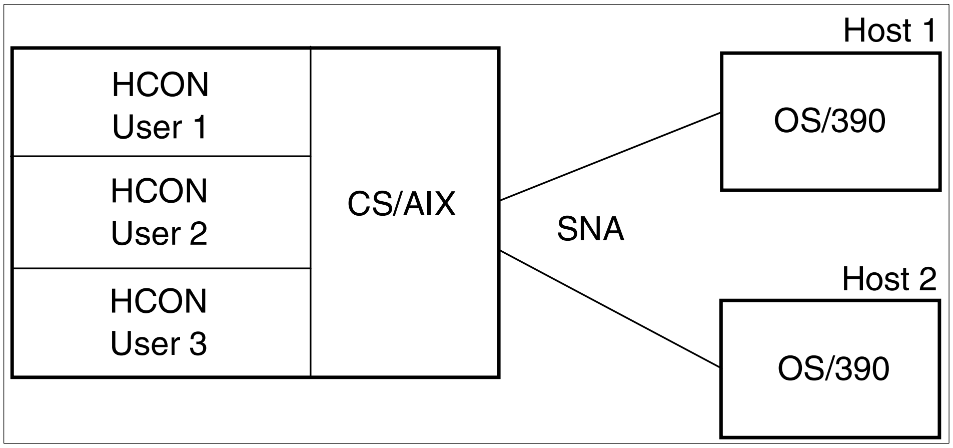


Figure 148. Local LU user licenses

In Figure 148, if the CS/AIX system is adjacent to the host system, CS/AIX may be used to connect local HCON 3270 emulator sessions with host applications. If the CS/AIX system is not adjacent to the host system, then APPN and DLUR are required to complete the connections.

Each HCON user requires a user license.

Again, assuming that Host 1 and Host 2 are attached to the CS/AIX system via different links, two user licenses are required for the two data links.

Therefore, this scenario requires five user licenses.

Note: HCON has been withdrawn from marketing and is used here only to illustrate the local dependent LU scenario for AIX licensing.

11.4 Monitoring usage of CS/AIX resources

As stated previously, CS/AIX user licenses are based on concurrent users of the product. However, it is difficult for CS/AIX to actually measure or report the number of users for many of the different types of communications resources it provides. In addition, the business world is constantly changing, so you may encounter situations that cause your usage of various functions provided by CS/AIX to change.

In order to assist in monitoring and assessing your usage of CS/AIX, a usage monitoring facility is provided. It enables you to monitor the usage of the different types of resources as an indicator of changes in overall usage or peak usage that may occur. This tool is available to help you understand your usage patterns and how they may change. It is *not* intended to monitor or control the CS/AIX licenses that you have previously acquired.

CS/AIX monitors the usage of the following types of communications resources it provides:

- Applications that use APPC or CPI-C APIs
- Applications that use the LUA API
- Active link stations
- Telnet sessions connected to the TN3270 server component of CS/AIX
- Telnet sessions connected to the TN Redirector component of CS/AIX
- Active SNA data sessions (LU1, 2, 3 and 6.2)

The utilization of each resource is measured at 30-minute intervals. In addition, the peak usage (the maximum usage level at any time since the AIX computer was restarted) is maintained. This data is recorded in a “usage log file” that is then available for your analysis and use. At each 30-minute sampling, both the current usage of the resource and the peak usage are recorded for each resource. See Figure 149.

CS/AIX records the usage information in the file /var/sna/sna.usage. The maximum number of bytes that may be recorded in this file is 1,000,000, at which time CS/AIX renames it to /var/sna/bak.usage and clears the log file. The snaadmin command-line administration program may be used to change the name and location of the usage log file, as well as its maximum size.

```
============ Log file initialized 14:10:31 EST  08 Mar 2000 ============

APPC/CPI-C apps|LUA apps     |Active link stations|TN3270 sessions|TN redirect sessions|
Current/Max    |Current/Max  |Current/Max         |Current/Max    |Current/Max         |
------------------------------------------------------------------------------------------


      0/       0|      0/     0|          0/       3|      0/      2|         0/        0|
      0/       0|      0/     0|          0/       3|      0/      2|         0/        0|
      0/       0|      0/     0|          1/       3|      0/      2|         0/        0|
      0/       0|      0/     0|          2/       3|      0/      2|         0/        0|
      0/       0|      0/     0|          4/       4|      1/      2|         0/        0|
      0/       0|      0/     0|          4/       4|      2/      2|         2/        2|
```

Figure 149. Partial listing of the sna.usage file

Figure 149 is a partial listing of the contents of the sna.usage log file. It has been truncated on the right. The format of the usage log file is as follows:

- The file is divided into columns, each recording usage of a particular resource type:
  - APPC and CPI-C applications
  - LUA applications
  - Active link stations
  - TN3270 sessions using TN Server
  - Telnet sessions using TN Redirector
  - Opens to the SNA device from back-level LU6.2 and LU1-3 applications
  - Opens to the SNA device from back-level LU0 and G-SNA applications
  - Data sessions (PLU-SLU sessions)
- Each column shows two figures: the current usage of a particular resource type at the time it was recorded, and the peak usage (the maximum usage level of the resource type at any time since the computer was restarted).
- Each line in the file represents a “snapshot” of the resource usage at a particular time, shown by a timestamp at the end of the line (not displayed in Figure 149 due to page width). Usage is recorded at 30-minute intervals.

CS/AIX provides an additional method for accessing usage information. You can get a “snapshot” of the current (right now) and peak usage at any time using the following command:

```
snaadmin query_node_limits
```

Chapter 12. HTML and docsearch

Product documentation for IBM Communications Server for AIX, Version 6 is distributed on the product CD as an install image that contains Hypertext Markup Language (HTML) softcopy format. This format enables you to search or browse for information more easily using hypertext links for related information. It also makes it easier to share the library across your site.

CS/AIX V6 also includes AIX docsearch indices.

This chapter discusses the installation steps to make this documentation available online.

12.1 Setting up CS/AIX HTML documentation

CS/AIX V6 documentation files are in the sna.html.$LANG.data fileset on the installation media, where $LANG is one of the supported locales:

en_US
Ja_JP
de_DE
es_ES
fr_FR
it_IT
ko_KR
pt_BR
zh_CN
zh_TW

The files are unloaded to the directory /usr/share/man/info/$LANG/sna and the main html file is /usr/share/man/info/$LANG/sna/SNABOOKS.HTM

Not all of the publications were translated for each language. If a particular book was not translated, the en_US equivalent will be displayed instead.

If you have a Web browser on your CS/AIX system, you can access the publications with the URL:

```
file:/usr/share/man/info/$LANG/sna/SNABOOKS.HTM
```

If you have a Web server on the CS/AIX system, you can access the publications with the URL:

```
http://AIXSERVER/doc_link/$LANG/sna/SNABOOKS.HTM
```

where AIXSERVER is the TCP/IP hostname or address.

If the Web server cannot find the file, create a logical link from the Web server's public directory to the /usr/share/man/info directory. For example:

```
ln -fs /usr/HTTPServer/htdocs/doc_link/usr/share/man/info
```

This link will have been already created if you have configured the AIX docsearch service.

In addition to the HTML files, CS/AIX also ships the search indices for use by the AIX docsearch service. These indices are in the sna.html.$LANG.docsearch fileset.

The AIX docsearch service is configured with:

```
smit web_configure
```

Select the option on that SMIT panel titled:

```
Change Documentation and Search Server
```

Once the search server has been configured, you can use the URL:

```
http://AIXSERVER/cgi-bin/ds_form?lang=$LANG
```

to search the CS/AIX manuals for keywords.

For example you can search on define_ip_port to find all the places that string appears in the CS/AIX publications.

Part 5. Application development

Chapter 13. 64-bit SNA applications

IBM Communications Server for AIX, Version 6 introduces support for 64-bit applications when running with AIX V4.3. Applications written to the APIs introduced in CS/AIX V5 (LUA, NOF, APPC, CPI-C, CSV, MS) may be compiled and linked to run in either 32-bit or 64-bit mode. Applications that use the jCPI-C API or the older CS/AIX V4 APIs do not support 64-bit mode.

13.1 Requirements for 64-bit support

IBM AIX V4.3.2 ML2 or later is required if you intend to compile, link or execute applications using CS/AIX APIs in 64-bit mode. 64-bit applications may be compiled and linked on an AIX 32-bit machine, but they must be executed on an AIX 64-bit machine.

The AIX bos.64bit option must be installed. bos.64bit is part of the AIX base operating system. AIX 64-bit support is configured using the command `smit load64bit`.

64-bit support within AIX 4.3 also requires the latest data link control filesets. Depending on your specific CS/AIX configuration, you may require at least one of the following filesets at the level indicated:

Table 2. 64-bit fileset requirements

Link Station Type	Fileset	Level
Token-ring	bos.dlc.token	4.3.3.11
Standard Ethernet	bos.dlc.ether	4.3.3.11
802.3 Ethernet	bos.dlc.8023	4.3.3.11
X.25	bos.dlc.qllc sx25.comio	4.3.3.1 1.1.5.6
SDLC	bos.dlc.sdlc	4.3.3.11
FDDI	bos.dlc.fddi	4.3.3.11
CDLC Channel	sna.dlcchannel	6.0.0.0
MPC Channel	sna.dlcmpc	6.0.0.0

All bos.dlc filesets except sna.dlcchannel and sna.dlcmpc are provided as part of the bos.dlc.usr package in the AIX base operating system.

The latest level for all these filesets may be downloaded from the following URL:

```
http://service.software.ibm.com/cgi-bin/support/rs6000.support/downloads
```

It is possible to have a CS/AIX configuration that does not require any fileset to be installed:

- Applications that use HPR/IP (Enterprise Extender)
- Applications that use APPC over IP
- U-shaped sessions (stays in the RS/6000 box)
- An application that uses one of the APIs that do not leave the box such as a NOF or CSV application

13.2 64-bit architecture and benefits

From an operation point of view, an architecture is said to be 64-bit when:

- It can handle 64-bit-long data. In other words, a contiguous block of 64 bits (8 bytes) in memory is defined as one of the elementary units that the CPU can handle. This means that the instruction set includes instructions for moving 64-bit-long data and instructions for performing arithmetic operations on 64-bit-long integers.
- It generates 64-bit-long addresses, both as effective addresses (the addresses generated and used by machine instructions) and as physical addresses (those that address the memory cards plugged into the machine memory slots). Individual processor implementations may generate shorter physical addresses, but the architecture must support 64-bit addresses.

The distinguishing technical features and benefits of 64-bit computing as contrasted to 32-bit computing are:

- 64-bit integer computation, using hardware with 64-bit general purpose registers
- Large file support
- Large application virtual address spaces
- Large physical memory support

13.2.1 64-bit integer computation

Native 64-bit integer computation is provided by 64-bit hardware, and utilized by programs computing on 64-bit data types. While there are some specialized applications that need to do computation on integer numbers larger than 2^{32}, the key benefit of this capability is in performing arithmetic operations on pointers in 64-bit programs. Floating point computation already includes 64-bit precision on all RS/6000 systems.

13.2.2 Large file support

The ability to create and maintain very large file systems is increasingly important for many users. In particular, data warehousing applications, and scientific and multimedia applications frequently require this support.

The ability to address data in files larger that 2 GB (32-bit addresses) requires that a program be able to specify file offsets larger than a 32-bit number. This capability is generally considered to be a 64-bit computing function even though it does not require 64-bit hardware support. AIX Version 4.2 provided this capability for 32-bit programs, and AIX Version 4.3 provides it for 64-bit programs as well. Since it does not depend on 64-bit hardware, this function can be used on any RS/6000 system running the appropriate release of AIX.

There is, however, synergy between large file support and 64-bit hardware capabilities, in that a 64-bit program can have much larger portions of 64-bit files in its address space, as well as in system memory, at one time, than a 32-bit system could provide.

13.2.3 Large application virtual address spaces

In 32-bit systems, an individual program, or process, may typically have between 2 GB and 4 GB of virtual address space for its own use to contain instructions and data. With 64-bit computing, applications may run in a 64-bit address space, where an individual program’s addressability becomes measured in terabytes (TB). Types of applications that currently understand how to exploit this opportunity include the following:

- Some database management programs use a large address space for scalability, in order to maintain very large data buffers in memory, reducing the amount of I/O they need to perform. Using a large address space, they can supply data to client applications at the pace needed to sustain the high transaction rate potential afforded by many of the new processors in the industry.
- In certain cases, database management programs or customer applications may benefit from keeping an entire database or large file immediately accessible in memory. Read-only data lends itself most

readily to this scenario. Significant improvements in response time or transaction rates are possible.

- Certain types of applications are able to directly attack larger problems by organizing larger arrays of data to be computed upon. Computer simulation of a physical phenomenon, such as aircraft flight or a nuclear reaction, are frequently cited examples.

Since internal memory is much faster than most storage devices, the ability to fetch and keep more data in memory, where it can be directly manipulated, should provide dramatic performance improvements. Table 3 provides the size of the address space that can be managed as a function of the length of the address.

Table 3. Size of address space as a function of address length

Address Length	Flat Address Space
8-bit	256 bytes
16-bit	64 Kilobytes
32-bit	4 Gigabytes
52-bit	4000 Terabytes
64-bit	16 Million Terabytes

13.2.4 Large physical memory support

Sufficient system memory is crucial for sustaining overall system performance. As a system’s processor capacity grows with the speed and number of processors in the system, so does the requirement for system memory. Memory is a key element to having “balance resources”, a requirement that applies whether the workload consists of 32-bit or 64-bit applications. For many customer environments, system memory capacity beyond 4 GB will be needed for optimum performance on an 8-way machine, with even more needed on a 12-way configuration. This is true even when the entire workload consists of growth in the throughput of 32-bit programs.

The new dimension of scalability introduced by 64-bit technology is the opportunity for some programs to keep very large amounts of data in memory, both resident in physical memory and accessible in their 64-bit virtual memory address space. While exploiting this new capability can significantly improve performance for some applications, there are relatively few types of applications that have evolved to make use of such techniques today. Those that have, however, most often make use of very large memory, that is, multiple gigabytes of system memory, just for one application program.

13.3 Compatibility and interoperability

If you consider the benefits of 64-bit computing in the context of a customer with an established information technology investment based on existing 32-bit system implementations, it seems obvious that 64-bit computing will complement 32-bit computing in different ways for different customers. Customers will move at a wide range of speeds into exploitation of the various elements of 64-bit programs. The 64-bit virtual address space is of value to specific applications that can exploit it; other applications are best left as 32-bit programs, but must be able to coexist and interoperate with the selective, but typically strategic, applications that are ported to 64-bit.

There is no single dimension to scalability. Some environments can grow with more 32-bit processes running on larger SMP systems. In many server environments, a critical server application must also scale with system throughput, using larger files and/or bigger data buffers large enough to demand a 64-bit address space. Customer investment protection assistance, combined with customer flexibility to implement 64-bit technology as their environment demands it, leads to the requirement that 64-bit systems should support 32-bit binary compatibility, and that 32-bit and 64-bit environments must coexist and cooperate and share resources as easily as 32-bit programs traditionally have in the past.

13.3.1 64-bit hardware compatibility

RS/6000 64-bit products are built upon the PowerPC processor architecture, which defines both 64-bit and 32-bit processors, the latter a subset of the former. In practical terms, this means a PowerPC 64-bit processor is a proper superset of a 32-bit processor, allowing a 64-bit processor to run 32-bit programs the same way the programs run on a 32-bit processor. Hardware 32-bit binary compatibility is native; it does not rely on high-overhead emulation techniques.

Hardware support for 32-bit binary compatibility is the first step in achieving 32-bit application binary compatibility on 64-bit systems under AIX V4.3. This hardware compatibility is also used by AIX itself, as a building block in maintaining binary compatibility for existing device drivers and kernel extensions running on 64-bit systems.

13.3.2 64-bit software compatibility

The 64-bit execution environment for application processes is an upward-compatible addition to AIX capability, not a replacement for existing 32-bit function. The design chosen for 64-bit AIX allows existing 32-bit applications to run with 64-bit applications with no changes, thus protecting the investment users have made in their current applications. Users can take advantage of the features of 64-bit AIX when business needs dictate.

AIX 64-bit support is intended to be run on 64-bit hardware systems, not simply any system containing a 64-bit PowerPC processor. A 64-bit hardware system is one that is based on the RS/6000 architecture and identifies 64-bit properties for the processor(s) and processor host bridges (PHBs) in configurations with memory addressing greater than 32 bits.

For AIX, and the applications that run on AIX, the 64-bit PowerPCs have two important attributes. They are very fast when running as 32-bit processors, and they offer the opportunity of running a 64-bit environment. AIX V4.3 exploits these attributes separately. There are two different execution environments in AIX V4.3, the 32-bit execution environment and the 64-bit execution environment. These two environments are only available for 64-bit hardware. There is no 64-bit execution environment on 32-bit hardware.

Generally, the AIX V4.3 kernel remains 32-bit, and only selected parts, such as the Virtual Memory Manager, are upgraded to be aware of the 64-bit address space. This means that the number of AIX kernels remains at two (uniprocessor and multiprocessor).

13.4 CS/AIX and 64-bit applications

What does all this mean to you as an application developer in the CS/AIX environment? If you choose to develop applications using the newer APIs, those applications can be compiled and linked as either 32-bit or 64-bit applications. A mixture of 32-bit and 64-bit APPC or CPI-C applications can be run on the same machine and communicate with other 32-bit or 64-bit applications on the same or different machines.

Applications that use the 64-bit APIs can run only on 64-bit hardware, while applications that use the 32-bit APIs can run on either 32-bit or 64-bit hardware.

In addition, 64-bit applications can be written, compiled and linked on an AIX 4.3 32-bit machine (development system), and then executed on an AIX 4.3 64-bit machine (production system).

13.4.1 Sample applications

CS/AIX does not ship any sample applications that explicitly use 64-bit capabilities. However, using the instructions in the appropriate manual, you can compile the APPC, CPI-C and LUA sample programs as 64-bit. The sample programs are in /usr/lib/sna/samples.

The APPC sample programs are “asample1.c” and “asample2.c”.

The CPI-C sample programs are “csample1.c” and “asample2.c”.

The LUA sample program is “lsample.c”.

Following are the commands that show how to configure, compile, and run the CPI-C sample programs in 64-bit mode. The steps below assume this is a new configuration and that the CPI-C programs will be run in a U-shaped session (not over a real physical link) where both the TPs are in the same CS/AIX node.

1. Make sure the software pre-reqs are installed:

   ```
   lslpp -h bos.64bit sna.rte64
   ```

2. Compile the sample CPI-C programs using the correct libraries and flags for 64-bit mode:

   ```
   cd /usr/lib/sna/samples
   cc -o csample1 -I /usr/include/sna \
   -bimport:/usr/lib/sna/cpic64.exp -q64 csample1.c
   cc -o csample2 -I /usr/include/sna \
   -bimport:/usr/lib/sna/cpic64.exp -q64 csample2.c
   ```

3. Confirm that the executables are 64-bit programs:

   ```
   file csample1 csample2
   ```

4. Set the permissions for the target TP:

   ```
   chown root csample2
   chmod +s csample2
   ```

5. Configure the CS/AIX node:

   ```
   snaadmin define_node, cp_alias=AIXCP, fqcp_name=NETID.AIXCP
   snaadmin define_mode, mode_name=LOCMODE
   snaadmin define_local_lu, lu_name=TPLU1, lu_alias=TPLU1
   snaadmin define_local_lu, lu_name=TPLU2, lu_alias=TPLU2
   snaadmin define_cpic_side_info, sym_dest_name=CPICTEST, \
      lu_alias=TPLU1, partner_lu_name=NETID.TPLU2, \
   ```

```
   mode_name=LOCMODE, tp_name=TPNAME2
snaadmin define_tp, tp_name=TPNAME2
snaadmin define_tp_load_info, tp_name=TPNAME2, userid=root, \
   path=/usr/lib/sna/samples/csample2, type=QUEUED, \
   env=APPCTPN=TPNAME2, env=APPCLLU=TPLU2
```

6. Start the CS/AIX node:

```
snaadmin init_node
```

7. Run the local TP:

```
export APPCLLU=TPLU1
export APPCTPN=TPNAME1
./csample1 /etc/hosts
   Q
```

Chapter 14. Java CPI-C

IBM Communications Server for AIX, Version 6 has been enhanced to enable customers to take advantage of Java as an efficient application development tool to more easily bridge the gap between the Internet and critical legacy data applications.

In addition to the standard C-language CPI-C API, CS/AIX now includes a CPI-C API for use by Java applications.

14.1 Overview

Java CPI-C (jCPI-C) is a new API for CS/AIX V6 that allows you to write Java programs that make CPI-C calls. These programs can be used as any of the LU6.2 Transaction Program (TP) types:

- Invoking TP
- Invokable TP
- Operator started TP

An invoking TP is sometimes called a *client TP* or a *local TP*. APING is an example of this type of TP.

An invokable TP is sometimes called a *server TP* or a *remote TP*. It has an entry in the /etc/sna/sna_tps file and is started automatically by CS/AIX when an ATTACH arrives with that TP name. AFTPD is an example of this type of TP.

An operator started TP is also sometimes called a *server TP* or a *remote TP*. The difference is that it is started by a user or application and not by CS/AIX and it has to be ready and waiting when the ATTACH arrives.

Not all of the CPI-C calls are available in the Java environment. For example, the nonblocking mode is not available in Java CPI-C. See the *CS/AIX V6 CPI-C Programmer's Guide*, SC31-8591-01, for more details about which calls are valid.

CS/AIX V6 ships a sample Java CPI-C program called *JPing* which shows an invoking TP, similar in function to APING. The source code for the JPing sample is in the directory:

    /usr/lib/sna/samples

The parameters for JPing are different from those for APING. Here is the usage statement:

```
JPing [-s symb_dest] [-n num_iter] [-d data_len]
```

Here are steps for using JPing on a U-shaped (loopback) session:

1. Must have Java 1.1.6, 1.1.8, 1.2.2, or 1.3.0 installed:

   ```
   lslpp -h 'Java*.rte.*'
   ```

2. Create a cpic side info definition:

   ```
   snaadmin define_cpic_side_info, sym_dest_name=LOOPBACK, \
   partner_lu_name=NETID.AIXCP, mode_name='#INTER', \
   tp_name=APINGD
   ```

   where `NETID.AIXCP` is the fully-qualified CP name of the CS/AIX node.

3. Set up the Java environment:

   a. For Java 1.1.6 or 1.1.8 do:

   ```
   export LIBPATH=$LIBPATH:/usr/lib/sna
   export CLASSPATH=/usr/lib/sna/samples:/usr/lib/sna/cpic.jar
   ```

   b. For Java 1.2.2 do:

   ```
   export PATH=/usr/java_dev2/jre/sh:/usr/java_dev2/sh:$PATH
   export LIBPATH=$LIBPATH:/usr/lib/sna
   export CLASSPATH=/usr/lib/sna/samples:/usr/lib/sna/cpic.jar
   ```

   c. For Java 1.3.0 do:

   ```
   export PATH=/usr/java130/jre/bin:/usr/java130/bin:$PATH
   export LIBPATH=$LIBPATH:/usr/lib/sna
   export CLASSPATH=/usr/lib/sna/samples:/usr/lib/sna/cpic.jar
   ```

4. Check the java environment:

   ```
   java -version
   ```

5. Run the JPing program:

   a. For Java 1.1.6, 1.1.8, or 1.2.2 do:

   ```
   java JPing -s LOOPBACK
   ```

   b. For Java 1.3.0 do:

   ```
   java -Djava.library.path=$LIBPATH JPing -s LOOPBACK
   ```

For an invokable TP you would need to create an /etc/sna/sna_tps entry similiar to this:

```
[JPINGD]
```

```
LUALIAS = ""
DESCRIPTION = ""
USERID = guest
GROUP = ""
TIMEOUT = 5
TYPE = NON-QUEUED
STYLE = EXTENDED
PATH = /usr/bin/java
ARGUMENTS = JPINGD
STDOUT = /tmp/stdout
STDERR = /tmp/stderr
ENV = CLASSPATH=/usr/lib/sna/cpic.jar:/u/jpingd
ENV = LIBPATH=/usr/lib/sna:/usr/jdk_base/lib/aix/native_threads
```

This example is for Java 1.1.6 or 1.1.8 and assumes the .class file for the Java CPI-C TP is in /u/jpingd. Changes would have to be made for Java 1.2.2 or 1.3.0 or more complex TPs.

Appendix A. Special notices

This publication is intended to help AIX systems and network administrators to plan, install and configure the new features and functions included in IBM Communications Server for AIX, Version 6. The information in this publication is not intended as the specification of any programming interfaces that are provided by CS/AIX, V6. See the PUBLICATIONS section of the IBM Programming Announcement for IBM Communications Server for AIX, Version 6 for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785.

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, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AIX
APPN
CICS
ES/9000
IBM
OS/2
RISC System/6000
S/390
SP
VTAM
Lotus
Tivoli

AnyNet
AS/400
CUA
ESCON
Micro Channel
OS/390
RS/6000
SecureWay
TCS
WebSphere
Domino
NetView

The following terms are trademarks of other companies:

Tivoli, Manage. Anything. Anywhere.,The Power To Manage., Anything. Anywhere.,TME, NetView, Cross-Site, Tivoli Ready, Tivoli Certified, Planet Tivoli, and Tivoli Enterprise are trademarks or registered trademarks of Tivoli Systems Inc., an IBM company, in the United States, other countries, or both. In Denmark, Tivoli is a trademark licensed from Kjøbenhavns Sommer - Tivoli A/S.

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. 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 and/or other countries.

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States and/or other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Appendix B. Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

B.1 IBM Redbooks

For information on ordering these publications see “How to get IBM Redbooks” on page 231.

- *IBM eNetwork Communications Server for AIX: Understanding and Migrating to Version 5 (Part 1): Configuration and New Features*, SG24-5215
- *IBM eNetwork Communications Server for AIX: Understanding and Migrating to Version 5: Part 2 - Performance,* SG24-2136

B.2 IBM Redbooks collections

Redbooks are also available on the following CD-ROMs. Click the CD-ROMs button at http://www.redbooks.ibm.com/ for information about all the CD-ROMs offered, updates and formats.

CD-ROM Title	Collection Kit Number
System/390 Redbooks Collection	SK2T-2177
IBM Networking Redbooks Collection	SK2T-6022
Transaction Processing and Data Management Redbooks Collection	SK2T-8038
Lotus Redbooks Collection	SK2T-8039
Tivoli Redbooks Collection	SK2T-8044
AS/400 Redbooks Collection	SK2T-2849
Netfinity Hardware and Software Redbooks Collection	SK2T-8046
RS/6000 Redbooks Collection (BkMgr)	SK2T-8040
RS/6000 Redbooks Collection (PDF Format)	SK2T-8043
Application Development Redbooks Collection	SK2T-8037
IBM Enterprise Storage and Systems Management Solutions	SK3T-3694

B.3 Other resources

These publications are also relevant as further information sources:

- *IBM eNetwork Communications Server for AIX Quick Beginnings Version 6*, GC31-8583

- *IBM eNetwork Communications Server for AIX Migration Guide Version 6*, SC31-8585
- *IBM eNetwork Communications Server for AIX Administration Guide Version 6*, SC31-8586
- *IBM eNetwork Communications Server for AIX Administration Command Reference Version 6*, SC31-8587
- *IBM SecureWay Communications Server for AIX Channel Connectivity User's Guide Version 6*, SC31-8219
- *IBM eNetwork Communications Server for AIX CPI-C Programmer's Guide Version 6*, SC31-8591
- *IBM eNetwork Communications Server for AIX APPC Application Suite Version 6*, SC31-8596
- *IBM eNetwork Communications Server for AIX Diagnostics Guide Version 6*, SC31-8588
- *S/390 ESCON Channel PCI Adapter User's Guide,* SC23-4232
- *PCI Adapter Placement Reference*, SA38-0538
- *OS/390 SecureWay Communications Server: SNA Resource Definition Reference*, SC31-8565
- *OS/390 SecureWay Communications Server: SNA Network Implementation*, SC31-8563

B.4 Referenced Web sites

These Web sites are also relevant as further information sources:

- `http://www.ibm.com/software/network/commserver/`

  Communications Server product home page
- `http://www.ibm.com/software/network/commserver/support/`

  Communications Server service and support page
- `http://www.ibm.com/software/network/library/whitepapers/`

  IBM networking white papers
- `http://www.ibm.com/software/network/commserver/library/`

  Communications Server white papers, documentation, and brochures

How to get IBM Redbooks

This section explains how both customers and IBM employees can find out about IBM Redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** http://www.redbooks.ibm.com/

  Search for, view, download, or order hardcopy/CD-ROM Redbooks from the Redbooks Web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this Redbooks site.

  Redpieces are Redbooks in progress; not all Redbooks become redpieces and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

- **E-mail Orders**

  Send orders by e-mail including information from the IBM Redbooks fax order form to:

	e-mail address
In United States	usib6fpl@ibmmail.com
Outside North America	Contact information is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	Country coordinator phone number is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Fax Orders**

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	Fax phone number is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

This information was current at the time of publication, but is continually subject to change. The latest information may be found at the Redbooks Web site.

IBM Intranet for Employees

IBM employees may register for information on workshops, residencies, and Redbooks by accessing the IBM Intranet Web site at http://w3.itso.ibm.com/ and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may access MyNews at http://w3.ibm.com/ for redbook, residency, and workshop announcements.

IBM Redbooks fax order form

Please send me the following:

Title	**Order Number**	**Quantity**

First name Last name

Company

Address

City Postal code Country

Telephone number Telefax number VAT number

□ Invoice to customer number

□ Credit card number

Credit card expiration date Card issued to Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

Index

IBM Redbooks review

Your feedback is valued by the Redbook authors. In particular we are interested in situations where a Redbook "made the difference" in a task or problem you encountered. Using one of the following methods, **please review the Redbook, addressing value, subject matter, structure, depth and quality as appropriate.**

- Use the online **Contact us** review redbook form found at **ibm.com**/redbooks
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Document Number **Redbook Title**	SG24-5947-00 IBM Communications Server for AIX, V6 New Features and Implementation Scenarios
Review	
What other subjects would you like to see IBM Redbooks address?	
Please rate your overall satisfaction:	O Very Good O Good O Average O Poor
Please identify yourself as belonging to one of the following groups:	O Customer O Business Partner O Solution Developer O IBM, Lotus or Tivoli Employee O None of the above
Your email address: The data you provide here may be used to provide you with information from IBM or our business partners about our products, services or activities.	 O Please do not use the information collected here for future marketing or promotional contacts or other communications beyond the scope of this transaction.
Questions about IBM's privacy policy?	The following link explains how we protect your personal information. **ibm.com**/privacy/yourprivacy/

IBM Communications Server for AIX, V6 New Features and Implementation Scenarios

(0.5” spine)
0.475”<->0.875”
250 <-> 459 pages

IBM Communications Server for AIX, V6

New Features and Implementation Scenarios

Scenarios for Telnet Redirector, SSL, and Service Location Protocol

Covers SNA features Enterprise Extender, Branch Extender, MPC+

Examples of Web Admin, 64-bit apps and more

This new release of Communications Server for AIX includes many new features and functions that make CS/AIX a more important player in bridging the e-business gap between the Internet and critical legacy data applications. Support for secure TN3270 communications with SSL and load balancing with SLP are critical in ensuring secure and consistent communications with the host. Support for high performance routing, branch network configurations, and channel attachment are significant in that they allow placement of Communications Server anywhere it benefits performance most in the customer's IP or SNA network.

This book covers the new features and functions in Communications Server for AIX, Version 6. Each feature is explained. Implementation steps are listed for most features, and sample scenarios are reviewed to give a better understanding of where a feature or function may fit in your networking environment.

Guidelines given in this redbook are general. Several scenarios are included, and although actual customer networks most likely will differ, these scenarios serve as examples for customers to develop proper plans to expand or migrate their networks to meet future business requirements. Customers are invited to engage IBM in the planning process.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by IBM's International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-5947-00 ISBN 0738417874