System z10

Processor Resource/Systems Manager Planning Guide

SB10-7153-02

System z10

Processor Resource/Systems Manager Planning Guide

SB10-7153-02

Note

| Before using this information and the product it supports, read the information in "Safety" on page
| xi, Appendix D, "Notices," on page 227, and *IBM Systems Environmental Notices and User Guide*,
| Z125-5823.

Third Edition (July 2009)

| This edition, SB10-7153-02, applies to the IBM® System z10™ Enterprise Class (z10™ EC) and System z10 Business
| Class (z10 BC) servers. This edition replaces SB10–7153–01 and SB10-7153-01a. Technical changes to the text are
| indicated by a vertical bar (|) to the left of the change.

| There may be a newer version of this document in a **PDF** file available on **Resource Link™**. Go to
| *http://www.ibm.com/servers/resourcelink* and click on **Library** on the navigation bar. A newer version is indicated by a
| lowercase, alphabetic letter following the form number suffix (for example: 00a, 00b, 01a, 01b).

Contents

Figures

Tables

Safety

Safety notices

Safety notices may be printed throughout this guide. **DANGER** notices warn you of conditions or procedures that can result in death or severe personal injury. **CAUTION** notices warn you of conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous. **Attention** notices warn you of conditions or procedures that can cause damage to machines, equipment, or programs.

There are no **DANGER** notices in this guide.

World trade safety information

Several countries require the safety information contained in product publications to be presented in their national languages. If this requirement applies to your country, a safety information booklet is included in the publications package shipped with the product. The booklet contains the safety information in your national language with references to the US English source. Before using a US English publication to install, operate, or service this IBM product, you must first become familiar with the related safety information in the booklet. You should also refer to the booklet any time you do not clearly understand any safety information in the US English publications.

Laser safety information

All System z models can use I/O cards such as PCI adapters, ESCON, FICON, Open Systems Adapter (OSA), InterSystem Coupling-3 (ISC-3), or other I/O features which are fiber optic based and utilize lasers or LEDs.

Laser safety compliance

All lasers are certified in the U.S. to conform to the requirements of DHHS 21 CFR Subchapter J for class 1 laser products. Outside the U.S., they are certified to be in compliance with IEC 60825 as a class 1 laser product. Consult the label on each part for laser certification numbers and approval information.

CAUTION:
Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

CAUTION:
This product contains a Class 1M laser. Do not view directly with optical instruments. (C028)

About this publication

This information is intended for system planners, installation managers, and other technical support personnel who need to plan for operating in logically partitioned mode (LPAR mode) on the IBM System z10 Business Class (z10 BC) and IBM System z10 Enterprise Class (z10 EC).

This publication assumes previous knowledge of the characteristics and functions of the installed central processor complex (CPC).

To improve readability, we refer to the different CPCs using the following terminology whenever possible:

Table 1. Terminology used in this publication

Terminology	Central Processor Complex (CPC)
z10 BC	Model E10
z10 EC	Model E12 Model E26 Model E40 Model E56 Model E64

Some features, panels, and functions are model-dependent, engineering change (EC) level-dependent, machine change level-dependent (MCL-dependent), or control program-dependent. For this reason, not all of the functions discussed in this publication are necessarily available on every CPC.

Some illustrations and examples in this publication describe operation with as few as 2 logical partitions (LPs), although up to 60 LPs can be defined on a z10 EC (or 30 LPs on a z10 BC).

Figures included in this document illustrate concepts and are not necessarily accurate in content, appearance, or specific behavior.

Sample tasks and panels explained in this publication reference tasks and panels available from the Support Element console. However, detailed procedures for operator tasks and accurate task and panel references are explained in the *System z10 Support Element Operations Guide*.

Hardware Management Console operators or Support Element console operators should use the appropriate operations guide for instructions on how to perform tasks. Control program operators should refer to the appropriate control program publication for information on control program commands.

For information about PR/SM™ LPAR mode on prior models, see the following publications:

- *System z9 Processor Resource/Systems Manager Planning Guide*, SB10-7041
- *zSeries 890 and 990 Processor Resource/Systems Manager Planning Guide*, SB10-7036
- *zSeries 800 and 900 Processor Resource/Systems Manager Planning Guide*, SB10-7033
- *S/390® Processor Resource/Systems Manager Planning Guide*, GA22-7236

- *ES/9000® Processor Resource/Systems Manager Planning Guide*, GA22-7123

However, for the most current coupling facility control code information for all models, use this publication.

What is included in this publication

The information presented in this publication is organized as follows:

- Chapter 1, "Introduction to logical partitions" describes the prerequisites for establishing and using LPAR, the general characteristics and some potential applications for LPs.
- Chapter 2, "Planning considerations" presents considerations and guidelines for I/O configuration planning and coupling facility planning.
- Chapter 3, "Determining the characteristics of logical partitions" includes a list of the panels, provides guidelines for determining the CPC resources, and describes the operator tasks used to define the characteristics of LPs.
- Chapter 4, "Operating logical partitions" describes how to operate the Hardware Management Console and the Support Element console, and describes the procedure for initializing the system.
- Chapter 5, "Monitoring the activities of logical partitions," on page 189 describes the panels and operator tasks used to monitor LP activity.
- Appendix A, "User interface (UI) styles," on page 207 describes the tree-style and classic user interface styles of the Support Element.
- Appendix B, "Coupling facility control code support," on page 211 lists and explains the support provided at different levels of coupling facility control code Licensed Internal Code (LIC).
- Appendix C, "Developing, building, and delivering a certified system," on page 213 provides guidance in setting up, operating, and managing a secure consolidated environment using System z10 EC PR/SM.
- Appendix D, "Notices," on page 227 contains electronic emission notices, legal notices, and trademarks.

Related publications

The following publications provide information about the functions and characteristics of the different CPCs and the related operating systems that run on them.

z/Architecture

- *z/Architecture Principles of Operation*, SA22-7832

Enterprise Systems Architecture/390 (ESA/390)

- *Enterprise Systems Architecture/390 Principles of Operation*, SA22-7201

Hardware

System z10 Business Class

- *System z10 Business Class System Overview*, SA22–1085
- *System z Input/Output Configuration Program User's Guide for ICP IOCP*, SB10-7037
- *System z10 and System z9 Stand-alone IOCP User's Guide*, SB10-7152
- *System z Hardware Management Console Operations Guide*, SC28-6873
- *System z10 Support Element Operations Guide*, SC28-6879

System z10 Enterprise Class

- *System z10 Enterprise Class System Overview*, SA22-1084
- *System z Input/Output Configuration Program User's Guide for ICP IOCP*, SB10-7037
- *System z10 and System z9 Stand-alone IOCP User's Guide*, SB10-7152
- *System z Hardware Management Console Operations Guide*, SC28-6873
- *System z10 Support Element Operations Guide*, SC28-6879

ESCON concepts

- *Introducing Enterprise Systems Connection*, GA23-0383
- *ESCON and FICON Channel-to-Channel Reference*, SB10-7034

FICON

- *ESCON and FICON Channel-to-Channel Reference*, SB10-7034

Crypto features

The following publications provide additional information on the Crypto features:

- *System z10 Support Element Operations Guide*, SC28-6868
- *User Defined Extensions Reference and Guide*, website: http://www.ibm.com/security/cryptocards (Select a cryptocard, and then click **Library**)
- *IBM System z10 Enterprise Class Technical Guide*, SG24-7516

Software

z/OS

zSeries Parallel Sysplex: The following publications provide additional information about the z/OS® Parallel Sysplex® environment:

- *z/OS Parallel Sysplex Overview*, SA22-7661
- *z/OS Parallel Sysplex Application Migration*, SA22-7662
- *z/OS MVS Setting Up a Sysplex*, SA22-7625
- *z/OS MVS Programming: Sysplex Services Guide*, SA22-7617
- *z/OS MVS Programming: Sysplex Services Reference*, SA22-7618

Multiple Image Facility: The following publications provide additional information about Multiple Image Facility in the z/OS environment:
- *z/OS Hardware Configuration Definition: User's Guide*, SC33-7988

Dynamic I/O Configuration: The following publication provides information about dynamic I/O configuration in the z/OS environment:
- *z/OS Hardware Configuration Definition Planning*, GA22-7525

Dynamic Storage Reconfiguration: The following publications provide additional information on the commands, functions, and capabilities of dynamic storage reconfiguration in the z/OS environment:
- *z/OS MVS Initialization and Tuning Reference*, SA22-7592
- *z/OS MVS Recovery and Reconfiguration Guide*, SA22-7623
- *z/OS MVS System Commands*, SA22-7627

Crypto features: The following publications provide additional information on the Crypto features:
- *z/OS ICSF Administrator's Guide*, SA22-7521
- *z/OS ICSF System Programmer's Guide*, SA22-7520
- *z/OS Cryptographic Services ICSF TKE Workstation User's Guide*, SA23-2211

Sysplex Failure Manager: The following publication provides an overview of SFM and practical information for implementing and using SFM in the z/OS environment:
- *z/OS MVS Setting Up a Sysplex*, SA22-7625

LPAR Management Time: The following publication provides information about the RMF™ Partition Data Report that includes LPAR Management Time reporting in a z/OS environment:
- *z/OS Resource Measurement Facility User's Guide*, SC33-7990

Intelligent Resource Director (IRD): The following publication provides information about Intelligent Resource Director in a z/OS environment:
- *z/OS Intelligent Resource Director*, SG24-5952

z/VM

Hardware Configuration Definition (HCD): The following publication provides information about the Hardware Configuration Definition (HCD):
- *z/VM I/O Configuration*, SC24-6100

Hardware Configuration Manager: The following publication provides information about the Hardware Configuration Manager:
- *z/OS and z/VM Hardware Configuration Manager User's Guide*, SC33-7989

Dynamic I/O Configuration: The following publication provides information about dynamic I/O configuration:
- *CP Planning and Administration*, SC24-6083
- *z/VM I/O Configuration*, SC24-6100

Guest Operating Systems: The following publication provides information about running ***guest*** operating systems:
- *z/VM Running Guest Operating Systems*, SC24-6115

How to send your comments

Your feedback is important in helping to provide the most accurate and high-quality information. Send your comments by using Resource Link at *http://www.ibm.com/servers/resourcelink*. Select **Feedback** on the navigation bar on the left. Be sure to include the name of the book, the form number of the book, the version of the book, if applicable, and the specific location of the text you are commenting on (for example, a page number or table number).

Summary of changes

Summary of changes for SB10-7153–02:

This revision contains editorial changes and the following new technical changes:

New information

- Added information regarding FICON Express8.

Summary of changes for SB10-7153–01a:

This revision contains editorial changes and the following new technical changes:

New information

- Added information regarding the use of the IFL feature for OpenSolaris™ workloads.

Summary of changes for SB10-7153–01:

This revision contains editorial changes and the following new technical changes:

New information

- This book was updated to include information for both the IBM System z10 Business Class (z10 BC) and the IBM System z10 Enterprise Class (z10 EC).
- Information about the Crypto Express2-1P feature was added. Crypto Express2–1P is supported on the z10 BC.
- Long reach 1x InfiniBand® coupling links (1x IB-SDR or 1x IB-DDR) information was added.
- The Level 16 Coupling Facility enhancements were added.
- Counter Facility Security Options and Sampling Facility Security Options were added, which may be changed with the Change Logical Partition Security task, or the Security page of the Customize Image Profiles task.

Changed information

- Control Program support information has been updated.

Chapter 1. Introduction to logical partitions

Overview

This chapter introduces the characteristics of logical partitioning and migration and compatibility considerations. Processor Resource/Systems Manager™ (PR/SM) is standard on all z10 BC and z10 EC models.

Prerequisites for operation

The prerequisites for operation are:
- Programming compatibility
- Hardware support
- Operator training
- Programming support
  - Control program support
  - Input/Output Configuration Program (IOCP) support

PR/SM

PR/SM enables logical partitioning of the central processor complex (CPC).

Logical partitioning

PR/SM enables the logical partitioning function of the CPC. The operator defines the resources that are to be allocated to each logical partition (LP). Most resources can be reconfigured without requiring a power-on reset. After an ESA/390, ESA/390 TPF, or Linux®-Only LP is defined and activated, you can load a supported control program into that LP. If a coupling facility logical partition is defined and activated, the coupling facility control code is automatically loaded into the LP.

Central storage

Central storage is defined to LPs before LP activation. When an LP is activated, the storage resources are allocated in contiguous blocks. These allocations can be dynamically reconfigured. Sharing of allocated central storage among multiple LPs is not allowed.

On System z10, all storage is defined as central storage. Allocation of storage to logical partitions can be made as either central storage or expanded storage. Any allocation of expanded storage to an LP reduces the amount of storage available for allocation as central storage. See “Single storage pool” on page 101. If no storage is allocated as expanded storage and no other LP is currently active, an individual LP can have a central storage amount equal to customer storage or 1 Terabyte, whichever is less. The sum total of all LP central and expanded storage cannot exceed the amount of customer storage. Central storage in excess of 2 GB should only be allocated in an LP that has an operating system capable of utilizing 64-bit z/Architecture®.

Expanded storage

Optional expanded storage is defined to LPs before LP activation. When an LP is activated, the storage resources are allocated in contiguous blocks. These allocations can be dynamically reconfigured. Sharing of allocated expanded storage among multiple LPs is not allowed.

See “Expanded storage” on page 104.

Central processors

Central processors (CPs) can be dedicated to a single LP or shared among multiple LPs. CPs are allocated to an LP when the LP is activated. You can use operator tasks to limit and modify the use of CP resources shared between LPs while the LPs are active.

Multiple Image Facility

The Multiple Image Facility (MIF) is available on all CPCs discussed in this publication. MIF allows channel sharing among LPs. For information about accessing devices on shared channel paths and defining shared channel paths, see “Defining shared channel paths” on page 138.

MCSS: Multiple Logical Channel Subsystems (CSS) are available on all CPCs discussed in this publication. Each CSS supports a definition of up to 256 channels.

Channel paths: Active LPs can share channels. Shared channels require that the channel subsystem establish a logical path for each channel image corresponding to an active LP that has the channel configured online. CNC, CTC, OSC, OSD, OSE, OSN, CBP, CFP, CIB, ICP, FC, FCV, FCP, and IQD channel path types can be shared. CVC and CBY channel paths ***cannot*** be shared.

For information about accessing devices on shared channel paths and defining shared channel paths, see “Defining shared channel paths” on page 138.

Crypto features

There are two optional crypto features available, which are designed for Federal Information Processing Standard (FIPS) 140-2 Level 4 Certification. The Crypto Express2 feature, available on the z10 BC and z10 EC, contains two PCI-X adapters, each of which can be configured independently as either a coprocessor or an accelerator. The default configuration is coprocessor. Crypto Express2 can be configured using the Cryptographic Configuration panel found under the Configuration tasks list.

The Crypto Express2-1P feature is identical to the Crypto Express2 feature in functionality, but contains a single PCI-X adapter. This adapter can also be defined as either a coprocessor or an accelerator. It is only supported on the z10 BC model.

Crypto Express2 Coprocessor (CEX2C) replaces the functions of the PCI X Crypto Coprocessor (PCIXCC), which was available on some previous zSeries processors, such as the z890 and z990.

Crypto Express2 Accelerator (CEX2A) replaces the functions of the PCI Crypto Accelerator (PCICA), which was available on some previous zSeries processors such as the z890 and z990.

Crypto Express2 Coprocessor is used for secure key encrypted transactions, and is the default configuration. CEX2C:

- Supports highly secure cryptographic functions, use of secure encrypted key values, and User Defined Extensions (UDX).
- Is designed for Federal Information Processing Standard (FIPS) 140-2 Level 4 certification.

Crypto Express2 Accelerator is used for SSL acceleration. CEX2A:

- Supports clear key RSA acceleration.

- Offloads compute-intensive RSA public-key operations employed in the SSL protocol.

CP Crypto Assist Functions

CP Crypto Assist Functions (CPACF), supporting clear key encryption, offers the following on every Processor Unit (PU) identified as a Central Processor (CP), including zIIPs and zAAPs, or Integrated Facility for Linux (IFL):

- Data Encryption Standard (DES)
- Triple Data Encryption Standard (TDES)
- Advanced Encryption Standard (AES) 128-bit, 192-bit and 256-bit keys
- SHA-1
- SHA-2
- Pseudo Random Number Generation (PRNG)

System z Parallel Sysplex support

Parallel sysplex makes use of a broad range of hardware and software products to process in parallel a transaction processing workload across multiple z/OS images running in a sysplex and sharing data in a coupling facility.

Parallel sysplex allows you to manage a transaction processing workload, balanced across multiple z/OS images running on multiple CPCs, as a single data management system. It also offers workload availability and workload growth advantages.

The parallel sysplex enhances the capability to continue workload processing across scheduled and unscheduled outages of individual CPCs participating in a sysplex using a coupling facility by making it possible to dynamically reapportion the workload across the remaining active sysplex participants. Additionally, you can dynamically add processing capacity (CPCs or LPs) during peak processing without disrupting ongoing workload processing.

CPC support consists of having the capability to do any or all of the following:

- Install coupling facility channels
- Define, as an LP, a portion or all of the CPC hardware resources (central processors, storage, and coupling facility channels) for use as a coupling facility that connects to z/OS images for data sharing purposes
- Connect to a coupling facility to share data
- Define a z10 BC or z10 EC with only ICFs to serve as a stand-alone coupling facility, which may contain one or more coupling facility images, but which cannot run z/OS or any other operating system.
- Define a z10 BC or z10 EC with both ICFs and other types of processors, where the ICF engines can be used to serve one or more coupling facility images, and the other types of processors can be used to run z/OS or any other operating system

For more information on the coupling facility including z/OS and CPC support for coupling facility levels, see “Coupling facility planning considerations” on page 63.

Guest coupling simulation

Guest coupling simulation is available with z/VM®.

z/VM guest coupling simulation allows you to simulate one or more complete parallel sysplexes within a single system image, providing a test environment for parallel sysplex installation. The simulated environment is not intended for production use since its single points of failure diminish the availability advantages of the parallel sysplex environment. There are no special hardware requirements – external coupling facility channels, external coupling facilities, and Sysplex Timers are neither necessary nor supported. Guest operating systems within a simulated sysplex can only be coupled (through simulated coupling facility channels) to coupling facilities also running as guests of the same z/VM system. You can have up to 32 virtual machines running z/OS within a simulated sysplex, with each z/OS virtual machine coupled to up to 8 virtual machines running as coupling facilities.

There is no system-imposed limit to the number of guest parallel sysplex environments that z/VM can simulate. However, practical limits on the number of guests that can be supported by a particular hardware configuration will also constrain the number of simulated parallel sysplex environments.

Control program support in a logical partition

Control programs require certain characteristics. Before planning or defining LP characteristics, call your installation management to determine which control programs are in use or planned for operation.

Notes:

1. Use IBM Service Link to view the appropriate PSP bucket subset ID for hardware and software maintenance information.
2. For more detailed information about support for coupling facility levels (including hardware EC, driver, and MCL numbers and software APAR numbers), see “Coupling facility level (CFLEVEL) considerations” on page 73.

z/OS

	z/OS 1.7[1,2]	z/OS 1.8	z/OS 1.9	z/OS 1.10
Support for System z10 EC	Yes	Yes	Yes	Yes
Support for System z10 BC	No	with applicable PTFs	with applicable PTFs	Yes
FICON Express8 (CHPID type FC), utilizing native FICON or Channel-To-Channel (CTC)	Yes	Yes	Yes	Yes
FICON Express8 (CHPID type FC), including High Performance FICON for System z (zHPF) single-track operations	with applicable PTFs	with applicable PTFs	with applicable PTFs	with applicable PTFs
FICON Express8 (CHPID type FC), for support of zHPF multitrack operations	No	No	with applicable PTFs	with applicable PTFs
12x InfiniBand coupling links (12x IB-SDR or 12x IB-DDR)	with applicable PTFs	with applicable PTFs	with applicable PTFs	with applicable PTFs
Long reach 1x InfiniBand coupling links (1x IB-SDR or 1x IB-DDR)	with applicable PTFs	with applicable PTFs	with applicable PTFs	with applicable PTFs

	z/OS 1.7[1 2]	z/OS 1.8	z/OS 1.9	z/OS 1.10
Secure Key Advanced Encryption Standard (AES)	No	Yes (available 11/2008)	Yes (available 11/2008)	Yes (available 11/2008)
Support for dynamically increasing the number of CPs, ICFs, IFLs, zAAPs or zIIPs without an intervening IPL	No	No	No	Yes
Large Page Support (1 megabyte pages)	No	No	with applicable PTFs	Yes
HiperDispatch	Yes	Yes	Yes	Yes
Support for CHPID type CIB for InfiniBand	with applicable PTFs	with applicable PTFs	with applicable PTFs	with applicable PTFs
Server Time Protocol	Yes	Yes	Yes	Yes
Support for zAAP	Yes	Yes	Yes	Yes
Support for zIIP	Yes	Yes	Yes	Yes
Maximum number of CPs	32	32	64	64
Maximum central storage on z10	128 GB	1 TB	1 TB	1 TB
Maximum number of channel paths	256	256	256	256
Support for multiple LCSS's	Yes	Yes	Yes	Yes
Maximum CFLEVEL supported	16 with applicable PTFs	16 with applicable PTFs	16 with applicable PTFs	16 with applicable PTFs
System-Managed CF Structure Duplexing support	Yes	Yes	Yes	Yes
Multiple subchannel sets (MSS) for ESCON® (CNC) and FICON® (FC)	Yes	Yes	Yes	Yes
OSA Express2 large send (TCP segmentation offload)	Yes	Yes	Yes	Yes
XES Coupling Facility cache structure architecture extensions for batch write, castout, and cross-invalidate functions	Yes	Yes	Yes	Yes
z/Architecture 64-bit addressing	Yes	Yes	Yes	Yes
Support for message time ordering facility (MTOF)	Yes	Yes	Yes	Yes
Support z ELC software pricing structure	Yes	Yes	Yes	Yes
Support for Crypto Express2 and Crypto Express2–1P features by the ICSF and system SSL functions	Yes	Yes	Yes	Yes
Intelligent Resource Director	Yes	Yes	Yes	Yes

	z/OS 1.7[1,2]	z/OS 1.8	z/OS 1.9	z/OS 1.10
Workload pricing	Yes	Yes	Yes	Yes
Peer mode channels (ICP, CFP, CBP)	Yes	Yes	Yes	Yes
Workload Manager (WLM) Multisystem Enclaves support	Yes	Yes	Yes	Yes
XES Coupling Facility List Structure architecture extensions for shared queues	Yes	Yes	Yes	Yes
Logical Partition time offset	Yes	Yes	Yes	Yes
Internal coupling facility channels (ICP)	Yes	Yes	Yes	Yes
System-Managed Rebuild	Yes	Yes	Yes	Yes

Notes:

1. For z10 BC: z/OS R1.7 + zIIP Web Deliverable required for z10 to enable HiperDispatch on z10 (does not require a zIIP). z/OS V1.7 support was withdrawn September 30, 2008. The Lifecycle Extension for z/OS V1.7 (5637-A01) makes fee-based corrective service for z/OS V1.7 available through September 2009. With this Lifecycle Extension, z/OS V1.7 supports the z10 BC server. Certain functions and features of the z10 BC server require later releases of z/OS. For a complete list of software support, see the PSP buckets and the Software Requirements section of the System z10 BC announcement letter, dated October 21, 2008.
2. For z10 EC: z/OS R1.7 + zIIP Web Deliverable required for z10 to enable HiperDispatch on z10 (does not require a zIIP). z/OS V1.7 support was withdrawn September 30, 2008. The Lifecycle Extension for z/OS V1.7 (5637-A01) makes fee-based corrective service for z/OS V1.7 available through September 2009. With this Lifecycle Extension, z/OS V1.7 supports the z10 EC server after its end of support date. Certain functions and features of the z10 EC server require later releases of z/OS. For a complete list of software support, see the PSP buckets and the Software Requirements section of the System z10 EC announcement letter, dated October 21, 2008.

z/VM

	z/VM 5.3	z/VM 5.4
Support for System z10 EC	Yes	Yes
Support for System z10 BC	with applicable PTFs	Yes
FICON Express8 (CHPID type FC), utilizing native FICON or Channel-To-Channel (CTC)	Yes	Yes
FICON Express8 (CHPID type FCP) for support of SCSI devices	Yes	Yes
12x InfiniBand coupling links (12x IB-SDR or 12x IB-DDR)	To define, modify, and delete an InfiniBand coupling link, CHPID type CIB, when z/VM is the controlling LPAR for dynamic I/O	To define, modify, and delete an InfiniBand coupling link, CHPID type CIB, when z/VM is the controlling LPAR for dynamic I/O

	z/VM 5.3	z/VM 5.4
Long reach 1x InfiniBand coupling links (1x IB-SDR or 1x IB-DDR)	To define, modify, and delete an InfiniBand coupling link, CHPID type CIB, when z/VM is the controlling LPAR for dynamic I/O	To define, modify, and delete an InfiniBand coupling link, CHPID type CIB, when z/VM is the controlling LPAR for dynamic I/O
Secure Key Advanced Encryption Standard (AES)	for guest exploitation	for guest exploitation
Support for z/VM-mode partition	No	Yes
Support for dynamic add of Reserved Central Storage	No	Yes
Support for z/VM Systems Management from the HMC	Yes	Yes
Support for installing Linux from the HMC	No	Yes
Dedicated OSA port to an operating system	Yes	Yes
z/VM integrated systems management	Yes	Yes
zIIP and zAAP Simulation on CPs	Yes	Yes
Support for zIIP	Yes	Yes
Support for zAAP	Yes	Yes
Maximum number of CPs	32	32
Maximum central storage	256 GB	256 GB
Maximum expanded storage	128 GB	128 GB
Maximum number of channel paths	256	256
Maximum CFLEVEL supported	16 for guest exploitation	16 for guest exploitation
Able to use IFLs for OpenSolaris workloads	Yes	Yes
Able to use IFLs for Linux workloads	Yes	Yes
System-managed Coupling Facility structure duplexing, for z/OS guests	Yes	Yes
CHPID type OSA performance enhancements, for z/OS guests	Yes	Yes
CHPID type FCP performance enhancements	Yes	Yes
Crypto Express2 and Crypto Express2-1P feature (guest use)	Yes	Yes
FICON Express4-2C SX on the z9™ BC	Yes	Yes
Hardware Decimal Floating Point facilities	Yes	Yes
Support for z9 BC and z9 EC	Yes	Yes
Support for FICON Express2 (CHPID type FC), including Channel-to-Channel (CTC)	Yes	Yes
Support for FICON Express2 (CHPID type FCP), for native support of SCSI disks	Yes	Yes
z/Architecture 64-bit addressing	Yes	Yes
Peer mode channels (ICP, CFP, CBP)	Yes	Yes
Guest Coupling simulation	Yes	Yes

	z/VM 5.3	z/VM 5.4
Dynamic I/O configuration support through the CP configurability function	Yes	Yes
Subspace group facility (guest use)	Yes	Yes
Performance assist via pass-through of adapter I/O operations and interruptions for CHPID types FCP, IQD, and OSD	Yes	Yes

z/VSE

	z/VSE 3.1	z/VSE 4.1	z/VSE 4.2
Support for System z10 EC	Yes	Yes	Yes
Support for System z10 BC	with applicable PTFs	with applicable PTFs	Yes
FICON Express8 (CHPID type FC), utilizing native FICON or Channel-To-Channel (CTC)	Yes	Yes	Yes
FICON Express8 (CHPID type FCP) for support of SCSI devices	Yes	Yes	Yes
z/Architecture mode only and 64-bit real addressing	No	Yes	Yes
ESA/390	Yes	No	No
31-bit addressing	Yes	Yes	Yes
Maximum central storage	2 GB	8 GB	32 GB
OSA-Express3 family	Yes	Yes	Yes
OSA-Express2 family	Yes	Yes	Yes
Support for FICON Express2 (CPHID type FC), including Channel-To-Channel (CTC)	Yes	Yes	Yes
Support for FICON Express2 (CHPID type FCP) for native support of SCSI disks	Yes	Yes	Yes
Support for FICON Express4 (CPHID type FC), including Channel-To-Channel (CTC)	Yes	Yes	Yes
Support for FICON Express4 (CHPID type FCP) for native support of SCSI disks	Yes	Yes	Yes
CHPID type FCP performance enhancements	Yes	Yes	Yes
CP Assist for Cryptographic Function (CPACF)	Yes	Yes	Yes
Configurable Crypto Express2 and Crypto Express2-1P (z10 BC only) (z/VSE offers support for clear-key SSL transactions only)	Yes	Yes	Yes
Features supported by z/VSE carried forward from IBM System z9	Yes	Yes	Yes

TPF (Transaction Processing Facility)

	TPF 4.1	z/TPF 1.1
Support for System z10 EC	Yes	Yes
Support for System z10 BC	Yes	Required to support 64 engines per z/TPF LPAR
FICON Express8 (CHPID type FC), utilizing native FICON or Channel-To-Channel (CTC)	with PUT 16	Yes
Crypto Express2 (EC and BC) and Crypto Express2-1P (BC only)	No	Acceleration mode only
Support for FICON Express2 (CHPID type FC), including Channel-to-Channel (CTC)	Yes	Yes
ESA/390 or ESA/390 TPF mode	Yes	Yes
Maximum number of CPs (either shared or dedicated LP)	16	64
Maximum central storage	2048 MB	1 TB
Maximum CFLEVEL supported	9 (with APAR support)	9 (with APAR support)
Maximum number of channel paths	256	256

Linux on System z

	Linux for S/390
Support for System z10 EC	Yes
Support for System z10 BC	Yes
FICON Express8 (CHPID type FC), utilizing native FICON or Channel-To-Channel (CTC)	Yes
FICON Express8 (CHPID type FCP) for support of SCSI devices	Yes
Crypto Express2 and Crypto Express2-1P configured as an accelerator	Yes
Secure Key support on Crypto Express2 and Crypto Express2-1P when using Linux Versions SUSE SP Level 10 or Red Hat Rel 5	Yes
Support for FICON Express2 (CHPID type FC), including Channel-To-Channel (CTC)	Yes
Support for FICON Express2 (CHPID type FCP) for support of SCSI disks	Yes
OSA Express2 large send (also called TCP segmentation offload)	Yes
Linux-Only mode	Yes
Maximum number of CPs	16
Maximum central storage	2048 MB
Maximum expanded storage	262144 MB
Maximum number of channel paths	256
PKCS #11 API support	Yes
WLM Management of shared logical processors	Yes

	Linux for S/390
Performance assist via passthrough of adapter interruptions for FCP, IQD, and OSD CHPID types	Yes
Support for SSL clear key RSA operations	Yes

Hardware Configuration Definition (HCD)

You can use HCD's interactive panels to define configuration information both to the CPC and to the operating system.

Note: HCD and Hardware Configuration Manager (HCM) are also available on z/VM.

HCD, running on z/OS allows you to dynamically change the current I/O configuration of the CPC. HCD allows you to dynamically change the current I/O configuration of the operating system and to create a new IOCDS and make it the active IOCDS.

HCD is required to define the I/O configuration to the operating system. HCD is also the recommended way to define hardware configurations.

The HCD component of z/OS allows you to define the hardware and software I/O configuration information necessary for a parallel sysplex solution environment, including the capability to define:

- peer-mode channel paths (CFP, CBP, CIB, and ICP) to connect z/OS systems to coupling facility images, and
- peer-mode channel paths (CFP, CBP, CIB, and ICP) to connect coupling facility images to one another, in support of System-Managed CF Structure Duplexing.

In addition to these two uses, the external coupling links (CFP, CBP, CIB) also support STP timing signals

Additionally, HCD allows you to remotely write IOCDSs from one Support Element CPC to another Support Element CPC as long as both Support Elements are powered-on, LAN-attached, enabled for remote licensed internal code (LIC) update, and defined to the same Hardware Management Console.

Dynamic I/O configuration does ***not*** support the following:

- Adding or deleting LPs
- Changing MIF image ID numbers (the MIF image ID number is different from the LP identifier [ID])

When using HCD in z/OS, you can define and control the configuration of the CPC affecting all LPs. Those LPs that run with HCD or z/VM can dynamically change their software configuration definitions. Other LPs may require an IPL in order to use the new configuration.

When you use HCD you must install, in the LP, the appropriate version of IOCP. Throughout the remainder of this publication, all the capabilities or restrictions documented regarding the IOCP program, also apply to definitions entered and controlled through HCD.

For more information about dynamic I/O configuration on z/OS see:

- *z/OS Hardware Configuration Definition Planning*, GA22-7525

- *z/OS Hardware Configuration Definition: User's Guide*, SC33-7988

z/VM dynamic I/O configuration

You can dynamically change the current I/O configuration of the CPC. You can also change the current I/O configuration of the operating system and create a new IOCDS and make it the active IOCDS.

Dynamic I/O configuration does ***not*** support the following:
- Adding or deleting LPs
- Changing MIF image ID numbers (the MIF image ID number is different from the LP identifier [ID])

You can define and control the configuration of the CPC affecting all LPs. Those LPs that run z/VM can dynamically change their software configuration definitions.

Input/Output Configuration Program (IOCP) support

To perform a power-on reset you must use an LPAR IOCDS. To generate an LPAR IOCDS you need to use the ICPIOCP program.

PTFs for supported IOCP versions must be applied and can be obtained from the IBM Software Support Center. For more information on ICPIOCP, see *System z Input/Output Configuration Program User's Guide for ICP IOCP*, SB10-7037.

Hardware support

LPs operate independently but can share access to I/O devices and CPC resources. Each active LP must have sufficient channel paths and storage to meet the particular requirements of that LP. Additional central storage, expanded storage, channel paths, consoles, and other I/O devices might be necessary for the planned configuration of LPs.

Operator training

A general knowledge of z/Architecture and ESA/390 is useful and, in some cases, required of all technical support personnel, LPAR planners, and operators.

Generally, the operator performs the following tasks:
- Edit activation profiles
  - Reset profiles
    - Select an IOCDS
    - Optionally specify LP activation sequence
  - Image profiles
    - Define LP characteristics
    - Optional automatic load specification
  - Load profiles
- Performing a CPC activation
- Activating an LP
- Performing a load on an LP or activating a load profile
- Deactivating a CPC
- Deactivating an LP

Logical partitions

This section provides an overview of LP characteristics. Some of the characteristics described in this section are model-dependent, EC-level dependent, MCL-dependent, LP mode dependent, or control-program dependent. For this reason, all of the characteristics described here are not necessarily available on all CPCs.

The resources of a CPC can be distributed among multiple control programs that can run on the same CPC simultaneously. Each control program has the use of resources defined to the logical partition in which it runs.

You can define an LP to include:
- One or more CPs
- Central storage
- Channel paths
- Optional expanded storage
- One or more optional Crypto Express2 Coprocessors or Crypto Express2 Accelerators

An LP can be defined to include CPs, zAAPs, and zIIPs, ICFs, and/or IFLs. The allowed combinations of defined processor types for an LP depends on the defined mode of the logical partition. Refer to Table 17 on page 153.

You can also define an LP to be a coupling facility running the coupling facility control code.

Characteristics

LPs can have the following characteristics. For more information or details about exceptions to any of the characteristics described below, see “Determining the characteristics” on page 99.

- The maximum number of LPs you can define on a z10 EC is 60 (and 30 LPs on a z10 BC).
- LPs can operate in ESA/390, ESA/390 TPF, Linux-Only, z/VM, or coupling facility mode.
- The storage for each LP is isolated. Central storage and expanded storage cannot be shared by LPs.
- Using dynamic storage reconfiguration, an LP can release storage or attach storage to its configuration that is released by another LP.
- All channel paths can be defined as reconfigurable. Channel paths are assigned to LPs. You can move reconfigurable channel paths between LPs using tasks available from either the Hardware Management Console or the Support Element console. If the control program running in the LP supports physical channel path reconfiguration, channel paths can be moved among LPs by control program commands without disruption to the activity of the control program.
- MIF allows channel paths to be shared by two or more LPs at the same time. All CHPID types **except** CVC and CBY can be shared.
- With a non-E64 model, the maximum number of CPs that can be defined is 56. However the total number of logical processors that can be defined is 64. For example, one could specify 8 initial CPs, 48 reserved CPs, and 8 reserved zAAPs. For a Model E64, the maximum number of CPs that can be defined is 64.

CPs can be dedicated to LPs or shared by them. CPs that you define as dedicated to an LP are not available to perform work for other active LPs. The resources of shared CPs are allocated to active LPs as needed. You can cap (limit) CP resources, if required. A CP LP has a maximum of 16 processors (ICFs or CPs), regardless of the model.

You cannot define a mix of shared and dedicated CPs for a single LP. CPs for an LP are either all dedicated or all shared. However, you can define a mix of LPs with shared CPs and LPs with dedicated CPs and activate them concurrently.

For security purposes, you can:

– Reserve reconfigurable channel paths for the exclusive use of an LP (unless overridden by the operator)
– Limit the authority of an LP to read or write any IOCDS in the configuration and limit the authority of an LP to change the I/O configuration dynamically
– Limit the authority of an LP to retrieve global performance data for all LPs in the configuration
– Limit the authority of an LP to issue certain control program instructions that affect other LPs

Figure 1 shows some of the characteristics that can be defined for an LP. You can view each LP as a CPC operating within the physical CPC.

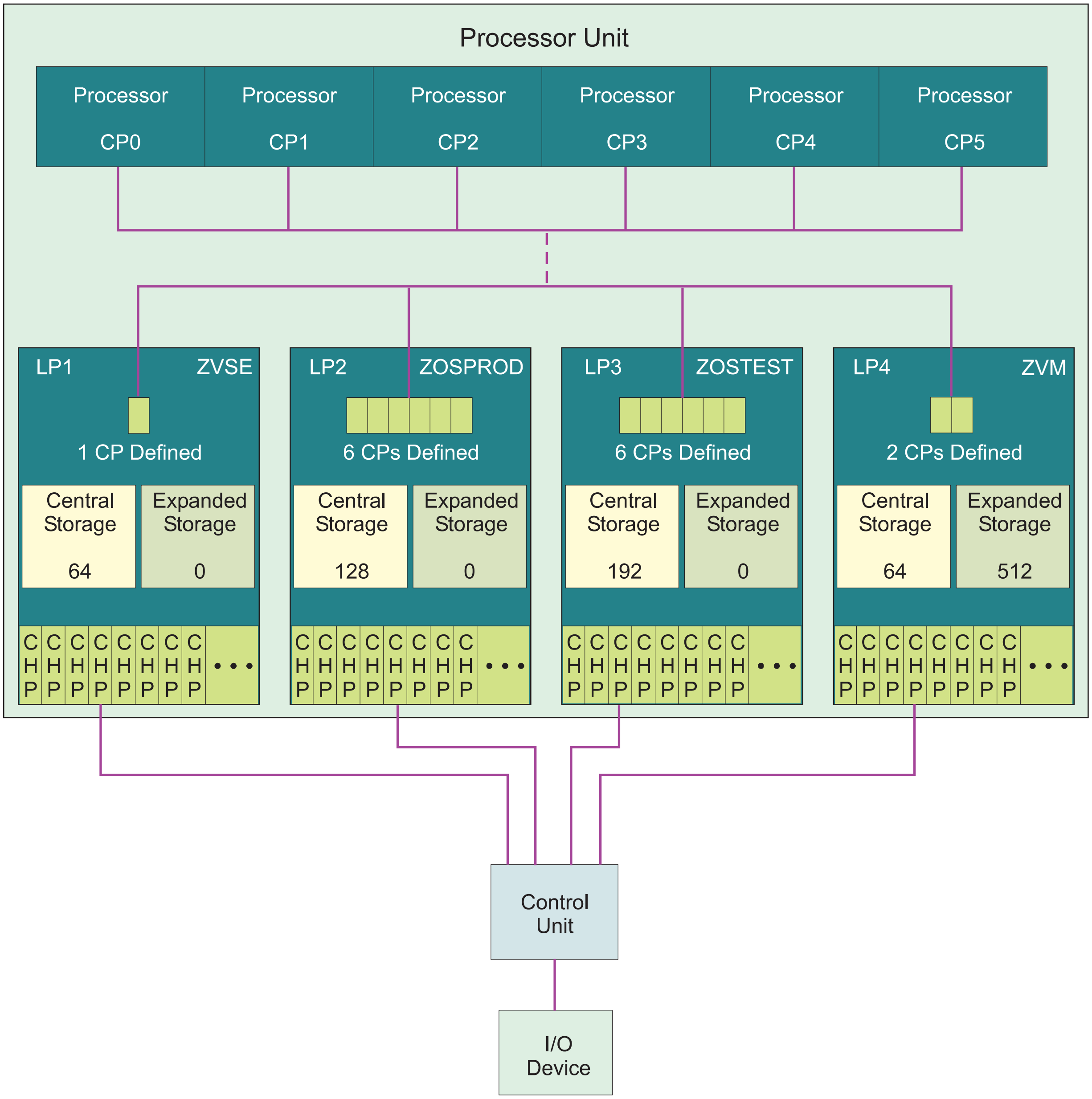


Figure 1. Characteristics of logical partitions

Potential applications

The use of LPs allows multiple systems, including the I/O for the systems, to be migrated to a single CPC while maintaining the I/O performance, recovery, and multipathing capability of each system, and with minimum impact to the system generation procedures.

LPs are suitable for consideration in the following environments:

Consolidation
Multiple production system images can be consolidated onto 1 CPC without having to merge them into one image.

Migration
Control programs or applications can be migrated by running the old and new systems or applications in independent LPs that are active on the same CPC at the same time.

Production and test
Multiple production and test systems can run on the same CPC at the same time.

Coupling facility
A coupling facility enables high performance, high integrity data sharing for those CPCs attached to it and configured in a sysplex.

Coupled systems
Multiple instances of the same workload can be run in multiple LPs on one or more CPCs as part of a sysplex configuration that takes advantage of the centrally accessible, high performance data sharing function provided by the coupling facility.

Extended Recovery Facility (XRF)
Primary and alternate XRF systems can run on 1 CPC. Multiple and alternate XRF systems can run on 1 CPC.

Communications Management Configuration (CMC)
The communications management configuration (CMC) machine, usually run on a separate CPC, can be run as an LP on the same CPC.

Departmental systems
Multiple applications can be isolated from one another by running each in a separate LP.

Constrained systems
Those systems that cannot fully use a large system because of storage constraints can alleviate the problem by using LPs to define multiple system images on the same CPC.

Diverse workloads
Interactive workloads such as the Customer Information Control System (CICS®) and time-sharing option (TSO) can be isolated by running each in a separate LP.

Examples of logical partition applications

Figure 2 and Figure 3 show examples of how LPs on a CPC can be used to support multiple systems.

Figure 2 represents the migration of two z/OS, one z/VM and one stand-alone coupling facility systems onto a single CPC. These systems, which were running on four separate IBM z900 CPCs, now operate as four LPs on a single z10 EC. Two LPs are each running a z/OS system in ESA/390 mode, one is running a z/VM system in ESA/390 mode, and one is running in coupling facility mode.

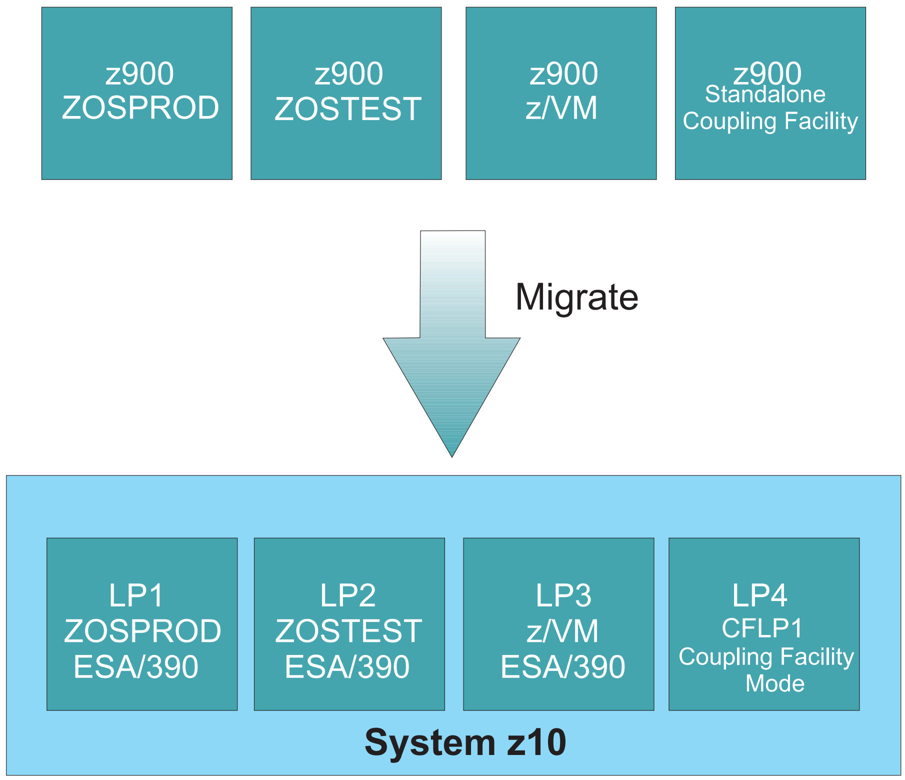


Figure 2. Migration of four production systems to LPs

Figure 3 represents a CPC with three LPs: an active XRF system, an alternate XRF system, and an alternate for another primary XRF system.

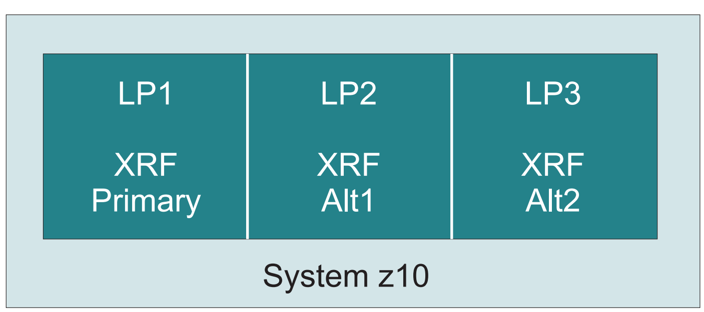


Figure 3. Support for three XRF systems

Compatibility and migration considerations

This section provides migration and compatibility information for the System z10.

Device numbers

When multiple systems are migrated to a System z10 CPC, the combination of systems could include different devices or shared devices with identical device numbers. Each system can operate in an LP without changing the device numbers as long as identical device numbers do not occur in the same LP. However, duplicate device numbers can exist in the same LP if these device numbers are in different subchannel sets.

Duplicate device number conflicts can occur when the I/O configuration is reconfigured. For example, if a reconfigurable channel path is reassigned to another LP and devices attached to the channel path have device numbers that are already assigned in the receiving LP to other online channel paths, a conflict results. When IOCP generates an LPAR IOCDS, the initial configuration contains no duplicate device number conflicts in an LP.

Device number conflicts are also detected when operator tasks change the I/O configuration (channel path tasks from the Hardware Management Console or Support Element console; or control program configuration command) or during LP activation.

Duplicate device number conflicts are also detected when a dynamic I/O configuration change is made.

Multiple Subchannel Sets (MSS)

Multiple Subchannel Sets (MSS) allow increased device connectivity for Parallel Access Volumes (PAVs). Two subchannel sets per Logical Channel Subsystem (LCSS) are designed to enable a total of 63.75K subchannels in set-0 and the addition of 64K-1 subchannels in set-1. MSS is supported by ESCON (CHPID type CNC), FICON when configured as CHPID type FC, and z/OS.

Control programs

PTFs for supported control programs must be applied and can be obtained from the IBM Software Support Center. A supported control program operates in an LP as it does in one of the basic modes, with the following exceptions:

z/OS

- Physical reconfiguration, either offline or online, of CPs is not supported on the System z10. Logical CP reconfiguration, either offline or online, is supported in an LP. This does not affect the online/offline status of the physical CPs. To reconfigure a logical CP offline or online, use the following z/OS operator command:

  ```
  CF CPU(x),<OFFLINE/ONLINE>
  ```

- Physical reconfiguration, either offline or online, of central and expanded storage is supported.

  To reconfigure a central storage element offline or online, use the following z/OS operator command:

  ```
  CF STOR(E=1),<OFFLINE/ONLINE>
  ```

  Additionally you can use the following command to reconfigure smaller amounts of central storage online or offline:

```
CF STOR(nnM),<OFFLINE/ONLINE>
```

Reconfigurable Storage Unit (RSU) Considerations: The RSU parameter should be set to the same value that you specified in the central storage Reserved field. See *z/OS MVS Initialization and Tuning Reference* for appropriate RSU parameter syntax.

- Reconfiguration, either offline or online, of channel paths by z/OS operator commands is supported on a System z10. This capability also allows channel paths to be moved among LPs using z/OS operator commands.
- Preferred paths to a device are supported on a System z10. If the preferred path parameter is specified in an LPAR IOCDS, it is accepted.
- Specifying SHAREDUP for devices is not recommended. If used, z/OS treats the device as a SHARED device.
- Each z/OS LP can run the Resource Measurement Facility (RMF). RMF enhancements for PR/SM allow a single LP to record system activities and report them in the Partition Data Report. To enable this, use the Change LPAR Security task available from the CPC Operational Customization task list and select Performance Data Control for the LP.

  For z/OS, RMF reporting includes LPAR Management Time.
- RMF provides enhanced reporting for coupling facility configurations.
- RMF with APAR support identifies which logical and physical CPs are of each type when any combination of general purpose, zAAP, IFL, zIIP and ICF processors are present in the configuration on its partition data report. You can have up to 32 virtual machines running z/OS within a simulated sysplex, with each z/OS virtual machine coupled to up to 8 virtual machines running as coupling facilities

EREP

Each control program operating in an LP has its own environmental recording, editing, and printing (EREP) processing. EREP records for ICP channel paths go to the z/OS logs of the z/OS systems attached to a coupling facility LP.

CPU IDs and CPU addresses

Application packages and software products that are licensed to run under specific CPU identification (CPU ID) information should be checked because they may need to be updated.

CPU ID information is system-generated for each logical CP in the LP during the LP activation. It consists of a version code for the CPC machine type, a CPU identification number that is unique for each logical partition, a model number for the CPC machine type, and a value of X'8000'.

The Store CPU ID (STIDP) instruction stores the CPU ID for each logical CP in storage in the following format (Figure 4):

0 7	8 31	32 47	48 63
Version Code	CPU Identification Number	Machine Type	8000

Figure 4. CPU ID format

Figure 5 shows the format of the CPU identification number (bits 8 through 31 of the CPU ID format).

PPnnnn

Legend :

P Logical partition identifier
n Digit derived from the serial number

Figure 5. CPU identification number format

CPU ID fields

The CPU identification number, with the version code and the machine type, permits a unique CPU ID for each logical partition.

- The **version code** for the System z10 is always zero and is not affected by the operating mode.
- The **CPU identification number** for each logical CP (see Figure 5) consists of a two-digit LP identifier, and digits derived from the serial number of the CPC.
  - The **logical partition identifier** is specified using the Partition identifier field on the General page in either the reset or image profile used by the LP and must be unique for each active LP in the configuration.
- The following machine types (CPC model numbers) are returned as indicated below:

Machine type	Models
2097	**System z10 EC** (E12, E26, E40, E56, E64)
2098	**System z10 BC** (E10)

Note: STIDP is provided for purposes of backward compatibility. IBM highly recommends that the Store System Information instruction (STSI) be used rather than STIDP. STSI is the preferred means to obtain all CPU information including machine serial number. When a unique logical CPU address is all that is required, use the Store CPU Address (STAP) instruction.

Examples of CPU ID information

The following examples show the format and contents of the CPU ID information stored by the STIDP instruction for logical CPs in active LPs.

Table 2 shows the CPU ID information for a z10 EC with 3 active LPs.

Table 2. CPU IDs for a z10 EC

LP name	LP identifier	Number of CPs defined	CPU ID returned by STIDP
ZVSE	1	1	00 019999 2097 8000
ZOSTEST	2	1	00 029999 2097 8000
ZOSPROD	3	8	00 039999 2097 8000 00 039999 2097 8000 00 039999 2097 8000 00 039999 2097 8000 00 039999 2097 8000 00 039999 2097 8000 00 039999 2097 8000 00 039999 2097 8000

HSA allocation

z10 EC has a fixed Hardware System Area (HSA) size of 16 GB. The z10 BC has a fixed HSA size of 8 GB.

TOD clock processing

The CPC TOD clocks of all the CPs are automatically set during CPC activation. The time reference used depends on whether or not a Sysplex Timer® is attached to the CPC or Server Time Protocol (STP) is enabled. When STP is enabled, a CPC can participate in: an ETR network, a Mixed Coordinated Timing Network (CTN), or an STP-only CTN. In an ETR network or Mixed CTN, the Sysplex Timer provides the timekeeping information. In an STP-only CTN, the Sysplex Timer is no longer required. In this case the Current Time Server for the STP-only CTN provides the time information.

No sysplex timer attached and Server Time Protocol not enabled

During PR/SM initialization, the CPC TOD clocks for each CP are set to the TOD value of the Support Element. Each LP starts out with this CPC TOD value at the completion of LP activation. The operating system running in an LP can set a TOD value for itself and this will be the only TOD reference it will see. Setting the TOD clock for one logical CP in the LP sets the TOD clock for all logical CPs in that LP, but does not affect the logical CPs in any other LP. The TOD clock value is used for the duration of the LP activation, or until a subsequent Set Clock instruction is issued in the LP.

Sysplex timer attached

The attachment and use of an IBM Sysplex Timer is supported. Also, during PR/SM initialization, when a Sysplex Timer is attached, the CPC TOD clocks for each CP are set to the TOD value from the Sysplex Timer.

The operating system in each LP can independently choose whether or not to synchronize to the Sysplex timer if one is present. Operating systems in LPs that do synchronize to the Sysplex Timer will all be running with identical TOD values. Operating systems in LPs that do not synchronize to the Sysplex Timer do not need to be aware of the presence of a Sysplex Timer and can set their TOD values independently of all other LPs.

Note that z/OS does not allow you to change the value of the TOD setting when it is using the Sysplex Timer (ETRMODE=YES in the CLOCKxx parmlib member).

The System z10 models support the specification of a logical partition time offset. When all members of a sysplex are in logical partitions on these supported models, the Logical partition time offset can be used for:

- Different local time zone support in multiple sysplexes using the same sysplex timer. Many sysplexes have the requirement to run with a LOCAL=GMT setting in a sysplex (ETRMODE=YES) where the time returned from a Store Clock instruction yields local time. To do this, the time returned by the sysplex timer must be local time. Prior to Logical partition time offset support, this could only be accomplished for one sysplex for a given sysplex timer. With Logical partition time offset support, multiple sysplexes can each have their own local time reported to them from the sysplex timer if desired. For instance, the sysplex timer can be set to GMT, one set of sysplex partitions could specify a Logical partition time offset of minus 5 hours, and a second set of sysplex partitions could specify a Logical partition time offset of minus 6 hours.

Server Time Protocol enabled

The enablement of STP is supported. Also, during PR/SM initialization, when STP is enabled, the CPC TOD clocks for each CP are set to the TOD value from STP.

The operating system in each LP can independently choose whether or not to synchronize to the current time source for STP, if present. Operating systems in LPs that do synchronize to STP will all be running with identical TOD values. Operating systems in LPs that do not synchronize to STP do not need to be aware of the presence of STP and can set their TOD values independently of all other LPs.

Note that z/OS does not allow you to change the value of the TOD setting when synchronized to STP (STPMODE=YES in the CLOCKxx parmlib member).

The System z10 models support the specification of a logical partition time offset. When all members of a sysplex are in logical partitions on these supported models, the Logical partition time offset can be used for:

- Different local time zone support in multiple sysplexes using the same CTN. Many sysplexes have the requirement to run with a LOCAL=GMT setting in a sysplex (STPMODE=YES) where the time returned from a Store Clock instruction yields local time. To do this, the time returned by STP must be local time. With Logical partition time offset support, multiple sysplexes can each have their own local time reported to them from STP if desired. For instance, STP can be set to GMT, one set of sysplex partitions could specify a Logical partition time offset of minus 5 hours, and a second set of sysplex partitions could specify a Logical partition time offset of minus 6 hours.

External coupling links (i.e. CFP, CBP, CIB) are also valid to pass time synchronization signals for Server Time Protocol (STP). Therefore the same coupling links can be used to exchange timekeeping information and Coupling Facility messages in a Parallel Sysplex.

Sysplex testing without a Sysplex Timer and Server Time Protocol not enabled

You can do sysplex testing without a Sysplex Timer or Server Time Protocol enabled by setting up a test sysplex of several z/OS LPs in multiple LPs in the same PR/SM LPAR configuration. Use the SIMETRID keyword in the CLOCKxx parmlib member for z/OS to synchronize the members of the sysplex in the LPs.

Synchronized Time Source and the coupling facility

Improved processor and coupling facility link technologies inherent on System z10 models necessitate more rigorous time synchronization tolerance for members of a parallel sysplex hosted by those models. To help ensure that any exchanges of time-stamped information between members of a sysplex observe the correct time ordering, time stamps are now included in the message-transfer protocol between the systems and the coupling facility.

Consequently, a coupling facility hosted by any System z10 model requires connectivity to the same synchronized time source as the other z/OS systems in its parallel sysplex. If a member of its parallel sysplex is on the same server as the coupling facility, required connectivity is already provided to the synchronized time source. However, when a coupling facility is a resident of a System z10 model, which **does not** include a member of the coupling facilities parallel sysplex, connectivity attached to the synchronized time source must be implemented.

Extended TOD-clock facility

The extended TOD-clock facility provides an extended form TOD clock and a TOD programmable register. The extended form TOD clock is a 128-bit value that extends the current basic form by appending 8 bits on the left and 56 bits on the right. The extended form TOD clock is returned by a new problem-program instruction, STORE CLOCK EXTENDED (STCKE). The contents of the TOD programmable register are stored into the rightmost portion of the extended form TOD value when the TOD clock is inspected by STCKE. A TOD programmable register exists for each CPU and contains the TOD programmable field in bits 16-31. The TOD programmable register is set by a new privileged instruction, SET TOD PROGRAMMABLE FIELD (SCKPF). The leftmost byte of the extended form TOD clock is the TOD Epoch Index (TEX), and is stored as zeros in machines running ESA/390.

The extended TOD clock facility satisfies three main objectives:

- Relieve constraints that exist in the current 64-bit TOD clock
- Extend the TOD-clock architecture to multi-system configurations
- Help ensure sysplex-wide uniqueness of the STCKE TOD values

The TOD Programmable Field (TODPF) is a 16-bit quantity contained in bit positions 16-31 of the TOD programmable register. The contents of the register can be set by the privileged instruction SET TOD PROGRAMMABLE FIELD. The contents of the register can be stored by the instruction STORE CLOCK EXTENDED, which stores the TOD programmable field in the last 16 bits of the extended form TOD clock. The contents of the register are reset to a value of all zeros by an initial CPU reset.

Clock Comparator on Shared Processors

The clock comparator has the same format as bits 0-63 of the TOD clock. The clock comparator nominally consists of bits 0-47, which are compared with the corresponding bits of the TOD clock. On some models, higher resolution is obtained by providing more than 48 bits. In most cases, a logical processor running in a logical partition will receive the model's resolution for the clock comparator.

However, when using shared logical processors in a logical partition, if the operating system running in a logical partition loads an enabled wait state with a clock comparator set on that logical processor, the LPAR Hipervisor will track that clock comparator value for the logical partition's processor at a less granular resolution. The granularity may be reduced to as little as bits 0-45 of the intended clock comparator value. This effect is not seen on dedicated logical processors nor is it seen on logical processors that are not in wait state.

Chapter 2. Planning considerations

Overview

This chapter describes planning considerations for I/O configuration and for coupling facility LPs.

Planning the I/O configuration

This section describes the planning considerations and guidelines for creating an IOCDS. It assumes you understand the IOCP configuration and coding requirements described in the *System z Input/Output Configuration Program User's Guide for ICP IOCP*, SB10-7037.

Planning considerations

PR/SM is standard on all System z10 models.

Control program support

The maximum number of supported devices is limited by the control program. In planning an I/O configuration, installation management should be aware of the maximum number of devices supported by the control program run in each LP. Please see the user's guide for the respective operating systems.

Hardware Configuration Definition (HCD) support

HCD supports definition of the I/O configuration for an entire installation. It is required for parallel sysplex and LPAR clusters. A single I/O data file is created for the installation and used for multiple machines and I/O configuration data sets.

HCD supports:

- Up to 60 logical partitions (LPs) per central processing complex (CPC) on a z10 EC, or 30 logical partitions on a z10 BC.
- Coupling facility configurations
- Multiple Image Facility (MIF)
- Dynamic CHPID Management (DCM) channel paths.
- MCSS
- Assigning reserved logical partitions a meaningful name

Table 3. HCD function support

HCD Function	z/OS	z/VM
Define 60 logical partitions?	Yes	Yes
Define shared channel paths?	Yes	Yes
Define coupling facility channel paths?	Yes	Yes[2]
Define dynamically managed channel paths?	Yes	Yes[2]
Write IOCDSs remotely?	Yes[1]	No
Access I/O devices on shared channel paths?	Yes	Yes
Use software-only dynamic I/O?	Yes	Yes

Table 3. HCD function support (continued)

HCD Function	z/OS	z/VM
Notes: 1. HCD, running on z/OS allows you to remotely write IOCDSs from one CPC to another CPC that is powered on, LAN-attached, enabled for remote LIC update, and defined to the same Hardware Management Console. 2. HCD, running on z/VM, allows you to define coupling facility channel paths or managed channel paths for a z/OS LP but z/VM does not support coupling facility channel paths or dynamically managed channel paths for use by z/VM or guest operating systems.		

For more information on using HCD with Multiple Image Facility, see
- *z/OS Hardware Configuration Definition: User's Guide*, SC33-7988
- *z/OS Hardware Configuration Definition Planning*, GA22-7525
- *z/VM I/O Configuration*, SC24-6100.

z/VM Dynamic I/O configuration support

z/VM support for the coupling facility: z/VM allows you to define configurations that use the coupling facility. However, z/VM does ***not*** support the coupling facility itself. Instead, z/VM's dynamic I/O configuration capability allows you to define resources that can be used by a z/OS system in another LP. For a summary of z/VM's support of dynamic I/O configuration, see Table 4.

z/VM support for the Multiple Image Facility (MIF): You can use z/VM to define shared channel paths. For a summary of z/VM support of dynamic I/O configuration, see Table 4.

Table 4. z/VM dynamic I/O support for MIF and the coupling facility

	Release
z/VM Function	**5.3, 5.4**
Define shared channel paths?	Yes
Define coupling facility channel paths?	Yes (Note)
Write IOCDSs remotely?	No
Access I/O devices on shared channel paths?	Yes
Use software-only dynamic I/O?	Yes
Use hardware and software dynamic I/O?	Yes
Use shared ESCON CTCs?	Yes
Note: z/VM can define coupling facility channel paths for a z/OS LP but does ***not*** support real coupling facility channel paths for use by z/VM or guest operating systems.	

Input/Output Configuration Program (IOCP) support

You can create up to four IOCDSs. ICP IOCP is the required supported version. You can define as many as 60 LPs. For more information on ICP IOCP, see *System z Input/Output Configuration Program User's Guide for ICP IOCP*, SB10-7037.

Characteristics of an IOCDS

The definitions for channel paths, control units, and I/O devices are processed by the IOCP and stored in an IOCDS. During initialization of the CPC, the definitions of a selected IOCDS are transferred to the hardware system area (HSA). The IOCDS is used to define the I/O configuration data required by the CPC to control I/O requests.

Channel paths in an IOCDS are assigned to one or more LPs. The characteristics of an IOCDS are:

- Using the IOCP RESOURCE statement, you define logical channel subsystems (CSSs) and the logical partitions that have access to the channel paths in a CSS.
- Using the IOCP RESOURCE statement, you can name logical partitions and assign MIF image ID numbers to them. MIF image ID numbers are necessary for ESCON CTC and FICON CTC definitions.
- Using the IOCP CHPID statement, you can assign a channel path as reconfigurable or shared.
- Using the IOCP CHPID statement, you can specify a Dynamic CHPID Management (DCM) channel path and the cluster to which the CHPID belongs. The CHPID is shareable among active LPs that have become members of the specified cluster.
- You can duplicate device numbers within a single IOCP input file, but the device numbers cannot be duplicated within an LP. See “IOCP coding specifications” on page 52.

Maximum number of logical partitions

The maximum number of LPs supported by z10 EC is 60. The z10 BC supports a maximum of 30 LPs.

Determining the size of the I/O configuration

To determine the size of the current I/O configuration (number of control unit headers and devices), review the IOCDS Totals Report for the current IOCDS.

Maximum size of the I/O configuration

Limits within an I/O configuration exist for the following:

- Devices
- Control unit headers
- Physical control units

System z10 models:

- The maximum number of control unit headers (CUHs) is 4096 per logical channel subsystem (CSS).
- The maximum number of physical control units is 8192.
- The maximum number of devices is 65280 per CSS for subchannel set 0.
- The maximum number of devices is 65535 per CSS for subchannel set 1.

Guidelines for setting up the I/O configuration

Follow these guidelines when setting up an I/O configuration.

1. Determine the number of LPs and in which logical channel subsystem (CSS) they should exist.
2. For dynamic I/O configurations, include any logical partitions for which you do not yet have a meaningful name. These logical partitions will be reserved until a subsequent dynamic I/O configuration change is made to assign them a name.
3. Determine if you want to move any channel paths among LPs. If you do, then these channel paths must be defined as reconfigurable in the IOCP CHPID statement. You cannot move a channel path from an LP in one CSS to an LP in another CSS.

4. Determine if you want to share any channel paths among LPs in the same CSS. If you do, then specify these channel paths as SHARED in the IOCP CHPID statement. Doing this, helps reduce the number of channel paths configured to a physical control unit and device. Make sure that the channel path type supports being shared.
5. Determine if you want to share any channel paths among LPs in different CSSs. If you do, then define these channel paths as spanned by specifying multiple CSS IDs in the PATH keyword of the IOCP CHPID statement. Doing this further helps reduce the number of channel paths configured to a physical control unit and device. Make sure that the channel path type supports being spanned.
6. Within each LP, configure primary and backup paths from separate channel adapter cards.
7. Within each LP, configure primary and backup paths from separate self-timed interfaces (STIs).

Recovery considerations

When planning for recovery, consider the following I/O configuration guidelines.

- Assign channel paths to LPs as described in “Guidelines for setting up the I/O configuration” on page 29.
- Review the recoverability characteristics of the I/O configuration described in the section “Shared devices” on page 55.

Managing logical paths for ESCON and FICON channels

This section describes logical paths, explains overall system considerations, and makes specific configuration recommendations.

Definition

A logical path is a logical connection between a control unit and an ESCON channel (TYPE=CNC or TYPE=CTC), a FICON channel (TYPE=FCV) attached to an ESCON Director, or a FICON channel (TYPE=FC). (FICON Express2, FICON Express4 and FICON Express8 features do not support TYPE=FCV channels.) Logical paths are important because each sharing LP on a CPC requires that a logical path be established between an ESCON or FICON channel and a control unit for I/O operations to occur.

Logical paths do ***not*** exist for ESCON channels attached to a 9034 ESCON Converter Model 1 (TYPE=CBY or TYPE=CVC).

Logical paths do ***not*** exist for coupling facility channel paths (TYPE=CFP), integrated cluster bus channel paths (TYPE=CBP), InfiniBand channel paths (TYPE=CIB), internal coupling channel paths (TYPE=ICP), Open Systems Adapter channel paths (TYPE=OSC, TYPE=OSD or TYPE=OSE, TYPE=OSN), internal queued direct communication (HiperSockets) channel paths (TYPE=IQD), or fibre channel protocol channel paths (TYPE=FCP).

Control unit allocation of logical paths

Control units allocate logical paths to channels dynamically on a first-come-first-served basis. Control units do not manage the allocation of logical paths but instead allow channels to compete for logical paths until all of the control unit's logical paths are used.

Why manage logical paths?

The ESCON and FICON environments (the use of ESCON channels, FICON Express channels, FICON Express2, FICON Express4, and FICON Express8 channels, and ESCON and FICON Directors) greatly enhances the connectivity potential for control units. In addition, you can define shared channels that can request additional logical paths. However, control units can only allocate a limited number of logical paths (see Table 5 on page 32) in relation to the number of logical paths that channels can request. In configurations where channels request more logical paths than a control unit can allocate, you must manage logical paths to help ensure that the I/O operations you intend take place.

The FICON Express2, FICON Express4, and FICON Express8 SX and LX features support all of the functions of FICON Express, with the exception of support for channel path type FCV. FICON Express2, FICON Express4, and FICON Express8, however, offer increased connectivity in the same amount of physical space, and offer the possibility of increased performance. Up to 240 FICON Express2, FICON Express4, and FICON Express8 channels on a z10 EC (and 128 channels on a z10 BC) can be employed to greatly expand connectivity and throughput capability. The FICON connectivity solution is based on industry-standard Fibre Channel technology and leverages our exclusive native FICON architecture. For detailed information, see *System z Input/Output Configuration Program User's Guide for ICP IOCP*, SB10-7037.

Table 5. Logical path summary by control unit

Control unit	Maximum physical links	Logical paths per link	Maximum logical paths
2105 storage control			
2105	32	64	2048
3990 storage control			
3990-2	16	Notes[1]	16
3990-3	16	Notes[1]	16
3990-6	16	Notes[2]	128
9343 storage controller			
9343 D04	4	64	64
9343 DC4	4	64	64
3590 magnetic tape subsystem			
3590	2	64	128
3490 magnetic tape subsystem			
3490 D31, D32, D33, D34	1	16	16
3490 C10, C11, C12	1	16	16
3490 A01	2	16	32
3490 A10	4	16	64
3490 A02	4	16	64
3490 A20	8	16	128
2074 console support controller			
2074 002	2	32	64
3172 interconnect controller			
3172-1	2	Notes[3]	16
3174 establishment controller			
3174 12L (SNA only)	1	Notes[3]	8
3174 22L (SNA only)	1	Notes[3]	8

Notes:

1. 3990-2 and 3990-3 Storage Controls can have eight logical paths per side, two sides, with a minimum of one logical path per adapter.
2. The 3990-6 Storage Control can have 64 logical paths per side, two sides, with a maximum of 32 logical paths per adapter.
3. The 3172 Interconnect Controller and the 3174 Establishment Controller can have one logical path per control unit header (CUH) with a maximum of eight CUHs per link.

ESCON example: Figure 6 shows a situation where 20 ESCON channel paths routed through an ESCON Director (ESCD) each attempt to establish a logical path to a 3990 Storage Control. The 3990 will allocate all 16 of its logical paths among the 20 channel paths dynamically on a first-come-first-served basis. Clearly, some of the ESCON channel paths will not operate in this configuration. Managing logical paths can provide a way to alleviate this situation.

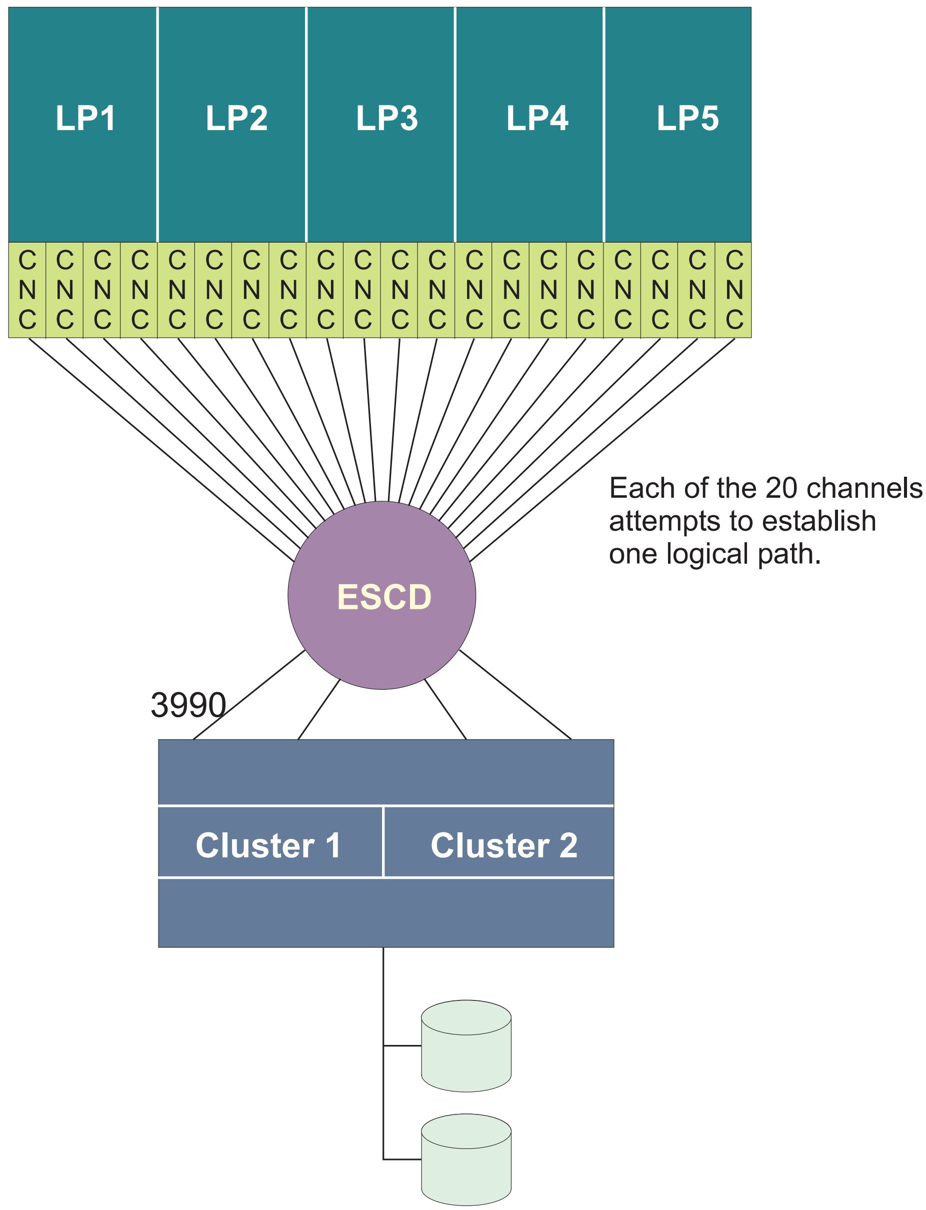


Figure 6. An ESCON configuration that can benefit from better logical path management

MIF example: Figure 7 shows an ESCON shared channel configuration on an MIF-capable CPC. In this example, all five LPs share each of four ESCON channels attached to a 3990. Each shared ESCON channel represents five channel images corresponding to the five LPs. Each channel image requests a logical path to the 3990. As in Figure 6 on page 33, a total of 20 logical paths is requested from the 3990, which can only satisfy 16 of the requests. Again, you can avoid this situation by managing logical paths.

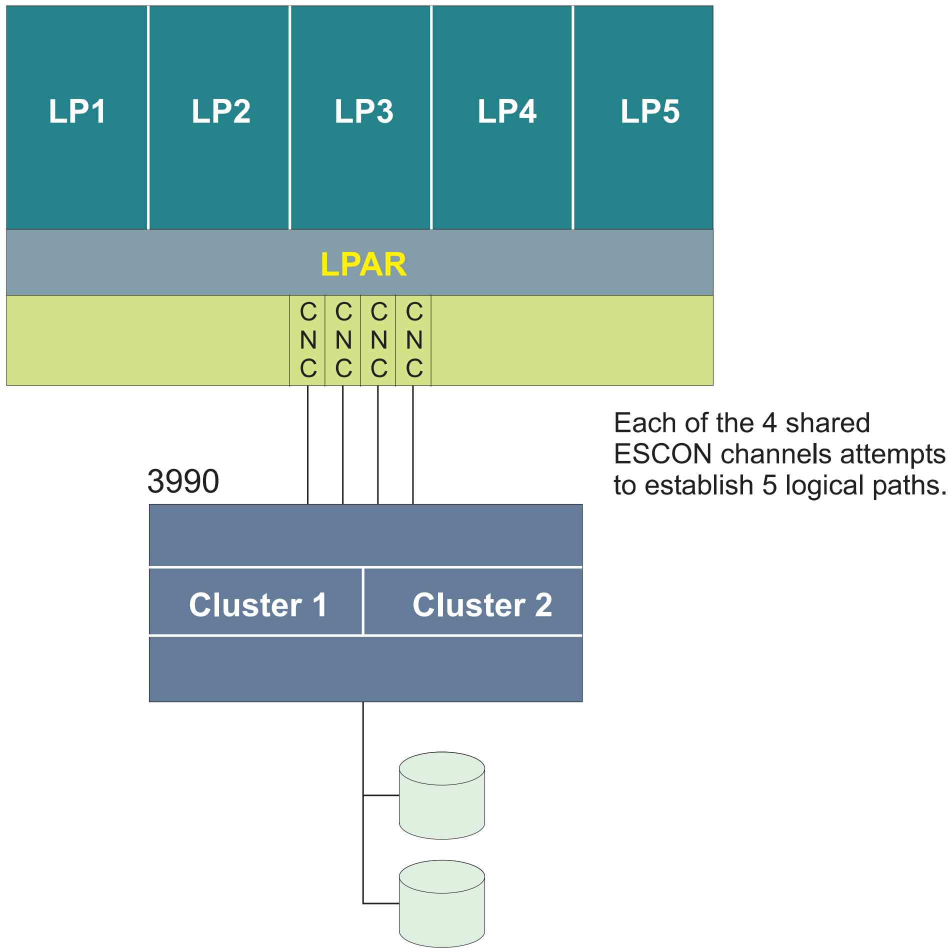


Figure 7. A shared ESCON configuration that can benefit from better logical path management

Managing the establishment of logical paths

You can manage the establishment of logical paths between channels and control units. With proper planning, you can create I/O configuration definitions that allow control units in the configuration to allocate logical paths for every possible request made by channels in either of the following ways:

- Create a one-to-one correspondence between the logical path capacity of all control units in the physical configuration and the channels attempting to request them.
- Create I/O configurations that can exceed the logical path capacity of all or some of the control units in the physical configuration but, at the same time, provide the capability to selectively establish logical connectivity between control units and channels as needed.

  This capability can be useful or even necessary in several configuration scenarios. See “Recommendations” on page 36.

Logical path considerations

You can better understand how to manage the establishment of logical paths by understanding the following:

- Control unit considerations
- Connectivity considerations
- Channel configuration considerations

Control unit considerations: Consider the following factors concerning the allocation of logical paths by control units:

- Control units allocate logical paths dynamically on a first-come-first-served basis.

  Control units do not manage the allocation of logical paths but instead allow channels to compete for logical paths until all of the control unit’s logical paths are used.
- Control units vary in the number of logical paths they support. See Table 5 on page 32.

Connectivity considerations: ESCON and FICON system hardware, CPCs, and ESCON and FICON Directors significantly affect the volume of logical path requests to a control unit as follows:

- Control units can attach to one or more ports on a Director or to additional ports on other Directors. Each Director port can dynamically connect to many other ports to which channels requesting logical paths are attached.
- For CPCs, each logical partition attaching to the same control unit will compete for the control unit’s logical paths.
- In a configuration where control units are shared by different CPCs, I/O configuration definitions for individual control units are not coordinated automatically among the IOCDSs of the different CPCs. Each CPC competes for a control unit’s logical paths.
- Shared channels require the establishment of a logical path for each channel image corresponding to an active LP sharing the channel. This can significantly increase the number of logical paths that a single channel requests.

Channel configuration considerations: The following configuration rules determine how logical paths are established for ESCON and FICON channels.

- A channel initially attempts to establish logical paths:

  - If you perform POR, only those channels configured online to LPs that are activated at POR will attempt to establish logical paths. Shared channels will attempt to establish logical paths only for those activated LPs with the channel configured online.
  - When the LP is activated.
  - When configured online (if previously configured offline).
- A channel cannot establish a logical path or will have its logical path removed when:
  - An LP is deactivated. A shared channel will continue to operate for any other remaining activated LPs to which it is defined. Logical paths to those LPs will remain established.
- A shared channel ***cannot*** establish a logical path to a control unit for an LP that ***cannot*** access any of the I/O devices on the control unit. In IOCP, the PARTITION or NOTPART keyword on the IODEVICE statement specifies which LPs can access a device.
- A channel that cannot initially establish a logical path can reattempt to establish a logical path if the channel detects or is notified of:
  - A change in the state of a control unit
  - A change in the state of a link or port
  - A dynamic I/O configuration change that frees previously allocated logical paths
- A channel cannot establish a logical path or will have its logical path removed if:
  - The Director that connects the channel to the control unit blocks either the channel port or control unit port used in the path.
  - The Director that connects the channel to the control unit prohibits the dynamic connection or communication between the channel port and the control unit port used in the path.
  - A link involved in the path fails or is disconnected. When a shared channel is affected by a port being blocked, a dynamic connection or communication being prohibited, or a link failing or being disconnected, each LP sharing the channel will be equally affected and all logical paths using the port or link (regardless of which LP they are associated) will be removed.
  - The channel is configured offline. When a shared channel is configured offline for an LP, it will continue to operate for any other LP that has the channel configured online. Logical paths to these other logical partitions will remain established.
  - Power to the channel, control units, or Directors in the configuration is turned off.

Recommendations

Creating I/O configuration definitions where channels could request more logical paths to control units than the control units could support can be useful in the following scenarios:

- **Workload balancing**

  When a system image becomes overloaded, you may need to reassign a workload and the necessary logical paths (for example, its tape or DASD volumes, a set of display terminals, or a set of printers) to another system image that has available capacity.

- **Backup**

  When an outage occurs, you can move the critical application set (the program and associated data) and the necessary logical paths to a backup or standby CPC. This process is simple if the CPCs have identical I/O configurations.

In I/O configurations where channels can request more logical paths to control units than the control units can support, you can manage how logical paths are established by:

- Deactivating unneeded LPs.
- Configuring offline unneeded channels. For shared channels, configure offline unneeded channels on an LP basis.
- Limiting the number of LPs that can access the I/O devices attached to a control unit when the control unit attaches to shared channels. In IOCP, specify the PARTITION or NOTPART keyword on the IODEVICE statement for every I/O device attaching to a control unit so that 1 or more LPs ***cannot*** access any of the I/O devices.
- Using the Director to block ports or prohibit dynamic connections or communication between ports.
- Combinations of the above.

To better understand how you can manage logical paths using these methods, consider the following examples.

Deactivating unneeded logical partitions: Deactivating unneeded LPs can prove useful for managing how logical paths are established on CPCs in some situations.

The system establishes logical paths only when an LP is activated. Deactivating an LP results in removal of those logical paths associated with the LP. This can greatly reduce the number of logical paths requested by the system at any given time.

In Figure 8 on page 38, if all five of the LPs each share all four of the ESCON channels and all of the LPs are activated, the 3990 would be requested to establish five logical paths for each of the four shared ESCON channels (or a total of 20 logical paths). Because the 3990-3 only supports 16 logical paths, you will need to manage how logical paths are established to help ensure the I/O connectivity you require.

For example, if you used LP4 and LP5 as test LPs that did not need to be active concurrently, you could reduce the number of logical paths requested by four by not activating either LP4 or LP5. In this case, four LPs (LP1, LP2, LP3, and LP4 or LP5) configured to four shared ESCON channels would request a total of 16 logical paths. Later, you could transfer logical paths between LP4 and LP5 by first deactivating one LP to remove its logical paths, then activating the other LP to use the freed logical paths.

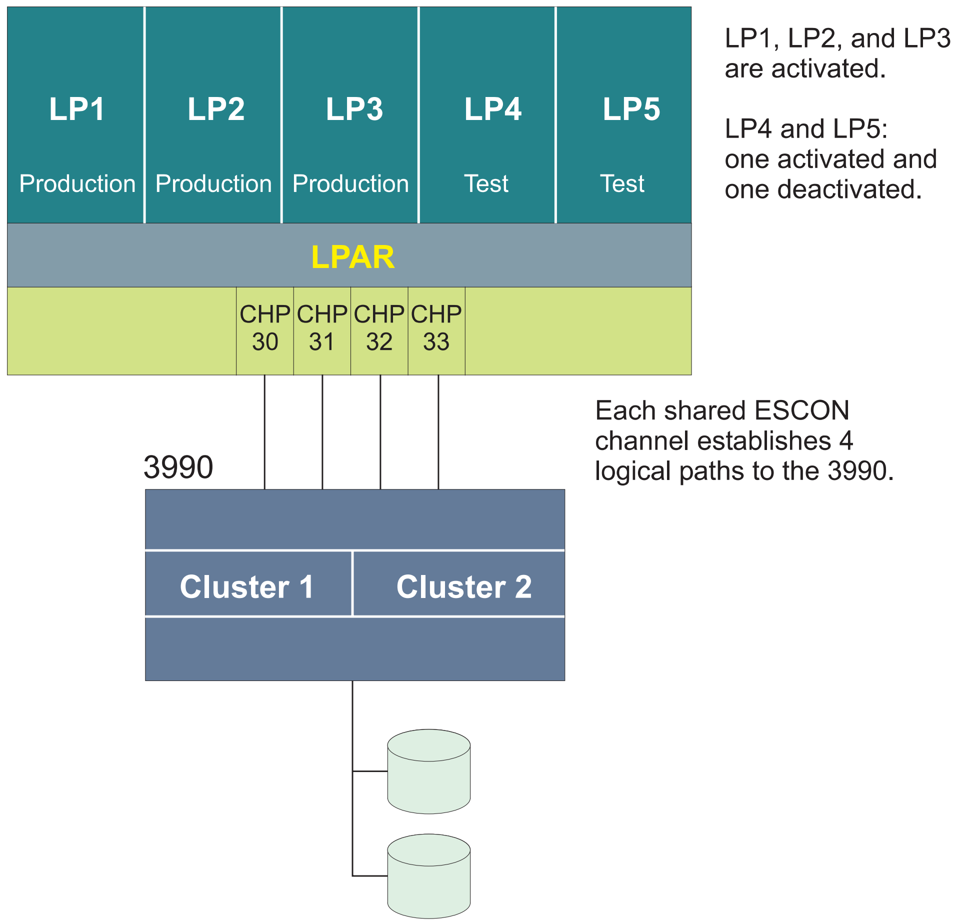


Figure 8. Deactivating unneeded logical partitions

Configuring offline unneeded channels or shared channels on an LP basis: You can configure offline unneeded channels or shared channels on an LP basis to manage how logical paths are established. In Figure 9 on page 39, all five LPs need to be active concurrently. If all five LPs had each of the four shared ESCON channels configured online, 20 logical paths (four logical paths for each of the five LPs) would be requested, exceeding the 3990's logical path capacity.

However, if LP4 or LP5 (both test LPs) did not require four channel paths each to the 3990, you could configure offline two of the four channel images used by LP4 and two of the four channel images used by LP5, reducing the total number of logical paths requested from 20 to 16 and matching the 3990's logical path capacity.

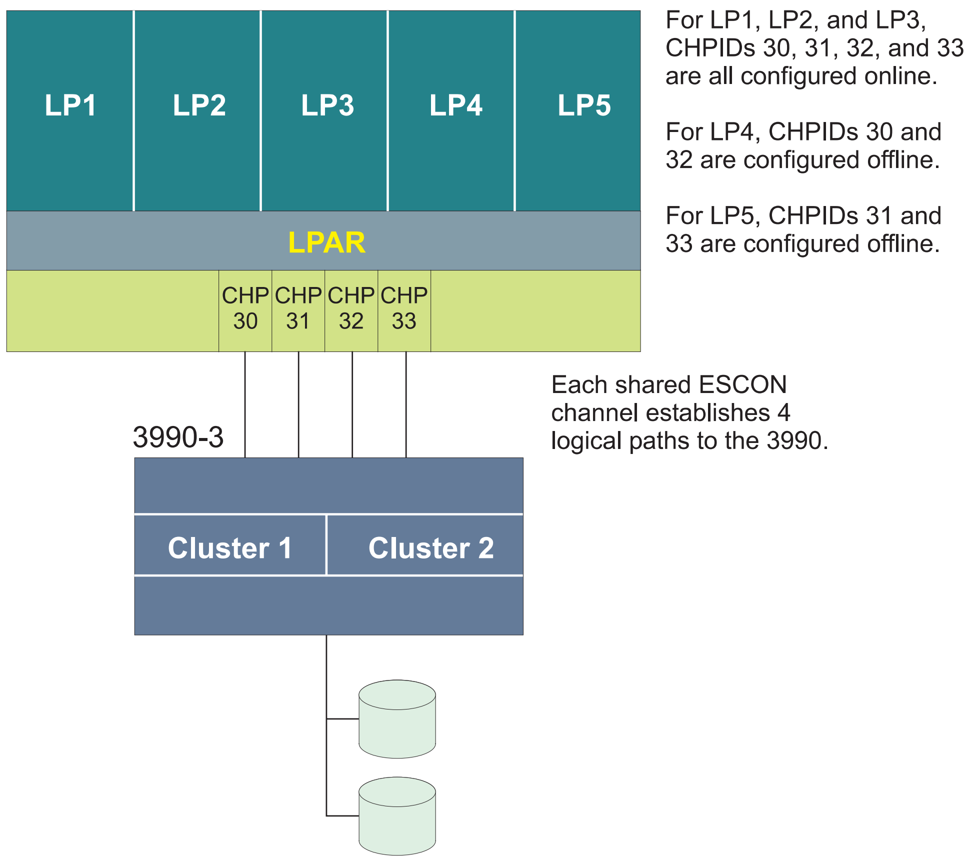


Figure 9. Configuring offline unneeded channels or shared channels on an LP basis

Note: Because the 3990-3 supports only eight logical paths per cluster, you would need to configure offline the channel images so that the number of logical paths requested from each cluster remains at eight.

It is also possible to manage how logical paths are established by using IOCP or Hardware Configuration Definition (HCD) to create I/O configuration definitions that:

- Define a subset of LPs that will have their corresponding channels configured online at power-on reset (POR) (CHPID access list)
- Allow LPs to configure online their channels at a later time (CHPID candidate list)

Use IOCP or HCD to define the access lists and candidate lists for channel paths to determine the configurability of a channel to an LP. This capability exists for both unshared and shared channels and can help automate and establish the configuration in Figure 9. Additionally, HCD allows you to dynamically change the access list and candidate list for a channel path.

Defining devices to a subset of logical partitions: You can limit I/O device access from LPs to I/O devices assigned to shared channels by using IOCP or HCD to specify device candidate lists. By defining devices attached to a control unit to a subset of LPs, you can manage which LPs will attempt to establish logical paths to the control unit through a shared channel.

If you define no devices to a control unit from a particular LP, the shared channel associated with the LP will not attempt to establish a logical path. However, if there is at least one device defined to the control unit for the shared channel associated with a particular LP, the shared channel for the LP will attempt to establish a logical path to the control unit for the LP.

In Figure 10 on page 41, LP access to a series of 3174s is managed through use of the device candidate lists for the I/O devices attached to the control units. The shared ESCON channel will attempt to establish only one logical path to each of the 3174s even though 5 LPs share the channel. This is useful because the 3174 in non-SNA mode only supports one logical path.

In the example, the channel only attempts to establish a logical path for LP1 to the 3174 defined as control unit 10 because only LP1 has a device defined to that control unit. Similarly, only LP2 can access the 3174 defined as control unit 11, only LP3 can access the 3174 defined as control unit 12, only LP4 can access the 3174 defined as control unit 13, and only LP5 can access the 3174 defined as control unit 14.

Partial IOCP Deck for the Configuration: The following is a partial IOCP deck for the example in Figure 10 on page 41.

```
CHPID PATH=30,SHARED

CNTLUNIT CUNUMBR=10,PATH=30
IODEVICE ADDRESS=VVVV,CUNUMBR=10,PART=LP1

CNTLUNIT CUNUMBR=11,PATH=30
IODEVICE ADDRESS=VVVV,CUNUMBR=11,PART=LP2

CNTLUNIT CUNUMBR=12,PATH=30
IODEVICE ADDRESS=VVVV,CUNUMBR=12,PART=LP3

CNTLUNIT CUNUMBR=13,PATH=30
IODEVICE ADDRESS=VVVV,CUNUMBR=13,PART=LP4

CNTLUNIT CUNUMBR=14,PATH=30
IODEVICE ADDRESS=VVVV,CUNUMBR=14,PART=LP5
```

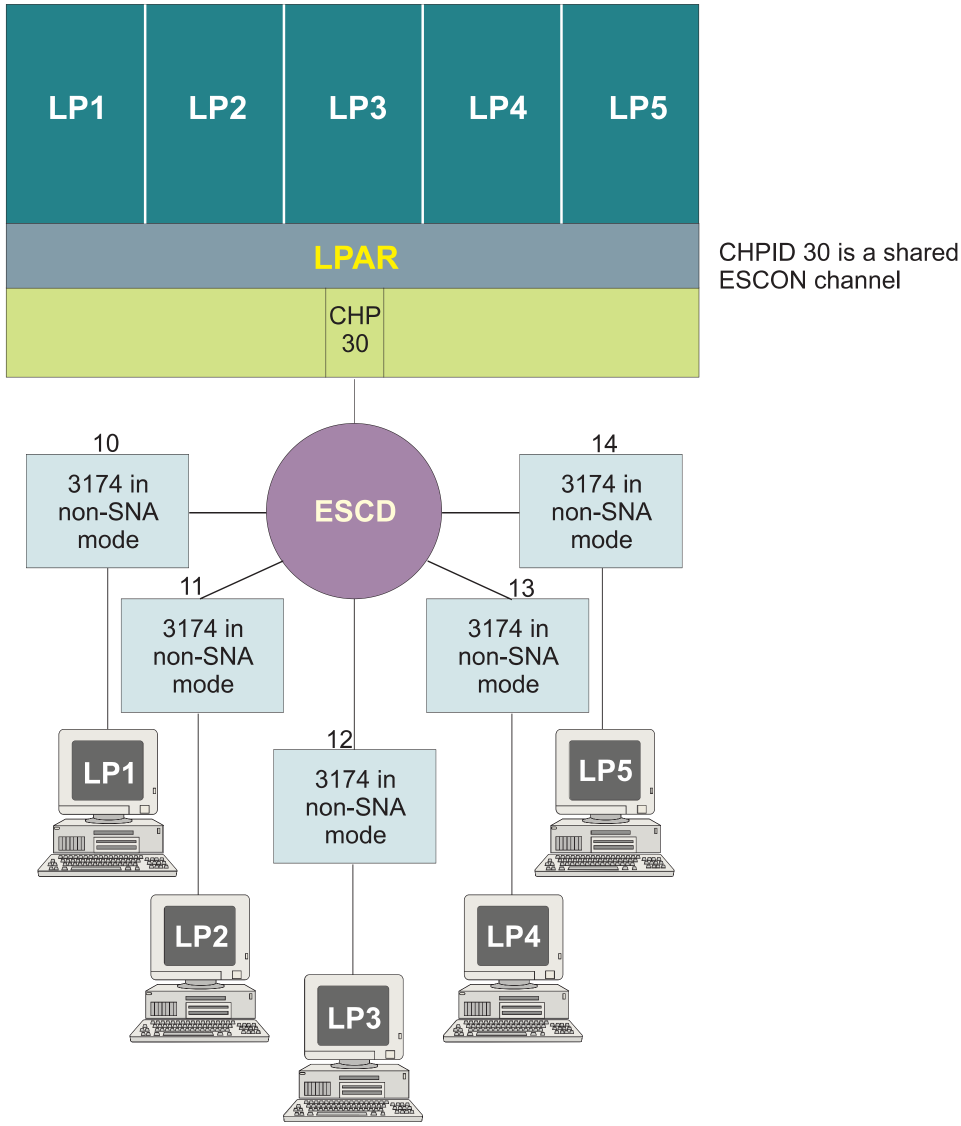


Figure 10. Defining devices to a subset of logical partitions

In Figure 11, a 3174 in SNA mode is defined as five control unit headers (CUHs). Because each 3174 CUH supports a maximum of one logical path, it is equally important in this example that the shared channel only attempts to establish a single logical path to each 3174 CUH.

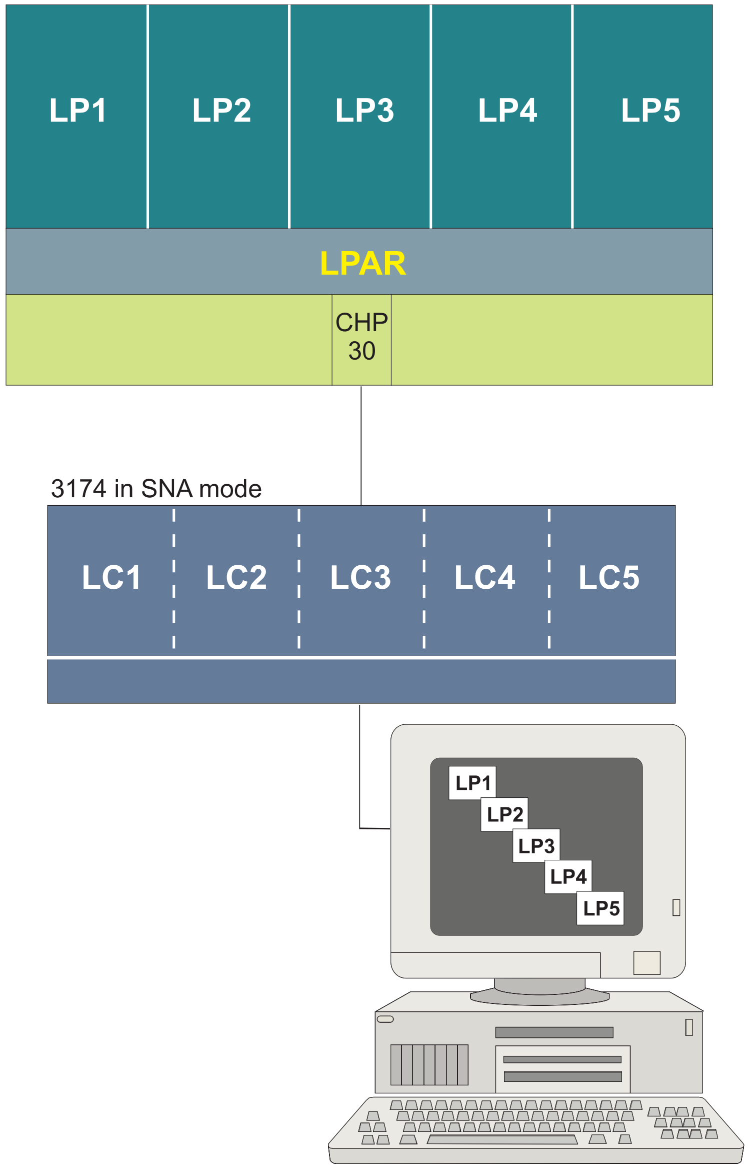


Figure 11. Defining devices to a subset of logical partitions

Even though 5 LPs share the ESCON channel, the channel will only attempt to establish a logical path for LP1 to CUH 0 because only LP1 has a device defined on that CUH. Similarly, only LP2 can access CUH 1, only LP3 can access CUH 2, only LP4 can access CUH 3, and only LP5 can access CUH 4.

Partial IOCP Deck for the Configuration: The following is a partial IOCP deck for the example in Figure 11.

```
CHPID PATH=30,SHARED

CNTLUNIT CUNUMBR=10,PATH=30,CUADD=0
IODEVICE ADDRESS=VVVV,CUNUMBR=10,PART=LP1

CNTLUNIT CUNUMBR=11,PATH=30,CUADD=1
IODEVICE ADDRESS=WWWW,CUNUMBR=11,PART=LP2

CNTLUNIT CUNUMBR=12,PATH=30,CUADD=2
IODEVICE ADDRESS=XXXX,CUNUMBR=12,PART=LP3

CNTLUNIT CUNUMBR=13,PATH=30,CUADD=3
IODEVICE ADDRESS=YYYY,CUNUMBR=13,PART=LP4

CNTLUNIT CUNUMBR=14,PATH=30,CUADD=4
IODEVICE ADDRESS=ZZZZ,CUNUMBR=14,PART=LP5
```

Using a director to block ports or prohibit dynamic connections or communication: When ESCON or FICON Directors are used in an I/O configuration, you can prevent channels from establishing logical paths or can remove established logical paths by either blocking a Director port or by prohibiting a dynamic connection or communication between two Director ports.

In terms of logical path removal, blocking a Director port connected to a channel produces a similar outcome to configuring offline a channel or all channel images of a shared channel. Blocking a Director port connected to a control unit prevents any logical path from being established to the attached control unit port.

You can more selectively prevent logical paths from being established by prohibiting a dynamic connection between two ESCON Director ports or dynamic communication between two FICON Director ports instead of blocking a Director port. By prohibiting a dynamic connection or communication between two Director ports, you can control which channels have connectivity to a control unit port rather than blocking all connectivity to the control unit port.

Prohibiting a dynamic connection or communication between two Director ports affects all channel images of a shared channel. The system will not establish any logical paths to the attached control unit port from any of the LPs that share the ESCON or FICON channel.

You can prohibit dynamic connections or communication between Director ports by modifying the active configuration table. The active configuration table specifies the connectivity status of a port relative to the other ports on the Director. When a Director is first installed, it has a default configuration that allows any-to-any connectivity (every port can dynamically connect or communicate with every other port). If you require a different configuration than this, you can define and designate a different table to be the default configuration used at power-on of the Director. This table will allow only those dynamic connections or communication necessary to establish the logical paths the configuration requires. Dynamic connections or communication necessary to establish other logical paths (for example, those necessary for backup configurations) would be prohibited by the default configuration of the Director.

Figure 12 on page 44 shows an example of prohibiting dynamic connections. CPC1, CPC2, CPC3, and CPC4 are all production systems and CPC5 is a backup system to be used only if one of the other CPCs fail. If the default configuration used by the ESCON Director (ESCD) prohibits all dynamic connections between CPC5 and the 3990, the 3990 will only be requested to establish a total of 16 logical paths from the channels on CPC1, CPC2, CPC3, and CPC4. If one of four production CPCs fails, you could transfer the logical paths from the failing CPC to the backup CPC by prohibiting the dynamic connection to the failed CPC and allowing the dynamic connection to the backup CPC.

If a control unit is connected to more than one Director, it is necessary to coordinate allocation of the control unit's logical paths across all of the Directors. You can use the System Automation for z/OS (SA z/OS) to dynamically manage the Directors and logical paths by sending SA z/OS commands to reconfigure one or more Directors. SA z/OS then sends the appropriate operating system Vary Path requests. SA z/OS can also provide coordination between operating systems when logical paths are removed from one system and transferred to another system as a result of blocking Director ports or prohibiting Director dynamic connections or communication.

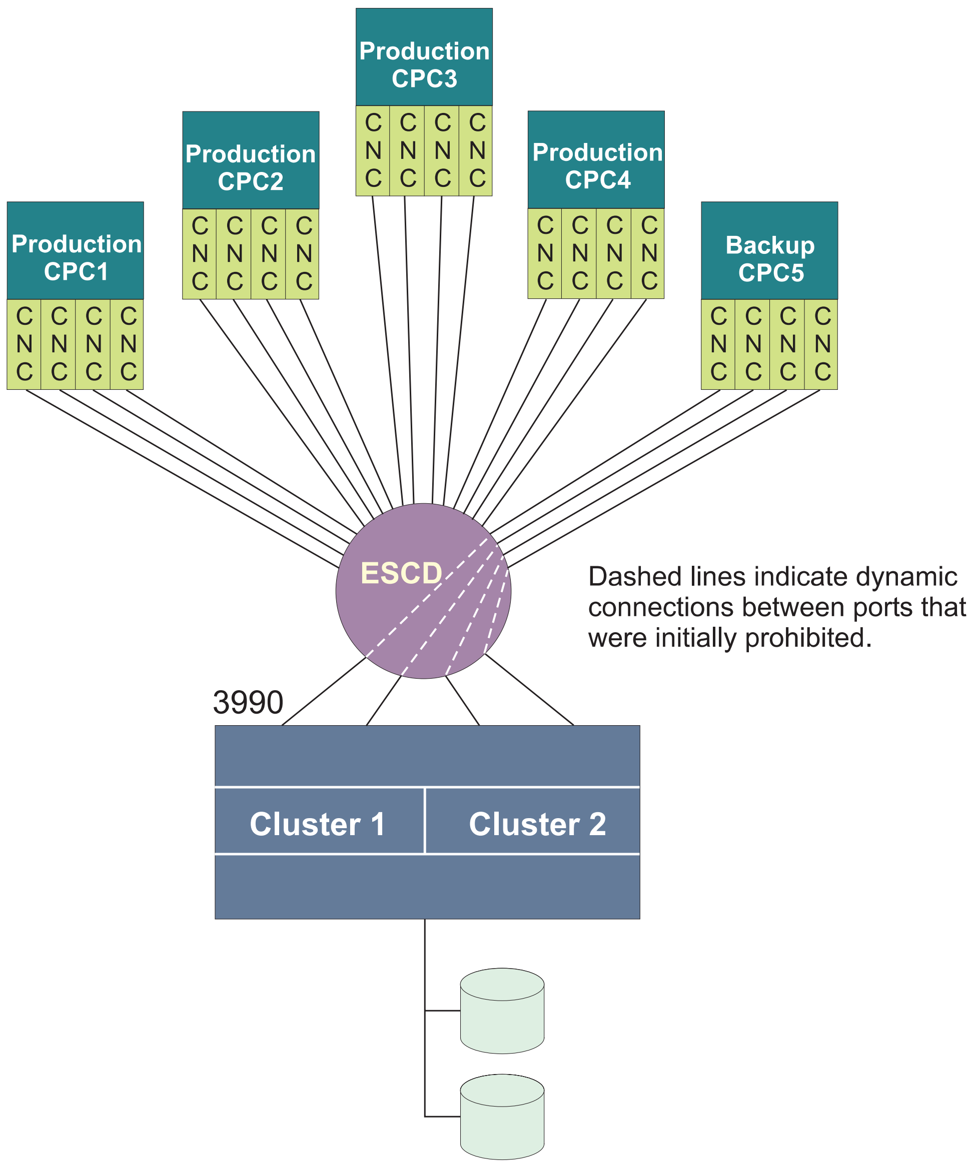


Figure 12. Using the ESCD to manage logical paths by prohibiting dynamic connections

Shared channel overview

MIF allows channels to be shared among multiple LPs. Shared channels are configured to an LP giving the LP a channel image of the shared channel that it can use. Each channel image allows an LP to independently access and control the shared channel as if it were a physical channel assigned to the LP.

By providing the logical equivalent of multiple physical channels dedicated to multiple LPs, a shared channel can reduce hardware requirements without a corresponding reduction in I/O connectivity. This reduction in hardware requirements can apply to physical channels, Director ports, and control unit ports, depending on the configuration.

MIF requirements

To take advantage of MIF, you need:

- An ESCON-capable operating system:
  - z/OS
  - z/VM
  - z/VSE
  - AIX/ESA®
  - TPF
  - z/TPF
- ESCON channels operating in native mode (CNC) or channel-to-channel mode (CTC), FICON channels attached to an ESCON director (FCV), FICON channels (FC), coupling facility channels (ICP, CBP, CIB, or CFP), open systems adapter channels (OSC, OSD, OSE or OSN), internal queued direct communication (HiperSockets) channels (IQD), and fibre channel protocol channels (FCP).

  Note: ESCON channels that attach to a 9034 ESCON Converter Model 1 (CVC or CBY) cannot be shared among LPs.
- IBM ESCON-capable or FICON-capable control units, or fibre channel switches.

Understanding ESCON and MIF topologies

This section describes the following I/O topologies:

- Point-to-point topology
- Switched point-to-point topology
- MIF channel sharing topology

Point-to-Point Topology: The traditional point-to-point topology requires a unique path between any two points that communicate. A channel and CU adapter are required between each communication point. In a point-to-point configuration, a channel can communicate with only one control unit. A control unit that communicates with more than one channel requires a separate control unit adapter interface to each channel. The configuration limitations in a point-to-point topology can lead to inefficient use of channels and control units. See Figure 13 on page 46 for an example of the point-to-point topology.

Switched Point-to-Point Topology: Switched point-to-point topologies eliminate the disadvantages of point-to-point and multidrop topologies. Switched point-to-point topology enables switching between any channel path and control unit adapter when using an ESCON or FICON Director. By using the Director, paths can also be shared by multiple points. The Director enables one channel to switch to multiple control units, or one control unit to switch to multiple channels. Paths necessary to satisfy connectivity requirements in a point-to-point topology are not required in the switched point-to-point topology. This can reduce the number of channels and control unit interfaces required without a corresponding reduction in I/O activity. See Figure 13 for an example of switched point-to-point topology.

MIF Channel Sharing Topology: MIF further improves control unit connection topologies for CPCs with multiple LPs. MIF enables many LPs to share a physical channel path. MIF can reduce the number of channels and control unit interfaces required without a corresponding reduction in I/O connectivity. See Figure 13 for and example of MIF channel sharing topology.

MIF performance planning considerations

Your installation can take advantage of MIF performance enhancements offered by:
- Understanding and utilizing I/O-busy management enhancements
- Planning for concurrent data transfer
- Understanding examples of MIF consolidation

Understanding and utilizing I/O-busy management enhancements: This section shows how the various ESCON or FICON and MIF topologies offer improvements in managing I/O-busy conditions. Figure 13 compares the point-to-point, switched point-to point, and MIF channel sharing topologies.

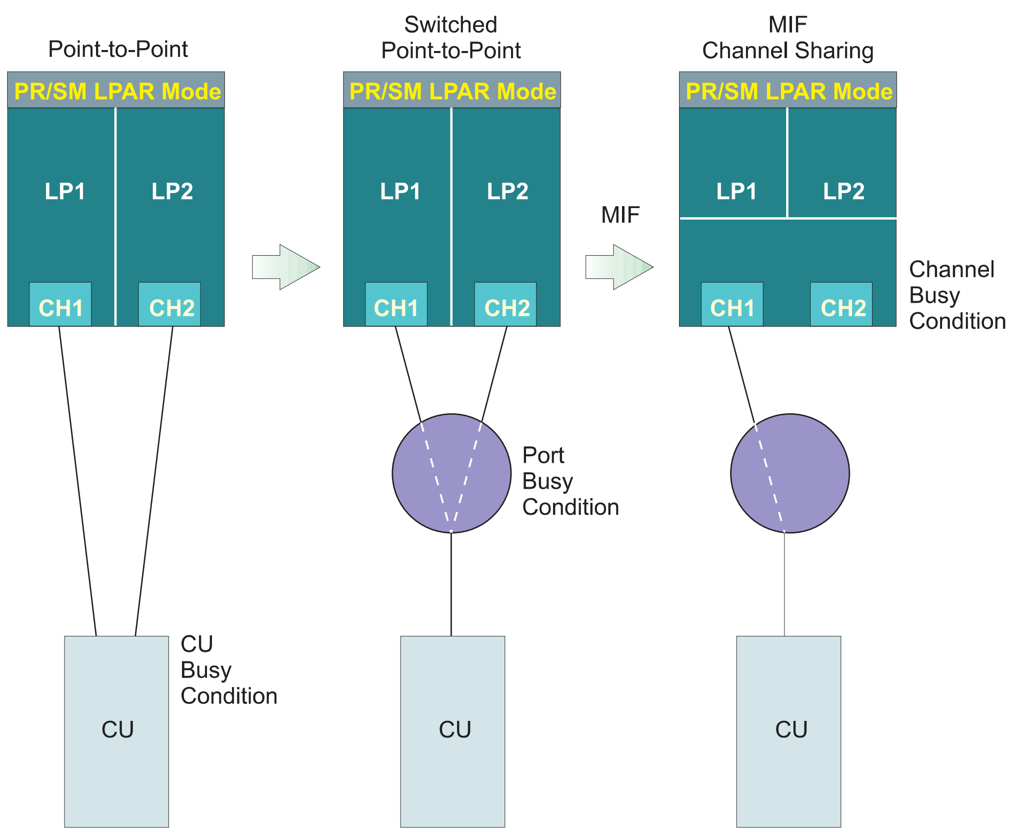


Figure 13. Progression of busy condition management improvements

Point-to-Point topologies: Concentrate I/O attempts at the control unit level and are distance dependent. At the time of a control unit busy encounter, the control unit must present control unit busy status to the channel. Once the control unit is free, it presents a control unit no longer busy status to the channel. This process of presenting status to the channel requires control unit processing and many trips over the control unit to channel link.

Switched Point-to-Point topologies: Concentrate I/O attempts within the Director and therefore encounter switch port busies. The processing of switch port busies does not require any control unit involvement. Busies are handled by the ESCON or FICON Director. Therefore, the control unit is effectively relieved of handling busy conditions and is able to handle more I/O requests. Because switch port busies require fewer trips over the ESCON or FICON connection link, they are less sensitive to increased distances than control unit busy encounters.

MIF channel sharing: Moves busy management back into the channel subsystem, providing the most efficient management of busy conditions. Because multiple LPs access the same physical channel, I/O attempts are concentrated at the channel level. A CU busy or a switch port busy is handled as a channel busy.

Planning for concurrent data transfer: Before you can consolidate channels, you must be aware of the channel requirements of the particular control units you are configuring. Table 6 shows the maximum recommended ESCON channels for a single system going to a control unit. The number of channels needed is independent of the number of LPs on a system. The number of channels is based on the number of concurrent data transfers the control unit is capable of. Although the recommended number of channels satisfies connectivity and performance requirements, additional channels can be added for availability.

Table 6. MIF maximum channel requirements

Control unit type	Maximum channels (see note)
9343 storage controller	
9343 D04	4
9343 DC4	4
3990 storage control	
3990-2	4
3990-3	4
3990-6	4
3490 magnetic tape subsystem	
3590	2
3490 D31, D32, D33, D34	1
3490 C10, C11, C12	1
3490 A01	1
3490 A10	1
3490 A02	2
3490 A20	2
2074 console support controller	
2074 002	2
3174 establishment controller	
3174 12L (SNA only)	1
3174 22L (SNA only)	1
Note: The recommended maximum channels given in this table are based on performance and connectivity requirements and do not include channels for availability.	

Understanding examples of MIF consolidation: The following examples provide some general guidelines to show how MIF can help you consolidate and use hardware resources more efficiently:

ESCON configurations: Figure 14 on page 48 shows how four shared ESCON channels can replace 16 unshared (dedicated or reconfigurable) ESCON channels and use 12 fewer control unit ports.

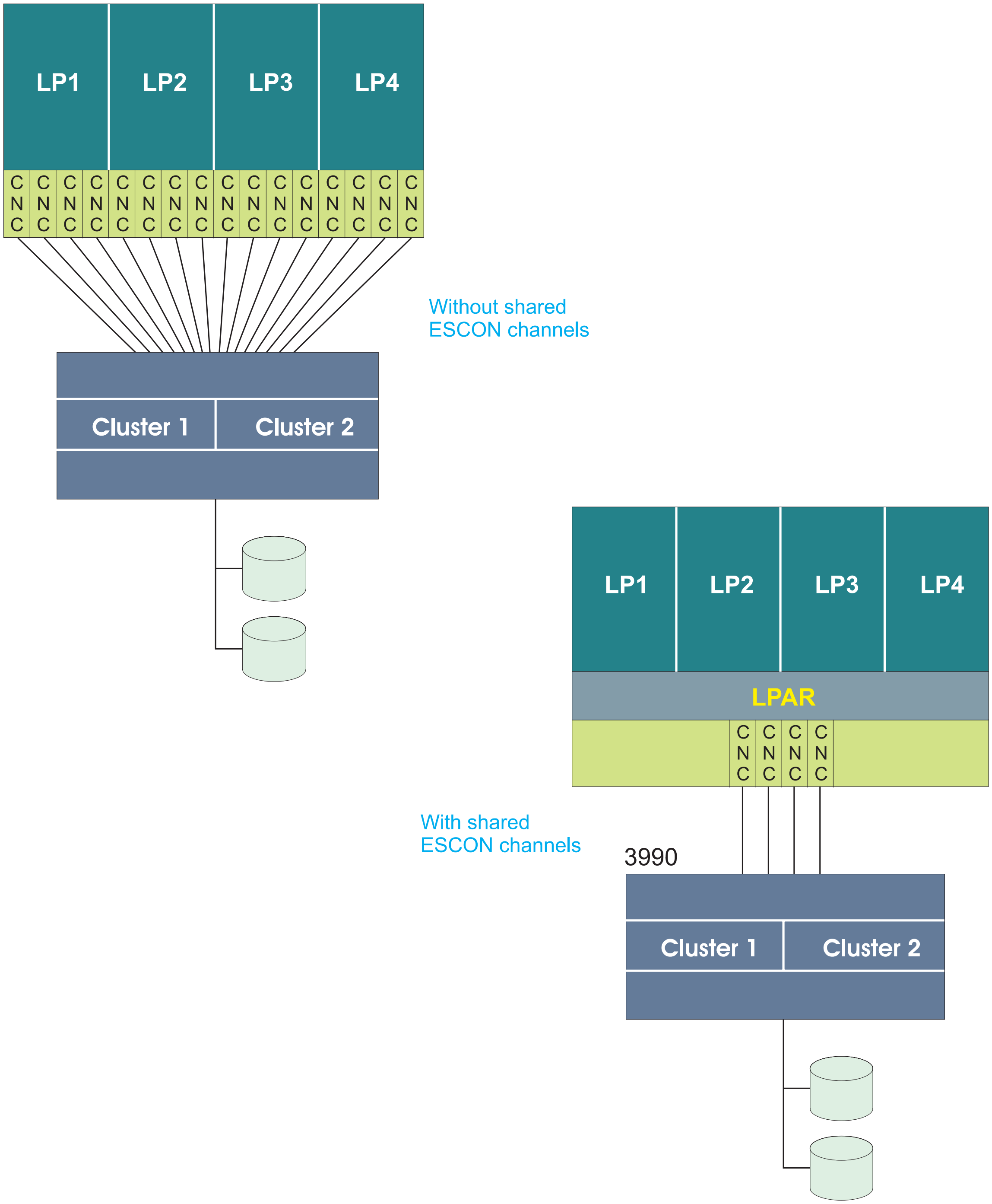


Figure 14. Consolidating ESCON channels and ESCON control unit ports

ESCD configurations: Figure 15 on page 49 shows how shared ESCON channels can reduce ESCD port requirements. In this example, two shared ESCON channels replace 10 unshared (dedicated or reconfigurable) ESCON channels and use eight fewer ESCD ports without a reduction in I/O connectivity.

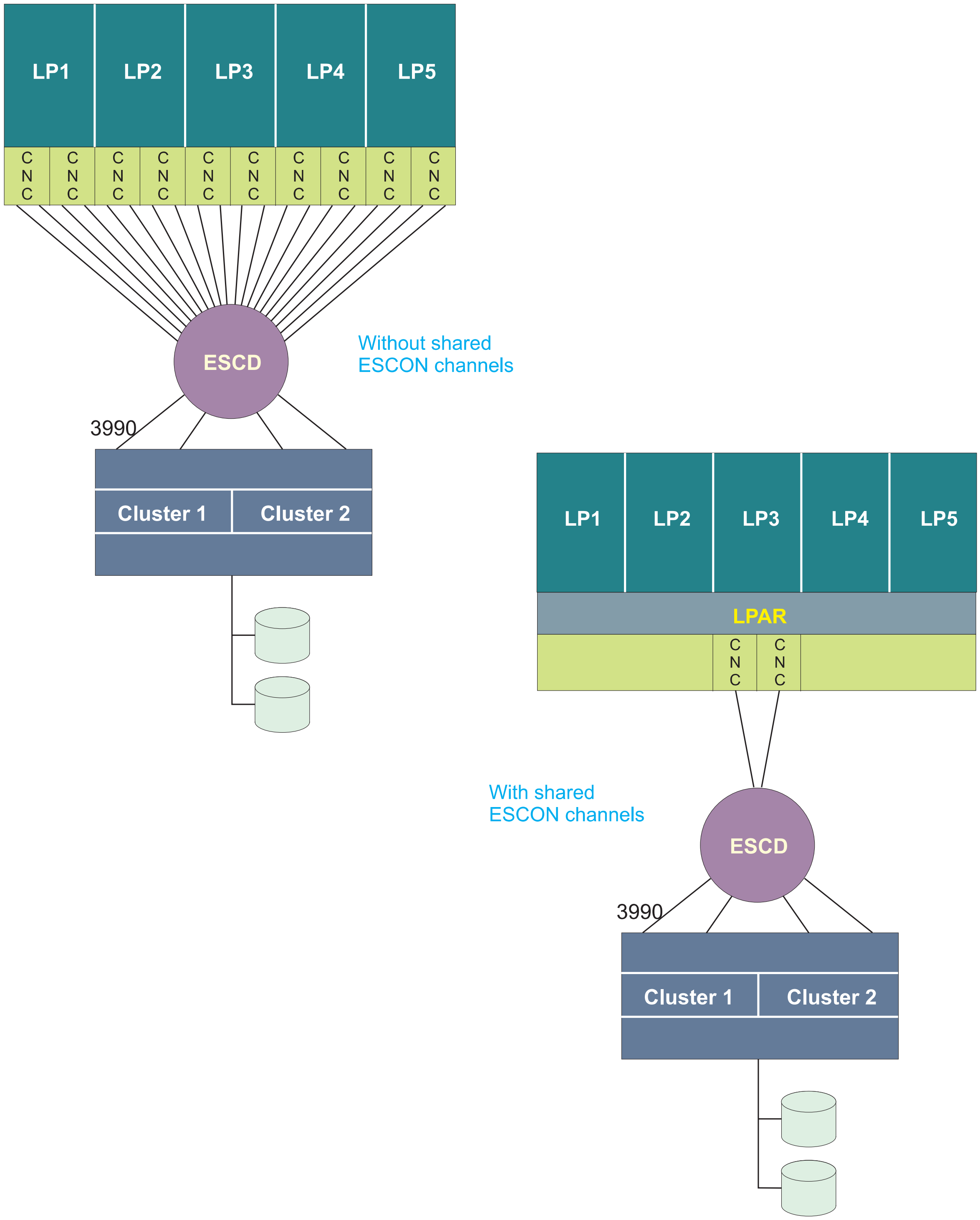


Figure 15. Consolidating ESCON channels and ESCD ports

ESCON CTC Configurations: Figure 16 shows how shared ESCON channels can reduce the ESCON channel requirements for ESCON CTC configurations. In this example, the CPC requires CTC communications among all its LPs.

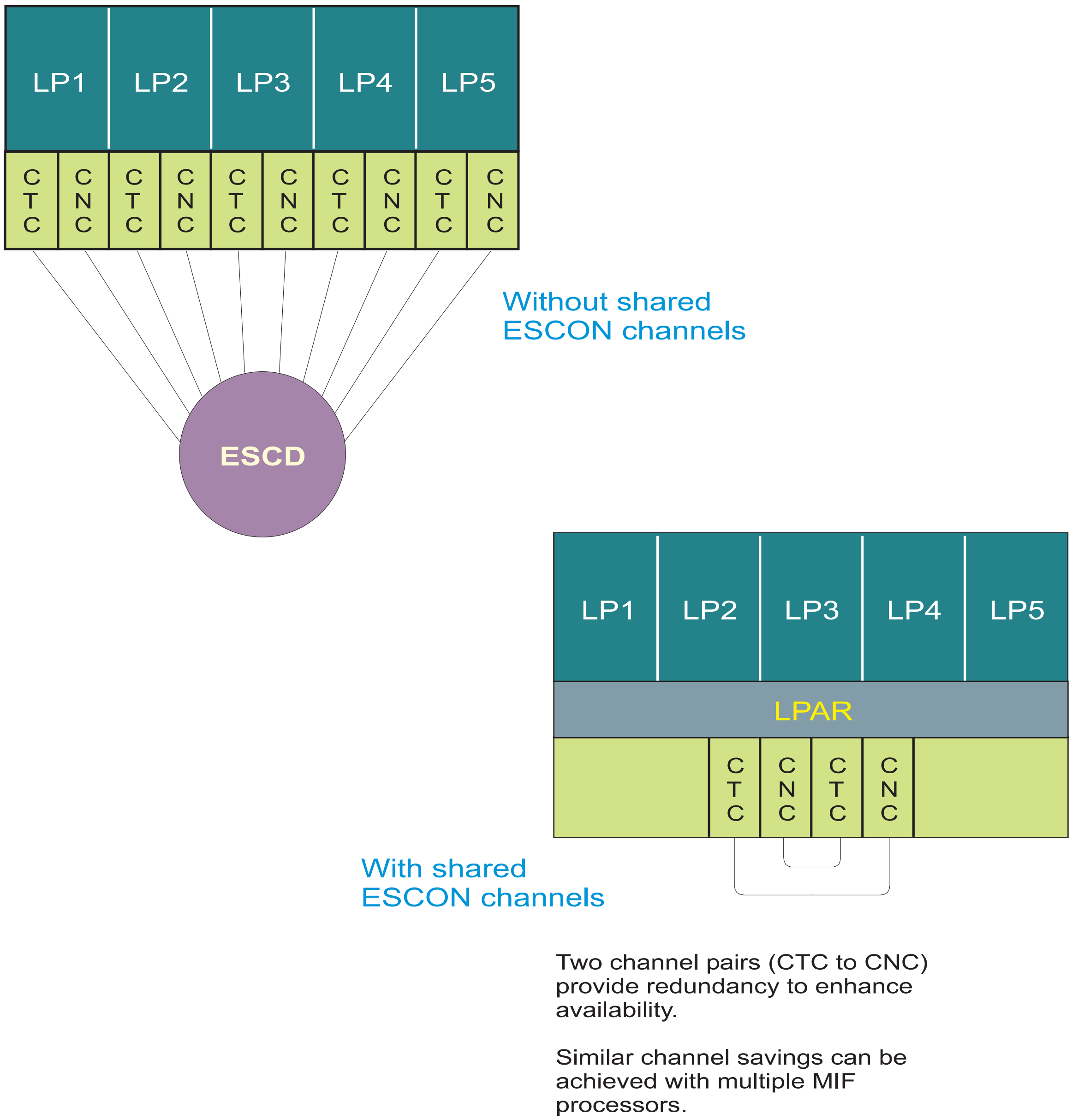


Figure 16. Consolidating ESCON channels used for ESCON CTC communications

By using two shared ESCON CTC/CNC pairs (4 shared ESCON channels), you can:

- Replace five unshared ESCON CTC/CNC pairs (10 unshared ESCON channels) and the ESCD used to connect them
- Provide full redundancy

I/O connectivity is maintained while hardware requirements (channels and an ESCD) are reduced.

In situations where ESCON CTC communication is required among LPs that exist on two or more CPCs, shared channels can reduce even further channel and other hardware requirements and their associated cost.

ESCON CTC configurations are well-suited to take advantage of the consolidation benefits associated with shared channels. CTC/CNC and CTC/FCV pairs used for ESCON CTC communications have no limitation on the number of logical paths that can be established between them. The only limitations are the number of control units that can be defined for an ESCON CTC channel and the performance expectations you determine for your configuration.

Infrequently Used ESCON or FICON Control Units: ESCON or FICON control units not frequently used can make use of shared channels. You can attach such a control unit to a shared channel that is also attached to other, more frequently used control units without adding greatly to the channel utilization of the shared channel. The control unit within the Director is a good example of this.

Notes:

1. You cannot define a control unit (or multiple control units with common I/O devices) to a mixture of shared and unshared channel paths in the same IOCDS.
2. You cannot define more than one control unit with the same CUADD to the same link on a Director (or point-to-point) if the attaching CHPIDs are shared.

Unshared ESCON or FICON channel recommendations

Not all ESCON or FICON configurations benefit from the use of shared channels. There are some configurations where use of an unshared channel is more appropriate. Consider the following:

- **Logical path limitations of the control Unit**

  While many ESCON control units can communicate with multiple LPs at a time using multiple logical paths, there are some ESCON-capable control units that can only communicate with one LP at a time. For example, consider the 3174 Establishment Controller (Models 12L and 22L). When configured in non-SNA mode, the 3174 establishes only one logical path at a time. A shared channel would offer no connectivity benefit in this situation. However, if you defined an unshared, reconfigurable channel to the 3174, it would allow you to dynamically reconfigure the channel for any LP that had to communicate with the 3174 at a given time.
- **Channel Utilization**

  Typically, the channel utilization of shared channels will be greater than unshared channels.

  If you use shared channels to consolidate channel resources, you must consider the channel utilization of all the channels you consolidate. The channel utilization of a shared channel will roughly equal the sum of the channel utilizations of each unshared channel that it consolidates. If this total channel utilization is capable of decreasing performance, you should consider using unshared channels or a different configuration of shared and unshared channels to meet your connectivity needs.

Dynamically managed CHPIDs

A key aspect of the Intelligent Resource Director (IRD) provided by z/OS's WLM component is Dynamic CHPID Management (DCM). DCM provides the ability to have the system automatically move the available channel bandwidth to where it is most needed. CHPIDs identified as managed in the IOCDS (via CHPARM and IOCLUSTER keywords) are dynamically shared among z/OS images within an LPAR cluster.

Prior to DCM, available channels had to be manually balanced across I/O devices in an attempt to provide sufficient paths to handle the average load on every controller. Natural variability in demand means that some controllers at times have more I/O paths available than they need, while other controllers possibly have too few. DCM attempts to balance responsiveness of the available channels maximizing the utilization of installed hardware. Fewer overall channels are required because the DCM CHPIDs are more fully utilized. RMF provides a report showing the average aggregate utilization for all managed channels.

By using DCM, you now only have to define a minimum of one nonmanaged path and up to seven managed paths to each control unit (although a realistic minimum of two nonmanaged paths are recommended), with dynamic channel path management taking responsibility for adding additional paths as required. For more information on defining and using DCM, including detailed examples, see the *z/OS Intelligent Resource Director*, SG24-5952.

IOCP coding specifications

ICP IOCP can only generate an LPAR IOCDS. No IOCP invocation parameter is required to generate an LPAR IOCDS.

IOCP statements for ICP

The RESOURCE statement is used to specify all the logical partition names defined in a machine configuration. To plan for growth in the number of logical partitions in the configuration, one or more asterisks (*) may be used to specify that one or more logical partitions are to be reserved along with their associated CSS and MIF image IDs. A reserved LP can only be specified for a dynamic-capable IOCDS. A dynamic-capable IOCDS is built when using HCD on z/OS or z/VM or specifying IOCP CMS utility option DYN for z/VM. Space in the hardware system area (HSA) is allocated for reserved LPs but cannot be used until a dynamic I/O configuration change is made to assign a name to the LP. The following rules apply when specifying reserved LPs:

- A reserved LP must have a user-specified MIF image ID
- A reserved LP cannot have any channel paths assigned to it
- An IOCDS cannot contain only reserved LPs. At least one LP must be defined with a name.

Dynamic CHPID Management (DCM) channel paths defined for a given LPAR cluster are shareable among all active LPs that have joined that cluster. Other than DCM channel paths, you must assign each channel path to a logical partition in an LPAR IOCDS. For each DCM channel path, ICP requires the CHPARM keyword have a value of 01 and the IOCLUSTER keyword on a CHPID statement. All other channel paths require the PART|PARTITION, NOTPART, or SHARED keyword on all CHPID statements unless a channel path is defined as spanned by specifying multiple CSS IDs in the PATH keyword of the IOCP CHPID statement.

Use the CHPARM and IOCLUSTER keywords on the CHPID statement to specify channel paths reserved for the use of a particular LPAR cluster. A DCM channel path becomes available to a candidate logical partition when the LP is activated and joins the specified cluster.

Use the CHPID PART|PARTITION, NOTPART, and SHARED keywords to determine which:
- Channel paths are assigned to each LP
- Devices and control units are shared among LPs
- Channel paths are reconfigurable
- Channel paths are shared

Use the CHPID CPATH keyword to connect two internal coupling channels.

Use the CHPID PATH keyword to define a channel path as spanned to multiple CSSs. Spanned channel paths are also shared channel paths.

DCM channel paths are implicitly shared. Use of the IOCLUSTER keyword implies a null access list (no logical partition has the channel path brought online at activation) and a candidate list of all defined logical partitions. The IOCLUSTER keyword is mutually exclusive with the PART|PARTITION and NOTPART keywords.

All LP names that you specify in the CHPID statements must match those specified in the RESOURCE statement. An IOCDS must have at least one LP name defined.

```
PARTITION={(CSS(cssid),{name|0}[,REC])|
          (CSS(cssid),access list)|
          (CSS(cssid),(access list)[,(candidate list)][,REC])|
       ((CSS(cssid),(access list)[,(candidate list)]),...)}

NOTPART={(CSS(cssid),access list)|
        ((CSS(cssid),(access list)[,(candidate list)]),...)}

IOCLUSTER=cluster_name

SHARED

CPATH=(CSS(cssid),chpid number)
```

Where:

name
specifies the name of the LP that has authority to access the CHPID. The LP name is a 1–8 alphanumeric (0–9, A–Z) character name that must have an alphabetic first character. Special characters ($, #, @) are not allowed. A reserved LP cannot have any channel paths assigned to it.

The following words are reserved and you cannot use them as LP names:
PHYSICAL
REC
SYSTEM
PRIM*nnnn* (where *nnnn* are digits)

ICP IOCP supports a maximum of 60 LP names for the CPC.

cluster_name
specifies the name of an LPAR cluster that has authority to access the specified DCM CHPID. The name of the LPAR cluster is a one- to eight- alphanumeric character name (0-9, A-Z) that must have an alphabetic first character. Special characters ($, #, @) are not allowed.

REC
specifies that the CHPID is reconfigurable. A reconfigurable CHPID must have an initial access list of one LP name. It's candidate list must consist of one or more LP names.

access list specifies the LPs that have initial access to the CHPID at the completion of the initial power-on reset. An LP name may only appear once in an access list.

You can specify that no LPs will access the channel path following LP activation for the initial POR of an LPAR IOCDS. Specifying 0 indicates a null access list.

candidate list specifies the LPs that have authority to access the CHPID. Any LP that is not in a CHPIDs candidate list cannot access the CHPID.

You may specify as many LP names as your CPC supports. However, the number of unique LP names specified in both the access list and candidate list may not exceed the number of LPs your CPC supports.

If you specify the candidate list, you do not need to specify again the LP names specified in the initial access list. The initial access list is always included in the candidate list.

An LP name can only appear once in a candidate list. If the candidate list is not specified, it defaults to all LPs in the configuration for reconfigurable and shared channels.

Note: It is highly recommended that a peer mode CHPID (CBP, CFP, CIB, or ICP) have at most one coupling facility LP specified in its initial access list in order to avoid confusion on subsequent LP activations. A peer mode CHPID can be online to only one coupling facility LP at a time.

Using the SHARED keyword specifies that the channel paths on the CHPID statement are shared. More than one LP, at the same time, can access a shared CHPID. When CHPIDs are not shared, only one LP can access it. Although you can dynamically move a reconfigurable CHPID between LPs, it can only be accessed by 1 LP at any given time. CVC and CBY channel paths (TYPE keyword) cannot be shared. On CF only models, CBP, CFP, and ICP channel paths cannot be shared.

The CPATH keyword is only valid for ICP and CIB channel paths (TYPE keyword) and required for all ICP and CIB definitions. CPATH specifies the connection between 2 ICPs at either end of a coupling link:

```
PATH=FE,TYPE=ICP,CPATH=FF,...
PATH=FF,TYPE=ICP,CPATH=FE,...
```

specifies that ICP channel path FF connects to ICP channel path FE. Every ICP channel path of a coupling facility must be connected to an ICP channel path of a z/OS LP. The connection needs to be specified for each channel path. ICP channel paths cannot connect to each other if they both have candidate lists with the same, single logical partition. Note that this prevents the definition of internal coupling channels in an LPAR configuration with only one logical partition. Also, an ICP channel path cannot connect to itself.

The CPATH value for a CIB CHPID specifies the CSS and CHPID number this CIB CHPID connects with on the target system. For example:

```
PATH=C0,TYPE=CIB,CPATH=(CSS(1),D0),...
```

Defines a CIB CHPID, C0, on this system that connects with CIB CHPID D0 in CSS 1 on the remote system.

Shared devices using shared channels

MIF allows you to use shared channels when defining shared devices. Using shared channels reduces the number of channels required, allows for increased channel utilization, and reduces the complexity of your IOCP input.

Note: You cannot mix shared and unshared channel paths to the same control unit or device.

The following is an example of an IOCDS with a shared device.

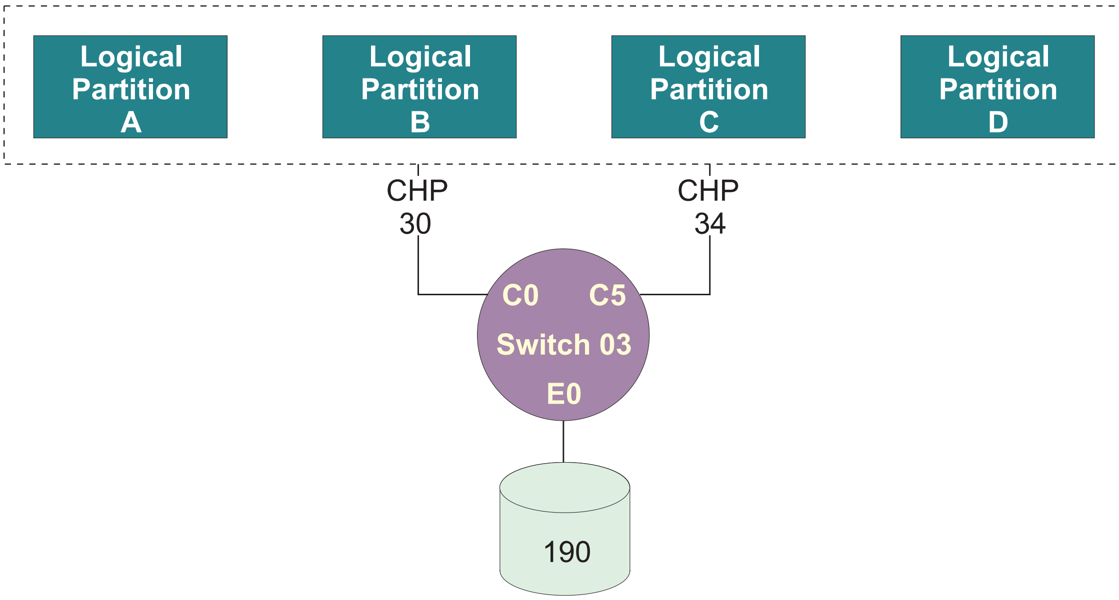


Figure 17. Shared devices using shared ESCON channels

The following is the IOCP coding for the above figure.

```
CHPID PATH=(30),TYPE=CNC,SWITCH=03,SHARED . . .
CHPID PATH=(34),TYPE=CNC,SWITCH=03,SHARED . . .
CNTLUNIT CUNUMBR=000,PATH=(30,34),UNITADD=((90)),LINK=(E0,E0),UNIT=xxx . . .
IODEVICE ADDRESS=(190),CUNUMBR=000,UNIT=xxx . . .
```

Shared devices using unshared channels

When coding an IOCP input file, the following specifications are allowed:

- Duplicate device numbers can be specified within a single IOCP input file, if device numbers are not duplicated within an LP.
- You can assign a maximum of eight channel paths from each LP to a device.

  Device sharing among LPs is accomplished by attaching multiple channel paths from each LP to a device.

The following section illustrates IOCP coding for IOCDSs when shared devices on unshared channels and duplicate device numbers are specified.

Shared devices: The following examples illustrate this concept by showing the physical connectivity of an I/O configuration for multiple LPs and the IOCP coding for the same configuration.

Using channels: Figure 18 on page 56 shows an example of an I/O configuration with a device shared by each of the four logical partitions. In this representation of a shared device, each logical partition views device 190 as part of its own I/O configuration. Notice the recoverability characteristics of this configuration: each logical partition has two channel paths to the shared device, each attached to a different storage director.

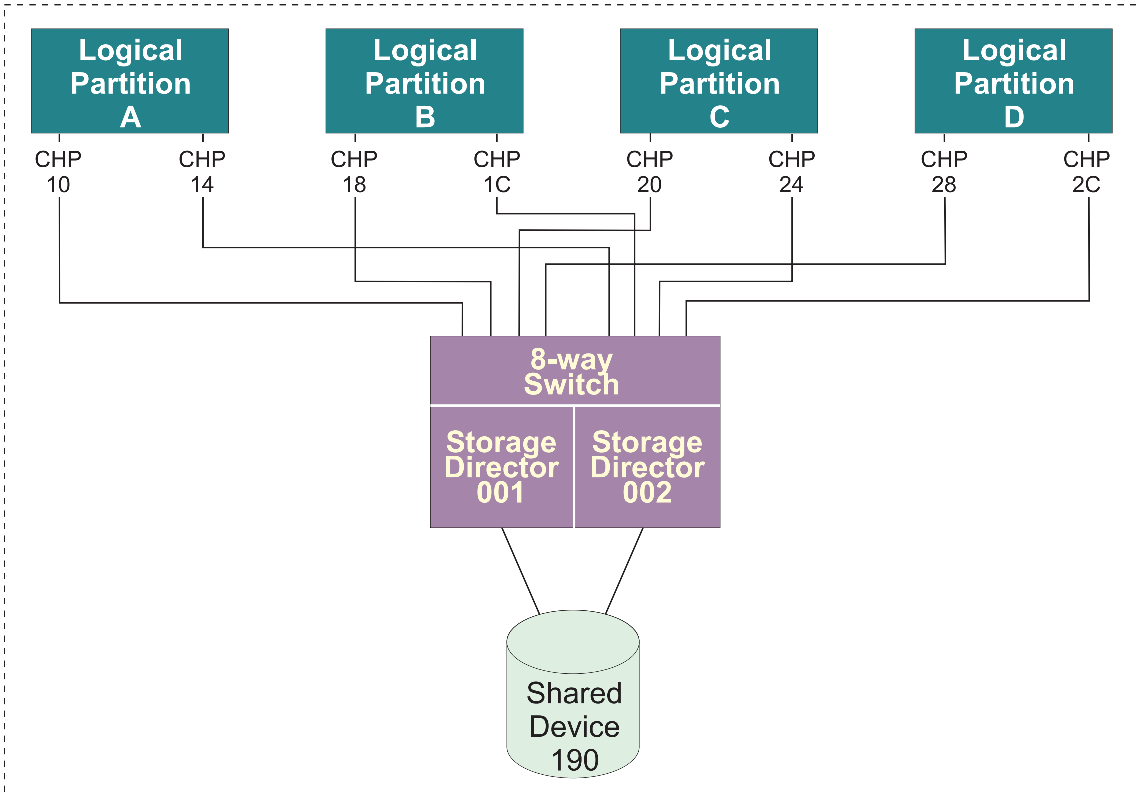


Figure 18. Physical connectivity of shared device 190

The following example shows the IOCP statement for Figure 18.

```
CHPID PATH=(10),PART=(A,REC)
CHPID PATH=(14),PART=(A,REC)
CHPID PATH=(18),PART=(B,REC)
CHPID PATH=(1C),PART=(B,REC)
CHPID PATH=(20),PART=(C,REC)
CHPID PATH=(24),PART=(C,REC)
CHPID PATH=(28),PART=(D,REC)
CHPID PATH=(2C),PART=(D,REC)
CNTLUNIT CUNUMBR=0001,PATH=(10,18,20,28),UNITADD=((90)) . . .
CNTLUNIT CUNUMBR=0002,PATH=(14,1C,24,2C),UNITADD=((90)) . . .
IODEVICE ADDRESS=(190),CUNUMBR=(0001,0002) . . .
```

If 8 or less channels attach to the device, this method of defining the IOCP input provides greater flexibility because it allows you to move CHPIDs from one LP to another and eliminates possible conflicts (see Figure 21 on page 59).

Figure 19 on page 57 shows an alternative method of defining the configuration. This method is required if there are greater than 8 paths to the device. Note that this logical representation has the same recoverability characteristics as the physical connectivity:

- Each LP has two channel paths to the shared device
- Each LP is attached to a different storage director

However, paths cannot be moved between the LPs.

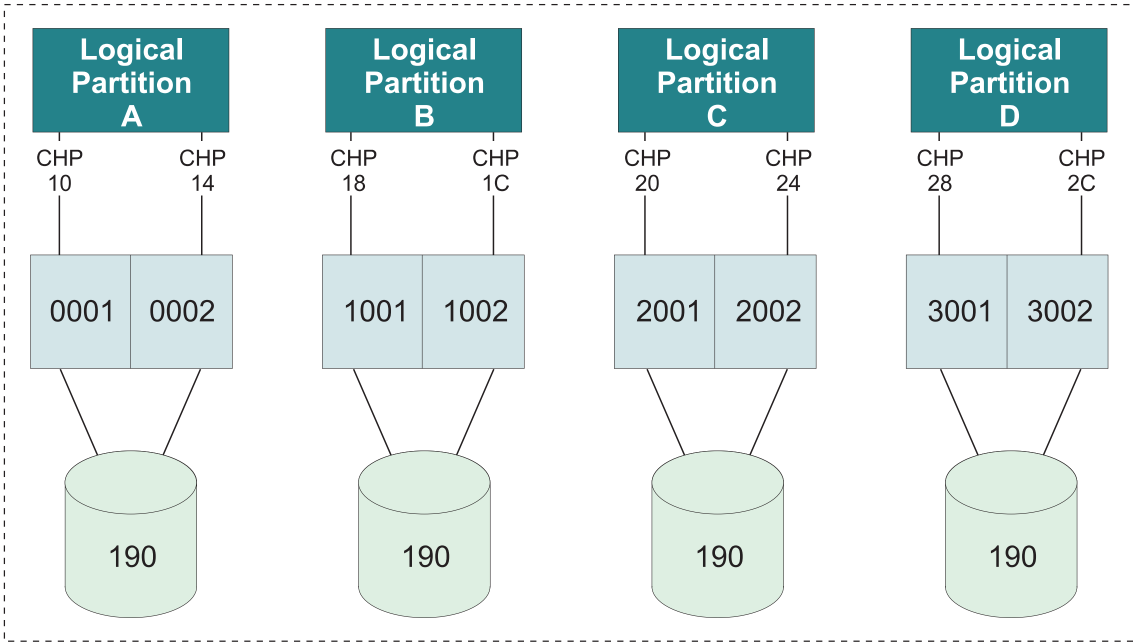


Figure 19. Logical view of shared device 190

The following example shows the IOCP statement for Figure 19.

```
CHPID PATH=(10),PARTITION=(A), . . .
CHPID PATH=(14),PARTITION=(A), . . .
CNTLUNIT CUNUMBR=0001,PATH=(10),UNITADD=((90)) . . .
CNTLUNIT CUNUMBR=0002,PATH=(14),UNITADD=((90)) . . .
IODEVICE ADDRESS=(190),CUNUMBR=(0001,0002) . . .

CHPID PATH=(18),PARTITION=(B), . . .
CHPID PATH=(1C),PARTITION=(B), . . .
CNTLUNIT CUNUMBR=1001,PATH=(18),UNITADD=((90)) . . .
CNTLUNIT CUNUMBR=1002,PATH=(1C),UNITADD=((90)) . . .
IODEVICE ADDRESS=(190),CUNUMBR=(1001,1002) . . .

CHPID PATH=(20),PARTITION=(C) . . .
CHPID PATH=(24),PARTITION=(C) . . .
CNTLUNIT CUNUMBR=2001,PATH=(20),UNITADD=((90)) . . .
CNTLUNIT CUNUMBR=2002,PATH=(24),UNITADD=((90)) . . .
IODEVICE ADDRESS=(190),CUNUMBR=(2001,2002) . . .

CHPID PATH=(28),PARTITION=(D), . . .
CHPID PATH=(2C),PARTITION=(D), . . .
CNTLUNIT CUNUMBR=3001,PATH=(28),UNITADD=((90)) . . .
CNTLUNIT CUNUMBR=3002,PATH=(2C),UNITADD=((90)) . . .
IODEVICE ADDRESS=(190),CUNUMBR=(3001,3002) . . .
```

Duplicate device numbers for different physical devices

Figure 20 on page 58 illustrates a configuration where duplicate device numbers are used to represent a console (110) and a printer (00E) within each of four logical partitions.

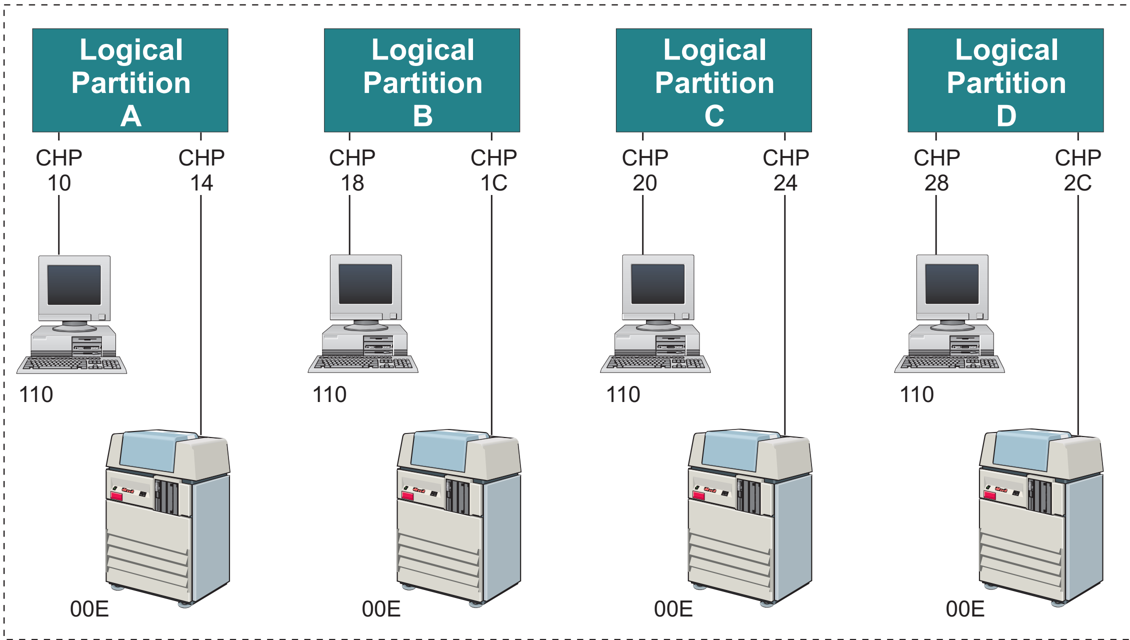


Figure 20. LPAR configuration with duplicate device numbers

The following example shows the IOCP statement for Figure 20. This IOCP coding example groups the input statements by logical partition. When coding IOCP, view the I/O devices from a logical partition perspective.

```
CHPID PATH=(10),PARTITION=(A), . . .
CHPID PATH=(14),PARTITION=(A), . . .
CNTLUNIT CUNUMBR=0011,PATH=(10),UNITADD=(10), . . .
CNTLUNIT CUNUMBR=0012,PATH=(14),UNITADD=(0E), . . .
IODEVICE ADDRESS=(110),CUNUMBR=(0011), . . .
IODEVICE ADDRESS=(00E),CUNUMBR=(0012), . . .

CHPID PATH=(18),PARTITION=(B), . . .
CHPID PATH=(1C),PARTITION=(B), . . .
CNTLUNIT CUNUMBR=0013,PATH=(18),UNITADD=(10), . . .
CNTLUNIT CUNUMBR=0014,PATH=(1C),UNITADD=(0E), . . .
IODEVICE ADDRESS=(110),CUNUMBR=(0013), . . .
IODEVICE ADDRESS=(00E),CUNUMBR=(0014), . . .

CHPID PATH=(20),PARTITION=(C), . . .
CHPID PATH=(24),PARTITION=(C), . . .
CNTLUNIT CUNUMBR=0015,PATH=(20),UNITADD=(10), . . .
CNTLUNIT CUNUMBR=0016,PATH=(24),UNITADD=(0E), . . .
IODEVICE ADDRESS=(110),CUNUMBR=(0015), . . .
IODEVICE ADDRESS=(00E),CUNUMBR=(0016), . . .

CHPID PATH=(28),PARTITION=(D), . . .
CHPID PATH=(2C),PARTITION=(D), . . .
CNTLUNIT CUNUMBR=0017,PATH=(28),UNITADD=(10), . . .
CNTLUNIT CUNUMBR=0018,PATH=(2C),UNITADD=(0E), . . .
IODEVICE ADDRESS=(110),CUNUMBR=(0017), . . .
IODEVICE ADDRESS=(00E),CUNUMBR=(0018), . . .
```

Eight IODEVICE statements are used, one for each console and one for each printer that has a duplicate device number. Device numbers 110 and 00E occur four times each; however, they are not duplicated within a logical partition. When coding an IOCP input file, remember that the unique device number rule applies for logical partitions in an IOCDS.

Figure 21 shows another example of a logical partition configuration in which the device number for a console (110) is duplicated for all four logical partitions.

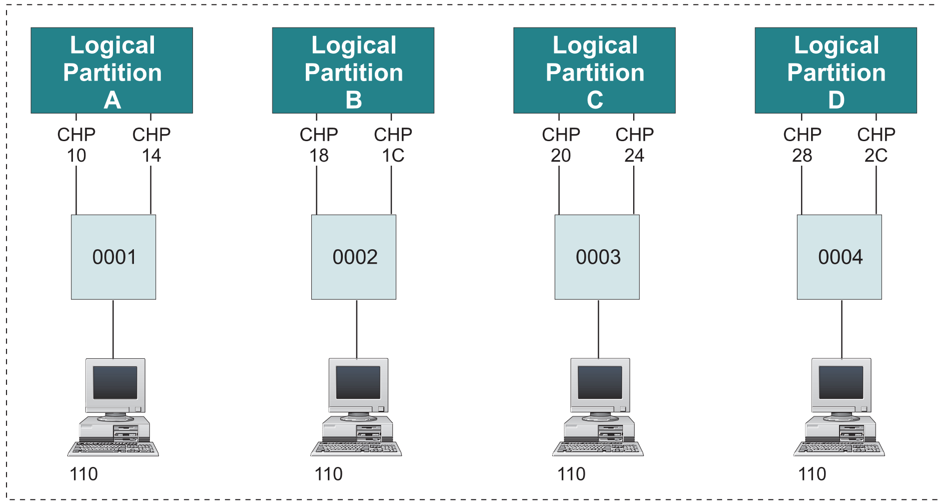


Figure 21. Duplicate device numbers for console

The following example shows the IOCP coding for the previous configuration. Four IODEVICE and four CNTLUNIT statements are used, one each for the console within each logical partition that has a duplicate device number.

```
CHPID PATH=(10),PARTITION=(A), . . .
CHPID PATH=(14),PARTITION=(A), . . .
CNTLUNIT CUNUMBR=0001,PATH=(10,14),UNITADD=((10)), . . .
IODEVICE ADDRESS=(110),CUNUMBR=(0001), . . .

CHPID PATH=(18),PARTITION=(B), . . .
CHPID PATH=(1C),PARTITION=(B), . . .
CNTLUNIT CUNUMBR=0002,PATH=(18,1C),UNITADD=((10)), . . .
IODEVICE ADDRESS=(110),CUNUMBR=(0002), . . .

CHPID PATH=(20),PARTITION=(C), . . .
CHPID PATH=(24),PARTITION=(C), . . .
CNTLUNIT CUNUMBR=0003,PATH=(20,24),UNITADD=((10)), . . .
IODEVICE ADDRESS=(110),CUNUMBR=(0003), . . .

CHPID PATH=(28),PARTITION=(D), . . .
CHPID PATH=(2C),PARTITION=(D), . . .
CNTLUNIT CUNUMBR=0004,PATH=(28,2C),UNITADD=((10)), . . .
IODEVICE ADDRESS=(110),CUNUMBR=(0004), . . .
```

Duplicate device number conflicts: IOCP allows duplicate device numbers in an IOCDS only if the duplicate device numbers do not occur in the same logical partition. Therefore, IOCP allows systems to use different logical partitions to integrate a processor complex without changing device numbers.

IOCP requires a unique device number for each device within a logical partition. When IOCP completes without error, the initial configuration contains no duplicate device number conflicts within a logical partition.

Conflicts can occur when the I/O configuration is modified. If a channel path is configured to a logical partition and devices attached to the channel path have device numbers that are already assigned in the receiving logical partition to other online channel paths, a conflict results.

When an I/O configuration is dynamically modified so the logical partition can gain access to a device not previously accessible, a device conflict can occur. The conflicts are detected when commands are processed that change the I/O configuration or when you attempt to activate the logical partition which has the device number conflict. A message displays identifying the error.

The identified device cannot be accessed while a conflict exists. Two types of conflict are possible:
- Conflicts between device numbers for the same device (a shared device)
- Conflicts between device numbers for different devices (unshared devices)

Activation fails if a duplicate device number conflict exists.

Examples of duplicate device number conflicts: Figure 22 provides two examples of duplicate device number conflict.

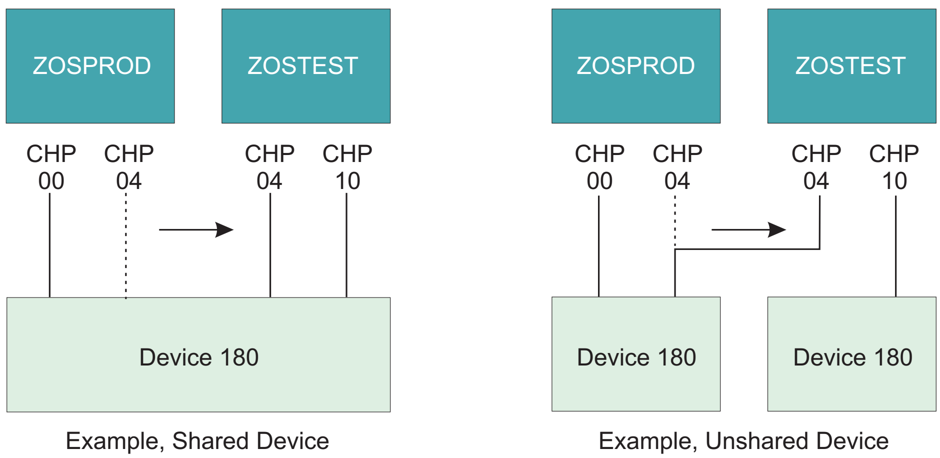


Figure 22. Two examples of duplicate device number conflicts

The following example shows the IOCP statement for Figure 22. Both examples use identical IOCP statements.

```
CHPID PATH=(00),PARTITION=(ZOSPROD,REC)
CHPID PATH=(04),PARTITION=(ZOSPROD,REC)
CNTLUNIT CUNUMBR=0001,PATH=(00,04),UNITADD=80
IODEVICE ADDRESS=180,CUNUMBR=0001

CHPID PATH=(10),PARTITION=(ZOSTEST)
CNTLUNIT CUNUMBR=0002,PATH=(10),UNITADD=80
IODEVICE ADDRESS=180,CUNUMBR=0002
```

Channel path 04 is reassigned from ZOSPROD to ZOSTEST in each example. This creates a duplicate device number conflict for device number 180 when the devices are connected to two different control units. This occurs because a device numbered 180 already exists on the original channel path 10. If such conflicts occur, the operator must know what configuration is desired.

Shared device

In the example on the left, the duplicate device numbers refer to the same device from different logical partitions (a new path to the same device has been moved to ZOSTEST). This may result in a performance problem because the control program in logical partition OS390 cannot access the device from channel path 4.

Unshared Device

In the example on the right, the duplicate device numbers refer to a different device from each logical partition (a new device has been moved to ZOSTEST). This may result in a data integrity problem because the control program in logical partition ZOSTEST cannot access the correct device from channel path 04.

Resolving duplicate device number conflicts: Consider options A, B, and C when planning the I/O configuration and the reconfigurability of channel paths. You can resolve duplicate device number conflicts by choosing one of the options:

A **Use the original channel path:**

If the receiving logical partition does not need a new path to a shared device or does not need the new (unshared) device, take no action. The conflict is resolved by using only the original path (shared device) or the original device. (Access is still allowed to any nonconflicting devices on the newly configured channel path.)

In Figure 22 on page 60 ZOSTEST can access device 180 only through channel path 10 if the operator takes no action in response to the conflict message.

B **Deconfigure the original channel path:**

If the logical partition must have the reassigned channel path to a shared device or access to a new (unshared) device, the conflict is resolved by substituting the reassigned channel path for the original channel path. Do the following:

1. Configure offline the original channel path (CHP 10 in Figure 22).
2. Configure offline and then online the reassigned channel path (CHP 04 in Figure 22).
3. If necessary, configure online the original channel path (CHP 10 in Figure 22). Another conflict message is issued because a new conflict has been created. The operator then ignores this conflict as described in option A. (Access is still allowed to any nonconflicting devices on the original channel path.)

In Figure 22, ZOSTEST can access device 180 only through channel path 04 if the preceding steps are performed in response to the conflict message.

C **Change the I/O configuration:**

Only option C provides a permanent resolution to a device number conflict.

If the logical partition must have access to all devices over the original channel path and the reassigned channel path (shared devices), or to a new device and the original device (unshared devices), do one of the following:

- Create a new configuration with unique device numbers, if they are unshared devices.
- For shared devices, define a single device with access to all of the channel paths attached to the physical control units.
- For a shared device assigned to unshared channel paths, change the channel paths to shared and consolidate the control units and device definitions to one each.
- If the device is assigned to shared channel paths, control access to the devices using their device candidate list.

The configuration can be activated by performing a POR or by performing a dynamic I/O configuration.

In Figure 22 (shared device), ZOSTEST can access device 180 through CHP 04 and CHP 10 if CHP 04 is defined to ZOSTEST in the IOCDS.

In Figure 22 (unshared device), ZOSTEST can access either device 180 (unshared device) if one or both of the devices are assigned a new device number in the IOCDS.

When a device number conflict exists, logical partitions will fail to activate. This will happen when one of the following occurs:

- The receiving logical partition was deactivated when a channel path is reassigned
- The receiving logical partition is deactivated after a channel path is reassigned

Failure to activate can result if options A or B are used. If a logical partition fails to activate, use option B or C to resolve the conflict and to activate the logical partition.

In Figure 22, if ZOSTEST is not active when CHP 04 is reassigned, or ZOSTEST is deactivated and then activated after CHP 04 is reassigned, ZOSTEST does not activate until the conflict over device 180 is resolved.

If you resolve the conflict by using option B do the following steps:

1. Establish the correct configuration by configuring offline one of the channel paths (CHP 04 or CHP 10)
2. Configure offline and then online the other channel path

If it's necessary to have access to other devices on the first channel path, the operator can configure online the first channel path while the LP is active. Ignore the messages issued at the hardware console.

The following IOCP statement example shows coding that removes duplicate device number conflicts for shared devices.

```
CHPID PATH=(00),PARTITION=(ZOSPROD,REC), . . .
CHPID PATH=(04),PARTITION=(ZOSPROD,REC), . . .
CHPID PATH=(10),PARTITION=(ZOSTEST), . . .
CNTLUNIT CUNUMBR=0001,PATH=(00,04),UNITADD=80
CNTLUNIT CUNUMBR=0002,PATH=(10),UNITADD=80
IODEVICE ADDRESS=180,CUNUMBR=(0001,0002)
```

Coupling facility planning considerations

The coupling facility provides shared storage and shared storage management functions for the sysplex (for example, high speed caching, list processing, and locking functions). Applications running on z/OS images in the sysplex define the shared structures used in the coupling facility.

The coupling facility allows applications, running on multiple z/OS images that are configured in a sysplex, to efficiently share data so that a transaction processing workload can be processed in parallel across the sysplex.

PR/SM LPAR allows you to define the coupling facility, which is a special logical partition (LP) that runs coupling facility control code. Coupling facility control code is Licensed Internal Code (LIC).

At LP activation, coupling facility control code automatically loads into the coupling facility LP from the Support Element hard disk. No initial program load (IPL) of an operating system is necessary or supported in the coupling facility LP.

Coupling facility control code runs in the coupling facility LP with minimal operator intervention. Operator activity is confined to the Operating System Messages task. PR/SM LPAR limits the hardware operator controls usually available for LPs to avoid unnecessary operator activity.

Coupling facility channel hardware provides the connectivity required for data sharing between the coupling facility and the CPCs directly attached to it. Coupling facility channels are point-to-point connections that require a unique channel definition at each end of the channel. See “Coupling facility channels” on page 76.

Test or migration coupling configuration

You can run a test or migration coupling facility to test and develop data sharing applications. You can define a test or migration coupling facility LP on the same CPC where other LPs are:
- Running z/OS images connected to the coupling facility
- Running non-coupled production work

A single CPC configuration has the following considerations:
- Simultaneous loss of the coupling facility and any z/OS images coupled to it (a more likely possibility in a single CPC configuration) can potentially cause extended recovery times

You can define a test or migration coupling facility with or ***without*** coupling facility channel hardware. See “Defining internal coupling channels (TYPE=ICP)” on page 81 for information on how to define a test or migration facility ***without*** coupling facility channel hardware.

CFCC Enhanced Patch Apply

With the CFCC Enhanced Patch Apply, you can perform a disruptive install of new CFCC code on a *test* CF and run it, while a *production* CF image in the same CEC remains at the base CFCC code level. Then when the test CF is successful, the new CFCC code can be installed on the production CF. Both installs can be done without a Power On Reset (POR) of the CEC.

Production coupling facility configuration

IBM recommends that you run your production applications on a sysplex that uses a production coupling facility configuration.

A properly configured production coupling facility configuration can reduce the potential for extended recovery times, achieve acceptable performance, and maximize connectivity to the coupling facility.

For production configurations, the use of one or more dedicated Coupling Facility engines is recommended; shared Coupling Facility engines are strongly discouraged. For more information, see the Important Note on page 119.

Production coupling facility configuration for full data sharing

The preferred solution for a full data sharing (IMS™, DB2®, VSAM/RLS) production parallel sysplex is a coupling facility configuration that consists of:

- One stand-alone coupling facility running as a single dedicated coupling facility LP to provide large capacity shared storage and maximum coupling facility channel connectivity (up to 64 coupling facility channels).
- A second stand-alone coupling facility, similarly configured, to reduce the possibility of a single point of failure. A second stand-alone coupling facility improves application subsystem availability by allowing fast recovery from one coupling facility to the other in the event of a coupling facility outage. Alternatively, an Internal Coupling Facility (ICF) feature can be used to provide the backup coupling facility. See "Internal Coupling Facility (ICF)" on page 65.

Notes:

1. The backup CF in the configuration must provide sufficient storage, processor, and connectivity resources to assume the workload of the other production CF in the event of its failure.
2. With the use of System-Managed CF Structure Duplexing for all relevant data sharing structures, it is possible to have a production data-sharing configuration that uses only 2 or more internal CFs, because duplexing avoids the "single point of failure" failure-isolation issue.

Production coupling facility configuration for resource sharing

A viable solution for a resource sharing (XCF Signaling, Logger Operlog, RACF®, BatchPipes®, Logger Logrec, Shared Tape, GRS, WLM Enclave Support, LPAR Clusters) production level parallel sysplex is a coupling facility configuration that consists of:

- One dedicated ICF provides reduced cost of ownership without compromising sysplex availability or integrity.
- A second dedicated ICF reduces the possibility of a single point of failure. A second ICF improves application subsystem availability by allowing fast recovery from one coupling facility to the other in the event of a coupling facility outage.

Note: The backup CF in the configuration must provide sufficient storage, processor, and connectivity resources to assume the workload of the other production CF in the event of its failure.

These configurations offer the best performance, the best reliability, availability, and serviceability (RAS).

Internal Coupling Facility (ICF)

You can purchase and install one or more ICF features for use in coupling facility LPs. With this feature, the coupling facility runs on special ICF CPs that no customer software can utilize. This allows the coupling facility function to be performed on the CPC without affecting the model group and thus without impacting software licensing costs for the CP resources utilized by the coupling facility. See “Considerations for coupling facilities using Internal Coupling Facility (ICF) CPs” on page 119.

These features are ordered separately, and are distinguished at the hardware level from any general purpose CPs, Integrated Features for Linux (IFLs), IBM System z10 Application Assist Processor (zAAPs) features, and System z10 Integrated Information Processor (zIIPs). ICFs, IFLs, zAAPs, or zIIPs are perceived by the system as multiple resource pools.

With the CFCC Enhanced Patch Apply process, you can perform a disruptive install of new CFCC code on an ICF image by simply deactivating and then reactivating the CF image, without the much greater disruption of a Power On Reset (POR) of the entire CEC that contains the CF image. This greatly improves the availability characteristics of using ICFs.

Coupling facilities that reside on the same CEC as one or more z/OS parallel sysplex logical partitions are ideal for coupling resource sharing sysplexes (sysplexes that are not in production data sharing with IMS, DB2 or VSAM/RLS). You can simplify systems management by using XCF structures instead of ESCON CTC connections.

IBM does not recommend use of coupling facilities that reside on the same CEC as one or more z/OS parallel sysplex logical partitions for most coupling facility structures involved in data sharing because of the possibility of *double outages* involving the simultaneous loss of a coupling facility image and one or more z/OS system images that are using the coupling facility for data sharing. Depending on the structure, a double outage can result in a significantly more involved recovery than a single outage of either a coupling facility image or a z/OS image in isolation from one another.

With the use of System-Managed CF Structure Duplexing for all relevant data sharing structures, it is possible to have a production data-sharing configuration that uses only 2 or more internal CFs, because duplexing avoids the “single point of failure” failure-isolation issue.

ICFs on stand-alone coupling facilities need configuration planning to account for storage and channels. ICFs will likely increase storage requirements for the CPC with an ICF installed, especially if software exploits the coupling facility to provide additional function not available except when running a coupling facility in a parallel sysplex.

The following table indicates the maximum number of ICFs that you can install on a given model.

CPC model	Maximum number of ICF’s supported
System z10 BC Model E10	10

CPC model	Maximum number of ICF's supported
System z10 EC	
Model E12	12
Model E26	16
Model E40	16
Model E56	16
Model E64	16

Dynamic Coupling Facility Dispatching (DCFD)

With DCFD, the coupling facility uses CP resources in a shared CP environment efficiently, making a coupling facility using shared CPs an attractive option as a back-up coupling facility. Without DCFD, a coupling facility using shared CPs would attempt to get all the CP resource it could even when there was no real work for it to do. With dynamic coupling facility dispatching, the coupling facility monitors the request rate that is driving it and adjust its usage of CP resource accordingly. If the request rate becomes high enough, the coupling facility reverts back to its original dispatching algorithm, constantly looking for new work. When the request rate lowers, the coupling facility again becomes more judicious in its use of CP resource.

This behavior plays well into a hot-standby back-up coupling facility role. In back-up mode, the coupling facility will have a very low request rate so it will throttle back to very low CP usage. In this mode, the requests themselves will experience some elongation in response time but this will not adversely affect the performance of the overall system. Since the coupling facility is not consuming more CP resource than it needs to, you can now set the processor weights for the coupling facility to a value high enough to handle the load if the coupling facility was to take over for a failing primary coupling facility. If the primary coupling facility does fail, the requests can be moved immediately to the back-up coupling facility which can then get the CP resource it needs automatically with properly defined LP weights.

Dynamic coupling facility dispatching is particularly useful in configurations where less than one CP of capacity is needed for the back-up coupling facility's use. Dynamic coupling facility dispatching is automatically enabled for any coupling facility LP that uses shared CPs, except for stand-alone coupling facilities. To enable dynamic coupling facility dispatching on stand-alone coupling facilities, use the DYNDISP coupling facility control code command. See "Coupling facility control code commands" on page 72. It is recommended that anytime a shared processor is used for a coupling facility, whether standalone or ICF processors, that DCFD be enabled by insuring that the DYNDISP coupling facility control command be set to ON.

Note: It is only for the first activation of a CF logical partition that the DCFD is to be automatically enabled. Once it is activated, the DYNDISP setting is recorded in the policy file for that CF logical partition. The DYNDISP setting is to be preserved and the subsequent activations are based on the DYNDISP setting recorded in the CF policy file. So, if the CF image profile is updated later to use shared CPs, the DCFD will not be automatically enabled. It needs to be enabled using the DYNDISP coupling facility control code command.

Coupling Facility Configuration	All Dedicated CPs or ICF(s)	Shared ICF	Shared CP	Shared ICF
CF Model	-	System z10 with only ICF processors	System z10 with 1 or more general purpose CPs	System z10 with 1 or more general purpose CPs
Dynamic Dispatching Default Value	Off	Off	On	Off

System-managed coupling facility structure duplexing

A set of parallel sysplex architectural extensions is provided for support of *system-managed* duplexing of coupling facility structures for high availability. All three structure types, cache, list, and locking, can be duplexed using this architecture.

Benefits of system-managed CF structure duplexing include:

- **Availability:** Faster recovery of structures by having the data already in the second CF.
- **Manageability and Usability:** A consistent procedure to set up and manage structure recovery across multiple exploiters
- **Cost Benefits:** Enables the use of non-standalone CFs (for example, ICFs) for all resource sharing and data sharing environments.

Preparations for CF duplexing include the requirement to connect coupling facilities to one another with coupling links. The required CF-to-CF connectivity is bi-directional, so that signals may be exchanged between the CFs in both directions. A single peer-mode coupling link between each pair of CFs can provide the required CF-to-CF connectivity; however, for high availability at least two peer-mode links between each pair of CFs are recommended.

Note that while peer-mode CHPIDs cannot be shared between multiple coupling facility images, they can be shared between a single coupling facility image and one or more z/OS images. With this sharing capability, a single peer-mode ISC-3 or ICB link can serve both as a z/OS-to-CF link and as a CF-to-CF link, and thus provide the connectivity between z/OS and CF partitions as well as the connectivity between CFs that is required for CF Duplexing. Of course, at least two such links is recommended for high availability. In addition IFB links can provide the ability to actually share the same physical link between multiple CF images. By defining multiple CHPIDs on the same physical IFB link, the individual CHPIDs can be defined for a single CF image while the physical link is being shared by multiple CF images.

Coupling Facility Level 16 duplexing enhancements

Prior to Coupling Facility Control Code (CFCC) Level 16, System-Managed Coupling Facility (CF) Structure Duplexing required two duplexing protocol exchanges to occur synchronously during processing of each duplexed structure request. CFCC Level 16 allows one of these protocol exchanges to complete asynchronously. This allows faster duplexed request service time, with more benefits when the Coupling Facilities are further apart, such as in a multi-site Parallel Sysplex.

Single CPC software availability sysplex

For single CPC configurations, System z10 models can utilize an ICF to form a single CPC sysplex, providing significant improvement in software continuous operations characteristics when running two z/OS LPs in data-sharing mode versus one large z/OS image. For these configurations, overall RAS is improved over that provided by a single z/OS image solution. Hardware failures can take down the entire single CPC sysplex, but those failures are far less frequent than conditions taking down a software image, and planned software outages are the predominant form of software image outages in any case. Forming a single CPC sysplex allows software updates to occur in a "rolling" IPL fashion, maintaining system availability throughout. An LPAR cluster is one example of a single CPC sysplex which has significantly improved system availability over a single LP. For additional benefits provided by an LPAR cluster using IRD technology, see redbook *z/OS Intelligent Resource Director*, SG24-5952.

Coupling facility nonvolatility

Continuous availability of the transaction processing workload in a coupling facility configuration requires continuous availability of the shared structures in the coupling facility. To help ensure this, you must provide an optional backup power supply to make coupling facility storage contents nonvolatile across utility power failures.

Nonvolatility choices

The following table indicates the optional nonvolatility choices available and their capabilities:

Table 7. Nonvolatility choices for coupling facility LPs

Nonvolatility Choices	z10 BC	z10 EC
Uninterruptible power supply (UPS) (See Notes[1])	Yes	Yes
Internal Battery Feature (IBF)	Yes	Yes
Local Uninterruptible Power Supply (LUPS) (See Notes[2])	Yes	Yes

Notes:

1. Optional uninterruptible power supply (UPS) provides a secondary power source for use during extended utility power outages allowing continuous coupling facility operation.
2. The optional Local Uninterruptible Power Supply supports 0 to 18 minutes of full power operation.

Setting the conditions for monitoring coupling facility nonvolatility status

In addition to installing an optional backup power supply to help ensure continuous availability, you **must** also set the conditions by which the coupling facility determines its volatility status. Software subsystems with structures defined in the coupling facility can monitor this status. Use the coupling facility control code MODE command as follows:

- MODE NONVOLATILE sets coupling facility volatility status to nonvolatile and should be used if a floor UPS is available to the CPC. Coupling facility control code does **not** monitor the installation or availability of UPS but maintains a nonvolatile status for the coupling facility.
- MODE VOLATILE sets coupling facility volatility status to volatile and should be used if no backup power supply is installed and available. Coupling facility control code maintains volatile status for the coupling facility even if a backup power supply is installed and available.

The coupling facility MODE setting is saved across power-on reset and activation of the coupling facility. You can use online help from the Operator Messages panel to get additional information on coupling facility control code commands.

Coupling facility mode setting

The following table summarizes the relationship between the coupling facility MODE setting, and the resulting conditions you can expect if utility power fails at your site.

Table 8. Coupling facility mode setting

CF MODE setting	Local UPS or IBF installed	Results on Utility Power Failure
VOLATILE	Yes	Ride out utility power failure on UPS/IBF. (Setting the mode to VOLATILE here would be a configuration error because there is local UPS or IBF to provide nonvolatility.)
VOLATILE	No	Machine down unless alternate floor level UPS/IBF provided.
NONVOLATILE	Yes	Ride out utility power failure on UPS/IBF.
NONVOLATILE	No	Machine down unless alternate floor level UPS/IBF provided. **Note:** This is the recommended setting when providing floor-wide UPS/IBF backup.
Note: Reflects the real time status of the power (volatile or nonvolatile).		

Coupling facility LP definition considerations

You can define coupling facility mode for an LP at the Hardware Management Console or Support Element console using the Activation Profiles task available from the CPC Operational Customization Tasks Area.

You can define coupling facility LPs with shared or dedicated CPs on all System z10 models. Coupling facility LPs must be defined with at least 128 MB of central storage. See Table 12 on page 102.

Coupling facility LPs do ***not*** support some LP definition controls typically available to other LPs. For coupling facility LPs, you ***cannot*** define:

- Reserved central storage (coupling facility LPs do ***not*** support dynamic storage reconfiguration)
- Expanded storage initial or reserved amounts or expanded storage origin
- Crypto Express2 Coprocessors or Crypto Express2 Accelerators
- Automatic load
- Automatic load address
- Automatic load parameters

Internal Coupling Facility (ICF)

You can install one or more internal coupling facility (ICF) features. See “Considerations for coupling facilities using Internal Coupling Facility (ICF) CPs” on page 119.

Coupling facility LP storage planning considerations

You must define at least 128 MB of central storage for a coupling facility LP to activate.

This storage is reserved for coupling facility control code use and ***cannot*** be used for other purposes. Minimum storage size for coupling facilities is ***primarily*** a function of the coupling facility control code level. This implies that, over time, the minimum storage size required by a coupling facility on a particular machine can grow as new coupling facility control code updates are applied.

You must also define additional storage to accommodate the shared structures and dump space used by software subsystems using the coupling facility.

If a hot standby back-up coupling facility is defined, you must allocate to the back-up coupling facility all the storage required by that coupling facility to handle the structures it may need to hold in an active takeover role. Storage resources for coupling facility LPs are static and must be allocated at LP activation time of the coupling facility LP.

Structures, dump space, and coupling facility LP storage

A coupling facility allocates storage for structures and for dump space based on values specified in the SIZE, INITSIZE, and DUMPSPACE parameters of the coupling facility resource management (CFRM) policy used for the coupling facility.

Structures consist of control objects and data elements. The control objects include entries and a variety of other control structures used to manipulate the entries. The data elements store user data associated with structure entries.

Dump space is storage in the coupling facility set aside for use as a dump table when a structure dump is taken. Dump tables are used for application development and problem determination purposes.

The following table indicates the maximum central storage possible for the System z10 models:

Table 9. Maximum central storage for System z10 models

Models	Maximum Central Storage (GB)
System z10 BC Model E10	120
System z10 EC Model E12 Model E26 Model E40 Model E56 Model E64	 352 752 1136 1520 1520

Note: The maximum single partition size is 1 TB (1024 GB).

Estimating coupling facility structure sizes

Estimating coupling facility structure sizes is useful to system programmers to help ensure that there is enough coupling facility storage to meet application needs. The estimation of the minimum central storage requirements of your List or Cache structure has been superseded by the following two commands used by the CFSizer Utility to make space calculations in the coupling facility:

- **Compute list-structure parameters:** For computing the minimum central storage requirements for a List structure. (What z/OS calls *lock structures* are actually a special form of list structure.)
- **Compute cache-structure parameters:** For computing the minimum central storage requirements for a Cache structure.

IMPORTANT NOTE

When implementing a new CFLEVEL in your configuration, redetermine the size of List and Cache structures using the CFSizer Utility and update the CFRM policy with the newly acquired values. For more information on the CFSizer Utility, see the following link:

http://www.ibm.com/systems/support/z/cfsizer/

Dump space allocation in a coupling facility

Dump space is storage you define using the DUMPSPACE parameter in the coupling facility resource management (CFRM) policy. It is set aside for the creation of dump tables. Dump tables are portions or snapshots of a structure typically saved for application development or problem determination purposes. The coupling facility allocates dump space in multiples of the coupling facility storage increment.

Dump tables for several different structures can exist in dump space at the same time. The amount of storage in any one dump table depends on the following factors:

- Amount of information you want to save to a dump table

  The software subsystem can request the portions of a structure that are to be captured in the dump table. For example, lock tables, lists within a list structure, or directory entries belonging to particular storage classes or castout classes.
- Free dump space

  Structures share dump space. If a structure is using some of the dump space, other structures cannot use that portion of the dump space until it is released.
- Characteristics of the structure saved to a dump table

  When saving structure objects to a dump table, the amount of dump space used depends on the parameters specified for the structure. For example, list entry size, the number of list entries in a specified list, the number of directory entries in a castout class, whether adjunct data is included, etc.

The coupling facility can return the maximum requested dump space value. This indicates the largest amount of dump space requested by the software subsystems using the coupling facility. This value allows you to adjust the amount of allocated dump space to better match actual usage.

Coupling facility LP activation considerations

At LP activation, coupling facility control code automatically loads into the coupling facility LP from Support Element hard disk. No initial program load (IPL) of an operating system is necessary or supported in the coupling facility LP.

All coupling facility channel path types targeted to be brought online will automatically be configured online.

Note: All channel paths types that are targeted to be brought online will automatically be configured online if the coupling facility LP is redefined as an ESA mode LP.

Coupling facility shutdown considerations

> **IMPORTANT NOTE**
>
> It is important to properly remove all structures from a coupling facility that will be permanently taken out of the sysplex prior to shutting down the coupling facility. Failure to remove all structures may result in a pending condition (or transitioning structure) when attempting to allocate structures in a new coupling facility. Reactivation of the old coupling facility may be required to resolve the condition.

A running coupling facility LP can contain structures and data important to a sysplex. Make sure that you take proper precautions to preserve these structures and data ***prior to*** a power off, power-on reset (POR), LP deactivation, or shutdown (using the coupling facility control code SHUTDOWN command) of the coupling facility LP. Coupling facility structures and data will ***not*** survive any of these actions. Loss of coupling facility structures and data will occur regardless of the volatility state of the coupling facility including situations where a battery backup is in place.

It is recommended to use the coupling facility SHUTDOWN command to shut down a CF image, because it performs a check to make sure that there are no allocated structure instances in the CF before proceeding to shut down the coupling facility.

For more information on removing, replacing, or shutting down a coupling facility, see *z/OS MVS Setting Up a Sysplex*, SA22-7625.

Coupling facility LP operation considerations

Coupling facility control code runs in the coupling facility LP with minimal operator intervention. Operator activity is confined to the Operating Systems Messages task. PR/SM LPAR limits the hardware operator controls usually available for LPs to avoid unnecessary operator activity.

Coupling facility LPs only support the following tasks typically available to the hardware console operator:
- Activate
- Deactivate
- Operating System Messages

Coupling facility control code commands

Coupling facility control code does provide a limited set of hardware operator controls unique to the coupling facility LP. These controls are available from the Operating System Messages panel. From this panel, you can enter the HELP command to display coupling facility control code command syntax.

Coupling facility control code provides the following commands for use in the coupling facility LP:
- CONFIGURE (configure coupling facility channel paths online or offline)
- CP (configure a central processor online or offline)
- DISPLAY (display coupling facility resource information)

- DYNDISP (turn dynamic coupling facility dispatching on or off for a coupling facility LP). See “Dynamic Coupling Facility Dispatching (DCFD)” on page 66.
- HELP (display coupling facility control code command syntax)
- MODE (define coupling facility volatility mode)
- SHUTDOWN (shutdown coupling facility operation)
- TIMEZONE (sets timezone offset from Greenwich Mean Time for a coupling facility)
- TRACE (sets or modifies tracing options)

Notes:

1. Support for the CP and HELP coupling facility control code commands is available on all System z10 models.
2. The settings established using DYNDISP, MODE and TIMEZONE commands are recorded in the policy file for the coupling facility. As a result, all values are persistent across resets, deactivations, and reactivations.

Coupling facility level (CFLEVEL) considerations

To support migration from one coupling facility level to the next, you can run different levels of the coupling facility concurrently as long as the coupling facility LPs are running on different CPCs. CF LPs running on the same CPC share the same coupling facility control code EC level.

When migrating CF levels, lock, list, and cache structure sizes might need to be increased to support new function. The amount of space needed for the current CFCC levels must be redetermined by visiting the CFSizer tool at http://www.ibm.com/systems/support/z/cfsizer/.

CPC support for coupling facility code levels

The following table summarizes CPC support for the different coupling facility code levels.

Table 10. CPC support for coupling facility code levels

CPC models	Coupling facility code level				
	Level 16	Level 15	Level 14	Level 13	Level 12
2098 z10 BC	EC N10964 (Ver 2.10.1) MCL 009	EC F85900 (Ver 2.10.0) MCL 006	NA	NA	NA
2097 z10 EC	EC N10964 (Ver 2.10.1) MCL 009	EC F85900 (Ver 2.10.0) MCL 006	NA	NA	NA
2096 z9 BC	NA	EC G40953 (Ver 2.9.2) MCL 011	EC J99670 (Ver 2.9.1) MCL 008	NA	NA
2094 z9 EC	NA	EC G40953 (Ver 2.9.2) MCL 011	EC J99670 (Ver 2.9.0) MCL 008	NA	NA
2084 z990	NA	NA	EC J13481 (Ver 1.8.2) MCL 026	EC J13481 (Ver 1.8.2) MCL 003	EC J12555 (Ver 1.8.0) MCL 007
2086 z890	NA	NA	EC J13481 (Ver 1.8.2) MCL 026	EC J13481 (Ver 1.8.2) MCL 003	NA

Notes:

1. Previous machine types that support the coupling facility are included for completeness and sysplex connectivity purposes.
2. The (Ver n.n.n) refers to the version of code installed in the Support Element. You can verify what version code you have by looking at the title bar on the Workplace window of your Support Element.
3. All MCLs cited in the table are current as of the publication date of this edition and can be superseded by later MCLs. The MCLs cited in the table are the latest service levels as of the current publication date of this edition. They do not necessarily reflect the minimum service level required for a particular CFLEVEL but rather the recommended service level. For the latest EC and MCL information, use IBM Service Link to view the appropriate PSP bucket subset ID for hardware and software maintenance information. The most current CPC Support for CFCC table can be found online at http://www1.s390.ibm.com/products/pso/cftable.html

Level 16 coupling facility

A level 16 coupling facility (CFLEVEL=16) provides the following enhancements:

- Latch Fairness provides more consistent response time from CF requests.
- CF structure expansion/contraction/reapportionment performance enhancement for list structures.
- Coupling Facility Duplexing Protocol Enhancements. This provides faster service time when running System-Managed CF Structure Duplexing by allowing one of the duplexing protocol exchanges to complete asynchronously. More benefits are seen as the distance between the CFs becomes larger, as in a multi-site Parallel Sysplex.
- CF subsidiary list notification enhancements, to avoid false scheduling overhead for Shared Message Queue CF exploiters.

Important Note

CF structures allocated in a CFLEVEL 16 coupling facility may need to be significantly larger than in previous CFLEVELs, in order to be allocated with a similar number of usable structure objects. It is highly recommended to use the CFSIZER tool for this: http://www.ibm.com/systems/support/z/cfsizer/.

CPC Support: See Table 10 on page 74 for a listing of the CPCs that support a level 16 coupling facility.

Level 15 coupling facility

A level 15 coupling facility (CFLEVEL=15) provides the following enhancements:

- Granular CF CPU Accounting by Structure
- System-Managed CF Structure Duplexing protocol enhancements (these enhancements have not been enabled by z/OS software)
- CFCC STP support
- CFCC multitasking enhancements (112 CF tasks) and associated CF storage management changes

Important Note

CF structures allocated in a CFLEVEL 15 coupling facility may need to be significantly larger than in previous CFLEVELs, in order to be allocated with a similar number of usable structure objects. It is highly recommended to use the CFSIZER tool for this: http://www.ibm.com/systems/support/z/cfsizer/.

CPC Support: See Table 10 on page 74 for a listing of the CPCs that support a level 15 coupling facility.

Level 14 coupling facility

A level 14 coupling facility (CFLEVEL=14) provides the following enhancement:

- CFCC Dispatcher Enhancements

CPC Support: See Table 10 on page 74 for a listing of the CPCs that support a level 14 coupling facility.

Level 13 coupling facility

A level 13 coupling facility (CFLEVEL=13) provides the following enhancement:

- Performance enhancements for Castout

CPC Support: See Table 10 on page 74 for a listing of the CPCs that support a level 13 coupling facility.

Software Corequisites: For a list of the software levels that exploit the function and levels that can coexist with CFLEVEL=13, see the “Summary of CFLEVEL Functions” section of the *z/OS MVS Setting Up a Sysplex* document.

Level 12 coupling facility

Enhancements: A level 12 coupling facility (CFLEVEL=12) provides the following enhancements:

- 64-bit CFCC support; removal of the 2 GB control store limit, and removal of the distinction between control and non-control store
- 48 concurrent tasks
- Support for Message Timing Ordering providing enhanced scalability of parallel sysplex.
- System-Managed Coupling Facility (CF) Duplexing
- Cache structure architecture extensions for Batch Write, Castout, and Cross-Invalidate functions
- Support for > 15 LPs
- Support for MCSS

CPC Support: See Table 10 on page 74 for a listing of the CPCs that support a level 12 coupling facility.

Software Corequisites: For a list of the software levels that exploit the function and levels that can coexist with CFLEVEL=12, see the "Summary of CFLEVEL Functions" section of the *z/OS MVS Setting Up a Sysplex* document.

Coupling Facility Resource Management (CFRM) policy considerations

To define how to manage z/OS images and coupling facilities in the sysplex, you must specify hardware configuration information in the coupling facility resource management (CFRM) policy as follows:

- Coupling facility node descriptor information

  You must identify each coupling facility in the sysplex and the processor complex on which it is running. To do so, you must specify the following information in the CFRM policy:

CFRM parameter	Description
PLANT	Plant of manufacture
SEQUENCE	Machine sequence number
SIDE	Machine side
TYPE	Machine type
MFG	Manufacturer
CPCID	CPC identifier

  This information is available on the CPC Details panel. You can access the CPC Details panel by opening the CPC object that is running the coupling facility LP.
- LP information for the coupling facility

  For a coupling facility residing on a System z10 model, the partition ID specified on the activation profile for the CF image on the Support Element or hardware master console must match the number specified in the PARTITION keyword of the CF statement in the policy information defined in the CFRM policy. IBM recommends that the LP names for the CF LPs in IOCP input files match the names used in the NAME keyword in the CF statement in the CFRM policy.

  You can find the LP names in either the IOCP or HCD reports.

Coupling facility channels

Coupling facility channels are System z10 channels that use fiber optic cables (CFP channel paths), the channel subsystem's self-timed interface (STI) cables (CBP channel paths), an InfiniBand host channel adapter (HCA) (CIB channel paths), or internal memory bus (ICP channel paths) to provide the connectivity for data sharing between a coupling facility and the central processor complexes (CPCs) or logical partitions (LPs) directly attached to it.

The class of CHPIDs, known as peer mode channels, provide both sender and receiver capability on the same link. Peer mode links come in these varieties: Internal Coupling channels (TYPE=ICP), Integrated Cluster Bus channels (TYPE=CBP), InfiniBand (TYPE=CIB), and ISC-3 links (TYPE=CFP). Each ICP, CBP, CIB, and CFP channel can be configured as an unshared channel path to a single coupling facility or z/OS image, or as a shared channel path among several z/OS images and one coupling facility image.

Note: The following bulleted items only describe z/OS to coupling facility connections. However, they also apply to coupling facility duplexing connections (CF to CF).

Coupling facility channels:

- Require a point-to-point connection (direct channel attach between a CPC or LP and a coupling facility). Internal Coupling channels can only be used to connect a coupling facility and LPs on the same CPC.
- Can be used to connect a coupling facility to other LPs on the same CPC when a coupling facility is one of multiple LPs running on a single CPC. Internal coupling channels should be used for these connections.
- Can be redundantly configured (two or more coupling facility channels from each CPC involved in coupling facility data sharing) to enhance availability and avoid extended recovery time. This does not apply to Internal Coupling channels.
- Require ICP, CBP, CIB, or CFP channel path definition at the coupling facility end of a coupling facility channel connection.
- Require ICP, CBP, CIB, or CFP channel path definition at the z/OS (and, for System-Managed CF Structure Duplexing, the coupling facility) end of a coupling facility channel connection.
- Require a CBP, CFP, CIB, or ICP channel path be connected to a CBP, CFP, CIB, or ICP channel path, respectively. You must define the ICP channel paths in pairs and you must connect each pair. You connect an ICP channel path to an ICP channel path by specifying the CPATH keyword on the CHPID statement for every ICP channel path.

Internal Coupling channel

The Internal Coupling channel emulates the coupling facility functions in LIC between images within a single system. Internal Coupling channel implementation is totally logical requiring no channel or even cable hardware. However, a CHPID number must be defined in the IOCDS. Internal Coupling channels cannot be used for coupling connections to images in external systems.

Partitions with Internal Coupling channels can also have coupling facility channels which allow external system coupling. ICs, which utilize the system bus, are extremely fast (approximately 6 GB/second).

Internal Coupling channels will have channel path type of ICP (Internal Coupling Peer). Internal Coupling channels are identified by 2 CHPIDs representing the two ends of a coupling link. The rules that apply to the ICP CHPID type are the same as those which apply to external coupling link types, with the exception that the following functions are not supported:

- Service On/Off
- Reset I/O Interface
- Reset Error Thresholds

- Swap Channel Path
- CHPID Reassign
- Channel Diagnostic Monitor
- R/V
- Configuration Manager Vital Product Data (VPD)

Internal coupling channels have improved coupling performance over ICBs and coupling facility channels.

Integrated cluster bus channels

Integrated cluster bus channels (ICBs) are coupling facility channels that use the channel subsystem's self-timed interface (STI) cables to provide the connectivity for data sharing between a coupling facility and the CPCs or LPs directly attached to it. This allows an integrated cluster bus channel to use most of the high bandwidth of the STI bus.

Additionally, the improved data rate made possible by the integrated cluster bus channel's superior bandwidth enhances performance by reducing the latency of synchronous send messages and CP idle time which results in improved workload throughput.

Integrated cluster bus channels:

- Require CBP channel path definition (coupling facility peer channel capability) at the coupling facility end of a coupling facility channel connection. CBP channel paths are defined for ICB-4 links.
- Require CBP channel path definition (coupling facility peer channel capability) at the z/OS (and, for System-Managed CF Structure Duplexing, the coupling facility) end of a coupling facility channel connection. CBP channel paths are defined for ICB-4 links.
- Each CBP channel path must be connected to another CBP channel path. ICB-4 links are defined as CBP channel paths. However, it is further required that an ICB-4 link be connected to another ICB-4 link.

Summary of CPC Support for Integrated Cluster Bus Channels: Integrated cluster bus channels are optional on System z10 models.

Note: ICB-4 links are **not** supported on System z10 Model E64.

ISC-3 Links

ISC-3 links (TYPE=CFP channel paths) process coupling facility requests.

InfiniBand host channel adapter (HCA)

An InfiniBand host channel adapter (HCA) can be used for a coupling link between a z/OS image and a coupling facility (CF) image. The IOP wraps the coupling messages in an InfiniBand packet and uses industry-standard InfiniBand link architecture to send the message. The IOP at the other end unwraps the coupling message and delivers it to the intended receiver.

InifiniBand coupling links for Parallel Sysplex

InfiniBand coupling link technology provides increased bandwidth at greater cable distances than ICB-4. The IBM System z10 supports a 12x (12 lanes of fibre in each direction) InfiniBand-Double Data Rate (IB-DDR) coupling link which is designed to support a total interface link data rate of 6 GigaBytes per second (GBps) in each direction. The maximum distance for this point-to-point link over fibre optic cabling is 150 meters (492 feet). This InfiniBand coupling link provides improved performance over the current ISC-3 coupling link in data centers where systems are less than 150 meters apart.

A 12x InfiniBand-Single Data Rate (IB-SDR) coupling link is available on all System z9 EC and System z9 BC servers. This coupling link is designed to support a total interface link data rate of 3 GigaBytes per second (GBps) in each direction. This InfiniBand coupling link provides improved performance over the current ISC-3 coupling link in data centers where systems are less than 150 meters apart. (These 12x IB-SDR coupling links cannot be used for coupling link connectivity between two z9 servers.) When a System z10 server is connected to a System z9 server using point-to-point InfiniBand cabling, the link auto-negotiates to the highest common data rate of 3 GBps.

InifiniBand coupling links also provide the ability to define up to 16 CHPIDs on a single HCA adapter, allowing physical coupling links to be shared by multiple sysplexes. This also provides additional subchannels for Coupling Facility communication, improving scalability, and reducing contention in heavily utilized system configurations. It also allows for one CHPID to be directed to one CF, and another CHPID directed to another CF on the same target server, using the same physical link. For detailed information about InfiniBand coupling links, see *Getting Started with InfiniBand on System z10 and System z9*, SG24–7539, available from the Redbooks Web site: http://www.redbooks.ibm.com/.

InfiniBand coupling links:

- Require CIB channel path definition (coupling facility peer channel capability) at the coupling facility end of a coupling facility channel connection. CIB channel paths are defined for IFB links.
- Require CIB channel path definition (coupling facility peer channel capability) at the z/OS (and, for System-Managed CF Structure Duplexing, the coupling facility) end of a coupling facility channel connection. CIB channel paths are defined for IFB links.
- Each CIB channel path must be connected to another CIB channel path. IFB links are defined as CIB channel paths. However, it is further required that an IFB link be connected to another IFB link.
- When defining CIB CHPIDs, you must specify both the name of the system (CSYSTEM keyword) this CHPID will connect to and the CSS and MIFID (CPATH keyword) on that system that this CHPID will connect to.

InfiniBand Long Reach: InfiniBand can be used for Parallel Sysplex coupling and STP communication at unrepeated distances up to 10 km (6.2 miles) and greater distances when attached to qualified optical networking solutions. InfiniBand coupling links supporting extended distance are referred to as Long Reach 1x (one pair of fiber) InfiniBand.

- Long Reach 1x InfiniBand coupling links support single data rate (SDR) at 2.5 gigabits per second (Gbps) when connected to a DWDM capable of SDR (1x IB-SDR).
- Long Reach 1x InfiniBand coupling links support double data rate (DDR) at 5 Gbps when connected to a DWDM capable of DDR (1x IB-DDR).

The link data rate will auto-negotiate from SDR to DDR depending upon the capability of the attached equipment.

Long reach 1x InfiniBand coupling links utilize the Host Channel Adapter2 Optical Long Reach fanout card. Like the 12x InfiniBand coupling link feature, the HCA2-O LR fanout card can also be used to exchange timekeeping messages for Server Time Protocol (STP).

This environment supports use of 9 micron single mode fiber optic cables with LC Duplex connectors, the same fiber optic cable used with InterSystem Channel-3 (ISC-3).

The Channel Path Identifier remains CHPID type CIB whether 12x IB-SDR or DDR or 1x IB-SDR or DDR.

Long reach 1x InfiniBand coupling links (1x IB-SDR or 1x IB-DDR) are an alternative to ISC-3 and offer greater distances with support for point-to-point unrepeated distances up to 10 km (6.2 miles) using 9 micron single mode fiber optic cables. Greater distances can be supported with System z-qualified optical networking solutions. Long Reach 1x InfiniBand coupling links support the same sharing capabilities as the 12x InfiniBand version, allowing one physical link to be shared by multiple operating system images or Coupling Facility images on a single system. They also provide the capability to have more than 1 CHPID associated with the physical IB Coupling link.

Note: The InfiniBand link data rates do not represent the performance of the link. The actual performance is dependent upon many factors including latency through the adapters, cable lengths, and the type of workload. Specifically, with 12x InfiniBand coupling links, while the link data rate is higher than that of ICB, the service times of coupling operations are greater, and the actual throughput is less.

Coupling facility channels (TYPE=CFP, TYPE=CBP, TYPE=CIB, or TYPE=ICP)

You can configure a CFP, CBP, CIB, or ICP channel path as:

- An unshared dedicated channel path to a single LP
- An unshared reconfigurable channel path that can be configured to only one LP at a time but which can be dynamically moved to another LP by channel path reconfiguration commands
- A shared channel path that can be shared between at most one coupling facility image and one or more z/OS images.

Shared coupling facility channel path recommendations: IBM recommends the following:

1. For shared coupling facility channel paths, make sure that only LPs that need to use the channel path have it configured online. This eliminates unnecessary traffic on the channel path from those systems that have it online but do not have the attached coupling facility in the active CFRM policy.
2. These channel paths can result in ’Path Busy’ conditions when another LP is using the path. This can result in delays in getting requests to the coupling facility on this path. The number of ’Path Busy’ conditions can be found in the RMF CF Subchannel Activity report in the BUSY COUNTS column labelled PTH. As a guideline, if this count exceeds 10% of the total requests, you should consider ***not*** sharing the channel path or adding additional coupling facility channel paths.

Defining internal coupling channels (TYPE=ICP)

Internal coupling channels are virtual attachments and, as such, require no real hardware. However, they do require CHPID numbers and they do need to be defined in the IOCDS.

It is suggested that you define a minimum of internal coupling channels. For most customers, IBM suggests defining just one pair of ICP channel paths for each coupling facility logical partition (LP) in your configuration. For instance, if your general purpose configuration has several ESA LPs and one CF LP, you would define one pair of connected ICP CHPIDs shared by all the LPs in your configuration. If your configuration has several ESA LPs and two CF LPs, you still would only define one connected pair of ICP CHPIDs, but one ICP CHPID should be defined as shared by the ESA LPs and one CF LP while the other ICP CHPID is defined as shared by the ESA LPs and the other CF LP. Both of these examples best exploit the peer capabilities of these coupling channels by using the *sending* and *receiving* buffers of both channels.

You must define ICP CHPIDs in pairs, and you must connect each pair. A connected pair of ICP CHPIDs is called an *internal coupling link*. Both ends of the internal coupling link must be specified by defining which ICPs are to communicate with each other. Use the CPATH keywords in the CHPID statement to connect internal coupling CHPIDs (see page 53).

Maximum recommended number of ICP CHPIDs: Real CPU resources are used to implement the link function of connected ICP CHPIDs. Production environments should limit the maximum number of internal coupling links that are defined for a CPC to optimize the internal coupling link function utilization of CPU resources. This maximum number of internal coupling links is based on the number of available physical CPs on the CPC. This maximum number of internal coupling links can be calculated by taking the number of CPs in the CPC that are used for general purpose CPs and for ICF CPs, and subtracting one from that total. For example: a CPC that consists of four general purpose CPs and two ICF CPs would have a maximum five [(4 + 2 = 6) - 1 = 5] internal coupling links recommended. This represents a maximum total of ten ICP CHPIDs being defined.

I/O configuration considerations

ICP IOCP supports coupling facility channel path definition on the System z10 CPC.

With z/OS, HCD provides controls for defining coupling facility channels. HCD also automatically generates the control unit and device definitions associated with CFP, CBP, CIB, or ICP channel paths.

IBM recommends that you use the Hardware Configuration Definition (HCD), when possible, to define the coupling facility channel configuration to the channel subsystem.

Considerations when migrating from ICMF to ICs

On previous CPCs, PR/SM LPAR provided an Integrated Coupling Migration Facility (ICMF) which is not supported on System z10.

- Use HCD to:
  - Define one shared ICP CHPID that is available for all the ESA logical partitions that were communicating with the *first* or only coupling facility logical partition using ICMF.

    - If there is a second coupling facility using ICMF being migrated, make this ICP CHPID available to the *second* coupling facility logical partition as well.
    - If there is **not a second** coupling facility, make this ICP CHPID available to the first or only coupling facility as well.
  - Define a second shared ICP CHPID that is available for the *first* or only coupling facility partition using ICMF.
    - If there is a second coupling facility using ICMF that is being migrated, make this second ICP CHPID available to all the ESA logical partitions that were communicating with the *second* coupling facility logical partition using ICMF as well.
    - If there is **not a second** coupling facility, make this second ICP CHPID available to all the ESA logical partitions that were communicating with the *first* or only coupling facility logical partition using ICMF as well. For more information, please see "Defining internal coupling channels (TYPE=ICP)" on page 81.)
  - Connect the two ICP CHPIDs together.

For the case above where there is only one coupling facility logical partition using ICMF being migrated, the result is that both ICP CHPIDs will be shared by all the ESA logical partitions and also the coupling facility logical partition that they are to communicate with. This is the correct configuration for a peer coupling link connected within the same CPC.

Linux operating system planning considerations

Linux is an open operating system with a wealth of applications which, in most cases, can run on a System z10 with a simple recompile. The System z10 includes features that provide an extremely cost-effective environment in which to run Linux.

Integrated Facility for Linux (IFL)

On System z10 models, you can purchase and install one or more IFL features exclusively for Linux and OpenSolaris workloads (a single Linux image, or z/VM Version 5.3 and later with only Linux and OpenSolaris guests) with no effect on the System z10 model designation. Consequently, no additional IBM operating system or middleware charges are incurred with the addition of this capacity unless that software is actually running in that additional capacity.

These features are ordered separately, and are distinguished at the hardware level from any general-purpose CPs, ICFs, zAAPs, or zIIPs. CPs, ICFs, IFLs, zAAPs and zIIPs are perceived by the system as multiple resource pools.

With this feature, Linux, or z/VM Version 5.3 and later with only Linux and OpenSolaris guests, runs on IFLs, which cannot be used to run other IBM operating systems such as z/OS, z/VSE, or TPF. Only logical partitions specified as either Linux-Only Mode or z/VM Mode in their Activation profiles can be allocated IFLs. IFLs can be allocated as either dedicated or shared. z/VM 5.3 and later can run in a logical partition that includes IFLs and can dispatch Linux and OpenSolaris guest virtual IFLs on the real IFLs. z/VM 5.3 and later can also simulate IFLs for Linux and OpenSolaris guests, dispatching virtual IFLs on real general-purpose processors (CPs).

z/VM version 5 utilizing IFL features

z/VM Version 5 utilizing IFL features provides an easy-to-use high-performance hypervisor that operates within a logical partition. It has the capability to create a significant number of Linux and OpenSolaris images. z/VM Version 5 creates and manages Linux and OpenSolaris images quickly and easily, providing the ability to share resources, and supports an arbitrary number of internal networks that can be used for high-speed communication among Linux images.

IBM System z10 Application Assist Processor (zAAP)

The IBM System z10 Application Assist Processor (zAAP) is available on the System z10. This specialized processing unit provides an economical Java™ execution environment for customers who desire the traditional Qualities of Service and the integration advantages of the System z10 platform.

When configured with general purpose processors within logical partitions running z/OS, zAAPs may help increase general purpose processor productivity and may contribute to lowering the overall cost of computing for z/OS Java technology-based applications. zAAPs are designed to operate asynchronously with the general processors to execute Java programming under control of the IBM Java Virtual Machine (JVM). This can help reduce the demands and capacity requirements on general purpose processors which may then be available for reallocation to other System z10 workloads.

The IBM JVM processing cycles can be executed on the configured zAAPs with no anticipated modifications to the Java application(s). Execution of the JVM processing cycles on the zAAP is a function of the Software Developer's Kit (SDK) 1.4.1 for zSeries, z/OS, and PR/SM.

The amount of general purpose processor savings will vary based on the amount of Java application code executed by zAAP(s). This is dependent upon the amount of Java cycles used by the relevant application(s) and on the zAAP execution mode selected by the customer.

Execution of the Java applications on zAAPs, within the same z/OS logical partition as their associated database subsystems, can also help simplify the server infrastructure and improve operational efficiencies. For example, use of zAAPs could reduce the number of TCP/IP programming stacks, firewalls, and physical interconnections (and their associated processing) that might otherwise be required when the application servers and their database servers are deployed on separate physical server platforms.

IBM does not impose software charges on zAAP capacity. Additional IBM software charges will apply when additional general purpose CP capacity is used.

Customers are encouraged to contact their specific ISVs/USVs directly to determine if their charges will be affected.

On System z10 models, you can purchase and install one or more zAAP features with no effect on the model designation. Consequently, no additional IBM operating system or middleware charges are incurred with the addition of this capacity unless that software is actually running in that additional capacity. zAAP features are ordered separately and are distinguished at the hardware level from any general purpose Central Processors (CPs), Internal Coupling Facility (ICF) processors, Integrated Features for Linux (IFLs), and System z10 Integrated Information Processor (zIIPs).

z/VM 5.3 and later can run in a logical partition that includes zAAPs and can dispatch z/OS guest virtual zAAPs on the real zAAPs. z/VM 5.3 and later can also simulate zAAPs for z/OS guests, dispatching virtual zAAPs on real general-purpose processors (CPs).

IBM System z10 Integrated Information Processor (zIIP)

The IBM System z10 Integrated Information Processor, or IBM zIIP, is the latest customer-inspired specialty engine for System z10. It provides a cost-effective workload reduction environment that is used by DB2 and other software products, some from ISVs. The zIIP is designed to help improve resource optimization and lower the cost of eligible workloads, enhancing the role of the mainframe as the data hub of the enterprise.

The IBM zIIP's execution environment will accept eligible work from z/OS 1.7 (with a required Web Deliverable function installed to support it), or z/OS 1.8 or higher, which will manage and direct the work between the general purpose processor and the zIIP. DB2 for z/OS V8 will exploit the zIIP capability for eligible workloads. IBM zIIPs are designed to free up general purpose capacity which may be utilized by other workloads.

In addition to improving the utilization of existing System z10 resources, the zIIP may help you to leverage the z/OS and DB2 for z/OS qualities of service for data access and information management across your enterprise. It does this by making direct access to DB2 more cost effective and potentially reducing the need for many local copies of the data and the complexity that brings.

On System z10 models, you can purchase and install one or more zIIP features with no effect on the model designation. Consequently, no additional IBM operating system or middleware charges are incurred with the addition of this capacity unless that software is actually running in that additional capacity. zIIP features are ordered separately and are distinguished at the hardware level from any general purpose Central Processors (CPs), Internal Coupling Facility (ICF) processors, Integrated Features for Linux (IFLs), and zAAPs.

z/VM 5.3 and later can run in a logical partition that includes zIIPs and can dispatch z/OS guest virtual zIIPs on the real zIIPs. z/VM 5.3 and later can also simulate zIIPs for z/OS guests, dispatching virtual zIIPs on real general-purpose processors (CPs).

Concurrent patch

Concurrent patch is available on all System z10 models. It is possible to apply BPC, UPC, Support Element (SE), Hardware Management Console, channel Licensed Internal Code (LIC), LPAR, coupling facility control code, I390, and PU patches nondisruptively and concurrent with system operation. There can still be situations where a small percentage of patches are disruptive; however, with all System z10 models, all major LIC components now support concurrent patch.

Additionally, there is also support for multiple EC streams (one per major LIC component) further minimizing the number of disruptive patch sessions. On previous models, a single EC stream contained all major LIC components and provided a mandatory sequence for patch application. This could lead to situations where a disruptive patch belonging to one LIC component, for example, PU, could prevent you from applying all nondisruptive SE patches if one or more of the SE patches came after this channel patch in the patch application sequence.

Patches for each major LIC component have their own sequence for patch application. This means that disruptive patches belonging to one LIC component no longer stand as an obstacle to the concurrent application of nondisruptive patches belonging to another LIC component as long as the patches in question are not otherwise defined as corequisite for each other.

CFCC enhanced patch apply

The CFCC patch apply process is enhanced to eliminate the need for a Power On Reset (POR) of the System z10 to apply a disruptive CFCC patch. CFCC enhanced patch apply provides you the ability to:

- Selectively apply the new patch to one of possibly several CFs running on a System z10. For example, if you have a CF that supports a test parallel sysplex and a CF that supports a production parallel sysplex on the same System z10, you have the ability to apply a disruptive patch to only the test CF without affecting the production CF. After you have completed testing of the patch, it can be applied to the production CF as identified in the example.
- Allow all other logical partitions on the System z10 where a disruptive CFCC patch will be applied to continue to run without being impacted by the application of the disruptive CFCC patch.

The enhanced patch apply does not change the characteristics of a concurrent CFCC patch, but does significantly enhance the availability characteristics of a disruptive CFCC patch by making it much less disruptive.

Note: Any POR of the servers will result in the disruptive patch being applied to CF partitions.

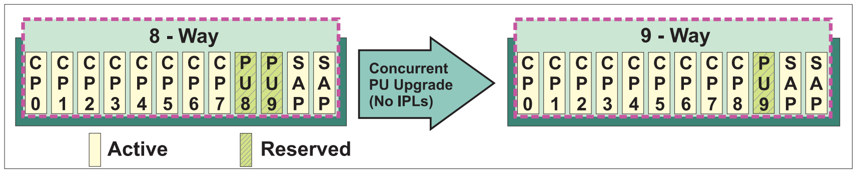
Dynamic capacity upgrade on demand

System z10 includes a function to dynamically increase the number of CPs, ICFs, IFLs, zAAPs or zIIPs without an intervening IPL. A logical partition (LP) may be defined with both an initial and reserved amount of logical CPs. This enables a definition where the number of logical CPs for a logical partition is greater than the number of physical CPs installed on the model. These reserved CPs are automatically in a deconfigured state at partition activation and can be brought online at any future time via the SCP operator command if the requested resource is available. To prepare for a nondisruptive upgrade, a Logical Partition simply needs to be defined and activated in advance with an activation profile indicating reserved CPs. This helps ensure that any planned logical partition can be as large as the possible physical machine configuration, nondisruptively.

Note that with enhanced support available on z10, the logical CP definition for a logical partition can be dynamically changed without requiring a reactivation of the logical partition. This allows you to add to the definition of offline CPs (or any other supported processor types) dynamically should the need arise. If the system control program running in that logical partition supports this dynamic add capability, the additional offline CPs can be configured online in the same way as preplanned reserved CPs are brought online.

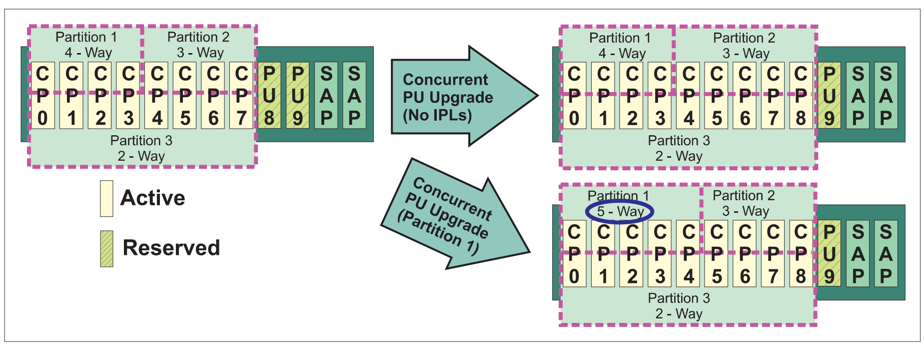
For more information on exploiting dynamic CPU addition, see *z/OS MVS Planning: Operations*.

The following example assumes a nondisruptive concurrent CP upgrade from an 8-Way to a 9-Way Server.



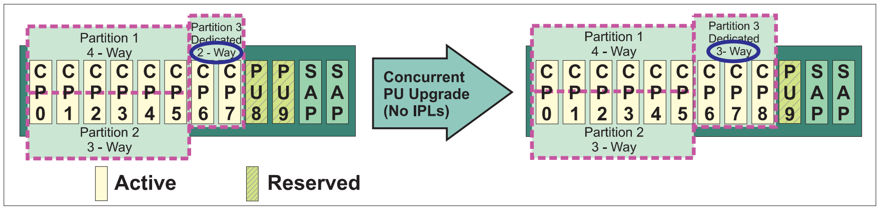
PR/SM shared partitions

PR/SM configurations supporting multiple partitions, all sharing CPs, support concurrent CP upgrades. PR/SM code, once signaled that one or more central processors have been made available to the configuration, will vary them online automatically into the "shared pool" of physical CPs and begin full utilization of the added capacity. In the following example, three partitions sharing eight physical CPs are able to share the increased capacity resulting from a nondisruptive upgrade to a 9-way server without any other configuration changes. In the second upgrade scenario, Partition 1 is additionally changed from a 4-way to a 5-way partition nondisruptively. The preparation for this is straightforward and easy. Simply define and activate logical Partition 1 with four initial and one reserved logical CPs (see Figure 37 on page 154 for a similar example). At the time of the concurrent CP upgrade, the SCP operator command can be used in Partition 1 to configure a fifth CP online to the shared partition without interruption to any logical partition.



Mixed shared and dedicated PR/SM partitions

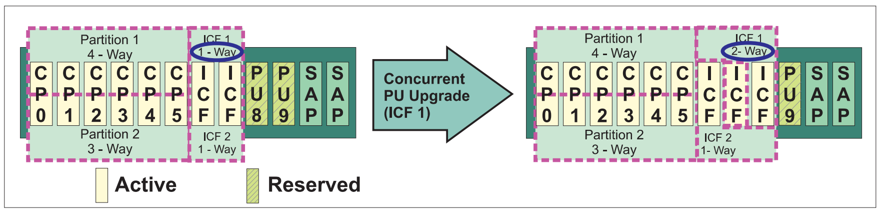
As with configurations in which all PR/SM partitions share available CPs, those shared partitions within a mixed configuration also support concurrent CP upgrade. CPs are added, without disruption to any of the partitions, to the pool of physical CPs shared amongst the shared CP LPs. In addition, partitions configured with dedicated CPs in a mixed environment can add new CP capacity while both the shared CP partitions and the dedicated CP partition run uninterrupted. To prepare for this ability, in the following example simply define Partition 3 as a 3-way dedicated partition with two initial logical CPs and one reserved logical CP (see Figure 37 on page 154 for a similar example). The reserved logical CP is offline automatically at the time of partition activation. At the time of the concurrent CP upgrade, the SCP operator command can be used in the dedicated partition to configure a third CP online to the dedicated partition without interruption to any logical partition.



Partition 1
4 - Way
Partition 3
Dedicated
2 - Way
CP0 CP1 CP2 CP3 CP4 CP5 CP6 CP7 PU8 PU9 SAP SAP
Partition 2
3 - Way
Concurrent
PU Upgrade
(No IPLs)
Partition 1
4 - Way
Partition 3
Dedicated
3- Way
CP0 CP1 CP2 CP3 CP4 CP5 CP6 CP7 CP8 PU9 SAP SAP
Partition 2
3 - Way
Active
Reserved

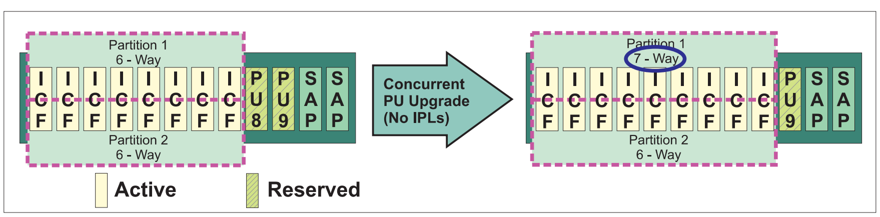
Multiple dedicated PR/SM partitions

Configurations in which all PR/SM partitions use dedicated CPs, where there is more than one dedicated partition, also support concurrent CP upgrade. CPs are added to the configuration, without disruption to any of the partitions, and can be brought online to a dedicated partition without an interruption. In the following example, all ICFs in the configuration are dedicated. The partition (ICF 1) is defined for the ability to be upgraded dynamically. To prepare for this ability, simply define ICF 1 as a 2-way dedicated partition with one initial and one reserved logical CP (see Figure 37 on page 154 for a similar example). At the time of the concurrent CP upgrade, the CF operator command can be used in the ICF 1 dedicated partition to configure a second ICF CP online to the dedicated partition without interruption to any logical partition. Note the same type of procedure can be accomplished with logical partitions using dedicated general purpose CPs.



Shared Internal Coupling Facility

Concurrent upgrade can be used to add a PU to a shared pool of PUs supporting existing Internal Coupling Facilities. In the following example, Partition 1 is defined for the ability to be upgraded dynamically. To prepare for this ability, simply define Partition 1 as a 7-way shared partition with six initial and one reserved logical CPs (see Figure 37 on page 154 for a similar example). At the time of the concurrent CP upgrade, the CF operator command can be used in Partition 1 shared partition to configure a seventh ICF CP online to the shared partition without interruption to any logical partition. Note that Partition 2 in this case could have also been defined as a 7-way shared ICF partition with one ICF configured offline. This would allow Partition 2 to grow concurrently without an outage as well.



Dynamic capacity upgrade on demand limitations

1. Valid upgrade towers are as follows starting at the smallest model in the pathway:

   z10 BC Models
   E10

   z10 EC Models
   E12, E26, E40, E56, E64

   Inactive (spare) PUs can be added concurrently, dynamically providing nondisruptive upgrade of processing capability. They can be characterized, in any combination, as CPs, ICFs, IFLs, zAAPs, or zIIPs. Neither the number of zAAPs nor zIIPs can exceed the number of CPs.
2. For shared CP PR/SM configurations, added CPs are brought into the pool of shared CPs, effectively increasing the number of physical CPs to be shared amongst partitions. To increase the number of logical CPs online to an LP, simply define the LP with both initial and reserved logical CPs. Then all you need to do is configure on the extra logical CP(s) after the concurrent upgrade.
3. All models have the ability to define logical partitions with as many reserved CPs as necessary. With thoughtful planning, there is never a need for a disruptive increase in the number of logical CPs
4. The maximum initially online logical CP width that logical partitions can be defined and activated with at any point in time is as follows (the maximum defined logical CP width is as great as the total number of CPs achievable via concurrent CPU upgrade):
   - Maximum initial logical CPs defined for a dedicated partition ***equals*** physical CPs online for the current model ***minus*** physical CPs currently dedicated and online to other dedicated partitions ***minus*** the maximum online number of shared CPs among all the activated logical partitions that are using shared CPs.
   - Maximum initially online logical CPs defined for a shared partition ***equals*** physical CPs online for the current model ***minus*** physical CPs currently dedicated and online to other partitions using dedicated CPs.
   - Maximum ***total*** logical CPs (including initial and reserved) for any partition ***equals*** the number of physical CPs achievable through concurrent CP upgrade.
   - When a logical partition is defined to use ICFs, IFLs, zIIPs or zAAPs, these rules are applied against the installed processors of that type. In the case of zAAPs and zIIPs, logical partitions can have a combination of general purpose processors and zAAPs/zIIPs defined. These rules apply to each processor type defined to the partition independently. The total number of all logical processors defined to the logical partition cannot exceed the maximum supported for a logical partition by the CEC, independent of processor type.

Concurrent Memory Upgrade

The System z10 includes a function to dynamically increase the amount of configured storage. Concurrent Memory Upgrade allows for a memory upgrade without changing hardware or experiencing an outage, provided there is enough spare memory already existing on the memory cards. An IML is not required to use the previously unavailable storage. It is immediately available for allocation to logical partitions as either central or expanded storage. The new storage can be allocated to either newly activated logical partitions or to already active logical partitions by using dynamic storage reconfiguration (see “Dynamic storage reconfiguration” on page 106). In planning for a concurrent memory upgrade, logical partition activation profiles should be defined with storage (central and/or expanded) specifications that include a reserved as well as an initial storage amount. Following the completion of the concurrent memory upgrade operation, issue the z/OS command CF STOR(E=1),ONLINE or the z/OS command CF ESTOR(E=1),ONLINE to bring the new memory online to already active LPs for which a reserved central storage amount, or a reserved expanded storage amount (respectively) was specified.

Capacity Backup Upgrade (CBU) capability

This orderable feature, available on z10 Models, can be integrated with Geographically Dispersed Parallel Sysplex™. This should reduce disaster recovery times by automating the Capacity Backup Upgrade process at a remote site.

Operationally, the planning considerations and limitations for Capacity Backup Upgrade, for mode purposes, are similar to those for Dynamic Capacity Upgrade on Demand. Planning is simple because reserved logical CPs can be specified for logical partitions on the backup system. The logical CPs can then be brought online, quickly and nondisruptively.

Concurrent Undo CBU is provided to dynamically remove from the configuration processors that had been added via Capacity Backup Upgrade. The server for disaster recovery with Capacity Backup Upgrade activated can now be restored to its base configuration without requiring a system outage.

When a disaster occurs, Capacity Backup Upgrade is intended to provide the extra capacity without disruption. When the disaster is over and normalcy is restored, Concurrent Undo CBU is intended to allow the system to be returned to its previous configuration without disruption.

Annual testing of a Capacity Backup Upgrade system is highly recommended. Invoking the Capacity Backup Upgrade configuration is nondisruptive and now returns to the original configuration, after the test, without disruption as well.

When a typical Capacity Backup Upgrade occurs, usually logical processors are configured online so that the system closely resembles the failing system. To prepare for Concurrent Undo CBU, the most expedient method is to simply configure offline all those logical processors that were configured online in support of the failing system.

In order for Concurrent Undo CBU to proceed, the restored original configuration must have a physical processor for each online dedicated logical processor. Theoretically, the only additional requirement is that at least one nondedicated physical processor remains that matches each type (general purpose, ICF, IFL, zAAP or zIIP) of online shared logical processors. However, it is highly recommended that shared logical processors be configured offline so that the highest number of online shared logical CPs for any active LP does not exceed the number of nondedicated physical CPs remaining. For further guidelines, see the rules governing the number of CPs that can be specified for an activating logical partition on page 116.

Enhanced Book Availability

The z10 is designed to allow a single book, in a multi-book server, to be concurrently removed from the server and reinstalled during an upgrade or repair action, while continuing to provide connectivity to the server I/O resources using a second path from a different book. To help minimize the impact on current workloads and applications, you should ensure that you have sufficient inactive physical resources on the remaining books to complete a book removal.

Enhanced book availability may also provide benefits should you choose not to configure for maximum availability. In these cases, you should have sufficient inactive resources on the remaining books to contain critical workloads while completing a book replacement. Contact your IBM representative to help you determine the appropriate configuration. With proper planning, you may be able to avoid planned outages when utilizing enhanced book availability.

Enhanced driver maintenance is another step in reducing the duration of a planned outage. One of the greatest contributors to downtime during planned outages is Licensed Internal Code (LIC) updates performed in support of new features and functions. When properly configured, the z10 is designed to support activating select new LIC level concurrently. Concurrent activation of the select new LIC level is only supported at specific sync points (points in the maintenance process when LIC may be applied concurrently - MCL service level). Sync points may exist throughout the life of the current LIC level. Once a sync point has passed, you will be required to wait until the next sync point supporting concurrent activation of a new LIC level. Certain LIC updates will not be supported by this function.

Preparing for Enhanced Book Availability

This option will determine the readiness of the system for the targeted book. The configured processors and the in-use memory will be evaluated for evacuation from the targeted book to the unused resources available on the remaining books within the system configuration. In addition, the I/O connections associated with the targeted book will be analyzed for any Single Path I/O connectivity.

There are three states which can result from the prepare option:

- The system is ready to perform the Enhanced Book Availability for the targeted book with the original configuration.
- The system is not ready to perform the Enhanced Book Availability due to conditions noted from the prepare step. See "Getting the system ready to perform Enhanced Book Availability" for more details.
- The system is ready to perform the Enhanced Book Availability for the targeted book. However, processors were reassigned from the original configuration in order to continue. "Reassigning non-dedicated processors" on page 93 for details.

Getting the system ready to perform Enhanced Book Availability

Review the conditions that are preventing the Enhanced book Availability option from being performed. There are tabs on the resulting panel for Processors, Memory, and for various Single Path I/O conditions. Only the tabs that have conditions preventing the perform option from being executed will be displayed. Each tab will indicate what the specific conditions are and possible options to correct the conditions. Following is an example panel:

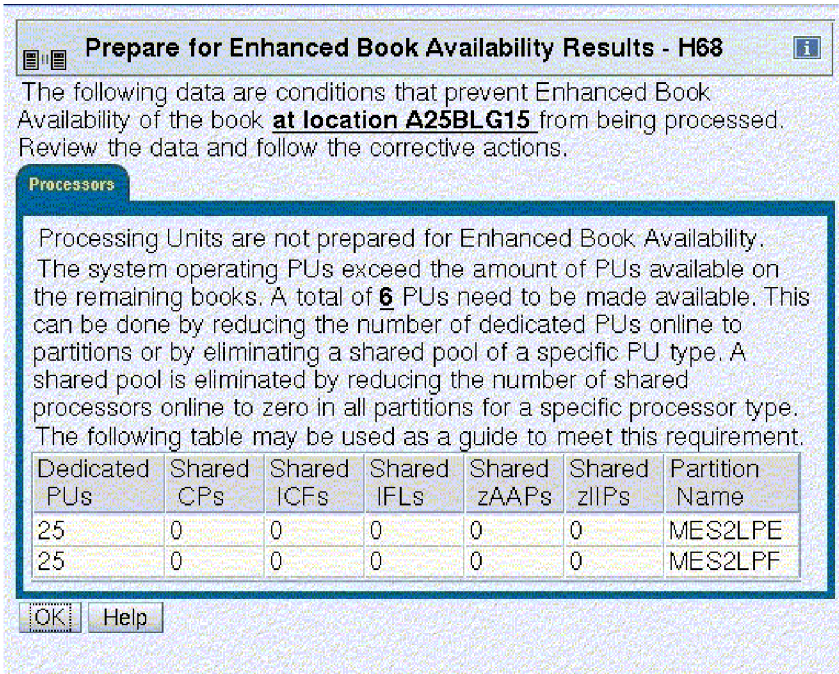


Figure 23. Example of a prepare for enhanced book availability results window

In the example shown in Figure 23, the Processor tab displays, indicating the corrective actions suggested for the processor configuration. Following is a list of tabs that may appear for your particular configuration:

Processors
: Use this tab to view the corrective actions required for the processor configuration conditions that are preventing the Perform Enhanced Book Availability option from being performed for the targeted book.You may need to deactivate partitions or deconfigure processors to meet requirements as indicated by the panel data.

Memory
: Use this tab to view the corrective actions required for the memory configuration conditions that are preventing the Perform Enhanced Book Availability option from being performed for the targeted book. You may need to deactivate partitions to meet requirements as indicated by the panel data. The In-Use memory must be less than or equal to the available memory on the remaining books within the system.

Single Path I/O
: Use this tab to view the corrective actions required for the single I/O configuration conditions that are preventing the Perform Enhanced Book Availability option from being performed for the targeted book. You will need to deconfigure all of the PCHIDs that are indicated by the panel data.

Single Domain
: Use this tab to view the corrective actions required for the single I/O domain configuration conditions that are preventing the Perform Enhanced

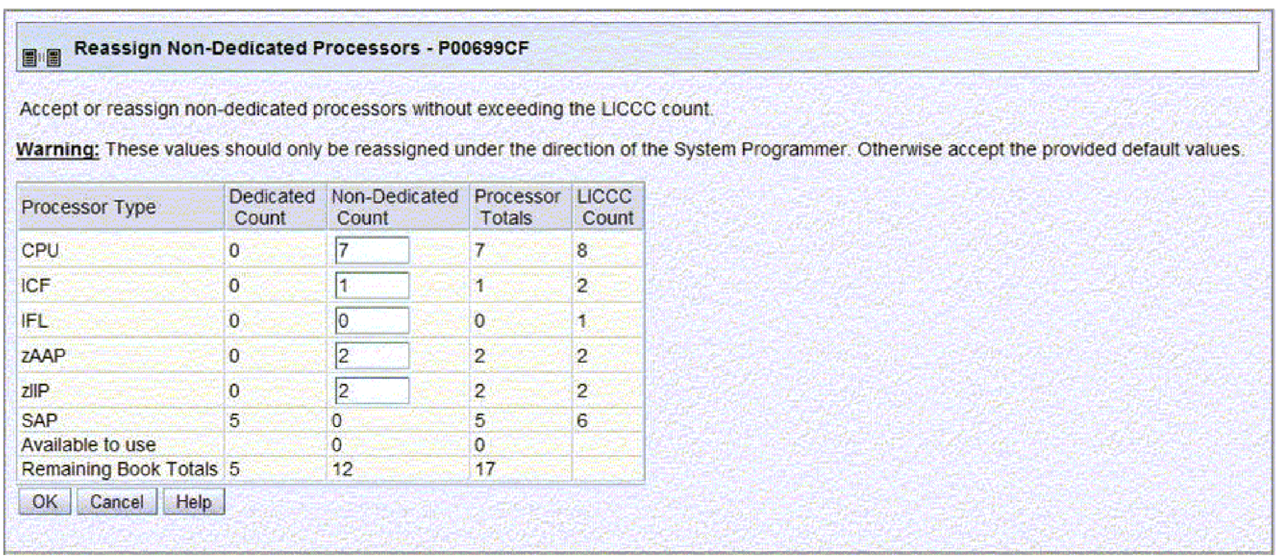
Book Availability option from being performed for the targeted book. You will need to change the alternate path to a different book or deconfigure the PCHID.

Single Alternate Path
Use this tab to view the corrective actions required for the single I/O configuration conditions that are preventing the Perform Enhanced Book Availability option from being performed for the targeted book. You will need to correct the alternate path error condition or deconfigure the PCHIDs.

Reassigning non-dedicated processors

Following is an example showing the Reassign Non-Dedicated Processors panel. Use this panel to change or accept the system processor assignments that are generated during the processing of the Prepare for Enhanced Book Availability option. The processor values that are entered from this panel will be the processor configuration utilized during the Perform Enhanced Book Availability processing.

ATTENTION
The values should never be altered without approval from the system programmer.


Reassign Non-Dedicated Processors - P00699CF

Accept or reassign non-dedicated processors without exceeding the LICCC count.

Warning: These values should only be reassigned under the direction of the System Programmer. Otherwise accept the provided default values.

Processor Type	Dedicated Count	Non-Dedicated Count	Processor Totals	LICCC Count
CPU	0	7	7	8
ICF	0	1	1	2
IFL	0	0	0	1
zAAP	0	2	2	2
zIIP	0	2	2	2
SAP	5	0	5	6
Available to use		0	0	
Remaining Book Totals	5	12	17	

OK Cancel Help

Figure 24. Reassign non-dedicated processors window

Customer Initiated Upgrade (CIU)

This feature is designed to allow timely response to sudden increased capacity requirements by downloading and automatically applying a processor and/or memory upgrade via the Web, using IBM Resource Link and the Remote Support Facility.

Operationally, the planning considerations and limitations for CIU are similar to those for Dynamic Capacity Upgrade on Demand and Concurrent Memory Upgrade. Planning is simple because reserved logical CPs can be specified for logical partition (LP)s in the original configuration. The logical CPs can then be brought online, quickly and nondisruptively at the completion of the Concurrent Upgrade.

Similarly, a reserved central and/or expanded storage amount can be specified for participating LPs and brought online non-disruptively following the completion of the concurrent memory upgrade.

Concurrent Processor Unit conversion

The System z10 supports concurrent conversion of different Processor Unit (PU) types. This capability is extended to Central Processor (CPs), Integrated Facility for Linux (IFLs), zAAPs, zIIPs, and Internal Coupling Facility (ICFs) providing flexibility in configuring a System z10 to meet the changing business environments.

For example, a Z10 EC Model E12 configured with eight CPs and two zAAPs could be reconfigured to eight CPs, one zAAP and one zIIP by ordering the appropriate PU conversion. This order will generate a new LIC CC which can be installed concurrently in two steps. First, one zAAP is removed from the configuration. Second, the newly available PU is activated as a zIIP.

Planning for nondisruptive install of crypto features

Crypto Express2 Coprocessors (CEX2C) or Crypto Express2 Accelerators (CEX2A) can be added to logical partitions nondisruptively using the Change LPAR Cryptographic Controls task. For more information, see “Changing LPAR cryptographic controls” on page 196. Logical partitions can either be configured in advance or dynamically with the appropriate domain indices and Cryptographic numbers (see the Cryptographic Candidate List information under “Parameter descriptions” on page 168).

If the customer plans to use ICSF or the optional cryptographic hardware, the CP Crypto Assist functions (CPACF DES/TDES) must be enabled. Many IBM products will take advantage of the cryptographic hardware using ICSF, so enabling CPACF is recommended. View the CPC Details panel to determine if the CPACF feature is installed. For more detailed information, see the *System z10 Support Element Operations Guide* and the *z/OS Cryptographic Services ICSF TKE Workstation User’s Guide*. It is important to remember that when nondisruptively installing Crypto Express2, the default configuration of the card is coprocessor (CEX2C). To change the configuration of Crypto Express2, use the Cryptographic Configuration Panel. Once the Crypto Express2 feature has been installed, and the previous preparations made, the CEX2C and/or CEX2A is available to any partition that specifies their assigned Cryptographic numbers in the Candidate List. To bring the Cryptographic numbers online, perform a Config On of the Crypto (nondisruptive).

The Cryptographic Online List needs to be set up in the Image Activation Profile to reflect the CEX2C and/or CEX2A that you want to bring online automatically during the partition activation. If the Cryptographic Candidate List does not reflect the CEX2C or CEX2A that you plan to use, then these Cryptos are not available to the logical partition after this partition is activated. If the Cryptographic Online List is setup properly, the crypto will be brought online when the partition is activated and available to the operating system when ICSF is started. Otherwise, a Configure On is necessary to bring the crypto online in the logical partition.

Chapter 3. Determining the characteristics of logical partitions

Planning overview

This chapter provides a planning overview for defining logical partitions (LPs). Support for features, functions, and panels can differ depending on machine type, engineering change (EC) level, or machine change level (MCL). During IOCP execution, the names and numbers of the LPs are specified and channel paths are assigned to the LPs. Sample tasks and panels are explained in this publication, including references to tasks and panels available from the Support Element console. For detailed procedures for these operator tasks, see the *System z Hardware Management Console Operations Guide* and the *System z10 Support Element Operations Guide*.

Performance considerations

The performance of an LP is controlled by:
- The number of logical CPs online
- Whether CPs are dedicated to or are shared by the LP
- The processing weight assigned to each LP
- The processor running time interval

The total number of logical CPs across all active LPs is one of the factors used to determine the dynamic dispatch interval. See "Processor running time" on page 133.

Use the RMF Partition Data Reports to determine the effective dispatch time for LPs. For more information about this RMF reporting enhancement see "RMF LPAR management time reporting" on page 203.

The greater the number of active logical CPs relative to the number of physical CPs configured, the smaller the dispatch interval.

Dedicated and shared central processors (CPs)

LPs can have CPs dedicated to them, or they can share CPs with other active LPs. Because the use of dedicated or shared CPs in an LP affects performance in several ways, the characteristics, limitations, and advantages of each should be carefully studied.

If zAAPs or zIIPs are defined for a logical partition, they are defined in the same way as the general purpose CPs for the logical partition. If the general purpose CPs for a logical partition are shared, the zAAPs/zIIPs are shared. If the general purpose CPs for a logical partition are dedicated, the zAAPs/zIIPs are dedicated.

Dedicated and shared channel paths

A configuration defining shared channel paths offers additional capabilities over an equivalent configuration containing unshared channel paths, while maintaining comparable system performance.

ITR performance

The best ITR performance is achieved with dedicated LPs. To achieve optimal ITR performance in sharing LPs, keep the total number of logical CPs online to a minimum. This reduces both software and hardware overhead.

Capped logical partitions

It is recommended that LPs be defined as capped LPs at the Support Element/Hardware Management Console only when needed to support planned requirements. When a capped LP does not obtain needed CP resources, because it has reached its cap, activity for that LP is similar to a system running out of CP resources. Response time can be slower on systems which operate at their cap. For this reason, interactive response times can suffer when there is a mix of interactive and CP-intensive work in the same capped LP.

Recovery considerations

Resources should be defined to LPs so that any hardware failure has a minimal impact on the remaining active LPs.

For example, the failure of a physical CP can cause the temporary loss of any logical CP that was dispatched on the physical CP. In many instances, recovery of a logical CP that was running on a failed physical CP will take place automatically when an available spare physical CP is dynamically brought into the configuration. Also, PR/SM LPAR is often able to transparently re-dispatch a shared logical CP on a different physical CP even when no spares are available. If a logical CP is still lost, the LP owning the logical CP can continue operating if it was running on an LP with at least two CPs dispatched on different physical CPs, and if the control program that is active in the LP can recover from CP failures.

Determining the characteristics

The information in this section should help you determine the type and amount of CPC resources you need for each LP.

The total amount of resources that you can define for all LPs can exceed the configured resources.

Individual LP definitions are checked against the total resources installed. The actual allocation of these resources takes place only when the LP is activated. This design characteristic allows considerable flexibility when defining and activating LPs.

Control program support

Table 11 on page 100 summarizes the characteristics of the control programs that can be supported in an LP. See “Control program support in a logical partition” on page 5 for more information.

Some control programs require specific LP characteristics. For this reason consider all control programs before planning or defining LP characteristics.

Table 11. Control program support on z10

Control program	Control program operating mode	Maximum number CPs	Maximum central storage	Maximum expanded storage	Maximum number channels
z/OS 1.10	ESA/390	64	1 TB	NA	256
z/OS 1.9	ESA/390	64	1 TB	NA	256
z/OS 1.8	ESA/390	32	1 TB	NA	256
z/OS 1.7	ESA/390	32	128 GB	NA	256
z/VM 5.4	z/VM, Linux-Only, or ESA/390	32	256 GB	128 GB	256
z/VM 5.3	Linux-Only or ESA/390	32	256 GB	128 GB	256
z/VSE 4.2	ESA/390	10	32 GB	NA	256
z/VSE 4.1	ESA/390	10	8 GB	NA	256
z/VSE 3.1	ESA/390	10	2 GB	NA	256
z/TPF 1.1	ESA/390 or ESA/390 TPF	64	1 TB	NA	256
TPF 4.1	ESA/390 or ESA/390 TPF	16	2 GB	NA	256
Linux for S/390	Linux-Only or ESA/390	16	2 GB	256 GB	256

Notes:

1. On all z/OS versions, ESA/390 mode is the initial mode at IPL time; however, during IPL z/OS switches to z/Architecture 64-bit addressing.
2. z/VM 5.4 and later support z/VM mode partitions. IPL of z/VM 5.3 is not supported in z/VM mode partitions. Use ESA/390 or Linux-Only mode partitions for z/VM 5.3.
3. z/VSE 4.1 and z/VSE 4.2 are initially in ESA/390 mode at IPL time; however, during IPL they switch to z/Architecture mode.

IOCDS requirements

You must use IOCP or BUILD IOCDS with HCD to create an LPAR IOCDS. You can specify the LP names and MIF image ID numbers in an LPAR IOCDS.

Logical partition identifier

The logical partition identifier (ID) is used as the third and fourth hexadecimal digits of the operand stored by the Store CPU ID instruction for each CP in the LP. Even though at most 60 (decimal) logical partitions can be defined on a z10 EC (and 30 logical partitions on a z10 BC), valid identifiers for LPs are X'00' through X'3F'. The LP identifier must be unique for each active LP.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization Tasks list to open a reset or image profile to define the LP identifier for an LP. The Partition identifier field is located on the General page for the LP. (See Figure 37 on page 154).

Mode of operation

The mode of an LP depending on the model can be ESA/390, ESA/390 TPF, Linux-Only, z/VM, or Coupling Facility.

The mode of an LP must support the mode of the control program loaded into it. ESA/390 LPs support ESA/390 control programs, Coupling Facility LPs support the coupling facility control code, z/VM LPs support z/VM, and Linux-Only LPs support Linux or z/VM.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization Tasks list to open a reset or image profile to define the mode for an LP. The Mode field is located on the General page for the LP. (See Figure 37 on page 154).

Storage configurations

The definition of central storage and expanded storage to the LP depends on the size of the I/O configuration, the storage limits of the control program loaded into the LP and on the storage requirements of the applications running in the LP.

Storage resources

Use standard capacity-planning procedures to assess CPC storage requirements for LPs.

With dynamic storage reconfiguration (see "Dynamic storage reconfiguration" on page 106), an appropriately defined LP can dynamically add storage to its configuration that is released when another active LP removes it from its configuration or is deactivated. Additionally, an LP can dynamically add storage to its configuration following an increase in configured storage via concurrent memory upgrade (see "Concurrent Memory Upgrade" on page 90).

Single storage pool

With this function, all physical storage is dynamically designated by LPAR as either central storage or expanded storage as requirements of active logical partitions dictate.

As a result, the need to predesignate configured storage as either central storage or expanded storage prior to IML on the Storage Page of the Customize Activation Profile panel is not necessary and is not provided. The system programmer now has greater flexibility when planning the division of storage in order to satisfy anticipated logical partition definitions. Single storage pool streamlines the planning effort because LPAR automatically provides the correct storage designation for any configuration as the need arises. This feature is especially useful as it simplifies planning for migration to z/OS a 64-bit capable operation system.

All configured storage is defined, at IML, as central storage. As logical partitions with initial expanded storage are activated (and when reserved expanded storage is configured online), LPAR automatically allocates backing physical storage from the available pool as expanded storage.

A feature of this function is that the central storage addressability ranges used to back expanded storage allocated to logical partitions are communicated on the logical partition storage allocation display of the Storage Information task.

Central storage

Central storage is defined to LPs before LP activation. When an LP is activated, storage resources are allocated in contiguous blocks. These allocations can be dynamically reconfigured. Sharing of allocated central storage among multiple LPs is not allowed.

Granularity of initial and reserved central storage amounts is dependent on the largest central storage amount (CSA) for the LP as follows:

Table 12. Central storage granularity for z10 EC

Largest Central Storage Amount	Storage Granularity
≤ 128 GB	256 MB
128 GB < CSA ≤ 256 GB	512 MB
256 GB < CSA ≤ 512 GB	1 GB
512 GB < CSA ≤ 1 TB	2 GB

Table 13. Central storage granularity for z10 BC

Largest Central Storage Amount	Storage Granularity
≤ 64 GB	128 MB
64 GB < CSA ≤ 128 GB	256 MB
128 GB < CSA ≤ 248 GB	512 MB

This granularity applies across the central storage input fields (Initial and Reserved fields). Use the larger of the initial and reserved central storage amounts to calculate storage granularity. For example, for an LP with an initial storage amount of 256 GB and a reserved storage amount of 512 GB, the central storage granularity of initial and reserved central storage fields is 1 GB, using the larger reserved storage amount to determine storage granularity. Central storage granularity for the initial storage origin input field is fixed at 256 MB.

Additionally, when migrating to these models, you must convert the existing central storage amounts that are not in multiples of the storage granularity supported.

For example, an LP with an initial central storage size of 10240 MB on a previous model with 16 GB of storage installed would require conversion of the initial central storage size to a multiple of 256 MB (64 MB granularity was valid on this prior model configuration).

Check your central storage definitions and consult your system programmer to ensure that they meet your processing needs.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization Tasks list to open a reset or image profile to define the central storage for an LP. The Initial, Storage Origin, and Reserved fields are located on the Storage page for the LP. See Figure 42 on page 164 for an example.

Initial central storage

- The initial amount of central storage represents the amount of storage allocated to an LP when it is activated.
- You must specify a nonzero number for the initial amount of central storage to activate the LP.

- If no origin is specified for the initial value, the LP will be treated as an LP that owns it's own **addressability range**. This means that no other LP can map over it.

Reserved central storage

- Only ESA/390, ESA/390 TPF, z/VM, and Linux-Only LPs can have nonzero amounts for this parameter. Coupling facility LPs cannot have reserved central storage amounts.
- The reserved amount of central storage defines the additional amount of central storage that can become available to an LP when no other activated LP has this reserved storage online. Reserved storage amounts are always offline after LP activation.
- Only LPs that specify a central storage origin can be allocated storage within the reserved central storage defined for another LP. Reserved central storage can only overlap LPs that specify an origin.
- For LPs that do not specify central storage origins, the LP's reserved storage is available to be brought online to the LP whenever there is any storage that is not being used by any other LPs.
- For LPs that do specify a central storage origin, if some of the reserved central storage is not available, the reserved central storage that is available can still be configured online starting at the reserved storage origin.
- Specifying a zero for the reserved size indicates the LP's central storage cannot get any larger than the initial size for the duration of the activation.

Central storage origin

- There must be enough contiguous central storage addressability to fit the reserved amounts, but the reserved amounts can be in use by other LPs (that specified origins for storage) at the time the LP is activated.
- The origin for central storage defines the starting megabyte where the central storage ***addressability range*** begins for the LP. If enough storage is not available to satisfy the initial central storage request starting at this origin, LP activation will fail.
- For central storage, the specification of the origin parameter provides the only way to overlap storage definitions. For example, the reserved storage definition for one LP can overlap the storage definition of another LP when the origin parameter is specified for both LPs.

  All ***customer*** storage is configured at IML as central storage. Storage will be configured as expanded storage when a logical partition with initial expanded storage is activated or when a reserved expanded storage element of an already active logical partition is configured online.

  The total amount of central storage ***addressability*** that can be used to map central storage for LPs is **at least** twice the amount of ***customer*** storage. You can review current LP storage allocations by using the Storage Information task available from the CPC Operational Customization Tasks lists.
- Since the specification of a central storage origin is optional, there are two implementations of dynamic storage reconfiguration for reserved central storage:

1. If you do not specify a central storage origin, the reserved central storage is available for the LP when there is sufficient physical storage available to meet the reserved central storage request.

   Storage can be reassigned between LPs that have noncontiguous address ranges. Reconfiguration is not limited to growing into an adjacent LP. LPs are eligible to use noncontiguous central storage if they have unique (not overlapping) storage range definitions. Specifying an origin is not required when defining a reserved storage amount for an LP, and by not specifying an origin, the LP is reserved an addressable storage range for its entire storage configuration (initial plus reserved amount). Not specifying an origin ensures no overlap. The reserved central storage is available for LPs that do not specify an origin when there is sufficient physical storage to meet the reserved central storage request.
2. If you specify a central storage origin, the entire reserved central storage amount is only available for the LP when:
   – No other LP has this central storage address range, to which the reserved central storage is mapped, online.
   – There is sufficient physical storage available to meet the reserved central storage request.

- If no origin is specified for an LP, the system assigns the storage to the LP using a top-down first-fit algorithm. Storage that is part of reserved central storage for another activated LP is not available for any LPs that do not specify a central storage origin.

Expanded storage

Optional expanded storage is defined to LPs before LP activation. When an LP is activated, storage resources are allocated in contiguous blocks. These allocations can be dynamically reconfigured. Sharing of allocated expanded storage among multiple LPs is not allowed.

For a z10 EC, expanded storage granularity is fixed at 256 MB. For a z10 BC, expanded storage granularity is fixed at 128 MB. Expanded storage granularity applies across the expanded storage input fields (Initial, Initial storage origin, and Reserved fields).

When migrating to these models, you must convert any existing expanded storage amounts that are not in multiples of the storage granularity supported.

For example, an LP with an initial expanded storage size of 10240 MB on a previous model with 16 GB of storage installed would require conversion of the initial expanded storage size to a multiple of 256 MB (64MB granularity was valid on this prior model configuration)

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization Tasks list to open a reset or image profile to define the expanded storage for an LP. The Initial, Initial storage origin, and Reserved fields are located on the Storage page for the LP. See Figure 42 on page 164.

Check your expanded storage definitions and consult your system programmer to ensure that they meet your processing needs.

Initial expanded storage

- The initial amount of expanded storage represents the amount of storage allocated to an LP when it is activated. Expanded storage cannot be defined for coupling facility mode LPs.
- Initial expanded storage is reconfigurable (can be configured offline or online by the control program) for ESA/390 LPs that have no reserved expanded storage defined.
- The initial amount of expanded storage can be zero when the reserved expanded storage is nonzero.
- A request for an initial expanded storage amount can be satisfied only when both sufficient expanded storage addressability and sufficient physical storage are available.

  Also, there must be a large enough contiguous central storage ***addressability range*** to back the initial expanded storage amount. This range will be chosen by the system in a top-down first-fit algorithm. It is not user-specifiable. If a large enough central storage ***addressability range*** is not available to satisfy the initial expanded storage request, LP activation will fail.

Reserved expanded storage

- Only LPs that specify a reserved expanded storage origin can be allocated storage within the reserved expanded storage for another LP. Reserved expanded storage can only overlap LPs that have an expanded storage origin specified.
- Expanded reserved storage is contiguous to and above the initial amount of expanded storage.
- ESA/390, z/VM, and Linux-Only LPs can have nonzero amounts for this parameter. Coupling facility LPs cannot have reserved expanded storage amounts.
- The reserved amounts of expanded storage defines the additional amounts of storage that can become available to an LP when no other activated LP has this reserved storage online. Reserved storage amounts are always offline after LP activation.
- For reserved expanded storage, all of the reserved expanded storage must be available to configure any reserved expanded storage online.
- Reserved expanded storage for an LP can be specified with or without specifying an origin.

  Also, there must be a large enough contiguous central storage ***addressability range*** to back the reserved expanded storage amount. This range will be chosen by the system in a top-down first-fit algorithm. It is not user-specifiable. If a large enough central storage ***addressability range*** is not available to satisfy the reserved storage request, the element cannot be brought online.

Expanded storage origins

- The origin for expanded storage defines the starting megabyte where the expanded storage ***addressability range*** begins for the LP. If enough expanded storage is not available to satisfy the initial request starting at this origin, LP activation will fail. If there is no initial amount of expanded storage defined, the reserved amount of expanded storage starts at this origin.
- There must be enough contiguous expanded storage ***addressability*** to fit the reserved amounts, but the reserved addressability can be in use by other LPs (that have expanded storage origins specified) at the time the LP is activated.
- For expanded storage, the specification of the origin parameter provides the only way to overlap storage definitions. For example, the reserved storage definition

for one LP can overlap the storage definition of another LP when the origin parameter is specified for both LPs. The total amount of expanded storage ***addressability*** that can be used to map expanded storage for LPs is ***at least twice*** the amount of ***installed*** storage. You can review current LP storage allocations by using the Storage Information task available from the CPC Operational Customization Tasks list.

- The availability of reserved expanded storage depends on whether or not you specify an expanded storage origin for an LP. By making the specification of an expanded storage origin optional, there are two implementations of dynamic storage reconfiguration for reserved expanded storage:
  1. If you do not specify an expanded storage origin, the reserved expanded storage is available for the LP when there is sufficient physical storage available to meet the reserved expanded storage request.

     Expanded storage can be reassigned between LPs that have noncontiguous address ranges. Reconfiguration is not limited to growing into an adjacent LP. LPs are eligible to use noncontiguous expanded storage if they have unique (not overlapping) storage range definitions. Specifying an origin is not required when defining a reserved storage amount for an LP and by not specifying an origin the LP is reserved an addressable storage range for its entire storage configuration (initial plus reserved amount). Not specifying an origin ensures no overlap.

     The reserved expanded storage is available for LPs that do not specify an origin when there is sufficient physical storage to meet the reserved expanded storage request.
  2. If you specify an expanded storage origin, the reserved expanded storage is only available for the LP when:
     – No other LP has this expanded storage address range online
     – There is sufficient physical expanded storage available to meet the reserved expanded storage request.
- If no origin is specified for an LP, the system assigns the storage to the LP using a top-down-first-fit algorithm.

Dynamic storage reconfiguration

Dynamic storage reconfiguration allows both central and expanded storage allocated to an LP to be changed while the LP is active. It is supported in ESA/390 LPs running z/OS. Dynamic storage reconfiguration is not supported in coupling facility, or Linux-Only LPs. z/VM 5.4 and later support dynamic storage reconfiguration (for central storage only) in any partition mode.

Dynamic storage reconfiguration provides the capability to reassign storage from one LP to another without the need to POR the CPC or IPL the recipient LP. Every LP has a storage range definition consisting of an origin, initial, and reserved amounts. The reserved value determines how much additional storage can be acquired using dynamic storage reconfiguration.

Storage is released when an LP is either deactivated or its reserved storage element is deconfigured. Additionally, you can release central storage in amounts smaller than the defined storage element size.

With dynamic storage reconfiguration, ESA/390 LPs can have reserved amounts of central storage and expanded storage. This storage can become available to the LP if no other active LP has this reserved storage online. Reserved central storage and reserved expanded storage can be made available to the LP by commands from the operating system console.

If the operating system running in the LP supports physical storage reconfiguration, use operating system commands to make the reserved storage available to the LP without disrupting operating system activities.

For z/OS, use the following command format to reconfigure central storage:

```
CF STOR(E=1),<OFFLINE/ONLINE>
```

Dynamic storage reconfiguration on the System z10 for central storage enables central storage to be reassigned between LPs that have noncontiguous address ranges. In this case, LPAR can allocate a “hole” or some set of central storage addresses for which there is no backing physical storage assigned. Later, LPAR is able to configure storage online to the LP by assigning some physical central storage to the hole.

Similarly, dynamic storage reconfiguration for expanded storage enables expanded storage to be reassigned between LPs that have noncontiguous expanded storage address ranges.

For central storage, you can reconfigure central storage in amounts equal to the storage granularity supported by the CPC. For z/OS, use the following command format:

```
CONFIG STOR(nnM),<OFFLINE/ONLINE>
```

Central storage dynamic storage reconfiguration examples

Figure 25 shows an example of central storage with dynamic storage reconfiguration capability. This figure shows LP-A, LP-B, and LP-C.

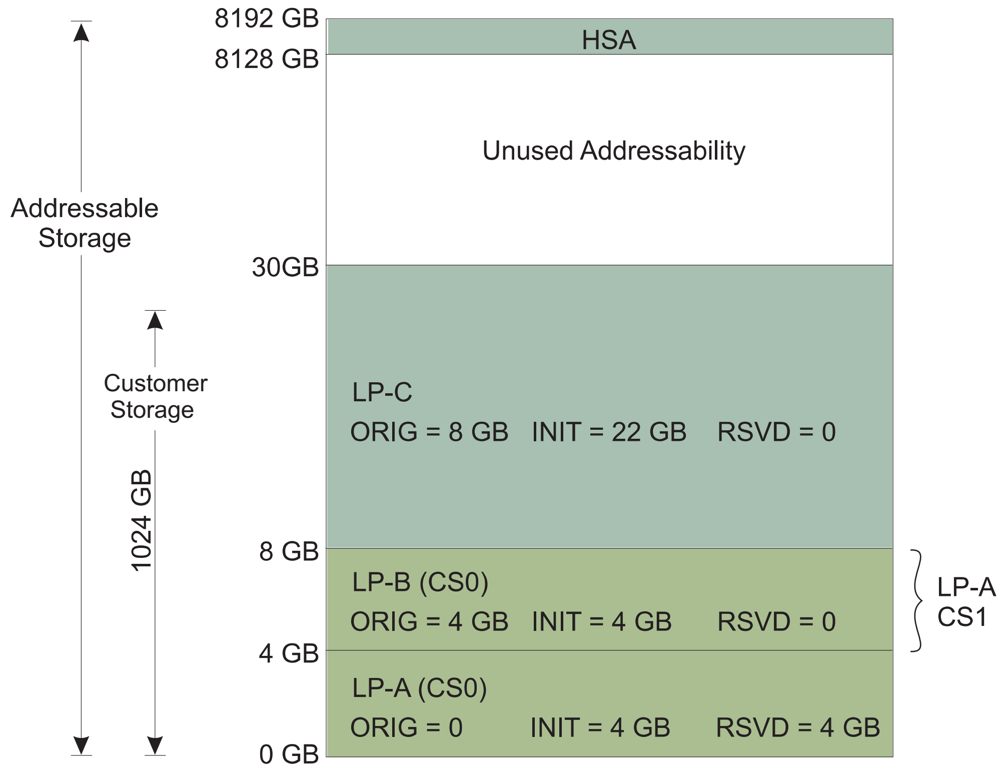


Figure 25. Central storage layout

To reconfigure central storage, deactivate LP-B to free up storage directly above LP-A. Figure 26 on page 109 shows how you may reconfigure central storage in this case.

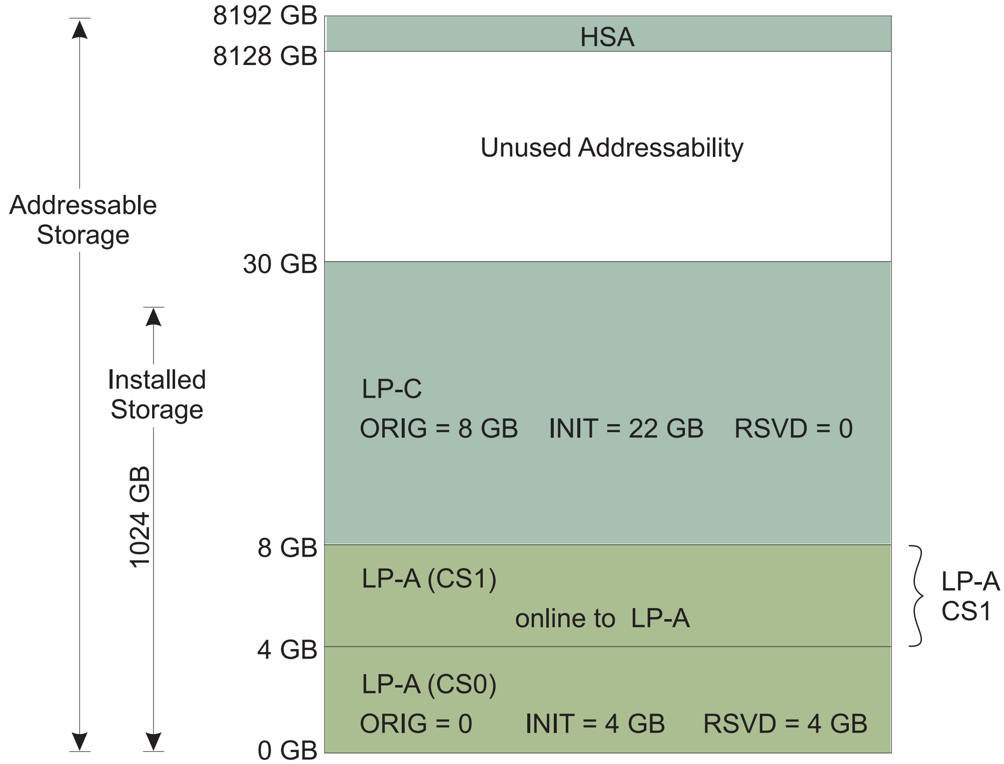


Figure 26. Reconfigured central storage layout

Figure 27 is another example of dynamic reconfiguration of central storage. For this example, assume the amount of customer storage is 1024 GB. The amount of addressable central storage used by hardware system area (HSA) is 64 GB in this example. The storage granularity is 256 MB. This leaves 8128 GB of central storage addressability to be allocated to LPs.

LP-A and LP-B are defined with an initial amount of 14 GB each of central storage, a reserved amount of 2 GB, and system determined central storage origins. LP-A and LP-B are activated and IPLed. At the completion of IPL, LP-A has its reserved central storage configured online by entering **CF STOR(E=1),ONLINE** from the z/OS software console for LP-A. Figure 27 shows the resulting storage layout following these actions.

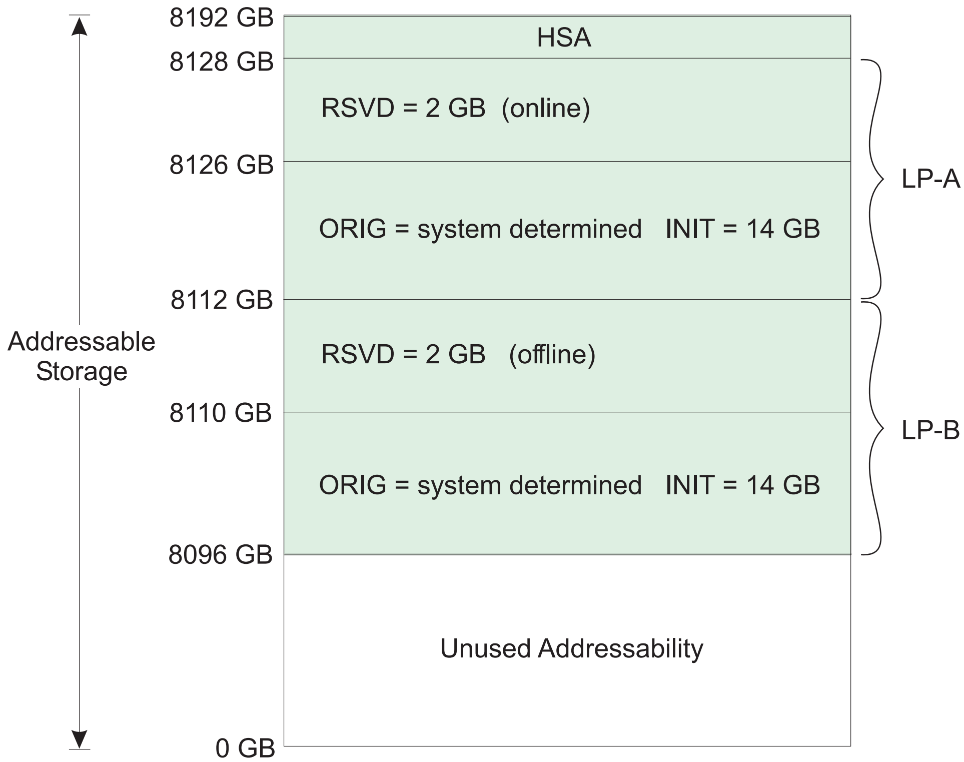


Figure 27. Initial central storage layout

At a later point in time, the reserved storage from LP-A can be reconfigured to LP-B. Note that both LPs should specify an RSU value of at least 8 (2048/256) for reconfigurations of storage to work. From the z/OS software console for LP-A, enter **CF STOR(E=1),OFFLINE**. Next, from the z/OS software console for LP-B, enter **CF STOR(E=1),ONLINE**. Figure 28 shows the resulting storage layout following these actions. The reserved storage is fully reconfigured without an outage to either LP. Also, the procedure can be reversed without an outage as well.

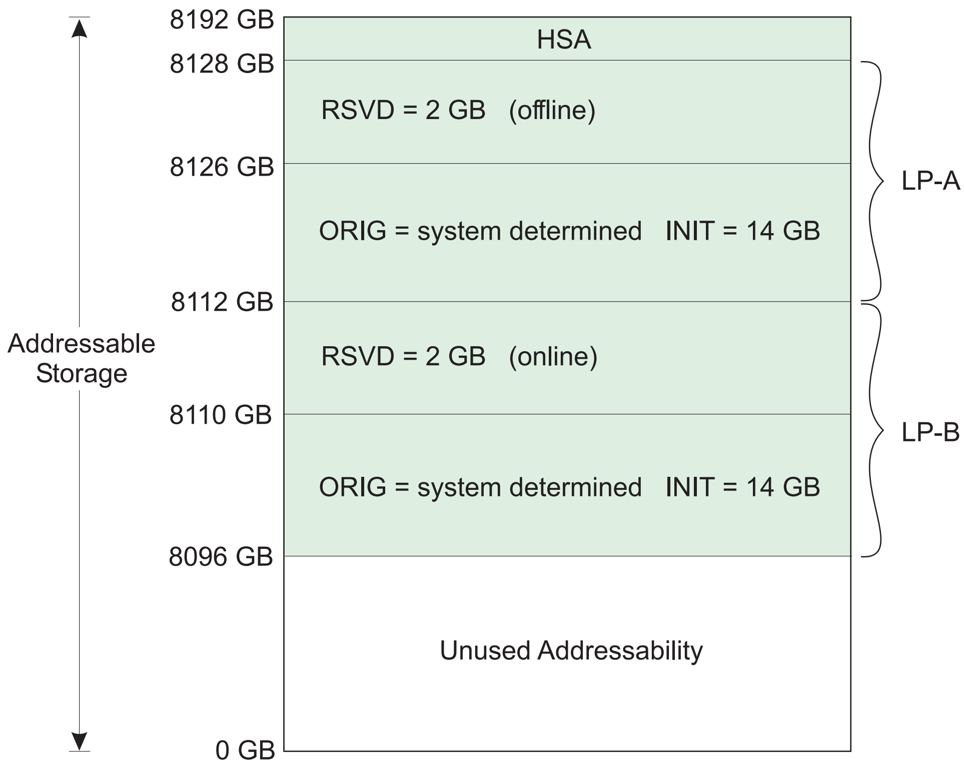


Figure 28. Central storage layout following reconfiguration

Figure 29 on page 112 and Figure 30 on page 113 are examples of dynamic reconfiguration of central storage. For this example, assume the amount of customer storage is 1024 GB. The amount of addressable central storage used by hardware system area (HSA) is 64GB in this example leaving 8128 GB of addressable storage for allocation to LPs. The storage granularity is 256 MB.

LP-A is defined with an initial amount of 14 GB of central storage, a reserved amount of 2 GB, and a system determined central storage origin. LP-B is defined with an initial amount of 14 GB of central storage, with a system determined central storage origin and an initial amount of 2 GB of expanded storage. The central storage addressability used to back online expanded storage is always system determined and in this case is coincidentally but not necessarily contiguous with the addressability used to back the logical partition's central storage. LP-A and LP-B are activated and IPLed. Figure 29 on page 112 shows the resulting storage layout following these actions.

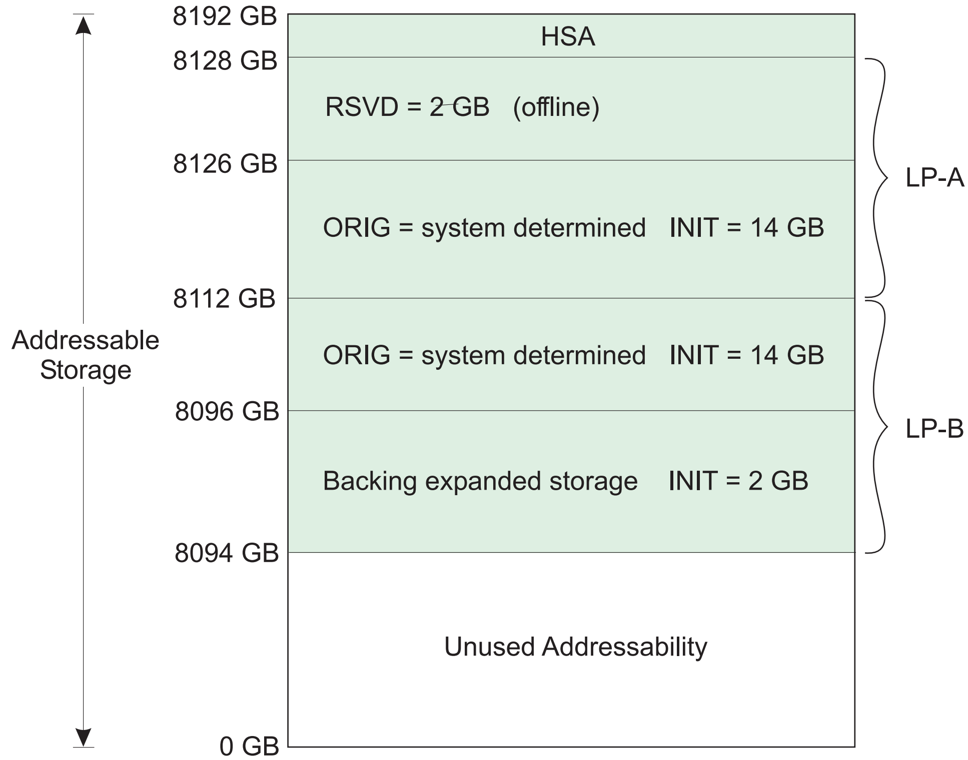


Figure 29. Initial central storage layout

At a later point in time, LP-B deconfigures its expanded storage and the physical storage that was used for its expanded storage is reconfigured to LP-A. Note that LP-A should specify an RSU value of at least 8 (2048/256) for reconfigurations of storage to work. First, from the z/OS software console for LP-B, enter CF ESTOR(E=0),OFFLINE. Next, from the z/OS software console for LP-A, enter **CF STOR(E=1),ONLINE**. Figure 30 shows the resulting storage layout following these actions. The reserved storage is fully reconfigured without an outage to either LP-A or LP-B.

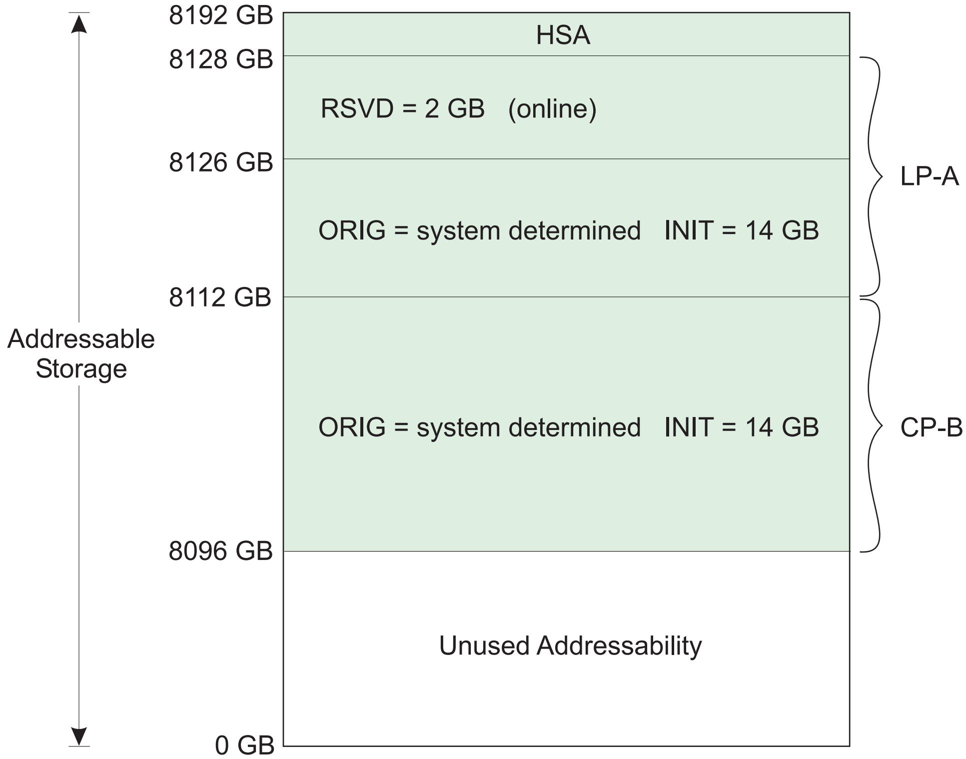


Figure 30. Central storage layout following reconfiguration

Recommendations for storage map planning

Planning storage maps as described below will help avoid storage fragmentation and remove dependencies on the order of activation of LPs.

For more information and examples of storage map planning, see the publications listed for dynamic storage reconfiguration in "About this publication" on page xiii.

Map all LPs that require an origin from the bottom up (that is, start with 0 MB and build upward).

If no origin is specified for an LP, the system assigns the storage to the LP using a top-down first-fit algorithm.

Operation considerations for dynamic storage reconfiguration:

- Initial central storage for an LP is allocated on logical storage element 0 and any reserved central is allocated on logical storage element 1.

- Whenever a load clear or system reset clear is performed on an LP, it forces the reserved central storage element offline. This allows z/OS to flag the reserved storage element as reconfigurable to allow it to be later deconfigured from the LP.

  Note: When z/OS is IPLed immediately after the LP is activated, the reserved central storage element is offline.
- Whenever z/OS is re-IPLed in an LP that has a reserved central storage element, a load clear or system reset clear followed by load normal should be performed to force the reserved central storage element offline.
- When a standalone dump is to be performed on an LP, perform a load normal (not a load clear) on that LP to keep the reserved storage element online and preserve the storage contents.

CPCs with the Sysplex Failure Manager (SFM)

The Sysplex Failure Manager (SFM) allows you to reset and reconfigure one or more logical LPs and their related storage. SFM allows workload redistribution from the failed primary system to the backup system without operator intervention. For a detailed description of how SFM works, see the z/OS Setting Up a Sysplex publication.

Note: SFM reset/deactivate functions are not compatible with the z/OS AutoIPL function (which is supported on z/OS 1.10 and higher). For example, suppose AutoIPL is being used on a particular z/OS system (LP) to automatically re-IPL that system if it requests a disabled wait state to be loaded. Clearly it is not desirable to have that same LP be the target of one of these cross-partition Reset or Deactivation functions, because these actions will prevent the system from re-IPLing itself successfully via AutoIPL.

To allow an LP to initiate these functions, use the Customize/Delete Activation Profiles task to open a reset profile to authorize an LP to issue instructions to other LPs. The Cross partition authority check box is located on the Security page for the LP.

The following functions exist for SFM:

- Cross Partition System Reset

  This function causes a specified LP to be reset. The reset is accomplished via the RESETTIME(nnn) keyword in the SYSTEM statement of the z/OS SFM policy.
- Cross Partition Deactivation

  This function causes a specified LP to be deactivated. The deactivation is accomplished via the DEACTTIME(nnn) keyword in the SYSTEM statement of the SFM policy, and also, the RECONFIG statement in the SFM policy with a specific TARGETSYS(sysname) specified.
- Cross Partition Nonspecific Deactivation

  This function causes all logical partitions which are currently using any portion of the reconfigurable central or expanded storage of the issuing partition to be deactivated. The issuing partition is not deactivated. The nonspecific deactivation is accomplished via the RECONFIG statement in the SFM policy with a non-specific TARGETSYS(ALL) issued.

The Automatic Reconfiguration Facility (ARF) function is a hardware/LPAR function that is part of the cross-partition authority control setting. ARF functions are used by

SFM policy functions within z/OS, when RESETTIME, DEACTTIME, or the RECONFIG statement is coded in the SFM policy.

TARGETSYS(ALL) examples

Specifying an Origin: Assume that the backup partition has specified an origin, minimal initial storage, and a large amount of reserved storage. Since the backup system does not own its complete addressable range, two other partitions, are defined in the reserved storage of the backup partition. See Figure 31 for the storage layout before nonspecific deactivation.

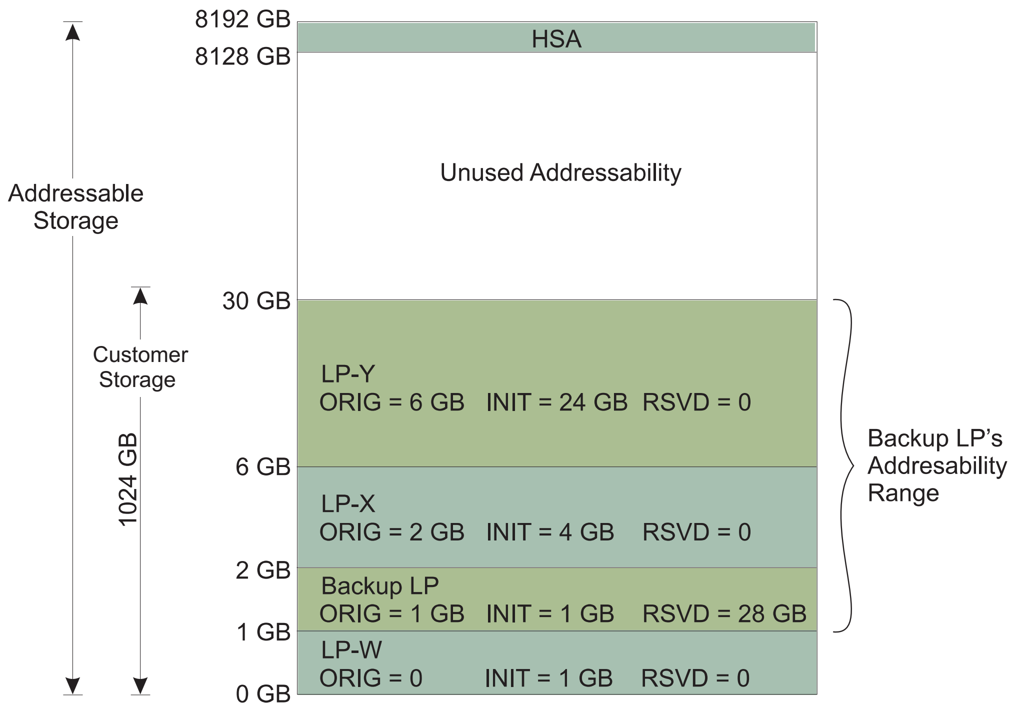


Figure 31. Backup partition layout before nonspecific deactivation

Assume that the backup LP has been given cross partition authority. See Figure 32 on page 116 for the storage layout at the completion of a takeover by the backup LP.

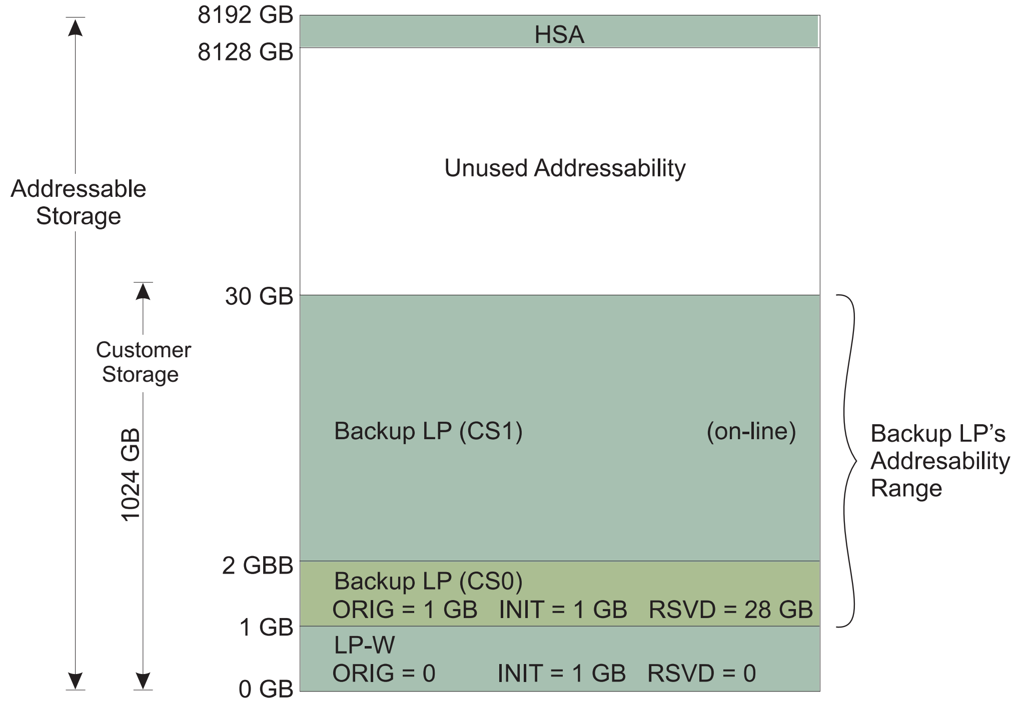


Figure 32. Backup partition layout after nonspecific deactivation

Number of central processors

The CPs defined to an LP are called logical CPs. The total number of initial logical CPs for each LP cannot be greater than the number of physical CPs installed. CPs can be dedicated to LPs or shared by LPs (*sharing* LPs).

The number of CPs defined for an LP represents the number of logical CPs on which the control program will dispatch work and is determined by several factors as described in "Maximum number of central processors" on page 117.

On a System z10, you can optionally install one or more Internal Coupling Facility (ICF) features for use by a coupling facility LP and/or one or more Integrated Facility for Linux (IFL) features for use by a Linux-Only LP. See "Coupling facility LPs using dedicated Central Processors (CPs) or dedicated Internal Coupling Facility (ICF) CPs" on page 119.

You can also optionally install one or more zAAP features for use by an LP. The total number of initial logical zAAPs for each LP cannot be greater than the number of physical zAAPs installed.

You can also optionally install one or more zIIP features for use by an LP. The total number of initial logical zIIPs for each LP cannot be greater than the number of physical zIIPs installed.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization Tasks list to open a reset or image profile to define the number of CPs for an LP. The Number of processors field is located on the Processor page for the LP.

Maximum number of central processors

The maximum number of CPs that can be defined depends on:

- The number of CPs that are available.

  The maximum number of logical CPs available for definition in a single LP is the total number of CPs achievable via concurrent CPU upgrade, or 64, whichever is less.

  Notes:

  1. The maximum initial logical CPs defined for a dedicated partition ***equals*** physical CPs online for the current model ***minus*** physical CPs currently dedicated and online to other dedicated partitions ***minus*** the maximum online number of shared CPs among all the activated logical partitions that are using shared CPs.
  2. The maximum initially online logical CPs defined for a shared partition ***equals*** physical CPs online for the current model ***minus*** physical CPs currently dedicated and online to other partitions using dedicated CPs.
  3. The preceding rules for maximum CPs apply independently to each type (general purpose, ICF, IFL, zAAP or zIIP) of processor defined to the logical partition. For instance, when defining a logical partition to use a combination of general purpose CPs and zAAPs/zIIPs, the rules for the maximum initially online of each type of processor is calculated independently against what is currently installed and in use for that type of physical processor.

- The number of CPs that are supported by the required control program.

  Some control programs support as many as 64 CPs. The number of CPs defined for an LP should not exceed the number supported by the control program used for that LP. The stated maximum supported processors for a particular control program is applied against the sum of the counts of all processor types defined to the partition.

Workload requirements

The number of logical CPs defined also depends on the workload requirements and the ability of the control program or application program to effectively use multiple logical CPs.

- The number of CPs required to meet the peak demands of the LP

  When a sharing LP is activated, it should be assigned enough CPs to meet its peak demands and any immediate growth requirements.

  Note: Too few CPs could limit the number of potential transactions, and too many active logical CPs could affect performance. In addition to a number of initially online logical CPs sufficient to meet the current peak demands of the LP, the definition should include the number of reserved logical CPs required for possible growth requirements.

  For an LP that uses dedicated CPs, the number of CPs required to meet peak demand should be determined.

- The number of CPs shared by an LP

  The physical CPs used by a sharing LP can be limited by the number of CPs defined to it. For example, on a six-way CPC, a two-way LP could never get more than a third of the CP resources.

  On most machines, there are many possible configurations. For example, if a two-way CPC is to be used by three sharing LPs, configuration options include all two-way LPs, all one-way LPs, or a mix of one-way and two-way LPs.

  Three two-way LPs should only be considered if all LPs have peak demands exceeding the capacity of a one-way CPC. In this instance, the average requirements during peak periods should be examined carefully to ensure that the total does not exceed the capacity of the CPC.

Three 1-way LPs are optimal for ITR performance and should be used if no LP has peaks exceeding half of the capacity of a two-way CPC.

Central processor recommendations for Intelligent Resource Director (IRD)

It is highly recommended that the number of initial CPUs specified be maximized for logical partitions whose CPU resources, enabled by IRD clustering technology, are managed by z/OS's WorkLoad Manager (WLM). WLM's LPAR CPU Management component will automatically configure ***off*** all initially online logical CPs in excess of the minimum required to meet current demands so over-specification has no negative consequences.

Moreover, only those logical CPs defined as initially online, or configured ***on*** explicitly by operator commands, will subsequently be configured ***on*** by WLM if and when increases in workload requirements demand. Specification of reserved logical CPs should be used only to accommodate potential increases to the number of installed physical CPs.

WLM CPU management does not currently manage any zAAP or zIIP logical processors defined to a WLM managed logical partition. As such, the maximizing of initial CPUs recommendation applies only to the general purpose processor definition for the logical partition; not the zAAP or zIIP definition. Maximizing reserved zAAPs and zIIPs is still recommended to allow for concurrently adding logical zAAPs or zIIPs to the partition if needed.

WLM managed CPs cannot have dedicated CPs. Though capping of shared CPs is also disallowed, WLM's License Manager component may soft-cap logical CPs when a LPs rolling 4-hour average CPU utilization has reached its defined capacity. (See "Workload charging by soft-capping to a defined capacity" on page 136.)

Processor considerations for Linux-only LPs

A Linux-Only mode LP can be allocated either general purpose CPs or IFLs. For optimum cost-effectiveness, IFLs should be used whenever possible. Choose IFL CPs on the Processor page of the Customize/Delete Activation Profile task. IFLs can be allocated to a Linux-Only mode LP as either dedicated or shared. Unlike Coupling Facility mode LPs, Linux-Only LPs cannot be defined with a mix of dedicated and shared processors or a mix of general purpose and ICF processors.

Utilization of IFLs will be included in the data reported for ICF CPs in RMF Partition Data reports and other similar reports. There is no way to distinguish on such a report between data reported for ICF CPs and IFLs.

A Linux-Only LP, whether allocated IFLs or general purpose CPs, will not support any of the IBM traditional operating systems (such as z/OS, TPF, or z/VSE). Only Linux or z/VM with only Linux and OpenSolaris guests can run in a Linux-Only mode LP. Logical partitions defined as Linux-Only that attempt to load a traditional operating system will be system check-stopped.

Processor considerations for coupling facility LPs

You can define a coupling facility to use any one of the following combinations of CP definitions:

- One or more dedicated general purpose CPs

- One or more shared general purpose CPs
- One or more dedicated ICF CPs
- One or more shared ICF CPs

Any other combination of processor definitions is not supported.

Coupling facility LPs using dedicated Central Processors (CPs) or dedicated Internal Coupling Facility (ICF) CPs

Important Note

IBM **strongly** recommends using dedicated CPs or dedicated ICFs for production coupling facility LPs because coupling facility channel paths and requests have critical response time requirements. When the coupling facility is running on a dedicated CP or dedicated ICF CP, an “active wait” polling algorithm is used to look for coupling facility requests. This results in the fastest response time and throughput possible for coupling facility requests.

Considerations for coupling facilities using Internal Coupling Facility (ICF) CPs: The following considerations apply to coupling facility LPs that use ICF CPs.

- ICF CPs are managed separately from general purpose CPs. Their presence and usage does not affect any of the definition or activation rules pertaining to LPs that use general purpose CPs.
- ICF CPs will appear in RMF Partition Data reports and other similar reports only when an LP is activated and assigned to use an ICF CP.
- Non-ICF work is never allowed to be run on an ICF CP. Only PR/SM (to manage the CP) or a logical partition defined to use ICFs is allowed on the ICF CP.

Coupling facility LPs using shared Central Processors (CPs) or shared Internal Coupling Facility (ICF) CPs

Using shared CPs for coupling facility LPs has the following considerations. The same set of considerations for using shared CPs equally apply to using shared ICF CPs.

- You should ***not*** cap the processing weights for a coupling facility LP. If you cap processing weights and you are running a coupling facility, LPAR attempts to support the cap but may not be successful and the system can be less responsive.
- A CF with shared CPs may use less CPU resource, but this may come at an expense to performance. The CF LIC runs in a polling loop so it always looks busy, even if there is little CF activity. If the CF is sharing a CP with a z/OS image that has low CPU demands, the CF could use the entire CP. If the CF is sharing CP(s) with another CF, both will look busy and the CPU resource will be split between them. For example, if a production CF and a test CF shared a CP with equal weights, each would only have use of one-half the CP. This would appear on the RMF CF Usage Summary Report as LOGICAL PROCESSORS: DEFINED 1 EFFECTIVE 0.5.

  Requests to a CF that is sharing a CP may have to wait if another image (z/OS or CF) is using the shared CP. In fact, the CF’s logical CP may have to wait for several logical CPs of other partitions to run before it runs again. This has the net effect of elongating response times. Requests to the CF that could typically take several microseconds in a dedicated environment can be elongated by many milliseconds, easily 12.5 to 25 milliseconds or more. If CF response time is not a consideration (for example, a test CF or a backup CF), the installation can further limit CF usage of CPU resource by enabling the Dynamic Dispatch option.

This will periodically pause the polling loop. The number and length of the pauses is determined by the activity in this CF. While this gives more CPU resource to the other partitions that are sharing the CP, it elongates the service time in this CF, in most cases, by a considerable amount.

- Shared ICF and shared general purpose processors are each managed as separate “pools” of physical resources. As such, the processing weights assigned to logical partitions using shared ICF processors are totaled and managed separately from the total weights derived from all of the logical partitions using shared general purpose processors. Similarly, when the processor running time is dynamically determined by the system, the calculation of the dynamic running time is performed separately for each pool. If a user supplied run time is specified, this will apply to both processor pools.
- RMF identifies which logical and physical CPs are of each type when both general purpose and ICF processors are present in the configuration on its partition data report.
- An uncapped coupling facility LP honors its processing weight up to a point. PR/SM LPAR attempts to help ensure that each logical CP defined to a coupling facility LP gets at least 1 run time interval of service per every 100 milliseconds. For example, for a typical 12.5 millisecond run time interval, each logical CP gets 1/8th of a physical CP. This can translate into a response time elongation that is several thousand times as long as a typical CF request using dedicated CPs.

  With dynamic coupling facility dispatch, the coupling facility will not necessarily consume entire run time intervals at low request rate times. In low request rate times, each coupling facility engine can consume far less than 1/8th of a physical CP. The CP resource consumption can be more in the 1-2% range. At higher request rates (for example, when the coupling facility is actually busy handling requests), the 1/8th minimum will again become effective.

  Note: Anticipated processor usage by a coupling facility may spike much higher than what you would intuitively expect given the non-CF workload. For instance, system reset of a system or logical partition that was communicating with (connected to) a coupling facility can temporarily cause a considerable increase in the demands placed on the coupling facility.
- All requests to coupling facilities from z/OS LPs that share CPs with a coupling facility are treated internally to the machine as asynchronous requests. This is true even if the requests are to a coupling facility that the z/OS LP is not sharing CPs with. This conversion is transparent to z/OS but it can result in increased synchronous service times to the coupling facility as reported by RMF. As far as the operating system, RMF, and the exploiter code is concerned, the requests that are initiated synchronously by software are still being processed synchronously, and they show up as such on RMF reports.
- Choose a weight for the coupling facility LP based on the anticipated CP requirements of the coupling facility. When deciding how much CP resource should be given to each coupling facility logical CP, consider the following:
  - When using dynamic CF dispatching, the weight for the coupling facility can safely be set to a value that affords the proper CP resources to the coupling facility in times of the highest volume of requests to the coupling facility. In low request rate periods, the coupling facility will automatically throttle back on its CP usage making the CP resource available for redistribution to the other defined LPs in the configuration. Also, note that at low request rate times, RMF Coupling Facility Activity Reports will show some elongation in response times for requests to the coupling facility. With the low rate of these requests, overall system performance should not be noticeably impacted.

- CP resource requirements vary depending on the coupling facility exploiter functions and your sysplex hardware and software configuration. As a general guideline, when the anticipated CP requirement of the coupling facility is less than one physical CP, set the weight of the coupling facility LP so that the coupling facility logical CP has 50% or more of a physical CP resource. If you have less than a full physical CP allocated to the coupling facility logical CP, **this will result in elongation of response times**.

  Examine the RMF Coupling Facility Activity Report and tune the coupling facility LP weight until your performance requirements are met.

  Note: When examining the RMF Coupling Facility Activity Report, you may see elongated average response times. Usually, these are accompanied with high standard deviations as well. This indicates most requests are in the expected range with an occasional very elongated response that throws the average off.
- Give more weight to the coupling facility LP for functions that have more stringent responsiveness requirements. For example, you can set the coupling facility weight higher for coupling facility exploiter functions such as IMS/IRLM. For IMS/IRLM, you may want to set the weight of the coupling facility LP so that each coupling facility logical CP runs almost dedicated. For example, you may want to set a weight that will give each coupling facility logical CP 95% or more of physical CP resources. In another case, if the CF contains structures which are using System Managed Duplexing, you should set the weight of the coupling facility LP so that the coupling facility CP has at least 95% of a physical CP. If the coupling facility has less than 95% of a physical CP, there is a possibility that response from the partner of the duplexed structure will timeout and the duplexing of that structure will cease.
- Less weight may be required for coupling facility exploiter functions, such as the JES2 Checkpoint data set. If your coupling facility is being used exclusively as a JES2 checkpoint, your coupling facility responsiveness requirements may be less stringent. If this is the case, try decreasing the weight of the coupling facility LP so that each coupling facility logical CP receives, for example, 40-50% of physical CP resources.
- As the total traffic (requests per second) to the coupling facility increases, there is a greater need for real coupling facility CP time. To a point, the increase in traffic may not require an increase in the coupling facility LP weight. This is because coupling facility active wait time turns into coupling facility busy time. You must monitor coupling facility utilization and adjust the LP weight to help ensure that your performance requirements are being met.

- Even in a test environment, the above guidelines should be followed. Optimally, a weight resulting in approximately 50% or more of a processor should be made for each coupling facility logical processor. ***Failure to provide sufficient weight to a coupling facility may result in degraded performance, loss of connectivity, and possible loss of coupling links due to time-outs.*** Dynamic CF dispatching must not be disabled. Dynamic CF dispatching is automatically enabled by default for coupling facility LPs that are using shared general purpose CPs. Additionally, processor resource capping of the coupling facility logical partition(s) logical CPs must **not** be enabled.

Considerations for coupling facilities running on uniprocessor models

On a uniprocessor or smaller machine, IBM strongly recommends that coupling facility LPs should not share general purpose CPs with non-CF workloads (for example, z/OS), even in a test environment. ***Such a configuration carries with it significant risks of degraded performance, loss of connectivity, and possible***

loss of coupling links due to time-outs and must not be used for a production level system. For production configurations, IBM strongly recommends using one or more internal coupling facility (ICFs) CPs for the coupling facility LPs.

For a test configuration only, if this option is not available and coupling facility LPs must share a general purpose CP with non-CF workloads, diligent adherence to the preceding recommendations for coupling facilities using shared CPs will minimize undesirable consequences.

For greater detail on how to plan for and set up a parallel sysplex in a shared CP environment, please see the following:

| **MVS/ESA™ Parallel Sysplex Performance - LPAR Performance
| **Considerations for Parallel Sysplex Environments** (http://www-03.ibm.com/
| support/techdocs/atsmastr.nsf/WebIndex/FLASH10002)

Processor considerations for z/VM mode LPs

You can define a logical partition to use one or more zAAPs, zIIPs, IFLs, and ICFs with z/VM 5.4 or higher with either of the following combinations:

- One or more dedicated general-purpose CPs and one or more dedicated zAAPs/zIIPs/IFLs/ICFs.
- One or more shared general-purpose CPs and one or more shared zAAPs/zIIPs/IFLs/ICFs.

The partition mode must be set to ″z/VM″ in order to allow zAAPs, zIIPs, IFLs, and ICFs to be included in the partition definition.

In a z/VM mode partition, z/VM will:

- Operate z/TPF, z/VSE, and z/OS guests on CPs.
- Operate Linux on System z® and OpenSolaris guests on IFLs and optionally on CPs.
- Offload z/OS guest system software process requirements, such as DB2 workloads, on zIIPs, and optionally on CPs.
- Provide an economical Java execution environment for z/OS guests on zAAPs, and optionally on CPs.
- Operate coupling facility virtual machines in support of a Parallel Sysplex test environment on ICFs and optionally on CPs.

For additional information about using these capabilities of z/VM, refer to *z/VM Running Guest Operating Systems*, SC24-6115.

Processor considerations for LPs with multiple CP types

You can define a logical partition to use one or more zAAPs and/or zIIPs with z/OS 1.7 or higher with either of the following combinations:

- One or more dedicated general purpose CPs and one or more dedicated zAAPs/zIIPs
- One or more shared general purpose CPs and one or more shared zAAPs/zIIPs

The mode specified for the logical partition must be set to ″ESA/390″ in order to allow the definition of zAAPs or zIIPs to the logical partition as stated above.

Dedicated central processors

An LP can have CPs dedicated to it. When an LP that uses dedicated CPs is activated, a physical CP is assigned to each defined logical CP. The LP then has exclusive use of its physical CPs.

The physical CPs that belong to an LP that uses dedicated CPs are always available for its use, but the capacity that is not used cannot be used by other LPs.

For coupling facility considerations, see "Processor considerations for coupling facility LPs" on page 118.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization Tasks list to open a reset or image profile to define dedicated CPs for an LP. The Dedicated field is located in the Logical processor assignment group box on the Processor page for the LP.

Suitable workloads

Workloads best suited for logical partitions that use dedicated processors are those that maintain a fairly even external throughput rate (ETR) while using most of the capacity of the logical partition. Logical partitions with timing dependencies might require dedicated processors.

The installation goals for a logical partition that uses dedicated processors should be similar to the goals of the processor complex. For example, if the goal is an average processor utilization rate of 70%–85%, then the same goal should be used for a logical partition that uses dedicated processors.

Shared central processors

LPs can share CPs with other LPs. A sharing LP does not have exclusive use of the physical CPs. There is no correspondence between the logical CPs in a sharing LP and the physical CPs on which the logical CPs are dispatched (except on a one-way CPC). A logical CP can be dispatched on any physical CP and, on successive dispatches, the logical CP can be dispatched on different physical CPs.

The number of CPs available for use by sharing LPs is determined by adding the number of CPs already assigned to active, dedicated LPs and subtracting that sum from the total number of physical CPs available.

The total of all logical CPs for all sharing LPs can be larger than the number of physical CPs serving the sharing LPs. For example, if four LPs are active on a six-way CPC and each LP is defined to have four CPs, the total number of online logical CPs is 16.

For coupling facility considerations, see "Processor considerations for coupling facility LPs" on page 118.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization Tasks list to open a reset or image profile to define shared CPs for an LP. The Not dedicated field is located in the Logical processor assignment group box on the Processor page for the LP.

Suitable workloads

Workloads best suited for sharing logical partitions are those that have a widely fluctuating ETR or would not fit well into the capacity of a dedicated logical partition. If a workload can use only a small portion of the capacity of a dedicated logical partition, redefine the logical partition to use shared processors to free the available capacity for use by other logical partitions.

A workload with a widely fluctuating ETR would experience peaks and valleys in its processor-utilization curve. Such fluctuations can occur over extremely short periods of time (minutes or seconds). This type of workload could take advantage of the time- and event-driven dispatching available. With event-driven dispatching, a sharing logical partition receives the resources required as needed and leaves the capacity free for other logical partitions when not needed. See “Wait completion” on page 134.

When combining workloads on a processor complex by means of logical partitions, examine their average and peak requirements carefully. If the workloads fluctuate over very short intervals, the total capacity of the system must meet the sum of the average requirements for each workload. If processor utilization fluctuates over longer periods, and the peak utilization periods for these workloads occurs simultaneously, then the total capacity of the logical partitions must meet the sum of the peak requirements for each workload.

Sharing logical partitions that use event-driven dispatching are better able to maintain high transaction rates with fluctuating demand while being responsive. However, the ITR for a sharing logical partition is lower than the ITR for a dedicated logical partition.

The capability to limit CPU usage for any or all logical partitions with shared processors is provided by the PR/SM capping function. The capping function enhances LPAR workload balancing controls for environments with a requirement that the CPU resources for a logical partition be limited. Capped logical partitions are recommended for use when CPU resources must be limited for business reasons (in accordance with a contract), or when the impact that one logical partition can have on other logical partitions needs to be limited.

Processing weights

An LP with dedicated CPs is not affected by processing weights.

Processing weights are used to specify the portion of the shared CP resources allocated to an LP. Although PR/SM always manages sharing LPs according to the specified processing weights, there are times when an LP will receive either more or less than its processing share:

- An LP will receive more than its processing share when there is excess CP capacity, provided it has work to do and other LPs are not using their share.
- An LP will receive less than its processing share when its workload demand drops below the capacity specified by its weight.
- An LP will not receive more than its processing share when the CP resources for that LP are capped.

The recommended procedure is to specify processing weights to satisfy the peak requirements of the LPs.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization Tasks list to open a reset or image profile to define the processing weight for a shared LP. The Processing weight field is located in the Logical processor assignment group box on the Processor page for the LP.

Use of processing weights: As an example, consider a system with 6 CPs and 3 LPs defined as follows:

```
LP Name   Logical CPs   Weight
-------   -----------   ------
ZVSE           1         300
ZOSTEST        6         100
ZVM            2         900
```

Processing weights can range from 1 to 999 (weights of less than 2% difference are not considered significant) and are used as follows:

- The processing weights for all active, sharing LPs are added together. This total is considered to be 100% of the processing resource available to shared CPs.
- The share of processing resources for each LP is calculated by dividing the processing weight for each sharing LP by the total processing weight. For example, at peak CP utilization levels, the dispatcher allocates shared processing resources to each of the LPs as follows:

```
ZVSE        300/1300 = 23.1%
ZOSTEST     100/1300 =  7.7%
ZVM         900/1300 = 69.2%
```

- The share of processing resource for each online logical CP with HiperDispatch disabled in the logical partition is calculated by dividing the share for each LP by the number of online logical CPs. The share for each logical CP is as follows:

```
ZVSE       23.1/1 CP  = 23.1%
ZOSTEST     7.7/6 CPs =  1.3%
ZVM        69.2/2 CPs = 34.6%
```

  These percentages are used to determine preemption priority for I/O interruptions. A lower priority logical CP can be preempted when an I/O interruption is pending for a higher priority logical CP when the following occurs:
  - The higher priority logical CP is further behind in its share, or
  - The higher priority logical CP is not as far ahead of its share as the lower priority logical CP.

  For example, the lower priority LP is receiving 15% more than its processing share, and the higher priority LP is receiving 10% more than its processing share.

As long as there is excess CP capacity, processing weights have no effect on the CP resources consumed. Weights affect processing when the number of logical CPs that need processing time is greater than the number of physical CPs available.

Processing weights and shared CP, ICF, zAAP, IFL and zIIP processors: Shared general purpose, ICF, zAAP, IFL and zIIP processors are each managed as separate "pools" of physical resources. The processing weights assigned to logical partitions using shared ICF, zAAP, IFL, zIIP or general purpose processors are totaled and managed together only with the total weights from all of the logical partitions using the same processor type. The calculations shown in previous examples as well as the examples to follow are done independently for general purpose, ICF, zAAP, IFL, or zIIP processors, on a machine that has them.

Processing weights for logical partitions with multiple shared CP types: When a logical partition is defined to use one or more shared general purpose CPs and one or more shared zAAPs/zIIPs, each of the types of logical processors is managed independently. The shared general purpose CPs compete with all other shared general purpose CPs defined in other logical partitions in the configuration. The zAAPs compete with all other shared zAAPs defined in other logical partitions.

The zIIPs compete with all other shared zIIPs defined in other logical partitions. General purpose, zAAP, and zIIP processors each have a separate processing weight specified. Note that if WLM weight management is being used for such a logical partition, only the weight of the shared general purpose processor portion of the logical partition will be altered by WLM. The specified weight for an LP's zAAP/zIIP processors is unaltered by WLM.

Effects of processing weights: Several implications are derived from the rules described above. First, every time a sharing LP is activated, the share of all other active LPs, using the same processor types, changes. This happens because the total of the processing weights has changed.

Because the processing share of LPs can vary, the actual utilization reported by monitors such as RMF can be different from the weights. In systems at less than 100% utilization, some LPs could receive greater than their share if other LPs are not using their share. The number of CPs defined also affects the maximum resource allocated to that LP. For example, an LP defined to have two CPs on a three-way CPC can never be allocated more than 67% of the CP resources no matter what its processing weight.

Capping processing weights: The PR/SM capping function provides the capability of limiting CPU resource usage for one or more LP. The relative processing weight of an LP is its capping value.

A capped LP running at its cap does not have access to the CP resources that are not utilized by other LPs. However, CP resources that are not used by a capped LP can be used by other LPs. Equitable distribution of CP resources is maintained.

Capping values can be dynamically adjusted. The capping function can be turned on and off, and provides the capability of specifying capping for individual LPs without a re-IPL of the LP.

Use the Change Logical Partition Controls task from the CPC Operational Customization Tasks list to change the Capped setting for the specific partition. Checking the Initial Capping check box turns the capping function on. Select the Save Running System push button to have this option take effect immediately for an active partition. (Save and Change will change the running system and update the partition's profile. Save to Profiles will not change the running system; it will just save the new definition to the partition's profile.) Alternatively, if you do not need to change a running system, the Customize/Delete Activation Profiles task available from the CPC Operational Customization Tasks list can be used to open a reset or image profile to cap processing weight for an LP. This change would take effect when the partition is activated.

With HiperDispatch disabled, an LP's relative weight is divided by the number of shared logical CPs online for the LP to give the share for each logical CP. The goal of the LPAR dispatcher is to give each logical CP its share of the total relative weight. Capping is done on a logical CP basis.

An LP's share of CP resources is determined by its weight. The combined processing weights for all active LPs are considered to be 100% of the available shared CP resources. The activating and deactivating of LPs changes the amount of CP resources available to LPs, making the percentage of CP resources requested for each active LP a relative one, and not a fixed percentage of CP resources.

Note: If an extremely low processing weight is specified for a capped logical partition, tasks such as Reset Clear, Activate, and Deactivate may fail due to a time-out. To prevent this problem, avoid use of capping in conjunction with low processing weight. A preferable solution is specification of a processing weight that results in a 1/10 share (the suggested minimum) or greater of one physical CP for a logical CP. If the extremely low weight cannot be avoided, temporarily turn capping off for the logical partition prior to activating, deactivating, resetting, or loading the logical partition. Restore the cap following completion of these operations.

Enforcement of processing weights

Processing weight management

PR/SM LPAR enforces LP processing weights as follows:

- For LPs with processor resource capping, PR/SM LPAR enforces the processing weights to within 3.6% of the LP's physical CP share for logical CPs entitled to 1/10 or more of one physical CP. Typically, PR/SM LPAR will manage processing weights to within 1% of the LP's physical CP share. See "Example 1. With processor resource capping."
- For LPs ***without*** processor resource capping, PR/SM LPAR enforces the processing weights to within 3.6% of the LP's physical CP share for logical CPs entitled to 1/2 or more of one physical CP. Typically, PR/SM LPAR will manage the processing weights to within 1% of the LP's physical CP share. See "Example 2. Without processor resource capping" on page 129.
- If a logical CP falls outside the enforceable ranges for logical CPs entitled to less than 1/10 of a physical CP using capping or less than 1/2 of a physical CP not using capping, PR/SM LPAR enforces the processing weights to within 3.6% of the total capacity of the shared physical CP resources. However, PR/SM LPAR should typically manage the processing weights to within 1% accuracy.
- Unused CP cycles to which a logical CP is entitled are made available to other logical CPs in proportion to the weights set for the other logical CPs.
- An uncapped coupling facility LP with shared CPs and coupling facility channels defined honors its processing weight up to a point. PR/SM LPAR attempts to help ensure that each logical CP defined to a coupling facility LP gets at least 1 run time interval of service per every 100 milliseconds. For example, for a typical 12.5 millisecond run time interval, each logical CP gets 1/8th of a physical CP.

Processing weight management examples

For the formulas used in the following two examples, see "Processing weight management formulas" on page 129.

Example 1. With processor resource capping: In the following example:

- Six physical CPs are online
- All LPs are capped
- All LPs have sufficient workload demand to use their shares

Table 14. PR/SM LPAR processor weight management with processor resource capping and with HiperDispatch Disabled

LP	LCPs Online	Weight (1)	Weight per LCP	LCP % of PCP	3.6% Share	3.6% Total	Resulting Weight Range	Resulting Utilization Range
A	6	500	83.3	50	3.0	–	80.3–86.3	48.2%–51.8%
B	3	480	160.0	96	5.8	–	154.2–165.3	46.3%–49.7%

Table 14. PR/SM LPAR processor weight management with processor resource capping and with HiperDispatch Disabled (continued)

LP	LCPs Online	Weight (1)	Weight per LCP	LCP % of PCP	3.6% Share	3.6% Total	Resulting Weight Range	Resulting Utilization Range
C(2) C(3)	3	20	6.7	4	0.2	– 12	6.5–6.9 0.0–18.7	2.0%– 2.1% 0.0%– 5.6%
Total Capacity of the Shared PCP Resources	1000 / 6 PCPs = 166.7 = PCP capacity							

Legend:
LCP Logical CP
PCP Physical CP

Notes:

1. Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open a reset or image profile to set the processing weight for an LP. The Processing weight field is located on the Processor page for the LP.
2. The logical CPs for LP C (2) fall outside the enforceable range because each logical CP's share is only 4% of a physical CP.
3. The LP's range is bounded by the line shown for LP C (3). Typically, though, even this configuration will see results comparable to the line shown for LP C (2).

Example 2. Without processor resource capping: In the following example:
- Six physical CPs are online
- No LPs are capped
- All LPs have sufficient workload demand to use their shares

Table 15. PR/SM LPAR processor weight management without processor resource capping and with HiperDispatch Disabled

LP	LCPs Online	Weight (1)	Weight per LCP	LCP % of PCP	3.6% Share	3.6% Total	Resulting Weight Range	Resulting Utilization Range
A	6	500	83.3	50	3.0	–	80.3–86.3	48.2%–51.8%
B	3	300	100.0	60	3.6	–	96.4–103.6	28.9%–31.1%
C (2) C (3)	3	200	66.7	40	2.4	– 12	64.3–69.1 54.7–78.7	19.3%–20.7% 16.4%–23.6%
Total Capacity of the Shared PCP Resources		1000 / 6 PCPs = 166.7 = PCP capacity						

Legend:

LCP Logical CP
PCP Physical CP

Notes:

1. Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open a reset or image profile to set the processing weight for an LP. The Processing weight field is located on the Processor page for the LP.
2. The logical CPs for LP C (2) fall outside the enforceable range because each logical CP's share is only 40% of a physical CP.
3. The LP's range is bounded by the line shown for LP C (3). Typically, though, even this configuration will see results comparable to the line for LP C (2).

Processing weight management formulas: The following formulas were used to compute the values in the previous two examples:

$$\text{Weight per LPC} = \frac{\text{LPCTL Weight}}{\text{Number of LCPs online}}$$

$$\text{LCP percent of PCP} = \frac{\text{LPCTL Weight}}{\text{Total of LPCTL Weights}} \times \frac{\text{Number of PCPs online}}{\text{Number of LCPs online}}$$

$$\text{3.6 percent Share} = \text{Weight per LCP} \times \text{3.6 percent}$$

$$\text{3.6 percent Total} = \frac{\text{Total Weight} \times \text{3.6 percent}}{\text{Number of LCPs online}}$$

$$\text{Resulting Weight Range} = \text{Weight per LCP} \pm \text{3.6 percent Share}$$

or

$$\text{Resulting Weight Range} = \text{Weight per LCP} \pm \text{3.6 percent Total}$$

$$\text{Resulting Utilization Range} = \text{Resulting Weight Range} \times \frac{\text{Number of LCPs online}}{\text{Total Weight}}$$

Maintaining the same relative percentages of CPU resources

To maintain the same relative percentage of CP resources requested for a capped LP, processing weights should be readjusted immediately prior to, or immediately after, the activation or deactivation of an LP.

Processing weight values for use when specific LPs are activated or deactivated should be calculated in advance, and be readily available. Otherwise, it is recommended that a convenient method be developed for changing the processing weight values to readjust relative shares after an LP is activated or deactivated.

For example, if the sum of the weights of the active LPs totals 100, then the sum of the relative weights of the active LPs also totals 100. This provides an easy means for adjusting weights upon the activation or deactivation of LPs. Another good approach to maintaining the desired share for a capped LP is to also readjust the processing weights for LPs with the capping function turned off, as shown in Table 16 for the LP ZOSTEST.

Table 16. Example of maintaining relative weight of a capped logical partition

	Four LPs Active			Three LPs Active		
LP Name	**Status**	**Weight**	**Capped**	**Status**	**Weight**	**Capped**
ZVSE	A	30	No	D	–	–
ZOSPROD	A	40	No	A	64	No
ZOSTEST	A	20	Yes	A	20	Yes

When the sum of all the relative weights is maintained at 100, it is easy to recalculate weights when an LP is deactivated. After deactivating ZVSE, the weight for ZOSPROD can be changed to 64 to maintain the same relative weight of 20 for ZOSTEST, the capped LP.

Capping in a single logical partition: In order to use capping for an LP on a CPC where there is a need for only one active LP using shared CPs, you must define and activate a second “dummy” LP. The dummy LP must also be defined as using shared CPs. The weights of the two LPs can be adjusted to attain the desired cap for the one LP that will actually be used.

The “dummy” LP does not have to be capped. In most cases, the “dummy” LP does not need to have anything IPLed into it. If nothing is IPLed into the “dummy” LP, the “dummy” LP will not use any CP resources. In some situations where the single capped LP runs an extremely CP-intensive workload, it may be necessary to run a program in the “dummy” LP to smooth distribution of CP resources to the LPs. The program can be a simple branch loop that spins to waste time. Without this program running in the “dummy” LP, the CP-intensive, capped LP can experience a lurching effect with its dispatched times. It will be capped to its weight properly, but it could get all of its allotted CP resource quickly and then wait for a period of time before it can run again.

If nothing is to be IPLed into the “dummy” LP, the “dummy” LP can be defined and activated with no channel paths or devices. A definition with no devices is desirable to prevent control unit logical paths from being established for the “dummy” LP. See “Managing logical paths for ESCON and FICON channels” on page 31.

Capping and disabling event-driven dispatching in a single LP configuration: If you want to disable event-driven dispatching and enable capping in a single LP configuration, you must do ***both*** of the following:

- Define a “dummy” LP (a “dummy” LP configured with 1 logical CP is sufficient)
- Make sure that the logical CP in the “dummy” LP is in a fully enabled wait state (the first four bytes of the PSW must be X'030E000')

  If you have configured the “dummy” LP with more than 1 logical CP (this is ***not*** recommended), you will have to put each logical CP in a fully enabled wait state. (Alternatively, each logical CP in the “dummy” LP can be running a branch loop to waste time.)

With event-driven dispatching disabled and the “dummy” LP in a fully enabled wait state, PR/SM LPAR will dispatch the logical CPs on the basis of time intervals according to the specified weights.

This situation does ***not*** apply if either of the following is true:
- Event-driven dispatching is enabled
- Event-driven dispatching is disabled and more than one LP is activated and running an operating system

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open a reset profile to enable or disable event-driven dispatching for an LP. On the Options page, select **Do not end the time slice if a partition enters a wait state** to disable event-driven dispatching for the LP. To enable event-driven dispatching for the LP, do not select this option.

HiperDispatch and Shared Logical Partitions

With the introduction of the z990, the zSeries LPAR hypervisor became aware of machine CP topology and began optimizing the allocation of logical partition CP resources to the physical resources accordingly. This support was enhanced in the z9 family of processors to dynamically re-optimize logical partition resource assignments as configuration changes were made. This support optimized physical CP selection for dispatching logical partition CPs in order to minimize disruption to the various levels of internal caches on the machine. For z10, IBM introduces a new level of synergy between the z10 LPAR hypervisor and z/OS software for managing logical CP resource allocations, called HiperDispatch.

HiperDispatch is the true start of having zSeries OS software become aware of the topology of the machine, presented as a logical partition topology, to then provide dynamic affinity dispatching with regards to CP placement in the z10 book structure.

One can think of the way zSeries LPAR has traditionally managed shared logical partitions as being *horizontally* polarized. That is, the processing weight for the logical partition is equally divided between all the online logical CPs in the logical partition. In turn, the OS running in the logical partition is obligated to use all of those online logical CPs equally in order to be assured of receiving its fair share of the physical CP resources. HiperDispatch introduces a new, optional form of polarization for managing the shared logical CPs of a logical partition called *vertical* polarization. z/OS running with HiperDispatch uses the logical partition topology information to decide how to group its logical CPs to set up its work queues and to exploit the vertical configuration of logical CPs to pack work into a smaller set of logical CPs, optimizing processor cache usage.

With HiperDispatch there is a common understanding in the z10 LPAR hypervisor and the z/OS software such that work can be concentrated on a smaller number of logical CPs within the logical partition that reflects the actual assigned weight of the logical partition. With HiperDispatch enabled in a logical partition, z/OS will redispatch its tasks back to a smaller set of logical CPs, and LPAR in turn can dispatch those logical CPs back to the same physical CPs, optimizing use of both the L1 and L2 caches. Work can still expand and flow into more logical processors dynamically should workload conditions warrant it.

Enabling HiperDispatch

HiperDipatch is enabled within a logical partition via software controls. To enable HiperDispatch under z/OS, specify a new keyword in the IEAOPTxx member of SYS1.PARMLIB. HiperDispatch=YES needs to be specified to turn on this mode of dispatching. The enablement is dynamic and can be changed without an IPL. Refer to the z/OS publications for further details. There are no new hardware controls or settings to enable use of HiperDispatch within a logical partition; however, the existing “control global performance data” security setting must be enabled for proper operation of HiperDispatch in a logical partition.

Allocating Processing Weights within a logical partition using HiperDipatch

Depending on the configuration of the logical partition running with HiperDipatch enabled, logical processors have high, medium or low vertical polarity. Polarity describes the amount of physical processor share vertical logical processors are entitled to. The relative processing weight that is defined for the logical partition effectively defines the amount of physical processor cycles the logical partition is entitled to.

Vertical polarity is measured by the ratio of a logical partition’s current weight to the number of logical processors configured to the logical partition. High polarity processors have close to 100% CP share. Medium polarity processors have >0 to close to 100% shares and low polarity processors have 0% share (or very close to it). Medium polarity processors act as an *anchor* with sufficient weight reserved to allow the medium and low polarity processors to get dispatched in times of contention. The medium and low processors employ a new sharing algorithm to draw on this portion of the partition’s processing weight for medium and low processors. As such, LPAR reserves at least 1/2 a physical CPU’s worth of weight in the medium polarity processor assignments, assuming the logical partition is entitled to at least that much service. High polarity logical CPs will be assigned a physical processor to run on very similar to dedicated CPs but the shared high polarity CP can still give up the physical resource and allow other shared logical CPs to use its excess cycles. The key here then becomes that z/OS software sees the logical topology and tries to exploit the highly polarized logical CPs for its work queues.

For example, consider a CEC that has 3 physical CPs with 2 active logical partitions, each defined with 2 logical processors and each with a processing weight of 50. If the first logical partition enabled HiperDispatch, it would have 1 high polarity and 1 medium polarity logical CP.

```
50/100 x 3 = 1.5 physical CPs
```

Effectively, one logical CP in the Hiperdispatch enabled logical partition is given an allocation of 33 1/3 for its portion of the partition’s processing weight, this is the high polarity logical processor. This processor is also ″assigned″ a physical processor similar to a dedicated logical CP. The other logical CP, the medium polarity CP, is allocated 16 2/3 for its processing weight, effectively entitling it to 50% of one physical CP.

As a second example, suppose the same three-way processor now has 3 active logical partitions, each with 2 logical processors and each with a processing weight of 50. If the first logical partition enabled HiperDipatch, it would have 1 medium polarity and 1 low polarity logical CP. No high polarity logical CPs are assigned because at least 1/2 a physical CP is kept in the medium/low pool.

```
50/150 x 3 = 1 physical CP
```

In this case, one logical CP in the Hiperdispatch enabled logical partition is given the complete allocation of 50 for its portion of the partition's processing weight; this is the medium polarity logical processor. There are no high polarity processors in this example. The other logical CP, the low polarity CP, is allocated 0 for its processing weight. Note the allocations for the medium and lows are really for bookkeeping. z/OS knows it has some capacity available for use by this set of logical CPs but it should only be expanding into these beyond the count of medium CPs when there is excess capacity available in the system because some other logical partition is not demanding its allocation. When the mediums and lows demand CP resource, they will effectively share the processing weight that was allocated to the medium logical CPs.

Notice that the logical partition's processing weight has a direct effect on the number of high polarity processors the logical partition will have when running with HiperDispatch. You should take care to set your processing weights to get your workload optimally allocated to the desired set of high polarity processors.

Note that when a logical partition chooses to run with HiperDispatch enabled, the entire logical partition runs enabled. This includes all of its secondary processors such as zAAPs and/or zIIPs. It is the responsibility of the user to define processing weights to all of the processor types for these logical partitions that will achieve the desired level of vertical processor allocations for each type.

It is also worth noting that while HiperDispatch was created primarily for logical partitions using shared logical CPs, HiperDispatch can be enabled in a logical partition using dedicated CPs. In this case, no change is seen in the way the z10 LPAR hypervisor will treat the dedicated logical partition, but z/OS will have knowledge of the logical topology it has been assigned and it will localize the redispatch of its tasks to get optimal use of the L1 and L2 caches.

Processor running time

The processor running time is the length of continuous time (determined by the dispatch interval) allowed for the dispatch of a logical CP.

When the processor running time is dynamically determined by the system, the calculation of the default running time is performed separately for general purpose and ICF CPs. All logical processors that are shared, either general purpose or ICF, will be assigned a default running time but the values used for each type of processor may be different. If a user-defined run time is specified, the value applies to all shared general purpose and shared ICF CPs.

The default value is dynamically calculated and changes when the number of active, scheduled logical CPs changes.

The default running time is determined using the formula:

25 milliseconds x (number of physical shared CPs)
(total number of logical CPs not in stopped state for all sharing LPs)

The default value is used whenever the processor running time is dynamically determined by the system. The run-time value can change whenever an LP is activated or deactivated and when a logical CP stops or starts (for instance, when a logical CP is configured online or offline). The default processor running time is limited to the range of 12.5 to 25 milliseconds.

The logical CP might not use all of its run time because it goes into a wait state. With event-driven dispatching, when a logical CP goes into a wait state, the physical CP is reassigned to another logical CP ready to do work. When a logical CP does not go into a wait state during its run time, it loses the physical CP when it reaches the end of its run time. Therefore, an LP with CP-bound work cannot permanently take control of the physical CPs.

You can choose to set the runtime value yourself. However, when event-driven dispatching is enabled, it is generally recommended that the processor running time be dynamically determined. If event-driven dispatching is disabled, you should consider setting runtime values of 2 to 8 milliseconds. The recommended procedure is to start by using the default processor running time. That value should be acceptable when all sharing LPs have similar proportions of interactive work; for example, two LPs each running 40%–70% of interactive work.

Adjustments to the runtime value might be necessary when one sharing LP contains a large proportion of CP-bound work and the other sharing LPs contain only short, interactive transactions. Degraded response time in one LP can indicate that the runtime value should be reduced to decrease the length of continuous time given to CP-bound work. The run-time value should be decreased by approximately 10% several times over several days while monitoring performance carefully. The processing weights should also be adjusted to favor the interactive LP. See “Processing weights” on page 124.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open a reset profile to define processor running time. Select either **Dynamically determined by the system** or **Determined by the user** on the Options page for the LP. See Figure 33 on page 148.

Wait completion

Shared CP resources can be divided on either an event-driven basis or a time-driven basis. The RMF Partition Data Report refers to these two forms of dispatching as Wait Completion=No (event-driven dispatching) and Wait Completion=Yes (time-driven dispatching). When the resource is divided on an event-driven basis, switching between users is done as the result of some event, such as a wait or an interruption. When the resource is divided on a time-driven basis, switching is done after a predetermined interval of time. The resource is given to a user for a fixed interval and then given to another user for a subsequent fixed interval. Either of these methods can divide CP resources between sharing LPs.

You can select either of these methods by using the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open the reset profile for the CPC. On the Options page, you can select **Do not end the time slice if a partition enters a wait state** to turn off event-driven dispatching and cause shared CP resources to be distributed on the basis of time intervals and according to the weights specified. Not selecting it (the default) requests event-driven dispatching. Event-driven dispatching also has an element of time-driven dispatching because the processor running time limits the time a logical CP can be continuously dispatched. This setting does not affect LPs that use dedicated CPs.

Event-driven dispatching has two advantages that are of special interest. The first advantage is a flexibility that allows the system to better meet the peak transaction rates of an LP. The event-driven dispatcher has the flexibility to manage CP resources to compensate for fluctuations in demand among the LPs instead of distributing CP resources in a rigid, predetermined manner.

The second advantage is improved responsiveness over time-driven scheduling through I/O interruption and wait detection. With event-driven dispatching, the time that one logical CP spends in a wait state can be made available to other logical CPs.

When event-driven dispatching is disabled, all logical CPs are given an entire dispatch interval even if they have no work to perform and even if they spend that time in a wait state because LPs are considered to be busy for 100% of their running time. Therefore, processing weights are always in effect.

Generally, response time is much better when event-driven dispatching is enabled and ITR is slightly better when event-driven dispatching is disabled. However, event-driven dispatching is recommended because improved responsiveness and the ability to use wait time more than compensates for a small decrease in ITR.

The wait completion setting applies to both shared general purpose and shared ICF processors.

Workload manager LPAR CPU management of shared CPs

WLM's LPAR CPU Management component, together with the LPAR clustering technology of the System z10 servers, provides the ability to dynamically manage workloads within an LPAR cluster comprised of multiple logical z/OS images on a single System z10 server. Each LP is assigned a ***transaction*** goal (desired response time) and an ***importance*** level. WLM monitors how well each LP is achieving its goals. A donor/receiver approach is utilized to reapportion CPU resources between LPs in the cluster. When WLM LPAR Weight CPU Management decides to change the weight of an LP, it adjusts the receiver LP and the donor LP by a percentage of the current weight of the receiver. WLM takes resources away from an LP that is over-achieving its target or has a workload that is less important (as defined by the installation). Any resource given to a particular LP is taken away from another LP in the LPAR cluster. LPs whose workloads are of the same importance level should all have similar performance indexes (a measure of how closely the workload is meeting its defined goal).

One can think of the entire LPAR cluster as having a total processing weight. The total weight for an LPAR cluster is the sum of all the initial processing weights of all the LPs that have joined the cluster. As a new logical partition joins the cluster, its initial processing weight is added to that of the cluster. Though weights are adjusted from one LP to another, the total weight for the cluster is consistent. When an LP leaves the LPAR cluster, as when it is either system reset, deactivated, or re-IPL'd, its initial processing weight, which it had been contributing to the LPAR cluster, is removed from the total weight available to the cluster. The weight removed from the cluster is not necessarily equal to the current weight for the exiting LP.

The optional minimum and maximum processing weights for an LP govern how much flexibility WLM has in adjusting weights from one LP in the cluster to another. The installation should assign a reasonably wide range of processing weights to each WLM managed LP. Assigning the same value for initial, minimum, and maximum weights effectively disables WLM LPAR CPU Management of processor weights.

Though logical CPs of WLM managed LPs may need to be soft-capped (as for workload pricing, see "Workload charging by soft-capping to a defined capacity"), initial capping (traditional hardware capping) of these LPs is disallowed. Similarly, if an LP is WLM managed, its logical CPs must be shared, not dedicated. For more information regarding internals of WLM CPU Management, see redbook *z/OS Intelligent Resource Director*, SG24-5952.

Workload charging by soft-capping to a defined capacity

Workload charging introduces the capability to pay software license fees based on the size of the LP the product is running in, rather than on the total capacity of the CPC. The capability is enabled by the LPAR clustering technology of the System z10 servers together with the License Manager component of z/OS. Each LP is assigned a ***defined capacity*** by the installation in terms of Millions of Service Units (MSUs).

WLM helps ensure that the rolling 4-hour average CPU utilization for the LP does not exceed this amount by tracking the CPU utilization for the logical partition. If the 4-hour average CPU consumption of the LP exceeds the defined capacity of the LP, WLM dynamically activates LPAR capping (soft-capping). When the rolling 4-hour average dips below the defined capacity, the soft-cap is removed.

WLM *will not* dynamically adjust the defined capacity for an LP. This is the responsibility of the installation. If an LP consistently exceeds its defined capacity, the license certificates and the defined capacity of the LP should be adjusted to reduce the amount of time the LP is soft-capped. If you have a configuration where the LP weights move significantly from one LP to another according to shift, then you must license the products in each LP at the highest capacity that will be used by that LP.

Recommendations on setting up an LPAR cluster

- An LPAR cluster is a collection of two or more logical partitions, on a particular CPC, that are part of the same parallel sysplex. LPAR clusters do not span CPCs as do parallel sysplexes. Though the member LPs of an LPAR cluster will all be in the same parallel sysplex, all members of a parallel sysplex might not be members of the same LPAR cluster. A given parallel sysplex can have member LPs that belong to multiple LPAR clusters, each on a different CPC.
- Identify logical partitions on the CPC that will be in the cluster (members of the same parallel sysplex). A single CPC can have several LPAR clusters just as a single CPC can have many LPs, each having membership in a different parallel sysplex.
- IBM recommends allocation of shared CPs and enablement of WLM management for cluster members (see Note 1). The number of initially online CPs should be maximized to provide optimum flexibility to WLM. The number of reserved CPs defined should be the maximum allowed for an LP in your configuration minus the number of initially online CPs. See "Number of central processors" on page 116 for additional information on central processors.
- Establish an initial weight for each LP in the cluster. This will be the weight for the LP immediately after it is activated (see Note 2). Triple digit values should be used, wherever possible, for initial weights because WLM reapportions weights on a percentage basis. The total weight of the cluster will equal the sum of all the initial weights of its member LPs. Leave the minimum and maximum weights blank or make the range as wide as possible (optimally 1 to 999) to provide WLM maximum flexibility as it distributes CPU resource among the cluster members.
- Enable each LP in the cluster for WLM management.

- To enable DCM of managed channel paths for a logical partition, the name specified on the IOCLUSTER keyword for managed channel paths in the IOCDS must match the sysplex name of the software running in the logical partition. See "Dynamically managed CHPIDs" on page 51 for more information on the IOCLUSTER keyword.
- Calculation to estimate the number of cache structures that can be supported:

  The number of cache buffer data items that can be maintained locally in a Logical Partition is directly proportional to the number of online central storage pages in the LP. Each cache buffer or data item needs a local cache vector space bit. A heuristic value of 4 bits per online central storage 4K page is assigned by the system to each exploiting logical partition.

  The number of cache buffers supportable is easily calculated. Multiply the number of online central storage pages, in the z/OS logical partition exploiting the cache vector space, by two to get the number of cache vector bytes provided.

  For instance, if an exploiting logical partition has 32 GB of central storage online the amount of cache vector space provided would be 32 * 1024 (MB per GB) * 256 (pages per MB) * 2 (nybbles per byte) = number of bytes provided. For an LP with 32 GB 16777216 bytes, or 16 MB is provided. The size of the cache vector for an LP whose central storage definition includes the capability of using Dynamic Storage Reconfiguration will grow when the reserved storage amount is configured online.
-

  Notes:

  1. Logical partitions in a sysplex that have dedicated CPs can join a cluster but will not be enabled for WLM LPAR Weight and Vary CPU Management. They can derive I/O management benefits, however, from WLM's Dynamic CHPID Management capability.
  2. Though the current weight of a logical partition can be changed (increased or decreased) by WLM once it joins an LPAR cluster, the initial weight will be restored when (on IPL) it leaves the cluster. Software can then rejoin the same or a different cluster, again donating its initial weight to the sum available for the entire cluster.

Enabling management of Linux shared logical processors by WLM's LPAR CPU management component

1. For the target Linux LP, use the **Options** page (see Figure 41 on page 162) of the Customize Image Profiles panel to specify the CP management cluster name of the intended LPAR cluster. Also select **Enable WorkLoad Manager** on the **Processor** page (see Figure 37 on page 154) of the Customize Image Profiles panel.
2. In the WLM policy statement, define a new service class giving it a velocity goal and an importance. Also, in the SYSH subsystem (create SYSH subsystem if one does not already exist), define a classification rule with the attribute **SY** (system name). Associate the system name of the target Linux logical partition and the service class you just defined.
3. IPL the Linux 2.4 kernel and provide a system name of the Linux logical partition by executing `insmod hwc_cpi.o system_name=xxxxxxx`, where `xxxxxxx` matches the system name communicated to WLM in Step 2.

Note: WLM is only able to manage Linux shared logical processors running on general purpose CPs. Management of Linux shared logical processors running on Integrated Facility for Linux (IFL) processors is not supported. It is important to realize that Linux mode partitions participating in a CP management cluster should be system reset through the Support Element/Hardware Management Console following a Linux shutdown command to help ensure accurate cleanup by WLM's LPAR CPU Management component.

Defining shared channel paths

Before defining shared channel paths, consider the following:

- Only CTC, CNC, CBP, CFP, CIB, ICP, OSC, OSD, OSE, OSN, FC, FCV, FCP, and IQD channel paths can be shared. CVC and CBY channel paths ***cannot*** be shared. On CF only models, CBP, CFP, CIB, and ICP channel paths ***cannot*** be shared.
- A failure in a shared channel path or I/O device can affect more than one LP; therefore, critical I/O devices (for example, DASD containing vital data sets) still need multiple channel paths. You can provide multiple shared channel paths (up to 8) to critical I/O devices.
- Using shared channel paths does not reduce the number of logical paths needed at a control unit. A control unit requires a logical path for each active LP that can access I/O devices through a shared channel path.

There are three possible channel path modes:

shared
A channel path that can be configured online to one or more LPs at the same time. One or more LPs can access I/O devices at the same time using this channel path. Spanned channel paths are shared by LPs in multiple logical channel subsystems (CSSs). Unspanned channel paths can only be shared by LPs in the same CSS.

reconfigurable
An unshared channel path you can reconfigure offline from one LP, then online to another, within the same CSS. Only one LP can access I/O devices on this channel path at a time.

dedicated
An unshared and nonreconfigurable channel path. Only one LP can access I/O devices on this channel path.

You cannot mix unshared and shared CHPIDs to a device.

Channel path access and candidate lists

If a channel path is either shared or reconfigurable, you can specify which LPs have access to that channel path. Use the channel path access list with or without the channel path candidate list.

Channel Path Access List
An LP has ***initial*** access to a channel path if the LP is on that channel path's access list.

For the first power-on reset with an LPAR IOCDS, the access list defines which LPs will initially have the channel path configured online. Reconfigurable and shared CHPIDs may later be accessed by LPs not in the access list. Subsequent power-on resets with the same LPAR IOCDS will have any reconfigurations applied and the LPs may have access to channel paths other than those that were specified in the initial access lists for the channel paths. See "Channel path reconfiguration and logical partition activation" on page 144 for more information on assigning channel paths to an LP.

Channel Path Candidate List

An LP can ***gain*** access to a channel path if the LP is on that channel path's candidate list. An LP is allowed to configure a channel path online if the LP is in that channel path's candidate list.

I/O device candidate list

The I/O device candidate list specifies the LPs which can access the device. You can use the I/O device candidate list to restrict LP access to I/O devices on shared channel paths. If you do not specify an I/O device candidate list, all LPs that share the channel paths, to which the device is attached, can have access to the device. For coupling facility devices, the device candidate list is not supported.

Procedure for defining shared channel paths

To share channel paths, use the following general procedure:

1. Select which I/O devices to access through shared channel paths
2. Select the LPs that will share channel paths
   - Specify the desired channel paths as shared
   - Use the access list and candidate list of the desired shared channel path to select which LPs can access that shared channel path.
3. For each I/O device that will be on a shared channel path, you can use the I/O device's candidate list to restrict which LPs can access that I/O device.
4. Make physical connections to the shared channel paths and the I/O devices.
5. Update the software I/O configuration for the control programs running in LPs that can access devices through shared channels.
6. Use IOCP or HCD to create an IOCDS that defines the I/O configuration, including shared channel paths, to the CPC channel subsystem. The channel subsystem includes all channel paths, control units, and I/O devices accessible by all LPs.

Communicating by means of ESCON or FICON CTC

You can connect shared or unshared CNC or FCV channel paths to shared or unshared CTC channel paths for the purpose of CTC communication. The connected CNC or FCV and CTC channel paths can be on the same CPC (to communicate between the LPs on that CPC) or on different CPCs.

You can connect shared or unshared FC channel paths to shared or unshared FC channel paths for the purpose of CTC communication. The connected FC channel paths can be on the same CPC (to communicate between the LPs on that CPC) or on different CPCs.

CTC communications involving a shared channel path require the specification of control unit logical addresses. The control unit logical address identifies the MIF image ID number for the LP to which the channel path is to communicate. If the remote channel path is not shared, the logical address must be zero or not specified. If the remote channel path is shared, the logical address must equal the desired MIF image ID number for the LP that the shared channel path can access. If the remote channel path is a shared FC channel path and the target LP has a CSS ID other than zero, then the logical address must equal the combination of the desired CSS ID and the MIF image ID for the LP with which you want to communicate. For example, if the remote channel path is shared within CSS 1 and you want to communicate with the LP that has MIF image ID 5, specify logical address 15. You must define a control unit and a control unit logical address for every LP that you want to communicate with.

For additional information, see *System z ESCON or FICON Channel-to-Channel Reference*, SB10-7034.

Dynamic CHPID management (DCM) considerations

DCM CHPIDs used by WorkLoad Manager (WLM) to optimize I/O throughput across an LPAR cluster are identified in the IOCDS by specifying CHPARM equals 01 and IOCLUSTER equals name (where name is an 8-byte EBCDIC cluster identifier).

All DCM CHPIDs are inherently shareable by all LPs but reserved for use by the WLM enabled members of the specified cluster. At completion of an LP activation, its DCM CHPIDs will be in a deconfigured state. When an LP joins a cluster, the DCM CHPIDs in that cluster become available for use by WLM but are not brought online until the need for greater throughput arises. System reset of an LP that was a member of a cluster causes each of the DCM CHPIDs that were online to the LP to be deconfigured. For information on how to define DCM CHPIDs, see "IOCP statements for ICP" on page 52. For allocation rationale of DCM CHPIDs, see redbook *z/OS Intelligent Resource Director*, SG24-5952.

I/O priority recommendations

Channel subsystem I/O priority queuing is used by z/OS WLM component to dynamically manage the priority of I/O operations for given workloads based on the performance goals for these workloads as specified in the WLM policy.

Channel subsystem I/O priority queueing is used by z/VM to manage the priority of I/O operations performed by guests. The VM Resource Manager adjusts guest I/O priorities based on the performance goals of the associated workloads. It is recommended that you establish a range of I/O priorities for z/VM logical partitions that is sufficient to enable effective discrimination among guest I/O requests of different importance.

In order to provide WLM the greatest flexibility in managing I/O requests across members of an LPAR cluster, it is highly recommended that you establish the same range of priorities for each member of an LPAR cluster. A range of eight priorities (from minimum to maximum) is optimum. If a range greater than eight is specified, only the top eight will be utilized by WLM.

Non-WLM managed LPs should be assigned I/O priorities according to their importance relative to the LPs that are members of LPAR clusters. Unless it is running z/VM (in which case the recommendations above should be followed), a non-WLM managed LP should be assigned equal values for minimum and maximum I/O priorities. For more information and examples of how I/O priorities are used by WLM to prioritize I/O requests across diverse workloads, see redbook *z/OS Intelligent Resource Director*, SG24-5952.

Security-related controls

You can define security-related controls for an LP.

Global performance data control authority

This control limits the ability of a LP to view CP activity data for other LPs. LPs with control authority for global performance data can view CP utilization data and Input/Output Processor (IOP) busy data for all of the LPs in the configuration. Additionally, gathering of FICON channel measurements requires selection of this parameter.

Note: Logical partitions that use HiperDispatch require global performance data authorization in order to properly utilize excess CPU resources in the configuration.

With the exception of an LP that is a member of a WLM Cluster, an LP without control authority for the performance data can view only the CP utilization data for that LP.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open a reset or image profile to enable global performance data control for an LP. The Global performance data control selection is located on the Security page for the LP.

Note: An LP running a level of RMF that supports FICON requires control authority even if no FICON is installed.

I/O configuration control authority

This control can limit the ability of the LP to read or write any IOCDS in the configuration locally or remotely. LPs with control authority for the I/O configuration data can read and write any IOCDS in the configuration, and can change the I/O configuration dynamically.

Additionally, this control allows the OSA Support Facility to control OSA configuration for other LPs.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open a reset or image profile to enable I/O configuration control for an LP. The Input/output (I/O) configuration control selection is located on the Security page for the LP.

Cross-partition authority

This control can limit the capability of the LP to issue certain control program instructions that affect other LPs. LPs with cross-partition authority can issue instructions to perform a system reset of another LP, deactivate any other LP, and provide support for the automatic reconfiguration facility.

The automatic reconfiguration facility permits a backup LP to deactivate a primary LP if a problem is detected in the primary LP. The backup LP can then configure online, storage resources that become available when the primary LP is deactivated. See “CPCs with the Sysplex Failure Manager (SFM)” on page 114.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open a reset or image profile to enable cross-partition authority for an LP. The Cross partition authority selection is located on the Security page for the LP.

Logical partition isolation

This control reserves reconfigurable unshared channel paths for the exclusive use of an LP. Channel paths assigned to an isolated LP are not available to other LPs and remain reserved for that LP when they are configured offline.

Use the Release task available from the CHPID Operations task list to release an unshared channel path from an isolated LP.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open a reset or image profile to enable isolation for an LP. The Logical partition isolation selection is located on the Security page for the LP.

Using IOCP, you can control access to channel paths using the channel path candidate list. Access to I/O devices on shared channel path can be further controlled through the I/O device candidate list.

Basic counter set

The basic counter set includes counts of central processing unit cycles, instructions executed, and directory-write and penalty cycles for level-1 instruction and data caches. For more information about the basic counter set, see the *The Set-Program-Parameter and CPU-Measurement Facilities*, SA23-2260.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to authorize the use of the basic counter set for an LP. The Basic counter set authorization control selection is located on the Security page for the LP.

Problem state counter set

The problem state counter set includes counts of central processing unit cycles, instructions executed, and directory-write and penalty cycles for level-1 instruction and data caches only when the processor is in problem state. For more information about the problem state counter set, see the *The Set-Program-Parameter and CPU-Measurement Facilities*, SA23-2260.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to authorize the use of the problem state counter set for an LP. The Problem state counter set authorization control selection is located on the Security page for the LP.

Crypto activity counter set

The crypto activity counter set can be used to identify the crypto activities contributed by the logical CPU and the blocking effects on the logical CPU. It included counters related to PRNG, SHA, DEA, and AES function. For more information about the crypto activity counter set, see the *The Set-Program-Parameter and CPU-Measurement Facilities*, SA23-2260.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to authorize the use of the crypto activity counter set for an LP. The Crypto activity counter set authorization control selection is located on the Security page for the LP.

Extended counter set

The extended counters provide information about hardware facilities and structures that are specific to a machine family. The extended counters are designed to expand upon information provided by the basic counter set. For more information about the extended counter set, see the *The Set-Program-Parameter and CPU-Measurement Facilities*, SA23-2260.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to authorize the use of the extended counter set for an LP. The Extended counter set authorization control selection is located on the Security page for the LP.

Coprocessor group counter sets

The coprocessor group counter sets include counters for all central processing units attached to the coprocessor related to PRNG, SHA, DEA, and AES function counts. For more information about the coprocessor group counter set, see the *The Set-Program-Parameter and CPU-Measurement Facilities*, SA23-2260.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to authorize the use of the coprocessor group counter sets for an LP. The Coprocessor group counter sets authorization control selection is located on the Security page for the LP.

Basic sampling

With basic sampling, samples are taken and stored at the end of each sampling interval.

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to authorize the use of basic sampling for an LP. The Basic sampling authorization control selection is located on the Security page for the LP.

Dynamic I/O configuration

Dynamic I/O configuration, available with z/OS and z/VM, provides the capability of changing the currently active I/O configuration. With dynamic I/O configuration, channel paths, control units, and devices of the currently active I/O configuration can be added, deleted, or modified without requiring a power-on reset and an IPL for the change to take effect. Changes made to the currently active I/O configuration can be saved and the IOCDS that reflects these changes can be written and made the active IOCDS.

Dynamic I/O configuration does ***not*** support the following:

- Changing MIF image ID numbers

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization Tasks list to open a reset profile to enable dynamic I/O configuration for the CPC. On the General page, select a dynamic IOCDS from the IOCDS list, then select the Dynamic page for the IOCDS and select the Allow dynamic changes to the channel subsystem input/output (I/O) definition check box.

Managing dynamic I/O configuration

For detailed information about changing the I/O configuration dynamically, refer to *z/OS Hardware Configuration Definition Planning*, GA22-7525, *CP Planning and Administration*, SC24-6083, and *z/VM I/O Configuration*, SC24-6100.

Planning and operation considerations

Guidelines for planning and operating in a dynamic I/O environment are detailed in the appropriate z/OS, and z/VM publications. The planning and operation considerations described in this section are additional guidelines that apply to a dynamic I/O environment.

Careful planning will avoid confusion when moving CHPIDs, and eliminate duplicate device situations should a backout be required when a power-on reset is performed.

- Prepare for a backout situation

  Before changing the currently active I/O configuration, prepare for a possible backout situation. Record the current CHPID assignments and the planned I/O changes.

It is important to prepare for a backout situation. A backout situation occurs when changes are made to the I/O configuration but the changes are not saved prior to performing a power-on reset. If the changes are not saved, the CHPID assignments prior to the first dynamic I/O change will take effect.

In addition CHPID assignments after a backout will also reflect any changes made by hardware operator tasks or control program commands.

- Avoid CHPID reconfigurations concurrent with dynamic I/O changes

  Do not perform hardware operator tasks and system control program commands to cause a CHPID to be moved from one LP to another or to give or take access to a shared channel path while dynamic I/O changes are being made. Use these commands only after dynamic I/O changes are saved.

Assigning channel paths to a logical partition

Channel paths are defined in the IOCDS. Channel paths that are specified as reconfigurable can be moved among LPs.

Channel paths that are specified as shared can be accessed by one or more LPs at the same time. Unshared channel paths that are defined to a LP as not reconfigurable are dedicated to that LP.

ESA/390 logical partitions

Channel paths assigned in the IOCDS to ESA/390 LPs can be shared, reconfigurable, or dedicated.

Coupling facility logical partitions

Channel paths (CFP, CBP, CIB, and ICP) assigned in the IOCDS to coupling facility LPs can be online to only one coupling facility at a time. On System z10 models a coupling facility can be assigned CBP, CFP, CIB, or ICP channel paths.

Note: CBP, CFP, CIB, and ICP channel paths that are online to a single coupling facility are shareable by multiple noncoupling facility logical partitions.

Channel path reconfiguration and logical partition activation

When a Configure on task or an equivalent system control program command is run successfully for a channel path in an ***active*** LP, the channel path is configured to the LP at that time.

When a successful Configure on task completes for a channel path in an LP that is ***not active***, the channel path is not actually configured online to the LP at that time. Rather, the channel path is ***targeted*** to be configured online to that LP when the LP is activated.

When an LP is deactivated, all shared channel paths configured to it at the time of deactivation are targeted to be configured online to it when it is subsequently activated. Unshared channels that were last configured to this LP and were not yet reconfigured to another LP are also targeted to be configured online to this LP at its next activation. However, the targeting of a channel path may change prior to the next activation due to channel reconfiguration commands, dynamic I/O configuration changes, or POR.

Channel paths can also be targeted to be configured online to an LP by using dynamic I/O configuration. See “Dynamic I/O configuration effects on channel path reconfiguration” on page 145 for more details.

LPAR manages lists of targeted channel paths for each LP on an IOCDS basis so that all channel paths that are targeted to be configured online to an LP will be automatically configured online when that LP is activated. Exceptions to this rule are:

- Targeted CBP, CFP, CIB, and ICP channel paths online to another coupling facility are not automatically configured online when that LP is activated.

  Note: CBP, CFP, CIB, and ICP channel paths can only be online to one active coupling facility LP at a time. If such a channel path is targeted to a coupling facility LP but is already online to another coupling facility LP, then it will be removed (deconfigured) from the activating LP.
- The targeted channel path is in single channel service mode or otherwise broken.

Dynamic I/O configuration effects on channel path reconfiguration

If a channel path is dynamically added to the configuration using dynamic I/O configuration, all the LPs in the channel path access list (for a shared channel path) or the one LP in the channel path access list (for an unshared channel path) are targeted to have this new channel path configured online. The dynamic I/O configuration change does not bring the channel path online.

The channel path will be configured online to the targeted LP when one of the following occurs:

- The system control program running in the targeted LP issues the appropriate reconfiguration command to configure the channel path online. For z/OS, this would be:

  CF CHP(*nn*),ONLINE

  For z/VM, this would be:

  VARY ON CHPID nn
- The Configure on task is used to configure the channel path online to the targeted LP while the LP is active.
- A power-on-reset is done with the IOCDS that has the new dynamic changes defined in it without the changes being made active using HCD z/OS, or z/VM commands. Subsequent to the POR, activation of the targeted LP will configure the channel path online.

Automatic channel path reconfiguration

LPAR records shared channel path configurations and unshared channel path reconfigurations and uses the information to modify the initial targeting of channel paths that are defined in the IOCDS. This information is maintained on an IOCDS basis.

When a particular IOCDS is used in a POR for the first time after it has been written, the definitions in that IOCDS are used to determine the assignment of channel paths to LPs according to the channel path access lists that are defined. All previous information about channel configuration associated with this IOCDS is discarded. The exception to this rule is when a newly written IOCDS is first used as part of a dynamic I/O change to the system. (For example, the new IOCDS is used as a result of a “Switch IOCDS for Next POR” action by HCD, or the new IOCDS is the target of the ACTIOCDS= parameter of the z/OS ACTIVATE command.) When a new IOCDS is used in this manner, the current state of channel configurations is preserved and immediately associated with the newly written IOCDS.

Over time, the list of channel paths targeted to be configured online to a given LP can be changed by system control program configuration commands, configure on tasks, or dynamic I/O configuration commands issued through HCD or z/VM. Similarly, reconfigurable unshared channel paths can be moved from one LP to another using the same commands; changing the owner of the unshared channel path. For activated coupling facility LPs, you can change the channel paths targeted to be configured online using coupling facility control code commands. Automatic channel path reconfiguration restores all of the latest changes for each POR with the IOCDS automatically.

Automatic channel path reconfiguration does ***not*** preserve the online/offline state of unshared channel paths (reconfigurable or dedicated). Rather, at POR time, all unshared channel paths are targeted to come online to the LP that last owned it. For dedicated channel paths, this owner never changes but for reconfigurable channel paths the owner can change and is remembered.

Following a POR, a channel path that is targeted to come online to a LP will be physically online to that LP and usable at the completion of activation for the LP.

Automatic load for a logical partition

If you want the control program to be loaded automatically each time the LP is activated, select the Load during activation checkbox. Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open a image profile. The Load during activation selection is located on the Load page for the LP. See Figure 43 on page 166.

Coupling Facility Logical Partitions
Do not support automatic load because the coupling facility control code is automatically loaded and made operational at LP activation. No IPL of an operating system is necessary.

z/OS LPs
Specify parameter (PARM) information if desired. Byte 2 and byte 3 of the PARM field are used to select an IOCONFIG member for this IPL if you do not want the default (00).

Defining logical partitions

Before using this section you should first read “Determining the characteristics” on page 99. This section describes the panels, parameters, and tasks, you can use to define LP definitions.

Sample tasks and panels explained in this section reference tasks and panels available from the Support Element console of a System z10. However, detailed procedures for operator tasks and accurate task and panel references are left to the appropriate operator guides. See the *System z Hardware Management Console Operations Guide* and *System z10 Support Element Operations Guide*.

LP definitions are saved across a power-on reset and are used during each power-on reset. You can use reset, image, and load profiles to modify LP definitions. Use image and load profiles to modify LP definitions after the CPC has been activated. Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open a reset, image, and load profiles.

You can change reset, image, and load profiles at any time. However, some of these definition parameters cannot affect the running system if the affected LP is currently activated. See “Changing logical partition definitions” on page 177.

LP definition parameters fall into the following categories:

Global reset profile definitions
- Enable global input/output I/O priority queuing
- Automatic I/O interface reset
- Processor running time
- LP automatic activation order

General
- Logical partition identifier
- LP mode of operation
- Enable logical partition time offset

Processor characteristics
- Dedicated or shared general purpose CPs
- Internal dedicated or shared coupling facility (ICF) CPs
- Initial, minimum, and maximum weight
- Weight capping
- Number of general purpose, and zAAP, IFL, zIIP, or ICF CPs

Security characteristics
- Global performance data control
- Input/output configuration control
- Cross partition authority
- Logical partition isolation

Storage
- Central storage
- Expanded storage

Time Offset
- Time offset

Load information
- Load during activation
- Load address
- Use of dynamically changed address
- Load parameter
- Use of dynamically changed parameter
- Time-out value

Cryptographic characteristics
- Candidate list
- Online list
- Control domain index
- Usage domain index

Note: Coupling Facility partitions cannot take on these characteristics.

Options
- Minimum and maximum input/output (I/O) priority queuing values
- Defined capacity

Global reset profile definitions

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open a reset profile.

Options page definitions

Open the Options page to define the following LP characteristics:

- Enable global input/output (I/O) priority queuing
- Automatic I/O interface reset
- Processor running time

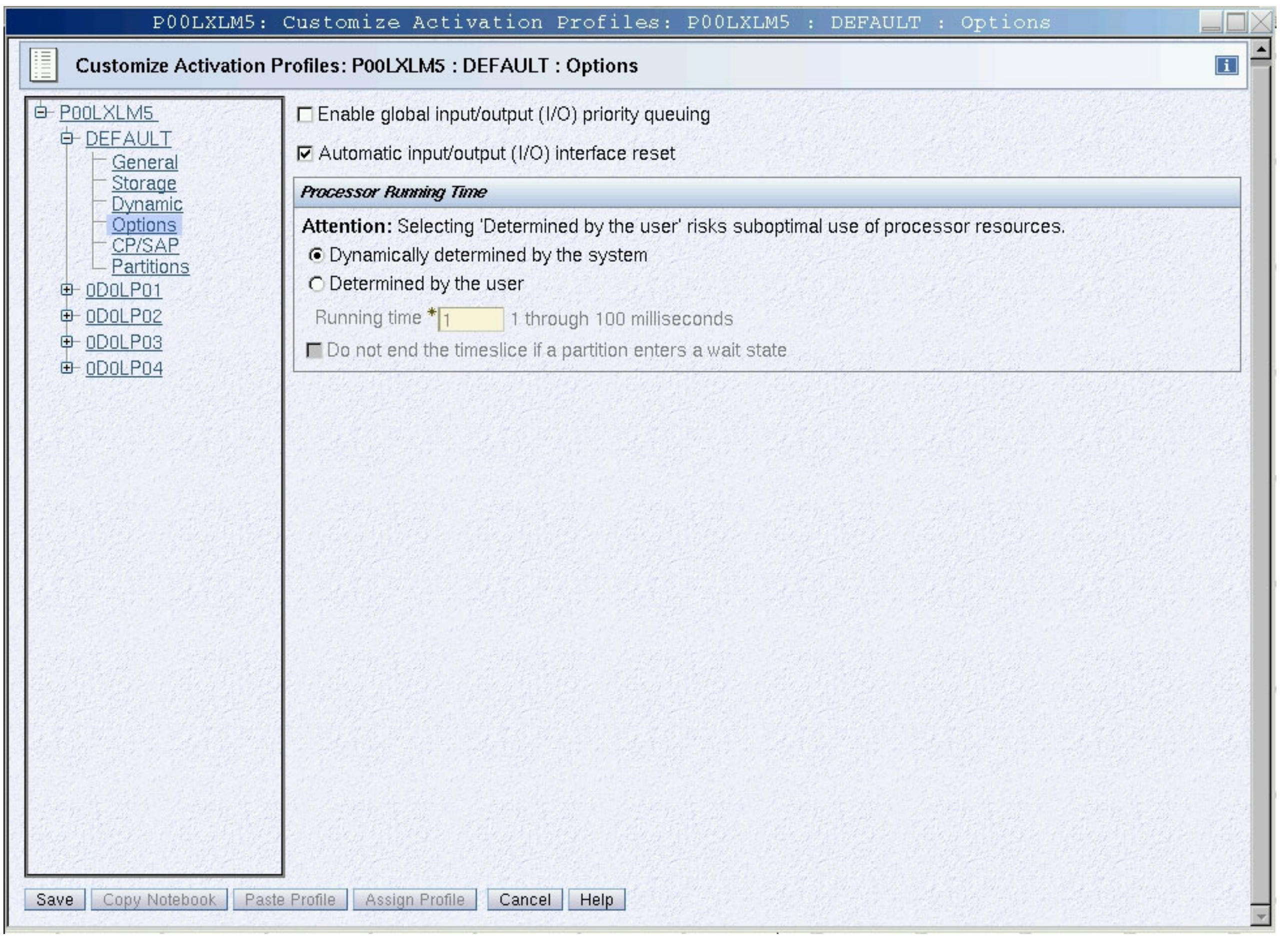


Figure 33. Options page, reset profile

Parameter descriptions

Enable global input/output (I/O) priority queuing
Select this option to enable I/O priority queuing. Selecting this option causes I/O requests to be prioritized according to the values specified on the Options page of the Image Profile.

Automatic input/output (I/O) interface reset
Enables automatic system reset of a logical partition on behalf of a software initiated recovery action.

Dynamically determined by the system
Select this option to allow the system to dynamically calculate the length of CP time dispatched. The default is selected for this checkbox.

Determined by the user
Select this option to manually set the length of CP time dispatched.

Processor running time
Selecting the **Determined by the user option** requires that you enter a running time amount from 1–100 milliseconds.

Do not end the timeslice if a partition enters a wait state
When the processor running time is determined by the user through this profile, check this box to indicate whether logical processors lose their share of running time when their logical partition enters a wait state.

Partitions page definitions

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open a reset profile. Open the Partitions page to define the following LP characteristics:

- LP automatic activation order

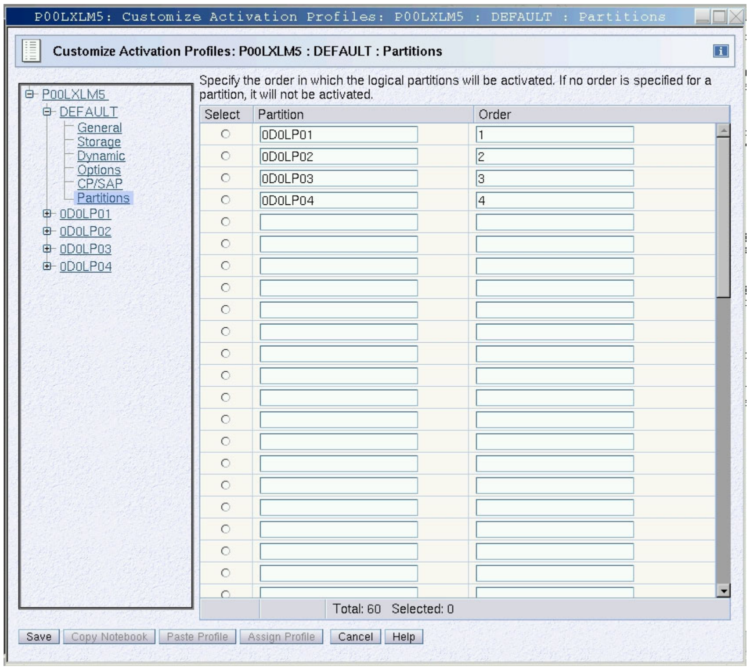


Figure 34. Partitions page, reset profile

Parameter descriptions

Partition
LP name.

Order
Enter a number indicating when the LP will be activated in the automatic activation order.

General

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open an image profile for an LP. Open the General page to define the following LP characteristics:

- Logical partition identifier
- LP mode of operation
- Clock type assignment

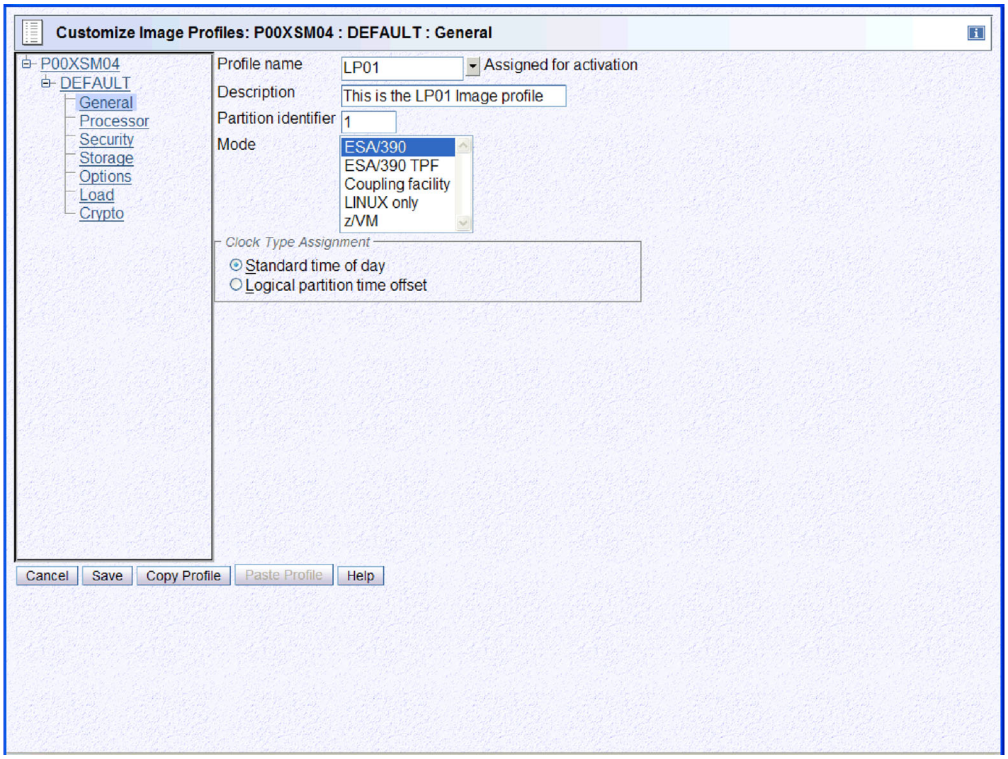


Figure 35. General page, image profile

Parameter descriptions

Partition identifier
Enter a hex value (X'00' through X'3F') for the LP. This parameter identifies the LP and is used as the third and fourth hexadecimal digit of the operand stored by the Store CPU ID Instruction for each logical CP in the LP. The partition identifier must be unique for each active LP.

Mode
Select an LP operating modes from this scrollable list - ESA/390, ESA/390 TPF, Linux-Only, or coupling facility mode.

Logical partition time offset
Select this choice to set the logical partition's clock using an offset from the time of day supplied by its time source. Then use the Time Offset window to set the offset.

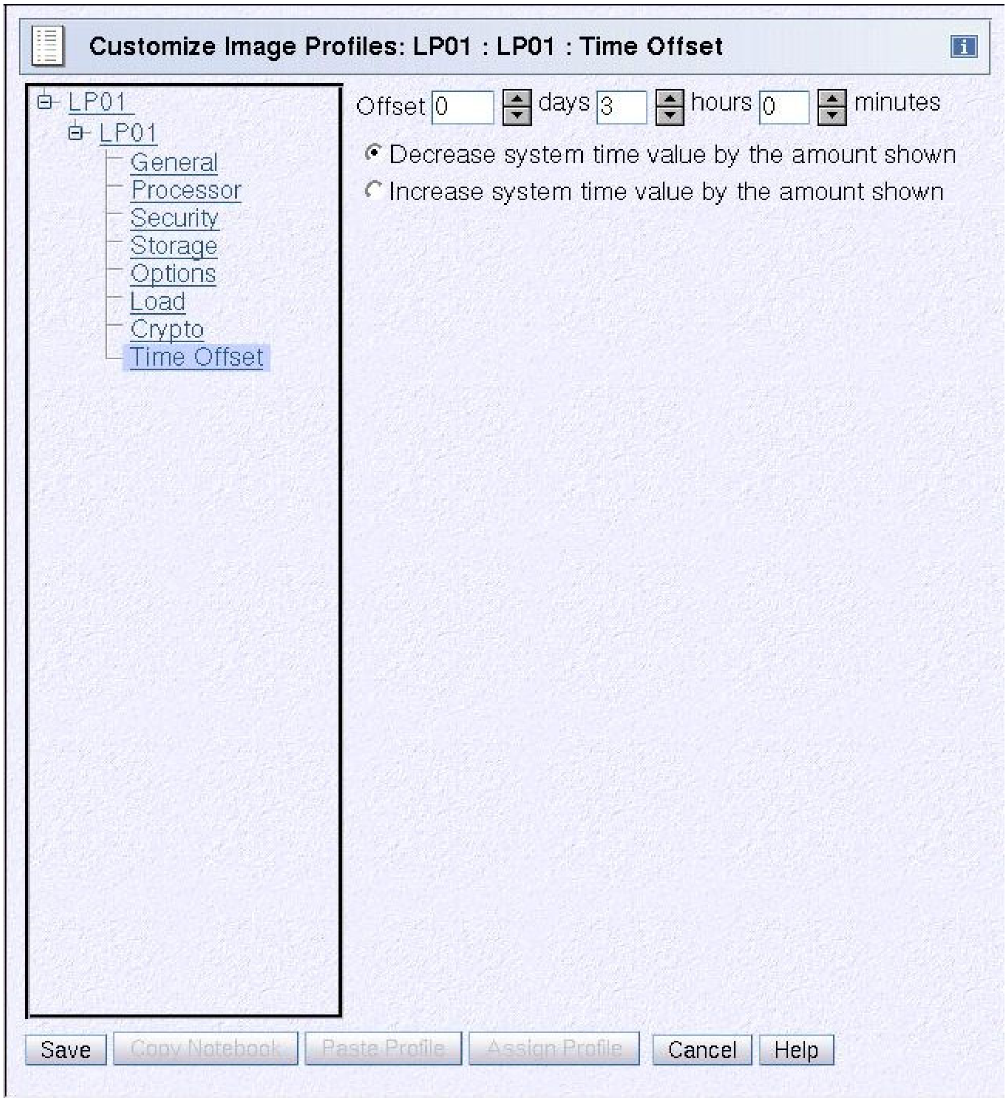


Figure 36. Time offset, image profile

Parameter descriptions

Offset Type or spin to the number of days, hours, and minutes you want to set as the offset from the time of day supplied by its time source. You can set an offset within the following range:

- 0 to 999 days
- 0 to 23 hours
- 0, 15, 30, or 45 minutes

Decrease system time value by the amount shown
Select this choice to set the logical partition's clock back from the time of day supplied by its time source by the number of days, hours, and minutes in the offset. Use this setting to provide a local time zone WEST of GMT.

Increase system time value by the amount shown
Select this choice to set the logical partition's clock ahead of the

time of day supplied by its time source by the number of days, hours, and minutes in the offset. Use this setting to provide a local time zone EAST of GMT or a date and time in the future.

Processor Characteristics

Table 17 shows all logical partitions, required characterized PUs, and operating systems, and which PU characterizations can be configured to a logical partition image. The available combinations of dedicated (DED) and shared (SHR) processors are also shown. For all combinations, a logical partition can also have reserved processors defined, allowing nondisruptive logical partition upgrades.

Table 17. LPAR mode and PU usage

Logical partition mode	PU type	Operating systems	PUs usage
ESA/390	CPs	z/Architecture operating systems ESA/390 operating systems Linux	CPs DED *or* CPs SHR
	CPs *and* zAAPs *or* zIIPs	z/OS z/VM (V5.3 and later, for guest exploitation)	CPs DED *and* zAAPs DED, *and/or* zIIPs DED *or* CPs SHR *and* zAAPs SHR *and/or* zIIPs SHR
ESA/390 TPF	CPs	TPF z/TPF	CPs DED *or* CPs SHR
Coupling facility	ICFs *or* CPs	CFCC	ICFs DED *or* ICFs SHR, *or* CPs DED *or* CPs SHR
Linux only	IFLs or CPs	Linux z/VM	IFLs DED *or* IFLs SHR, *or* CPs DED *or* CPs SHR
z/VM	CPs, IFLs, zAAPs, zIIPs ICFs	z/VM V5.4 or later	All PUs must be either SHR *or* DED

Processor page definitions

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open a reset or image profile for an LP. Open the Processor page to define the following LP characteristics:
- Dedicated or shared general purpose CPs
- Dedicated or shared internal coupling facility (ICF) CPs
- Number of initial and reserved processors
- Initial processing weight
- Initial weight capping
- Workload manager enablement
- Minimum processing weight
- Maximum processing weight

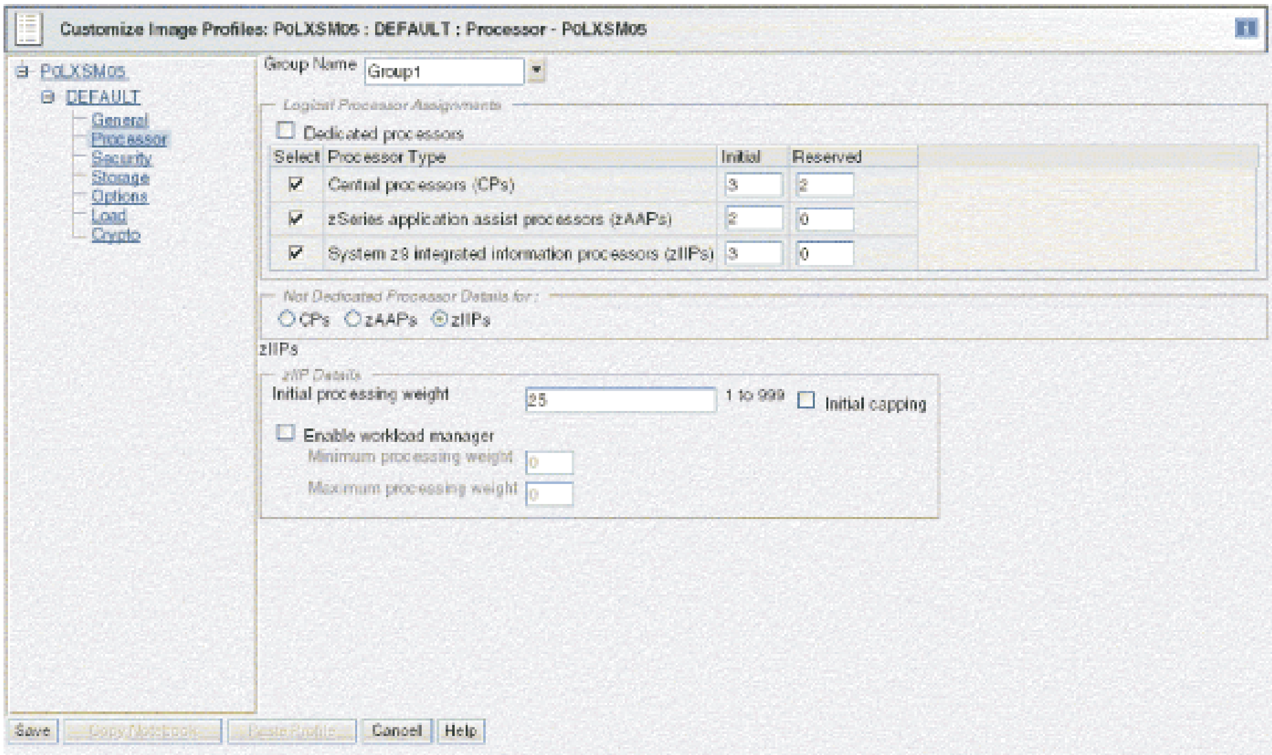


Figure 37. ESA mode logical partition with shared CPs, zAAPs, and zIIPs. There can be both an initial and reserved specification for each processor type. Each processor can have its own processing weight(s). If WLM is enabled, it is enabled for the entire partition. If WLM is not enabled for the partition, you may specify initial capping for the various processor types defined for the partition, but you do not have to set it the same for all the processor types; they can be set independently. For example, you can specify initial capping on for zIIPs but not for CPs in that same partition. WLM enablement and Initial Capping are mutually exclusive.

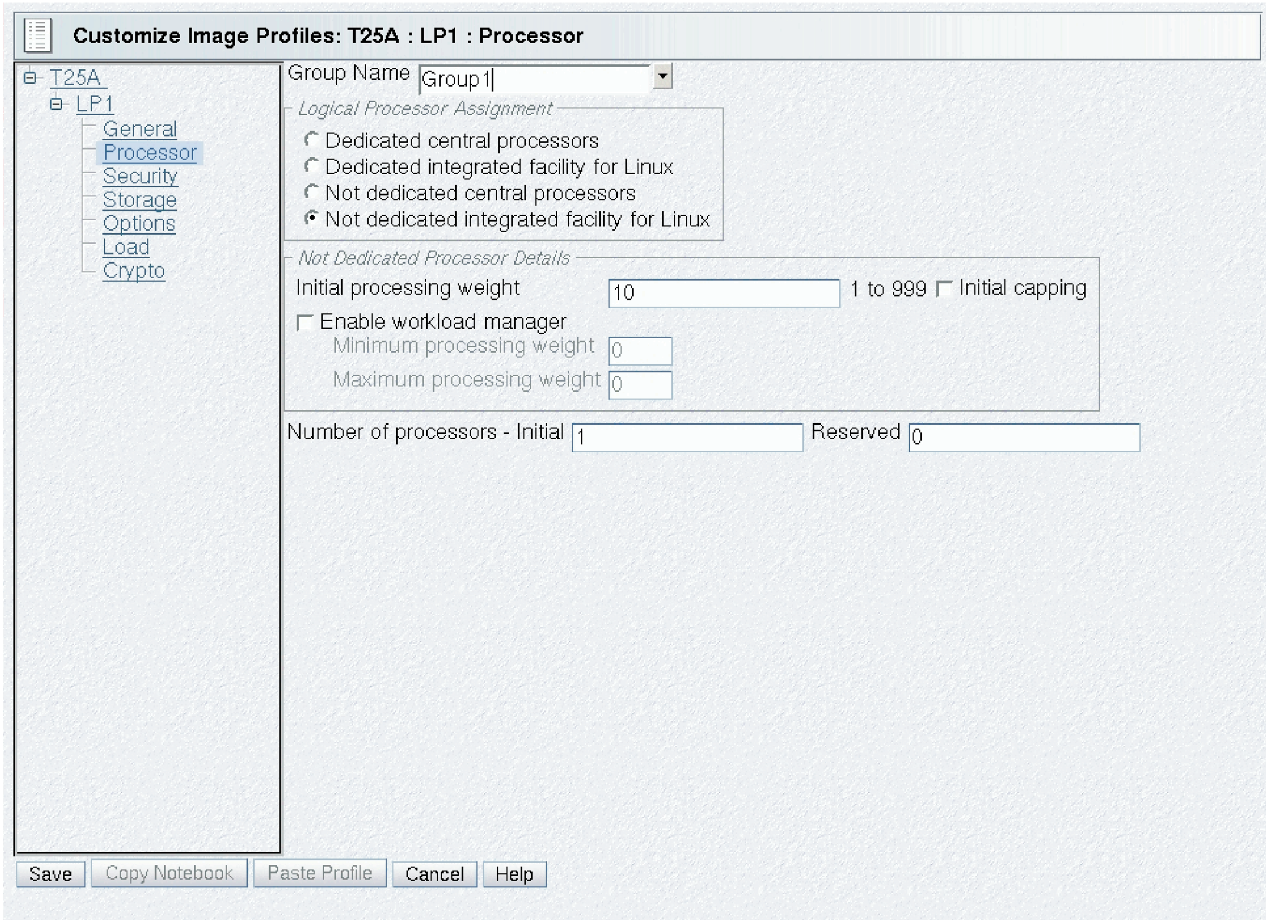


Figure 38. Customization for a Linux-only mode logical partition with shared Integrated Facilities for Linux (IFLs). There can be both an initial and reserved specification for the IFLs.

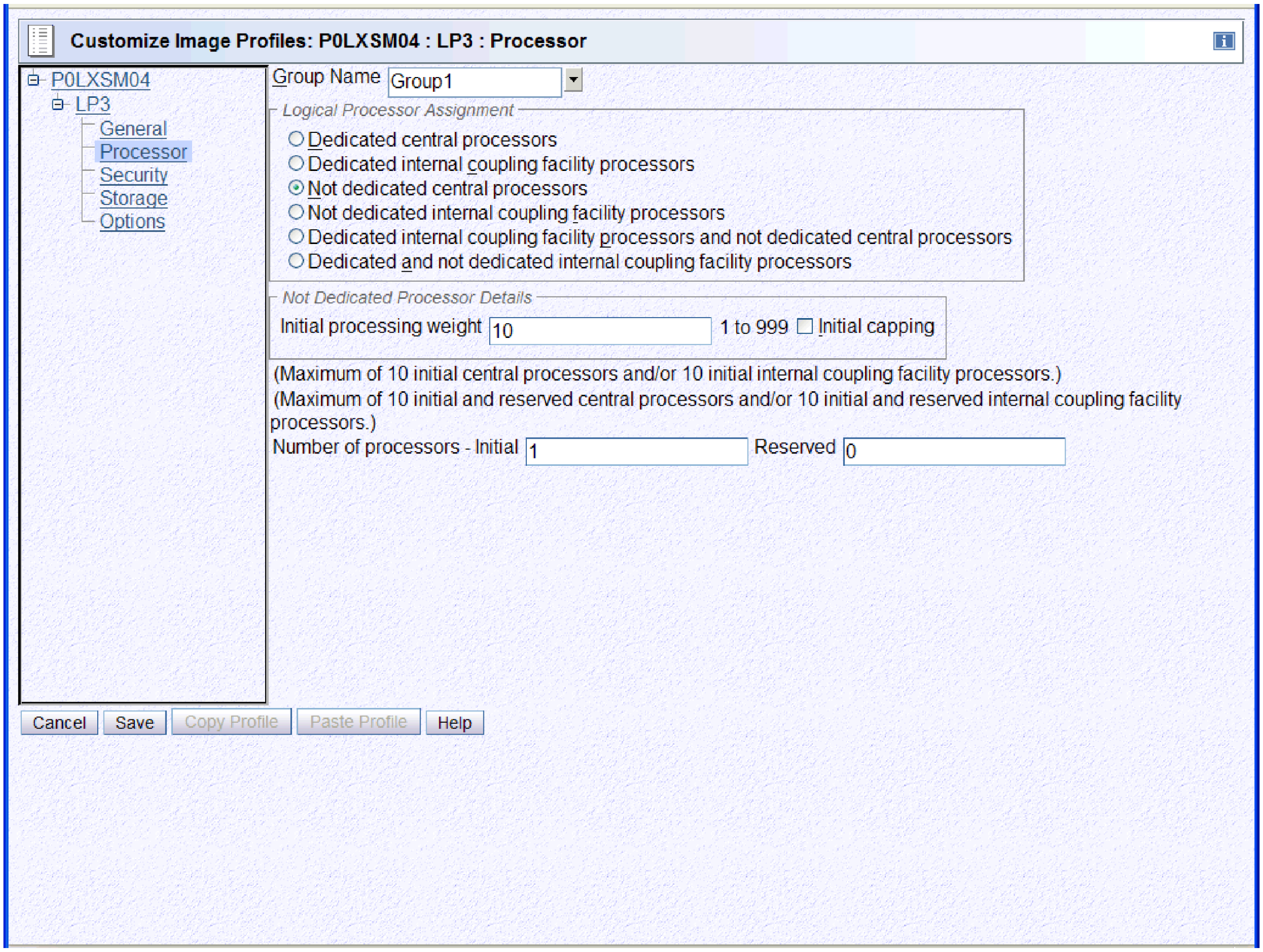


Figure 39. Customization for a coupling facility mode logical partition with shared central processors. There can be both an initial and reserved specification for the Central Processors.

Parameter descriptions

Note: Depending on the processor page, (see Figure 37, Figure 38 and Figure 39) some of the following parameters may not be present.

Group Name
If you choose to assign the processor to a group, select a defined group from the list.

Dedicated processors
Select this option if you want to select general purpose CPs, zAAPs or zIIPs to be dedicated when the LP is activated. You can then specify the number of initial and reserved processors for each.

Not dedicated processor details
Select the processor (CPs, zAAPs, or zIIPs) to display details such as Initial processing weight, Initial capping, and Enable workload manager.

Dedicated central processors
Select this option if you want the general purpose CPs that are allocated for the LP to be dedicated when the LP is activated.

Not dedicated central processors
Select this option if you want the general purpose CPs that are allocated for the LP to be shared when the LP is activated.

Dedicated integrated facility for Linux

Note: All processors assigned to a coupling facility partition should be dedicated to that logical partition if it is used for primary production workload.

If Integrated Facility for Linux (IFL) is supported and installed in the Central Processor Complex (CPC), select Dedicated integrated facility for Linux if you want an IFL processor dedicated to each logical processor.

Not dedicated integrated facility for Linux
If you want the logical processors to share not dedicated integrated facility for Linux (Integrated Facility for Linux (IFL) processors that are not already dedicated to other activated logical partitions when this logical partition is activated), select Not dedicated integrated facility for Linux.

Dedicated internal coupling facility processors
If internal coupling facility processors are supported by and installed in the Central Processor Complex (CPC), select Dedicated internal coupling facility processors if you want one dedicated to each logical processor.

Not dedicated internal coupling facility processors

Note: All processors assigned to a coupling facility partition should be dedicated to that logical partition if it is used for primary production workload.

If you want the logical processors to share not dedicated internal coupling facility processors (internal coupling facility processors that are not already dedicated to other activated logical partitions when this logical partition is activated), select Not dedicated internal coupling facility processors.

Dedicated internal coupling facility processors and not dedicated central processors

Note: This option is part of a facility (Dynamic ICF Expansion) that IBM has announced plans to pull complete support from in a future product. IBM recommends against using this option.

Note: All processors assigned to the coupling facility partition should be dedicated to that logical partition if it is used for primary production workload.

If internal coupling facility processors are supported by and installed in the CPC, select Dedicated internal coupling facility processors and not dedicated central processors if you want to assign a combination of dedicated internal coupling facility processors and not dedicated central processors to the logical partition.

Dedicated and not dedicated internal coupling facility processors

Note: This option is part of a facility (Dynamic ICF Expansion) that IBM has announced plans to pull complete support from in a future product. IBM recommends against using this option.

Note: All processors assigned to the coupling facility partition should be dedicated to that logical partition if it is used for primary production workload.

If internal coupling facility processors are supported by and installed in the CPC, select Dedicated and not dedicated internal coupling facility processors and not dedicated central processors if you want to assign a combination of dedicated internal coupling facility processors and not dedicated internal coupling facility processors to the logical partition.

Initial processing weight
: Enter a value between 1–999 to set the processing weight for the type of processor for an LP. The default value is 10.

Initial capping
: Select this option to cap the CP resources for the type of processor for an LP. Capping has no effect on LPs with dedicated CPs.

Enable WorkLoad Manager
: Select this option so that CPU and I/O resources can be managed by WLM using IRD clustering technology.

Minimum processing weight
: Select this option to establish a minimum processing weight that WLM will allocate to the LP. Do not specify a value here unless you determine a true need for it in your configuration. Specifying a value here can needlessly constrain what WLM can do to optimize the management of your workload.

Maximum processing weight
: Select this option to establish a maximum processing weight that WLM will allocate to this LP. Do not specify a value here unless you determine a true need for it in your configuration. Specifying a value here can needlessly constrain what WLM can do to optimize the management of your workload.

Security characteristics

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open a reset or image profile for an LP. Open the Security page to define the following LP characteristics:

- Partition Security Options
- Counter Facility Security Options
- Sampling Facility Security Options

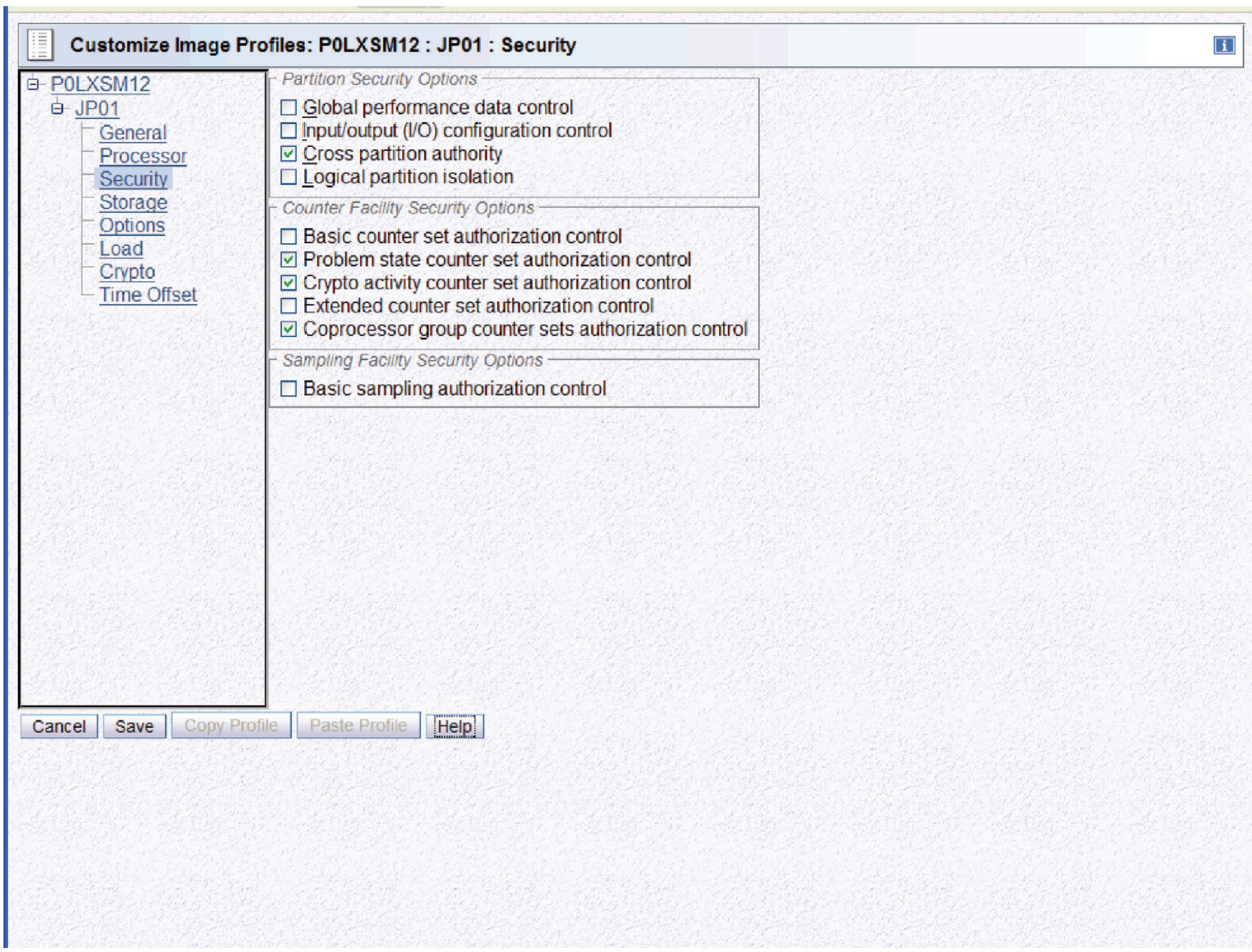


Figure 40. Security page, image profile

Parameter descriptions

Partition security options:

Global performance data control
Select this option to allow the LP to view the CPU utilization data and the Input/Output Processor (IOP) data for all LPs in the configuration. Not selecting this option only allows the LP to view its own CPU utilization data. Additionally, gathering of FICON channel measurements requires selection of this parameter. The default is selected.

Note: An LP running a level of RMF that supports FICON requires control authority even if no FICON is installed.

Input/output (I/O) configuration control
Select this option to allow the LP to read or write any IOCDS in the configuration and to make dynamic I/O changes. Additionally, this parameter allows the OSA Support Facility for z/OS, z/VM, and z/VSE to control OSA configuration for other LPs. The default is selected.

Cross partition authority
Select this option to allow the LP to issue control program commands that affect other LPs; for example, perform a system reset of another LP, deactivate an LP, or provide support for the automatic reconfiguration facility. The default is not selected.

Logical partition isolation
Select this option to reserve unshared reconfigurable channel paths for the exclusive use of the LP. The default is not selected.

Counter facility security options:

Basic counter set authorization control
Select this option to authorize the use of the basic counter set. This set includes counts of central processing unit cycles, instructions executed, and directory-write and penalty cycles for level-1 instruction and data caches.

Problem state counter set authorization control
Select this option to authorize the use of the problem state counter set. This set includes counts of central processing unit cycles, instructions executed, and directory-write and penalty cycles for level-1 instruction and data caches only when the processor is in problem state.

Crypto activity counter set authorization control
Select this option to authorize the use of the crypto activity counter set. This set includes counters for a central processing unit related to PRNG, SHA, DEA, and AES function counts.

Extended counter set authorization control
Select this option to authorize the use of the extended counter set. The extended counters provide information about hardware facilities and structures that are specific to a machine family. The extended counters are designed to expand upon information provided by the Basic Counter Set.

Coprocessor group counter sets authorization control
Select this option to authorize the use of the coprocessor group

counter sets. This set includes counters for all central processing units attached to the coprocessor related to PRNG, SHA, DEA, and AES function counts.

Sampling facility security options:

Basic sampling authorization control
Select this option to authorize the use of the basic sampling function. Samples are taken and stored at the end of each sampling interval.

Establishing optional characteristics

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open a reset or image profile for an LP. Open the Options page to define the following LP characteristics:

- Minimum input/output (I/O) priority
- Maximum input/output (I/O) priority
- Defined capacity

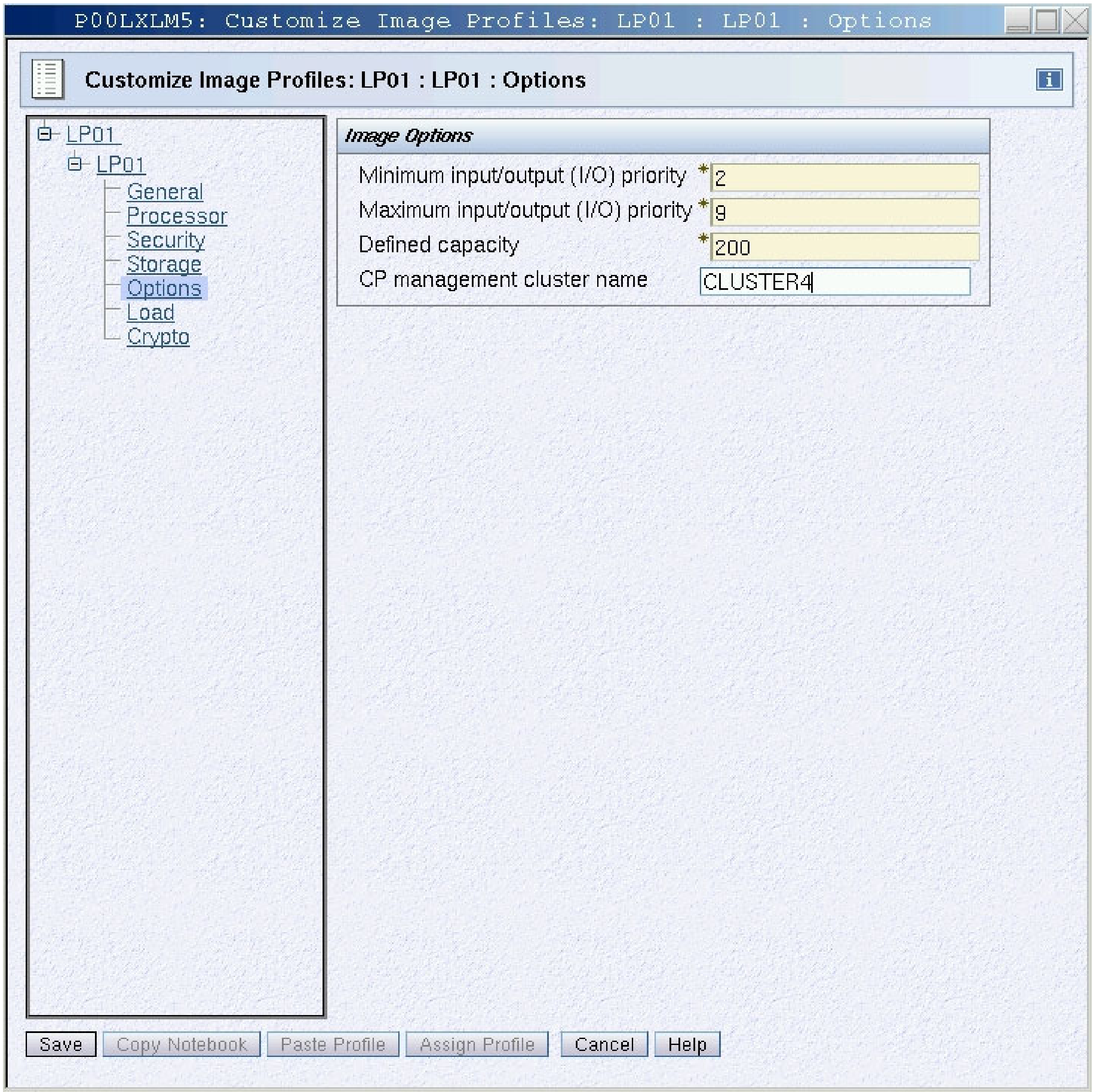


Figure 41. Options page, image profile

Parameter descriptions

Minimum input/output (I/O) priority
Enter the minimum priority to be assigned to I/O requests from this logical partition.

Maximum input/output (I/O) priority
Enter the maximum priority to be assigned to I/O requests from this logical partition.

Defined capacity
Enter the upper bound in terms of millions of service units (MSUs) beyond which the rolling 4-hour average CPU utilization cannot proceed.

CP management cluster name
Enter the name of the Sysplex Cluster of which this logical partition will be made a member. z/OS will not IPL if the name defined in the Image Profile does not match the sysplex name with which the IPLing system is associated.

Storage characteristics

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization Tasks list to open a reset or image profile for an LP. Open the Storage page to define the following LP characteristics:

- Central storage
- Expanded storage

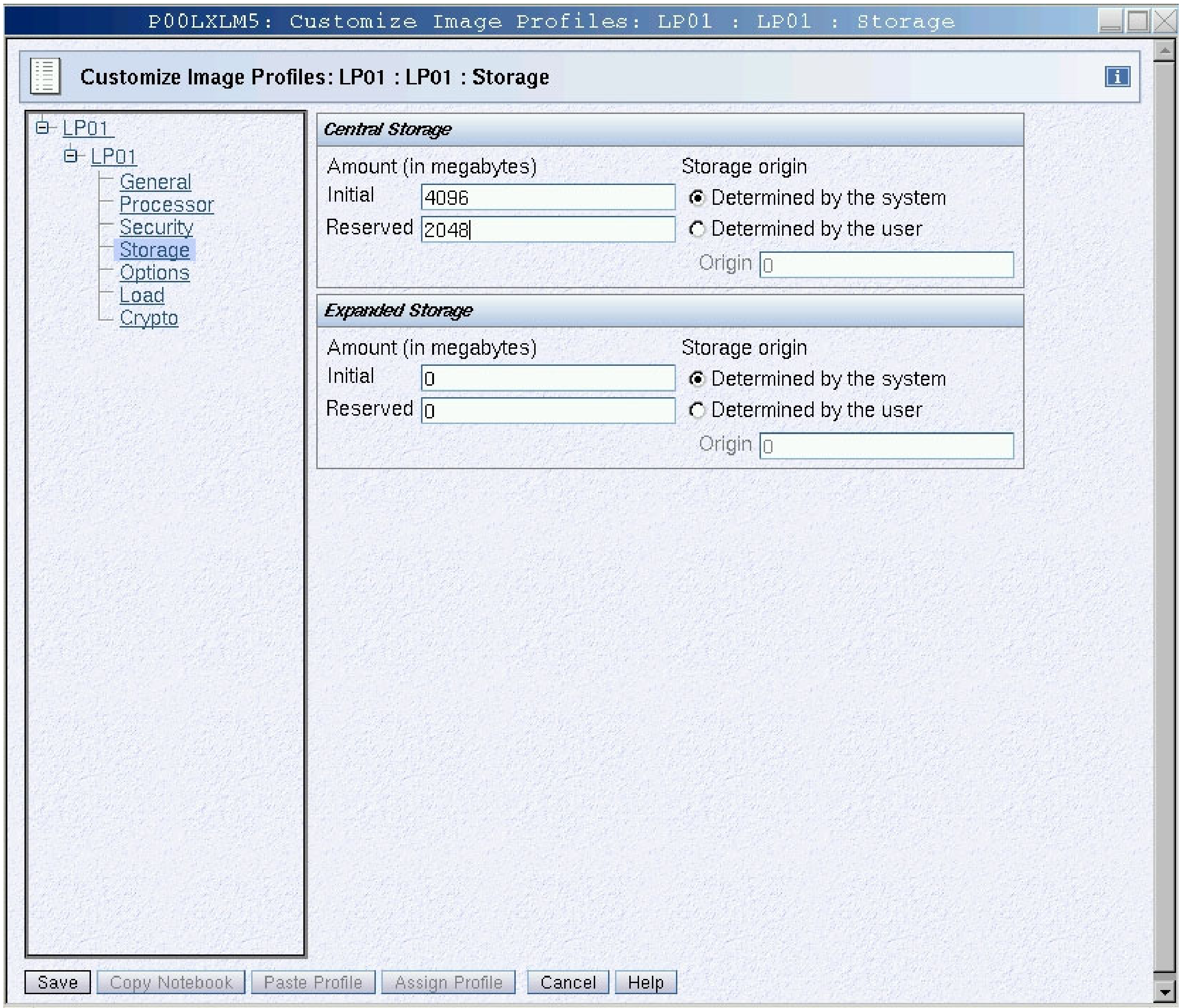


Figure 42. Storage page, image profile

Central storage parameter descriptions

See “Central storage” on page 102 for a discussion of the appropriate entries for these fields.

Initial
Enter, in MB, the initial amount of central storage to be allocated to the LP at activation.

Reserved
Enter, in MB, the amount of additional central storage requested for the LP. The reserved storage space is storage that can be dynamically brought online to the LP at some point after LP activation. Entering 0 limits central storage to the initial amount for

the duration of the LP activation. Enter a value that is compatible with the storage granularity supported by your CPC.

Storage origin
If **Determined by the user** is selected, enter, in MB, the central storage origin for the LP. When the LP is activated, it is allocated at the origin you specify here. Enter a value that is compatible with the storage granularity supported by your CPC.

Determined by the system
Select this option if you want the system to allocate where the LP storage resides.

Determined by the user
Select this option if you want to allocate where the LP storage resides.

Expanded storage parameter descriptions

See "Expanded storage" on page 104 for a discussion of the appropriate entries for these fields.

Initial Enter, in MB, the initial amount of expanded storage to be allocated to the LP at activation. Enter a value that is compatible with the storage granularity supported by your CPC.

Reserved Enter, in MB, the amount of additional expanded storage requested for the LP. The reserved storage space is storage that might be dynamically brought online to the LP at some point after LP activation. Entering 0 limits expanded storage to the initial amount for the duration of the LP activation. Enter a value that is compatible with the storage granularity supported by your CPC.

Storage origin
Enter, in MB, the expanded storage origin for the LP. When the LP is activated, it is allocated at the origin you specify here. Enter a value that is compatible with the storage granularity supported by your CPC.

Determined by the system
Select this option if you want the system to allocate where the LP storage resides.

Determined by the user
Select this option if you want to allocate where the LP storage resides.

Load information

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open an image or load profile for an LP. Open the Load page to define the following LP characteristics:

- Load during activation
- Load address
- Load parameter
- Load timeout value

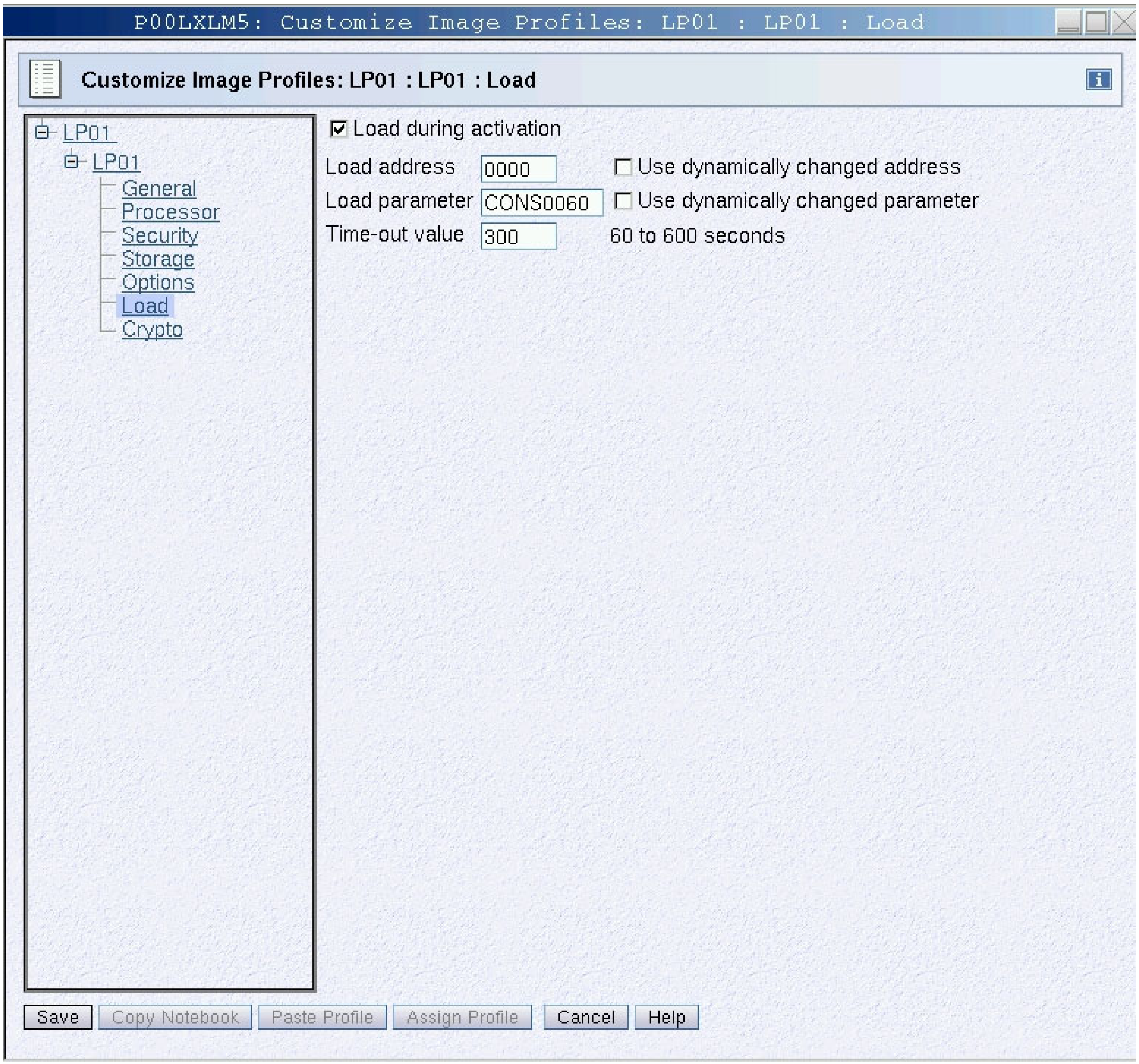


Figure 43. Load page, image profile

Parameter descriptions

Load during activation
Selecting this option allows initial program load of the operating system to occur automatically at LP activation. The default is not selected.

Load address
Enter the hex address of the I/O device containing the operating system to be loaded automatically at LP activation.

Use dynamically changed address
Select this option if you want to use the load address from a dynamically changed I/O configuration. This option and the **Load address** option are mutually exclusive.

Load parameter
Enter a 1 to 8 character, optional IPL load parameter for loading an operating system on each activation of the LP. This is useful for loading z/OS, or z/VSE.

Use dynamically changed parameter
Select this option if you want to use the load parameter from a dynamically changed I/O configuration. This option and the **Load address** option are mutually exclusive.

Time-out value
Enter a time-out value in seconds to limit the amount of time for successful completion of the operating system load.

Cryptographic characteristics

Use the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list to open a reset or image profile for an LP.

Note: Any changes to the Crypto Image Profile Page settings require a DEACTIVATE and ACTIVATE of the LP to have the change take effect. To verify the active settings for the Cryptographic characteristics use the View LPAR Cryptographic Controls task available from the CPC Operational Customization tasks list (For information regarding the View LPAR Cryptographic Controls page, see "Reviewing and changing current logical partition cryptographic controls" on page 196.)

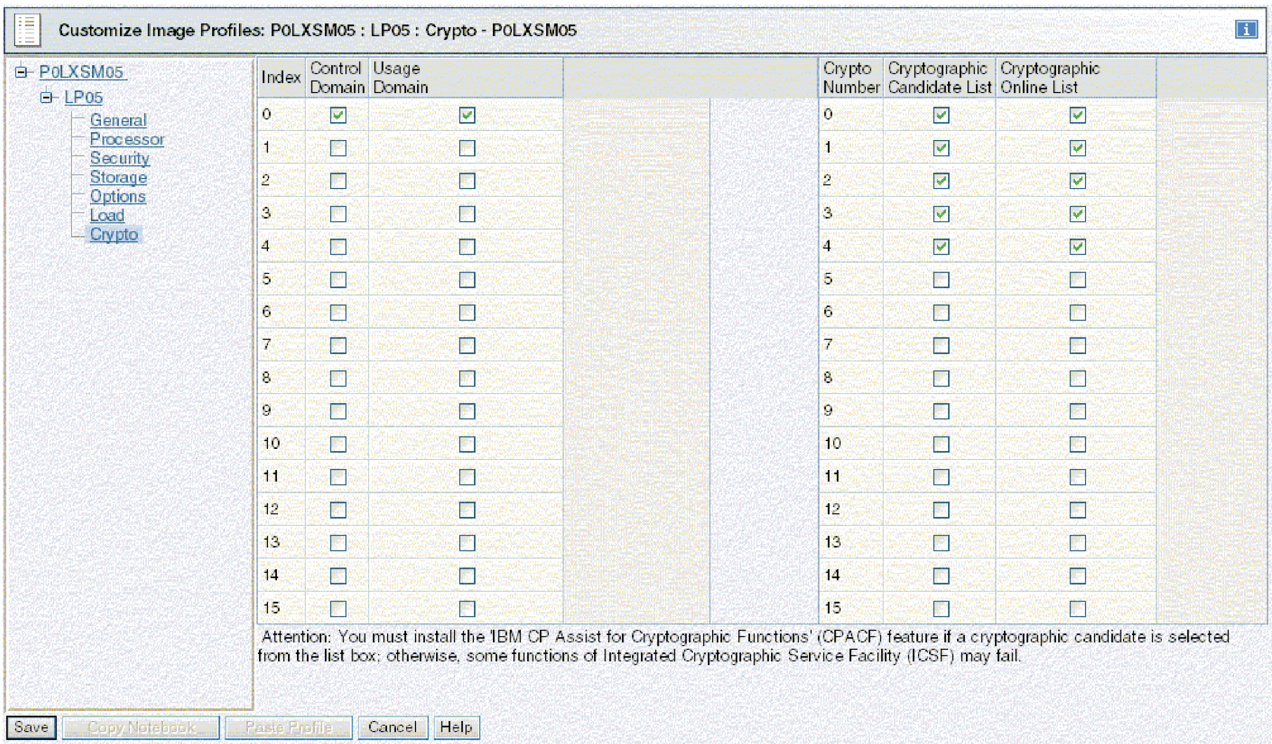


Figure 44. Crypto page, image profile

Parameter descriptions

Control domain index

The Control Domain Index identifies the Crypto domain index(es) that can be administered from this logical partition when a partition is set up as the TCP/IP host for the TKE Workstation. The Control Domain Index selected must also be selected in the Usage Domain Index of the logical partitions to be managed by the TKE Workstation.

If you are setting up the host TCP/IP in this logical partition for communicating with the TKE Workstation, the partition will be used as a path to this and the other domains' keys. Indicate all the domains you want to access, including this partition's own domain, from this partition as control domains.

Note: You can manage both master keys and operational keys from a TKE.

For more TKE Workstation information, refer to the *z/OS ICSF TKE Workstation User's Guide*.

Usage domain index

The Usage Domain Index identifies the cryptographic domain(s) assigned to the partition for all cryptographic coprocessors or accelerators that are configured for the partition. The usage domain denotes where a specific partition's secure crypto data resides and where applications running on that partition will be obtaining the cryptographic data.

If running z/OS, one of the usage domain index(es) selected should match the domain number entered in the Options dataset when starting this partition's instance of ICSF. As of z/OS 1.2 the usage domain specification in the Options dataset is only required if multiple usage domain index(es) are selected.

If running z/VM in a logical partition with guests, such as Linux or z/OS, a range of usage domain indices should be selected when assigning access to the cryptographic accelerator or coprocessor. A range will allow more than one guest to have dedicated or shared access to the cryptographic queues. For further information, see the *z/VM CP Planning and Administration* and *z/VM Running Guest Operating Systems* documents.

The Usage Domain Index in combination with the Cryptographic Number selected in the Candidate List, must be unique across all partitions defined to the CPC. Although the Customize Image Profiles panel allows you to define duplicate combinations of Cryptographic number(s) and Usage Domain Index(es), such logical partitions cannot be concurrently active. This is a useful option, for example, for backup configurations.

Cryptographic Candidate List

The Cryptographic Candidate List identifies the Cryptographic numbers that are eligible to be accessed by this logical partition. Select from the list the number(s), from 0 to 15, that identify the coprocessor or accelerator to be accessed by this partition.

When the partition is activated, an error condition is not reported if a Cryptographic number selected in the Candidate list is not installed in the system. Selecting a Cryptographic number that is not installed prepares the settings in the active partition in the event that you wish to nondisruptively install the crypto in the future.

Crypto Express2, available on the z10 BC and z10 EC, contains two PCI-X adapters, each of which can be configured independently as either a coprocessor or an accelerator. The default configuration is coprocessor. Crypto Express 2-1P, available on the z10 BC, contains one PCI-X adapter per feature. Crypto Express2-1P can also be defined as either a coprocessor or an accelerator. Each of those PCI-X adapter cards will have a unique cryptographic number assigned. These numbers are assigned in sequential order during installation. A CEX2A or a CEX2C can be shared across 16 partitions.

It is possible to select all 16 index values (0-15) even before a Crypto Express2 feature is installed. When a new Crypto Express2 feature is installed and its cryptographic number(s) have been previously selected in the Candidate list of an active partition, it can be configured on to the partition from the Support Element using the **Configure On/Off** option in the Crypto Service Operations task list.

Selecting all the values will not cause a problem if you have 16 or fewer partitions in your configurations that will be using the Crypto Express2 feature. If you have more than 16 partitions that will need access to cryptographic coprocessors or accelerators, you will have to carefully assign the selection of cryptographic numbers across the partitions. Or, if you are running z/VM in one or more partitions, you may want to assign more than one Cryptographic number to each VM partition so that one or more than one type of Crypto card is available for use by VM guests.

For example, you have 19 logical partitions defined, and all will require the use of Crypto Express2. Some partitions will only need Crypto for acceleration of SSL handshakes using CEX2A, and others will need secure key operations from CEX2C. Assume the 19 partitions will share 2 CEX2C features and 2 CEX2A features. The Crypto selection could be as shown here for the following Crypto numbers:

Table 18. Example Selection of Crypto Numbers

Feature	Adapter	Crypto Configuration	Type	Crypto Number
Crypto Express2 1	1	Accelerator	A	00
	2	Accelerator	A	01
Crypto Express2 2	1	Coprocessor	X	02
	2	Coprocessor	X	03
Crypto Express2 3	1	Accelerator	A	04
	2	Coprocessor	X	05
Crypto Express2 4	1	Coprocessor	X	06
	2	Accelerator	A	07

Note: For Availability reasons, it is recommended that at least two cryptographic adapters of the same type and capability be assigned to each partition that executes cryptographic operations. Because CEX2As do not contain any internal security data (cryptographic keys), all CEX2As are equivalent. CEX2Cs, on the other hand, will contain cryptographic keys and it is recommended that at least two CEX2Cs with the appropriate domains and cryptographic keys be assigned to a logical partition (LP) that requires secure key operations.

Table 19. LP & crypto assignments

LP & Crypto Use	Usage Domain Assignment	Logical Partition Assignment	Backup Required? Specify 2nd Logical Partition
ACME0 Prod SSL only[1,2]	UD=0	A00	A04
ACME1 Prod SSL only[1]	UD=1	A00	A04
ACME2 Prod SSL & secure	UD=2	A00 & X02	A04 & X05
ACME3 Prod SSL only[2]	UD=0	A01	A07
.... SSL only	UD=3...10	A00	A01
ACMEF Prod SSL only	UD=0	A04	A07
ACM17 Prod SSL & secure[3]	UD=4	A00 & X05	A01 & X06
ACM18 Test SSL & secure[3]	UD=5, 2[4]	A00 & X02	A04 & X05

Table 19. LP & crypto assignments (continued)

LP & Crypto Use	Usage Domain Assignment	Logical Partition Assignment	Backup Required? Specify 2nd Logical Partition
ACM19 Test SSL only	UD=6	A00	A04
ACM5VM Prod VM	UD=7, 8, 9, 10	A07 & X05	

Notes:

1. LPs ACME0 and ACME1 both use Accelerator cards A00 and A04, however, they use two different Usage Domains on these cards.
2. LPs ACME0 and ACME3 both use Usage Domain 0, but they use them on different accelerator cards, A00/A04 and A01/A07.
3. LPs ACM17 and ACM18 both use Crypto Coprocessor X05, but they use different Usage Domains on those cards, so there is no conflict.
4. ACM18 has two Usage Domains assigned, but only one can be used at a time. Normally, this TEST LP will provide SSL and Secure support for the Test environment using Usage Domain 5 on crypto accelerator cards A00 and A01, and crypto coprocessor cards X05 and X06. By defining this LP with access to Usage Domain 2 it can be a backup LP for ACME2. If and when there is a problem with LP ACME2, that operating system can be IPL'd in this LP, with the ICSF started task pointing to UD=2, and it will be able to access the cryptographic keys for ACME2, which are stored in Usage Domain 2 on X02 and X05.

It is very important to make the correct Crypto number assignments in the Cryptographic Candidate List for each of these logical partitions to avoid assignment conflicts.

If the customer plans to use ICSF or the optional cryptographic hardware, the CP Crypto Assist functions (CPACF DES/TDES) must be enabled. Many IBM products will take advantage of the cryptographic hardware using ICSF, so enabling CPACF is recommended. See the*z/OS ICSF Administrator's Guide* and the *z/OS ICSF System Programmer's Guide* for complete information.

Cryptographic Online List

The Cryptographic Online List identifies the Cryptographic numbers that are automatically brought online during logical partition activation. The Cryptographic numbers selected in the Online List must also be selected in the Candidate List.

After partition activation, installed Cryptographic features that are in the partition Cryptographic Candidate list but not in the Cryptographic Online List are in a *configured off* state (Standby). They can be later configured *on* to the partition from the Support Element using the **Configure On/Off** option in the Crypto Service Operations task list.

When the partition is activated, an error condition is not reported if the Cryptographic number selected in the Online list is not installed in the system. The Cryptographic number is ignored and the activation process continues.

If a Cryptographic number selected in the Online list has been configured off to the partition, it is automatically configured back on during the next partition activation.

Creating a logical partition group profile

Creating a group, or grouping logical partitions, is a way to assign more than one activation profile to an object, rather than changing the object's assigned activation profile every time you want to activate it differently. Grouping creates copies of objects on the Support Element workplace. The objects can be the CPC or its images. Different groups can contain the same object, such as the CPC, but the object's settings in one group can be customized independently of its settings in other groups. One such setting is the activation profile assigned to the object.

Use the Customize Group Profiles task available from the CPC Operational Customization tasks list to create a logical partition group profile. To access this task, select the default Group profile and click **Customize selected profile**:

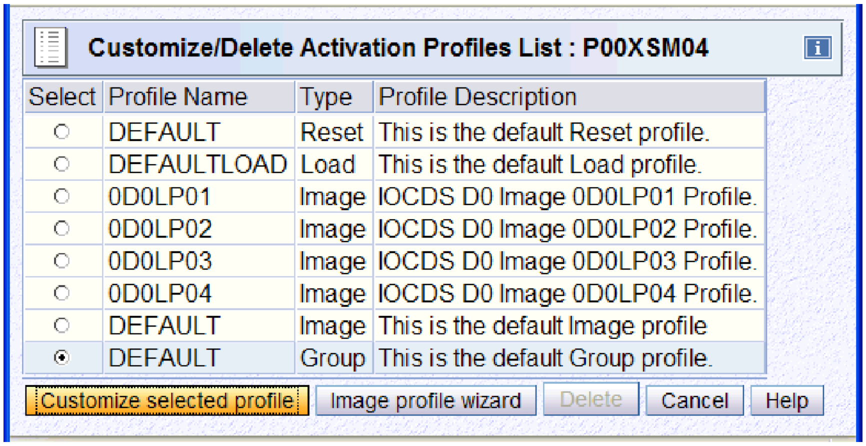


Figure 45. Customize/Delete Activation Profiles List

The Customize Group Profiles window appears:

Figure 46. Customize Group Profiles window

On the Customize Group Profiles window, select the **Group name** list to select a group to use as a template for the new group, or use DEFAULT if no other groups exist. Then enter a unique name for the logical partition in the Group name field. Enter a description of the new group name in the **Group description** field. Click **Save** to save the new group profile.

For detailed information about grouping objects for activation, see the *System z10 Support Element Operations Guide*.

Enabling Input/Output priority queuing

Use the Enable I/O Priority Queuing task available from the CPC Operational Customization tasks list to either enable or disable I/O priority queuing for the entire CPC.

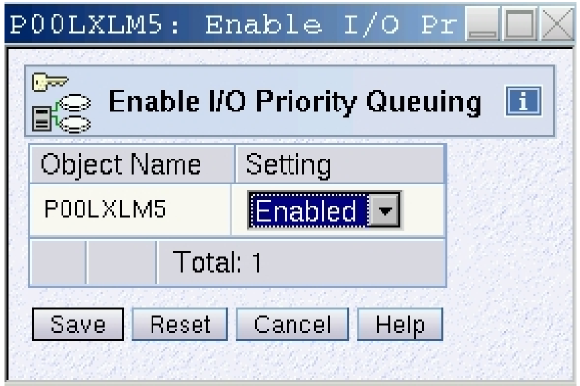


Figure 47. Enabling I/O priority queuing

Changing logical partition Input/Output priority queuing values

Use the Change Logical Partition I/O priority queuing task available from the CPC Operational Customization tasks list to set the minimum and maximum I/O priority queuing values for logical partitions.

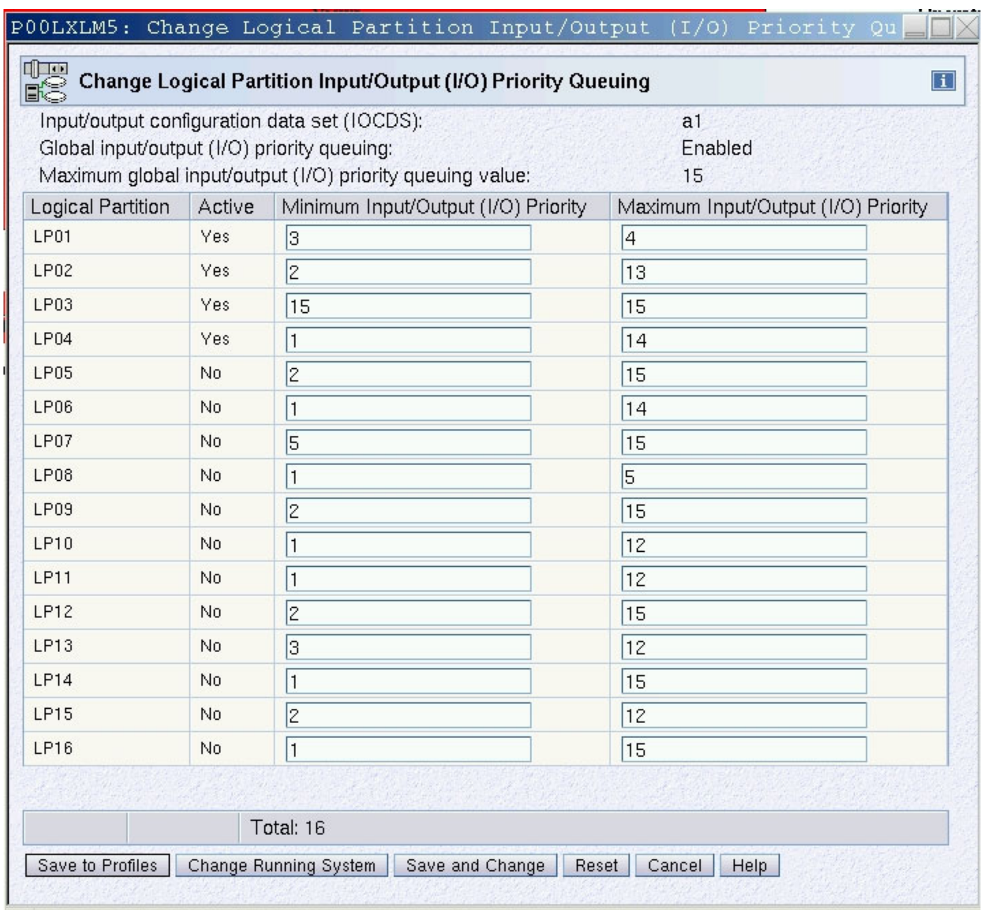


Figure 48. Change Logical Partition I/O priority queuing

Note: **Minimum I/O Priority** and **Maximum I/O Priority** should be specified as a range of values that give software some ability to make choices. All logical partitions in a given LPAR cluster should be given the same range of values so that WorkLoad Manager can optimize I/O throughput across the LPAR cluster.

If the software in the logical partition does not have an understanding of I/O Priority Queuing, the system programmer should set the Minimum and Maximum I/O priorities to the same value. The value chosen will be assigned to that logical partition as a constant priority value relative to all other logical partitions. This way even logical partitions that do not employ IRD technologies can benefit from this support.

Parameter descriptions

Minimum input/output (I/O) priority
: Enter the minimum priority to be assigned to I/O requests from this logical partition.

Maximum input/output (I/O) priority
: Enter the maximum priority to be assigned to I/O requests from this logical partition.

Moving unshared channel paths

You can move reconfigurable channel paths owned by one LP to another LP.

Moving unshared channel paths from a z/OS system

1. Select the LP that owns the channel path to display channel path information for the LP.
2. Move the channel path from the z/OS console.
   a. Enter **CF CHP(***nn***),OFFLINE**, where *nn* is the number of the desired channel path, from the z/OS operator console that has the reconfigurable channel path online.
   b. Enter **CF CHP(***nn***),ONLINE**, where *nn* is the number of the desired channel path, from the z/OS operator console that is the target LP.

   Notes:

   1) If a channel path is configured offline while the LP is isolated and remains offline when you change the LP's isolation status from enabled to disabled, the channel path must be configured offline again. See "Releasing reconfigurable channel paths."
   2) If the channel path you want to move is currently assigned to a deactivated LP, you must configure it offline from the hardware console.
   3) If the LP is not running a system control program that supports channel path configuration commands, you can move the channel path from the hardware console.

Moving a channel path from the hardware console

1. Select the LP that owns the channel path to display channel path information for the LP.
2. Select a reconfigurable channel path from the CHPIDs work area. Drag and drop the CHPID on the Reassign Channel Path task available from the CHPID Operations task list.
3. The Reassign a Channel Path panel displays the targeted channel path, the current owning LP, and a list of target LPs to which you can reassign the channel path. Select the LP to which you want to reassign the channel path.
4. Click on the Reassign push button and confirm the action to release the channel path.
5. When the "Requested operation is complete" message appears, click on the OK push button.

Releasing reconfigurable channel paths

Use this procedure when the owning LP has LP isolation enabled.

1. Select the LP that owns the channel path to display channel path information for the LP.
2. Select a reconfigurable channel path from the CHPIDs work area. Drag and drop the CHPID on the Release task available from the CHPID Operations task list.

   A Confirm the Action panel will display warning you that the channel paths will be released and made available for reassignment to other LPs. Confirming the action will release the channel path and a "Requested operation is complete" message will display. Click on the OK push button to complete the task.

Configuring shared channel paths

Verify the status of the channel path for each LP to which you plan to configure the channel path by opening each LP's CHPIDs Work Area.

Enter **CF CHP(*nn*),ONLINE** (where *nn* is the number of the desired CHPID) from each z/OS operator console to which the CHPID is to be brought online.

If the operating system running in the LP is not z/OS, use the Configure On/Off task available from the CHPID Operations task list to configure the CHPID online. The shared channel path will be physically configured when the first LP configures the channel path online.

Note: Dynamically managed channel paths can be configured ***Off*** but **cannot** be configured ***On*** from the Support Element's CHPID Operations task list.

Deconfiguring shared channel paths

Verify the status of the channel path for each LP to which you plan to configure the channel path by opening each LP's CHPIDs Work Area.

Enter **CF CHP(*nn*),OFFLINE** (where *nn* is the number of the desired CHPID), from each z/OS operator console from which the CHPID is to be taken offline.

If the operating system running in the LP is not z/OS, use the Configure On/Off task available from the CHPID Operations task list to configure the CHPID offline. The shared channel path will be physically deconfigured when the last LP that had the channel path online configures it offline.

Removing shared channel paths for service

1. Enter (from the z/OS console that has the shared channel path online) **CF CHP(*nn*) OFFLINE**, where *nn* is the number of the desired CHPID.
2. Use the Toggle all off option in the Configure On/Off task available from the CHPID Operations task list to remove the CHPID.

   The Toggle all off option detaches the CHPID from all LPs that it is currently attached to regardless of the target LP. A CHPID that is shared by multiple LPs is detached from all LPs without forcing you to detach it individually from each LP.

   Toggle all off is also valid for unshared CHPIDs and it is mutually exclusive of the Release task.
3. Use the Service On/Off task available from the CHPID Operations task list to remove the CHPID.

Changing logical partition definitions

You can make changes to LP definitions that are available dynamically to a running LP or that are available at the next LP activation.

Changes available dynamically to a running LP

The following changes are available dynamically to a running LP:

- Using the Change Logical Partition Controls task, you can change the following LP definitions:
  - Initial processing weight

- Minimum processing weight
  - Maximum processing weight
  - WorkLoad Manager enablement
  - Processor weight capping
  - Processor running time (globally applicable to logical CPs of all shared LPs)
  - Global enablement of event-driven dispatching
  - Defined capacity
- Using the Change Logical Partition Input/Output (I/O) Priority Queuing Controls task, you can change the following LP definitions:
  - Minimum input/output (I/O) priority
  - Maximum input/output (I/O) priority
- Using the Change Logical Partition Security task, you can change the following LP definitions:
  - Global performance data control
  - Input/Output configuration control
  - Cross partition authority
  - Logical partition isolation
  - Basic counter set authorization control
  - Problem state counter set authorization control
  - Crypto activity counter set authorization control
  - Extended counter set authorization control
  - Coprocessor group counter sets authorization control
  - Basic sampling authorization control
- Using the Logical Processor Add task, you can do the following:
  - Increased the reserved value for a processor (general, zAAP, zIIP, IFL, etc)
  - Add a new processor type not yet in use for that partition
  - increase the initial value for a given processor type
  - Can change the running system or save the changes to profiles.
- Using the Change Logical Partition Cryptographic Controls task, you can:
  - Add a crypto adapter to a partition for the first time
  - Add a crypto adapter to a partition already using crypto adapters
  - Remove a crypto adapter from a partition
  - Zeroize, or clear the cryptographic secure keys for a given usage domain.

Changes available at the next LP activation

The following changes are available at the next LP activation:

- Use the IOCP RESOURCE statement to specify the MIF image ID numbers assigned to the LPs. The only way to change the specified MIF image ID numbers is by creating a new IOCDS.
- Use the Partitions page in the reset profile to change the:
  - LP automatic activation order
- Use the General page in the image profile to change the:
  - Logical partition identifier
  - Mode of the LP
  - Enablement of the Logical partition time offset
- Use the Processor page in the image profile to change the:
  - Number of CPs, ICFs, IFLs, zAAPs, or zIIPs
  - Whether or not CPs are dedicated to an LP
  - Weight capping
  - WorkLoad Manager enablement
  - Initial processing weight
  - Initial capping enablement
  - Minimum processing weight

- Maximum processing weight

- Use the Options page in the image profile to change the:
  - Minimum input/output (I/O) priority
  - Maximum input/output (I/O) priority
  - Defined capacity
- Use the Security page in the image profile to change the:
  - Global performance data control
  - Input/output configuration control
  - Cross partition authority
  - Logical partition isolation
  - Basic counter set authorization control
  - Problem state counter set authorization control
  - Crypto activity counter set authorization control
  - Extended counter set authorization control
  - Coprocessor group counter sets authorization control
  - Basic sampling authorization control
- Use the Storage page in the image profile to change the:
  - Central storage definitions
  - Expanded storage definitions
- Use the Time Offset page in the image profile to change the:
  - Logical partition time offset
- Use the Load page in the image or load profile to change the:
  - Automatic load data
- Use the Crypto page in the image profile to update the:
  - Control domain index
  - Usage domain index
  - Cryptographic Candidate List
  - Cryptographic Online List

Changes available at the next Power-On Reset (POR)

The following changes are available at the next power-on reset.

- Use the Options page in the reset profile to change the:
  - Global enablement of input/output (I/O) priority queuing
  - Processor running time interval
  - Enablement of event-driven dispatching
  - Automatic input/output (I/O) interface reset

Chapter 4. Operating logical partitions

Overview

This chapter provides information on operating the hardware system.

Sample tasks and panels explained in this chapter reference tasks and panels available from the Support Element console of a System z10. However, detailed procedures for operator tasks and accurate task and panel references are explained in the *System z10 Support Element Operations Guide*, SC28-6879.

Available operator controls

The following tasks are available when logged on in system programmer mode:

Task	Tasks List
Hardware System Messages	All
Operating System Messages	All
Activate	Daily Tasks
Reset Normal	Daily Tasks
Deactivate	Daily Tasks
Grouping	Daily Tasks
Activity	Daily Tasks
Start All	CPC Recovery
Stop All	CPC Recovery
Reset Normal	CPC Recovery
Reset Clear	CPC Recovery
Load	CPC Recovery
Power-on Reset	CPC Recovery
Load from CD-ROM, DVD, or Server	CPC Recovery
Service Status	Service
View Service History	Service
Checkout Tests	Service
Report a Problem	Service
Transmit Service Data	Service
Dump LPAR Data	Service
Delete LPAR Dump Data	Service
Dump Machine Loader Data	Service
Off-load Virtual Retain Data To HMC-DVD	Service
Global OSA Status	Service
InfiniBand multiport Status and Control	Service
Perform Problem Analysis	Service
Define Clonable Internal Code Levels	Change Management
Change Internal Code	Change Management
System Information	Change Management
Force Channel Internal Code Change	Change Management
Authorize Internal Code Changes	Change Management
Alternate Support Element	Change Management
Query Coupling Facility Reactivations	Change Management
Check Dependencies	Change Management
Query Channel/Crypto Configure On/Off Pending	Change Management
Selective Channel Path Controls	Change Management
Remote Service	CPC Remote Customization
Customer Information	CPC Remote Customization

Task	Tasks List
Customize/Delete Activation Profiles	CPC Operational Customization
Automatic Activation	CPC Operational Customization
Customize Scheduled Operations	CPC Operational Customization
Change Logical Partition Controls	CPC Operational Customization
Change Logical Partition Security	CPC Operational Customization
Storage Information	CPC Operational Customization
System Activity Profiles	CPC Operational Customization
Enable/Disable Dynamic Channel Subsystem	CPC Operational Customization
View LPAR Cryptographic Controls	CPC Operational Customization
Export/Import Profile Data	CPC Operational Customization
Enable I/O Priority Queuing	CPC Operational Customization
Change Logical Partition I/O Priority Queuing	CPC Operational Customization
Change LPAR Cryptographic Controls	CPC Operational Customization
Change LPAR Group Controls	CPC Operational Customization
Logical Processor Add	CPC Operational Customization
Perform Model Conversion	CPC Configuration
Transmit Vital Product Data	CPC Configuration
View Frame Layout	CPC Configuration
System (Sysplex) Time	CPC Configuration
Input/Output (I/O) Configuration	CPC Configuration
View Hardware Configuration	CPC Configuration
Channel PCHID Assignment	CPC Configuration
Cleanup Discontinuance	CPC Configuration
Cryptographic Configuration	CPC Configuration
Cryptographic Management	CPC Configuration
Display Adapter ID	CPC Configuration
Display NPIV Configuration	CPC Configuration
Prepare System for Discontinuance	CPC Configuration
Send Processor Change Notification	CPC Configuration
Start	CP Toolbox
Stop	CP Toolbox
Display or Alter	CP Toolbox
PSW Restart	CP Toolbox
Stop on CP Address Match	CP Toolbox
Interrupt	CP Toolbox
Store Status	CP Toolbox
Configure On/Off	CHPID Operations
Release	CHPID Operations
Show LED	CHPID Operations
Channel Problem Determination	CHPID Operations
FCP NPIV On/Off	CHPID Operations
Configure On/Off	Crypto Service Operations
Service On/Off	Crypto Service Operations
Advanced Facilities	Crypto Service Operations
Channel Problem Determination	Crypto Service Operations
Configure On/Off	Channel Operations
Release	Channel Operations
Service On/Off	Channel Operations
Show LED	Channel Operations
Advanced Facilities	Channel Operations
Reassign Channel Path	Channel Operations
Channel Problem Determination	Channel Operations

Operator controls not available

The following tasks are not available when logged on in system programmer mode:

- Enable TOD
- Change Operation Rate
- Stop on I/O Address Match
- Stop on I/O Event
- Stop on PSW Event
- Trace

Operator tasks

Editing activation profiles

You can edit reset, image, and load profiles for configurations using the Customize/Delete Activation Profiles task available from the CPC Operational Customization tasks list.

Reset profiles

Use the reset profile to:
- Select an IOCDS
- Optionally specify an LP activation sequence
- Enable I/O Priority Queuing.

You can select an IOCDS using the General page of the reset profile. To specify an optional LP activation sequence, use the Partitions page of the reset profile.

Image profiles

Use the image profile to:
- Define LP characteristics
- Optionally specify automatic load settings.

To define LP characteristics, use the General, Processor, Security, Storage, Options, Crypto, and Time Offset pages of the image profile (see “Defining logical partitions” on page 146). To specify optional automatic load settings, use the Load page of the image profile (see “Load information” on page 166).

Load profiles

If you are not using the image profile to specify load options for an LP, use the load profile.

Activating a CPC

To activate a CPC, locate the CPC icon and open the Activate task available from the Daily Tasks task list. This task will activate the hardware system and, if LP activation sequence is enabled for LPs, will activate those LPs in the order specified in the reset profile for the CPC. You can also automatically load the LP’s operating system as specified in the image profile for the LP.

Activating an LP

To activate an LP, locate the LP icon, and open the Activate task available from the Daily Tasks list. This task will activate the LP and, if automatic load is specified for an LP, will automatically load the LP’s operating system as specified in the image profile for the LP.

Performing a load on an LP or activating a load profile

Perform a load on an LP or activate a load profile for an LP by locating the LP icon for a previously activated LP and opening the Customize/Delete Activation Profiles task available from the CPC Operational Tasks list.

Select or, if necessary, customize or create a load profile for the LP. Assign the load profile to the LP’s activation profile and exit the Customize/Delete Activation Profiles task, saving your changes. Next, locate the LP icon and open the Activate task available from the Daily Tasks list.

Also, in recovery situations, you can locate the LP icon and open the Load task available from the CPC Recovery tasks list.

Deactivating an LP

To deactivate an LP, locate the LP icon and open the Deactivate task available from the Daily Tasks list. This task will deactivate the LP and any operating system running in the LP.

Locking and unlocking an LP

Lock an LP by double-clicking on the CPC image icon representing the LP to open its Detail page. Set the Lockout Disruptive Tasks radio button to Yes and select the Apply button.

You can use this same procedure to unlock an LP by setting the Lockout Disruptive Tasks radio button to No and applying the setting.

Locking an LP can prevent accidentally performing disruptive tasks on an LP. You can lock the following system programmer mode tasks:

- **Daily tasks**
  - Activate
  - Reset Normal
  - Deactivate
- **CPC Recovery tasks**
  - Start all
  - Stop all
  - Reset Normal
  - Reset Clear
  - Load
  - Power-on Reset
  - Load from CD-ROM, DVD, or Server
- **Service tasks**
  - Checkout Tests
  - Dump Machine Loader Data
- **Change Management tasks**
  - Define Clonable Internal Code Levels
  - Query Coupling Facility Reactivations
- **CPC Operational Customization tasks**
  - Change Logical Partition Controls
  - Change LPAR Group Controls
  - Change Logical Partition Security
- **CPC Configuration**
  - System (Sysplex) Time
- **CP Toolbox tasks**
  - Start
  - Stop
  - Display or Alter
  - PSW Restart
  - Interrupt
  - Store Status
- **CHPID Operations tasks**
  - Configure On/Off
  - Release
  - Channel Problem Determination

- **Crypto Service Operations tasks**
  - Configure On/Off
  - Service On/Off
  - Advanced Facilities
  - Channel Problem Determination
- **Channel Operations tasks**
  - Configure On/Off
  - Release
  - Service On/Off
  - Advanced Facilities
  - Reassign Channel Path
  - Channel Problem Determination

Deactivating a CPC

To deactivate a CPC, locate the CPC icon and open the Deactivate task available from the Daily Tasks list. This task will deactivate the CPC and any activated LPs and their associated operating systems.

Chapter 5. Monitoring the activities of logical partitions

Overview

This chapter describes the panels and tasks that can be used to monitor LP activity. It also provides LP performance information and provides guidelines and suggestions for planning a recovery strategy for operation.

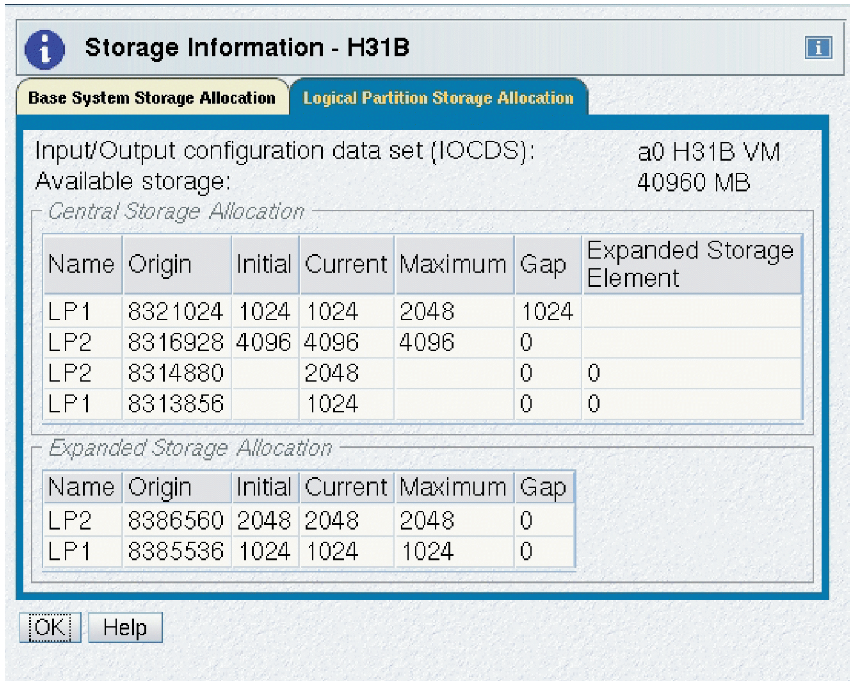
Monitoring logical partition activity

In addition to viewing LP information located in the General, Processor, Security, Storage, Load, and Channels pages of an LP's reset, image, and load profiles, you can use the following tasks to further monitor LP activity:
- Current storage information
- Current channel information
- Current System activity profile information

Reviewing current storage information

Use the Storage Information task available from the CPC Operational Customization tasks list to open the Storage Information task to display LP storage information for LPs currently activated on the CPC.

For this example, assume the amount of customer storage is 49152 MB (48 GB). The amount of addressable central storage is 8388608 MB (8192 GB). The amount of addressable central storage used by hardware system area (HSA) is 65536 MB, leaving 8323072 MB of addressable storage for allocation to LPs.



Central Storage Allocation

Name	Origin	Initial	Current	Maximum	Gap	Expanded Storage Element
LP1	8321024	1024	1024	2048	1024	
LP2	8316928	4096	4096	4096	0	
LP2	8314880		2048		0	0
LP1	8313856		1024		0	0

Expanded Storage Allocation

Name	Origin	Initial	Current	Maximum	Gap
LP2	8386560	2048	2048	2048	0
LP1	8385536	1024	1024	1024	0

Figure 49. Storage information task. This example shows two partitions active. LP2 has 4096 MB of initial central storage and 2048 MB of initial expanded storage. LP1 has 1024 MB of initial central storage, 1024 MB of reserved central storage and 1024 MB of initial expanded storage. LP1 was activated first, without any expanded storage. Then, LP2 was activated and LP1 was activated again with expanded storage.

Note: The central storage addressability required for LP1's expanded storage is not necessarily contiguous to the CS addressability for LP1's initial or reserved central storage.

Reviewing and changing current channel status

Use the tasks available on the CHPID Operations task list to display and modify channel status information in an LP's CHPID work area.

Reviewing and changing current logical partition controls

Use the Change Logical Partition Controls task available from the CPC Operational Customization tasks list to display and modify LP controls for an LP.

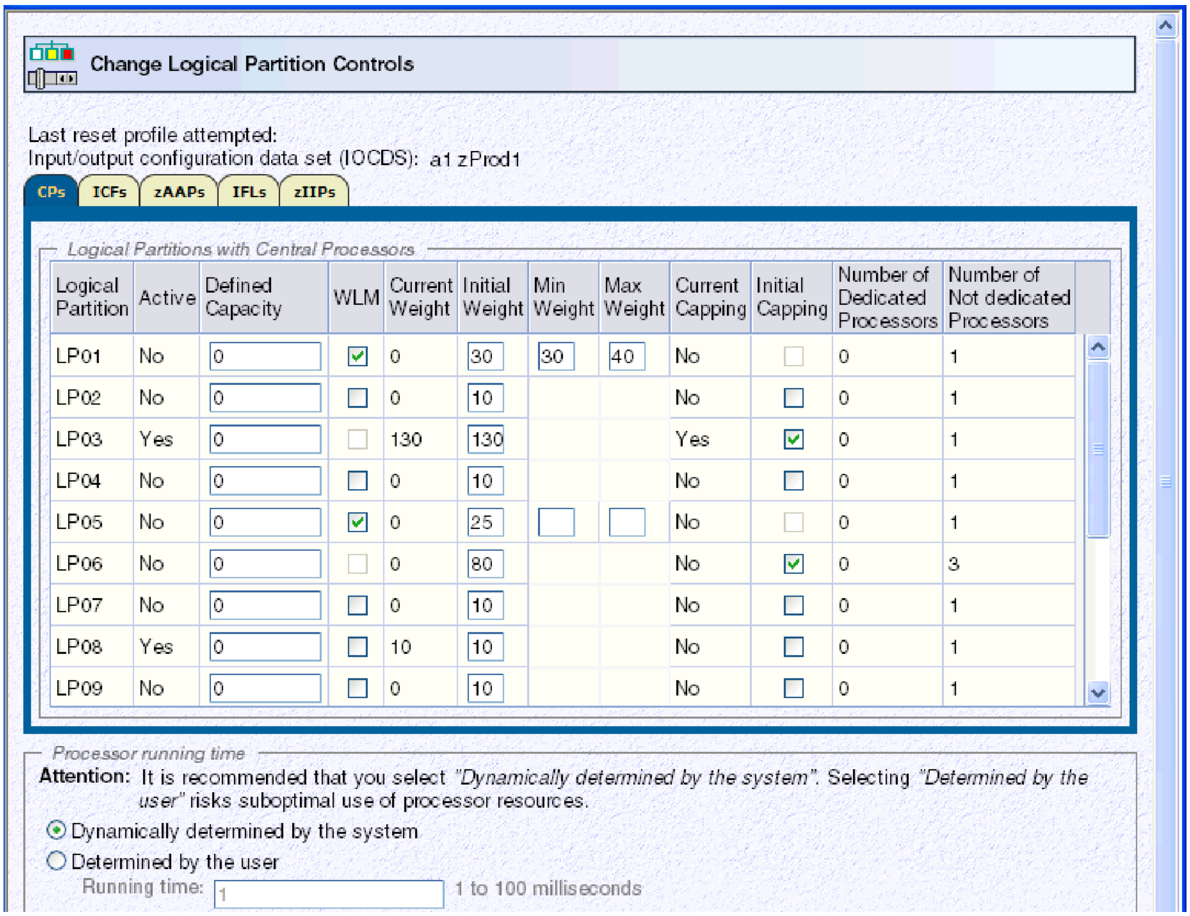


Figure 50. Change logical partition controls page. The Current Weight for an active shared LP will always show nonzero. For non-WLM managed logical partitions, the Current Weight will always be equal to the Initial Processing Weight. The Current Weight for WLM managed logical partitions will be whatever value WLM has currently assigned to the LP. Current Capping will always be indicated for an active LP that has Initial Capping. Current capping will also be indicated for an LP which has been dynamically soft-capped by the Workload Manager (WLM).

Reviewing and adding logical processors

The Logical Processor Add task allows you to select logical processor definitions to be changed dynamically on the system, in the image profile, or both. Dynamic changes will take effect without performing a reactivation of the logical partition. This tasks allows you to:

- Increase the initial and/or reserved values for installed logical processor type(s)
- Add a reserved value and set weight and capping indicators for logical processor type(s) that have not yet been installed and have no reserved CPs defined
- Increase the reserved value for logical processor type(s) that have not been installed and already have reserved CP(s) defined

The partition status (active/inactive) is indicated in the panel title, along with the logical partition name. If the logical partition is active, the current settings are displayed. If the logical partition is inactive, the settings contained in the image profile will be displayed.

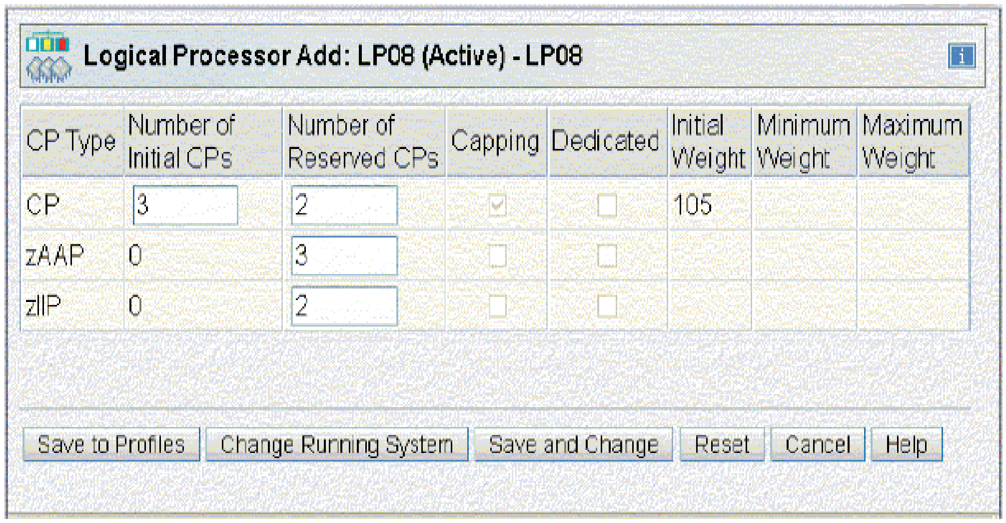


Figure 51. Logical processor add. This is an active, ESA mode partition. There are currently only CPs defined to the partition, so only reserved can be increased for zAAP and zIIP.

Reviewing and changing current logical partition group controls

Change LPAR Group Controls allows you to define LPAR group capacity limits, allowing you to specify one or more groups of LPARs on a server, each with its own capacity limit. This is designed to allow z/OS to manage the groups in such a way that the sum of the LPARs' CPU utilization within a group will not exceed the group's defined capacity. Each Logical partition in a group can still optionally continue to define an individual logical partition capacity limit.

LPAR group capacity limit requires that all logical partitions to be managed in the group be running z/OS or z/OS.e V1.8 or later. LPAR group capacity limits may help provision a portion of a System z10 server to a group of logical partitions allowing the CPU resources to float more readily between those logical partitions, resulting in more productive use of ″white space″ and higher server utilization.

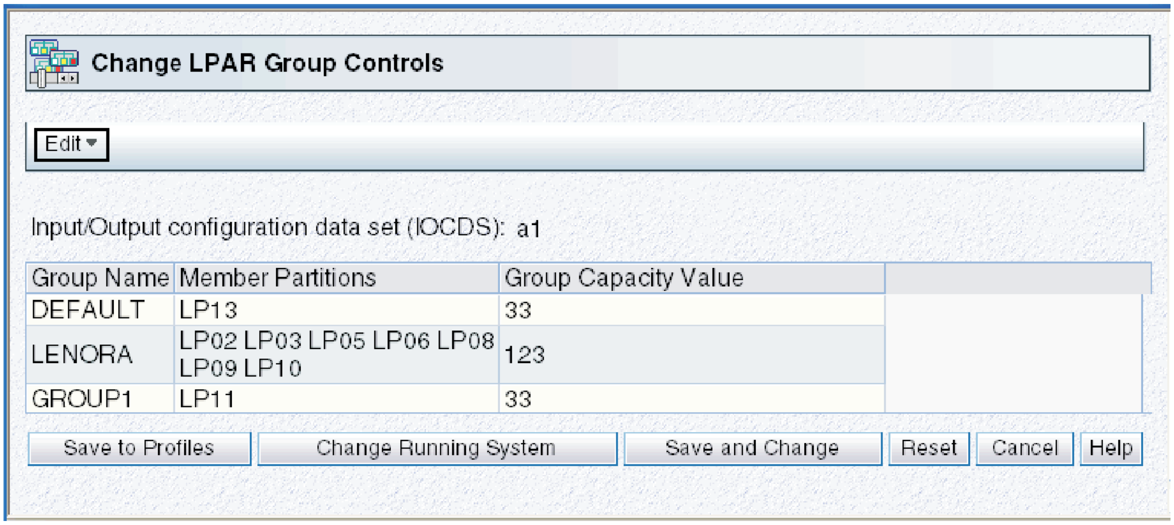


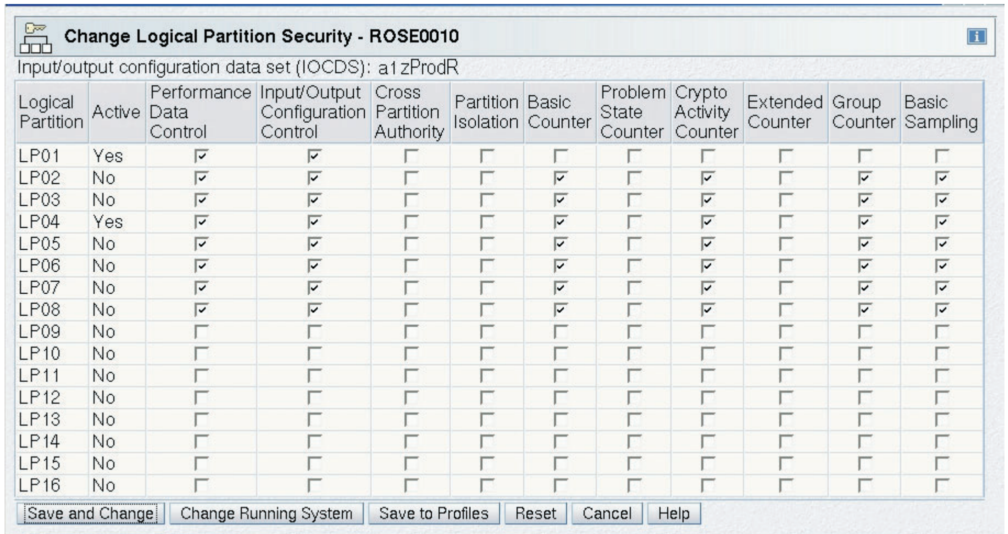
Figure 52. Change LPAR group controls

For information about creating a group, see “Creating a logical partition group profile” on page 172. For detailed information about grouping objects for activation, see the *System z10 Support Element Operations Guide*.

For information about how workload management and workload license charges relate to the Group Capacity setting, see *z/OS MVS Planning: Workload Management*, SA22-7602.

Reviewing and changing current logical partition security

Use the Change Logical Partition Security task available from the CPC Operational Customization tasks list to display and modify LP security controls for an LP.



Logical Partition	Active	Performance Data Control	Input/Output Configuration Control	Cross Partition Authority	Partition Isolation	Basic Counter	Problem State Counter	Crypto Activity Counter	Extended Counter	Group Counter	Basic Sampling
LP01	Yes	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐
LP02	No	☑	☑	☐	☐	☑	☐	☑	☐	☑	☑
LP03	No	☑	☑	☐	☐	☑	☐	☑	☐	☑	☑
LP04	Yes	☑	☑	☐	☐	☑	☐	☑	☐	☑	☑
LP05	No	☑	☑	☐	☐	☑	☐	☑	☐	☑	☑
LP06	No	☑	☑	☐	☐	☑	☐	☑	☐	☑	☑
LP07	No	☑	☑	☐	☐	☑	☐	☑	☐	☑	☑
LP08	No	☑	☑	☐	☐	☑	☐	☑	☐	☑	☑
LP09	No	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
LP10	No	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
LP11	No	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
LP12	No	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
LP13	No	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
LP14	No	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
LP15	No	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
LP16	No	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Save and Change | Change Running System | Save to Profiles | Reset | Cancel | Help

Figure 53. Change logical partition security page

Reviewing and changing current logical partition cryptographic controls

View LPAR cryptographic controls

Use the View LPAR Cryptographic Controls task available from the CPC Operational Customization tasks list to display CEX2C and CEX2A characteristics for an LP. The Summary tab displays the current crypto configuration settings for all active and inactive partitions in the CPC. (The inactive partition information displayed is a result of the settings selected in the Image Activation profile.) The tab with the name of the partition displays the current crypto configuration for that active partition.

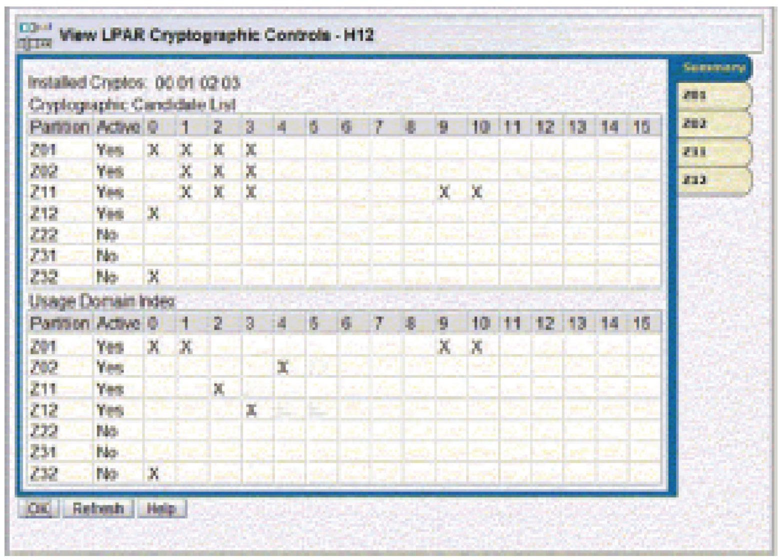


Figure 54. View LPAR cryptographic controls window (summary tab)

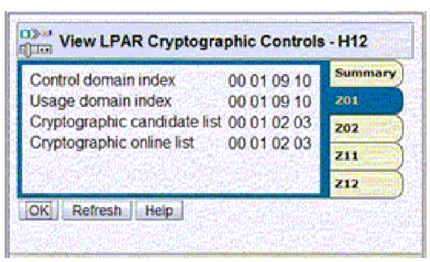


Figure 55. View LPAR cryptographic controls (showing tab containing crypto configuration information for an active partition)

Changing LPAR cryptographic controls

Use the Change LPAR Cryptographic Controls task to make changes to the crypto configuration of an active partition without affecting the operating status of the partition. This allows you to update your crypto configuration without reactivating the logical partition. You can add cryptos to a partition, delete cryptos from a partition, and/or move a crypto from one partition to another using the following task:

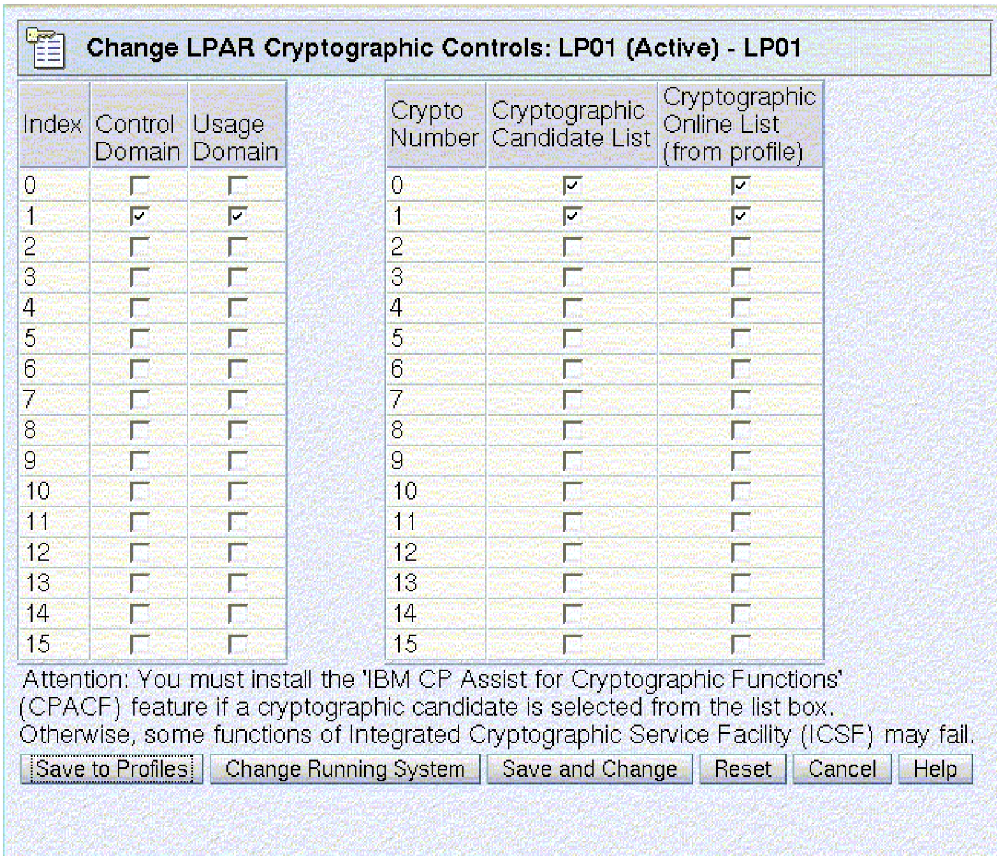


Figure 56. Change LPAR cryptographic controls

There are requirements for adding, removing and moving a crypto:

- The crypto that is assigned to this partition must be configured offline before the removal of the crypto from the partition can be done. If the crypto was operating as a coprocessor, and a removal of a crypto is being done, the user is given the opportunity to remove the cryptographic keys from the partition associated with the selected usage domain, using the usage domain zeroize function.
- If the crypto is not online to the partition, but the associated PCHID is online/operating, the usage domain zeroize action can immediately be done. If the crypto assigned to the partition and the PCHID are both offline, the usage domain zeroize action will be pending until the next time this crypto is brought online.
- To move a crypto from one partition to another requires you to perform two steps. First, remove the crypto from the first partition and then add it to the second partition.
- After a crypto is added to a partition, the crypto needs to be brought online using the config On/Off task found in Crypto Operations.

Note: Changes made using the Change LPAR Cryptographic Controls task can be made to both active and inactive partitions. When performed on an inactive partition, the changes are made to the image activation profile, since the partition is not active.

The cryptographic domain index table displays the current settings of the usage domain indexes and control domain indexes which can be modified in the logical partition and/or the image profile.

Control Domain
: A logical partition's control domains are those cryptographic domains for which remote secure administration functions can be established and administered from this logical partition. This logical partition's control domains must include its usage domains. For each index selected in the usage domain index list, you must select the same index in the control domain index list.

Usage Domain
: A logical partition's usage domains are domains in the cryptos that can be used for cryptographic functions. The usage domains cannot be removed if they are in use by the partition. The usage domains you select for this logical partition must also be selected in the control domain index.

The cryptographic list table displays the current settings of the cryptographic candidate list and cryptographic online list settings which can be modified in the logical partition and/or the image profile:

Cryptographic Candidate List
: The candidate list identifies which cryptos are assigned to the active logical partition. Cryptos cannot be removed if they are online to this partition.

Cryptographic Online List (from profile)
: The online list identifies which cryptos will be brought online at the next activation. Changes to the online list do not affect the running system.

To commit your changes, use one of the following:

Save to Profiles
: Select this if you want new settings to take effect whenever the logical partition is activated with the modified profile. This changes the cryptographic settings in the logical partition's image profile. The settings take effect whenever the logical partition is activated with its image profile.

Change Running System
: Select this if you want the new settings to take effect in the active logical partition immediately. This changes the cryptographic settings in the logical partition without reactivating the partition. The new settings remain in effect for the logical partition until you either dynamically change the settings again or reactivate the partition.

Note: This button can be used for an active logical partition only. For an inactive partition, this button is disabled.

Save and Change
: Select this if you want the new settings to take effect immediately and whenever the logical partition is activated with the modified profile. Save and Change:

- Saves a logical partition's cryptographic control settings in its image profile. The settings take effect whenever the logical partition is activated with its image profile.
- Changes the cryptographic settings in the logical partition without reactivating the partition. The new settings remain in effect for the logical partition until you either dynamically change the settings again or reactivate the partition.

Note: This button can be used for an active logical partition only. For an inactive partition, this button is disabled.

Reset Select this to revert the settings back to their original values.

When a crypto with it's associated usage domains are removed from a partition, this partition will no longer have access to the cryptographic keys. But if this crypto is then assigned to a different partition utilizing the same usage domains as before, then this new partition will have access, possibly unintentional access, to the cryptographic keys. Therefore, when a crypto is removed from an active partition, the Usage Domain Zeroize panel is displayed, providing the opportunity to clear the cryptographic keys associated with the given usage domain(s).

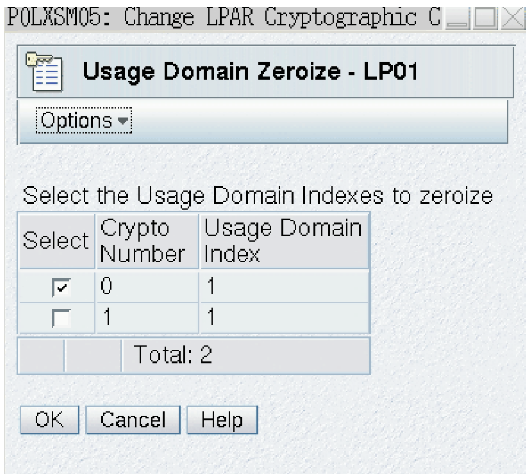


Figure 57. Usage domain zeroize

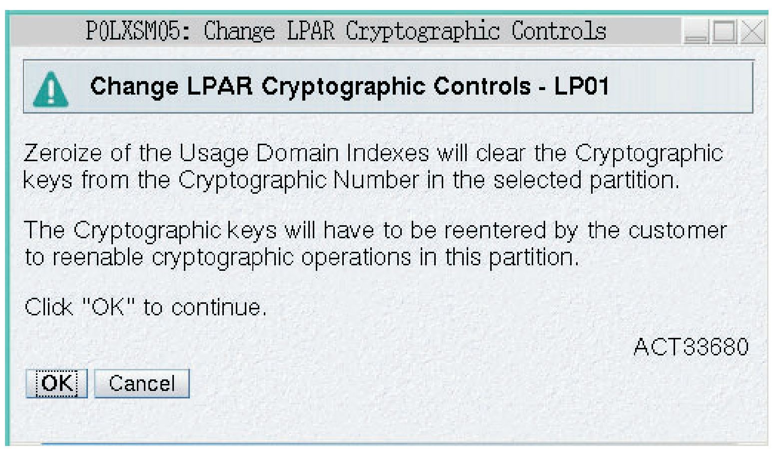


Figure 58. Message received from change LPAR cryptographic controls

Note: If the crypto device you remove is the last remaining one, you will receive a cautionary note that all cryptographic candidates have been removed from the partition, which will remove the partitions access to all cryptos.

Cryptographic configuration - usage domain zeroize

The opportunity to zeroize the usage domains associated with a crypto is available when removing a crypto using the Change LPAR Cryptographic Controls task. The usage domain zeroize can also be performed using the Cryptographic Configuration task.

The Cryptographic Configuration window can be used to configure and monitor the cryptos that are installed on your system. Use this window to perform various tasks, including:

- Checking the status and details of your cryptos.
- Testing the Random Number (RN) generator of the crypto.
- Manually zeroizing cryptos and erasing configuration data from the Support Element.
- Importing and activating the UDX configuration
- Indicating whether to permit TKE commands for the selected crypto.
- Indicating the crypto type configuration for the Crypto Express2 feature.

The removal of a crypto from a partition exposes the cryptographic keys within the associated usage domains, if the crypto and usage domains are then reassigned to a new partition. Such an exposure can occur when:

- removing the crypto from the candidate list in the Activation profile, then reassigning the crypto to another active partition.
- moving a crypto using the Change LPAR Cryptographic Controls task, as discussed earlier in this chapter.

The Usage Domain Zeroize function as part of the Cryptographic Configuration task offers the opportunity to clear the cryptographic keys when desired, not just when the cryptographic settings are modified using the Change LPAR Cryptographic Controls task.

It is recommended that the usage domain zeroize be performed with the crypto offline, but it is not required. When performing the usage domain zeroize with the crypto offline, the zeroize of the usage domain index(es) selected is deferred until the selected crypto is configured online, using the Config On/Off task, found under Crypto Operations.

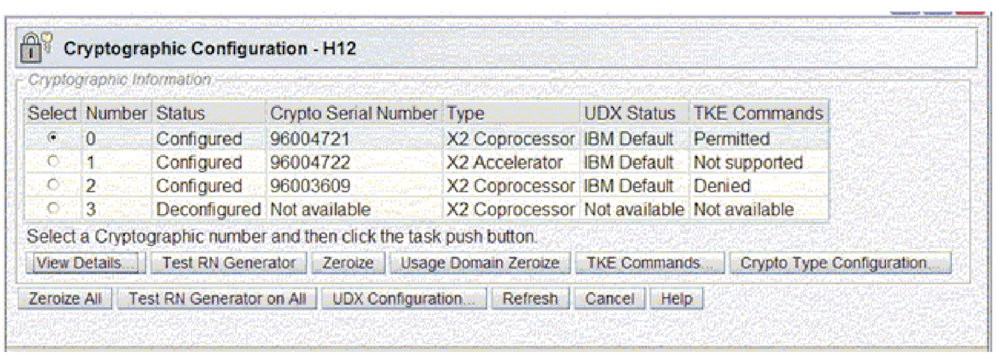


Figure 59. Cryptographic configuration window

On the Cryptographic Configuration window, select the crypto, and click **Usage Domain Zeroize**. The Usage Domain Zeroize window displays:

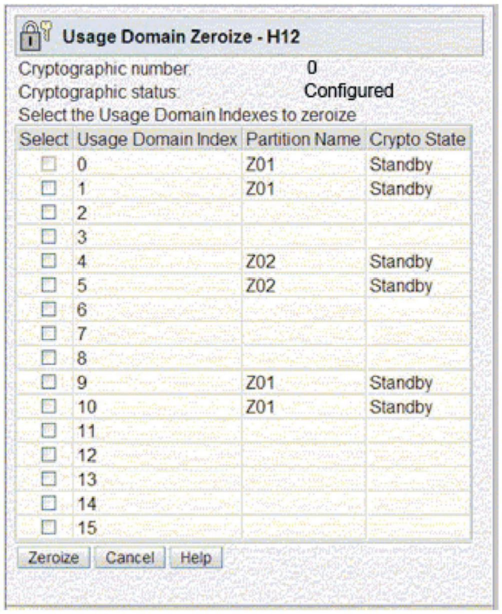


Figure 60. Usage domain zeroize window

On the Usage Domain Zeroize window, select the usage domain index(es) that have the cryptographic keys you wish to zeroize, and then click **Zeroize**. The zeroize of the Usage Domain Index(es) is deferred until the selected Cryptographic number is configured online (Configure On). When the selected cryptographic number is configured online, the selected Usage Domain indexes will be cleared of cryptographic keys.

Reviewing current system activity profile information

Use the System activity profiles task available from the Daily Tasks list to open a System activity information window. Locate the System Activity profile, which displays the system activity information you want to view.

Reviewing and changing logical partition I/O priority values

Use the Change Logical Partition I/O Priority Queuing task available from the CPC Operational Customization tasks list to display and modify I/O priority queuing values for one or more LPs.

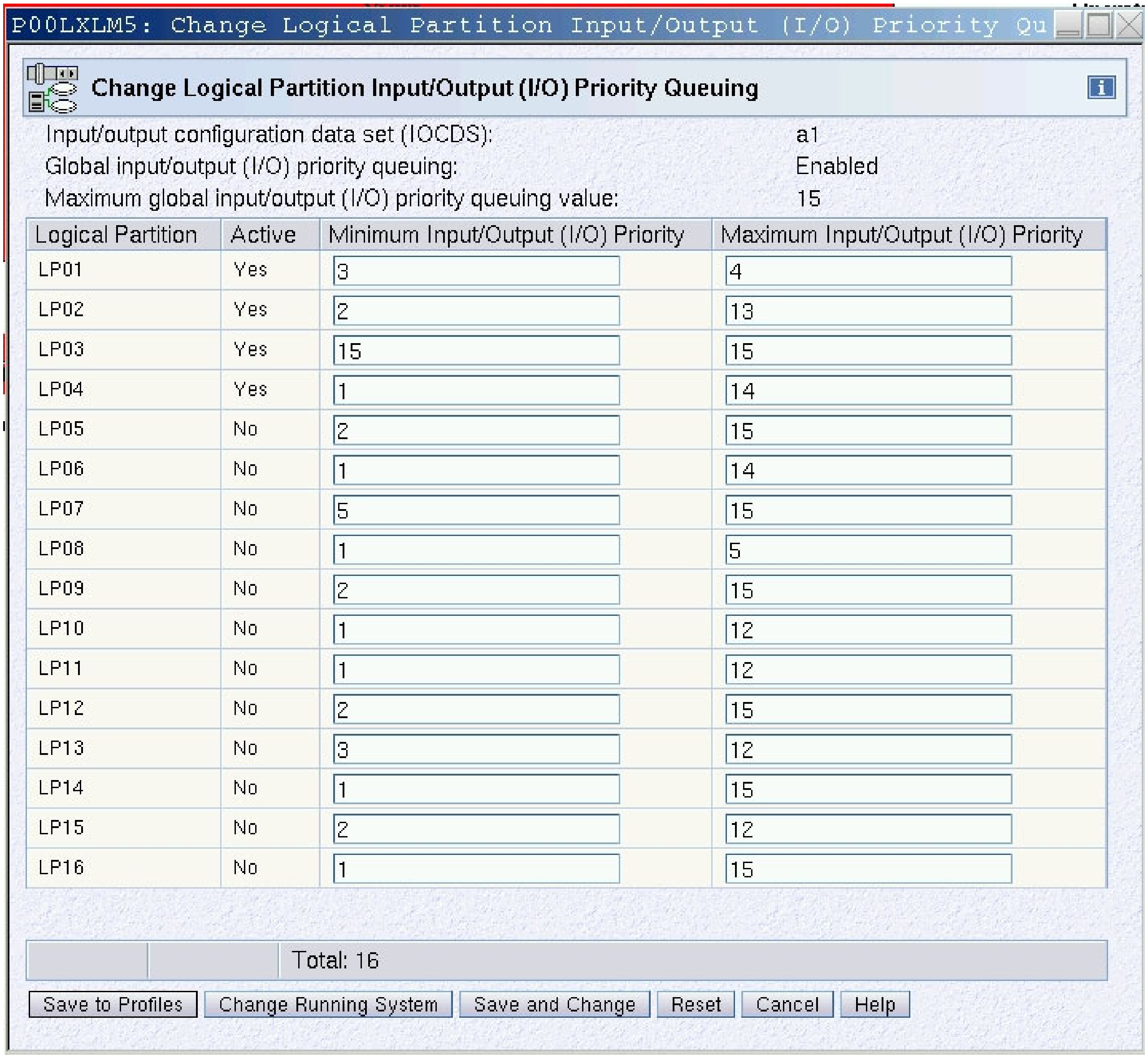


Figure 61. Change Logical Partition I/O priority queuing window

Logical partition performance

Contact your IBM service representative for assistance in planning configuration capacity requirements.

The performance of LPs depends on:
- The operating systems and their workloads
- The configuration of the LPs
- The configuration of the CPC
- The performance tuning parameters

You can contact an service representative who has access to a proprietary IBM performance planning tool (LPARCE from CPSTOOLS at WSCVM) to assist you in this task.

RMF LPAR management time reporting

RMF processor utilization reporting includes LPAR Management Time on the Partition Data Report. RMF provides information about all shared logical CPs that remain active for the duration of the reporting interval. RMF can also be run on a single LP if additional information is required.

There are two types of LPAR management time reporting: time spent managing the LP, and time spent managing the physical configuration. With LPAR Management Time reporting, the time used to manage an LP can be separated from the time used by the workload in an LP.

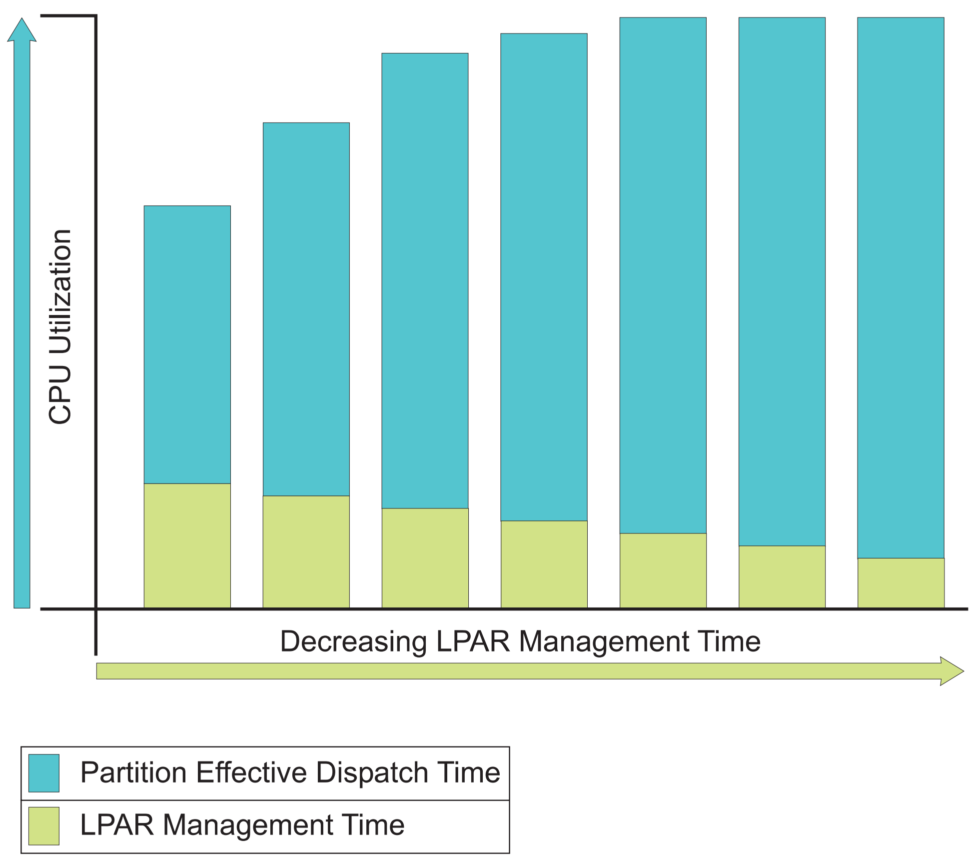


Figure 62. ETR increasing with CPU utilization

Figure 62 on page 203 is an example of how information from the enhanced RMF LPAR Management Time reports can be used. This example shows the LPAR Management Time and the partition effective dispatch time for each LP. As CPU utilization increases, LPAR management time decreases, and the external throughput rate (ETR) increases.

Using the RMF report, CPU-utilization calculations can be based on an LP's effective dispatch time. The effective dispatch time can be determined by excluding LPAR Management Time from the time that a physical CP is assigned to a logical CP.

Note: For more information about RMF support, the RMF Partition Data Report, and LPAR Management Time see the *Resource Measurement Facility User's Guide*.

Dedicated and shared central processors

Generally, LPs with dedicated CPs require fewer processing resources. The internal throughput rate (ITR) of LPs with dedicated CPs is higher than that of identically defined LPs with shared CPs. Also, IBM recommends that dedicated processors (ICFs or CPs) be used in a coupling facility partition that is used in a production configuration.

Generally, the capability to recognize CP resources that are not used and to balance workloads can result in an improved ETR for LPs with shared CPs. In particular, for workloads that exhibit fluctuations in processing demands, the consolidation of several systems as LPs with shared CPs on a CPC can improve responsiveness and increase ETR.

CPENABLE

The z/OS CPENABLE parameter can be used to provide selective enablement for I/O interrupts. On System z10 CPCs, the best ITR is achieved when the fewest CPs are enabled for I/O interrupts. Selective enablement for I/O and the CPENABLE parameter are described in the *z/OS MVS Initialization and Tuning Reference*, SA22-7592.

For logical partitions using dedicated processors, IBM recommends a CPENABLE=(10,30) setting to minimize the number of CPs handling I/O interrupts in an LP.

A CPENABLE=(0,0) setting, enabling all CPs to handle I/O interrupts, can cause performance degradation for logical partitions with dedicated CPs.

For logical partitions sharing CP resources, IBM recommends a CPENABLE=(10,30) setting. There is a negligible ITR impact between a CPENABLE=(0,0) setting versus a CPENABLE=(10,30) setting for logical partitions sharing CP resources.

Start Interpretive Execution (SIE) performance

PR/SM implementation uses CPC hardware mechanisms that are also used to implement the SIE facility when operating in ESA/390 mode. Therefore, if SIE is executed in an LP, SIE performance is reduced relative to operation in ESA/390 mode. The performance reduction depends on the frequency of SIE invocation and should be evaluated for each application.

Recovery strategy

Recovery planning requires that the appropriate planners and technical support personnel understand the recovery strategy.

In planning for recovery, consider the following guidelines:

- Recovery is considered successful if an LP is able to perform useful work and critical application programs remain operational (even if one or more LPs are disabled) after a failure occurs. Recoverability depends on the extent and location of a failure and the ability of the operating system to handle the failure.
- Develop a recovery strategy for the specific installation that addresses the specific hardware and applications of that installation. For example, if a failure occurs that might disrupt multiple LPs or a critical LP, the operator should be able to determine what must remain active and what can be deactivated, and to perform the appropriate recovery procedures.
- The operator should follow established local procedures for reporting problems and for performing recovery procedures. It is recommended that recovery procedures be ranked from least to most disruptive. The operator should know what procedures to follow if any or all LPs do not respond to the recovery actions directed to it.
- Assign channel paths to LPs as described in the guidelines under "Guidelines for setting up the I/O configuration" on page 29.
- Define resources to LPs so that any hardware failure has a minimal impact on any LP that must remain active.

  For example, the failure of a physical CP causes the temporary loss of the logical CP that was dispatched on the physical CP. The LP owning that logical CP may continue running if it was running on an LP with at least two CPs and if the operating system can recover from a CP failure.

Operation considerations

If an individual LP is affected, the following recovery actions (ranked from least to most disruptive) should be considered when planning recovery procedures.

- If an affected LP continues to operate with a problem, allow it to do so.
- If the operating system in an LP remains active but processing is interrupted, consider the applicability of a restart or IPL.
- Perform a stand-alone dump and IPL the operating system.
- Perform an orderly shutdown of the operating system in an affected LP. If the LP is not critical, allow the other LPs to continue.

If all LPs are affected, or if a critical LP is affected and did not respond to the recovery actions directed only to it, the following recovery actions (also ranked from least to most disruptive) should be considered when planning recovery procedures.

- Perform an orderly shutdown of all the operating systems. Activate the LPs and IPL the operating systems.
- Perform an orderly shutdown of all the operating systems. Perform the most appropriate recovery action (for example, in response to a hardware failure). Perform a power-on reset.
- If a power-on reset fails to initialize the LPs, perform a power-on reset to attempt a recovery. IPL the most critical operating system.

Application preservation

The application preservation facility enhances system availability and provides additional protection from CP failures. This support is available on System z10 CPC models with two or more central processors (CPs). Using application preservation, the system moves an application in process from a failing CP to another operating CP. Both the CP failure and the move are transparent to the application.

There are no software corequisites when running with shared CPs. For LPs using shared CPs, even 1-way LPs can survive a CP failure without experiencing a failure to the application or the LP, providing the 1-way LP is being run on a model with more than one physical CP.

Transparent sparing

Transparent sparing takes LP recovery one step further by combining the benefits of application preservation and concurrent CP sparing to allow for the transparent recovery of an LP and its applications (including CF LPs). Transparent sparing uses hardware to handle the recovery, requires no software support or operator intervention, and is effective for both shared and dedicated LP environments.

Transparent sparing configures a spare PU (processor unit) to replace a failed CP, ICF, IFL, zAAP, zIIP or SAP. Each of the z10 EC models has 2 spare PUs. There are no dedicated spare PUs on the z10 BC.

Appendix A. User interface (UI) styles

User interface (UI) styles

The Hardware Management Console and Support Element allow you to choose the interface style in which you prefer to work:

- Tree style user interface
- Classic style user interface (an older interface with object-oriented design).

The tree style user interface is the default for Operator, Advanced Operator, Access Administrator, and System Programmer user roles. The classic user interface is the default for the Service Representative user role.

Tree style user interface

The tree style user interface is the default for Operator, Advanced Operator, Access Administrator, and System Programmer user roles, but not for the Service Representative user role. When you first log on, the Welcome pane is displayed. Figure 63 shows the Welcome pane on the Support Element.

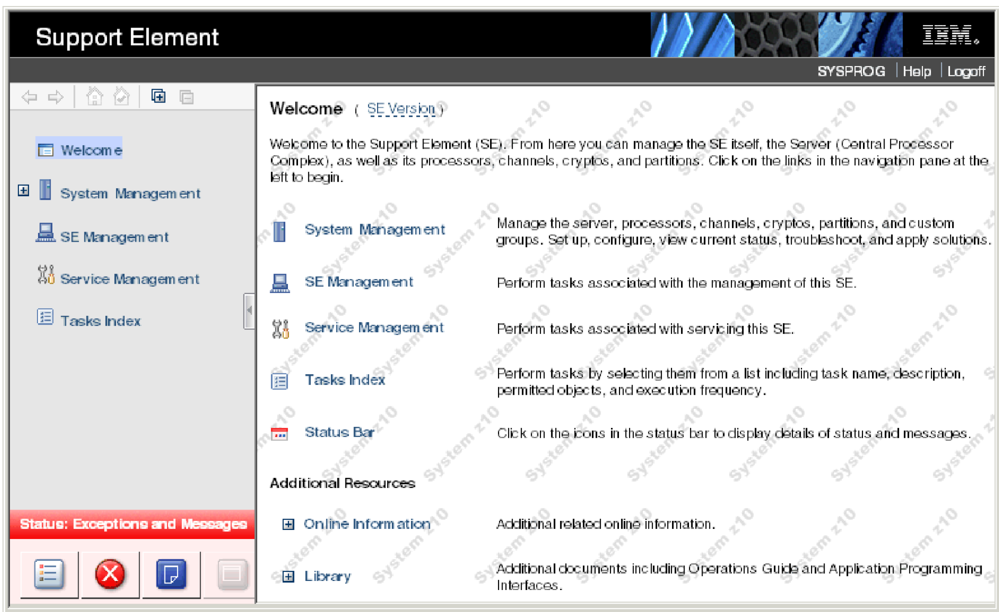


Figure 63. Support Element - tree style user interface - Welcome pane

The tree style user interface is comprised of several major components as shown in Figure 63:

Banner
Is optionally displayed across the top of the workplace and identifies the product and logo.

Taskbar
Is below the banner. This displays:

- The names of any tasks that are running (Task names are displayed on the left; no tasks are running in the example.)
- The user role (`sysprog` in the example)
- A link to online **Help** information

- A link to the **Logoff** task.

Navigation pane
Is in the left portion of the window. This contains the primary navigation links for managing your system resources and the console. The items are referred to as nodes.

Work pane
Is in the right portion of the window. This displays information based on the current selection from the navigation pane. For example, when Welcome is selected in the navigation pane, the Welcome content is displayed in the work pane, as shown in the example.

Status bar
Is in the bottom left portion of the window. This provides visual cues of current overall system status. It also contains a Status Overview icon which may be selected to display more detailed status information in the work pane.

Tree style navigation provides hierarchical views of system resources and tasks using drill-down and launch-in-context techniques to enable direct access to hardware resources and task management capabilities. Figure 64 shows this.

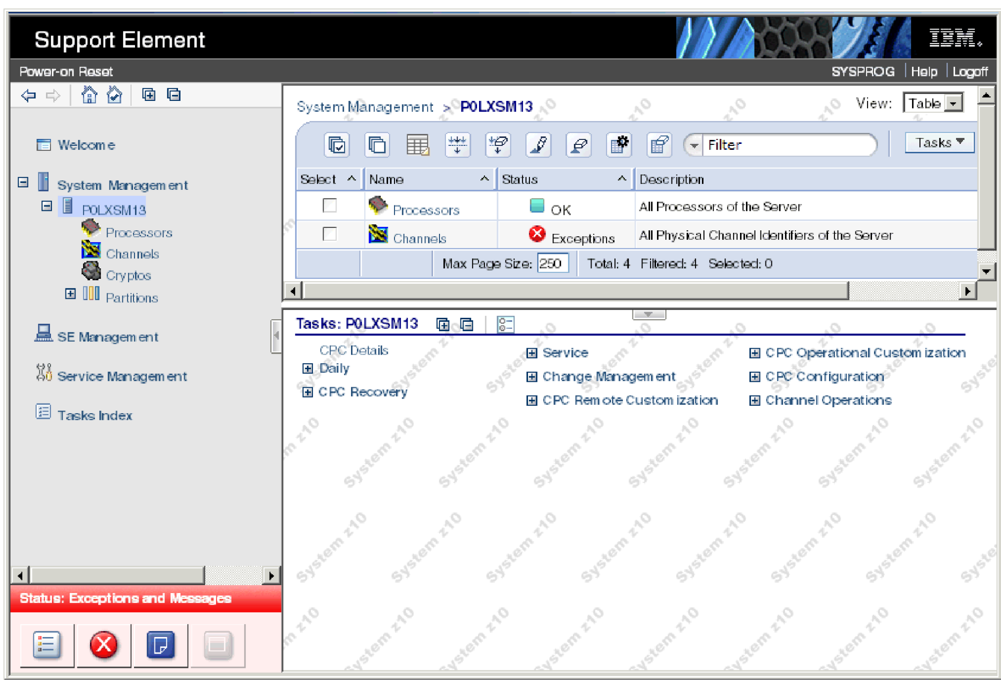


Figure 64. Server selected and task categories displayed

The tree style user interface uses common terminology where possible. For example, instead of referring to a *CPC*, a more general term of *server* is used for this interface. Similarly, in the tree style *partitions* are equivalent to *images* in the classic style.

For panes other than the Welcome pane, the contents of the work pane on the right portion of the window reflect your selections in the navigation pane on the left. The top portion of the work pane displays a table of objects based on your selection. The bottom portion of the work pane is called the tasks pad. Figure 64 shows this.

Tasks pad
: Is in the bottom portion of the work pane after you select an object in the navigation pane, such as server, partition, channel, or crypto. The tasks pad contains a list of available task categories or tasks for the selected object.

Classic style user interface

The classic style user interface (classic interface) is the original user interface. It has an object-oriented design. Figure 65 shows the classic style user interface for the Support Element.

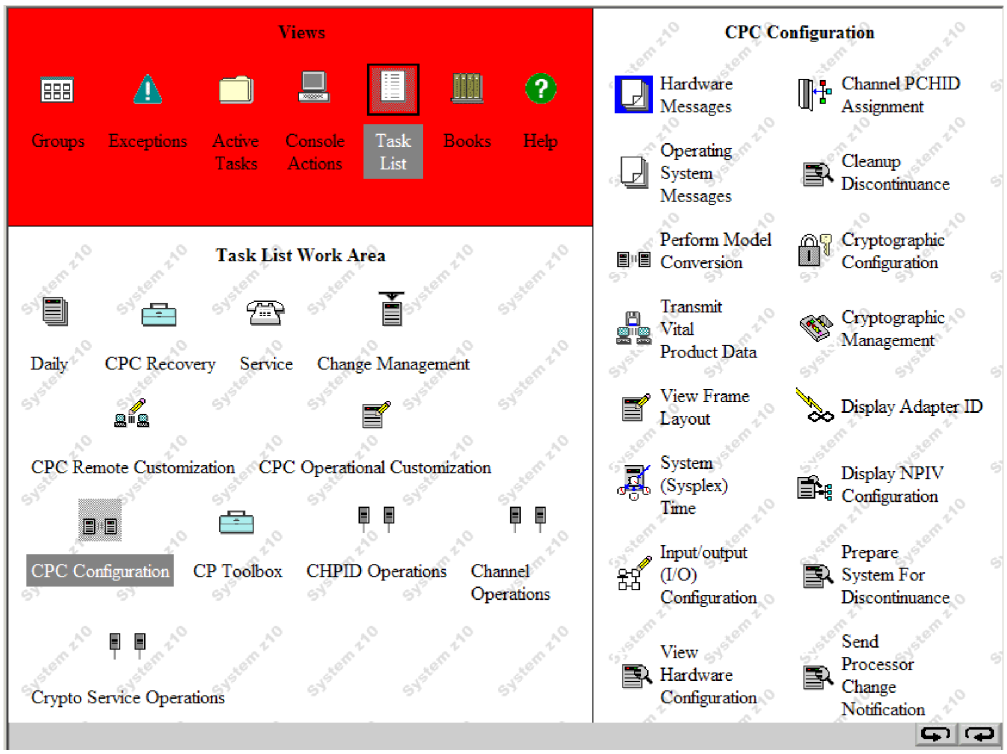


Figure 65. Support Element - Classic style user interface

You can directly manipulate the objects (such as CPCs) that are defined and be aware of changes to hardware status as they are detected. You can work with the objects on the workplace using the mouse to select them. There are several techniques for manipulating objects and tasks. One way to do this is to left-click an object to select it and double-click the task. An alternate method is the drag and drop technique, which involves using the mouse to pick up one or more objects, dragging them to a task, and then dropping them. These techniques are examples of what is known as direct manipulation.

Changing the user interface style

To change from the tree style interface to classic style, perform the following steps:

1. In the navigation pane in the left portion of the window, click **SE Management**.
2. In the tasks pad in the bottom portion of the Work Pane, under Configuration, click **User Settings**.
3. Click the **UI Style** tab. This displays the User Style Information window.
4. Select **Classic Style**, and then click **Apply**.
5. Click **OK**.

To change from classic style back to tree style, perform the following steps:

1. Open **User Settings** (under **Console Actions** in the classic interface). The User Settings window is displayed.
2. Click the **UI Style** tab. The User Style Information window is displayed.
3. Select **Tree Style**, and then click **Apply**.
4. Click **OK**.

Appendix B. Coupling facility control code support

Coupling facility control code is Licensed Internal Code (LIC) that supports the following coupling facility limits:

Table 20. Coupling facility limits at different coupling facility code levels

Coupling Facility Limit	Coupling Facility Code Level				
	Level 16	**Level 15**	**Level 14**	**Level 13**	**Level 12**
Maximum number of CPs	16	16	16	16	16
Storage increment	1 MB	512 KB	256 KB	256 KB	256 KB
Structure ID limit	1023	1023	1023	1023	1023
Retry buffer limit	1799	1799	1799	1799	1559
Facility information	64 bytes	64 bytes	64 bytes	64 bytes	64 bytes
Maximum list element characteristic	4	4	4	4	4
Maximum lock table entry characteristic	5	5	5	5	5
User identifier limit	32	32	32	32	32
Maximum data area element characteristic	4	4	4	4	4
Local cache identifier limit	255	255	255	255	255
Storage class limit	63	63	63	63	63
Castout class limit	1024	1024	1024	1024	1024

Legend

Maximum number of CPs
Indicates the maximum number of CPs that can be used by a coupling facility logical partition.

Storage increment
Indicates the granularity with which storage allocation requests are rounded, to the amount shown in the table for a particular CFCC level.

Structure ID limit
Cache and list structure ID. Effectively, this limit defines the maximum number of coupling facility structure instances that a coupling facility at this level may contain.

Retry buffer limit
Retry buffer range upper limit.

Facility information
This area contains coupling facility control code release and service level information

Maximum list element characteristic
The size of a list structure list element in bytes equals 256 * (2 ** list element characteristic), for example, 256 * (2**4) = 4K.

Maximum lock table entry characteristic
The size of a lock table entry in bytes equals 2 ** lock table entry characteristic.

User identifier limit
The maximum number of users and list notification vectors that can be attached to a list structure.

Maximum data area element characteristic
The size of a data area element in bytes equals 256 * (2 ** data area element characteristic, for example, 256 * (2**4) = 4K).

Local cache identifier limit
The maximum number of local caches that can be attached to a cache structure.

Storage class limit
Storage classes are in the range 1 to the value shown in the table.

Castout class limit
Castout classes are in the range 1 to the value shown in the table.

Appendix C. Developing, building, and delivering a certified system

This appendix is intended to provide guidance in setting up, operating, and managing a secure environment using System z10 PR/SM. It is primarily for the security administrator, but can also be useful to other involved operations technical support personnel.

Creating Common Criteria-Based evaluations

In October 1998, after two years of intense negotiations, government organizations from the United States, Canada, France, Germany, and the United Kingdom signed a historic mutual recognition arrangement for Common Criteria-based evaluations. This arrangement, officially known as the Arrangement of the Recognition of Common Criteria Certificates in the field of IT Security, was a significant step forward for government and industry in the area of IT product and protection profile security evaluations. The partners in the arrangement share the following objectives in the area of Common Criteria-based evaluation of IT products and protection profiles:

- To help ensure that evaluations of IT products and protection profiles are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles
- To increase the availability of evaluated, security-enhanced IT products and protection profiles for national use
- To eliminate duplicate evaluations of IT products and protection profiles, and
- To continuously improve the efficiency and cost-effectiveness of security evaluations and the certification/validation process for IT products and protection profiles.

The purpose of this arrangement is to advance those objectives by bringing about a situation in which IT products and protection profiles which earn a Common Criteria certificate can be procured or used without the need for them to be evaluated and certified/validated again. It seeks to provide grounds for confidence in the reliability of the judgement on which the original certificate was based by declaring that the Certification/Validation Body associated with a Participant to the Arrangement shall meet high and consistent standards. The Arrangement specifies the conditions by which each Participant will accept or recognize the results of IT security evaluations and the associated certifications/validations conducted by other Participants and to provide for other related cooperative activities.

The IBM System z10 PR/SM functionality and assurances have been evaluated and certified at an EAL5 level of assurance. This assurance enables z10 PR/SM to meet stringent requirements for confidentiality of processed information including requirements mandated by the federal government and the banking industry.

This appendix must be used in conjunction with other pertinent System z10 manuals supplied with the System z10 to give a security administrator all the required information to configure and operate an LPAR-mode system in a secure manner. This appendix provides instruction on the correct use of the system so that a secure environment is created and maintained. It defines and explains the parameters, settings, and commands recommended by IBM, including references to those sections in the manuals being discussed in "Trusted facility library" on page 226.

Functional characteristics

PR/SM is a cornerstone of IBM's server security. PR/SM's logical partitioning facility enables the resources of a single physical System z10 machine to be divided and shared by distinct logical machines, each capable of running its own operating system.

The security administrator can configure one or more distinct logical machines to ensure complete isolation from one another; one logical machine cannot gain knowledge about any other logical machine's available I/O resources or performed operations. Logical Partitions configured in this manner will be referred to as *Isolated Logical Partitions* throughout the remainder of this appendix.

A single physical System z10 machine allows any combination of Isolated and non-Isolated logical partitions to be configured. The non-Isolated logical partitions can be configured in any manner supported by System z10. Any level of sharing or cooperation among the non-Isolated logical partitions (e.g. Parallel Sysplex) is permitted and will not have any impact on the Isolated logical partitions.

Logical partitions are defined, and the I/O resources of the overall physical computing system are pre-allocated by the security administrator. I/O allocation is an integral part of the process of defining a total system configuration, and must be completely performed before that system configuration can be initialized. This preallocation is done by executing the Input/Output Configuration Program (IOCP) or Hardware Configuration Definition (HCD) to create a hardware-specific data set, called an Input/Output Configuration Data Set (IOCDS), of the I/O resources and their allocation to specific logical partitions. LPAR allocates an entire resource, such as an I/O channel path or a contiguous region of storage. At no time is any real resource allocated to more than one Isolated logical partition. Each complete I/O resource allocation is called a *configuration*. During the period between processor initializations, several IOCDS configurations can be stored, but only one is in effect at any time. The configuration becomes effective as part of the power-on reset sequence. In order to change the active configuration it is necessary to perform an activation of the hardware.

The preceding paragraph deliberately omits any discussion of Dynamic I/O Configuration, Dynamic CHPID management, Reconfigurable channel paths (CHPIDs), I/O resource sharing using Multiple Image Facility (MIF) or Intelligent Resource Director (IRD), because each of them has characteristics that, if inappropriately used, can compromise the secure capability of PR/SM. Cautions and requirements relating to their use are included throughout this appendix.

The reminder of the logical partition's resources are defined by the security administrator prior to the activation of the logical partition. These resources include storage size, number of logical processors, scheduling parameters, and security controls, which can be specified by the security administrator using the appropriate interfaces on the HMC/SE. Many of the control and security parameters can be changed at any time and will take effect dynamically with few exceptions (e.g., specifying dedicated processors for a partition will only take effect if the partition is not yet activated.) Logical partition definitions take effect at logical partition activation, and generally are static while the partition they pertain to is active.

When a resource is allocated to a logical partition, it is set to its architecturally-defined reset state. Channel paths are reset, main and expanded storage is zeroed.

Trusted configuration

This section describes the actions the Security Administrator must take to help ensure that the computer system is configured for a secure mode of operation. The contents of this section specify the configuration of the evaluated product. Any deviation from the specified configuration will not be consistent with that of the evaluated product and may result in partitions that do not provide strict separation.

Subsequent sections in this document detail the security related characteristics of the evaluated product as well as security configurations that were not included in the evaluation. These details are provided to explain and highlight the differences between the various security settings. Nevertheless, to insure strict separation of Isolated logical partitions, only the configuration specified in this section should be used.

The Licensed Internal Code level of the evaluated configuration is specified in a Common Criteria related document called the Security Target. The installed LIC level for a CPC can be determined via the System Information task available in the Change Management Task List of the HMC. A User ID with its authority based on the default SERVICE User ID must be used to display the complete configuration information.

Note: All configuration requirements listed in subsequent sections are mandatory regardless of whether the term *must* or *should* is used.

- The hardware and any networks used to connect the hardware must be physically secure. Access to I/O devices must be restricted to authorized personnel. The Hardware Management Console must be physically protected from access other than by authorized system administrators.
- The remote support facility must be disabled.
- Devices must be configured so that no device is accessible by any partition other than the partition to be isolated (although they may be accessible by more than one channel path).
- Each I/O (physical) control unit must be allocated only to an Isolated logical partition in the current configuration.
- The Security Administrator must not reconfigure a channel path owned by an Isolated partition unless all attached devices and control units are attached to that path only.
- The Security Administrator should ensure that all devices and control units on a reconfigurable path owned by an Isolated partition are reset before the path is allocated to another partition.
- No channel paths may be shared between an Isolated partition and any other partition(s).
- Although the system will help ensure that the total number of dedicated and shared processors are not over allocated, the System Administrator must ensure that the number of processors dedicated to activated partitions is less than the total number available. This is important so that some processors are available for partitions that do not have dedicated access.
- Dynamic I/O Configuration changes must be disabled.
- If I/O Priority Queuing is enabled for the system an Isolated partition's minimum and maximum I/O Priority values must be equal.
- For Isolated partitions, Workload Manager must be disabled so that CPU and I/O resources are not managed across partitions.

- An Isolated partition must not be configured to enable hipersockets (Internal Queued Direct I/O).
- Partitions must be prevented from receiving performance data from resources that are not allocated to them (Global Performance Data Control Authority must be disabled).
- At most one partition can have I/O Configuration Control Authority (i.e. No more than one partition must be able to update any IOCDS.) and this partition must be administered by a trustworthy administrator (i.e. the administrator of this partition is considered to be the Security Administrator). I/O Configuration Control should be enabled for a single, specific logical partition only during the short period of time when it is permitted to write a new IOCDS.
- The Security Administrator must ensure that write access is disabled for each IOCDS, unless that IOCDS is to be updated (the current IOCDS must not be updated).
- The Security Administrator must verify any changed IOCDS after a power-on reset with that IOCDS, before any partitions have been activated (the Security Administrator may determine whether the IOCDS has been changed by inspecting the date of the IOCDS).
- No partition should have Cross-partition Control Authority (i.e. No partition should be able to reset or deactivate another partition).
- No Isolated partition may have coupling facility channels which would allow communication to a Coupling Facility partition.
- The 'Use dynamically changed address' and 'Use dynamically changed parameter' checkboxes must not be selected in the Image or Load profile.
- No Isolated partition should have the following Counter Facility Security Options enabled:
  - Crypto activity counter set authorization control
  - Coprocessor group counter sets authorization control

  Disabling these options will ensure that its crypto and coprocessor activities are not visible to any other partitions.

System z10 PR/SM characteristics

- There is a Hardware Management Console (HMC) and Support Element (SE) from which the system can be operated. Therefore the system administrators of the system must be cleared for the highest security classification of work being performed on the system.
- Hardware-related operations for each logical partition will be conducted from the HMC or SE. Operations are invoked by selecting the desired CPC image (representing a logical partition) and invoking the desired task.
- For enhanced integrity of execution, locking of partitions is recommended. The partition must then be unlocked before other disruptive operations can be performed on that partition. Lock a logical partition by selecting the CPC image representing the logical partition and invoking the Image Details task. Set the Lockout disruptive tasks radio button to Yes and click the Apply button. You can use this same procedure to unlock a logical partition by setting the Lockout disruptive tasks radio button to No and saving the setting. Locking a logical partition can prevent accidentally performing disruptive tasks on it.
- When entering values on an HMC or SE panel, values are not recognized by the system until you save the data and confirm the changes appearing on the screen.

- The Security Log records system operator actions and responses for operations that are security relevant. The entries are in chronological order and provide an audit log. Entries also include a user (system administrator) identifier when appropriate.
- The Security Log, when full, will be pruned to 2/3 of its capacity. The pruned records, the oldest 1/3 of the log, are discarded. Care should be taken to periodically off load the security log to insure that no records are lost.
- When the security log is successfully off loaded to removable media, the active log is pruned so that it does not exceed 20% of it's capacity. If the active security log is below 20%, then no entries are removed. If it is above 20%, then enough active security log entries are removed (from oldest to newest) to reduce the size of the active security log to 20%. The oldest entries are still in the offloaded log.
- The security log on both the HMC and SE is 10 megabytes. Entries range from 40 bytes to 400 bytes.
- Access to the security log is achieved by selecting ″View Security Logs″ from the list of console actions. This is available on both the SE and HMC. Access to the Security Log from a logical partition is impossible (this capability does not exist).

Central and expanded storage

Throughout this document there are statements that announce ″Sharing of allocated central/expanded storage among multiple logical partitions is not allowed″., ″... it becomes available to the logical partition if no other logical partition is using the same storage.″, and ″No other logical partition has this expanded storage address range on line.″ This is because PR/SM* has a mechanism that detects conditions where sharing was defined (where address ranges overlap), and rejects such requests. PR/SM* licensed internal code (LIC) and hardware rigidly enforce the ″no-sharing″ rule at logical partition definition, during logical partition activation, during logical partition reconfiguration, and during logical partition execution. PR/SM* monitors each instruction's storage accesses for validity; accesses outside the logical partition's defined storage are not permitted to proceed.

Only storage increments within the logical partition's storage allocation as defined in the activation profile can be placed offline. Storage is varied off and on line by using the z/OS or MVS/ESA CONFIG (CF) operator command. See *z/OS MVS System Commands* for further detail. While processing this command, MVS must interact with PR/SM, via a service call instruction, to request that the storage be varied. Because storage cannot be varied without PR/SM involvement, no way exists to circumvent the validity checking PR/SM does to confine a partition occupant within the storage limits defined for the logical partition.

I/O security considerations

IOCDS considerations

Chapter 2, "Planning considerations" contains a very thorough discussion of I/O configuration-related topics. It should be read in its entirety before reading the following security considerations.

When the IOCDS does not specify any sharing, I/O devices are owned solely by the logical partitions that own the channel paths that are attached to them. Even if a channel path has been designated as reconfigurable, that channel path cannot be removed from a logical partition unless the channel path has first been taken offline from within that logical partition. For z/OS System Control Program (SCP) partitions, this is done with the SCP operator command CONFIG (CF). For partitions containing other SCPs, the **Channel Operations** task list must be used. Use the **Configure On/Off** task to configure channel paths that are online. Use the **Release task** to release the channel paths that are assigned to logical partitions that have the Logical Partition Isolation security control enabled or, use the **Reassign Channel Path** task to reconfigure a CHPID in one step.

I/O sharing should never be allowed for Isolated logical partitions. If the IOCDS were to specify I/O sharing, it would be indicated in the Input/Output Configuration Program's Configuration Reports (see the *System z Input/Output Configuration Program User's Guide for ICP IOCP*.)

Isolated logical partitions must never define channel paths as shared in the IOCDS. Specification of a shared channel path can compromise the security of the Isolated logical partitions in the installation. A shared channel path is defined by specifying one of the following on the CHPID statement:
- SHARED keyword
- NOTPART keyword
- PARTITION keyword with more than one logical partition in the access list
- IOCLUSTER keyword
- PATH keyword with more than one CSS ID (i.e. a spanned channel path)

Use of a shared channel path allows the possibility of two partitions having access to the same I/O control units and devices. This is in contradiction to the policy of strict separation. Additionally, the use of shared channels may facilitate some form of covert signaling. However, if covert signaling is not perceived to be a significant threat, it is highly recommended that each use of a shared channel be carefully analyzed for its possible effect on the installations security policy. Although a shared channel path is defined to be shared, **none** of the devices that are connected to it need to be shared among logical partitions. When devices are assigned to a single logical partition, they cannot be accessed by any other logical partition.

Low-speed devices (such as SCP Operator's Consoles) are especially inviting targets for sharing a single channel path using multiple image facility (MIF). The following paragraph discusses how to share the channel path, but none of the console devices.

If you choose to share channel paths between Isolated logical partitions, and their access to specific devices attached to that channel path must be restricted, I/O Device Candidate Lists are the means for restricting access to devices. The default, if no I/O Device Candidate List is specified, is that all partitions sharing the MIF channel path, also share access to all attached devices. Such free access is incompatible with the concept of a secure platform that provides disjoint, non-communicating logical partitions, and is therefore not recommended. We recommend that when sharing is specified for a CHPID, all the associated, attached I/O devices (IODEVICE statement) must have a candidate list specified. Following a rule of always specifying a device's partition explicitly prevents unexpected results from defaults being applied. For further details on I/O device candidate list, refer to the discussion of the IODEVICE statement's PARTITION parameter in the *System z Input/Output Configuration Program User's Guide for ICP IOCP*.

Sharing of channel paths is controlled by the **SHARED** parameter, and the partition names specified in the **PARTITION** and **NOTPART** parameters for each channel path definition (CHPID statement) in the IOCDS. If the PARTITION parameter specifies multiple partition names, it specifies that this particular CHPID is shared among the named partitions. If a NOTPART parameter is used, it implies the sharing characteristic. However, if a NOTPART parameter excludes all partition names but one, in both access and candidate lists, no sharing is permitted. Devices attached to a shared CHPID are restricted to the partitions included in the device candidate list (specified in the IODEVICE PARTITION parameter). If the IOCDS does not specify sharing, then no sharing of CHPIDs will take place.

Operational considerations

Global, system-wide control of Dynamic I/O Configuration is provided by the **I/O Configuration Control Authority**. Use of this facility does not result in strict separation of partitions and was not included in the evaluated product. At most, only use the **Customize/Delete Activation Profiles** task from the CPC Operational Customization tasks list to open a reset or image profile to enable I/O Configuration control for a logical partition. The I/O configuration control selection is located on the **Security** page for the logical partition.

Logical partitions may also be defined with their Logical Partition Isolation security control enabled. **Isolated** For such logical partitions, an offline, reconfigurable CHPIDs cannot be assigned to another logical partition unless the CHPID **Release** task is invoked (or the **Reassign** task) by the System Administrator from the SE or HMC. These tasks are available from the **Channel Operations** task list. The CHPID statement's candidate list can be used to limit the ″mobility″ of a reconfigurable channel. The system will only accept configure on commands for CHPIDS in partitions specified in the candidate list of the target channel path.

All channel path reconfiguration procedures should be specifically described in the secure installation's procedures. Any not described, must not be permitted. While developing these procedures, consideration must be given to the security implications of defining a channel path (and its attached devices) to be reconfigurable. Specifically, which from-to pairs of logical partitions are valid? (When this has been established, candidate lists are the means for implementing this aspect of the installation's security policy). In the process of reconfiguration, could data be passed from one logical partition to another via one of the attached devices? What other procedural controls must be followed in order that your organization's security policy is maintained? What operator actions are required to reconfigure this specific channel path in a secure manner? Lastly, careful attention to the IOCDS language rules relating to the CHPID REC parameter is necessary to achieve the result desired.

Channel path reassignments which result from executing configure CHPID actions, are remembered by the system by recording these changes on the SE hard disk and associating them with the IOCDS (the IOCDS itself is not changed). These changes to channel path assignments (I/O Configuration) take effect whenever the logical partitions are again activated. If the IOCDS is rewritten (by invoking HCD or IOCP), the channel path reassignments are erased (at the first Activation using that newly rewritten IOCDS).

When a channel path is deconfigured from a logical partition, each subchannel (an internal structure that provides the logical appearance of an I/O device, and is uniquely associated with one I/O device) for which this channel path is the only (remaining) online path, is removed from the logical partition. Before the subchannels are removed, they are drained and disabled. Subsequently the channel path is reset. If the channel path being deconfigured is the last channel path to a device, that device is also reset. Actions directed to a removed subchannel result in a condition code=3 (not operational).

At that very first use of a newly created IOCDS, activation configures all channel paths to the logical partitions as defined by the IOCDS. The subsequent movements of reconfigurable channel paths, from one logical partition to another, is remembered by the system. During subsequent activations, as each logical partition is activated, if a channel path was (previously) moved out of a logical partition, the channel path is taken offline to that logical partition; if a channel path was moved into a logical partition, the channel path is brought on line to that logical partition. These logical configuration changes can be viewed by performing the following steps:

- Go to the **CPC Configuration** task list
- Select **Input/Output (I/O) Configuration** task
- Select the IOCDS which is marked **Active**
- Select the **View** pulldown
- In the **View** pulldown, select **Channel Path Configuration**
- Select a **PCHID**
- Select the **View** pulldown
- In the **View** pulldown, select **CHPID information**

The Security Administrator can repeat the final three steps shown above to see all defined CHPIDS and determine which partition(s) each is assigned to, whether they are Dedicated, Shared or Reconfigurable, and the type of each CHPID. In a secure installation, CHPIDs must not be shared among Isolated logical partitions.

Careful review of installation security guidelines must precede using the **Swap Channel Path** procedure available from the **Channel Operations** task list. All devices attached to the channel path being switched in, may be accessible to the logical partition. This caution does not apply to a truly ″spare″ channel path, one with no devices currently defined or attached.

Input/Output Configuration Data Set (IOCDS)

An IOCDS defines the logical partitions by name, allocates I/O resources to each of them, and specifies the security characteristics of those I/O resources. The following list describes the security-relevant parameters of each type of IOCDS source statement.

Statement Type — **Discussion**

ID
: No security-relevant parameters.

RESOURCE
: Assign logical partition names and MIF image IDs so that explicit control is asserted, and maximum checking of following IOCDS source statements is enabled.

CHPID

- Use **PARTITION** parameter to specify which logical partition each channel path is allocated to.
- Don't use the **SHARED** parameter for Isolated logical partitions without study of the security implications.
- Don't use the **REC** parameter without study of the security implications.
- Specify whether the channel path is **REConfigurable**, and specify which logical

	partitions are to have access (using logical partition names in the candidate list). • Don’t use the **IOCLUSTER** keyword for any Isolated logical partitions.
CNTLUNIT	Specification of the **PATH** parameter must be accorded care so that a secure configuration results.
IODEVICE	Specification of the **CUNUMBR** parameter must be accorded care so that a secure configuration results.

LPAR Input/Output configurations

- In general, I/O devices must not be shared by isolated logical partitions, since they can be used to pass information from one partition to another. There may be special cases, such as an output-only device which an installation may consider sharable after careful review of any related security risks, and defining related security procedures and processes.
- The PCHID Summary Report, Channel Path Identifier (CHPID) Summary Report and I/O Device Report produced by the Input/Output Configuration Program must be thoroughly examined by the Security Administrator for indications of unwanted sharing or reconfigurability of channels and devices.
- A thorough review of the actual physical connections/links of the I/O configuration must be performed to establish that the physical configuration is identical to that specified in the IOCDS source file. Specific attention should be given to devices with multiple device path capability, to help ensure that one device (or control unit) does not (accidentally) connect to more than one isolated logical partition’s channel paths.
- All IOCDSs should be write-protected except for the few minutes during which they are actually updated.
- The time stamps of the production-level IOCDSs should be recorded. By selecting the CPC and invoking the I/O Configuration task, a display of the available IOCDSs will be generated. Periodic audits should be made to assure that the IOCDSs have remained unchanged.

Activation

A reset profile includes information for activating a central processor complex (CPC) and its images (logical partitions).

- In the reset profile, after selecting an LPAR IOCDS (A0-A3) deemed valid for secure operation via the Input/Output (I/O) Configuration task.
- Dynamic I/O changes can be disabled on the Dynamic Page of the Power-on Reset Notebook displayed during Power on Reset of the CPC. Ensuring the ’Allow dynamic changes to the channel subsystem input/output (I/O) definition)’ is not selected, disables dynamic I/O for the CPC. Globally disabling dynamic I/O configuration narrows the control of the I/O configuration control parameter to only controlling a logical partition’s reading and writing of IOCDS.
- Workload Manager (found on the Processor page of the Image profile) should not be enabled for Isolated logical partitions.

  Enabling Workload Manager (WLM) enables Dynamic CHPID Management (DCM) to optimize I/O throughput across an LPAR cluster by sharing CHPIDs among partitions who have joined the cluster. Any logical partition that is WLM enabled may join the cluster and therefore share CHPIDs reserved for use by members of the specified cluster. Furthermore, partitions within a cluster may issue a special DIAGNOSE instruction to obtain information about other partitions within the same cluster even when Global Performance Data Authority is not enabled. See Chapter 3, “Determining the characteristics of logical partitions” for more information.

Security controls

- A logical partition’s initial security settings are set in the image profile used to activate it. Afterwards, the Change Logical Partition Security task can be used to view or change the settings. Changes must be saved in the profile in order to have them available for subsequent use. Security settings are saved by the system across activations for the current configuration. Therefore, if the same configuration is used, Security settings need not be reentered (but should be checked).

> **Important Note**
> The default values for the Logical Partition Security controls are not appropriate for secure operation, and must not be specified.

- The following Logical Partition Security Controls settings are required for a secure mode of operation:
  - **ISOLATION should be enabled**. This option binds the partition’s allocated I/O configuration to it, even when a Channel Path (CHPID) is in an offline state. An overt, auditable operator action is required to unbind an item of the I/O configuration and move it to another partition.
  - **I/O CONFIGURATION CONTROL should be disabled for every partition**. By negating this option, the partitions are prevented from accessing (read or write) the existing IOCDS data sets, or dynamically altering the current I/O configuration. IOCDSs can be a means to surreptitiously pass data between partitions. In addition, dynamic alteration of the current I/O configuration can result in a partition having access to data that it is not authorized to access. Dynamic I/O Configuration is supported by the Hardware Configuration Definition (HCD) product for the z/OS or z/VM operating system.

    Note: I/O Configuration control should be enabled for a single, specific logical partition only during the short period of time when it is permitted to write a new IOCDS. Only the IOCDS to be written should have its write-protection temporarily reset. All other IOCDSs should remain write-protected during an IOCDS update operation. The Security Administrator should remain logged onto the console until the IOCDS update is complete, and the IOCDS update authority is disabled.

    Note: Neither Isolation nor I/O Configuration Control option has any effect on the sharing of CHPIDS or I/O Devices. Sharing is enabled by parameters of the CHPID statement used in the definition of the IOCDS.
  - **GLOBAL PERFORMANCE DATA AUTHORITY should be disabled for every partition**. This recommendation is based on a desire to block any possibility of a partition extracting meaning from another partition’s performance data.
  - **CROSS-PARTITION CONTROL should be disabled for every partition**. Enabling cross-partition control permits one partition to disrupt processing in other partitions, resulting in the threat of denial of service to those partition’s users. When cross-partition control is disabled, Automatic Reconfiguration

Facility (ARF) is disabled. ARF uses the cross-partition control capability of PR/SM. ARF is not generally appropriate in a tightly managed, secure system.

– **CRYPTO ACTIVITY COUNTER SET AUTHORIZATION CONTROL should be disabled for Isolated partitions.** Enabling Crypto activity counter set authorization control makes counter data indicating the crypto activities of the Isolated partition visible to other partitions.
– **COPROCESSOR GROUP COUNTER SETS AUTHORIZATION CONTROL should be disabled for Isolated partitions**. Enabling Coprocessor group counter sets authorization control makes counter data indicating the coprocessor group activities of the Isolated partition visible to other partitions.

Reconfiguring the system

Deconfiguration

The recommended way to deconfigure objects owned by a logical partition is to first deconfigure the object from the operating system's point of view, and when necessary (z/OS interacts with PR/SM to complete the reconfiguration process, other operating systems may not), use the Hardware Management Console's tasks to request PR/SM to deconfigure the identical object. The z/OS operating system expects operations personnel to use the HMC/SE based configuration tasks to request deconfiguration of a logical partition object.

Reconfiguration

If the objects are not presently part of the logical partition's configuration, they must be made available to the partition with the use of facilities at the Hardware Management Console. Channel Paths (CHPIDs) may be made available to the target logical partition using the CHPID Operations tasks; reserved storage may be available, but if it isn't, it can be made available by a Security Administrator action by updating the Image profile's Storage page of the Customize/Delete Activation Profiles task. There are many operational considerations relating to reconfiguration that are covered in greater detail in the *z/OS MVS Planning: Operations* document and the *z/OS MVS Recovery and Reconfiguration Guide*.

The following elements can be reconfigured from the z/OS Operator's console using a CONFIG command. Such a reconfiguration is limited to the objects owned by the logical partition:

- Logical Processors
- Central Storage
- Expanded Storage
- Channel Paths

See *z/OS MVS System Commands* for further detail on the CONFIG command.

MVS is aware of the logical partition objects it owns, and interacts with PR/SM to reconfigure them using the service call instruction. This Execution of this instruction results in a mandatory interception (by the System z10 processor hardware) which causes every use thereof to be mediated by PR/SM. PR/SM mediates the instruction to limit the scope of such requests to the objects that the security administrator defined for the specific logical partition.

Audit trail

All security-relevant events initiated from the HMC/SE by the System Administrator will be written to the security log. When these logs become full, they are *pruned*. This means that the oldest one-third of the entries are deleted and the log is reduced to two-thirds full. The log has the capability to store many weeks worth of security relevant events under normal system operation.

To insure the no security relevant information is lost, the security log should be offloaded periodically to removable media provided with the processor. When the security log is successfully off loaded to removable media, the active log is pruned so that it does not exceed 20% of it's capacity. If the active security log is below 20%, then no entries are removed. If it is above 20%, then enough active security log entries are removed (from oldest to newest) to reduce the size of the active security log to 20%. The oldest entries are still in the offloaded log.

Refer to the *System z10 Support Element Operations Guide* for additional information on how to look at the contents of the security log.

Recovery planning

You should read "Recovery strategy" on page 205, and then adapt it to your configuration's requirements for security and processing priorities. Installation-specific recovery procedures must be developed and documented in advance, always giving consideration to where the sensitive data will be after each recovery scenario has completed.

Service and maintenance

Many secure accounts are hesitant about enabling remote service. Consideration should be given to enabling outbound RSF calls that contain the data necessary to automatically dispatch an IBM service representative. Since there is considerable customizing capability provided, RSF can probably be tailored to match your installation's security policy and practices.

This product has support for the concurrent service and maintenance of hardware. The following can be serviced concurrently while normal customer operations continue:

- Power supplies
- Channel cards
- Licensed Internal Code (LIC)
- Processor Book

When service is performed on the above-listed elements of the processor, the physical elements are logically and electrically isolated from the remaining portions of the system still in use. This is begun by first logging on the HMC with a SERVICE ID and then performing the desired maintenance or service task. Refer to the *Service Guide* for information on how to perform the desired task.

Note: Before placing a reconfigurable or shared channel path into a service configuration, record the logical partition name(s) that it's currently assigned to. This will assure that after service is complete, the channel path will be returned to the logical partition(s) to which it was previously allocated, even if different operations personnel are now in charge.

When a partial or complete configuration is surrendered for service or maintenance the following recommendations should be followed:

- The IOCDSs should remain write-protected.
- All installation configuration data should be, or has been previously, saved. The installation configuration data should be restored, and the initial activation must be fully manual. When activation completes, use the following procedure to check the active I/O configuration:

  – go to the **CPC Configuration** panel
  – select **Input/Output (I/O) Configuration**
  – select the IOCDS which is marked **Active**
  – select the **View** pulldown
  – in the **View** pulldown, select **Channel Path Configuration**
- Prior to giving the system to the service representative for disruptive maintenance, it is advisable to idle the partitions (perform an orderly shutdown of the applications and control programs occupying the partitions, followed by stopping each partition) rather than deactivating them. Doing this allows the system to perform automatic (re)activation on the subsequent activation. Automatic activation offers fewer opportunities for human error to affect the controlling parameters of the system, and hence is more secure.

After completion of a disruptive service operation, the CPC should be selected and the I/O Configuration task invoked to display a list of the available IOCDSs. Use this list to check the IOCDS time stamps against the values recorded the last time the IOCDSs were updated. This is to help ensure that the IOCDSs remain unchanged.

Logical processors

A logical CP may be taken offline as the result of an MVS operator entering an MVS CONFIG command to take one (or more) CPs offline. When this is done, MVS performs the work necessary to no longer dispatch work on the CP(s), and then executes a service call instruction to request that PR/SM take the logical CP(s) offline. See *z/OS MVS System Commands* for further detail on the CONFIG command. Lastly, a logical CP may be taken off line at the next activation of the partition by reducing the number of CPs defined for a logical partition in the image profile for the logical partition.

The maximum number of logical processors for each logical partition is defined at logical partition activation, and remains fixed for the duration of the activation. Each of these logical CPs is represented by a data structure that is associated only with its specific logical partition. There are no circumstances where a logical CP can be ″transferred″ to another logical partition, nor is there a capability within the system to accomplish this.

When a logical CP is taken offline, the data structure that represents it is marked as ″offline″, and continues to be maintained in PR/SM-accessible storage, remaining absolutely bound to its logical partition for the duration of that partition’s activation. An offline logical CP presents a checkstopped status when interrogated by the other logical CPs in the partition. An offline logical CP can be restored to the online status by issuing an MVS CONFIG command. MVS uses the service call instruction to request PR/SM bring an offline logical CP back on line. If successful, MVS prepares its control structures to add the CP to its pool of available resources.

Initial Program Load

An Initial Program Load (IPL) resets a logical partition to prepare it for loading an operating system, and then loads the operating system using the specified IPL address and IPL parameter. The IPL address and IPL parameter are normally entered manually in the image activation profile or the load profile. However, a partition with I/O Configuration authority has the capability of dynamically changing an IPL address and IPL parameter. This could potentially cause an unintended operating system to be loaded into the partition. To prevent this, the ’Use dynamically changed address’ and ’Use dynamically changed parameter’ checkboxes must not be selected in the Image or Load profile of an Isolated logical partition.

Trusted facility library

Use the manuals listed in this section as needed for background or supplemental information.

Check the edition notices in the beginning of each manual for correspondence to the appropriate driver level. For manuals that do not specify driver level, the highest (most recent) suffix (last two digits of the form number) is required.

Table 21. Trusted facility library for PR/SM

Title	**Order Number**
System z10 Enterprise Class System Overview	SA22-1084
System z10 Business Class System Overview	SA22–1085
System z Hardware Management Console Operations Guide	SC28-6873
System z10 Support Element Operations Guide	SC28-6879
System z Service Guide for Hardware Management Consoles and Support Elements	GC28-6861
System z Service Guide for Trusted Key Entry Workstations	GC28-6862
System z10 Enterprise Class Installation Manual	GC28-6864
System z10 Business Class Installation Manual	GC28–6874
System z10 Enterprise Class Installation Manual for Physical Planning (IMPP)	GC28-6865
System z10 Business Class Installation Manual for Physical Planning (IMPP)	GC28–6875
System z10 and System z9 Stand-alone IOCP User's Guide	SB10-7152
System z Input/Output Configuration Program User's Guide for ICP IOCP	SB10-7037
System z10 Enterprise Class Safety Inspection	GC28-6870
System z10 Business Class Safety Inspection	GC28–6877
System z Application Programming Interfaces	SB10-7030
Security Architecture: Securing the Open Client/Server Distributed Enterprise	SC28-8135
Enterprise Systems Architecture/390 ESCON I/O Interface	SA22-7202
MVS Planning: Security	GC28-1439
Introducing Enterprise Systems Connection	GA23-0383
z/OS Hardware Configuration Definition: User's Guide	SC33-7988
z/OS MVS System Commands	SA22-7627
z/OS MVS Planning: Operations	SA22-7601
z/OS MVS Recovery and Reconfiguration Guide	SA22-7623
z/OS Cryptographic Services ICSF TKE Workstation User's Guide	SA23-2211

Appendix D. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

INFINIBAND, InfiniBand Trade Association, and the INFINIBAND design marks are trademarks and/or service marks of the INFINIBAND Trade Association.

Linux is a trademark of Linux Torvalds in the United States, other countries, or both.

OpenSolaris, Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Electronic emission notices

The following statements apply to this IBM product. The statement for other IBM products intended for use with this product will appear in their accompanying manuals.

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions contained in the installation manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, by installation or use of this equipment other than as specified in the installation manual, or by any other unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Canadian Department of Communications Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformlté aux normes du ministère des Communications du Canada

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

European Union (EU) Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

European Community contact:
IBM Technical Regulations
Pascalstr. 100, Stuttgart, Germany 70569
Telephone: 0049 (0) 711 785 1176
Fax: 0049 (0) 711 785 1283

email: tjahn@de.ibm.com

EC Declaration of Conformity (In German)

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 89/336/EWG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: ″Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen.″

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)“. Dies ist die Umsetzung der EU-Richtlinie 89/336/EWG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 18. September 1998 (bzw. der EMC EG Richtlinie 89/336) für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

update: 2004/12/07

People’s Republic of China Class A Compliance Statement

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may need to perform practical actions.

声明

此为A级产品，在生活环境中，
该产品可能会造成无线电干扰。
在这种情况下，可能需要用户对其
干扰采取切实可行的措施。

Japan Class A Compliance Statement

This product is a Class A Information Technology Equipment and conforms to the standards set by the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korean Class A Compliance Statement

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Taiwan Class A Compliance Statement

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user will be required to take adequate measures.

警告使用者:
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Glossary

This glossary includes terms and definitions from:

- The *Dictionary of Computing*, SC20-1699.
- The *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies can be purchased from the American National Standards Institute, 1430 Broadway, New York, New York 10018. Definitions are identified by the symbol (A) after the definition.
- The *ANSI/EIA Standard - 440A: Fiber Optic Terminology*, copyright 1989 by the Electronics Industries Association (EIA). Copies can be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue N.W., Washington, D.C. 20006. Definitions are identified by the symbol (E) after the definition.
- The *Information Technology Vocabulary*, developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.

The following cross-references are used in this glossary:

Contrast with. This refers to a term that has an opposed or substantively different meaning.

See. This refers the reader to multiple-word terms in which this term appears.

See also. This refers the reader to terms that have a related, but not synonymous, meaning.

Synonym for. This indicates that the term has the same meaning as a preferred term, which is defined in the glossary.

A

absolute address. (1) A direct address that identifies a location without reference to a base address. An absolute address may itself be a base address. (T) (2) In ESA/390 modes, an address that exists after translation and prefixing, but before configuration occurs.

active logical partition. An operator-initiated procedure that performs a system reset to a logical partition and assigns the previously defined hardware to that partition. It causes an automatic IPL of the system control program to occur in the partition unless the operator performs the IPL manually. Contrast with *deactivate logical partition*.

active configuration. In an ESCON environment, the ESCON Director configuration determined by the status of the current set of connectivity attributes.

adapter. (1) Hardware that provides some transitional functions between two or more devices. (2) A mechanism for attaching parts, for example, parts having different diameters. (3) In an ESCON or FICON environment, link hardware used to join different optical fiber connector types.

address. (1) A value that identifies a register, a particular part of storage, a data source, or a data sink. The value is represented by one or more characters. (T) (2) To refer to a device or an item of data by its address. (I) (A) (3) The location in the storage of a computer where data is stored. (4) In data communication, the unique code assigned to each device or workstation connected to a network. (5) The identifier of a location, source, or destination.

allocate. To assign a resource, such as a disk or a diskette file, to perform a task. Contrast with *deallocate*.

AP. Adjunct processor.

APAR. Authorized program analysis report.

application. (1) The use to which an information processing system is put, for example, a payroll application, an airline reservation application, a network application. (2) A collection of software components used to perform specific types of work on a computer.

application program. (1) A program that is specific to the solution of an application problem. (T) (2) A program written for or by a user that applies to the user's work, such as a program that does inventory control or payroll. (3) A program used to connect and communicate with stations in a network, enabling users to perform application-oriented activities.

ARF. Automatic Reconfiguration Facility. A hardware/LPAR function that is part of the cross-partition authority control setting. ARF functions are used by the Sysplex Failure Manager (SFM) policy functions within z/OS, when RESETTIME, DEACTTIME, or the RECONFIG statement is coded in the SFM policy.

asynchronous. (1) Pertaining to two or more processes that do not depend upon the occurrence of specific events such as common timing signals. (T) (2) Without regular time relationship; unexpected or unpredictable with respect to the execution of program instructions. Contrast with *synchronous*.

authorized program analysis report (APAR). A request for correction of a problem caused by a defect in a current release of a program unaltered by the user.

B

basic mode. A central processor mode that does not use logical partitioning. Contrast with *logically partitioned (LPAR) mode*.

batch. (1) An accumulation of data to be processed. (2) A group of records or data processing jobs brought together for processing or transmission. (3) Pertaining to activity involving little or no user action. Contrast with *interactive*.

bit. Either of the digits 0 or 1 when used in the binary numeration system. (T) See also *byte*.

block. A string of data elements recorded or transmitted as a unit. The element may be characters, words, or physical records. (T)

byte. (1) A string that consists of a number of bits, treated as a unit, and representing a character. (T) (2) A binary character operated upon as a unit and usually shorter than a computer word. (A) (3) A string that consists of a particular number of bits, usually eight, that is treated as a unit, and that represents a character. (4) A group of eight adjacent binary digits that represent one extended binary-coded decimal interchange code (EBCDIC) character.

byte multiplexer channel. A multiplexer channel that interleaves bytes of data.

C

CBP. Integrated cluster bus coupling facility peer channel.

central processor. A processor that contains the sequencing and processing facilities for instruction execution, interruption action, timing functions, initial program loading, and other machine-related functions.

central processor complex (CPC). A physical collection of hardware that consists of central storage, one or more central processors, timers, and channels.

central storage. Storage that is an integral part of the processor and includes both main storage and the hardware system area.

CF. Coupling Facility.

CFCC. Coupling Facility control code.

CFP. Coupling facility peer channel.

channel. The system element that controls one channel path, whose mode of operation depends on the type of hardware to which it is attached.

channel control check. A category of I/O errors affecting channel controls and sensed by the channel to which a device is attached.

channel data check. A category of I/O errors, indicating a machine error in transferring data to or from storage and sensed by the channel to which a device is attached.

channel path (CHP). A single interface between a central processor and one or more control units along which signals and data can be sent to perform I/O requests.

channel path configuration. In an ESCON or FICON environment, the connection between a channel and a control unit or between a channel, an ESCON Director, and one or more control units. See also *point-to-point channel path configuration,* and *switched point-to-point channel path configuration*.

channel path identifier (CHPID). In a channel subsystem, a value assigned to each installed channel path of the system that uniquely identifies that path to the system.

channel subsystem (CSS). A collection of subchannels that directs the flow of information between I/O devices and main storage, relieves the processor of communication tasks, and performs path management functions.

channel-attached. (1) Pertaining to attachment of devices directly by data channels (I/O channels) to a computer. (2) Pertaining to devices attached to a controlling unit by cables rather than by telecommunication lines.

CHP. Channel path.

CHPID. Channel path identifier.

CIB. Coupling over InfiniBand channel.

CICS. Customer Information Control System.

CMC. Communications management configuration.

CNC. Mnemonic for an ESCON channel attached to an ESCON-capable device.

command. (1) A character string from a source external to a system that represents a request for system action. (2) A request from a terminal for performance of an operation or execution of a program. (3) A value sent on an I/O interface from a channel to a control unit that specifies the operation to be performed.

configuration. (1) The arrangement of a computer system or network as defined by the nature, number, and the chief characteristics of its functional units. More specifically, the term configuration may refer to a hardware configuration or a software configuration. (I) (A) (2) In an ESCON Director, the physical connection capability determined by a set of attributes. The attribute values specify the connectivity control status and identifiers associated with the ESCD and its ports.

console. A logical device used for communication between the user and the system.

control program. A computer program designed to schedule and to supervise the execution of programs of a computer system. (I) (A)

control unit. A hardware unit that controls the reading, writing, or displaying of data at one or more input/output units.

controller. A unit that controls input/output operations for one or more devices.

conversion. (1) In programming languages, the transformation between values that represent the same data item but belong to different data types. Information can be lost through conversion because accuracy of data representation varies among different data types. (I) (2) The process of changing from one method of data processing to another or from one data processing system to another. (3) The process of changing from one form of representation to another; for example, to change from decimal representation to binary representation.

coupling facility. A special logical partition that provides high-speed caching, list processing, and locking functions in a sysplex.

coupling facility channel. A high bandwidth fiber optic channel that provides the high-speed connectivity required for data sharing between a coupling facility and the central processor complexes (or logical partitions) directly attached to it.

coupling facility control code. The Licensed Internal Code (LIC) that runs in a coupling facility logical partition to provide shared storage management functions for a sysplex.

CP. Central processor.

CPC. Central processor complex.

CPU. Central processing unit.

CS. (1) Central storage. (2) Channel set. (3) Control storage.

CTC. (1) Channel-to-channel. (2) Mnemonic for an ESCON channel attached to another ESCON channel.

CUADD. Control unit logical address.

Customer Information Control System (CICS). An IBM licensed program that enables transactions entered at remote terminals to be processed concurrently by user-written application programs. It includes facilities for building, using, and maintaining data bases.

D

DASD. Direct access storage device.

data transfer. (1) The result of the transmission of data signals from any data source to a data receiver. (2) The movement, or copying, of data from one location and the storage of the data at another location.

DCM. Dynamic CHPID Management.

DDR. Double data rate.

deactivate logical partition. An operator-initiated procedure that releases the hardware assigned to a logical partition, making it available to other partitions. Contrast with *activate logical partition*.

Note: The operator should first deactivate the system control program, if possible or necessary, and then reactivate the partition, which could provide a reset to that partition, if required.

deallocate. To release a resource assigned to a task. Contrast with *allocate*.

deconfigure. To remove a system resource from the currently active configuration, usually through the system control program (SCP) or through the Configuration (CONFIG) frame on the system console.

default. Pertaining to an attribute, value, or option that is assumed when none is explicitly specified. (I)

degraded. Pertaining to a mode of operation in which the system operates with some resources not available.

device. A mechanical, electrical, or electronic contrivance with a specific purpose.

device address. The 8 rightmost bits of an I/O address that identify a particular I/O device and a control unit on the designated channel.

device number. In a channel subsystem, four hexadecimal digits that uniquely identify an I/O device.

direct access storage device (DASD). A device in which access time is effectively independent of the location of the data.

domain. (1) That part of a computer network in which the data processing resources are under common control. (T) (2) In SNA, a system services control point (SSCP) and the physical units (PUs), logical units (LUs), links, link stations, and all associated resources that the SSCP has the ability to control by means of activation requests and deactivation requests.

dynamic connection. In an ESCON Director, a connection between two ports, established or removed by the ESCD and that, when active, appears as one continuous link. The duration of the connection depends on the protocol defined for the frames transmitted through the ports and on the state of the ports.

dynamic reconfiguration. Pertaining to a processor reconfiguration between a single-image (SI) configuration and a physically partitioned (PP) configuration when the system control program is active.

dynamic storage reconfiguration. A PR/SM LPAR function that allows central or expanded storage to be added or removed from a logical partition without disrupting the system control program operating in the logical partition.

E

element. A major part of a component (for example, the buffer control element) or a major part of a system (for example, the system control element).

environmental error record editing and printing program (EREP). The program that makes the data contained in the system recorder file available for further analysis.

EREP. Environmental error record editing and printing program.

error. A discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition. (I) (A)

ESA/390. Enterprise Systems Architecture/390.

ESCD. Enterprise Systems Connection (ESCON) Director.

ESCM. Enterprise Systems Connection Manager.

ESCON. Enterprise Systems Connection.

ESCON channel. A channel having an Enterprise Systems Connection channel-to-control-unit I/O interface that uses optical cables as a transmission medium.

ESCON Director (ESCD). A device that provides connectivity capability and control for attaching any two links to each other.

ESCON environment. The data processing environment having an Enterprise Systems Connection channel-to-control-unit I/O interface that uses optical cables as a transmission medium.

ESCON Manager (ESCM). A licensed program that provides host control and intersystem communication capability for ESCON Director connectivity operations.

ETR. External time reference.

event. (1) An occurrence or happening. (2) An occurrence of significance to a task; for example, the completion of an asynchronous operation, such as an input/output operation.

expanded storage. Optional high-speed storage that transfers 4 KB pages to and from central storage.

extent. (1) Continuous space on a disk or diskette that is occupied by or reserved for a particular data set, data space, or file. (2) A set of consecutively addressed tracks that a channel program can access. The limits of an extent are defined by specifying the addresses of the first and last tracks in the extent.

F

failure. An uncorrected hardware error.

Note: Failures are either recoverable or not recoverable by the software or the operator. The operator is always notified when failures occur. Usually, system recovery occurs through a hardware reconfiguration. If this is not possible, recovery requires a repair of the failed hardware.

FCC. Federal Communications Commission.

feature. A part of an IBM product that may be ordered separately by the customer. A feature is designated as either special or specify and may be designated also as diskette-only.

Federal Communications Commission (FCC). A board of commissioners appointed by the President under the Communications Act of 1934, having the power to regulate all interstate and foreign communications by wire and radio originating in the United States.

G

GB. Gibabyte.

GMT. Greenwich mean time.

guest. In interpretive execution mode, the interpreted or virtual machine as opposed to the real machine (the host).

H

hardware system area (HSA). A logical area of central storage, not addressable by application programs, used to store Licensed Internal Code and control information.

hex. Hexadecimal.

hexadecimal. (1) Pertaining to a selection, choice, or condition that has 16 possible values or states. (I) (2) Pertaining to a fixed-radix numeration system, with radix of 16. (I) (3) Pertaining to a numbering system with base of 16; valid numbers use the digits 0–9 and characters A–F, where A represents 10 and F represents 15.

HSA. Hardware system area.

I

I/O. Input/output.

ICF. Internal coupling facility.

ICP. Internal coupling facility peer channel.

ID. Identifier.

identifier (ID). (1) One or more characters used to identify or name a data element and possibly to indicate certain properties of that data element. (T) (2) A sequence of bits or characters that identifies a program, device, or system to another program, device, or system. (3) In an ESCON Director, a user-defined symbolic name of 24 characters or fewer that identifies a particular ESCD.

IFL. Integrated Facility for Linux.

IML. Initial machine load.

IMS. Information Management System.

initial program load (IML). A procedure that prepares a device for use.

initial program load (IPL). (1) The initialization procedure that causes an operating system to commence operation. (2) The process by which a configuration image is loaded into storage at the beginning of a work day or after a system malfunction. (3) The process of loading system programs and preparing a system to run jobs.

initialization. (1) The operations required for setting a device to a starting state, before the use of a data medium, or before implementation of a process. (T) (2) Preparation of a system, device, or program for operation. (3) To set counters, switches, addresses, latches, or storage contents to zero or to other starting values at the beginning of, or at the prescribed points in, a computer program or process.

input/output (I/O). (1) Pertaining to a device whose parts can perform an input process and an output process at the same time. (I) (2) Pertaining to a functional unit or channel involved in an input process, output process, or both, concurrently or not, and to the data involved in such a process. (3) Pertaining to input, output, or both.

input/output configuration. The collection of channel paths, control units, and I/O devices that attaches to the processor.

input/output configuration data set (IOCDS). The data set that contains an I/O configuration definition built by the I/O configuration program (IOCP).

input/output configuration program (IOCP). A program that defines to a system all the available I/O devices and the channel paths.

interactive. Pertaining to a program or system that alternately accepts input and then responds. An interactive system is conversational; that is, a continuous dialog exists between the user and the system. Contrast with *batch*.

interface. (1) A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics as appropriate. The concept includes the specification of the connection of two devices having different functions. (T) (2) Hardware, software, or both, that links systems, programs, or devices.

interrupt. (1) A suspension of a process, such as execution of a computer program caused by an external event, and performed in such a way that the process can be resumed. (A) (2) To stop a process in such a way that it can be resumed. (3) In data communication, to take an action at a receiving station that causes the sending station to end a transmission. (4) To temporarily stop a process.

interruption. Synonym for *interrupt*.

IOCDS. I/O configuration data set.

IOCP. I/O configuration program.

IOP. Input/Output processor.

IPL. Initial program load.

IRD. Intelligent Resource Director.

ITR. Internal throughput rate.

L

LIC. Licensed Internal Code.

Licensed Internal Code (LIC). Software provided for use on specific IBM machines and licensed to customers under the terms of IBM's Customer Agreement. Microcode can be Licensed Internal Code and licensed as such.

link. (1) In an ESCON or FICON environment, the physical connection and transmission medium used between an optical transmitter and an optical receiver. A link consists of two conductors, one used for sending and the other for receiving, providing a duplex communication path. (2) In an ESCON or FICON I/O interface, the physical connection and transmission medium used between a channel and a control unit, a channel and an ESCD, a control unit and an ESCD, or, at times, between two ESCDs.

local. Synonym for *channel-attached*.

log. (1) To record, for example, to log all messages on the system printer. (2) A record of events that have occurred.

logical address. The address found in the instruction address portion of the program status word (PSW). If translation is off, the logical address is the real address. If translation is on, the logical address is the virtual address.

logical partition (LP). A subset of the processor hardware that is defined to support the operation of a system control program (SCP). See also *logically partitioned (LPAR) mode*.

logical processor. In LPAR mode, a central processor in a logical partition.

logically partitioned (LPAR) mode. A central processor mode, available on the Configuration frame when using the PR/SM feature, that allows an operator to allocate processor unit hardware resources among logical partitions. Contrast with *basic mode*.

logout. Log data that has been collected, formatted, and recorded.

LP. Logical partition.

LPAR. Logically partitioned.

M

machine check. An error condition that is caused by an equipment malfunction.

MB. Megabyte.

megabyte (MB). (1) A unit of measure for storage size. One megabyte equals 1 048 576 bytes. (2) Loosely, one million bytes.

monitor. A device that observes and records selected activities within a data processing system for analysis.

multidrop. A network configuration in which there are one or more intermediate nodes on the path between a central node and an endpoint node. (T)

multidrop topology. A network topology that allows multiple control units to share a common channel path, reducing the number of paths between channels and control units. Contrast with *switched point-to-point topology*. See also *point-to-point topology*.

multiple image facility (MIF). A facility that allows channels to be shared among PR/SM logical partitions in an ESCON environment.

MVS/ESA. Multiple Virtual Storage/Enterprise Systems Architecture.

N

network. (1) An arrangement of nodes and connecting branches. (T) (2) A configuration of data processing devices and software connected for information exchange.

nybble. Equal to 4 bits.

O

offline. (1) Pertaining to the operation of a functional unit that takes place either independently of, or in parallel with, the main operation of a computer. (T) (2) Neither controlled by, nor communicating with, a computer. Contrast with *online*.

online. (1) Pertaining to the operation of a functional unit when under the direct control of a computer. (T) (2) Pertaining to a user&csq.s ability to interact with a computer. (A) (3) Pertaining to a user's access to a computer via a terminal. (A) (4) Controlled by, or communicating with, a computer. Contrast with *offline*.

operating system. Software that controls the execution of programs and that may provide services such as resource allocation, scheduling, input/output control, and data management. Although operating systems are predominantly software, partial hardware implementations are possible. (T)

operator console. (1) A functional unit containing devices that are used for communications between a computer operator and a computer. (T) (2) A display used for communication between the operator and the system, used primarily to specify information concerning application programs and I/O operations and to monitor system operation.

option. (1) A specification in a statement that may be used to influence the execution of the statement. (2) A hardware or software function that can be selected or enabled as part of a configuration process. (3) Hardware (such as a network adapter) that can be installed in a device to change or enhance device functions.

P

page. In a virtual storage system, a fixed-length block that has a virtual address and is transferred as a unit between real storage and auxiliary storage. (I) (A)

parallel. (1) Pertaining to a process in which all events occur within the same interval of time, each handled by a separate but similar functional unit; for example, the parallel transmission of the bits of a computer word along the lines of an internal bus. (T) (2) Pertaining to concurrent or simultaneous operation of two or more devices or to concurrent performance of two or more activities in a single device. (A) (3) Pertaining to concurrent or simultaneous occurrence of two or more related activities in multiple devices or channels. (A) (4) Pertaining to the simultaneity of two or more processes. (A) (5) Pertaining to the simultaneous processing of the individual parts of a whole, such as the bits of a character and the characters of a word, using separate facilities for the various parts. (A)

parameter. (1) A variable that is given a constant value for a specified application and that may denote the application. (I) (A) (2) An item in a menu for which the user specifies a value or for which the system provides a value when the menu is interpreted. (3) Data passed between programs or procedures.

partition. See *logical partition*.

path. In a network, any route between any two nodes. (T)

PCI. Peripheral component interconnect.

point-to-point channel path configuration. In an I/O interface, a configuration that consists of a single link between a channel and one control unit. Contrast with *switched point-to-point channel path configuration*.

point-to-point topology. A network topology that provides one communication path between a channel and a control unit and does not include switching facilities. Contrast with *switched point-to-point topology*. See also *multidrop topology*.

POR. Power-on reset.

PR/SM. Processor Resource/Systems Manager.

problem determination. The process of determining the source of a problem; for example, a program component, machine failure, telecommunication facilities, user or contractor-installed programs or equipment, environmental failure such as a power loss, or user error.

problem state. A condition during which the processor cannot execute input/output and other privileged instructions.

Processor Resource/Systems Manager (PR/SM) feature. The feature that allows the processor to use several system control programs (SCPs) simultaneously, provides logical partitioning capability for the real machine, and provides support for multiple preferred guests.

program status word (PSW). An area in storage used to indicate the sequence in which instructions are executed, and to hold and indicate the status of the computer system.

program temporary fix (PTF). A temporary solution or bypass of a problem diagnosed by IBM as resulting from a defect in a current, unaltered release of the program.

program version. A separate IBM licensed program, based on an existing IBM licensed program, that usually has important new code or functions.

PSW. Program status word.

PTF. Program temporary fix.

R

reconfiguration. (1) A change made to a given configuration in a computer system; for example, isolating and bypassing a defective functional unit or connecting two functional units by an alternative path. Reconfiguration is effected automatically or manually and can be used to maintain system integrity. (T) (2) The process of placing a processor unit, main storage, and channels offline for maintenance, and adding or removing components.

recovery. To maintain or regain system operation after a failure occurs. Generally, to recover from a failure is to identify the failed hardware, to deconfigure the failed hardware, and to continue or restart processing.

RMF. Resource Measurement Facility.

S

SCP. System control program.

SCSW. Subchannel status word.

SDR. Single data rate.

SEC. System engineering change.

security administrator. Any user(s) of the HMC who are defined with a user mode of System Programmer or Service Representative.

Server Time Protocol (STP). A time synchronization feature designed to enable multiple servers to maintain time synchronization with each other. This technology uses coupling links to exchange timing signals directly between participating CECs. STP can operate either in a mode with no Sysplex Timer or can operate in a mixed mode in conjunction with a Sysplex Timer.

service representative. A person who performs maintenance services for IBM hardware products or systems.

SFM. Sysplex Failure Manager.

SIE. Start Interpretive Execution (370-XA or ESA/370 instruction).

SNA. Systems Network Architecture.

start interpretive execution (SIE). An instruction that causes the CPU to enter interpretive-execution mode and to begin running the guest program.

storage. (1) A functional unit into which data can be placed, in which they can be retained, and from which they can be retrieved. (T) (2) The action of placing data into a storage device. (I) (A)

storage control. In a DASD subsystem, the component that connects the DASD to the host channels, performs channel commands, and controls the DASD devices. For example, the 3990 Model 2 and Model 3 are storage controls.

storage director. In a logical entity consisting of one or more physical storage paths in the same storage cluster.

STP. See Server Time Protocol (STP).

subchannel. In 370-XA and ESA/390 modes, the facility that provides all of the information necessary to start, control, and complete an I/O operation.

subchannel number. A system-unique 16-bit value used to address a subchannel.

subsystem. A secondary or subordinate system, or programming support, usually capable of operating independently of or asynchronously with a controlling system. (T)

switched point-to-point channel path configuration. In an ESCON or FICON I/O interface, a configuration that consists of a link between a channel and an ESCON Director and one or more links from the ESCD, each of which attaches to a control unit. This configuration depends on the capabilities of the ESCD for establishing and removing connections between channels and control units. Contrast with *point-to-point channel path configuration*.

switched point-to-point topology. A network topology that uses switching facilities to provide multiple communication paths between channels and control units. See also *multidrop topology*. Contrast with *point-to-point topology*.

synchronous. (1) Pertaining to two or more processes that depend on the occurrence of specific events, such as common timing signals. (T). (2) Occurring with a regular or predictable time relationship. Contrast with *asynchronous*.

sysplex. A set of systems communicating and cooperating with each other through certain multisystem hardware components and software services to process customer workloads.

Sysplex Timer. An IBM table-top unit that synchronizes the time-of-day (TOD) clocks in as many as 16 processors or processor sides.

system administrator. Any user(s) with access to the Hardware Management Console (HMC).

system control program (SCP). Programming that is fundamental to the operation of the system. SCPs include MVS, VM, and VSE operating systems and any other programming that is used to operate and maintain the system. Synonymous with *operating system*.

system reset. To reinitialize the execution of a program by repeating the load operation.

Systems Network Architecture (SNA). The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks.

T

threshold. A level, point, or value above which something is true or will take place and below which it is not true or will not take place.

time-of-day (TOD) clock. A system hardware feature that is incremented once every microsecond, and provides a consistent measure of elapsed time suitable for indicating date and time. The TOD clock runs regardless of whether the processor is in a running, wait, or stopped state.

TOD. Time of day.

topology. The physical or logical arrangement of nodes in a computer network.

TPF. Transaction processing facility.

Transaction Processing Facility. Transaction Processing Facility is a specialized high availability operating system designed to provide quick response times to very high volumes of messages from large networks of terminals and workstations.

TSO. Time sharing option.

V

variable. (1) In programming languages, a language object that may take different values, one at a time. The values of a variable are usually restricted to a certain data type. (I) (2) A quantity that can assume any of a given set of values. (A) (3) A name used to represent a data item whose value can be changed while the program is running.

virtual machine (VM). (1) A virtual data processing system that appears to be at the exclusive disposal of a particular user, but whose functions are accomplished by sharing the resources of a real data processing system. (T) (2) A functional simulation of a computer system and its associated devices, multiples of which can be controlled concurrently by one operating system.

VM. Virtual machine.

VSE. Virtual storage extended.

W

warning message. An indication that a possible error has been detected.

WLM. WorkLoad Manager.

Z

zAAP. IBM System z10 Application Assist Processor.

zIIP. IBM System z10 Integrated Information Processor.

Index

A

B

C

D

E

M

O

P

R

Printed in USA

SB10-7153-02