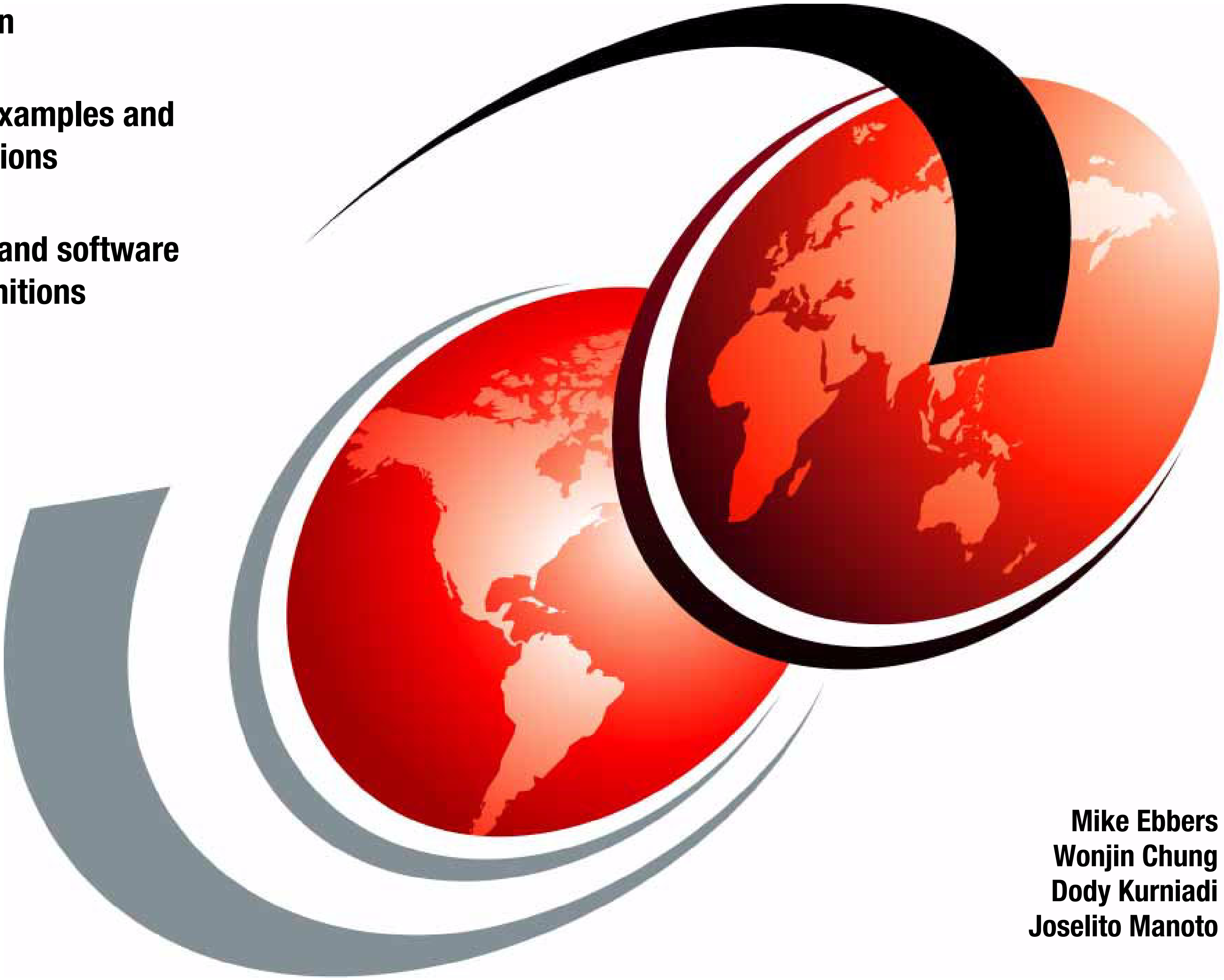
OSA-Express Implementation Guide

Product, planning, and quick start information

Realistic examples and considerations

Hardware and software setup definitions



Mike Ebbers
Wonjin Chung
Dody Kurniadi
Joselito Manoto

Redbooks

ibm.com/redbooks

International Technical Support Organization

OSA-Express Implementation Guide

June 2014

SG24-5948-06

Note: Before using this information and the product it supports, read the information in “Notices” on page xix.

Seventh Edition (June 2014)

This edition applies to OSA-Express4S and OSA-Express5S on z/OS Version 2, Release 1.

Contents

Figures

Tables

Examples

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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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.

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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

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. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US 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 http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX®
BladeCenter®
CICS®
HiperSockets™
IBM®
IMS™
MVS™
OMEGAMON®
Power Systems™
RACF®
Redbooks®
Redbooks (logo) ®
Resource Measurement Facility™
RMF™
System z®
System z10®
System z9®
Tivoli®
VTAM®
WebSphere®
XIV®
z/Architecture®
z/OS®
z/VM®
z/VSE®
z10™
z9®
zEnterprise®

The following terms are trademarks of other companies:

Pentium, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Preface

This IBM® Redbooks® publication will help you to install, tailor, and configure the Open Systems Adapter (OSA) features that are available on IBM zEnterprise® servers. It focuses on the hardware installation and the software definitions that are necessary to provide connectivity to LAN environments. This information will help you with planning and system setup. This book also includes helpful utilities and commands for monitoring and managing the OSA features.

This information will be helpful to systems engineers, network administrators, and system programmers who plan for and install OSA features. The reader is expected to have a good understanding of IBM System z® hardware, Hardware Configuration Definition (HCD) or the input/output configuration program (IOCP), Open Systems Adapter Support Facility (OSA/SF), Systems Network Architecture/Advanced Peer-to-Peer Networking (SNA/APPN), and TCP/IP protocol.

Authors

This book was produced by a team of specialists from around the world working through the International Technical Support Organization (ITSO), Poughkeepsie Center in the US.

Mike Ebbers is a Consulting IT Specialist and Project Leader at the International Technical Support Organization, Poughkeepsie Center. He has worked with IBM mainframe hardware and software products since 1974 in the field, in education, and in the ITSO.

Wonjin Chung is an advisory System Service Representative based in IBM Korea. He has six years of experience in System z and IBM disk storage hardware. He is also well versed on UNIX system platforms. His areas of expertise include hardware related to System z, IBM Power Systems™ solutions, IBM AIX®, and IBM DS8K and IBM XIV® storage. He holds a bachelor’s degree in Mechanical Engineering.

Dody Kurniadi is an IBM IT Specialist based in Indonesia. He supports System z mainframes and the IBM z/OS® operating system and related subsystems, including IBM CICS®, IBM WebSphere® MQ, and IBM Information Management System (IMS™). He works with large bank customers and configures z/OS environments, including the Open Systems Adapter (OSA). He holds a bachelor’s degree in Electrical Engineering

Joselito Manoto is an IBM mainframe network engineer based in Australia. He supports and maintains IBM z/OS Communications Server software (IBM Virtual Telecommunications Access Method [IBM VTAM®] and IBM z/OS Communications Server TCP/IP) for clients in various industries such as banking, airline, and telecommunications. Joselito has worked with the IBM mainframes since 1992, when he began working on the IBM VM operating system. He holds a Bachelor of Science degree in Electrical Engineering.

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

David Bennin
Richard Conway
Roy Costa
Robert Haimowitz
IBM ITSO Poughkeepsie Center

Now you can become a published author, too

Here’s an opportunity to spotlight your skills, grow your career, and become a published author - all at the same time. Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us.

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

- Use the online **Contact us** Redbooks form:

  ibm.com/redbooks

- Send your comments by email:

  redbook@us.ibm.com

- Mail your comments:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD, Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

1

Open Systems Adapter overview

This chapter describes the IBM Open Systems Adapter-Express 5S (OSA-Express5S) and Open Systems Adapter-Express4S (OSA-Express4S) features that are available on an IBM System z mainframe computer. These features connect to other servers and clients in 1000BASE-T Ethernet (10, 100, and 1000 Mbps), Gigabit Ethernet (GbE), and 10-Gigabit Ethernet environments.

> **Terminology:** If not specifically stated otherwise, the term *OSA* applies to the OSA-Express5S and OSA-Express4S features throughout this book.

The information covers the following topics, which includes supported CHPID types and OSA capabilities:

- 1.1, “Introduction to the Open Systems Adapter” on page 2
- 1.2, “OSA-Express for ensemble connectivity” on page 4

1.1 Introduction to the Open Systems Adapter

The Open Systems Adapter (OSA) is a network controller that you can install in an IBM System z mainframe I/O cage. The adapter integrates several hardware features and supports many networking transport protocols. The OSA card is the strategic communications device for the System z architecture. It has several key features that distinguish it from communications that are based on channel control words (CCWs).

The OSA integrates the control unit and device into the same hardware. It does so by placing them on a single card that directly connects to the central processor complex I/O bus. There are several current versions of the Open Systems Adapter:

- Open Systems Adapter-Express3 (OSA-Express3)
- Open Systems Adapter-Express4S (OSA-Express4S)
- Open Systems Adapter-Express5S (OSA-Express5S)

In this book, we describe OSA-Express4S and OSA-Express5S and their functions. Although this book is an update of the previous edition, we describe OSA-Express3 features if nothing has changed since the particular information was written.

Table 1-1 summarizes the availability of the OSA-Express features.

Table 1-1 OSA-Express availability, OSA-Express3 and later versions

Feature	IBM zEnterprise systems: 10 EC, 10 BC, 196, 114	IBM zEnterprise EC12 and BC12	CHPIDs per feature	Ports per CHPID	Total ports
OSA-Express3	Gigabit Ethernet	Gigabit Ethernet	2	2	4
	10-Gigabit Ethernet	10-Gigabit Ethernet	2	1	2
	1000BASE-T Ethernet	1000BASE-T Ethernet	2	2	4
OSA-Express3-2P	1000BASE-T Ethernet (IBM z10™ BC)	1000BASE-T Ethernet (zBC12)	1	2	2
	Gigabit Ethernet SX (z10 BC)	Gigabit Ethernet SX (zBC12)	1	2	2
OSA-Express4S	Gigabit Ethernet	Gigabit Ethernet	1	2	2
	10-Gigabit Ethernet	10-Gigabit Ethernet	1	1	1
		1000BASE-T Ethernet (zEC12)	1	2	2
OSA-Express5S		Gigabit Ethernet	1	2	2
		10-Gigabit Ethernet	1	1	1
		1000BASE-T Ethernet	1	2	2

All OSA-Express features share these characteristics:

- They are hot-pluggable and support the multiple image facility (MIF), which shares channels across logical partitions (LPARs).
- They can be defined as a shared channel among LPARs within and across logical channel subsystems (LCSSs).
- They support Queued Direct I/O (QDIO) mode. QDIO continues to be the preferred architecture on IBM System z for high-speed communication because it reduces host interruptions and improves response time.

- They help ensure that you have a balanced system to meet the bandwidth demands of your applications.

1.1.1 Operating modes

The integration of a channel path with network ports makes the OSA a unique channel or channel-path identifier (CHPID) type. This is recognized by the hardware I/O configuration on a port-by-port basis as one of the following types (CHPID types are shown in parentheses):

- Queued Direct Input/Output (QDIO, CHPID type OSD)
- Non-Queued Direct Input/Output (non-QDIO, CHPID type OSE)
- OSA Integrated Console Controller (OSA-ICC, CHPID type OSC)
- Open Systems Adapter for NCP (OSN)
- OSA-Express for zEnterprise IBM BladeCenter® Extension (zBX, CHPID type OSX)
- OSA intranode management network (OSM)

CHPID type definitions

OSC: OSA Integrated Console Controller support

OSD: OSA direct (QDIO mode)

OSE: IP Passthru and Systems Network Architecture (SNA), Advanced Peer-to-Peer networking (APPN), High-Performance Routing (HPR) traffic (non-QDIO mode)

OSM: OSA intranode management

OSN: OSA for the Network Control Program (also written as OSA for NCP)

OSX: OSA System z Blade Center Extension (also written as OSA for zBX)

The following information about how to configure the OSA-ICC is in the IBM Redbooks publication titled *OSA-Express Integrated Console Controller Implementation Guide*, SA24-6364.

Note: Not all features support all CHPID types.

Table 1-2 gives an overview of the type of traffic supported and whether OSA/SF is required to configure the OSA-Express5S or OSA-Express4S CHPID, based on the supported modes of operation. OSA-Express3 information is included for reference.

Table 1-2 Supported CHPID types

CHPID type	Feature	SNA/APPN/ HPR traffic	TCP/IP traffic	3270 traffic	OSA/SF
OSD	OSA-Express5S 10GbE OSA-Express4S 10GbE OSA-Express3 10GbE OSA-Express5S GbE OSA-Express4S GbE OSA-Express3 GbE OSA-Express5S 1000BASE-T OSA-Express4S 1000BASE-T OSA-Express3 1000BASE-T	No[a,b]	Yes	No	Optional
OSE	OSA-Express5S 1000BASE-T OSA-Express4S 1000BASE-T OSA-Express3 1000BASE-T	Yes	Yes	No	Required
OSC	OSA-Express5S 1000BASE-T OSA-Express4S 1000BASE-T OSA-Express3 1000BASE-T	No	No	Yes	n/a
OSN	OSA-Express3 GbE OSA-Express5S 1000BASE-T OSA-Express4S 1000BASE-T OSA-Express3 1000BASE-T	Yes[c]	No	No	Optional
OSM	OSA-Express5S 1000BASE-T OSA-Express4S 1000BASE-T OSA-Express3 1000BASE-T	No	Yes	No	N/A
OSX	OSA-Express5S 10GbE OSA-Express4S 10GbE OSA-Express3 10GbE	No	Yes	No	N/A

a. SNA over IP with the use of Enterprise Extender or TN3270
b. Layer 2 support allows for non-IP protocols, such as SNA
c. Supports SNA PU Type 5 and PU Type2.1

1.2 OSA-Express for ensemble connectivity

The following OSA features are used to connect the IBM zEnterprise central processor complex (CPC)[1] to the attached zBX and other ensemble nodes:

- OSA-Express4S 1000BASE-T Ethernet, feature code 0408
- OSA-Express4S 10-Gigabit Ethernet (GbE) Long Range (LR), feature code 0406
- OSA-Express4S 10-Gigabit Ethernet (GbE) Short Range (SR), feature code 0407
- OSA-Express5S 1000BASE-T Ethernet, feature code 0417
- OSA-Express5S 10-Gigabit Ethernet (GbE) Long Range (LR), feature code 0415
- OSA-Express5S 10-Gigabit Ethernet (GbE) Short Range (SR), feature code 0416

[1] Unless otherwise specified, zEnterprise CPC refers to zBC12, zEC12, z114z, and z196.

The IBM zEnterprise 196 (z196) and zEnterprise 114 (z114) provide control support for the zBX Model 002, whereas the zEnterprise EC 12 (zEC12) and zEnterprise BC 12 (zBC12) provide control support for the zBX Model 003.

Figure 1-1 illustrates the required network connectivity to attach a zBX to a zEC12 (INMN and IEDN, which are described in the sections that follow).

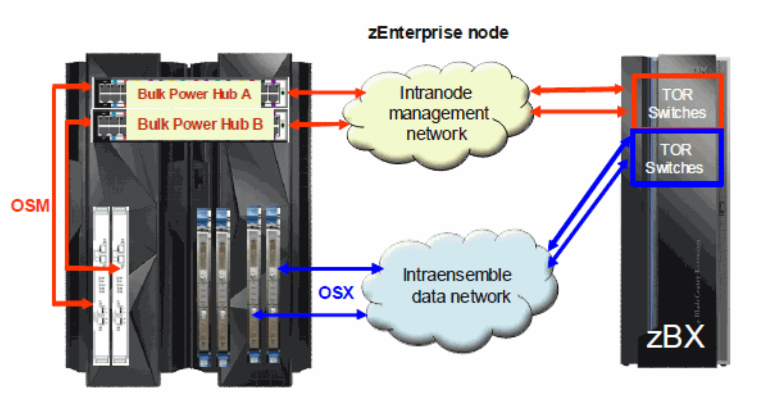


Figure 1-1 zBX connectivity to a zEC12 system

1.2.1 Intraensemble data network (IEDN)

The IEDN is a private and secure 10 Gbps Ethernet network that connects all elements of an ensemble. *Access is controlled* by using integrated virtual LAN (VLAN) provisioning. No customer-managed switches or routers are required. The IEDN is managed by the ensemble primary Hardware Management Console (HMC).[2]

IEDN requires two OSA-Express5S or OSA-Express4S 10GbE ports on two different OSA-Express5S or OSA-Express4S adapters. One port is used from each OSA, and the adapters are configured as CHPID type OSX. The connection is from the zEnterprise CPC to the IEDN top-of-rack (TOR) switches on the zBX.

1.2.2 Intranode management network (INMN)

The INMN is a private and physically isolated 1000BASE-T Ethernet internal management network that operates at 1 Gbps. It connects all resources of an ensemble node (zEnterprise CPC and the controlled zBX components) for management purposes. It is prewired, internally switched, configured, and managed with full redundancy for high availability.

The INMN requires two ports (CHPID port 0) from two OSA-Express5S or OSA-Express4S 1000BASE-T features. CHPID port 1 is not used in this case.

The adapters are configured as CHPID type OSM (OSA intranode management network). The connection is through port J07 of the bulk power hubs (BPHs) in the zEnterprise CPC. The INMN TOR switches on the zBX also connect to the BPHs.

[2] This HMC must be running with Version 2.11 or later with feature codes 0091, 0025, 0019, and, optionally, 0020.

For detailed information about an ensemble network, see *Building an Ensemble Using IBM zEnterprise Unified Resource Manager*, SG24-7921, and the applicable Technical Guide for your system:

- *IBM zEnterprise 196 Technical Guide*, SG24-7833
- *IBM zEnterprise 114 Technical Guide*, SG24-7954
- *IBM zEnterprise EC12 Technical Guide*, SG24-8049
- *IBM zEnterprise BC12 Technical Guide*, SG24-8138

In this book, we cover how to implement the OSA-Express features. You can find more about functions, OSA capabilities, and connectivity in Chapter 7 of the *IBM System z Connectivity Handbook*, SG24-5444.

2

Quick Start guide

This chapter provides information to help you get started quickly with your IBM Open Systems Adapter-Express (OSA) installation. It helps you determine which elements you need, based on your requirements, and directs you to the appropriate sections in this book for more information.

The information in this chapter covers the following topics:

2.1 Software support

The following operating systems that support IBM System z systems also support the OSA:

- IBM z/OS operating system:

  `http://www.ibm.com/servers/eserver/zseries/zos/support/`

- IBM z/VM® operating system:

  `http://www.vm.ibm.com/techinfo/lpmigr/vmleos.html`

- IBM z/VSE® operating system:

  `http://www.ibm.com/systems/z/os/zvse/support/index.html`

- IBM z/Transaction Processing Facility (z/TPF) operating system:

  `http://www.ibm.com/software/htp/tpf/index.html`

- Linux operating system:

  `http://www.ibm.com/servers/eserver/zseries/os/linux/dist.html`

Note: Certain functionality might require specific levels of an operating system or program temporary fixes (PTFs). That information is provided in this chapter.

2.2 Hardware and software definitions for the OSA

Before you can use your OSA features, you must define your hardware and software. In doing so, you need to answer the following questions:

- What is the physical channel identifier (PCHID) assigned to the OSA?
- To which channel identifier (CHPID) will the OSA be assigned?
- Will the OSA CHPID be shared or dedicated?
- To which channel subsystem (CSS) will the OSA CHPID be defined?
- Will the OSA CHPID be spanned across channel subsystems (CSSs)?
- Which OSA CHPID type will be required?
- Which network protocol or protocols will be used with the OSA CHPID?

Note: See the shaded box in the Chapter 1, “Open Systems Adapter overview” on page 1 for definitions of CHPID types.

OSA device types

The different types of OSA channels (CHPID types) require the following device types:

- OSA device for QDIO (OSD) and non-QDIO (OSE)
- 3270-X and 3287 devices for the OSA-ICC (OSC)
- 3745 device for the OSA for Network Control Program, or NCP (OSN)
- OSA device for ensemble network connectivity (OSX) and ensemble management (OSM)

See the IBM z/OS Quick Start table (Table 2-4 on page 13), which provides a quick reference for relating the CHPID type to an operation mode.

The OSA Support Facility (OSA/SF) requires one device (defined by using the Hardware Configuration Definition (HCD) to be associated with the OSA CHPID as device type OSAD (`UNITADD=FE`). OSA/SF uses this device to communicate with the OSA feature.

The OSA-Express Network Traffic Analyzer (NTA) for z/OS requires one or more data path devices for the NTA trace interface, depending on the configuration.

Multiple image facility (MIF)

The multiple image facility enables OSA CHPIDs on System z installations to be shared among logical partitions. For more information, see the *IBM System z Connectivity Handbook*, SG24-5444.

Spanned channels

Spanning is the ability to configure channels to multiple channel subsystems (CSSs). When defined that way, the channels can be shared by any or all of the configured logical partitions (LPARs), regardless of the CSSs to which the LPAR is configured.

OSA ports can be spanned across multiple CSSs on System z systems. For more information about defining the OSA to hardware, see Chapter 3, “Hardware configuration definitions” on page 15.

2.2.1 Modes of operation and addressing support

The OSA features provide direct LAN connectivity as integrated System z features. This brings the strengths of System z servers, such as security, availability, enterprise-wide access to data, and systems management and IBM z/Architecture® to the client/server environment. Table 2-1 on page 10 summarizes the OSA features as they relate to the different modes of operation and maximum addressing ranges that are supported by System z systems.

Table 2-1 OSA modes of operation and addressing support

	OSA-Express4S[a] OSA-Express5S[b]
Addresses	
IP addresses per channel path (IPv4, IPv6, VIPA)	4096
Multicast addresses (IPv4 + IPv6)	16384
ARP table size	16384
MAC addresses	2048
Non-QDIO (OSE)[c]	
Subchannels per IP link	2
TCP/IP stacks per channel path	120
SNA PUs per port	4096
Subchannels per channel path	240
Control units (CUs) per channel path	1
QDIO (OSD)	
Subchannels per IP link	3
TCP/IP stacks per channel path	640[d]
Subchannels per channel path	1920[d]
CUs per channel path	16

a. This applies to IBM zEnterprise central processor complexes (CPCs) only.
b. This applies to IBM zEnterprise EC 12 (zEC12) and IBM zEnterprise BC12 (zBC12) only.
c. This applies to the 1000BASE-T feature only.
d. If multiple priority for queues is enabled, the maximum is reduced to 160 TCP/IP stacks, 480 devices.

Note: The Address Resolution Protocol (ARP) table and multicast addresses are obtained from the same storage pool. The overall capacity limit for both tables is the sum of the IPv4 addresses plus the IPv6 addresses, plus the IPv4 multicast addresses, plus the IPv6 multicast addresses, plus the IPv4 remote addresses. Although the maximum number of multicast addresses is 2048, if there are a large number of other addresses that make up the same storage pool, the amount of multicast addresses might be fewer than 2048. Keep in mind that some operating systems generate a multicast address for each IPv6 address that is specified.

2.3 OSA Support Facility (OSA/SF) requirements

Open Systems Adapter Support Facility (OSA/SF) is used to configure OSA features for non-QDIO mode, but with one exception: the TCP/IP Passthru mode (non-shared).

Notes:
Either OSA/SF on the HMC or the OSA/SF in the operating system component can be used for the OSA-Express4S features. For the OSA-Express5S features, OSA/SF on the Hardware Management Console (HMC) is required.

See Appendix E, “Using the Open Systems Adapter Support Facility” on page 191, for a description of using OSA/SF in the operating system.

For a quick check to determine whether OSA/SF is required for your installation, use Table 2-2 as a reference.

Table 2-2 OSA/SF requirement for configuring OSA features

OSA feature	OSD (QDIO)	OSE (non-QDIO)	OAT built	OSA/SF required
10GbE	Yes		Dynamic	No
GbE	Yes		Dynamic	No
1000BASE-T Ethernet	Yes		Dynamic	No
		Yes	Manual	Yes

2.4 Quick Start tables

This section provides tables to help you identify your OSA feature and implementation requirements. These tables direct you to installation information and setup examples.

For more information about the different types of OSA features, see Appendix A, “Open Systems Adapter-Express features by version” on page 141.

2.4.1 OSA function support

Table 2-3 lists the functions that are supported, based on an OSA feature.

Table 2-3 OSA function support

	OSA-Express4S and OSA-Express5S		
Function	**10GbE**	**GbE**	**1000BASE-T**
Jumbo frame support (8992 bytes frame size)	x	x	x[a]
Network Traffic Analyzer for z/OS[b]	x	x	x
QDIO Diagnostic Synchronization for z/OS[b]	x	x	x
640 TCP/IP (with priority queues disabled)[b]	x	x	x
Virtual IP address (VIPA)	x	x	x
Primary/secondary router function	x	x	x

	OSA-Express4S and OSA-Express5S		
Function	**10GbE**	**GbE**	**1000BASE-T**
Internet Protocol Version 6 (IPv6)	x	x	x[a]
Large send support for IPv4	x	x	x[a]
Large send support for IPv6	x	x	x[a]
VLAN (IEEE 802.1q)	x	x	x[a]
VLAN support of GVRP (IEEE 802.1p)[b]	x	x	x
SNMP support for z/OS and Linux System z	x	x	x
Multicast and broadcast support	x	x	x
ARP cache management	x	x	x[a]
ARP statistics[b]	x	x	x
ARP takeover	x	x	x
IP network availability	x	x	x[a]
Checksum offload support for IPv4	x	x	x[a]
Checksum offload support for IPv6	x	x	x[a]
Dynamic LAN idle for z/OS[b]	x	x	x
QDIO optimized latency mode	x	x	x[a]
Layer 2 support	x	x	x[a]
Link aggregation for z/VM layer 2 mode[b]	x	x	x
QDIO data connection isolation for z/VM	x	x	x[a]
QDIO interface isolation for z/OS	x	x	x[a]
Layer 3 VMAC for z/OS[b]	x	x	x
Enterprise Extender	x	x	x
TN3270E server for z/OS	x	x	x
OSA for NCP support	n/a	n/a	x
Adapter interruptions for QDIO[b]	x	x	x
Inbound workload queuing (IWQ)	x	x	x[a]
Query and display OSA configuration	x	x	x[a]
OSA-Express for IEDN connectivity	x	n/a	n/a
OSA-Express for INMN connectivity	n/a	n/a	x

a. Only in QDIO mode (CHPID types: OSD, OSX)
b. Only in QDIO mode (CHPID type: OSD)

2.4.2 Quick Start tables for IBM z/OS and z/VM operating systems

When reviewing Table 2-4 or Table 2-5 on page 14, keep the following considerations in mind for your OSA implementation:

- If you are using the *default* OSA Address Table (OAT) for the OSA 1000BASE-T features, OSA/SF is not required. The default OAT *values* allow only the following:
  - Non-shared CHPID (port is not shared between logical partitions, or LPARs)
  - CHPID type OSE (non-QDIO)
  - Ports not shared between TCP/IP stacks
  - TCP/IP and SNA do not share a port concurrently
  - Default unit addresses (starting with 00)
  - TCP/IP Passthru mode only
- The OSA/SF configuration is not required for OSA features when defined as CHPID types OSC, OSN, OSD, OSX, and OSM.
- If Systems Network Architecture (SNA) and Advanced Peer-to-Peer Networking (APPN, LU6.2) are required for an OSA feature that is defined as CHPID type OSD, you must use the Enterprise Extender.
- Layer 2 support for an OSA feature that is defined as CHPID type OSD allows for communication with IP and non-IP protocols, such as NetBIOS, SNA, and others.
- OSA features can work in conjunction with the virtual switch (a component of z/VM software) to enable Layer 2 functionality for guest systems, such as Linux on System z. See Chapter 11, “z/VM virtual switch” on page 111.
- You can use a Telnet 3270 (TN3270) terminal emulator in conjunction with SNA (LU2) applications when the OSA feature is defined as CHPID type OSD.

IBM z/OS Quick Start table

Table 2-4 contains TCP/IP and Virtual Telecommunications Access Method (VTAM) definitions and the CHPID types that are necessary when configuring the OSA ports for use in an IBM z/OS environment. It also provides references to the relevant sections in this book.

Table 2-4 z/OS Quick Start table

OSA feature	Operation mode	CHPID type	TCP/IP device type	IP link type	VTAM definitions	See this chapter
10GbE	QDIO TCP/IP	OSD	MPCIPA	IPAQENET	TRLE	Chapter 4, “QDIO mode for the IBM z/OS operating system” on page 31
GbE	QDIO TCP/IP	OSD	MPCIPA	IPAQENET	TRLE	
1000BASE-T	QDIO TCP/IP	OSD	MPCIPA	IPAQENET	TRLE	
	Non-QDIO TCP/IP Passthru	OSE	LCS	ETHERNET or 802.3		Chapter 6, “Non-QDIO mode for the IBM z/OS operating system” on page 51
	Non-QDIO SNA	OSE			XCA, SWNET	

IBM z/VM Quick Start table

Table 2-5 contains CHPID and TCP/IP definitions to use when you configure the OSA ports for use in an IBM z/VM environment. It also provides references to the appropriate sections in this publication.

Table 2-5 z/VM Quick Start table

OSA feature	Operation mode	CHPID type	TCP/IP device type	IP link type	VTAM definitions	Go to...
10GbE	QDIO TCP/IP	OSD	OSD	QDIOETHERNET		Chapter 5, “QDIO mode for the IBM z/VM operating system” on page 43
GbE	QDIO TCP/IP	OSD	OSD	QDIOETHERNET		
1000BASE-T	QDIO TCP/IP	OSD	OSD	QDIOETHERNET		
	Non-QDIO TCP/IP Passthru	OSE	LCS	ETHERNET, 802.3 or ETHEROR802.3		Chapter 7, “Non-QDIO mode for the IBM z/VM operating system” on page 63
	Non-QDIO SNA	OSE			XCA	

For your z/VM and guest system environment, consider using the virtual switch (VSWITCH) in conjunction with your OSA and LAN environment. The virtual switch provides IEEE 802.3 capabilities, such as VLAN and link aggregation support, as well as port isolation. See Chapter 11, “z/VM virtual switch” on page 111 for details.

2.5 Policy-based networking

The z/OS Policy Agent (PAGENT) is not required for OSA. The PAGENT is a component in z/OS that implements policy decisions. It enforces a set of rules and policies that dictate how users, applications, and organizations can access and use IT resources. From an OSA perspective, you can set up policies to manage and prioritize network traffic.

For more information about the PAGENT, see *IBM z/OS V2R1 Communications Server TCP/IP Implementation Volume 4: Security and Policy-Based Networking*, SG24-8099*.*

3

Hardware configuration definitions

As with all channel-attached devices, you must define an IBM Open Systems Adapter (OSA) in the input/output configuration data set (IOCDS) with a channel path, a control unit, and input/output (I/O) devices. This chapter takes you through the steps to define OSA to the IBM System z environment by using the IBM z/OS Hardware Configuration Definition (HCD) tool. To simplify the configuration process of the environment, we have extracted the portions of the setup that are common to all modes and types of the OSA.

Your IBM representative can supply a *physical channel identifier (PCHID) report* that specifies where the OSA feature is plugged into your server. The channel path identifier (CHPID) number and PCHID number are required for all OSA configuration and setup tasks.

The information in this chapter covers the following topics:

- 3.1, “Configuration chart” on page 16
- 3.2, “Hardware Configuration Definition” on page 16

3.1 Configuration chart

The environment that is shown in Figure 3-1 uses one IBM System zEnterprise EC 12 (zEC12) server. The SCZP401 server has one OSA-Express5S 1000BASE-T feature (CHPID 04) and one OSA-Express5S 10GbE feature (CHPID 07). We defined one CHPID (04) to PCHID 534 and one CHPID (07) to PCHID 570. The CHPIDs were spanned across two channel subsystems (CSSs) and shared within two logical partitions (LPARs).

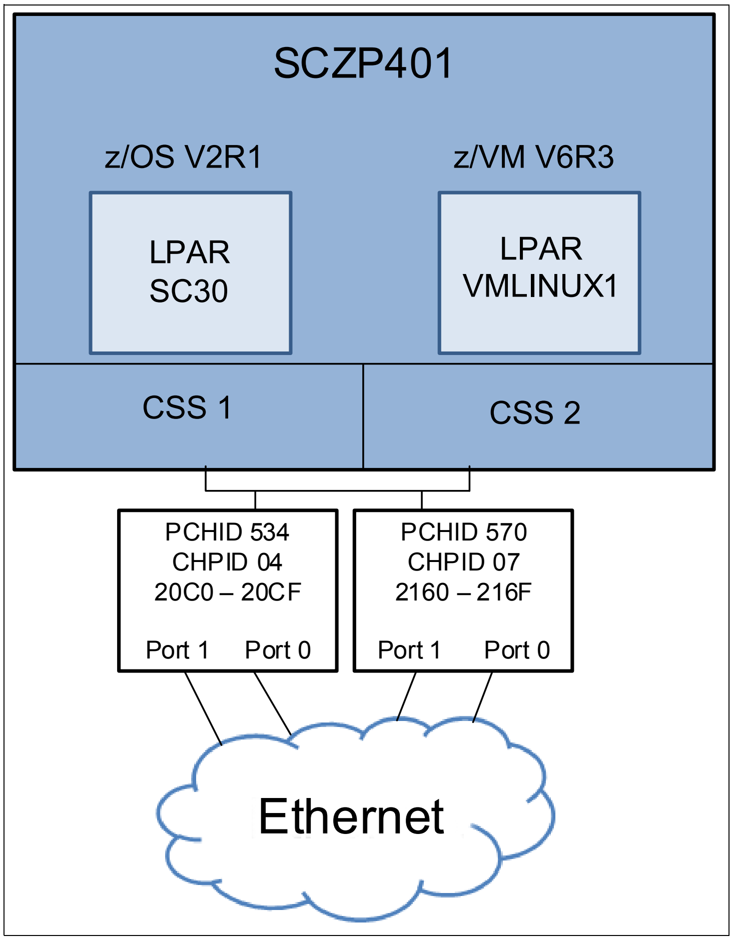


Figure 3-1 HCD definitions for OSA CHPIDs, SCZP401 server

3.2 Hardware Configuration Definition

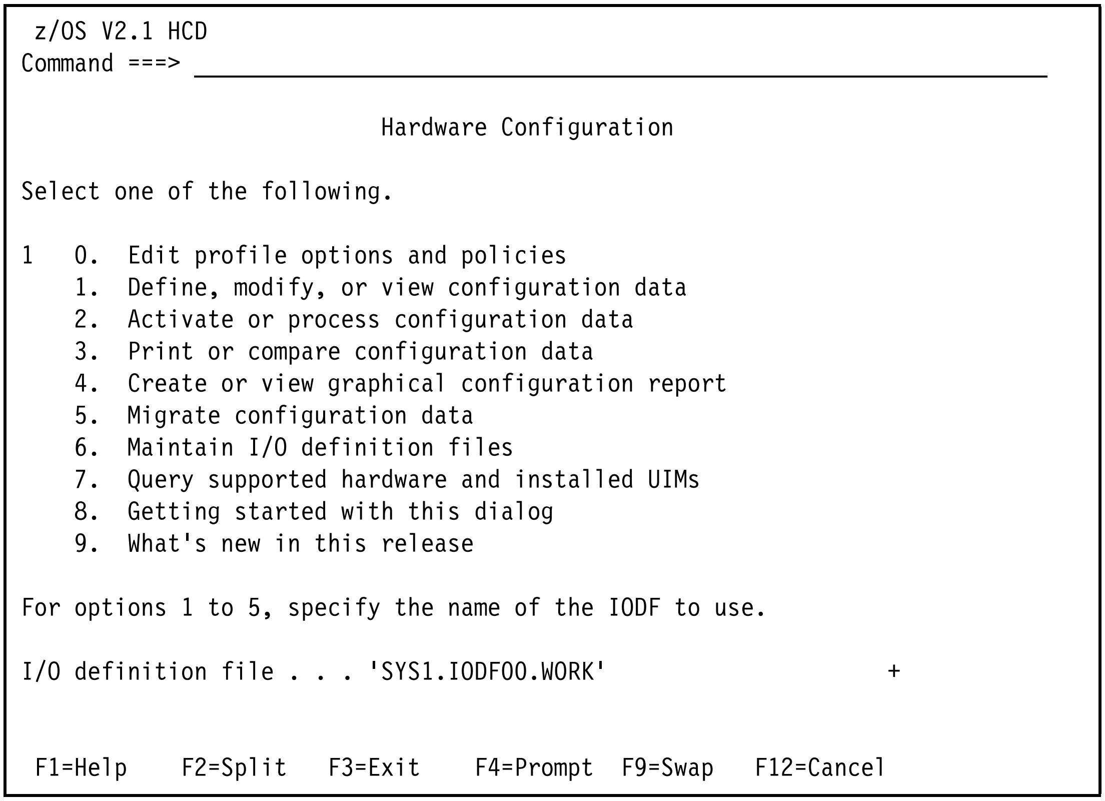
The Hardware Configuration Definition (HCD)) is used to define OSA to the I/O hardware configuration. Examples of the following definitions are included:

- Channel path
- Control unit
- Devices

3.2.1 Channel path definition

We created our definitions on a z/OS Version 2, Release 1 system. Starting from the HCD main menu panel (Figure 3-2), follow these steps:

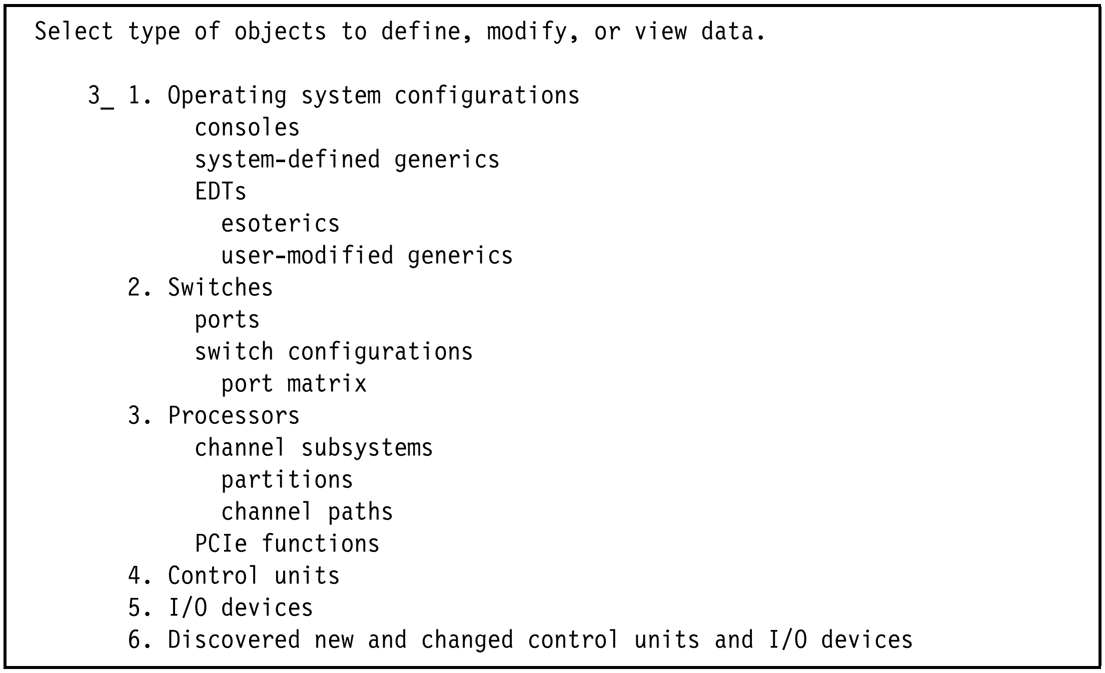
1. Select **1** (Define, modify, or view configuration data) and press **Enter**.



```
 z/OS V2.1 HCD
Command ===> ________________________________________________________________

                           Hardware Configuration

Select one of the following.

1   0.  Edit profile options and policies
    1.  Define, modify, or view configuration data
    2.  Activate or process configuration data
    3.  Print or compare configuration data
    4.  Create or view graphical configuration report
    5.  Migrate configuration data
    6.  Maintain I/O definition files
    7.  Query supported hardware and installed UIMs
    8.  Getting started with this dialog
    9.  What's new in this release

For options 1 to 5, specify the name of the IODF to use.

I/O definition file . . . 'SYS1.IODF00.WORK'                    +


 F1=Help    F2=Split   F3=Exit    F4=Prompt  F9=Swap   F12=Cancel
```

Figure 3-2 HCD main menu, Hardware Configuration panel

2. In the Define, Modify, or View Configuration Data panel (Figure 3-3), select **3** (Processors) and press **Enter**.

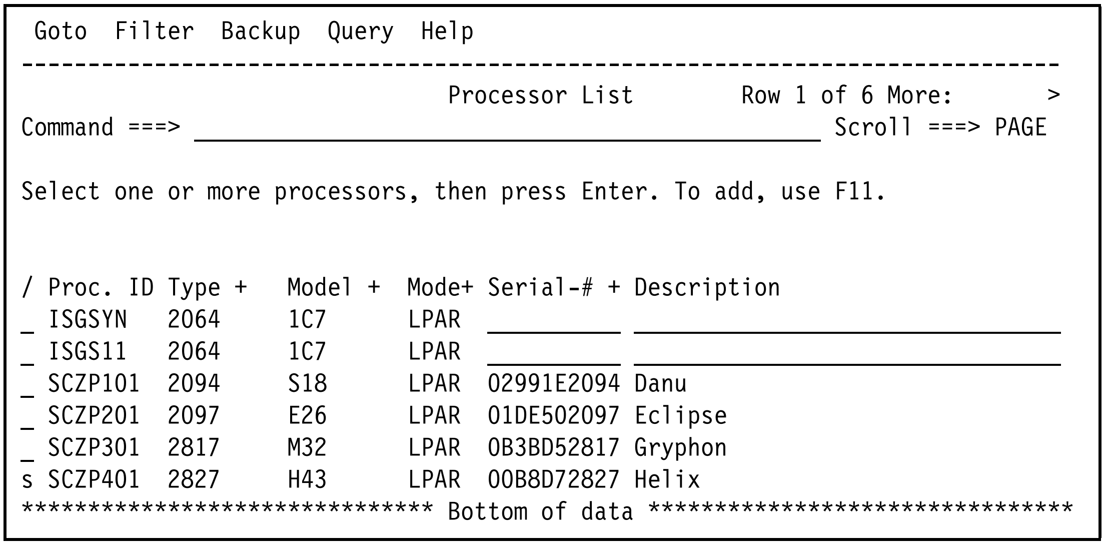


```
 Select type of objects to define, modify, or view data.

     3_ 1. Operating system configurations
             consoles
             system-defined generics
             EDTs
               esoterics
               user-modified generics
        2. Switches
             ports
             switch configurations
               port matrix
        3. Processors
             channel subsystems
               partitions
               channel paths
             PCIe functions
        4. Control units
        5. I/O devices
        6. Discovered new and changed control units and I/O devices
```

Figure 3-3 Define, Modify, or View Configuration Data panel

3. In the Processor List display (Figure 3-4), select the processor that you want to update by typing action code S next to the selected processor. Then press **Enter**.

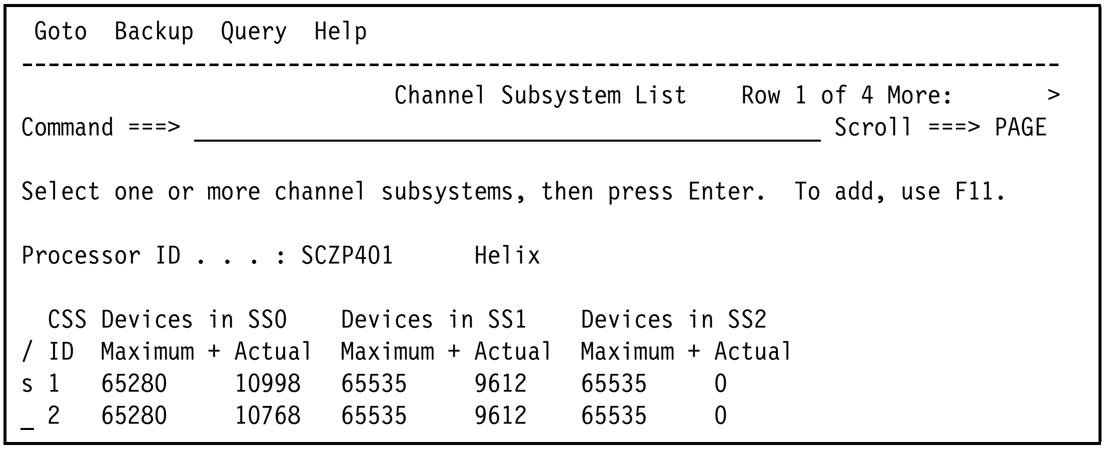
Note: We identify the panel selection options by using the action code, rather than the item number, to avoid confusion when a particular HCD menu changes.



```
 Goto  Filter  Backup  Query  Help
------------------------------------------------------------------------------
                                Processor List       Row 1 of 6 More:       >
Command ===> ______________________________________________ Scroll ===> PAGE

Select one or more processors, then press Enter. To add, use F11.


/ Proc. ID Type +   Model +  Mode+ Serial-# + Description
_ ISGSYN   2064     1C7      LPAR  __________ ________________________________
_ ISGS11   2064     1C7      LPAR  __________ ________________________________
_ SCZP101  2094     S18      LPAR  02991E2094 Danu
_ SCZP201  2097     E26      LPAR  01DE502097 Eclipse
_ SCZP301  2817     M32      LPAR  0B3BD52817 Gryphon
s SCZP401  2827     H43      LPAR  00B8D72827 Helix
******************************* Bottom of data ********************************
```

Figure 3-4 Processor List panel

4. In the Channel Subsystem List display (Figure 3-5 on page 19), type an S next to the channel subsystem that you want to work with, and then press **Enter**.



```
 Goto  Backup  Query  Help
------------------------------------------------------------------------------
                            Channel Subsystem List    Row 1 of 4 More:       >
Command ===> _______________________________________________ Scroll ===> PAGE

Select one or more channel subsystems, then press Enter.  To add, use F11.

Processor ID . . . : SCZP401      Helix

  CSS Devices in SS0    Devices in SS1    Devices in SS2
/ ID  Maximum + Actual  Maximum + Actual  Maximum + Actual
s 1   65280     10998   65535     9612    65535     0
_ 2   65280     10768   65535     9612    65535     0
```

Figure 3-5 Channel Subsystem List panel

5. In the Channel Path List panel, press **F11** to add a channel path.
6. In the Add Channel Path panel (Figure 3-6 on page 20), enter all of the required information:
   a. We defined `04` for the CHPID and `534` as the PCHID.
   b. For Channel path type, we specified `Tivoli Provisioning Manager for OS Deployment` because we are defining an OSA-Express5S 1000BASE-T, which supports Queued Direct I/O (QDIO).
   c. For Operation mode, we specify `SPAN` because the feature will be shared among LPARs and CSSs.
   d. For Description, use a meaningful description to serve as a reference in HCD.
   e. Press **Enter**.

Note: This example shows how to configure an OSA-Express5S 1000BASE-T feature. The process is identical for the other OSA-Express5S features:

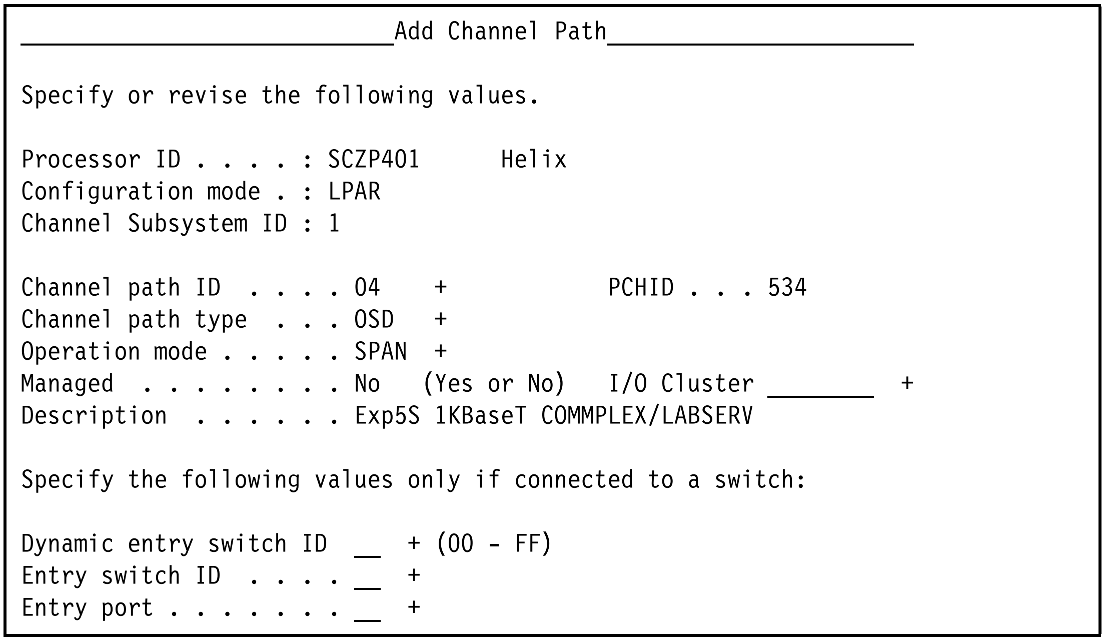
- The channel path type must be OSD for QDIO support or OSE for non-QDIO support. The OSA-Express5S 1000BASE-T features also support the Integrated Console Controller (ICC) for CHPID type OSC and the Intranode Management Network (INMN) for CHPID type OSM.
- You can specify the following Operation modes for channel paths:

  DED: Allows only one logical partition to access a channel path.

  REC: Allows only one logical partition at a time to access a channel path, but you can reconfigure that channel path from one logical partition to another. You reconfigure a channel path by using the IBM Multiple Virtual Storage (MVS™) **`CONFIG CHP(xx)`** command.

  SHR: Allows more than one logical partition to access a channel path simultaneously. You can specify shared mode only when the support level of the processor has multiple image facility (MIF) capability.

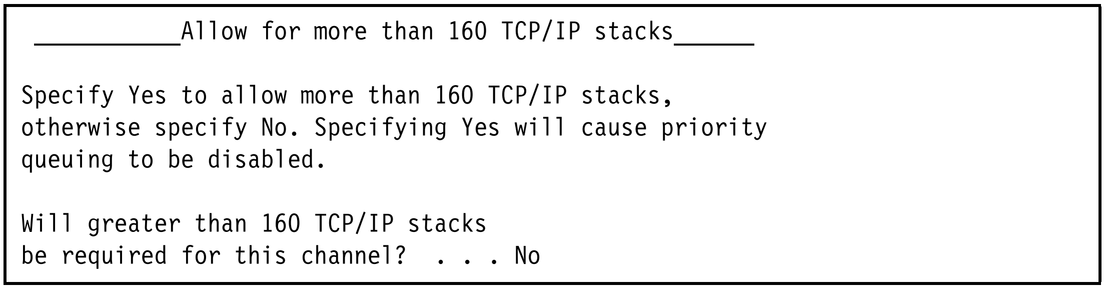
  SPAN: Allows partitions in more than one logical channel subsystem to share the same channel. Not all types of channel paths can be defined as *spanned*.



```
____________________________Add Channel Path_______________________

Specify or revise the following values.

Processor ID . . . . : SCZP401      Helix
Configuration mode . : LPAR
Channel Subsystem ID : 1

Channel path ID  . . . . 04    +           PCHID . . . 534
Channel path type  . . . OSD   +
Operation mode . . . . . SPAN  +
Managed  . . . . . . . . No   (Yes or No)   I/O Cluster ________  +
Description  . . . . . . Exp5S 1KBaseT COMMPLEX/LABSERV

Specify the following values only if connected to a switch:

Dynamic entry switch ID  __  + (00 - FF)
Entry switch ID  . . . . __  +
Entry port . . . . . . . __  +
```

Figure 3-6 Add Channel Path panel

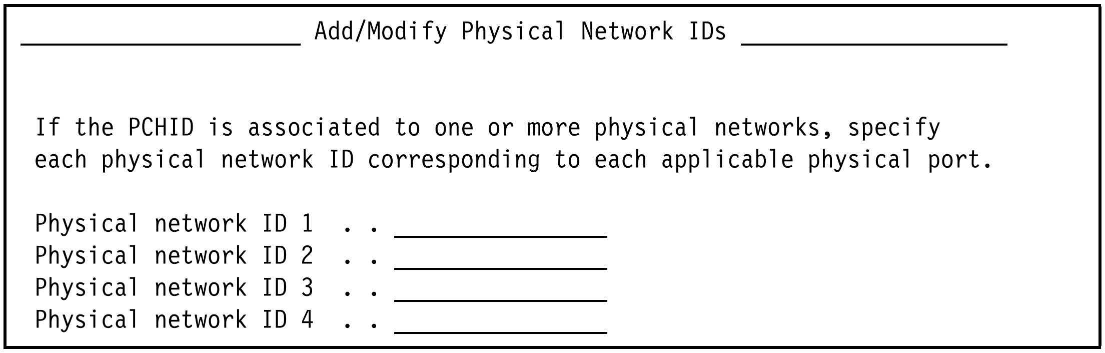
7. In the next display (Figure 3-7), specify whether you want more than 160 TCP/IP stacks. For more information see the *IBM System z Connectivity Handbook*, SG24-5444.



```
 ___________Allow for more than 160 TCP/IP stacks______

Specify Yes to allow more than 160 TCP/IP stacks,
otherwise specify No. Specifying Yes will cause priority
queuing to be disabled.

Will greater than 160 TCP/IP stacks
be required for this channel?  . . . No
```

Figure 3-7 Allow TCP/IP stacks

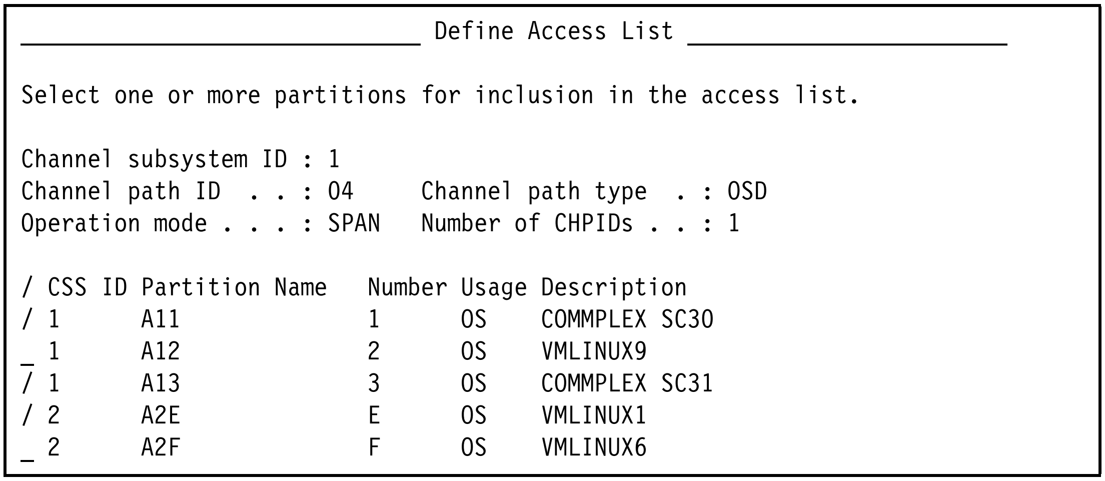
8. If you are working on Peripheral Component Interconnect Express (PCIe) functions (RDMA over Converged Ethernet, or RoCE), you can specify the physical network ID for the PCHID in the display shown in Figure 3-8. If not, you can press **Enter.**



```
_____________________ Add/Modify Physical Network IDs ____________________


 If the PCHID is associated to one or more physical networks, specify
 each physical network ID corresponding to each applicable physical port.

 Physical network ID 1  . . ________________
 Physical network ID 2  . . ________________
 Physical network ID 3  . . ________________
 Physical network ID 4  . . ________________
```

Figure 3-8 Add/Modify Physical Network IDs panel

9. Complete the Define Access List selections for the partitions that are sharing the channel, as shown in Figure 3-9. In this example, two partitions share the OSA CHPID.



```
______________________________ Define Access List ________________________

Select one or more partitions for inclusion in the access list.

Channel subsystem ID : 1
Channel path ID  . . : 04     Channel path type  . : OSD
Operation mode . . . : SPAN   Number of CHPIDs . . : 1

/ CSS ID Partition Name   Number Usage Description
/ 1      A11              1      OS    COMMPLEX SC30
_ 1      A12              2      OS    VMLINUX9
/ 1      A13              3      OS    COMMPLEX SC31
/ 2      A2E              E      OS    VMLINUX1
_ 2      A2F              F      OS    VMLINUX6
```

Figure 3-9 Define Access List panel

10. Review the partition names and descriptions. You have two choices:

    a. Select the ones to include, and press **Enter**.
    b. If you do not want any partitions in that candidate list, press **Enter**.

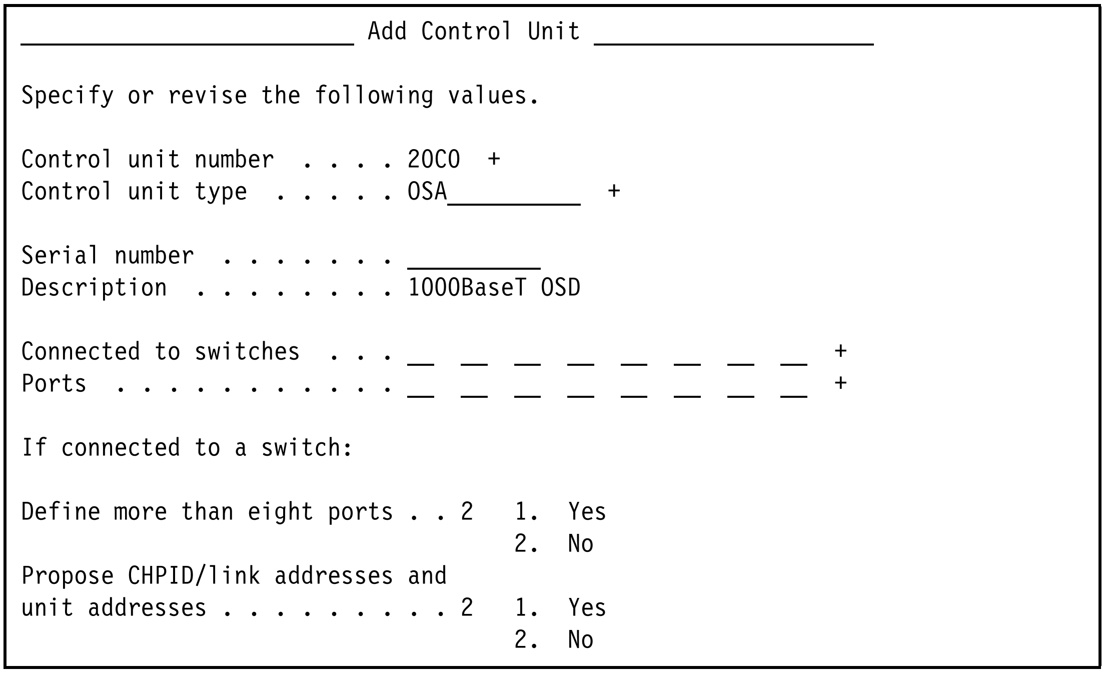
The Channel Path List panel is then displayed.

3.2.2 Control unit definition

From the Channel Path List panel, follow these steps:

1. Type an `S` next to the CHPID that you just defined (04 in our example), and press **Enter**.
2. Press **F11** to add a control unit.
3. In the Add Control Unit panel (Figure 3-10 on page 22), enter the required information:

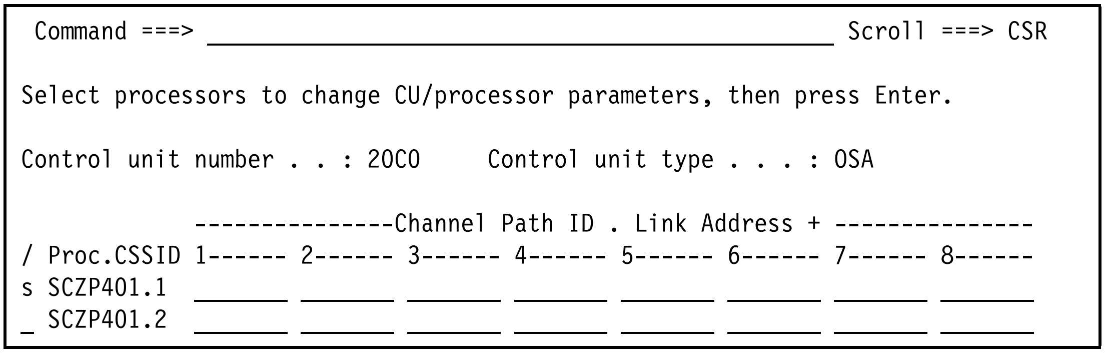
    a. For Control unit number, we chose `20C0`.
    b. Control unit type must be `OSA`.
    c. Press **Enter**.



```
_________________________ Add Control Unit _____________________

Specify or revise the following values.

Control unit number  . . . . 20C0  +
Control unit type  . . . . . OSA__________  +

Serial number  . . . . . . . __________
Description  . . . . . . . . 1000BaseT OSD

Connected to switches  . . . __  __  __  __  __  __  __  __  +
Ports  . . . . . . . . . . . __  __  __  __  __  __  __  __  +

If connected to a switch:

Define more than eight ports . . 2   1.  Yes
                                     2.  No
Propose CHPID/link addresses and
unit addresses . . . . . . . . . 2   1.  Yes
                                     2.  No
```

Figure 3-10 Add Control Unit panel (Part 1 of 2)

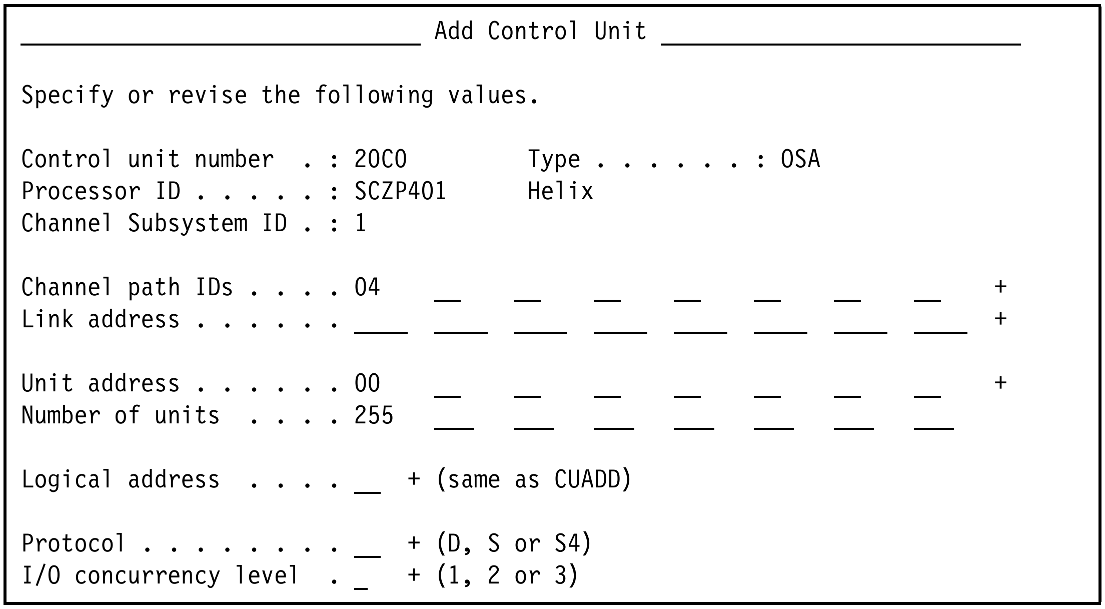
4. As shown in Figure 3-11, type an `S` next to the processor for the control unit. Then press **Enter**.



```
 Command ===> _______________________________________________ Scroll ===> CSR

Select processors to change CU/processor parameters, then press Enter.

Control unit number . . : 20C0     Control unit type . . . : OSA

             ---------------Channel Path ID . Link Address + ---------------
/ Proc.CSSID 1------ 2------ 3------ 4------ 5------ 6------ 7------ 8------
s SCZP401.1  _______ _______ _______ _______ _______ _______ _______ _______
_ SCZP401.2  _______ _______ _______ _______ _______ _______ _______ _______
```

Figure 3-11 Processor selection panel

5. Figure 3-12 shows the OSA control unit information. Set the Channel path IDs to the CHPID number that you just defined (`04` in our example). **Note:** The Unit address must be set to `00`, and the number of units must be `255`. Then press **Enter**.



```
 ______________________________ Add Control Unit ___________________________

 Specify or revise the following values.

 Control unit number  . : 20C0        Type . . . . . . : OSA
 Processor ID . . . . . : SCZP401     Helix
 Channel Subsystem ID . : 1

 Channel path IDs . . . . 04   __   __   __   __   __   __   __   +
 Link address . . . . . . ____ ____ ____ ____ ____ ____ ____ ____ +

 Unit address . . . . . . 00   __   __   __   __   __   __   __   +
 Number of units  . . . . 255  ___  ___  ___  ___  ___  ___  ___

 Logical address  . . . . __  + (same as CUADD)

 Protocol . . . . . . . . __  + (D, S or S4)
 I/O concurrency level  . _   + (1, 2 or 3)
```

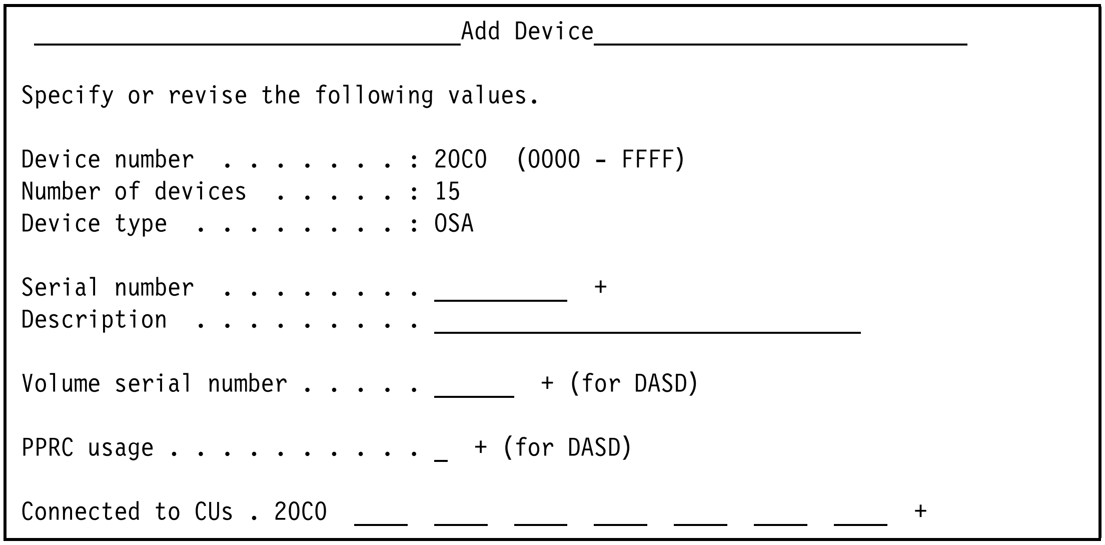
Figure 3-12 Add Control Unit panel (Part 2 of 2)

6. Press Enter again to return to the Control Unit List panel.

3.2.3 Device definition

From the Control Unit List panel, follow these steps:

1. Type an `S` to select the control unit. Then press **Enter**.
2. Press **F11** to add devices.
3. In the Add Device panel, enter the required information as shown in Figure 3-13 on page 24:
   a. For Device number, we chose `20C0`.
   b. For Number of devices, we chose `15`.
   c. Device type must be `OSA`.
   d. Press **Enter**.



```
 ________________________________Add Device____________________________

Specify or revise the following values.

Device number  . . . . . . . : 20C0  (0000 - FFFF)
Number of devices  . . . . . : 15
Device type  . . . . . . . . : OSA

Serial number  . . . . . . . . __________  +
Description  . . . . . . . . . ________________________________

Volume serial number . . . . . ______  + (for DASD)

PPRC usage . . . . . . . . . . _  + (for DASD)

Connected to CUs . 20C0  ____  ____  ____  ____  ____  ____  ____  +
```

Figure 3-13 Add Device panel

How many devices to define

The answer depends on the CHPID type, the number of TCP/IP stacks, the use the OSA-Express Network Traffic Analyzer, and the SNA definitions that are required. Consider the following for the number of devices:

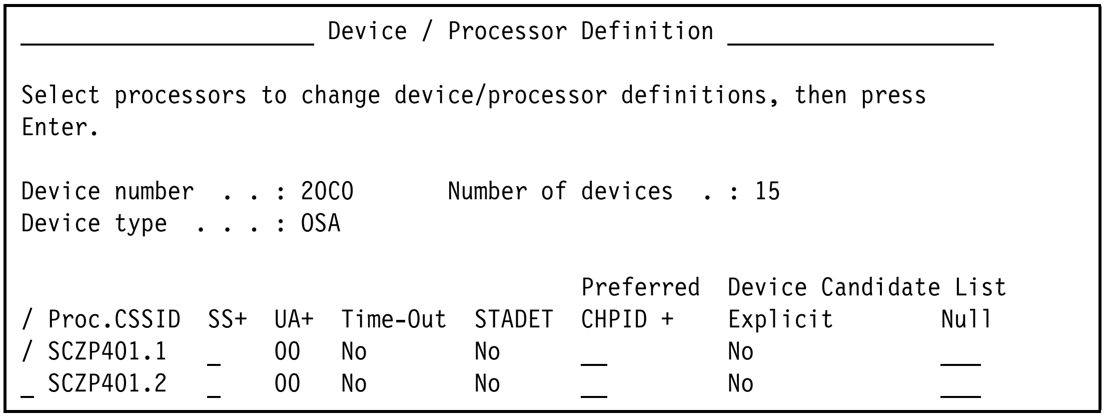
- Any OSD, OSX, or OSM CHPID (QDIO mode) requires at least three devices for each TCP/IP stack: read, write, and data path. For z/OS, only the first TCP/IP stack requires three devices. Any additional TCP/IP stack requires only one device (data path).

  If you define both IPv4 and IPv6 with `INTERFACE` statements, z/OS will use two data devices, one for each protocol.

- If you plan to use the OSA-Express Network Traffic Analyzer, you need one more data device, which is used to transmit the captured trace data to TCP/IP.
- Any OSE CHPID requires two devices (read and write) for each TCP/IP. SNA requires one device.

4. A panel is displayed in which you can edit information for the specific devices. Make any changes that you need, and then press **Enter**.

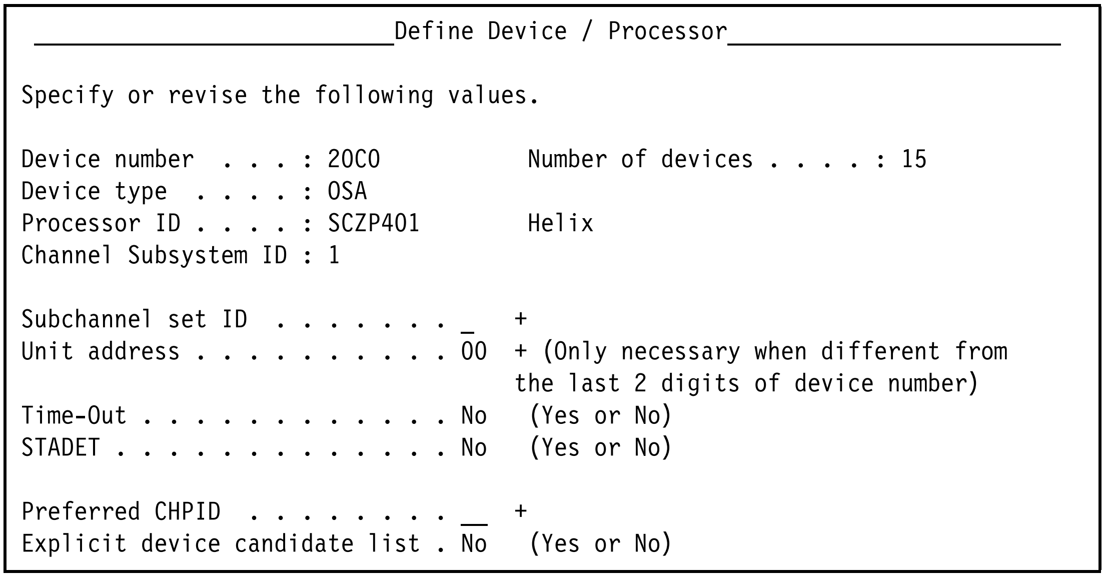
5. When the Device / Processor Definition panel (Figure 3-14) displays, type a slash mark (/) next to the processors that you want to select, and then press **Enter**.



```
______________________ Device / Processor Definition ____________________

Select processors to change device/processor definitions, then press
Enter.

Device number  . . : 20C0      Number of devices  . : 15
Device type  . . . : OSA

                                       Preferred  Device Candidate List
/ Proc.CSSID  SS+  UA+  Time-Out  STADET  CHPID +    Explicit       Null
/ SCZP401.1   _    00   No        No      __         No             ___
_ SCZP401.2   _    00   No        No      __         No             ___
```

Figure 3-14 Device / Processor Definition panel

6. In the panel shown in Figure 3-15, you can change the starting unit address. Verify the value (00 is required only with the default OAT, for CHPID type OSE), and then press **Enter**.

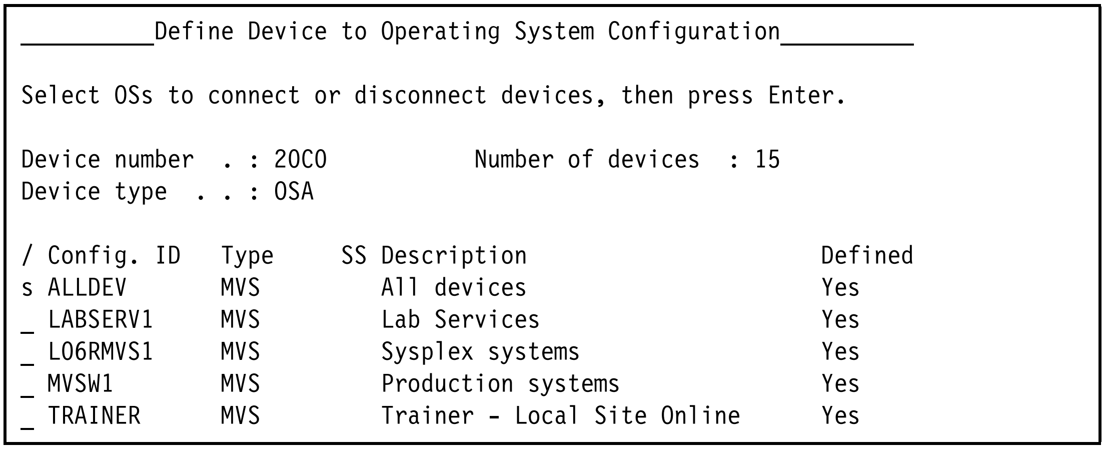


```
 ___________________________Define Device / Processor_________________________

Specify or revise the following values.

Device number  . . . : 20C0          Number of devices . . . . : 15
Device type  . . . . : OSA
Processor ID . . . . : SCZP401       Helix
Channel Subsystem ID : 1

Subchannel set ID  . . . . . . . _   +
Unit address . . . . . . . . . . 00  + (Only necessary when different from
                                     the last 2 digits of device number)
Time-Out . . . . . . . . . . . . No   (Yes or No)
STADET . . . . . . . . . . . . . No   (Yes or No)

Preferred CHPID  . . . . . . . . __  +
Explicit device candidate list . No   (Yes or No)
```

Figure 3-15 Define Device / Processor panel

7. Press Enter again.

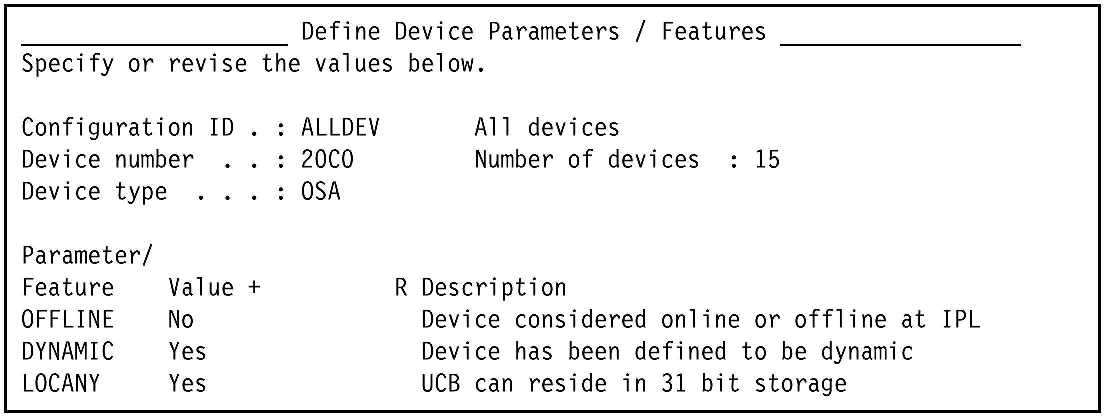
8. In the Define Device to Operating System Configuration panel (Figure 3-16 on page 26), type an S next to the operating system to which you want to connect the devices. Then press Enter.



```
__________Define Device to Operating System Configuration__________

Select OSs to connect or disconnect devices, then press Enter.

Device number  . : 20C0          Number of devices  : 15
Device type  . . : OSA

/ Config. ID   Type     SS Description                     Defined
s ALLDEV       MVS         All devices                     Yes
_ LABSERV1     MVS         Lab Services                    Yes
_ L06RMVS1     MVS         Sysplex systems                 Yes
_ MVSW1        MVS         Production systems              Yes
_ TRAINER      MVS         Trainer - Local Site Online     Yes
```

Figure 3-16 Define Device to Operating System Configuration panel

9. In the resulting display (Figure 3-17), press Enter to accept the default values.



```
____________________ Define Device Parameters / Features __________________
Specify or revise the values below.

Configuration ID . : ALLDEV       All devices
Device number  . . : 20C0         Number of devices  : 15
Device type  . . . : OSA

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

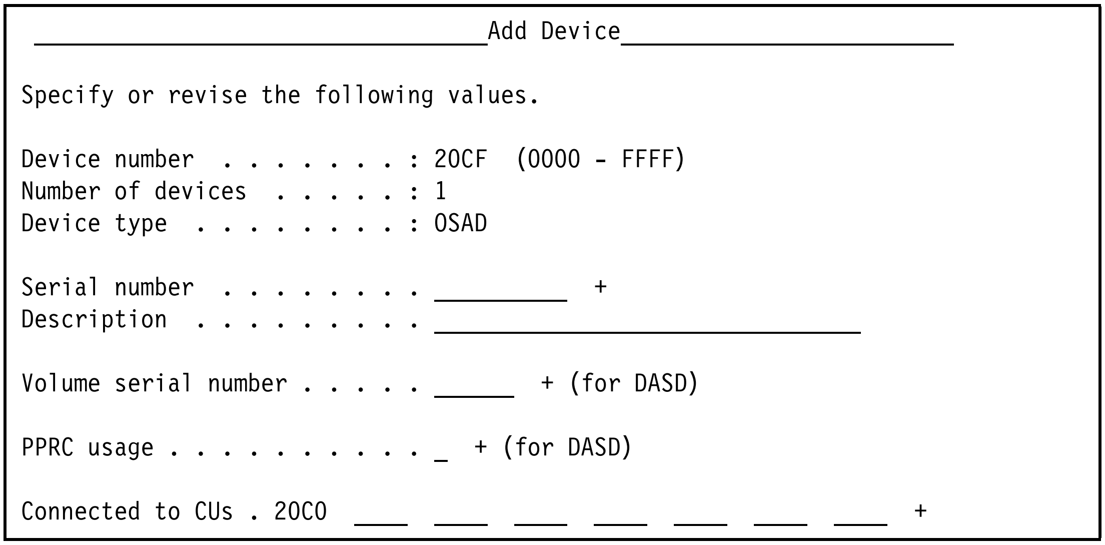
Figure 3-17 Define Device Parameters / Features panel

10. Repeat the process for each operating system, as necessary.

You should now see the Device List display. If you plan to use OSA/SF, you need to define an OSAD device.

11. Press **F11** to add a new device.

12. In the Add Device display, define the new device as shown in Figure 3-18.

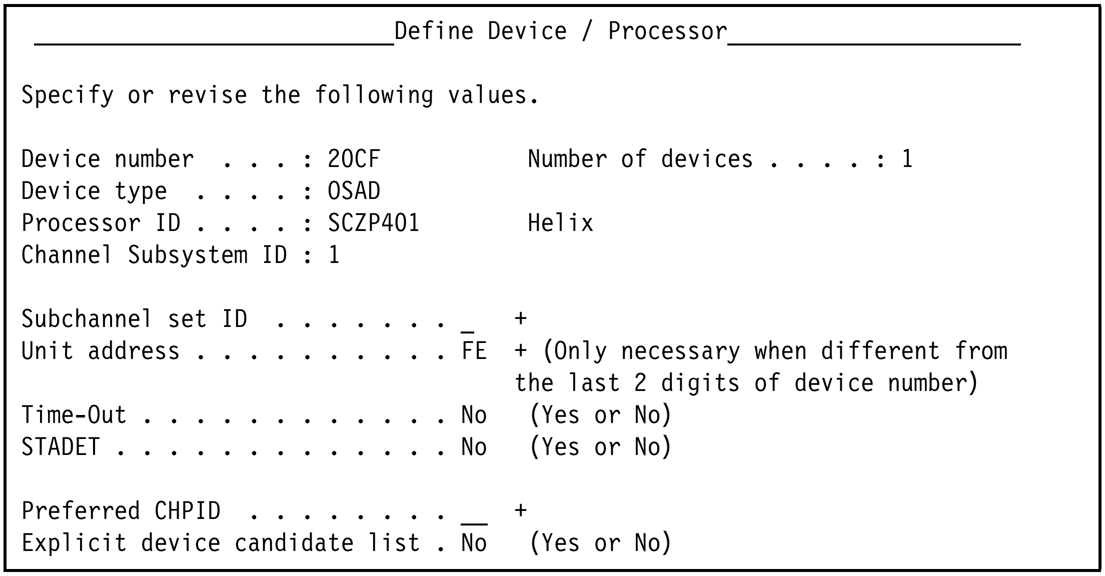


```
 _________________________________Add Device________________________

Specify or revise the following values.

Device number  . . . . . . . : 20CF  (0000 - FFFF)
Number of devices  . . . . . : 1
Device type  . . . . . . . . : OSAD

Serial number  . . . . . . . . __________  +
Description  . . . . . . . . . ________________________________

Volume serial number . . . . . ______  + (for DASD)

PPRC usage . . . . . . . . . . _  + (for DASD)

Connected to CUs . 20C0  ____  ____  ____  ____  ____  ____  ____  +
```

Figure 3-18 OSAD definition (Part 1 of 2), Add Device panel

13. Repeat the process as you did for the other devices, except that you must associate the unit address (FE) with the OSAD Device number (20CF), as shown in Figure 3-19.

14. When you have finished adding the required information, press **Enter**.



```
 ___________________________Define Device / Processor______________________

Specify or revise the following values.

Device number  . . . : 20CF          Number of devices . . . . : 1
Device type  . . . . : OSAD
Processor ID . . . . : SCZP401       Helix
Channel Subsystem ID : 1

Subchannel set ID  . . . . . . . _   +
Unit address . . . . . . . . . . FE  + (Only necessary when different from
                                     the last 2 digits of device number)
Time-Out . . . . . . . . . . . . No   (Yes or No)
STADET . . . . . . . . . . . . . No   (Yes or No)

Preferred CHPID  . . . . . . . . __  +
Explicit device candidate list . No   (Yes or No)
```

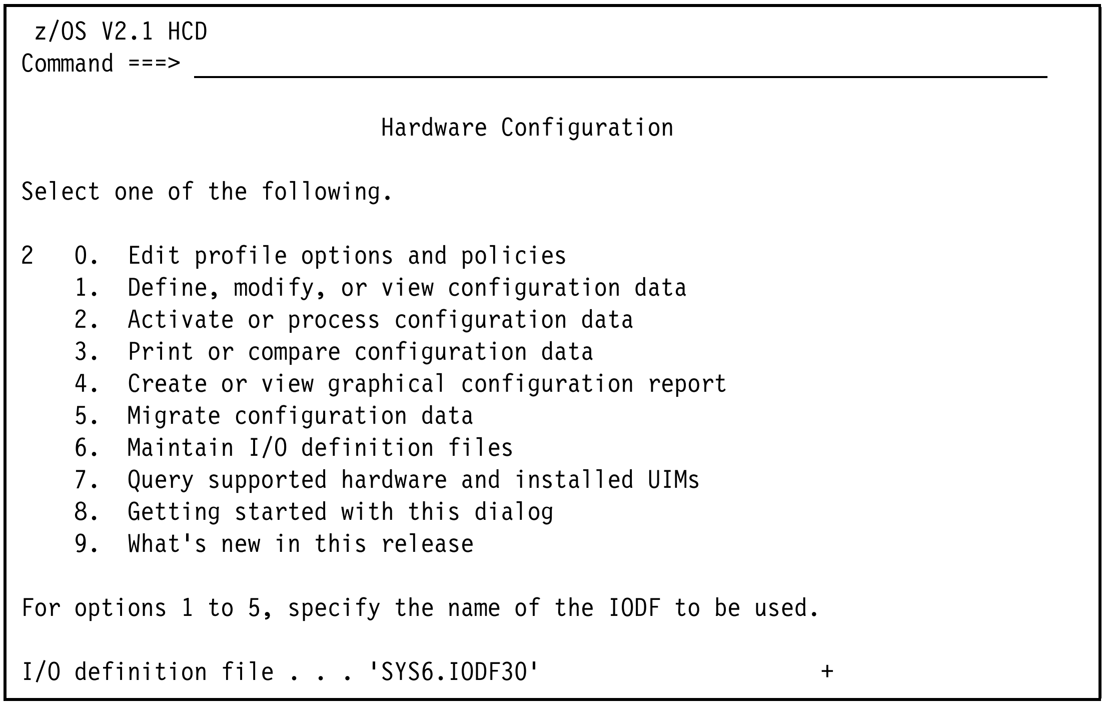
Figure 3-19 OSAD definition (Part 2 of 2), Define Device / Processor panel

3.2.4 Generating the IOCDS input from the HCD

From the HCD, you can generate input to use for the input/output configuration data set (IOCDS). It is used to write the macro definitions to the System z server and can be used for quick debugging purposes. Before you do that, you need to build the production input/output definition file (IODF) by using the HCD. The production IODF is required to create the IOCP input data set.

After that, you can generate input for IOCDS by following these steps:

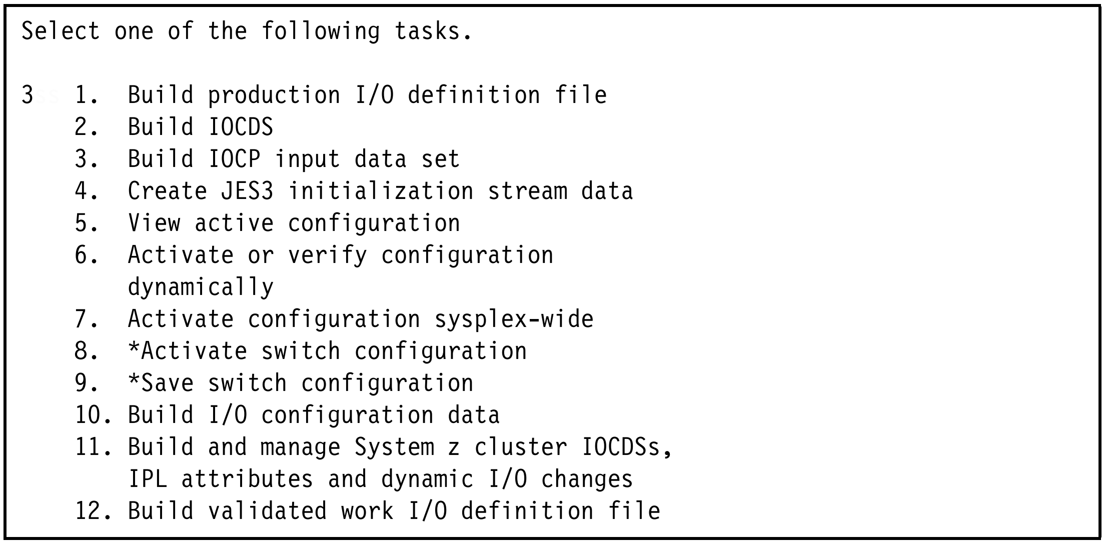
1. From the HCD main menu (Figure 3-20), enter your production IODF data set at the bottom of the window. In our example, we use `SYS6.IODF30`. Then, select **2** and press **Enter.**



```
 z/OS V2.1 HCD
Command ===> ________________________________________________________________

                           Hardware Configuration

Select one of the following.

2   0.  Edit profile options and policies
    1.  Define, modify, or view configuration data
    2.  Activate or process configuration data
    3.  Print or compare configuration data
    4.  Create or view graphical configuration report
    5.  Migrate configuration data
    6.  Maintain I/O definition files
    7.  Query supported hardware and installed UIMs
    8.  Getting started with this dialog
    9.  What's new in this release

For options 1 to 5, specify the name of the IODF to be used.

I/O definition file . . . 'SYS6.IODF30'                    +
```

Figure 3-20   HCD, Hardware Configuration panel

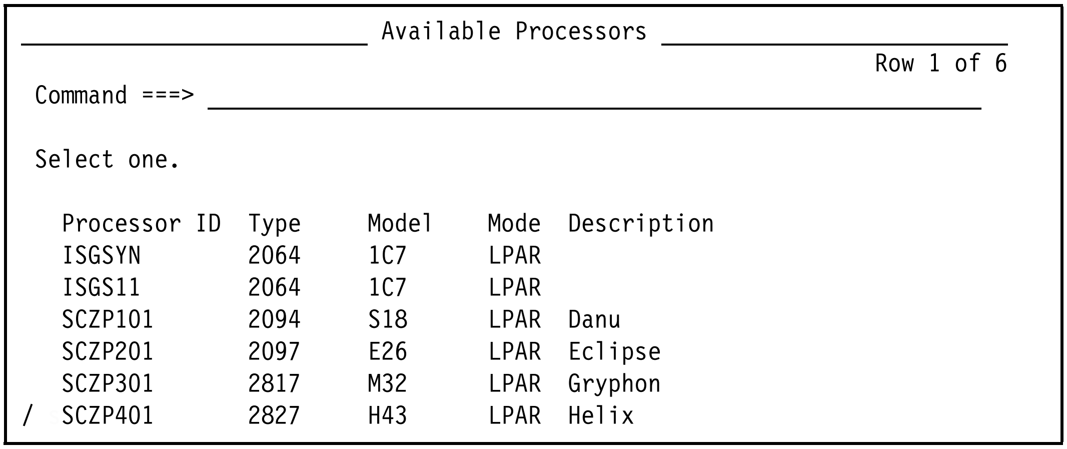
2. From the next display (Figure 3-21), select **3** and press **Enter**.



```
Select one of the following tasks.

3   1.  Build production I/O definition file
    2.  Build IOCDS
    3.  Build IOCP input data set
    4.  Create JES3 initialization stream data
    5.  View active configuration
    6.  Activate or verify configuration
        dynamically
    7.  Activate configuration sysplex-wide
    8.  *Activate switch configuration
    9.  *Save switch configuration
    10. Build I/O configuration data
    11. Build and manage System z cluster IOCDSs,
        IPL attributes and dynamic I/O changes
    12. Build validated work I/O definition file
```

Figure 3-21   Activate or Process Configuration Data panel

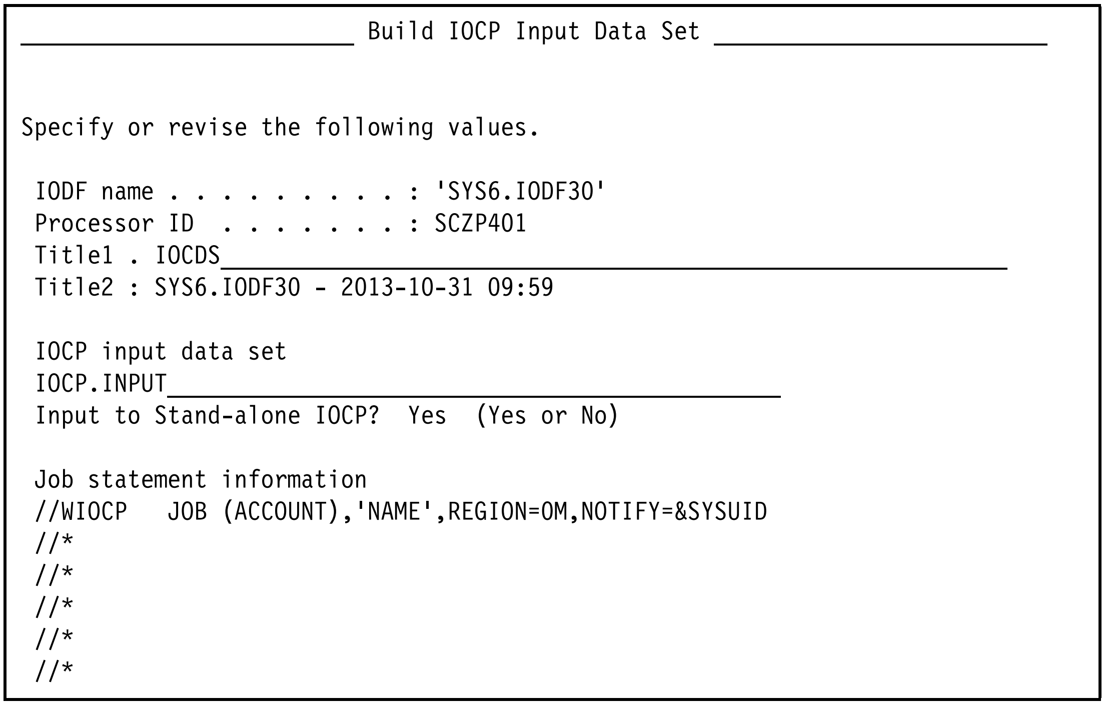
3. Select the processor and press Enter (see Figure 3-22 on page 29).



```
_________________________ Available Processors _________________________
                                                              Row 1 of 6
 Command ===> ___________________________________________________________

 Select one.

   Processor ID  Type     Model    Mode  Description
   ISGSYN        2064     1C7      LPAR
   ISGS11        2064     1C7      LPAR
   SCZP101       2094     S18      LPAR  Danu
   SCZP201       2097     E26      LPAR  Eclipse
   SCZP301       2817     M32      LPAR  Gryphon
/  SCZP401       2827     H43      LPAR  Helix
```

Figure 3-22 Available Processors panel

4. You will get a Build IOCP Input Data Set panel (Figure 3-23) to enter the required data. You can use any title and data set. The IOCP Input Data Set field is the target data set where the job writes the input IOCDS. We use the following values in our example:
   - Title1: `IOCDS`
   - IOCP Input Data Set: `IOCP.INPUT`



```
_________________________ Build IOCP Input Data Set _________________________


Specify or revise the following values.

 IODF name . . . . . . . . . : 'SYS6.IODF30'
 Processor ID  . . . . . . . : SCZP401
 Title1 . IOCDS___________________________________________________________
 Title2 : SYS6.IODF30 - 2013-10-31 09:59

 IOCP input data set
 IOCP.INPUT_______________________________________________
 Input to Stand-alone IOCP?  Yes  (Yes or No)

 Job statement information
 //WIOCP   JOB (ACCOUNT),'NAME',REGION=0M,NOTIFY=&SYSUID
 //*
 //*
 //*
 //*
 //*
```

Figure 3-23 Build IOCP Input Data Set panel

5. Example 3-1 on page 30 shows IOCDS input that was generated by the HCD for spanned OSA CHPIDs running in QDIO mode.

Example 3-1 IOCDS generated by HCD

```
ID    MSG1='IOCDS',MSG2='SYS6.IODF30 - 2013-10-31 09:59',     *
      SYSTEM=(2827,1),LSYSTEM=SCZP401,                        *
      TOK=('SCZP401',00800003B8D72827095916150113304F00000000,*
      00000000,'13-10-31','09:59:16','SYS6','IODF30')
RESOURCE PARTITION=((CSS(0),(A0A,A),(A0B,B),(A0C,C),(A0D,D),(A*
      0E,E),(A0F,F),(A01,1),(A02,2),(A03,3),(A04,4),(A05,5),(A*
      06,6),(A07,7),(A08,8),(A09,9)),(CSS(1),(A1A,A),(A1B,B),(*
      A1C,C),(A1D,D),(A1E,E),(A1F,F),(A11,1),(A12,2),(A13,3),(*
      A14,4),(A15,5),(A16,6),(A17,7),(A18,8),(A19,9)),(CSS(2),*
      (A2A,A),(A2B,B),(A2C,C),(A2D,D),(A2E,E),(A2F,F),(A21,1),*
      (A22,2),(A23,3),(A24,4),(A25,5),(A26,6),(A27,7),(A28,8),*
      (A29,9)),(CSS(3),(A3D,D),(A3E,E),(A3F,F),(A31,1),(A32,2)*
      ,(A33,3),(A34,4),(A35,5),(*,6),(*,7),(*,8),(*,9),(*,A),(*
      *,B),(*,C)))
CHPID PATH=(CSS(0,1,2),04),SHARED,                            *
      PARTITION=((CSS(0),(A03),(=)),(CSS(1),(A11,A13,A15,A16,A*
      18),(=)),(CSS(2),(A2E),(=))),PCHID=534,TYPE=OSD
CHPID PATH=(CSS(1,2),07),SHARED,                              *
      PARTITION=((CSS(1),(A11,A13,A16,A18),(=)),(CSS(2),(A2E),*
      (=))),PCHID=570,TYPE=OSD
CNTLUNIT CUNUMBR=20C0,                                        *
      PATH=((CSS(0),04),(CSS(1),04),(CSS(2),04)),UNIT=OSA
IODEVICE ADDRESS=(20C0,015),UNITADD=00,CUNUMBR=(20C0),UNIT=OSA
IODEVICE ADDRESS=(20CF,001),UNITADD=FE,CUNUMBR=(20C0),        *
      UNIT=OSAD
CNTLUNIT CUNUMBR=2160,PATH=((CSS(1),07),(CSS(2),07)),UNIT=OSA
IODEVICE ADDRESS=(2160,015),UNITADD=00,CUNUMBR=(2160),UNIT=OSA
IODEVICE ADDRESS=(216F,001),UNITADD=FE,CUNUMBR=(2160),        *
      UNIT=OSAD
```

3.2.5 Dynamic reconfiguration

Dynamic reconfiguration management is the ability to select a new I/O configuration during normal processing, without the need to do a power-on reset (POR) of the hardware nor an initial program load (IPL) of the z/OS operating system. The ability of the HCD to provide equivalent hardware and software I/O definitions and to detect when they are not in sync is essential for dynamic I/O reconfiguration management. HCD compares both the old and the new configuration and informs the hardware and software about the differences. You can add, delete, and modify definitions for channel paths, control units, and I/O devices without having to do a POR or an IPL.

A system programmer (or other authorized person) can use the HCD option to “Activate or verify configuration dynamically” or the ACTIVATE operator command (**`ACTIVATE IODF=xx`**) to make changes to a running configuration. On the HCD panel, specify the name and volume serial number (if applicable) for the production IODF.

4

QDIO mode for the IBM z/OS operating system

This chapter covers the implementation steps to establish IBM z/OS network connectivity with an IBM Open Systems Adapter (OSA) channel path identifier (CHPID), using Queued Direct I/O (QDIO) mode.

Although the Open Systems Adapter Support Facility (OSA/SF) is not required because all definitions are set dynamically, use OSA/SF for monitoring and controlling the OSA port.

For more information about installing and using OSA/SF, see Appendix E, “Using the Open Systems Adapter Support Facility” on page 191.

The information in this chapter covers the following topics:

- 4.1, “QDIO environment” on page 32
- 4.2, “Hardware Configuration Definition” on page 32
- 4.3, “Missing-interrupt handler for QDIO” on page 32
- 4.4, “Customizing the z/OS network environment” on page 33
- 4.5, “Activation” on page 38
- 4.6, “Relevant status displays” on page 39
- 4.7, “Systems Network Architecture support for QDIO mode” on page 42

4.1 QDIO environment

Figure 4-1 shows the z/OS operating system environment that we describe in this chapter.

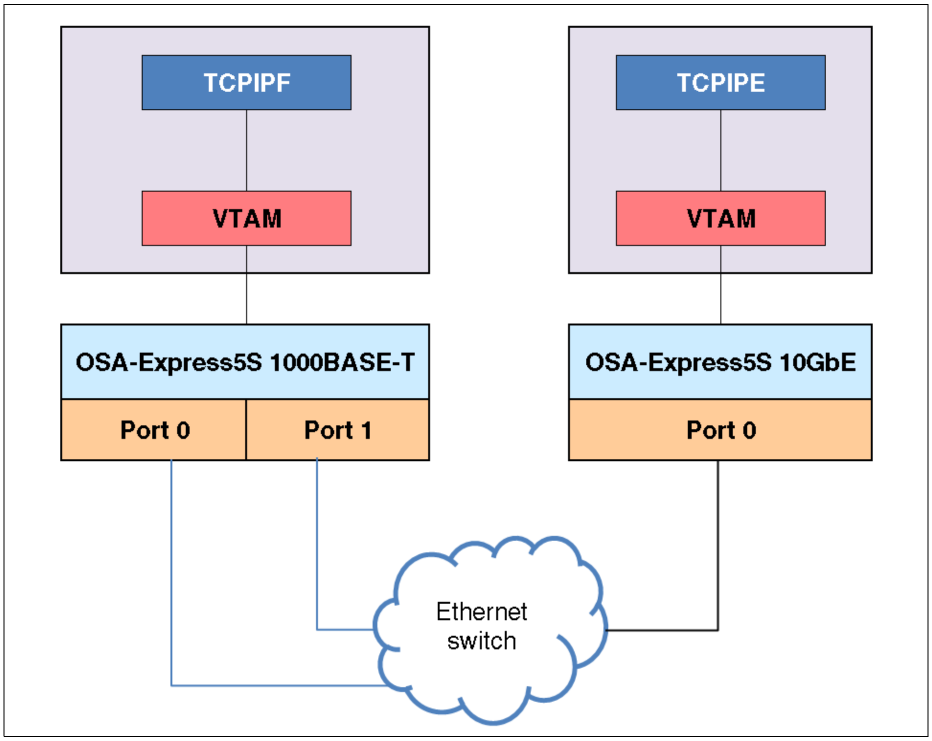


Figure 4-1 QDIO mode example for z/OS

4.2 Hardware Configuration Definition

The OSA CHPID, the control unit, and the OSA devices must be defined to the System z hardware, either by coding suitable IOCP statements or through the Hardware Configuration Definition (HCD). See Chapter 3, “Hardware configuration definitions” on page 15, for the procedure to create the definitions.

The necessary definitions for CHPID 04 and CHPID 07 are also shown in the IOCDS format in 3.2.4, “Generating the IOCDS input from the HCD” on page 27.

4.3 Missing-interrupt handler for QDIO

The WRITE devices (as defined in the transport resource list element, or TRLE) must have a missing-interrupt handler (MIH) value of at least 15 seconds (or 30 seconds if it is running as a guest system on z/VM).

To determine the current missing-interrupt handler (MIH) value for the device (20C1 in our example), enter this command:

```
D IOS,MIH,DEV=20C1
```

To dynamically change the MIH value, enter this command:

```
SETIOS MIH,DEV=20C1,TIME=00:15
```

To set these values at IPL time, update the IECIOSxx member in PARMLIB.

Important: On a multiple subchannel device, the MIH is automatically configured as OFF by Virtual Telecommunications Access Method (VTAM) on the READ subchannel or subchannels. Setting an MIH value of 0 (zero) for a TCP/IP or VTAM WRITE device disables MIH on those devices.

4.4 Customizing the z/OS network environment

Figure 4-2 shows the network configuration, which consists of two z/OS logical partitions (LPARs) that share two OSA devices: OSA-Express5S 10GbE with a single port and OSA-Express5S 1000BASE-T with two ports.

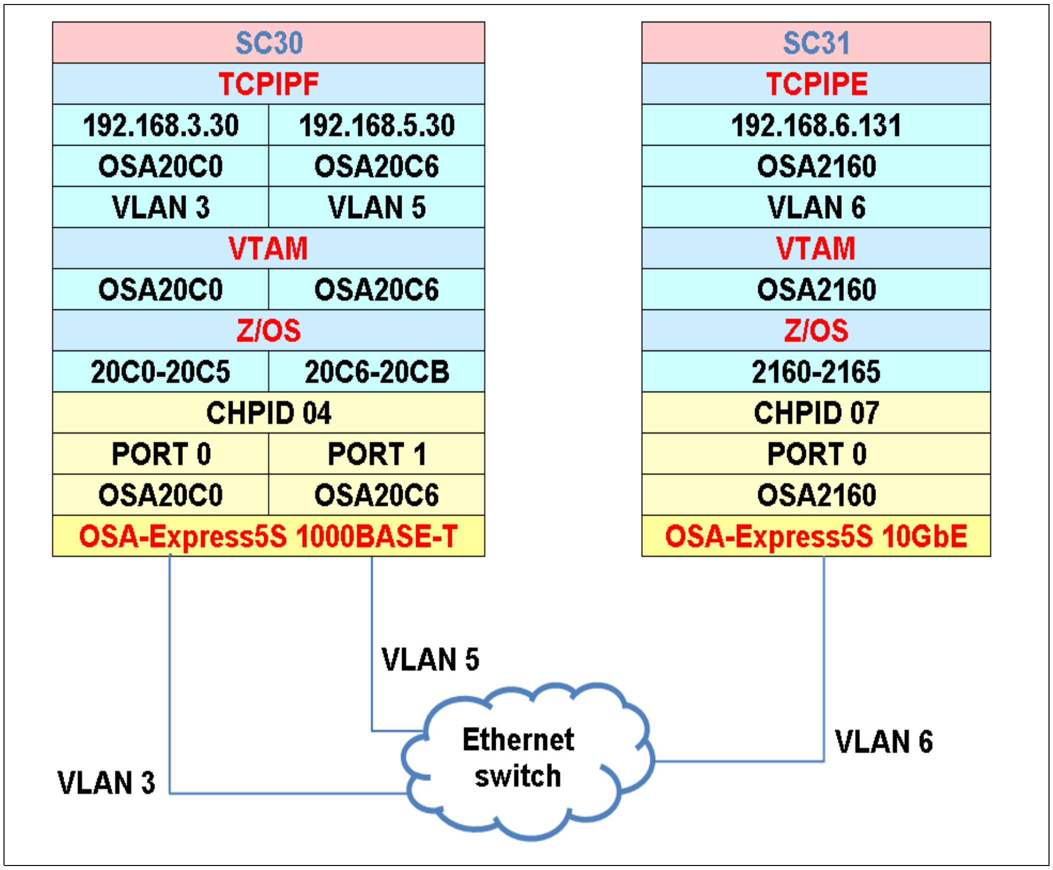


Figure 4-2 Network configuration

In our environment, we are using the first CHPID of each feature with the associated ports (0 and 1) on each OSA-Express5S 1000BASE-T feature for demonstration purposes only. In a production environment, use both CHPIDs and connect them to at least two different Ethernet switches to avoid a single point of failure.

4.4.1 Defining OSA devices to the z/OS Communications Server for QDIO

To define an OSD OSA device for the z/OS Communications Server by using QDIO, you need to define a QDIO TRLE. Example 4-1 shows the TRLE definition for our OSA-Express5S 1000BASE-T feature related to CHPID 04 (port 0 and 1) and OSA-Express5S 10GbE related to CHPID 07 (port 0). For an OSX device, the TRLE is dynamically generated.

VTAM definitions (TRL major node)

Example 4-1 shows the VTAM transport resource list (TRL) major node definition that is required for TCPIPE and TCPIPF.

Example 4-1 VTAM TRL major node that is related to TCPIPE and TCPIPF

```
OSA20C0 VBUILD TYPE=TRL
*
* QDIO TRLE FOR OSA-Express5S 1000Base-T CHPID 04 PORT 0
*
OSA20C0P TRLE  LNCTL=MPC,                                              *
               READ=20C0,                                              *
               WRITE=20C1,                                             *
               DATAPATH=(20C2,20C5),                                   *
               PORTNAME=OSA20C0,                                       *
               MPCLEVEL=QDIO
*
* QDIO TRLE FOR OSA-Express5S 1000Base-T CHPID 04 PORT 1
*
OSA20C6P TRLE  LNCTL=MPC,                                              *
               READ=20C6,                                              *
               WRITE=20C7,                                             *
               DATAPATH=(20C8,20CB),                                   *
               PORTNAME=OSA20C6,                                       *
               PORTNUM=1,                                              *
               MPCLEVEL=QDIO
*
* QDIO TRLE FOR OSA-Express5S 10GbE CHPID 07 PORT 0
*
OSA2160P TRLE  LNCTL=MPC,                                              *
               READ=2160,                                              *
               WRITE=2161,                                             *
               DATAPATH=(2162,2165),                                   *
               PORTNAME=OSA2160,                                       *
               MPCLEVEL=QDIO
```

TCP/IP uses a VTAM interface to run the OSA in QDIO mode. You must define and activate a TRL major node before TCP/IP starts its QDIO device.

Table 2-4 on page 13 lists the various uses of VTAM TRLE definitions, and this chapter provides implementation examples and the associated TRLE definition requirements.

Table 4-1 lists and describes the definitions that we used in the TRL major node for our OSA-Express5S 1000BASE-T feature for CHPID 04, port 0.

Table 4-1 VTAM TRL major node definition for port 0, related to TCPIPE and TCPIPF

Required parameters	**Explanation**	**Remarks**
TYPE=TRL	TRL major node	MPC TRL major node that is known to VTAM.
OSA20C0P	TRLE minor node	The name of the TRLE in VTAM. This name is downloaded to OSA and is used as OSANAME.
READ=20C0	READ device	The READ device number must be the even number of the device pair. The Read/Write pair of the OSA port is used only to exchange control data.
WRITE=20C1	WRITE device	The WRITE device number must be the odd number of the device pair. The Read/Write pair of the OSA port is used only to exchange control data.
DATAPATH= (20C2,20C5)	Data devices	The device address of the DATAPATH of each OSA port. For QDIO, the device 20C2 is used for the data transfer in both directions. The additional device 20C3, 20C4, and 20C5 is needed by other TCP/IP stacks and the OSA Network Traffic Analyzer trace function, which is covered in Appendix B, “Network Traffic Analyzer” on page 151.
PORTNAME= OSA20C0	PORTNAME associated with the devices	PORTNAME must match the TCP/IP device name in the TCP/IP profile for this connection. The association between TCP/IP and VTAM is done through the PORTNAME.
PORTNUM=0	Physical Port number that is associated with this CHPID	PORTNUM specifies which physical port on an OSA is to be used for this QDIO device. For OSA-Express3, OSA-Express4S and OSA-Express5S, multiple ports (0 and 1) are supported. The default is port number 0.
MPCLEVEL=QDIO	MPC compatibility level	This indicates that the QDIO interface is used for the OSA port.

TRLE considerations

For OSA, there are two types of subchannels:

1. Subchannels that are dedicated to control flows. The control subchannels are defined on the `READ` and `WRITE` operands.
2. Subchannels that are dedicated to data. The data subchannels are specified on the `DATAPATH` operand.

   Data subchannels are used for sending and receiving data through the OSA device or for receiving trace data from the OSA device, such as the OSA-Express Network Traffic Analyzer (`OSAENTA`).

It is important to note that a sufficient number of DATAPATH subchannel addresses must be defined to accommodate the number of concurrent instances or users of an OSA port. Consider the following factors:

- Each TCP/IP in the same logical partition instance that starts an OSA port in QDIO mode gets one of the DATAPATH channels assigned to it by VTAM. That means that you must code at least one DATAPATH subchannel.
- To add a second TCP/IP stack in the same LPAR, an additional DATAPATH device must be added to the `TRLE` statement and HCD.
- Each TCP/IP in the same logical partition instance that starts an OSA-Express Network Traffic Analyzer (`OSAENTA`) trace is also assigned one of the DATAPATH channels by VTAM.

- With z/OS Version 1, Release 10 and later, you can set up multiple VLANIDs per OSA port per stack per IP protocol version. You need to configure a separate interface to the OSA port for each VLAN. Each of these interfaces also requires a separate DATAPATH device in the TRLE definition.

The DATAPATH addresses do not need to be immediate after the WRITE address. It can be any address in the range of the defined devices of the OSA in the HCD.

Note: We describe the setup of multiple VLAN support in more detail in Chapter 10, “VLAN support” on page 89.

4.4.2 TCP/IP definitions

This section describes several helpful components.

Device, link, home, and interface statements

TCP/IP requires `DEVICE`, `LINK`, and `HOME` or `INTERFACE` statements that correspond to the port name in a VTAM TRLE. Example 4-2 shows the TCP/IP profile definitions by using `INTERFACE` statements of both OSA-Express5S 1000BASE-T ports 0 and 1 and OSA-Express5S 10GbE port 0 defined to CHPID 04 for TCPIPE. Example 4-3 on page 37 shows the `DEVICE`, `LINK`, and `HOME` statements.

Important: z/OS V1R10 introduced the INTERFACE statement, which provides the equivalent of DEVICE, LINK, and HOME definitions in one statement. You can still use the DEVICE, LINK, and HOME statements for IPv4 traffic, as we did for port 0 in Example 4-3 on page 37. However, there are configurations that require you to migrate to the INTERFACE statement, for example when using multiple VLANs.

Note: When an INTERFACE statement is supported, use that (rather than DEVICE, LINK, and HOME) to get the latest functionality from your IBM products.

In our environment, stack TCPIPE uses the INTERFACE statement and stack TCPIPF uses the `DEVICE`, `LINK`, and `HOME` statements.

Example 4-2 TCP/IP profile for TCPIPE

```
; OSA-Express5S 10GbE CHPID 07 Port 0
;
INTERFACE OSA2160LNK
   DEFINE IPAQENET
   PORTNAME OSA2160
   IPADDR 192.168.6.130/24
   VLANID 6
   VMAC ROUTEALL
;
BEGINROUTES
 ROUTE DEFAULT             192.168.6.1     OSA2160LNK    MTU 8992
 ROUTE 192.168.6.0 255.255.255.0 =         OSA2160LNK    MTU 8992

ENDROUTES
;
START OSA2160LNK
```

We defined the following values for OSA-Express5S 10GbE port 0, using the INTERFACE statement on TCPIPE:

OSA2160LNK Interface name
OSA2160 The OSA port name
192.168.6.130 IP address (CHPID 07 Port 0)

Example 4-3 TCP/IP profile for TCPIPF

```
; OSA-Express5S 1000BASE-T Port 0
;
DEVICE OSA20C0  MPCIPA ; OSD Devices on CHPID 04
LINK   OSA20C0LNK  IPAQENET OSA20C0  VLANID 3
;
DEVICE OSA20C6 MPCIPA ; OSD Devices on CHPID 04
LINK   OSA20C6LNK  IPAQENET OSA20C6 VLANID 5
;
HOME
  192.168.3.30  OSA20C0LNK
  192.168.5.30  OSA20C6LNK
;
BEGINROUTES
 ROUTE DEFAULT              192.168.3.1     OSA20C0LNK    MTU 1492
 ROUTE 192.168.3.0 255.255.255.0 =          OSA20C0LNK    MTU 1492
 ROUTE 192.168.5.0 255.255.255.0 =          OSA20C6LNK    MTU 1492
ENDROUTES
;
START OSA20C0
START OSA20C6
```

We defined the following values for OSA-Express5S 1000BASE-T port 0, using the INTERFACE statement on TCPIPF:

OSA20C0 Device name, which must match port name (port 0 of CHPID 04) in TRLE
OSA20C0LNK The link name of port 0 of CHPID 04
192.168.3.30 The IP address of port 0 of CHPID 04

Optimized latency mode (OLM)

Optimized latency mode (OLM) provides a method to provide the lowest-possible latency in OSA for processing interactive workloads. With this method, OSA provides an early interrupt to notify z/OS that inbound data is imminent. It allows the overhead of dispatching the interrupt handler to overlap with the OSA inbound data processing. OSA also provides a polling mode for outbound traffic, which reduces the latency of the QDIO Signal Adapter (SIGA) instruction.

Inbound workload queuing (IWQ)

Inbound workload queuing (IWQ) provides a method for OSA to route specific data packets to specific z/OS inbound queues. The specific data packets are communicated to OSA by z/OS by using a new IP assist. The IP assist allows z/OS to configure routing variables (RVs) to identify specific fields in a TCP/IP packet that causes the inbound packet to be routed to a specific z/OS inbound QDIO queue. When configuring this mode under z/OS, another inbound QDIO queue is added for each RV type. The currently supported RV types are for *Sysplex Distributor*, *Streaming*, and *Enterprise Extender*.

4.5 Activation

Normally, the CHPID should be online. If the CHPID is offline, configure it to online by using the following command:

```
CF CHP(04),ONLINE
```

After all of the definitions are added to VTAM and TCP/IP, you can activate the configuration, which requires completing these tasks:

1. Verify that the devices are online.
2. Activate the VTAM resources.
3. Activate TCP/IP.

4.5.1 Verifying that devices are online

The IBM z/OS display command (**`D U,,,20C0,16`**) can verify that the required devices for the OSA-Express5S 1000BASE-T feature are online (see Example 4-4).

Example 4-4 Output of the z/OS command to check OSA port devices related to CHPID 04

```
IEE457I 15.30.54 UNIT STATUS 421
 UNIT TYPE STATUS        VOLSER     VOLSTATE
 20C0 OSA  A-BSY
 20C1 OSA  A
 20C2 OSA  A-BSY
 20C3 OSA  A-BSY
 20C4 OSA  O
 20C5 OSA  O
 20C6 OSA  A-BSY
 20C7 OSA  O
 20C8 OSA  A-BSY
 20C9 OSA  A-BSY
 20CA OSA  O
 20CB OSA  O
 20CC OSA  O
 20CD OSA  O
 20CE OSA  O
 20CF OSAD O-RAL
```

All devices (read, write, data, and OSA-Express Network Traffic Analyzer) are either active or online for each OSA port. If the devices are not online, use the vary command:

```
V (20C0-20CF),ONLINE
```

4.5.2 VTAM activation

Next, activate the corresponding TRL by using the following VTAM commands:

```
V NET,ACT,ID=OSA20C0
V NET,ACT,ID=OSA20C6
V NET,ACT,ID=OSA2160
```

TCP/IP requires an active TRL before starting its device.

After activating the TRL, the status of the TRLE is NEVAC or INACT until TCP/IP starts it. When the TCP/IP device is started, configuration information (for example, HOME IP address) is loaded into the OSA feature.

4.5.3 TCP/IP devices

There are two ways to activate the TCP/IP devices: Either restart the TCP/IP stack or use the Start command:

```
V TCPIP,TCPIPF,START,OSA20C0
```

You can use this command to stop the device:

```
V TCPIP,TCPIPF,STOP,OSA20C0
```

4.6 Relevant status displays

Example 4-5 shows the status of port 0 of the OSA-Express5S 1000BASE-T devices for TCPIPE. To display the status, you can use the **D TCPIP,TCPIPE,NETSTAT,DEV** command.

Example 4-5 Display of the status of a 1000BASE-T device

```
DEVNAME: OSA20C0           DEVTYPE: MPCIPA
  DEVSTATUS: READY         CFGROUTER: NON  ACTROUTER: NON
  LNKNAME: OSA20C0LNK        LNKTYPE: IPAQENET    LNKSTATUS: READY
    SPEED: 0000000100
    IPBROADCASTCAPABILITY: NO
    ARPOFFLOAD: YES                ARPOFFLOADINFO: YES
    ACTMTU: 1492
    VLANID: 980                    VLANPRIORITY: DISABLED
    DYNVLANREGCFG: NO              DYNVLANREGCAP: YES
    READSTORAGE: GLOBAL (4096K)    INBPERF: BALANCED
    CHECKSUMOFFLOAD: YES
    SECCLASS: 255                  MONSYSPLEX: NO
  BSD ROUTING PARAMETERS:
    MTU SIZE: N/A               METRIC: 00
    DESTADDR: 0.0.0.0           SUBNETMASK: 255.255.255.0
  MULTICAST SPECIFIC:
    MULTICAST CAPABILITY: YES
...
```

Example 4-6 on page 40 shows the status of port 0 of the OSA-Express5S 10GbE device, which we defined with the INTERFACE statement. Again, to display the status, use the **D TCPIP,TCPIPE,NETSTAT,DEV** command.

Example 4-6 Display of the status of a 10GbE device

```
IntfName: OSA2160LNK        IntfType: IPAQENET   IntfStatus: Ready
    PortName: OSA2160   Datapath: 2163     DatapathStatus: Ready
    CHPIDType: OSD      SMCR: Disabled (GLOBALCONFIG NOSMCR)
    PNetID: *None*
    Speed: 0000010000
    IpBroadcastCapability: No
    CfgRouter: Pri                  ActRouter: Pri
    ArpOffload: Yes                 ArpOffloadInfo: Yes
    CfgMtu: None                    ActMtu: 8992
    IpAddr: 192.168.6.130/24
    VLANid: 6                       VLANpriority: Disabled
    DynVLANRegCfg: No               DynVLANRegCap: Yes
    ReadStorage: GLOBAL (4096K)
    InbPerf: Balanced
    ChecksumOffload: Yes            SegmentationOffload: No
    SecClass: 255                   MonSysplex: No
    Isolate: No                     OptLatencyMode: No
  Multicast Specific:
    Multicast Capability: Yes
...
```

As you can see, the output differs slightly, for example showing the VMAC address of this OSA-Expresss5S port.

The **D TCPIP,TCPIPE,NETSTAT,HOME** command can be used to display IPv4 home addresses and determine whether each address is associated with a LINK definition or an INTERFACE definition (see Example 4-7).

Example 4-7 The HOME command

```
EZD0101I NETSTAT CS V2R1 TCPIPE 723
HOME ADDRESS LIST:
LINKNAME:   LOOPBACK
  ADDRESS:  127.0.0.1
    FLAGS:
INTFNAME:   OSA2160LNK
  ADDRESS:  192.168.6.130
    FLAGS:
INTFNAME:   LOOPBACK6
  ADDRESS:  ::1
    TYPE:   LOOPBACK
    FLAGS:
3 OF 3 RECORDS DISPLAYED
```

To determine the devices that are used and allocated by TCP/IP, you must display the VTAM TRLE. Example 4-8 on page 41 shows the TRLE of port 0 (CHPID 04) of the active

OSA-Express5S 1000BASE-T that belongs to TCPIPF. Message IST1221I tells you which devices TCPIPF uses for READ, WRITE, and DATA, and for OSAENTA.

Example 4-8 D NET,TRL,TRLE=OSA20C6P for TCPIPE results

```
D NET,TRL,TRLE=OSA20C6P
IST097I DISPLAY ACCEPTED
IST075I NAME = OSA20C6P, TYPE = TRLE
IST1954I TRL MAJOR NODE = OSA20C6
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = LEASED             , CONTROL = MPC , HPDT = YES
IST1715I MPCLEVEL = QDIO       MPCUSAGE = SHARE
IST2263I PORTNAME = OSA20C6    PORTNUM =   1   OSA CODE LEVEL = 0C8C
IST2337I CHPID TYPE = OSD      CHPID = 04  PNETID = ITSOPNET1
IST1577I HEADER SIZE = 4096 DATA SIZE = 0 STORAGE = ***NA***
IST1221I WRITE DEV = 20C7 STATUS = ACTIVE     STATE = ONLINE
IST1577I HEADER SIZE = 4092 DATA SIZE = 0 STORAGE = ***NA***
IST1221I READ  DEV = 20C6 STATUS = ACTIVE     STATE = ONLINE
IST924I -------------------------------------------------------------
IST1221I DATA  DEV = 20C8 STATUS = ACTIVE     STATE = N/A
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST1717I ULPID = TCPIPF ULP INTERFACE = OSA20C6
IST2310I ACCELERATED ROUTING DISABLED
IST2331I QUEUE   QUEUE     READ             QUEUE
IST2332I ID      TYPE      STORAGE          STATUS
IST2205I ------  --------  ---------------  ----------------------
IST2333I RD/1    PRIMARY   4.0M(64 SBALS)   ACTIVE
IST2305I NUMBER OF DISCARDED INBOUND READ BUFFERS = 0
IST2386I NUMBER OF DISCARDED OUTBOUND WRITE BUFFERS = 0
IST1757I PRIORITY1: UNCONGESTED PRIORITY2: UNCONGESTED
IST1757I PRIORITY3: UNCONGESTED PRIORITY4: UNCONGESTED
IST2190I DEVICEID PARAMETER FOR OSAENTA TRACE COMMAND = 01-01-00-08
IST1801I UNITS OF WORK FOR NCB AT ADDRESS X'2386B010'
IST1802I P1 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P2 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P3 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P4 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST924I -------------------------------------------------------------
IST1221I DATA  DEV = 20C9 STATUS = RESET      STATE = N/A
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST924I -------------------------------------------------------------
IST1221I DATA  DEV = 20CA STATUS = RESET      STATE = N/A
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST924I -------------------------------------------------------------
IST1221I DATA  DEV = 20CB STATUS = RESET      STATE = N/A
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST924I -------------------------------------------------------------
IST314I END
```

Tip: If your static TRLE definition is incorrect, an active TRLE entry cannot be deleted. *Vary* activate the TRL major node with a blank TRLE to delete previous entries. Then, code the TRL major node with the correct TRLE entry and definitions, and vary activate the TRL/TRLE node. Consider this blank entry in Example 4-9 on page 42 for both OSA-Express5S 1000BASE-T ports (0 and 1) that belong to CHPID 04.

See Table D-3 on page 185 for the *vary* commands.

Example 4-9 Coding blank TRLE names for deletion

```
OSA20C0 VBUILD TYPE=TRL
         TRLE  LNCTL=MPC,                                         *
               READ=20C0,                                         *
               WRITE=20C1,                                        *
               DATAPATH=(20C2,20C5),                              *
               PORTNAME=OSA20C0,                                  *
               PORTNUM=0,                                         *
               MPCLEVEL=QDIO

         TRLE  LNCTL=MPC,                                         *
               READ=20C6,                                         *
               WRITE=20C7,                                        *
               DATAPATH=(20C8,20CB),                              *
               PORTNAME=OSA20C6,                                  *
               PORTNUM=1,                                         *
               MPCLEVEL=QDIO
```

4.7 Systems Network Architecture support for QDIO mode

There might be cases where you need to transmit Systems Network Architecture (SNA) traffic over OSA-Express and you want to get the benefits of QDIO. IBM provides two technologies to integrate SNA-based traffic when using TCP/IP:

- Use Enterprise Extender to connect SNA (LU6.2,0,1,2,3) endpoint traffic over TCP/IP directly into the System z server. See Chapter 7 of the *IBM System z Connectivity Handbook*, SG24-5444.
- The TN3270E server supports TCP/IP host access to SNA applications. For more information, see Chapter 7 in the *IBM System z Connectivity Handbook*, SG24-5444.

5

QDIO mode for the IBM z/VM operating system

This chapter covers the implementation steps to establish network connectivity with an IBM Open Systems Adapter-Express (OSA) channel path identifier (CHPID) in Queued Direct I/O (QDIO) mode.

Although the Open Systems Adapter Support Facility (OSA/SF) is not required because all definitions are set dynamically, you need to use the OSA/SF for monitoring and controlling the OSA port.

For more information about installing and using OSA/SF, see Appendix E, “Using the Open Systems Adapter Support Facility” on page 191.

The information in this chapter covers the following topics:

- 5.1, “QDIO environment” on page 44
- 5.2, “Hardware Configuration Definition” on page 44
- 5.3, “Missing-interrupt handler for QDIO” on page 44
- 5.4, “Customizing the z/VM network environment” on page 45
- 5.5, “Activation” on page 46
- 5.6, “Relevant status displays” on page 48

5.1 QDIO environment

Figure 5-1 shows a logical representation of the z/VM environment that is described in this chapter.

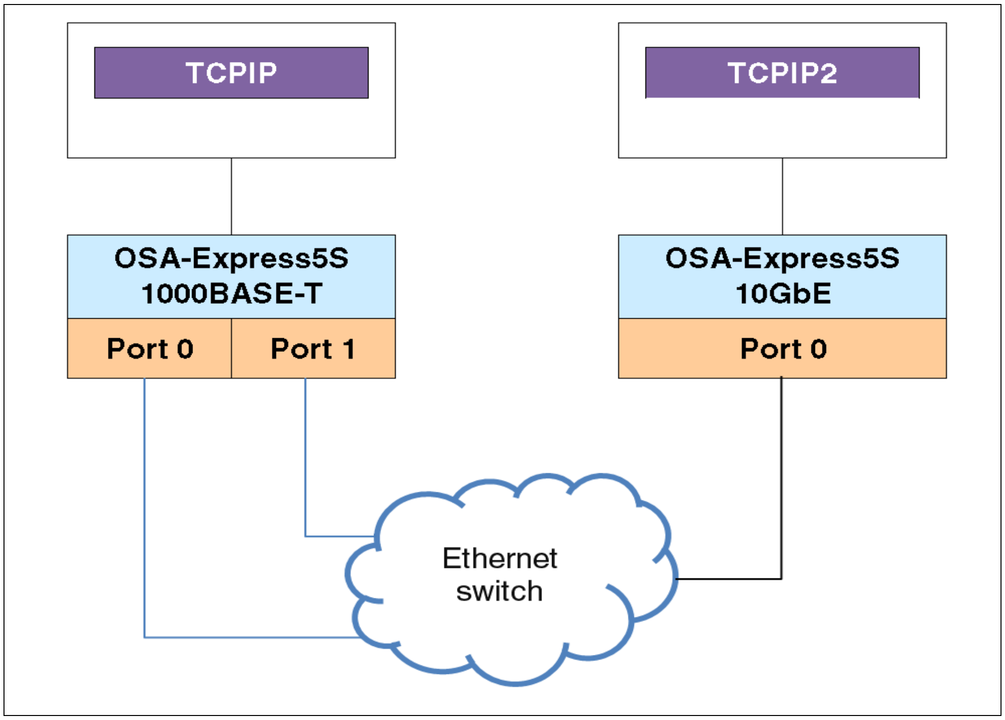


Figure 5-1 QDIO mode example for z/VM

5.2 Hardware Configuration Definition

The OSA CHPID, the control unit, and the OSA devices must be defined to the IBM System z hardware either by coding suitable input/output configuration program (IOCP) statements or through Hardware Configuration Definition (HCD). See Chapter 3, “Hardware configuration definitions” on page 15, for the procedure to create the definitions.

The necessary definitions for CHPID 04 and CHPID 07 are also shown in the IOCP and input/output configuration data set (IOCDS) format in 3.2.4, “Generating the IOCDS input from the HCD” on page 27.

5.3 Missing-interrupt handler for QDIO

The WRITE devices must have a missing-interrupt handler (MIH) value of at least 15 seconds. To determine the current MIH value for the device (20C1 in our example), use the following command:

```
Q MITIME
```

To dynamically change the MIH value, use either of the following commands:

```
SET MITIME 20C1 00:15  (for a single device)
SET MITIME 20C0-20CF 00:15  (for a range of devices)
```

To set these values at IPL time, update the PROFILE EXEC of the AUTOLOG1 user ID.

5.4 Customizing the z/VM network environment

Figure 5-2 shows our z/VM network configuration, which consists of a z/VM logical partition (LPAR) with two TCP/IP stacks and three OSA ports that are connected to an Ethernet switch.

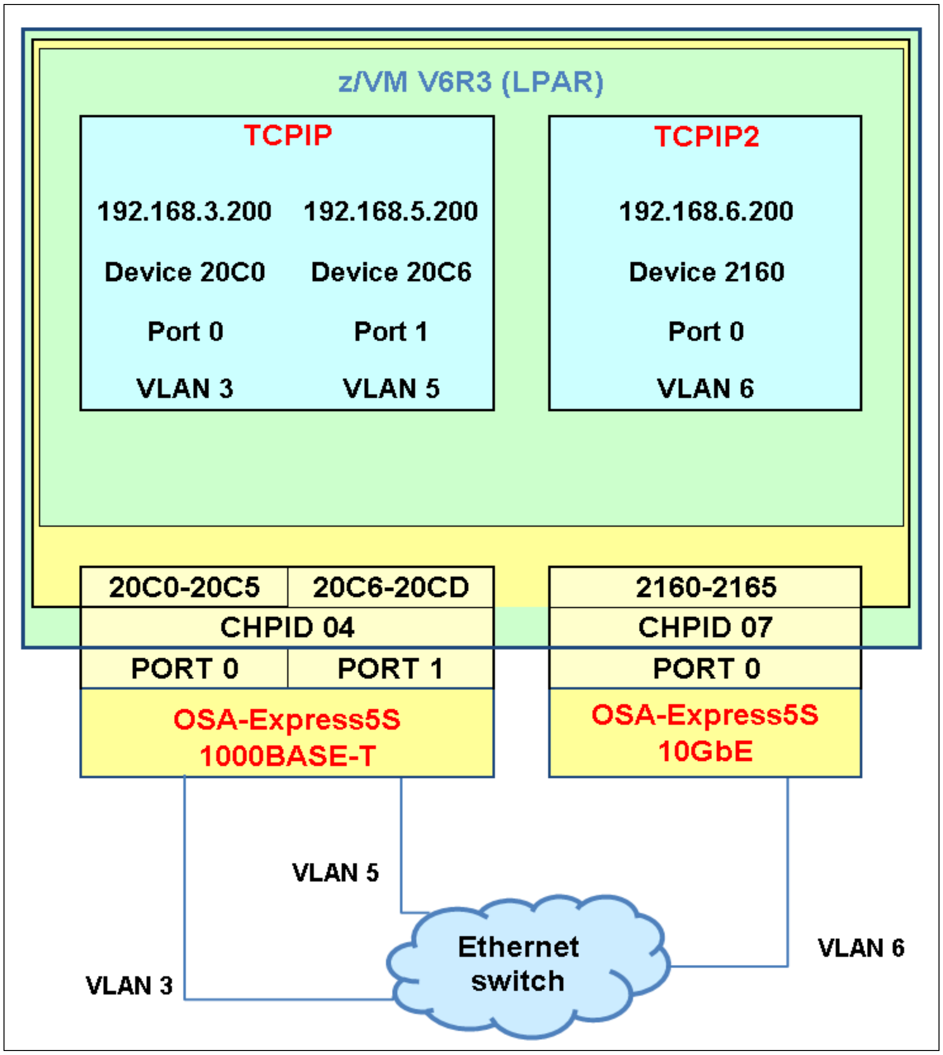


Figure 5-2 Network configuration

To demonstrate the setup for OSA connectivity, we use only the first CHPID of each OSA-Express5S 1000BASE-T and OSA-Express5S 10GbE feature with the associated port or ports. In a production environment, both CHPIDs should be used and the ports should be connected to at least two different Ethernet switches to avoid single points of failure.

The TCP/IP stack for z/VM user ID TCPIP2 has one port that is defined to it to show how all OSA-Express4S and OSA-Express5S features that support only one port per CHPID are configured.

5.4.1 TCP/IP definitions

TCP/IP requires DEVICE, LINK, and HOME definitions that correspond to the hardware device addresses and port numbers.

> **Note:** Although DEVICE and LINK statements are still supported, the INTERFACE statement has more functions and is preferable.

Example 5-1 shows the TCP/IP profile definitions of the stack for z/VM user ID TCPIP for both OSA-Express5S 1000BASE-T ports from CHPID 04. The device addresses are 20C0 (port 0) and 20C6 (port 1).

Example 5-1 Profile for TCP/IP stack for user ID TCPIP

```
DEVICE OSA20C0 OSD 20C0 PORTNUMBER 00
LINK OSA20C0 QDIOETHERNET OSA20C0 MTU 1500 ETHERNET VLAN 3
;
DEVICE OSA20C6 OSD 20C6 PORTNUMBER 01
LINK OSA20C6 QDIOETHERNET OSA20C6 MTU 1500 ETHERNET VLAN 5
;
HOME
192.168.3.200 255.255.255.0 OSA20C0
192.168.5.200 255.255.255.0 OSA20C6
;
START OSA20C0
START OSA20C6
```

Example 5-2 shows the TCP/IP profile definitions of the stack for z/VM z/VM user ID TCPIP2 for one OSA-Express5S 10GbE port from CHPID 07. The device address is 2160.

Example 5-2 Profile for TCP/IP stack for user ID TCPIP2

```
DEVICE OSA2160 OSD 2160
LINK OSA2160 QDIOETHERNET OSA2160 MTU 1500 ETHERNET VLAN 6
;
HOME
192.168.6.200 255.255.255.0 OSA2160
;
START OSA2160
```

Notice that PORTNUMBER 00 is the default value. Therefore, it does not need to be defined in the DEVICE statement.

5.5 Activation

Normally, the CHPID should be online. If it is offline, configure it to online by using the following command:

```
VARY ON CHPID 04
```

After all the definitions are added to TCP/IP, you can activate the configuration, which includes these tasks:

- Verify that the devices are online
- Activate TCP/IP devices

5.5.1 Verify that devices are online

With the **QUERY CHPID** command, you can verify that the OSA devices are online (see Example 5-3).

Example 5-3 CP command - QUERY CHPID 04 and 07

```
QUERY CHPID 04
Path 04 online to devices 20C0 20C1 20C2 20C3 20C4 20C5 20C6 20C7
Path 04 online to devices 20C8 20C9 20CA 20CB 20CC 20CD 20CE 20CF

QUERY CHPID 07
Path 07 online to devices 2160 2161 2162 2163 2164 2165 2166 2167
Path 07 online to devices 2168 2169 216A 216B 216C 216D 216E 216F
```

All devices that are necessary for our environment are online. If the devices are not online, you can use the **VARY ON** command:

```
VARY ON 20C0-20CF
```

The **QUERY OSA ALL** command also shows the OSAD device (20CF and 216F) for each adapter (see Example 5-4).

Example 5-4 CP command - QUERY OSA ALL

```
QUERY OSA ALL
QUERY OSA ALL
OSA  20C0 ATTACHED TO DTCVSW1  061B DEVTYPE OSA         CHPID 04 OSD
OSA  20C1 ATTACHED TO DTCVSW1  061C DEVTYPE OSA         CHPID 04 OSD
OSA  20C2 ATTACHED TO DTCVSW1  061D DEVTYPE OSA         CHPID 04 OSD
OSA  20C3 ATTACHED TO DTCVSW2  0627 DEVTYPE OSA         CHPID 04 OSD
OSA  20C4 ATTACHED TO DTCVSW2  0628 DEVTYPE OSA         CHPID 04 OSD
OSA  20C5 ATTACHED TO DTCVSW2  0629 DEVTYPE OSA         CHPID 04 OSD
OSA  20C6 ATTACHED TO TCPIP    20C6 DEVTYPE OSA         CHPID 04 OSD
OSA  20C7 ATTACHED TO TCPIP    20C7 DEVTYPE OSA         CHPID 04 OSD
OSA  20C8 ATTACHED TO TCPIP    20C8 DEVTYPE OSA         CHPID 04 OSD
OSA  20C9 ATTACHED TO DTCVSW1  062D DEVTYPE OSA         CHPID 04 OSD
OSA  20CA ATTACHED TO DTCVSW1  062E DEVTYPE OSA         CHPID 04 OSD
OSA  20CB ATTACHED TO DTCVSW1  062F DEVTYPE OSA         CHPID 04 OSD
OSA  2160 ATTACHED TO TCPIP2   2160 DEVTYPE OSA         CHPID 07 OSD
OSA  2161 ATTACHED TO TCPIP2   2161 DEVTYPE OSA         CHPID 07 OSD
OSA  2162 ATTACHED TO TCPIP2   2162 DEVTYPE OSA         CHPID 07 OSD
OSA  20CC FREE    , OSA  20CD FREE    , OSA  20CE FREE    , OSA  20CF FREE
OSA  2163 FREE    , OSA  2164 FREE    , OSA  2165 FREE    , OSA  2166 FREE
OSA  2167 FREE    , OSA  2168 FREE    , OSA  2169 FREE    , OSA  216A FREE
OSA  216B FREE    , OSA  216C FREE    , OSA  216D FREE    , OSA  216E FREE
OSA  216F FREE

An offline OSA was not found.
OSA  204F is an OSA Agent
OSA  206F is an OSA Agent
OSA  20CF is an OSA Agent
OSA  216F is an OSA Agent
```

5.5.2 Activate the TCP/IP devices

There are two ways to activate the TCP/IP devices: Either restart the TCP/IP stack or use the TCP/IP **OBEYFILE** command. We chose to restart the stack to implement the changes.

5.6 Relevant status displays

To display the status of the OSA connections and to verify the configuration, you can use the TCPIP **NETSTAT DEV** command.

Example 5-5 shows the status of the OSA-Express5S 1000BASE-T devices for z/VM user ID TCPIP. OSA devices 20C0 and 20C6 are in a ready state, 20C0 is using port 0, and 20C6 is using port 1.

Example 5-5 NETSTAT DEV for TCPIP

```
netstat tcp tcpip dev
VM TCP/IP Netstat Level 630       TCP/IP Server Name: TCPIP

Device OSA20C0                 Type: OSD            Status: Ready
  Queue size: 0     CPU: 0     Address: 20C0        Port name: UNASSIGNED
    Link OSA20C0               Type: QDIOETHERNET   Port number: 0
      Transport Type: Ethernet MAC: 02-00-00-00-00-50
      Speed: 1000000000
      BytesIn: 1080            BytesOut: 484
      Forwarding: Enabled      MTU: 1500            IPv6: Disabled
      IPv4 Path MTU Discovery: Disabled
      VLAN ID: 3                                    GVRP: Disabled
      IPv4 VIPA ARP
      Multicast Group                         Members
      ---------------                         -------
      224.0.0.1                                  1

Device OSA20C6                 Type: OSD            Status: Ready
  Queue size: 0     CPU: 0     Address: 20C6        Port name: UNASSIGNED
    Link OSA20C6               Type: QDIOETHERNET   Port number: 1
      Transport Type: Ethernet MAC: 02-00-00-00-00-51
      Speed: 1000000000
      BytesIn: 412             BytesOut: 818
      Forwarding: Enabled      MTU: 1500            IPv6: Disabled
      IPv4 Path MTU Discovery: Disabled
      VLAN ID: 5                                    GVRP: Enabled
      IPv4 VIPA ARP
      Multicast Group                         Members
      ---------------                         -------
      224.0.0.1                                  1
```

Example 5-6 on page 49 shows the status of the OSA-Express5S 10GbE devices for z/VM user ID TCPIP2. OSA device 2160 is in a ready state and using port 0.

Example 5-6 NETSTAT DEV for TCPIP2

```
netstat tcp tcpip2 dev
VM TCP/IP Netstat Level 630       TCP/IP Server Name: TCPIP2

Device OSA2160                 Type: OSD           Status: Ready
  Queue size: 0     CPU: 0     Address: 2160       Port name: UNASSIGNED
    Link OSA2160               Type: QDIOETHERNET   Port number: 0
      Transport Type: Ethernet MAC: 02-00-00-00-00-52
      Speed: 10000000000
      BytesIn: 490             BytesOut: 1820
      Forwarding: Enabled      MTU: 1500           IPv6: Disabled
      IPv4 Path MTU Discovery: Disabled
      VLAN ID: 6                                   GVRP: Enabled
      IPv4 VIPA ARP
      Multicast Group                         Members
      ---------------                         -------
      224.0.0.1                                  1
```

The **NETSTAT HOME** command can be used to display IPv4 and IPv6 home addresses. See Example 5-7 for the server named TCPIP and Example 5-8 for z/VM user ID TCPIP2.

Example 5-7 NETSTAT HOME for TCPIP

```
netstat home
VM TCP/IP Netstat Level 630       TCP/IP Server Name: TCPIP

IPv4 Home address entries:
Address         Subnet Mask      Link              VSWITCH
-------         -----------      ------            -------
192.168.3.200   255.255.255.0    OSA20C0           <none>
192.168.5.200   255.255.255.0    OSA20C6           <none>

IPv6 Home address entries: None

Ready; T=0.01/0.01 07:04:39
```

Example 5-8 NETSTAT HOME for TCPIP2

```
netstat tcp tcpip2 home
VM TCP/IP Netstat Level 630       TCP/IP Server Name: TCPIP2

IPv4 Home address entries:
Address         Subnet Mask      Link              VSWITCH
-------         -----------      ------            -------
192.168.6.200   255.255.255.0    OSA2160           <none>

IPv6 Home address entries: None
```

6

Non-QDIO mode for the IBM z/OS operating system

This chapter describes customizing the IBM Open Systems Adapter-Express (OSA) channel path identifiers (CHPIDs) in non-Queued Direct I/O (non-QDIO) mode for TCP/IP and Systems Network Architecture (SNA) for an IBM z/OS operating system environment. To configure an OSA CHPID in non-QDIO mode, the Open Systems Adapter Support Facility (OSA/SF) is required.

This chapter does not cover the setup process for an OSA CHPID running in *default* mode, using the default OSA Address Table (OAT). That information is in Appendix G, “TCP/IP Passthru mode” on page 219.

The information in this chapter covers the following topics:

6.1 Configuration information

Figure 6-1 shows a functional view of the connectivity that is described in this chapter for a non-QDIO OSA CHPID in a z/OS environment.

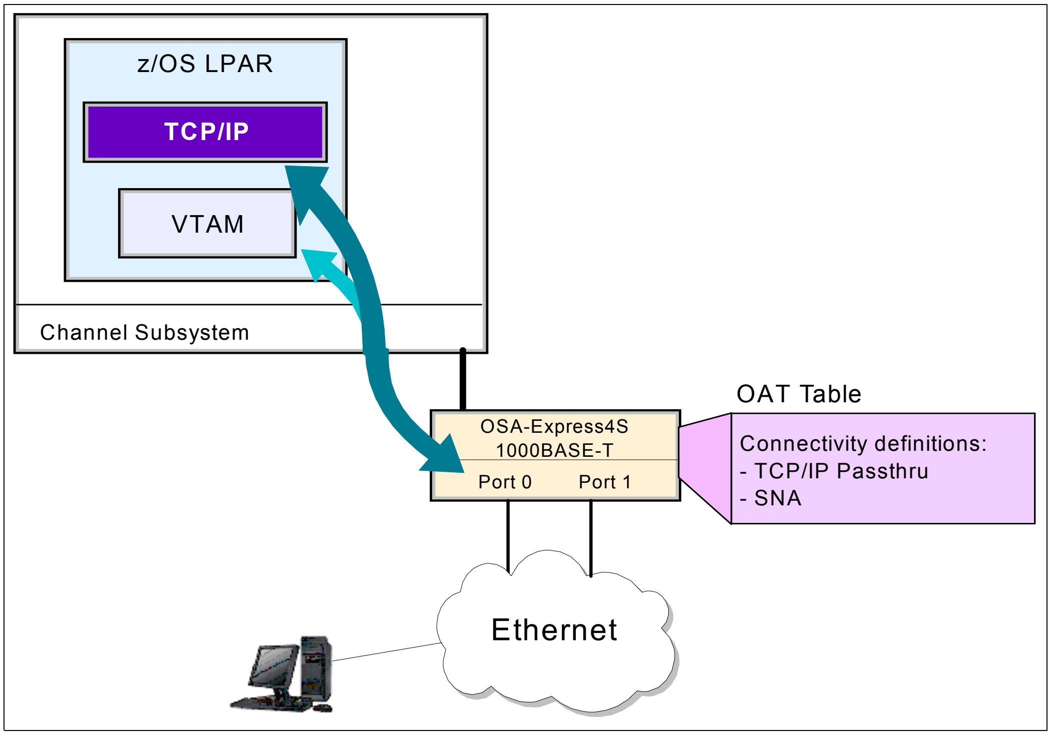


Figure 6-1 Non-QDIO mode shared port

In the following topics, we describe what components must be configured and activated to use any type of OSA port in non-QDIO mode:

- Hardware definitions
- Creating and activating the OSA configuration
- Customizing the z/OS network environment

6.2 Hardware definitions

The OSA CHPID, control unit, and OSA devices must be defined to HCD/IOCP, and must be activated. See Chapter 3, “Hardware configuration definitions” on page 15, for the procedure to create the definitions.

Example 6-1 on page 53 shows the IOCP definitions that are used for CHPID `06`. For future use, we defined 15 OSA devices, although only three are needed in our configuration.

Example 6-1 IOCP input for CHPID 06 example

```
ID    MSG1='iocds',MSG2='SYS6.IODF30 - 2013-10-31 09:59',     *
      SYSTEM=(2827,1),LSYSTEM=SCZP401,                        *
      TOK=('SCZP401',00800003B8D72827095916150113304F00000000,*
      00000000,'13-10-31','09:59:16','SYS6','IODF30')
RESOURCE PARTITION=((CSS(0),(A0A,A),(A0B,B),(A0C,C),(A0D,D),(A*
      0E,E),(A0F,F),(A01,1),(A02,2),(A03,3),(A04,4),(A05,5),(A*
      06,6),(A07,7),(A08,8),(A09,9)),(CSS(1),(A1A,A),(A1B,B),(*
      A1C,C),(A1D,D),(A1E,E),(A1F,F),(A11,1),(A12,2),(A13,3),(*
      A14,4),(A15,5),(A16,6),(A17,7),(A18,8),(A19,9)),(CSS(2),*
      (A2A,A),(A2B,B),(A2C,C),(A2D,D),(A2E,E),(A2F,F),(A21,1),*
      (A22,2),(A23,3),(A24,4),(A25,5),(A26,6),(A27,7),(A28,8),*
      (A29,9)),(CSS(3),(A3D,D),(A3E,E),(A3F,F),(A31,1),(A32,2)*
      ,(A33,3),(A34,4),(A35,5),(*,6),(*,7),(*,8),(*,9),(*,A),(*
      *,B),(*,C)))
CHPID PATH=(CSS(1,2),06),SHARED,
      PARTITION=((CSS(1),(A11,A13),(=)),(CSS(2),(A2E),(=))),
      PCHID=50C,TYPE=OSE

CNTLUNIT CUNUMBR=0040,PATH=((CSS(1),06)),UNIT=OSA
IODEVICE ADDRESS=(0040,15),UNITADD=00,CUNUMBR=(0040),UNIT=OSA
IODEVICE ADDRESS=004F,UNITADD=FE,CUNUMBR=(0040),UNIT=OSAD
```

6.3 Creating and activating the OSA configuration

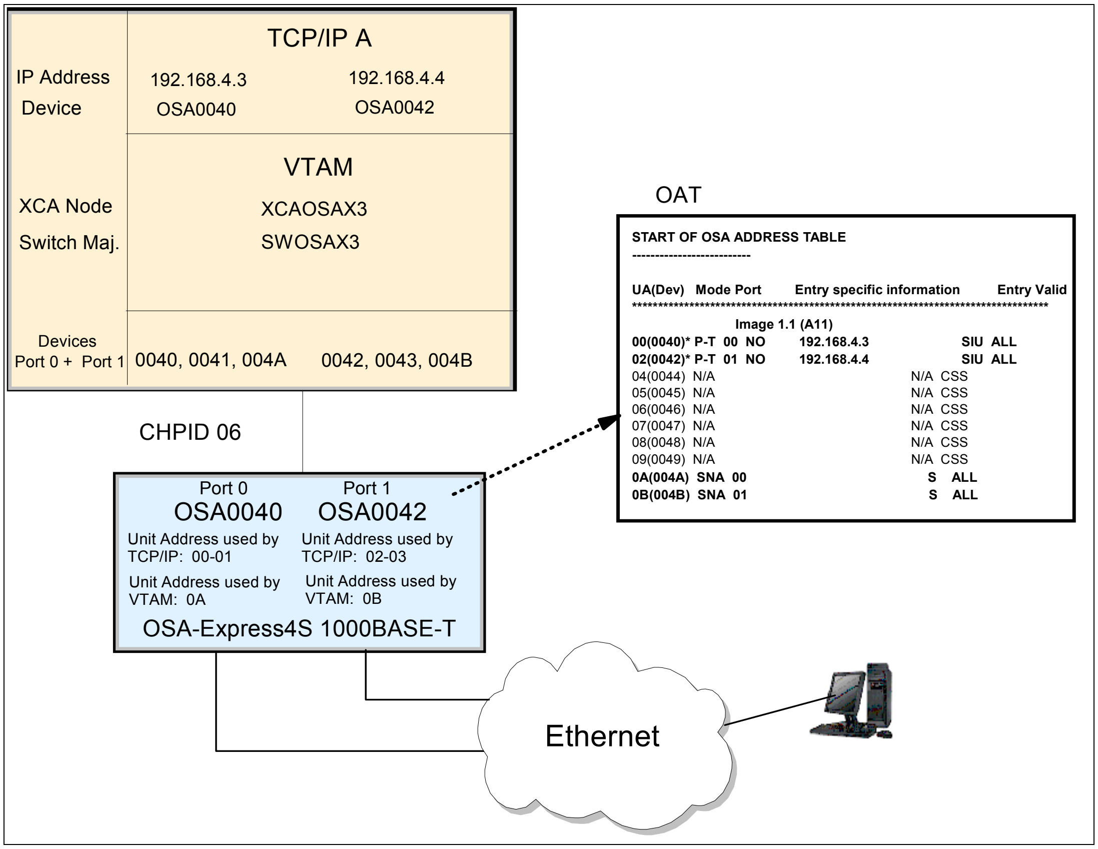
To set up the data paths for the OSA port, two files are required:

- The OSA configuration file, which contains information about the hardware characteristics of the OSA port, such as MAC address, line speed, and timer values.
- The OSA Address Table (OAT), which consists of parameters that map the LPAR, mode, unit address, and network protocol (TCP/IP and SNA) specifics to the OSA port.

The Open Systems Adapter Support Facility (OSA/SF) is an application that helps you to customize and manage your OSA features. You can use it to get status and operational information about the HCD-defined OSA ports to assist in problem determination.

When the `Activate` option is selected from OSA/SF, the OSA configuration file and OAT are downloaded to the OSA, using the FE unit address (OSAD device). After they are downloaded, the OSA ports are automatically disabled and re-enabled. This causes the OSA hardware to be reset. It also activates the new OSA configuration.

In this chapter, we use the configuration in Figure 6-2 on page 54.



```
START OF OSA ADDRESS TABLE
--------------------------

UA(Dev)   Mode Port      Entry specific information       Entry Valid
********************************************************************************
                     Image 1.1 (A11)
00(0040)* P-T  00  NO      192.168.4.3                SIU  ALL
02(0042)* P-T  01  NO      192.168.4.4                SIU  ALL
04(0044)  N/A                                 N/A  CSS
05(0045)  N/A                                 N/A  CSS
06(0046)  N/A                                 N/A  CSS
07(0047)  N/A                                 N/A  CSS
08(0048)  N/A                                 N/A  CSS
09(0049)  N/A                                 N/A  CSS
0A(004A)  SNA  00                               S   ALL
0B(004B)  SNA  01                               S   ALL
```

Figure 6-2 Connectivity layout

Creating (adding) and saving an OSA port configuration is not disruptive. The only time that a definition can have an effect on the OAT configuration is when the `Activate` option is selected.

OSA/SF

For creating and activating the OSA configuration and OAT, you can use OSA/SF. There are two versions: HMC and operating system-based interface. OSA-Express4S devices are supported by either interface. Earlier OSA devices are supported only on the OS-based interface. Later OSA devices must use the HMC interface.

For the HMC version, see *Open Systems Adapter/Support Facility on the Hardware Management Console*, SC14- 7580. For the OS-based interface version, see Chapter 8, *OSA-Express Customer's Guide*, SA22-7935.

6.4 Customizing the z/OS network environment

In our environment, TCP/IP and VTAM coexist and share the OSA port without affecting each other. This allows the definitions for TCP/IP and VTAM to be done independently, as though the OSA port was owned by VTAM or TCP/IP exclusively.

The OSA port is defined as a local area network (LAN) Channel Station (LCS) to TCP/IP. An LCS uses two devices for TCP/IP operation.

VTAM sees the OSA port as an external communications adapter (XCA). One OSA port is linked to one device for SNA operation.

Reminder: Port sharing is set up in OSA/SF, not in TCP/IP or VTAM.

6.4.1 VTAM definitions

This section describes the definitions that are required in VTAM to allow SNA applications to access the LAN over the OSA port. To describe the VTAM setup, the network configuration that is shown in Figure 6-2 on page 54 is used. In this example VTAM communicates over an Ethernet switch by using port 0 (device number 004A).

You need to define two types of major nodes in VTAM:

- XCA major node
- Switched major node (SWNET)

XCA major node

Define one XCA major node for each SNA OSA device with:

- The node type (VBUILD definition statement)
- The port that is used by the LAN (port definition statement)
- The switched peripheral nodes (type 2) attached to an Ethernet LAN through an OSA port (Group, Line, and PU definition statements)

Example 6-2 shows the XCA major node definitions that are used for this connection.

Example 6-2 XCA major node definition

```
XCAOSA   VBUILD TYPE=XCA
OSAX3    PORT  MEDIUM=CSMACD,                                         X
               ADAPNO=0,                                              X
               CUADDR=004A,                                           X
               TIMER=60,                                              X
               SAPADDR=04
*********************************************************************
OSAX3G   GROUP DIAL=YES,                                              X
               DYNPU=YES,                                             X
               ANSWER=ON,                                             X
               AUTOGEN=(3,L,P),                                       X
               CALL=INOUT,                                            X
               ISTATUS=ACTIVE
```

Table 6-1 lists the port parameters.

Table 6-1 XCA major node port definition for XCAOSAX3

Required parameters	Explanation	Remarks
TYPE=XCA	XCA major node	The OSA functions as an XCA to VTAM.
ADAPNO=0	*PORT* statement	Code `ADAPNO=0` for port 0 of OSA-Express4S 1000BASE-T
CUADDR= 004A	Channel unit address	Code the device number that is defined for this port. In our example, VTAM uses device number `004A` for port 0.
MEDIUM= CSMACD	LAN type	Use `CSMACD` for Ethernet.
SAPADDR=04	Service access point address	Code a value that is a multiple of 4. This address *must* be unique for each VTAM communicating with a port. Use different SAP addresses if a port is shared by multiple VTAMs. See the SAPADDR value of XCAOSAX3.

Table 6-2 identifies the significant group parameters.

Table 6-2 XCA major node group definition for XCAOSAX3

Required parameters	Explanation	Remarks
DIAL=YES	Switched peripheral node	You *must* code `DIAL=YES` to specify that the switched line control protocol is required.
AUTOGEN= (3,L,P)	Auto-generation of LINE and PU statements	This parameter enables VTAM to automatically generate three sets of LINE and PU statements. The LINE names begin with *L*. The PU names begin with *P*.

Note: The current OSA features support 4096 SNA PU Type 2 connections per port on System zEC12 servers.

Switched major node

Define *one* switched major node for each switched connection to the peripheral nodes attached on the LAN. Code the following items:

- A remote physical unit (PU definition statement)
- The corresponding logical units (LU definition statements)

Example 6-3 shows how 3270 sessions are set up with a switched major node. It lists the important parameters in the PU definition.

Example 6-3 Switched major node definition

```
VBUILD TYPE=SWNET
OSASW    PU    ADDR=02,                                                X
               IDBLK=05D,                                              X
               IDNUM=12863,                                            X
               CPNAME=OSANT,                                           X
               IRETRY=YES,                                             X
               MAXOUT=7,                                               X
               MAXPATH=1,                                              X
               MAXDATA=1024,                                           X
               PACING=0,                                               X
               VPACING=0,                                              X
               PUTYPE=2,                                               X
               DISCNT=(NO),                                            X
               ISTATUS=ACTIVE,                                         X
               MODETAB=NEWMTAB,                                        X
               DLOGMOD=DYNTRN,                                         X
               USSTAB=USSLDYN,                                         X
               SSCPFM=USSSCS
OSASWL0  LU    LOCADDR=0,MODETAB=MTAPPC,DLOGMOD=APPCMODE
OSASWL1  LU    LOCADDR=1                                3270 SESSIONS
OSASWL2  LU    LOCADDR=2
```

Table 6-3 lists the important parameters in the LU definition.

Table 6-3 Switched major node LU definition for SWOSAX3

Parameters	Explanation	Remarks
LOCADDR=0	LU local address at the PU	LOCADDR=0 denotes an independent LU.
MODETAB=MTAPPC	Logon mode table	Code a separate logon mode table for APPC.
LOCADDR=2		LOCADDR=2 denotes a dependent LU.

6.4.2 TCP/IP definitions

TCP/IP uses the OSA port as an LCS device. Each port has its own unique DEVICE and LINK statement that is defined in the TCP/IP profile.

Figure 6-2 on page 54 shows the network and the connections for our configuration example. Port `0` is connected to an Ethernet LAN, using IP address `192.168.4.3`.

Tip: The required TCP/IP definitions are in Example 6-4 on page 58.

1. Define one DEVICE statement per OSA port. Use the even device number of the two device numbers that are assigned in the hardware to the port.
    a. Define two device numbers per OSA port for TCP/IP mode, in HCD, because TCP/IP is running in full-duplex mode. One device is used by TCP/IP for reading and the other is used for writing.
    b. Using the DEVICE statement, define the DEVICE statement name, the DEVICE type (LCS) for the OSA port and the DEVICE number (the read device number, which is the even number).
2. Define one LINK statement per OSA TCP/IP DEVICE statement.

    Using the LINK statement, define the LINK name, the LINK type, the PORT number, and the DEVICE statement name.

> **Note:** Although the OSA port is addressed by the device number, the port number in the LINK statement must match the actual OSA port number.

3. Define the HOME IP address of the OSA port.
4. Using the `HOME` statement, define an IP address that refers to a `LINK` statement name.
5. Define static routes through the `BEGINROUTES` statement.
6. Define one **`START`** command per `DEVICE` name.

    After defining an OSA device in the TCP/IP profile, the device must still be started. Use one TCP/IP **`START`** statement with the `DEVICE` statement name for each TCP/IP READ device that must be started.

Example 6-4 shows the TCP/IP PROFILE definitions that are needed to define OSA to TCP/IP A.

Example 6-4 z/OS TCP/IP PROFILE definitions

```
; OSA DEFINITIONS FOR LCS  TCPIP PATHTHRU PORT 0
DEVICE OSA0040  LCS 0040
LINK   OSA0040LNK  ETHERNET  0   OSA0040
;
; OSA DEFINITIONS FOR LCS  TCPIP PATHTHRU PORT 1
;DEVICE OSA0042 LCS 0042
;LINK   OSA0042LNK  ETHERNET  1 OSA0042
;
HOME
   192.168.4.3    OSA0040LNK
;  192.168.4.4    OSA0042LNK
;
BEGINROUTES
ROUTE 192.168.4.0/24            = OSA0040LNK  MTU 1492
;ROUTE 192.168.4.0/24            = OSA0042LNK  MTU 1492
ENDROUTES
;
START OSA0040
;START OSA0042
```

6.5 Activating the connections

After all of the definitions are added to OSA/SF, VTAM, and TCP/IP, we can activate the configuration. Activation can require several tasks, such as:

- Verifying that the devices are online
- Activating VTAM resources (for an SNA environment)
- Activating TCP/IP

6.5.1 Verifying that devices are online

The z/OS console display command can verify that the required devices are online (see Figure 6-3).

```
D U,,,0040,2
IEE457I 11.03.53 UNIT STATUS 173
UNIT TYPE STATUS        VOLSER     VOLSTATE
0040 OSA  A-BSY
0041 OSA  A

D U,,,004A,1
IEE457I 11.04.33 UNIT STATUS 177
UNIT TYPE STATUS        VOLSER     VOLSTATE
004A OSA  A
```

Figure 6-3 z/OS Display U command

If they are not online, enter the z/OS console VARY command:

```
V (0040,0041,004A),ONLINE
```

6.5.2 VTAM activation

VTAM activation is no different from any other VTAM resource. Use the VTAM VARY NET command. Activate the XCA major node and the switched major node. Typically, the commands are of the following format:

```
V NET,ACT,ID=XCAOSAX3
V NET,ACT,ID=SWOSAX3
```

6.5.3 TCP/IP activation

There are three ways to activate TCP/IP devices:

- Restart the TCP/IP stack.
- Use the TCP/IP **obeyfile** command.
- Issue the z/OS command:

```
V TCPIP,tcpipproc,START,OSA0040
```

6.6 Relevant status displays

We monitored the status of the VTAM resources with the VTAM DISPLAY NET command. Figure 6-4 displays the XCA major node for the OSA-Express 1000Base-T connection.

```
D NET,E,ID=XCAOSAX3
IST097I DISPLAY ACCEPTED
IST075I NAME = XCAOSAX3, TYPE = XCA MAJOR NODE 704
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1021I MEDIUM=CSMA/CD,ADAPNO= 0,CUA=004A,SNA SAP= 4
IST1885I SIO = 54 SLOWDOWN = NO
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST170I LINES:
IST232I L004A000 ACTIV
IST232I L004A001 ACTIV
IST232I L004A002 ACTIV
IST314I END
```

Figure 6-4 Display of XCA major node

Figure 6-5 shows the results from the switched major node.

```
D NET,E,ID=SWOSAX3
IST097I DISPLAY ACCEPTED
IST075I NAME = SWOSAX3, TYPE = SW SNA MAJ NODE 707
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST084I NETWORK RESOURCES:
IST089I OSASW    TYPE = PU_T2           , CONCT
IST089I OSASWL1  TYPE = LOGICAL UNIT    , CONCT
IST089I OSASWL2  TYPE = LOGICAL UNIT    , CONCT
IST314I END
```

Figure 6-5 Display of switched major node

The NETSTAT DEV command displays the TCP/IP devices. Figure 6-6 shows both the device and link in the READY state.

```
DEVNAME: OSA0040          DEVTYPE: LCS       DEVNUM: 0040
  DEVSTATUS: READY
  LNKNAME: OSA0040LNK       LNKTYPE: ETH        LNKSTATUS: READY
    NETNUM: 0    QUESIZE: 0
    IPBROADCASTCAPABILITY: YES
    MACADDRESS: 00145E74A950
    ACTMTU: 1500
    SECCLASS: 255                MONSYSPLEX: NO
  BSD ROUTING PARAMETERS:
    MTU SIZE: N/A             METRIC: 00
    DESTADDR: 0.0.0.0         SUBNETMASK: 255.255.255.0
  MULTICAST SPECIFIC:
    MULTICAST CAPABILITY: YES
    GROUP            REFCNT      SRCFLTMD
    -----            ------      --------
    224.0.0.1        0000000001  EXCLUDE
      SRCADDR: NONE
```

Figure 6-6 Display of TCP/IP device and link

OSA/SF is a useful tool when verifying your setup. Example 6-5 shows the TCP/IP Passthru and the SNA devices for CHPID 06.

Example 6-5 Excerpt of the OAT showing the TCP/IP Passthru and SNA devices

```
START OF OSA ADDRESS TABLE
--------------------------

UA(Dev)   Mode Port        Entry specific information         Entry Valid
********************************************************************************
                           Image 1.1 (A11)
00(0040)* P-T  00  NO        192.168.4.3                        SIU  ALL
02(0042)  N/A                                                   N/A  CSS
03(0043)  N/A                                                   N/A  CSS
04(0044)  N/A                                                   N/A  CSS
05(0045)  N/A                                                   N/A  CSS
06(0046)  N/A                                                   N/A  CSS
07(0047)  N/A                                                   N/A  CSS
08(0048)  N/A                                                   N/A  CSS
09(0049)  N/A                                                   N/A  CSS
0A(004A)  SNA  00                                               SIU  ALL
```

Example 6-6 on page 62 shows another excerpt of the Query CHPID 06 command. We verified that our configuration was active and the mode that was configured.

Example 6-6 Excerpt of the OSA/SF Query CHPID 06 command output

```
INFORMATION FOR PORT 0
----------------------
  Port type                                                 1000Base-T Ethernet
  Configuration name                                 non qdio chpid 06 (ip+sna)
  LAN traffic state                                                     Enabled
  Port disabled state                                                       N/A
  Service mode                                                               No
  Modes configured                                         SNA, TCP/IP Passthru
  Local MAC address                                                00145E74A950
  Universal MAC address                                            00145E74A950
  Configured speed/mode                                          Auto negotiate
  Active speed/mode                                       1000 Mbps full duplex
  TCP port name                                                        1GIGPCIe
```

See Appendix D, “Useful setup and verification commands” on page 183, for a list of other useful commands.

7

Non-QDIO mode for the IBM z/VM operating system

This chapter describes customizing Open Systems Adapter-Express (OSA) channel path identifiers (CHPIDs) in non-Queued Direct I/O (non-QDIO) mode for TCP/IP and Systems Network Architecture (SNA for a z/VM environment. To configure an OSA CHPID in non-QDIO mode, the Open Systems Adapter Support Facility (OSA/SF) is required.

This chapter does *not* cover the setup process for an OSA CHPID running in *default* mode, using the default OSA Address Table (OAT). That information can be found in Appendix G, “TCP/IP Passthru mode” on page 219.

The information in this chapter covers the following topics:

7.1 Configuration information

Figure 7-1 shows a functional view of the connectivity that is described in this chapter for a non-QDIO OSA CHPID in a z/VM environment.

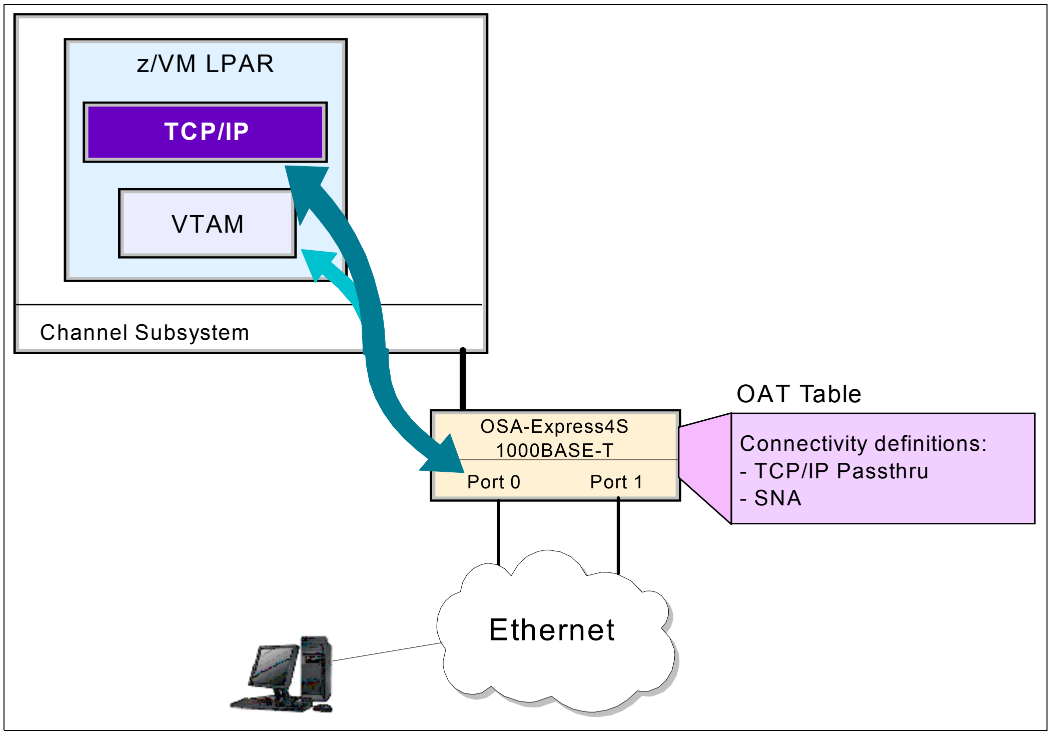


Figure 7-1 Non-QDIO mode shared port

The following elements must be configured and activated to use any type of OSA port in non-QDIO mode:

- Hardware definitions
- OSA configuration and OAT definitions
- Network definitions

7.2 Hardware definitions

The OSA CHPID, control unit, and OSA devices must be defined to HCD/IOCP and must be activated. See Chapter 3, “Hardware configuration definitions” on page 15, for the procedure to create the definitions.

Example 7-1 on page 65 shows the input/output configuration program (IOCP) definitions that we used for CHPID 06. For future considerations, we defined 15 OSA devices, although only three are necessary in our configuration.

Example 7-1 IOCP input for CHPID 06 example

```
ID NAME=SCZP401,UNIT=2827,MODEL=H43,DESC='Helix',              *
      SERIAL=00B8D72827,MODE=LPAR,LEVEL=H130331,               *
      LSYSTEM=SCZP401,SNAADDR=(USIBMSC,SCZP401),               *
RESOURCE PARTITION=((CSS(1),(A11,1),(A12,2),(A13,3))),
      MAXDEV=((CSS(1),65280,65535,65535)),
      DESCL=('COMMPLEX SC30','VMLINUX9','COMMPLEX SC31'),
      USAGE=(OS,OS,OS)
RESOURCE PARTITION=((CSS(2),(A2E,E),(A2F,F))),
      MAXDEV=((CSS(2),65280,65535,65535)),
      DESCL=('VMLINUX1','VMLINUX6'),
      USAGE=(OS,OS)
CHPID PATH=(CSS(1,2),06),SHARED,
      PARTITION=((CSS(1),(A11,A13),(=)),(CSS(2),(A2E),(=))),
DESC='Exp4S 1KBaseT OSE',PCHID=50C,TYPE=OSE
CNTLUNIT CUNUMBR=0040,PATH=((CSS(1),06)),UNIT=OSA
IODEVICE ADDRESS=(0040,15),UNITADD=00,CUNUMBR=(0040),UNIT=OSA
IODEVICE ADDRESS=004F,UNITADD=FE,CUNUMBR=(0040),UNIT=OSAD
```

7.3 OSA configuration and OAT definitions

To set up the data paths for the OSA port, two files are required:

- The OSA configuration file, which contains information pertaining to the hardware characteristics of the OSA port, such as MAC address, line speed, and timer values
- The OSA Address Table (OAT), with parameters that map the logical partition (LPAR), mode, unit address, and network protocol (TCP/IP and SNA) specifics to the OSA port

When the **Activate** option is selected from OSA/SF, the OSA configuration file and OAT are downloaded to the OSA, using the FE unit address (OSAD device). After they are downloaded, the OSA CHPID is automatically configured offline to all systems and then configured online. This causes the OSA hardware to be reset. It also activates the new OSA configuration.

In this chapter, we use the configuration that is shown in Figure 7-2 on page 66.

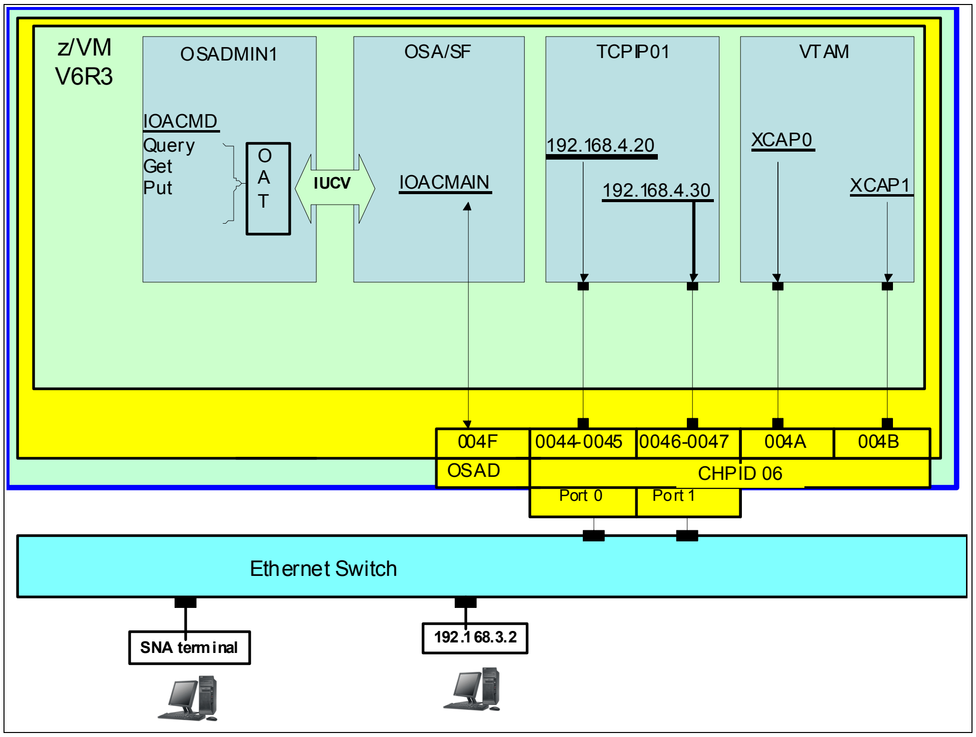


Figure 7-2 Connectivity layout

For information about installing and customizing OSA/SF for the z/VM operating system, as well as the user interface (OSA/SF operating system-based interface or OSA/SF GUI), see the *OSA-Express Customer's Guide and Reference*, SA22-7935.

If you want to use the OSA/SF OS-based command interface, you can follow the steps in Appendix F, "Using the OSA/SF operating system-based interface" on page 211.

7.4 Network definitions

In this section, we describe the Virtual Telecommunications Access Method (VTAM) and TCP/IP definitions that we used in our environment.

TCP/IP and VTAM coexist and share the OSA port. The definitions can be done independently, as though the OSA port were owned by VTAM or TCP/IP exclusively.

The OSA port is defined to TCP/IP as a LAN Channel Station (LCS). An LCS uses two devices for TCP/IP operation.

VTAM sees the OSA port as an external communications adapter (XCA). One OSA port is linked to one device for SNA operation.

Reminder: Port sharing is set up in OSA/SF, not in TCP/IP or VTAM.

7.4.1 VTAM definitions

This section describes the definitions that are required in VTAM to allow SNA applications to access the LAN over the OSA port. To describe the VTAM setup, we use the network configuration that is shown in Figure 7-2 on page 66. In this example, VTAM communicates over an Ethernet switch through ports 0 and 1 of OSA CHPID `06`, using device numbers `004A` and `004B`.

You need to define two types of major nodes in VTAM:

- External communications adapter (XCA) major node
- Switched network (SWNET) major node

External communications adapter (XCA) major node

Define one XCA major node for each SNA OSA device, and include this information:

- The node type (`VBUILD` definition statement)
- The port that is used by the LAN (port definition statement)
- The switched peripheral nodes (type 2) that are attached to an Ethernet LAN through an OSA port (`Group`, `Line`, and `PU` definition statements)

Example 7-2 and Example 7-3 show the VTAM coding to implement the connections. The PORT parameters map to the OAT entries is defined in Example 7-6 on page 73.

Example 7-2 XCA major node definitions for 004A

```
XCAP0    VBUILD TYPE=XCA
OSAX3P0  PORT  MEDIUM=CSMACD,                                          X
               ADAPNO=0,                                               X
               CUADDR=004A,                                            X
               TIMER=60,                                               X
               SAPADDR=8
****************************************
OSAX3GP0 GROUP DIAL=YES,                                               X
               DYNPU=YES,                                              X
               ANSWER=ON,                                              X
               AUTOGEN=(3,L,P),                                        X
               CALL=INOUT,                                             X
               ISTATUS=ACTIVE
```

Example 7-3 XCA major node definitions for 004B

```
XCAP1    VBUILD TYPE=XCA
OSAX3P1  PORT  MEDIUM=CSMACD,                                          X
               ADAPNO=1,                                               X
               CUADDR=004B,                                            X
               TIMER=60,                                               X
               SAPADDR=8
****************************************
OSAX3GP1 GROUP DIAL=YES,                                               X
               DYNPU=YES,                                              X
               ANSWER=ON,                                              X
               AUTOGEN=(3,L,P),                                        X
               CALL=INOUT,                                             X
               ISTATUS=ACTIVE
```

Table 7-1 lists the PORT parameters

Table 7-1 XCA major node port definition for XCAP0 and XCAP1

Required parameters	Explanation	Remarks
`TYPE=XCA`	XCA major node	The OSA functions as an `XCA` to VTAM.
`ADAPNO=0`	PORT statement	Code `ADAPNO=0` for port 0 of OSA-Express 1000BASE-T
`CUADDR= 004A (or 004B)`	Channel unit address	Code the device number defined for this port. In our example, VTAM uses device number `004A` for port `0`.
`MEDIUM= CSMACD`	LAN type	Use `CSMACD` for Ethernet.
`SAPADDR=08`	Service access point address	Code a value that is a multiple of 4. This address *must* be unique for each VTAM that communicates with a port. Use different SAP addresses if a port is shared by multiple VTAMs. See the SAPADDR value of `XCAOSAX3` in Chapter 6, “Non-QDIO mode for the IBM z/OS operating system” on page 51.

Table 7-2 identifies the significant GROUP parameters.

Table 7-2 XCA major node group definition for XCAP0 and XCAP1

Required parameters	Explanation	Remarks
`DIAL=YES`	Switched peripheral node	You *must* code `DIAL=YES` to specify that the switched line control protocol is required.
`AUTOGEN= (3,L,P)`	Auto-generation of LINE and PU statements	This parameter enables VTAM to automatically generate three sets of `LINE` and peripheral physical unit (`PU`) statements. The `LINE` names begin with *L*. The `PU` names begin with *P*.

Note: The current OSA features in System zEC12 servers support 4096 SNA PU Type 2 connections per port.

7.4.2 TCP/IP definitions

TCP/IP uses the OSA port as an LCS device. Each port has a unique `DEVICE` and `LINK` statement that is defined in the TCP/IP profile.

Figure 7-2 on page 66 shows the network and the connections for our configuration example. Port 0 is connected to an Ethernet switch, using IP address `192.168.4.20`, while port 1 is using IP address `192.168.4.30`. These parameters map to the OAT entries that are defined in Example 7-6 on page 73.

1. Define one `DEVICE` statement per OSA port. Use the *even* device number of the two device numbers that are assigned in the hardware to the port.

   Using the `DEVICE` statement, define the DEVICE statement name, the DEVICE type (LCS) for the OSA port, and the DEVICE number (the read number, which is the even number).

2. Define one LINK statement for each OSA TCP/IP DEVICE statement.

   Using the LINK statement, define the LINK name, the LINK type, the PORT number, and the DEVICE statement name.

   > **Note:** Although the OSA port is addressed by the device number, the port number in the LINK statement must match the actual OSA port number.

3. Define the HOME IP address of the OSA port (the IP address refers to the LINK statement name).
4. Define static routes through the GATEWAY statement.
5. Define one **START** command per DEVICE name.

   After defining an OSA device in the TCP/IP profile, the device must still be started. There is one TCP/IP **START** statement entry per TCP/IP device. It uses the DEVICE statement name.

   Example 7-4 shows the TCP/IP PROFILE definitions for an OSA port.

Example 7-4 z/VM TCP/IP PROFILE definitions

```
; OSA DEFINITIONS FOR LCS  TCPIP PATHTHRU
; -------------------------------------------
DEVICE DEV_0044  LCS 0044
LINK   DEV_0044 ETHERNET 00 DEV_0044
DEVICE DEV_0046  LCS 0046
LINK   DEV_0046 ETHERNET 01 DEV_0046
; -------------------------------------------
HOME
192.168.4.20 255.255.255.0 DEV_0044
192.168.4.30 255.255.255.0 DEV_0046
START DEV_0044
; START DEV_0046
```

7.5 Activating the connections

After all of the definitions were added to OSA/SF, VTAM, and TCP/IP, we activated the configuration. Activation includes the following tasks:

- Verify that the devices are online.
- Activate the VTAM resources.
- Activate TCP/IP.

7.5.1 Verifying that devices are online

You can use the z/VM console display command (**CP Q OSA**) to verify that the required devices are online (see Figure 7-3).

```
CP Q OSA
OSA  0044 ATTACHED TO TCPIP01  0044 DEVTYPE OSA        CHPID 06 OSE
OSA  0045 ATTACHED TO TCPIP01  0045 DEVTYPE OSA        CHPID 06 OSE
OSA  0046 ATTACHED TO TCPIP01  0046 DEVTYPE OSA        CHPID 06 OSE
OSA  0047 ATTACHED TO TCPIP01  0047 DEVTYPE OSA        CHPID 06 OSE
OSA  004A ATTACHED TO VTAM     004A DEVTYPE OSA        CHPID 06 OSE
OSA  004B ATTACHED TO VTAM     004B DEVTYPE OSA        CHPID 06 OSE
```

Figure 7-3 z/VM Q OSA command

If they are not online, enter the z/VM console **VARY ON** on command:

```
VARY ONLINE 004A 004B
```

7.5.2 VTAM activation

VTAM activation is no different from any other VTAM resource. Use the VTAM **VARY NET** command. Activate the XCA major node and the switched major node. The commands have the following syntax:

```
V NET,ACT,ID=XCAP0
V NET,ACT,ID=XCAP1
```

7.5.3 TCP/IP activation

There are two ways to activate TCP/IP devices:

- Restart the TCP/IP stack.
- Use the TCP/IP **obeyfile** command.

7.6 Relevant status displays

We queried the status of the VTAM resources with the VTAM **DISPLAY NET** command. Example 7-5 on page 71 displays the XCA major node for the OSA connection.

Example 7-5 Results of the XCA majnode display command

```
vtam d net,id=xcap0,scope=all
Ready;
IST097I DISPLAY ACCEPTED
IST075I NAME = XCAP0, TYPE = XCA MAJOR NODE
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1021I MEDIUM=CSMA/CD,ADAPNO= 0,CUA=004A,SNA SAP= 8
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST170I LINES:
IST232I L004A000, ACTIV
IST232I L004A001, ACTIV
IST232I L004A002, ACTIV
IST314I END
vtam d net,id=xcap1,scope=all
Ready;
IST097I DISPLAY ACCEPTED
IST075I NAME = XCAP1, TYPE = XCA MAJOR NODE
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1021I MEDIUM=CSMA/CD,ADAPNO= 1,CUA=004B,SNA SAP= 8
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST170I LINES:
IST232I L004B000, ACTIV
IST232I L004B001, ACTIV
IST232I L004B002, ACTIV
IST314I END
```

The **NETSTAT DEV** command displays the TCP/IP devices. Figure 7-4 shows both the device and link in the READY state.

```
netstat dev
VM TCP/IP Netstat Level 630        TCP/IP Server Name: TCPIP01

Device DEV_0044               Type: LCS           Status: Ready
  Queue size: 0     CPU: 0    Address: 0044
    Link DEV_0044             Type: ETHERNET      Net number: 0
      Speed: 10000000
      BytesIn: 62             BytesOut: 0
      Forwarding: Enabled     MTU: 1500
      IPv4 Path MTU Discovery: Disabled
      Broadcast Capability: Yes
      Multicast Capability: Yes
      IPv4 VIPA ARP
      Multicast Group                        Members
      ---------------                        -------
      224.0.0.1                                 1

Device DEV_0046               Type: LCS           Status: Inactive
  Queue size: 0     CPU: 0    Address: 0046
    Link DEV_0046             Type: ETHERNET      Net number: 1
      Speed: 10000000
      BytesIn: 0              BytesOut: 0
      Forwarding: Enabled     MTU: 1500
      IPv4 Path MTU Discovery: Disabled
      Broadcast Capability: Yes
      Multicast Capability: Unknown
```

Figure 7-4 Display of TCP/IP device and link

OSA/SF is also useful for the verification of your setup. We used the OSA/SF administration user, `OSADMIN2`, and the **ioacmd** command. Example 7-6 on page 73 shows both the TCP/IP Passthru and the SNA devices for our OSA CHPID `06`.

Example 7-6   Extract of the OAT showing TCP/IP Passthru and SNA devices

```
***              Start of OSA address table for CHPID 06             ***
************************************************************************
* UA(Dev) Mode     Port     Entry specific information      Entry  Valid
************************************************************************
                               Image 1.1 (A11     )
00(0040)* passthru  00  no  192.168.004.003                      S   ALL
02(0042)* passthru  01  no  192.168.004.004                      S   ALL
04(0044)  N/A                                                    N/A CSS
05(0045)  N/A                                                    N/A CSS
06(0046)  N/A                                                    N/A CSS
07(0047)  N/A                                                    N/A CSS
08(0048)  N/A                                                    N/A CSS
09(0049)  N/A                                                    N/A CSS
0A(004A)  SNA       00                                           SIU ALL
0B(004B)  SNA       01                                           S   ALL
0C(004C)  N/A                                                    N/A CSS
************************************************************************
                               Image 1.2 (A12     )
00(0040)  N/A                                                    N/A CSS
01(0041)  N/A                                                    N/A CSS
02(0042)  N/A                                                    N/A CSS
03(0043)  N/A                                                    N/A CSS
04(0044)* passthru  00  no  192.168.004.020                      SIU ALL
06(0046)* passthru  01  no  192.168.004.030                      S   ALL
08(0048)  N/A                                                    N/A CSS
09(0049)  N/A                                                    N/A CSS
0A(004A)  SNA       00                                           S   ALL
0B(004B)  SNA       01                                           S   ALL
0C(004C)  N/A                                                    N/A CSS
0D(004D)  N/A                                                    N/A CSS
0E(004E)  N/A                                                    N/A CSS
0F(004F)  N/A                                                    N/A CSS
```

Example 7-7 shows another extract of the OSA/SF query for CHPID 06. We verified that our configuration was active and that the mode configured was correct.

Example 7-7   Extract of the OSA/SF query CHPID 06 command output

```
INFORMATION FOR PORT 0
----------------------
  Port type                                                  1000Base-T Ethernet
  Configuration name                                  non qdio chpid 06 (ip+sna)
  LAN traffic state                                                      Enabled
  Port disabled state                                                        N/A
  Service mode                                                                No
  Modes configured                                          SNA, TCP/IP Passthru
  Local MAC address                                                 00145E74A950
  Universal MAC address                                             00145E74A950
  Configured speed/mode                                           Auto negotiate
  Active speed/mode                                        1000 Mbps full duplex
  TCP port name                                                         1GIGPCIe
```

See Appendix D, “Useful setup and verification commands” on page 183, for a list of other helpful commands.

8

QDIO and non-QDIO modes for the IBM z/VSE operating system

This chapter covers the basic implementation steps to establish network connectivity with an Open Systems Adapter-Express channel path identifier (CHPID) in Queued Direct I/O (QDIO) mode or non-QDIO mode in an IBM System z VSE (z/VSE) environment. OSA-Express in QDIO mode has been supported since IBM VSE/ESA 2.6 (Virtual Storage Extended/Enterprise Systems Architecture). To configure an OSA CHPID in non-QDIO mode, Open Systems Adapter Support Facility (OSA/SF) is required.

The information in this chapter covers the following topics:

- 8.1, “QDIO compared to non-QDIO in z/VSE” on page 76
- 8.2, “Related publications” on page 77

8.1 QDIO compared to non-QDIO in z/VSE

IBM z/VSE software supports QDIO and non-QDIO mode. OSA-Express in QDIO mode has been supported since VSE/ESA 2.6. To access an OSA-Express adapter in QDIO mode, you need three OSA-Express devices:

- A read device
- A write device
- A data path device

To configure an OSA CHPID in non-QDIO mode, OSA/SF is required.

Note: Use QDIO mode whenever possible.

8.1.1 TCP/IP stacks in z/VSE

In z/VSE, there are two TCP/IP products from vendors that can use OSA-Express adapters.

- TCP/IP for VSE/ESA (licensed from Connectivity Systems, Inc.)

  This is a well-known TCP/IP stack with applications for IPv4 traffic. It provides secure transmission of data by using the SSL protocol.

  For more information about TCP/IP for VSE/ESA, see the CSI website:

  http://www.csi-international.com/

- IPv6/VSE (licensed from Barnard Software Inc.)

  This is a full-function TCP/IP stack with applications for IPv4 and IPv6 network traffic. Since December 2012, secured transmission of data by using the Secure Sockets Layer (SSL) protocol, HTTPS, FTPS, SMTPS, and TN3270E over SSL are supported. It is available for z/VSE 4.3 and z/VSE 5.1.

  For more information about IPv6/VSE, see the Barnard Software website:

  http://www.bsiopti.com

8.1.2 TCP/IP setup with OSA CHPID in QDIO mode

Setting up TCP/IP is a relatively simple process, but we do not describe it here. Just one short remark: The device numbers in the DEV parameter of the DEFINE LINK statement (TCP/IP for VSE/ESA) or DEVICE statement (IPv6/VSE) must be an even/odd pair for the read and write device. If it is running on z/VM, ensure that the real device numbers that are generated in the IOCP are an even/odd pair.

Additionally the device number of the write device has to be the successor (+1) of the device number of the read device.

Setup of OSA in TCP/IP for VSE/ESA

In TCP/IP for VSE/ESA, you define a LINK with type OSAX.

```
DEFINE LINK,ID=...,TYPE=OSAX,DEV=cuu1,DATAPATH=cuu3,IPADDR=addr,..
```

OSA setup in IPv6/VSE

In IPv6/VSE, you define a DEVICE with type OSAX.

```
DEVICE device_name OSAX cuu1 portname cuu3
```

8.1.3 TCP/IP setup with OSA CHPID in non-QDIO mode

Setting up TCP/IP for OSA CHPID in non-QDIO mode needs some preparation work. You first have to configure the OSA CHPID with OSA/SF.

Note: Use QDIO mode where possible.

Setup of OSA in TCP/IP for VSE/ESA

In TCP/IP for VSE/ESA, you define a LINK with type OSA.

```
DEFINE LINK,ID=...,TYPE=OSA,DEV=(cuu1,cuu2), .......
```

Setup of OSA in IPv6/VSE

When using IPv4, use the following DEVICE command:

```
DEVICE device_name OSA cuu1 ETHERNET
```

IPv6 is not supported by CHPID type OSE.

8.2 Related publications

For more information about TCP/IP in z/VSE, see the following publications:

- *Enhanced Networking on IBM z/VSE*, SG24-8091
- *Introduction to the New Mainframe: z/VSE Basics*, SG24-7436
- *z/VSE Planning*, SC33-8301
- *z/VSE Administration*, SC33-8304
- *z/VSE Operation*, SC33-8309
- *z/VSE V5R1 e-business Connectors User's Guide*, SC34-2629
- *z/VSE V5R1 TCP/IP Support*, SC34-2640

9

IBM z/OS virtual MAC support

Virtual Media Access Control (VMAC) support for the IBM z/OS Communications Server is a function that affects the operation of an Open Systems Adapter-Express (OSA) interface at the OSI Layer 2 level, which is the data link control (DLC) layer with its sublayer, Media Access Control (MAC).

The information in this chapter covers the following topics:

9.1 Virtual MAC overview

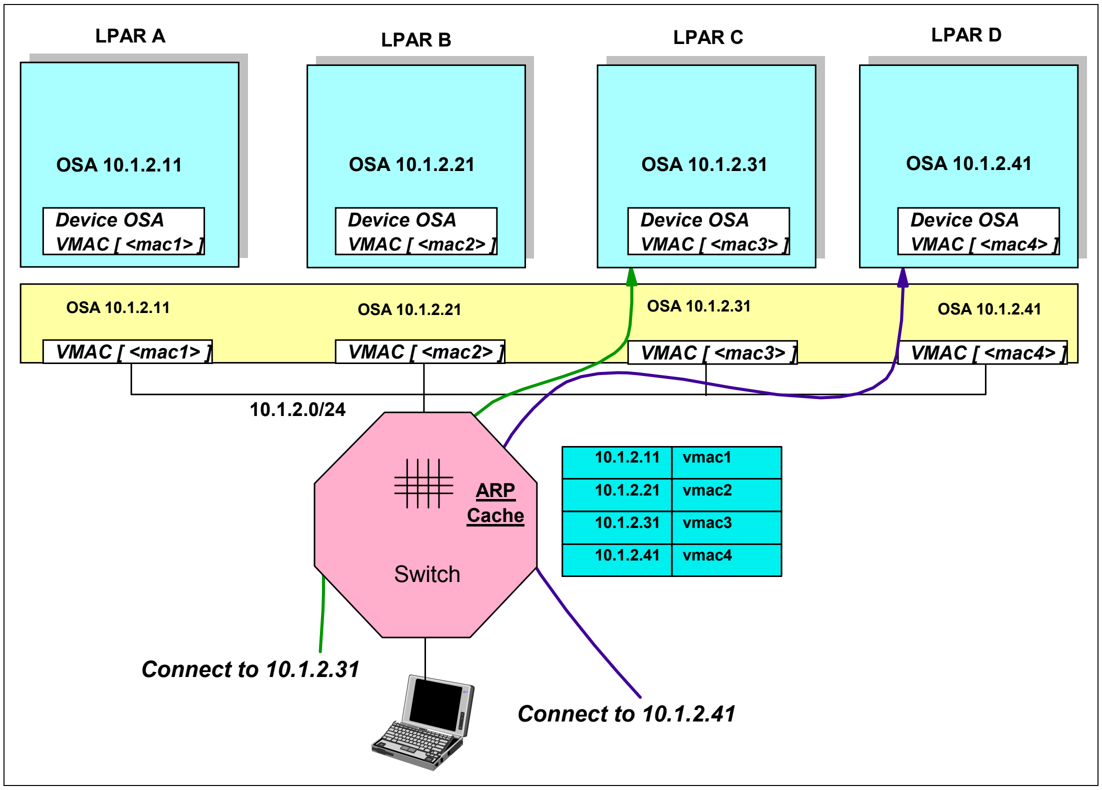
Before the introduction of the *virtual* MAC function (VMAC), an OSA interface had only one MAC address. This restriction caused problems when using load balancing technologies with z/OS TCP/IP stacks that share OSA interfaces. The single MAC address of the OSA also causes a problem when using a z/OS TCP/IP stack as a forwarding router for packets that are destined to unregistered IP addresses.

VMAC support enables an OSA interface to have not only a physical MAC address but also multiple virtual MAC addresses for each device or interface in the stack. Each stack can define up to eight VMACs per protocol (IPv4 or IPv6) for each OSA interface.

Using VMACs, forwarding decisions in the OSA can be made without having to involve the OSI Layer 3 level (network layer / IP layer). From the LAN perspective, the OSA interface with a VMAC appears as a dedicated device or interface to a TCP/IP stack. Packets that are destined for a TCP/IP stack are identified by an assigned VMAC address, and packets sent to the LAN from the stack use the VMAC address as the source MAC address. This means that all IP addresses associated with an IBM z/OS TCP/IP stack are accessible by using their own VMAC addresses rather than sharing a single physical MAC address of an OSA interface.

9.1.1 Virtual MAC concept

Figure 9-1 on page 81 shows how the definition of VMACs in the z/OS TCP/IP stacks gives the appearance of having a dedicated OSA interface on each stack. When packets arrive at the shared OSA interface, the individual VMAC assignments allow the packets to be forwarded directly to the correct stack. In this example, no individual stack needs to be defined as a primary or secondary router, which offloads this function from the z/OS TCP/IP stack.



10.1.2.11	vmac1
10.1.2.21	vmac2
10.1.2.31	vmac3
10.1.2.41	vmac4

Figure 9-1 Forwarding packets to VMAC targets

This simplifies a shared OSA configuration significantly. Defining VMACs uses few system resources. It is an alternative to Generic Route Encapsulation (GRE) or network address table (NAT) when load balancing technologies are used.

For IPV6, TCP/IP uses the VMAC address for all neighbor discovery address resolution flows for that stack’s IP addresses. Likewise, it uses the VMAC as the source MAC address for all IPv6 packets that are sent from that stack. From a LAN perspective, the OSA interface with a VMAC appears as a dedicated device to that stack.

Note: VMACs supersede primary and secondary routing. VMAC definitions on a device in a z/OS TCP/IP stack override any `NONRouter`, `PRIRouter`, or `SECRouter` parameters. If necessary, selected stacks on a shared OSA can define the device with VMAC and others can define the device with `PRIRouter` and `SECRouter` capability.

9.1.2 Virtual MAC address assignment

The VMAC address can be defined in the stack or generated by the OSA. If it is generated by the OSA, it is unique among all other physical MAC addresses and all other VMAC addresses that are generated by any OSA-Express feature.

Note: Allow the OSA to generate the VMACs rather than assigning an address in the TCP/IP profile. If VMACs are defined in the TCP/IP profile, they must be defined as locally administered MAC addresses and must be unique to the LAN where they reside.

The same VMAC can be defined for both IPv4 and IPv6 use, or a stack can use one VMAC for IPv4 and one for IPv6. Also, a VLAN ID can be associated with an OSA-Express device or interface that is defined with a VMAC.

9.2 Virtual MAC implementation

In this section, we describe a scenario in which two OSA ports are shared between TCPIPE and TCPIPF. We define VMACs for those two z/OS TCP/IP stacks. From a LAN perspective, the OSA ports of both stacks then appear as dedicated devices or interfaces. See Figure 9-2 on page 83.

When implementing VMAC support, keep in mind the following points:

- The VMAC function is available only for OSA interfaces that are configured in QDIO mode.
- Each stack can define one VMAC per protocol (IPv4 or IPv6) for each OSA interface.
- If a VMAC is defined, the stack does not receive any packets that are destined to the physical MAC.
- VLAN IDs also apply to VMACs, such as physical MACs.
- Allow the OSA to generate VMAC addresses.
- When configuring VMACs to solve load balancing problems, remember to do these tasks:
  - Remove GRE tunnels as appropriate.
  - Change external load balancer configurations (such as directed mode to dispatch mode).

Note: To enable virtual MAC support, you must be running at least an IBM System z9® Enterprise Class (z9EC) or System z 9 Business Class (z9BC) system and have an OSA-Express feature with OSA Layer 3 virtual MAC support.

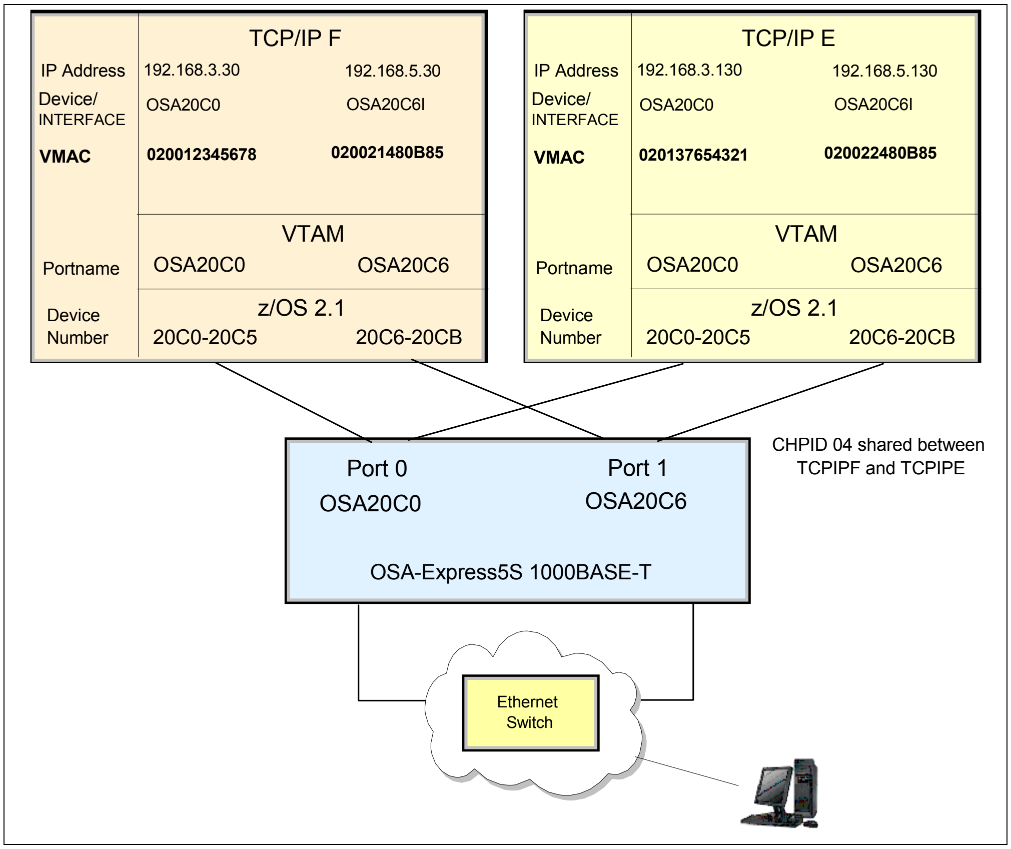


Figure 9-2 Our configuration for the implementation of VMAC

We shared an OSA-Express5S 1000BASE-T feature (CHPID 04) between the TCPIPF and TCPIPE stacks.

We configured port 0 of the OSA-Express5S 1000Base-T within TCPIPF and TCPIPE by using the `DEVICE`, `LINK`, and `HOME` statements.

Note: Figure 9-2 is used only for demonstration purposes. We do *not* recommend implementing any configuration with a single point of failure.

Configuring the VMAC

The VMAC can be defined on either the `LINK` statement or the `INTERFACE` statement in the TCP/IP profile. Example 9-1 on page 84 and Example 9-2 on page 84 show the VMAC definitions for TCPIPF and TCPIPE and their OSA ports.

*Example 9-1 DEVICE/LINK (**port 0**) and INTERFACE (**port 1**) VMAC definition for TCPIPF*

```
DEVICE OSA20C0  MPCIPA
LINK   OSA20C0LNK  IPAQENET      OSA20C0 VMAC 020012345678 1
;
INTERFACE OSA20C6I
    DEFINE IPAQENET
    PORTNAME OSA20C6
    IPADDR 192.168.5.30/24
    MTU 1492
    VMAC ROUTEALL 2
HOME
   192.168.3.30 OSA20C0LNK
BEGINROUTES
 ROUTE DEFAULT              192.168.3.1     OSA20C0LNK    MTU 1492
 ROUTE 192.168.3.0 255.255.255.0 =          OSA20C0LNK    MTU 1492
 ROUTE 192.168.5.0 255.255.255.0 =          OSA20C6I      MTU 1492
ENDROUTES
```

If VMAC is defined without a MAC address 2, OSA generates a VMAC by using a part of the burned-in MAC address of the OSA. (We intentionally specified `ROUTEALL` here, which is the default for demonstration purposes only.)

You can also specify the MAC address for VMAC 1. as we did when defining OSA port 0 of the OSA-Express5S 1000BASE-T feature. If you decide to specify a MAC address, it must be a locally administered address, which means that bit 6 of the first byte is `1` and bit 7 of the first byte is `0`.

*Example 9-2 DEVICE/LINK (**port 0**) and INTERFACE (**port 1**) VMAC definition for TCPIPE*

```
DEVICE OSA20C0  MPCIPA
LINK   OSA20C0LNK  IPAQENET      OSA20C0 VMAC 020087654321 1
;
INTERFACE OSA20C6I
    DEFINE IPAQENET
    PORTNAME OSA20C6
    IPADDR 192.168.5.130/24
    MTU 1492
    VMAC ROUTEALL
;
HOME
   192.168.3.130 OSA20C0LNK
BEGINROUTES
 ROUTE DEFAULT              192.168.3.1     OSA20C0LNK    MTU 1492
 ROUTE 192.168.3.0 255.255.255.0 =          OSA20C0LNK    MTU 1492
 ROUTE 192.168.5.0 255.255.255.0 =          OSA20C6I      MTU 1492
ENDROUTES
```

Note: There is no need to define `PRIRouter` or `SECRouter` in the `DEVICE` statement. Also, when VMAC is specified on the `LINK` statement, `PRIRouter` and `SECRouter` are ignored.

ROUTELCL option

The ROUTELCL option on the VMAC statement specifies that only traffic that is destined to the virtual MAC and with a destination IP address that is registered with the OSA-Express device by this TCP/IP stack is forwarded by the OSA. ROUTELCL requires the IP address to be registered to OSA for the packet to be properly routed. This is the suggested setting for non-routing z/OS IP stacks. ROUTEALL requires only the VMAC address to match for inbound routing and is used when the z/OS IP stack is doing IP routing.

9.2.1 Verification

We verified that our VMACs were correctly defined in TCPIPF (see Example 9-3) and TCPIPE (see Example 9-4 on page 86).

Example 9-3 Display VMACs of both OSA-Express5S ports on TCPIPF

```
D TCPIP,,N,DEV
DEVNAME: OSA20C0           DEVTYPE: MPCIPA
  DEVSTATUS: READY
  LNKNAME: OSA20C0LNK        LNKTYPE: IPAQENET    LNKSTATUS: READY
    SPEED: 0000000100
    IPBROADCASTCAPABILITY: NO
    VMACADDR: 020012345678 1 VMACORIGIN: CFG 2 VMACROUTER: ALL
    ARPOFFLOAD: YES                ARPOFFLOADINFO: YES
    ACTMTU: 1492
    VLANID: NONE                   VLANPRIORITY: DISABLED
...
INTFNAME: OSA20C6I          INTFTYPE: IPAQENET   INTFSTATUS: READY
    PORTNAME: OSA20C6 DATAPATH: 20C8 DATAPATHSTATUS: READY
    SPEED: 0000000100
    IPBROADCASTCAPABILITY: NO
    VMACADDR: 020021850B85 3 VMACORIGIN: OSA 4 VMACROUTER: ALL
    ARPOFFLOAD: YES                  ARPOFFLOADINFO: YES
    CFGMTU: 1492                     ACTMTU: 1492
    IPADDR: 192.168.5.30/24
    VLANID: NONE                     VLANPRIORITY: DISABLED
```

We specified a MAC address 1 for the OSA-Express5S 1000BASE-T port 0 in TCPIPF and TCPIPE, so VMACORIGIN is CFG 2. Because we did not specify a MAC address for the OSA-Express5S 1000BASE-T port 1 in TCPIPF and TCPIPE, the OSA generated the MAC address 3. Because this is an OSA-generated MAC address, VMACORIGIN is OSA 4.

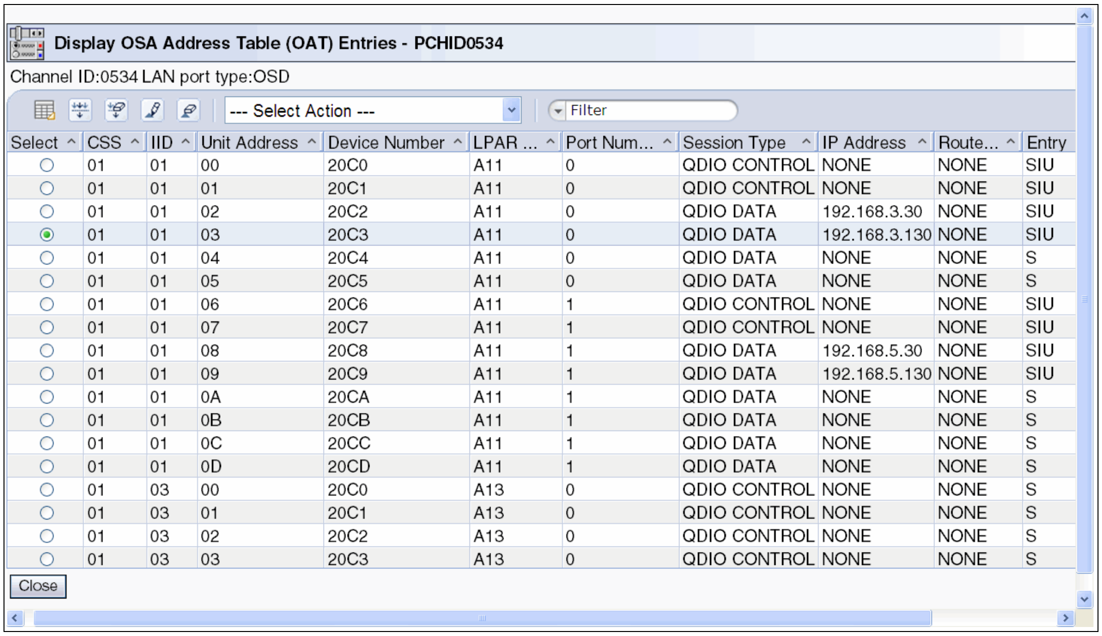
Example 9-4 Display VMACs of both OSA-Express5S ports on TCPIPE

```
D TCPIP,,N,DEV
DEVNAME: OSA20C0          DEVTYPE: MPCIPA
  DEVSTATUS: READY
  LNKNAME: OSA20C0LNK        LNKTYPE: IPAQENET    LNKSTATUS: READY
    SPEED: 0000000100
    IPBROADCASTCAPABILITY: NO
    VMACADDR: 020137654321 1 VMACORIGIN: CFG 2 VMACROUTER: ALL
    ARPOFFLOAD: YES                ARPOFFLOADINFO: YES
    ACTMTU: 1492
    VLANID: NONE                   VLANPRIORITY: DISABLED
...
INTFNAME: OSA20C6I          INTFTYPE: IPAQENET   INTFSTATUS: READY
    PORTNAME: OSA20C6 DATAPATH: 20C8     DATAPATHSTATUS: READY
    SPEED: 0000000100
    IPBROADCASTCAPABILITY: NO
    VMACADDR: 020022850B85 3 VMACORIGIN: OSA 4 VMACROUTER: ALL
    ARPOFFLOAD: YES                  ARPOFFLOADINFO: YES
    CFGMTU: 1492                     ACTMTU: 1492
    IPADDR: 192.168.5.130/24
    VLANID: NONE                     VLANPRIORITY: DISABLED
```

We can also see the VMAC in the OSA Address Table (OAT) that is queried by Display OAT entries on the Hardware Management Console (HMC), as shown in Figure 9-3 on page 87 and Figure 9-4 on page 87. OSA registers all IP addresses (including Virtual IP Addresses, or VIPAs) in the z/OS TCP/IP stack, and maps them to the VMAC address.

Notice that the last 3 bytes of the OSA-generated VMAC 7 are identical to that of the universal MAC address, the burned-in address of the OSA 5 (see Figure 9-5 on page 88). The first byte of the OSA-generated VMAC is always 02, which is to make the VMAC a locally administered address. To make the VMAC unique among all z/OS TCP/IP stacks, the second and third bytes are used as a counter that is incremented each time that OSA generates a MAC address.

The OSA-Express5S does not support the Open Systems Adapter Support Facility (OSA/SF) GUI, but we displayed OAT entries on the HMC, as shown in Figures Figure 9-3 on page 87 and Figure 9-4 on page 87.

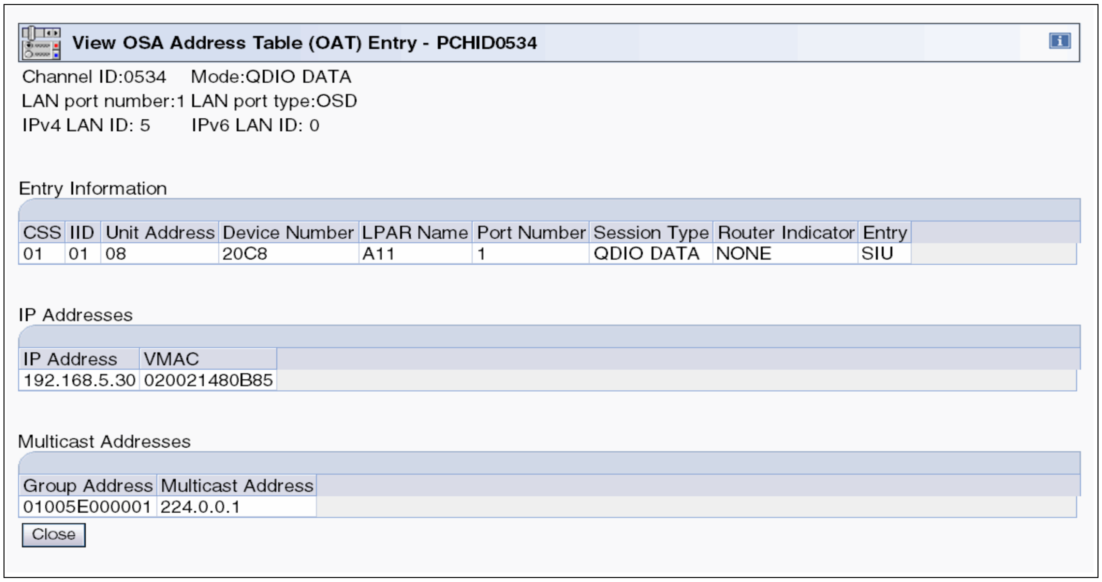


Display OSA Address Table (OAT) Entries - PCHID0534

Channel ID:0534 LAN port type:OSD

Select	CSS	IID	Unit Address	Device Number	LPAR ...	Port Num...	Session Type	IP Address	Route...	Entry
○	01	01	00	20C0	A11	0	QDIO CONTROL	NONE	NONE	SIU
○	01	01	01	20C1	A11	0	QDIO CONTROL	NONE	NONE	SIU
○	01	01	02	20C2	A11	0	QDIO DATA	192.168.3.30	NONE	SIU
●	01	01	03	20C3	A11	0	QDIO DATA	192.168.3.130	NONE	SIU
○	01	01	04	20C4	A11	0	QDIO DATA	NONE	NONE	S
○	01	01	05	20C5	A11	0	QDIO DATA	NONE	NONE	S
○	01	01	06	20C6	A11	1	QDIO CONTROL	NONE	NONE	SIU
○	01	01	07	20C7	A11	1	QDIO CONTROL	NONE	NONE	SIU
○	01	01	08	20C8	A11	1	QDIO DATA	192.168.5.30	NONE	SIU
○	01	01	09	20C9	A11	1	QDIO DATA	192.168.5.130	NONE	SIU
○	01	01	0A	20CA	A11	1	QDIO DATA	NONE	NONE	S
○	01	01	0B	20CB	A11	1	QDIO DATA	NONE	NONE	S
○	01	01	0C	20CC	A11	1	QDIO DATA	NONE	NONE	S
○	01	01	0D	20CD	A11	1	QDIO DATA	NONE	NONE	S
○	01	03	00	20C0	A13	0	QDIO CONTROL	NONE	NONE	S
○	01	03	01	20C1	A13	0	QDIO CONTROL	NONE	NONE	S
○	01	03	02	20C2	A13	0	QDIO CONTROL	NONE	NONE	S
○	01	03	03	20C3	A13	0	QDIO CONTROL	NONE	NONE	S

Figure 9-3 Display OSA address table (OAT) entries



View OSA Address Table (OAT) Entry - PCHID0534

Channel ID:0534 Mode:QDIO DATA
LAN port number:1 LAN port type:OSD
IPv4 LAN ID: 5 IPv6 LAN ID: 0

Entry Information

CSS	IID	Unit Address	Device Number	LPAR Name	Port Number	Session Type	Router Indicator	Entry
01	01	08	20C8	A11	1	QDIO DATA	NONE	SIU

IP Addresses

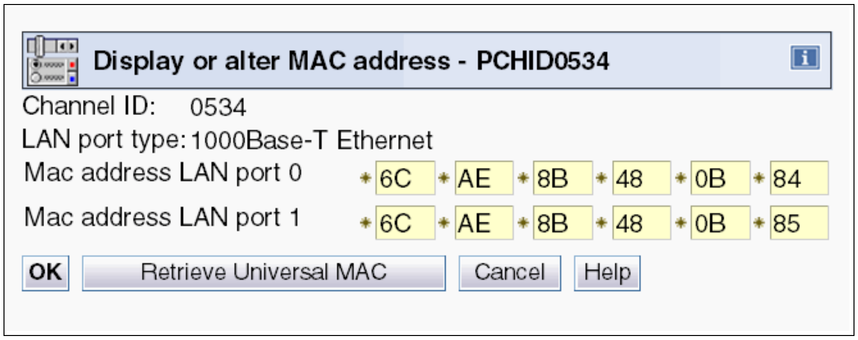
IP Address	VMAC
192.168.5.30	020021480B85

Multicast Addresses

Group Address	Multicast Address
01005E000001	224.0.0.1

Figure 9-4 The details of View OSA Address Table (OAT) entry

Figure 9-5 shows our display of the MAC addresses.



Display or alter MAC address - PCHID0534

Channel ID: 0534

LAN port type: 1000Base-T Ethernet

Mac address LAN port 0	6C	AE	8B	48	0B	84
Mac address LAN port 1	6C	AE	8B	48	0B	85

Figure 9-5 Display or alter MAC address

10

VLAN support

Virtual local area network (VLAN) technology is becoming more important in network planning. A VLAN is a logical grouping of nodes that might be physically separate but can be connected by using switches. A VLAN provides many benefits, such as improved network performance by reducing traffic on a physical LAN, enhanced security by isolating traffic, and providing more flexibility in configuring networks.

The VLAN IEEE standard 802.1p/Q is supported by OSA-Express3, OSA-Express4S, and OSA-Express5S when running in QDIO mode.

This chapter briefly explains the concepts of VLANs and provides examples of how to set up VLAN support in the TCP/IP stacks of IBM z/OS, IBM z/VM, and IBM Linux on System z operating systems. It covers the following topics:

10.1 VLAN overview

A VLAN is a group of workstations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN, even though they might not be on the same LAN segment. VLANs can be used to increase bandwidth and reduce overhead by allowing networks to be organized for optimum traffic flow.

Figure 10-1 shows an example of VLANs segmented into logically defined networks.

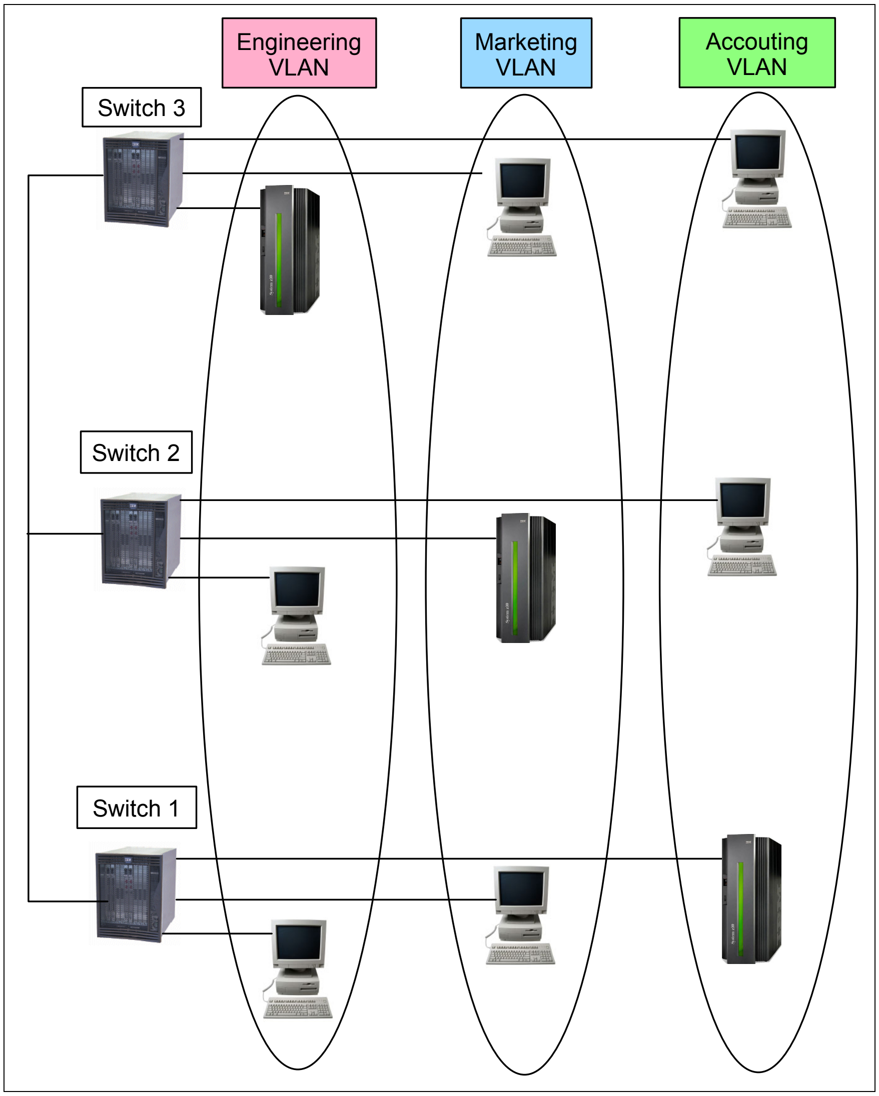


Figure 10-1 Logically defined networks that are using VLANs

10.1.1 Types of connections

IEEE 802.1p/Q VLANs operate by defining switch ports as members of virtual LANs. Devices on a VLAN can be connected in three ways, depending on whether the connected devices are VLAN-aware or VLAN-unaware: trunk mode, access mode, or a hybrid of the two. VLAN-aware devices understand VLAN memberships (which users belong to a particular VLAN) and VLAN formats.

Ports that are used to attach VLAN-unaware equipment are called *access ports*, and ports that are used to connect to other switches or VLAN-aware servers are known as *trunk ports*. Network frames that are generated by VLAN-aware equipment are marked with a *tag,* which identifies the frame to the VLAN.

Trunk mode

Trunk mode indicates that the switch should allow all VLAN ID tagged packets to pass through the switch port without altering the VLAN ID. This mode is intended for servers that are VLAN-capable, so the switch filters and processes all VLAN ID tagged packets. In trunk mode, the switch is programmed to receive VLAN ID-tagged packets that are inbound to the switch port.

Access mode

Access mode indicates that the switch should filter on specific VLAN IDs and allow only packets that match the configured VLAN IDs to pass through the switch port. The VLAN ID is then removed from the packet before it is sent to the server. That is, VLAN ID filtering is controlled by the switch. In access mode, the switch is programmed to receive packets *without* VLAN ID tags that are inbound to the switch port.

Hybrid mode

Hybrid mode is a combination of the previous two modes. This is a port where both VLAN-aware and VLAN-unaware devices are attached. A hybrid port can have both tagged and untagged frames.

Figure 10-2 shows a logical diagram of a VLAN environment with two switches and several VLANs.

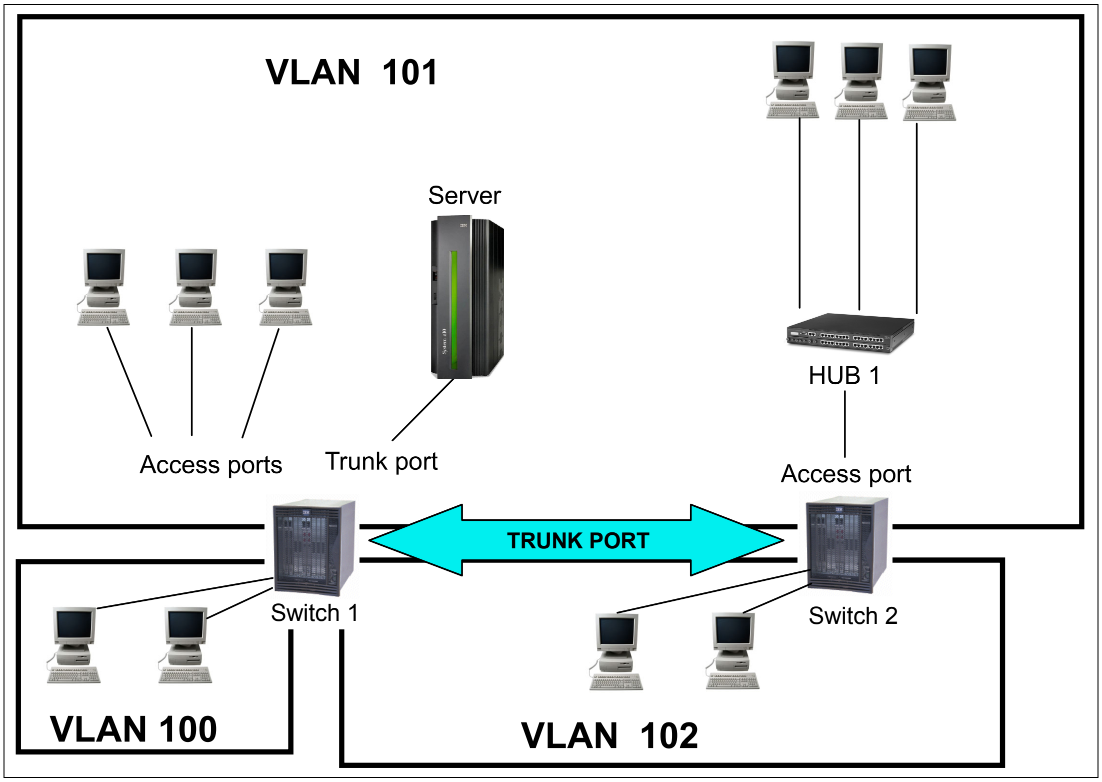


Figure 10-2 VLAN logical diagram

In this sample network, VLAN 100 exists only in Switch 1 because the trunk port to Switch 2 is not a member of VLAN 100. VLANs 101 and 102 span the two switches because the trunk ports in each switch are members of both VLANs.

This example illustrates two of the usual reasons that VLANs are used:

- Staff in different locations retains common access to resources.

  The server is used by staff in both buildings. By defining these workstations on the same VLAN, no additional configuration or equipment is required for either location to access the Linux server, yet you ensure that other staff do not have access.

- Consolidation of resource access.

  The external network must be accessed by different staff in both buildings. Extending VLAN 102 across to Switch 1 avoids having to provide another link from the other building.

Broadcast in VLANs

All ports that are members of the same VLAN, including trunk ports, operate as though they are part of the same physical network. When a multicast or broadcast frame is received from a device on a particular VLAN, the switch transmits the frame to all ports (both trunk and access ports) that belong to the same VLAN.

The only difference between the trunk and access port, in this case, is that the frame transmitted to the trunk port has the VLAN tag intact so that the VLAN-aware equipment at the other end of the link knows how to handle it.

VLAN isolation

VLANs provide isolation. VLANs behave like separate physical networks, even if they are within the same switch.

For devices in different VLANs to communicate, IP routing must occur. In the network that is shown in Figure 10-2 on page 91, workstations in VLAN 100 and VLAN 101 cannot communicate because there is no routing path between the two VLANs. Workstations in VLANs 100 and 102 can communicate if the IP router to which they are attached is configured appropriately.

10.1.2 VLAN tagging basics

In a VLAN environment, you find two types of frames:

- Untagged frames

  There is no tag header following the source MAC address.

- Tagged frames

  - Priority-tagged frame

    The tag header includes only VLAN priority information, but no VLAN ID. (VLAN ID is zero and is referred to as a null-tagged frame.)

  - VLAN-tagged frame

    The tag header includes both VLAN priority information and VLAN ID.

Figure 10-3 illustrates these descriptions.

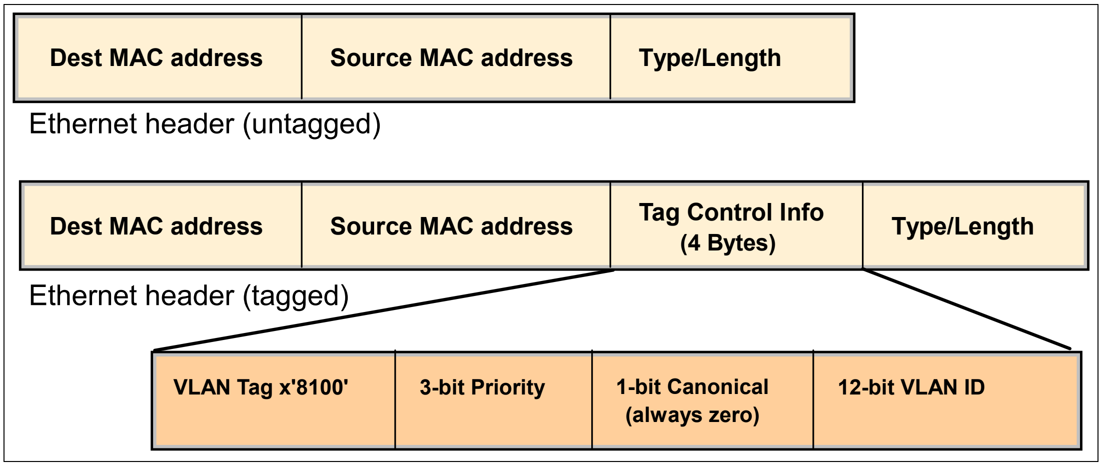


Figure 10-3 VLAN tagging

10.2 General VLAN design considerations

Consider the following items when designing VLANs that include OSA Ethernet features:

- If a VLAN ID is defined to the TCP/IP stack for an OSA port, the Ethernet switch port to which the OSA port is attached must be configured in *trunk mode*.
- If no VLAN ID is defined to the TCP/IP stack for an OSA port, the Ethernet switch port to which the OSA port is attached must be configured in *access mode*.
- If an OSA port is shared across multiple TCP/IP stacks and all are not defined with a VLAN ID, the Ethernet switch port must be defined in *trunk mode*. Untagged traffic from the TCP/IP stacks that does not have a VLAN ID defined is tagged by the switch with the *default* VLAN ID.

Important: Some Ethernet switch vendors use VLAN ID 1 for vendor-specific purposes or as the default VLAN ID. Therefore, avoid the use of VLAN ID 1.

IBM z/OS VLAN support allows a TCP/IP stack to register up to eight VLAN IDs for both IPv4 and IPv6 for the same OSA port. VLAN IDs for IPv4 can be different from the VLAN ID for IPv6.

When a VLAN ID is configured to an OSA port in the TCP/IP stack, the following actions occur:

- The TCP/IP stack becomes VLAN-aware or enabled, and the OSA port is considered to be part of a VLAN.
- During activation, the TCP/IP stack registers the VLAN ID value to the OSA port.
- A VLAN tag is added to all outbound packets.
- The OSA port filters all inbound packets that are based on the configured VLAN ID.

Tip: Create and maintain diagrams of your physical and logical LAN layout. These diagrams can be helpful when configuring your VLANs and for problem determination.

10.2.1 VLAN configuration example

When designing VLANs with an OSA port, we suggest that deployment be symmetrical with the configuration of the corresponding Ethernet switch. For example, the Ethernet switch port that is associated with an OSA port must be configured in trunk mode when the OSA port performs VLAN tagging and VLAN ID filtering.

If a VLAN ID is not configured to an OSA port (VLAN tagging and VLAN ID filtering are not performed), access mode must be configured at the Ethernet switch port with the appropriate VLAN ID.

Figure 10-4 shows an example of trunk mode compared to access mode, with four VLANs deployed through two shared OSA ports. The TCP/IP stacks operate as though they have their own unique and isolated networks:

- VLAN 100 - IP-stack #1 and clients 1 and 2
- VLAN 200 - IP-stack #2 and clients 3 and 4
- VLAN 300 - IP-stack #3 and clients 5 and 6
- VLAN 400 - IP-stack #4 and #5, and IP router (for access beyond that LAN segment)

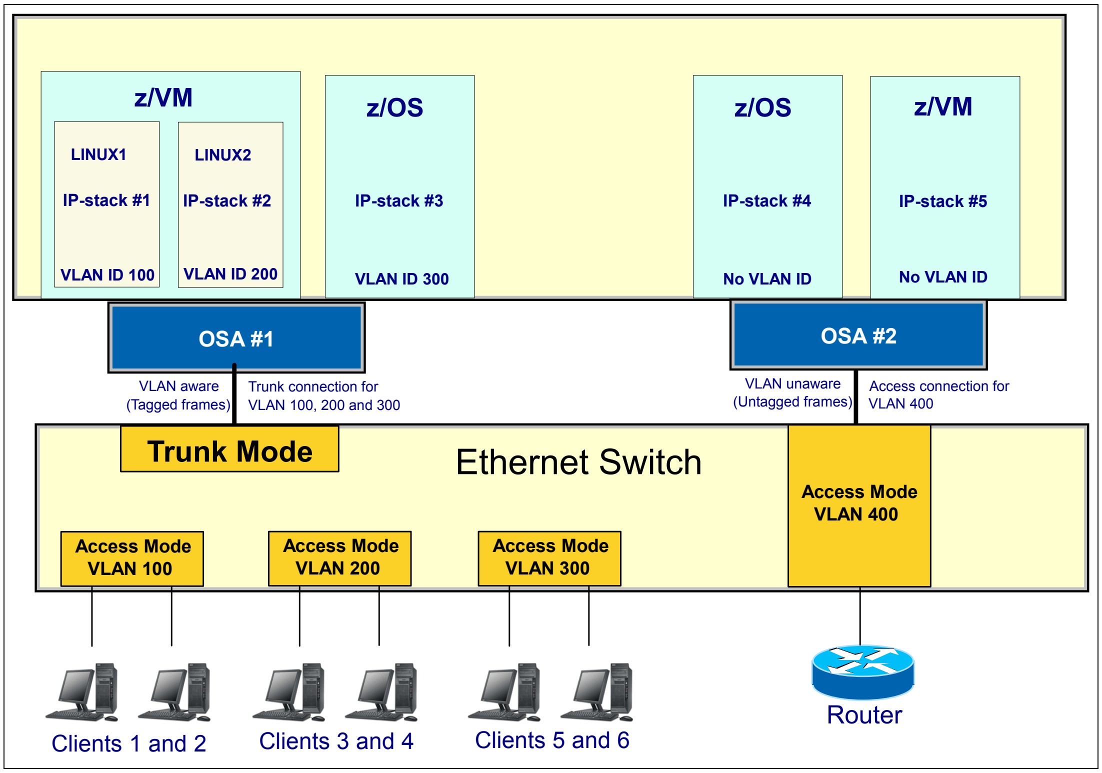


Figure 10-4 Trunk mode versus access mode

IP stacks #4 and #5 do not have a VLAN ID defined, and therefore are unaware of the existence of VLAN IDs and VLAN tagging. The Ethernet switch port to which OSA port #2 is connected is configured in access mode.

IP stacks #1, #2, and #3 are configured with a VLAN ID, which will be registered with OSA port #1. Notice that the Ethernet switch port in this case is configured in trunk mode. Also notice that VLAN-aware and VLAN-unaware IP stacks are not defined to the same OSA port.

Note: This example is used solely to demonstrate the VLAN design rules. We do not recommend implementing OSA features with a single point of failure.

10.2.2 Sharing an OSA port with the same VLAN ID

Figure 10-5 shows a single OSA port shared between IP-stack #4 and #5, both configured with the same VLAN ID. The IDs in both TCP/IP stacks are identical and the next-hop IP address is registered in the OSA Address Table (OAT). Therefore, the OSA logic bypasses the LAN environment and the packets are sent directly to the destination TCP/IP stack.

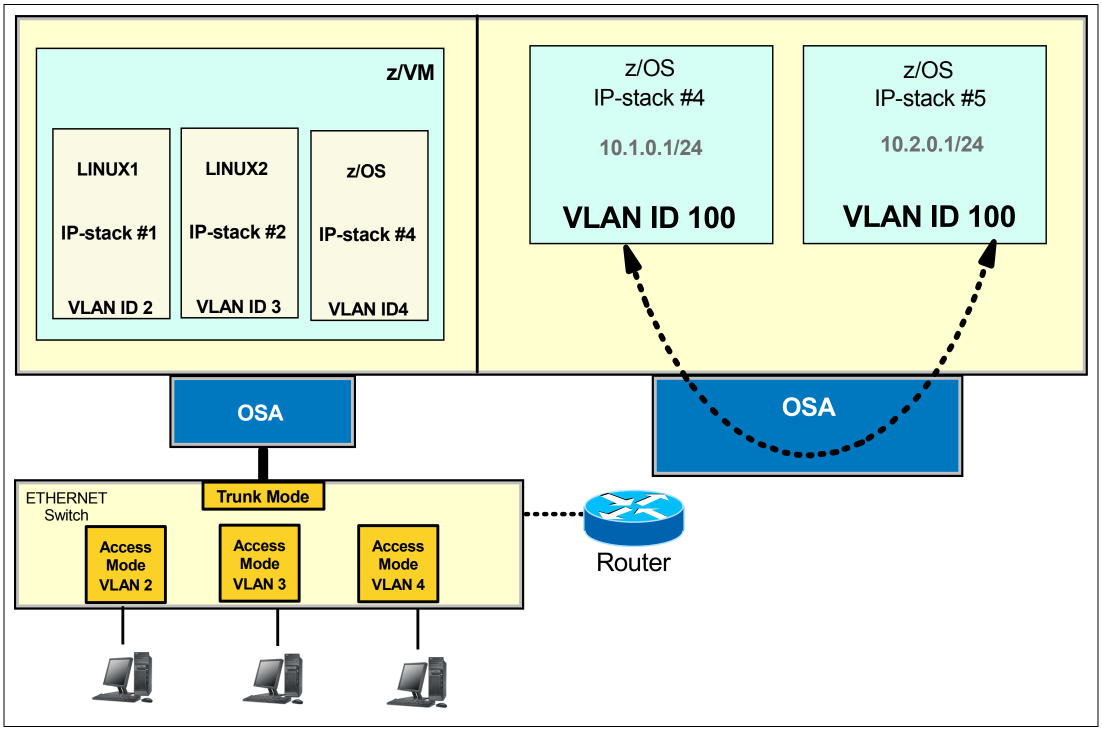


Figure 10-5 OSA port that is shared between two stacks in the same VLAN

10.2.3 Primary and secondary router support with VLANs

OSA provides primary (PRIRouter) and secondary (SECRouter) router support. This function allows a single TCP/IP stack, on a per-protocol basis (IPv4 and IPv6) to register and act as a router stack that is based on a particular OSA port. Secondary routers can also be configured in case the primary router becomes unavailable and the secondary router takes over for the primary one. An OSA port supports the primary and secondary router function on the basis of registered VLAN IDs. Therefore, if an OSA port is configured with a VLAN ID and a `PRIRouter` or `SECRouter` statement, that TCP/IP stack serves as an IP router for that specific VLAN.

VMAC support enables an OSA interface to have not only a physical MAC address but also distinct virtual MAC addresses for each device or interface in a stack.

Tip: If your OSA ports are shared across multiple TCP/IP routing stacks, we strongly suggest using VMAC in your environment. It can simplify network infrastructure and avoid PRIROUTER or SECROUTER setup issues when sharing a port between multiple LPARs. See Chapter 9, “IBM z/OS virtual MAC support” on page 79 for more details about VMAC.

10.2.4 Operating system support

z/OS, z/VM, and Linux on System z provide full VLAN support using the OSA features. It is possible to share an OSA port between Linux on System z and other operating systems.

Note: On the System z EC12 server, multiple VLAN IDs on a single OSA port are supported by z/OS V2R1 TCP/IP and Linux on System z TCP/IP stacks.

Multiple VLAN IDs defined to a single OSA port are not supported by z/VM in native mode. However, guest systems that are running under z/VM are supported.

10.3 VLAN support for the IBM z/OS operating system

z/OS provides full VLAN support for OSA devices that are running in QDIO mode. You can configure multiple VLANs from the same TCP/IP stack for a single OSA feature. You can use the multiple VLAN function to consolidate multiple application servers across multiple stacks into a single z/OS image where the traffic related to these servers is on unique VLANs.

Note: The stack supports a maximum of eight VLANs for each OSA port and each IP version (IPv4 and IPv6). This function is limited to OSA features in QDIO mode (CHPID type OSD) that support the Layer 3 Virtual MAC address (VMAC) function.

10.3.1 VLAN implementation

In our VLAN environment, the zEC12 server consisted of two z/OS V2R1 LPAR and one z/VM V6.3 LPAR with two Linux guests. We shared the OSA-Express5S 1000BASE-T feature (CHPID 04) and OSA-Express5S 10GbE (CHPID 07) between the z/OS and z/VM LPARs.

We configured z/OS TCP/IP so that port 0 of the OSA-Express5S 1000BASE-T feature belongs to VLAN 3 by using the `DEVICE`, `LINK`, and `HOME` statements. Only one VLAN ID per OSA port per stack per IP version is supported. However, we suggest using the `INTERFACE` statement in the TCP/IP profile to configure IPv4 definitions for OSA ports in QDIO mode rather than using the `DEVICE`, `LINK`, and `HOME` statements. The stack supports a maximum of eight VLAN IDs per interface to the same OSA port.

We use the `INTERFACE` statement to configure our OSA-Express5S 1000BASE-T port 1 to belong to VLAN 5 and VLAN 8.

Figure 10-6 on page 97 provides an overview of our configuration. We enabled a connection between the VLANs through an Ethernet switch and defined three trunk ports for the OSA-Express5S 1000BASE-T.

Remember that if the OSA port is connected to an Ethernet switch port that is defined to run in access mode, then no VLAN definitions are required in the z/OS TCP/IP profile.

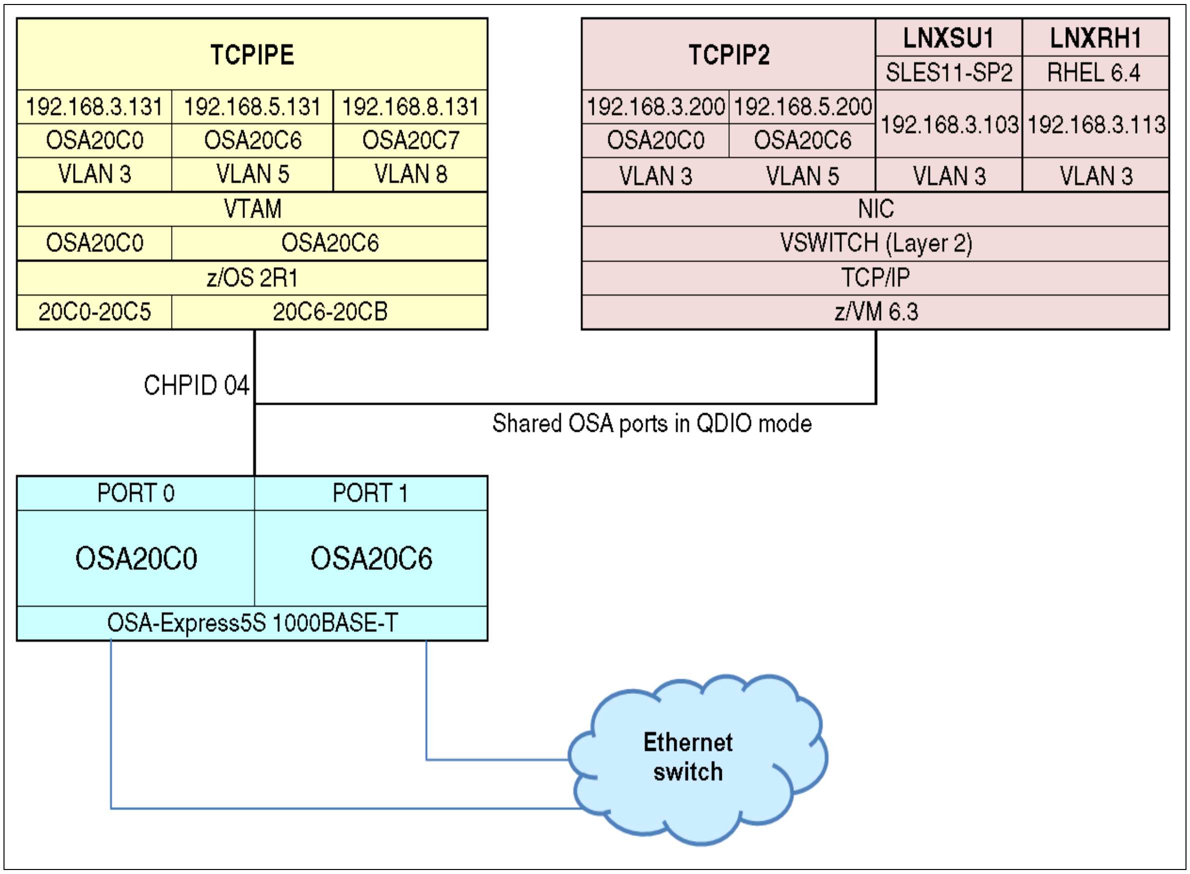


Figure 10-6 Our z/OS VLAN configuration

To define an OSA port in QDIO mode, see Chapter 4, “QDIO mode for the IBM z/OS operating system” on page 31 for details.

10.3.2 Configuring OSA with VLAN ID

The first step is to plan the configuration of the switch that the OSA ports will connect to.

Planning, configuration, and verification of the switch ports

It is important to be aware of the switch configuration and the definitions that the OSA ports connect to. Table 10-1 shows that information for our configuration.

Table 10-1 Switch port assignment with VLAN IDs

Ethernet switch port	VLAN ID (mode)	Connection type
Interface 1/0/13	3 (Trunk mode)	OSA (CHPID 04) port 0 (20C0)
Interface 1/0/15	5 and 8(Trunk mode)	OSA (CHPID 04) port 1(20C6)
Interface 1/0/26	6 (Trunk mode)	OSA (CHPID 07) port 0(2160)

We altered the configuration of the Ethernet switch to support four VLANs: 3, 5, 6, and 8. Switch port interface 1/0/13 supports VLAN3 and connects to port 0 of OSA-Express5S 1000BASE-T. Switch port interface 1/0/15 supports VLAN 5 and VLAN 8 and connects to port 1 of OSA-Express5S 1000BASE-T. We added VLAN 6 to port 1/0/26 for the OSAExpress5S 10GbE port 0. Example 10-1 on page 98 shows the configuration of the Netgear switch.

Example 10-1 Configuration of the Netgear switch

```
1000Baset

interface 1/0/13
vlan pvid 3
vlan participation include 3
vlan tagging 3
exit
interface 1/0/15
bandwidth 1000000
vlan pvid 5
vlan participation include 5,8
vlan tagging 5,8
ip mtu 1500
exit

interface vlan 3
bandwidth 1000
description 'vlan 3'
routing
ip address  192.168.3.1  255.255.255.0
ip mtu 1500
exit

interface vlan 5
bandwidth 1000
description 'vlan 5'
routing
ip address  192.168.5.1  255.255.255.0
ip mtu 1500
exit

interface vlan 8
bandwidth 1000
description 'vlan 8'
routing
ip address  192.168.8.1  255.255.255.0
ip mtu 1500
exit

10GB

interface 1/0/26
no auto-negotiate
vlan tagging 3
exit

interface vlan 6
bandwidth 1000
description 'Vlan 6'
routing
ip address  192.168.6.1  255.255.255.0
ip mtu 1500
exit
```

Define a TRLE in VTAM to represent each OSA port

TCP/IP uses a VTAM interface to run the OSA in QDIO mode. You must define and activate a Transport Resource List (TRL) major node before TCP/IP starts the QDIO device. Example 10-2 shows the TRLE definition that we used for our OSA-Express5S 1000BASE-T.

Example 10-2 VTAM TRL major node for port 0

```
OSA20C0  VBUILD TYPE=TRL
OSA20C0P TRLE  LNCTL=MPC,                                              *
               READ=20C0,                                              *
               WRITE=20C1,                                             *
               DATAPATH=(20C2-20C5),                                   *
               PORTNAME=OSA20C0,                                       *
               MPCLEVEL=QDIO
```

Example 10-3 shows the TRLE definition for our second OSA-Express5S 1000BASE-T.

Example 10-3 VTAM TRL major node for port 1

```
OSA20C6  VBUILD TYPE=TRL
OSA20C6P TRLE  LNCTL=MPC,                                              *
               READ=20C6,                                              *
               WRITE=20C7,                                             *
               DATAPATH=(20C8-20CD),                                   *
               PORTNAME=OSA20C6,                                       *
               PORTNUM=1,                                              *
               MPCLEVEL=QDIO
```

To use multiple VLANs for our OSA, we needed to configure a separate INTERFACE to the OSA for each VLAN. See Example 10-5 on page 100 for the INTERFACE definitions in TCPIP. Each of these interfaces requires a separate DATAPATH device in the TRLE definition.

We activated our Transport Resource List (TRL) major node before TCP/IP starts its QDIO device. You can activate the corresponding TRL minor node with this VTAM command:

```
V NET,ACT,ID=OSA20C0 and V NET,ACT,ID=OSA20C6
```

TCPIP profile definition for OSA-Express5s port 0 (DEVICE and LINK)

This example uses the `DEVICE`, `LINK`, and `HOME` statements. We define and assign port 0 to VLAN 3. Example 10-4 shows the TCPIP profile definition for OSA-Express5S port 0. Notice that the `VLANID` parameter is part of the `LINK` statement.

Example 10-4 Extract of the TCPIP profile that shows the definitions for OSA (port 0)

```
DEVICE OSA20C0  MPCIPA
LINK   OSA20C0LNK  IPAQENET OSA20C0 VLANID 3
;
HOME
   192.168.3.31  OSA20C0LNK
;
BEGINROUTES
 ROUTE DEFAULT              192.168.3.1     OSA20C0LNK    MTU 1492
 ROUTE 192.168.3.0 255.255.255.0 =          OSA20C0LNK    MTU 1492
ENDROUTES
;
START OSA20C0
```

TCPIP Profile definitions for OSA-Express5s port 1 (INTERFACE)

This example uses the INTERFACE statement. We create the INTERFACE statement that is required to define and assign VLAN 5 and 8 to OSA port 1. **Note:** Use the INTERFACE statement rather than DEVICE and LINK statements, because it is newer and more strategic.

Using the INTERFACE statement

When defining multiple VLANs to an OSA port, use the following configuration rules:

- Define a unique VLAN ID in the stack profile for each IP version (IPv4 and IPv6).
- Configure the VMAC parameter on each INTERFACE statement with the default ROUTEALL attribute. The VMAC address can either be specified or OSA-generated. If you specify a VMAC address, it must be unique for each INTERFACE statement.
- Configure a unique subnet for each IPv4 interface for this OSA feature by using the subnet mask specification on the IPADDR parameter on the INTERFACE statement.

> **Note:** Changing from DEVICE and LINK to INTERFACE statements is strongly suggested in z/OS Version 1, Release 10 and newer releases.

Example 10-5 shows the TCPIP profile definition for OSA-Express5S 1000BASE-T (port 1). Notice that the two interface definitions are using the same port name, OSA20C6.

Example 10-5 Extract of our TCPIP profile that shows the definitions for port 1

```
INTERFACE OSA20C6I
   DEFINE IPAQENET
   PORTNAME OSA20C6
   IPADDR 192.168.5.131/24
   VLANID 5
   VMAC ROUTEALL
;
INTERFACE OSA20C7I
   DEFINE IPAQENET
   PORTNAME OSA20C6
   IPADDR 192.168.8.131/24
   VLANID 8
   VMAC ROUTEALL
;
BEGINROUTES
 ROUTE DEFAULT             192.168.5.1     OSA20C6I       MTU 8992
 ROUTE 192.168.5.0 255.255.255.0 =         OSA20C6I       MTU 8992
 ROUTE 192.168.8.0 255.255.255.0 =         OSA20C7I       MTU 8992
ENDROUTES
;
START OSA20C6I
START OSA20C7I
```

SOURCEVIPAINT

The SOURCEVIPAINTERFACE parameter must point to the link name of a static VIPA. For interfaces that are defined by using DEVICE/LINK/HOME, source VIPA selection continues to work, based on the ordering of the home list.

IPADDR with subnet mask

With the INTERFACE statement, you can control VIPA ARP processing by configuring a subnet mask for the OSA. If you specify a non-0 num_mask_bits value on the IPADDR parameter of the INTERFACE statement, then the stack informs OSA to perform ARP processing for a VIPA only if the VIPA is configured in the same subnet as the OSA.

INTERFACE statement resource considerations:

- Each VLAN requires a separate interface definition.
- Each interface requires a separate DATAPATH device in the TRLE definition.
- Each DATAPATH device uses fixed storage. You can control the amount of storage, by in either of two ways:
  - QDIOSTG in the **VTAM start** option
  - READSTORAGE parameter on the INTERFACE statement

10.3.3 Verification

After activation, we verify that the VLAN IDs in our z/OS TCP/IP environment are defined correctly, by issuing the z/OS **d tcpip,tcpipf,netstat,dev** command. See Example 10-6 for the output regarding OSA-Express5S 1000BASE-T port 0.

Example 10-6 Results of the netstat dev command for OSA ***port 0***

```
DevName: OSA20C0          DevType: MPCIPA
   DevStatus: Ready
   LnkName: OSA20C0I         LnkType: IPAQENET   LnkStatus: Ready
     Speed: 0000001000
     IpBroadcastCapability: No
     CfgRouter: Non                  ActRouter: Non
     ArpOffload: Yes                 ArpOffloadInfo: Yes
     ActMtu: 8992
     VLANid: 3                       VLANpriority: Disabled
     DynVLANRegCfg: No               DynVLANRegCap: Yes
     ReadStorage: GLOBAL (4096K)
     InbPerf: Balanced
     ChecksumOffload: Yes            SegmentationOffload: No
     SecClass: 255                   MonSysplex: No
   Routing Parameters:
     MTU Size: n/a              Metric: 00
     DestAddr: 0.0.0.0          SubnetMask: 255.255.255.0
   Multicast Specific:
...
```

The OSA device OSA20C0 (port 0) shows the status ready and the VLANID 3 is assigned.

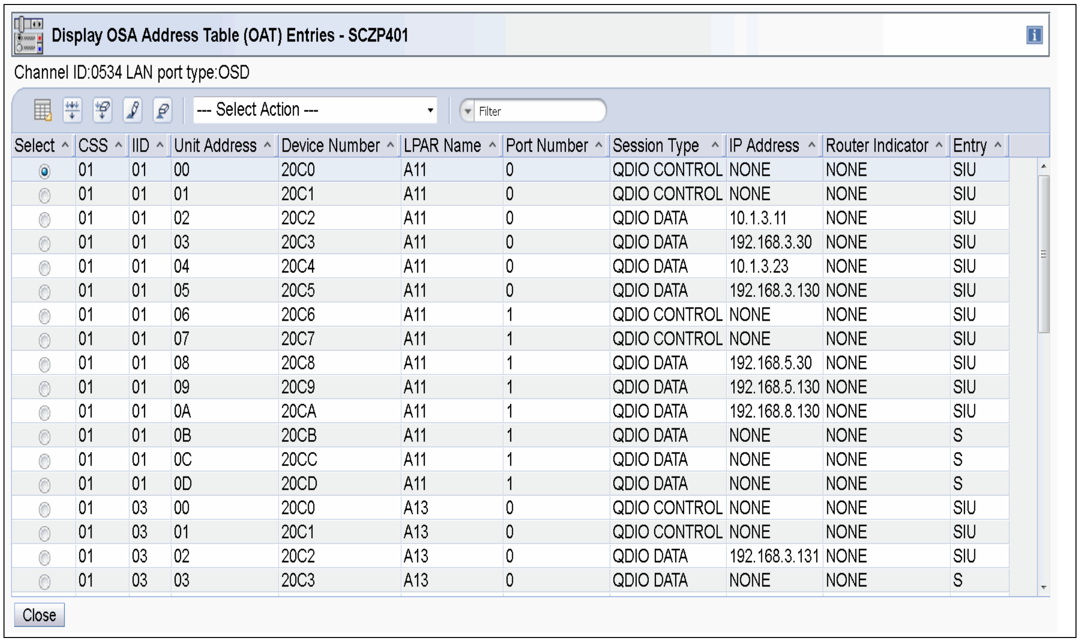
Now, we verify that OSA device OSA20C6 is working properly. Again, we issue the z/OS **d tcpip,tcpipe,netstat,dev** command. See Example 10-7 on page 102 for the output regarding OSA-Express5S 1000BASE-T (port 1).

Example 10-7 Results of the netstat dev command for OSA ***port 1***

```
INTFNAME: OSA20C6I         INTFTYPE: IPAQENET   INTFSTATUS: READY
    PORTNAME: OSA20C6   DATAPATH: 20C9     DATAPATHSTATUS: READY
    CHPIDTYPE: OSD      SMCR: DISABLED (GLOBALCONFIG NOSMCR)
    PNETID: ITSOPNET1
    SPEED: 0000001000
    IPBROADCASTCAPABILITY: NO
    VMACADDR: 02006D480B85   VMACORIGIN: OSA    VMACROUTER: ALL
    ARPOFFLOAD: YES                 ARPOFFLOADINFO: YES
    CFGMTU: NONE                    ACTMTU: 8992
    IPADDR: 192.168.5.130/24
    VLANID: 5                       VLANPRIORITY: DISABLED
    DYNVLANREGCFG: NO               DYNVLANREGCAP: YES
    READSTORAGE: GLOBAL (4096K)
    INBPERF: BALANCED
    CHECKSUMOFFLOAD: YES            SEGMENTATIONOFFLOAD: NO
    SECCLASS: 255                   MONSYSPLEX: NO
    ISOLATE: NO                     OPTLATENCYMODE: NO
  MULTICAST SPECIFIC:
...

INTFNAME: OSA20C7I         INTFTYPE: IPAQENET   INTFSTATUS: READY
    PORTNAME: OSA20C6   DATAPATH: 20CA     DATAPATHSTATUS: READY
    CHPIDTYPE: OSD      SMCR: DISABLED (GLOBALCONFIG NOSMCR)
    PNETID: ITSOPNET1
    SPEED: 0000001000
    IPBROADCASTCAPABILITY: NO
    VMACADDR: 02006E480B85   VMACORIGIN: OSA    VMACROUTER: ALL
    ARPOFFLOAD: YES                 ARPOFFLOADINFO: YES
    CFGMTU: NONE                    ACTMTU: 8992
    IPADDR: 192.168.8.130/24
    VLANID: 8                       VLANPRIORITY: DISABLED
    DYNVLANREGCFG: NO               DYNVLANREGCAP: YES
    READSTORAGE: GLOBAL (4096K)
    INBPERF: BALANCED
    CHECKSUMOFFLOAD: YES            SEGMENTATIONOFFLOAD: NO
    SECCLASS: 255                   MONSYSPLEX: NO
    ISOLATE: NO                     OPTLATENCYMODE: NO
  MULTICAST SPECIFIC:
...
```

The output proves that both OSA interfaces OSA20C6I and OSA20C7I are up and ready. Each interface has its VLANID assigned and we can discover the two datapath devices that TCP/IP has allocated: 20C9 for OSA20C6I and 20CA for OSA20C7LNK. The VMAC addresses are shown as well.

Displaying the OSA Address Table can help you in your installation, even if you are running OSA in QDIO mode only. Here is an example. In Figure 10-7 on page 103 we used HMC to show the contents of the OAT:



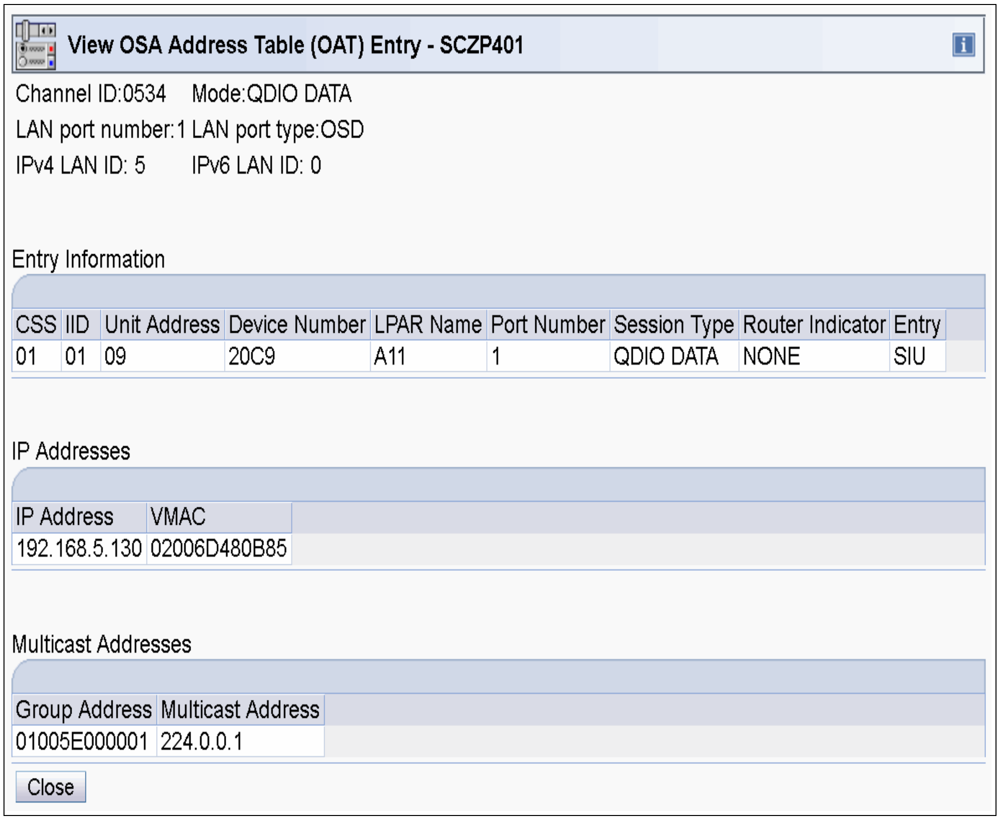
Display OSA Address Table (OAT) Entries - SCZP401

Channel ID:0534 LAN port type:OSD

Select	CSS	IID	Unit Address	Device Number	LPAR Name	Port Number	Session Type	IP Address	Router Indicator	Entry
●	01	01	00	20C0	A11	0	QDIO CONTROL	NONE	NONE	SIU
○	01	01	01	20C1	A11	0	QDIO CONTROL	NONE	NONE	SIU
○	01	01	02	20C2	A11	0	QDIO DATA	10.1.3.11	NONE	SIU
○	01	01	03	20C3	A11	0	QDIO DATA	192.168.3.30	NONE	SIU
○	01	01	04	20C4	A11	0	QDIO DATA	10.1.3.23	NONE	SIU
○	01	01	05	20C5	A11	0	QDIO DATA	192.168.3.130	NONE	SIU
○	01	01	06	20C6	A11	1	QDIO CONTROL	NONE	NONE	SIU
○	01	01	07	20C7	A11	1	QDIO CONTROL	NONE	NONE	SIU
○	01	01	08	20C8	A11	1	QDIO DATA	192.168.5.30	NONE	SIU
○	01	01	09	20C9	A11	1	QDIO DATA	192.168.5.130	NONE	SIU
○	01	01	0A	20CA	A11	1	QDIO DATA	192.168.8.130	NONE	SIU
○	01	01	0B	20CB	A11	1	QDIO DATA	NONE	NONE	S
○	01	01	0C	20CC	A11	1	QDIO DATA	NONE	NONE	S
○	01	01	0D	20CD	A11	1	QDIO DATA	NONE	NONE	S
○	01	03	00	20C0	A13	0	QDIO CONTROL	NONE	NONE	SIU
○	01	03	01	20C1	A13	0	QDIO CONTROL	NONE	NONE	SIU
○	01	03	02	20C2	A13	0	QDIO DATA	192.168.3.131	NONE	SIU
○	01	03	03	20C3	A13	0	QDIO DATA	NONE	NONE	S

Figure 10-7 OSA Address Table Entries

To check the VLAN assignment, select the device. Then, in the Select Action pull-down, choose **Details**. Figure 10-8 shows the details for device 20C9. Its VLAN ID is 5.



View OSA Address Table (OAT) Entry - SCZP401

Channel ID:0534 Mode:QDIO DATA

LAN port number:1 LAN port type:OSD

IPv4 LAN ID: 5 IPv6 LAN ID: 0

Entry Information

CSS	IID	Unit Address	Device Number	LPAR Name	Port Number	Session Type	Router Indicator	Entry
01	01	09	20C9	A11	1	QDIO DATA	NONE	SIU

IP Addresses

IP Address	VMAC
192.168.5.130	02006D480B85

Multicast Addresses

Group Address	Multicast Address
01005E000001	224.0.0.1

Figure 10-8 Device 20C9 details from the OSA Address Table Entry.

We successfully tested the connections from SC30 to SC31 by using ping to check each other's IP addresses. Additionally, z/OS can also ping the z/VM TCPIP2 IP addresses on VLAN 3, 5, and 6.

10.4 VLAN support in the IBM z/VM operating system

z/VM provides the following support:

- Enhancements to TCP/IP for z/VM to enable membership in a VLAN
- Enhancements to z/VM virtual QDIO and IBM HiperSockets™ networking interfaces to support VLAN frame tagging as described in IEEE 802.1q
- Management and control of VLAN IDs that can be used by guest virtual machines

10.4.1 z/VM native VLAN support

In our environment (see Figure 10-9), we had a z/VM Version 6, Release 3 LPAR and two OSA features: OSA-Express5S 1000BASE-T with two ports and OSA-Express5S 10GbE with one port. The OSA ports are connected to trunk ports on an Ethernet switch.

On OSA-Express5S 1000BASE-T, we configured VLAN 3 on port 0 and VLAN 5 on port 1. On OSA-Express5S 10GbE, we configured VLAN 6 on port 0. We used the VLAN parameter on the LINK statement in the TCP/IP profile. VLAN is an optional parameter followed by a number that indicates the VLAN identifier that is to be assigned to the OSA port. The valid range is 1 - 4094. The value used must be a VLAN identifier that is recognized by the Ethernet switch to which the OSA port is connected.

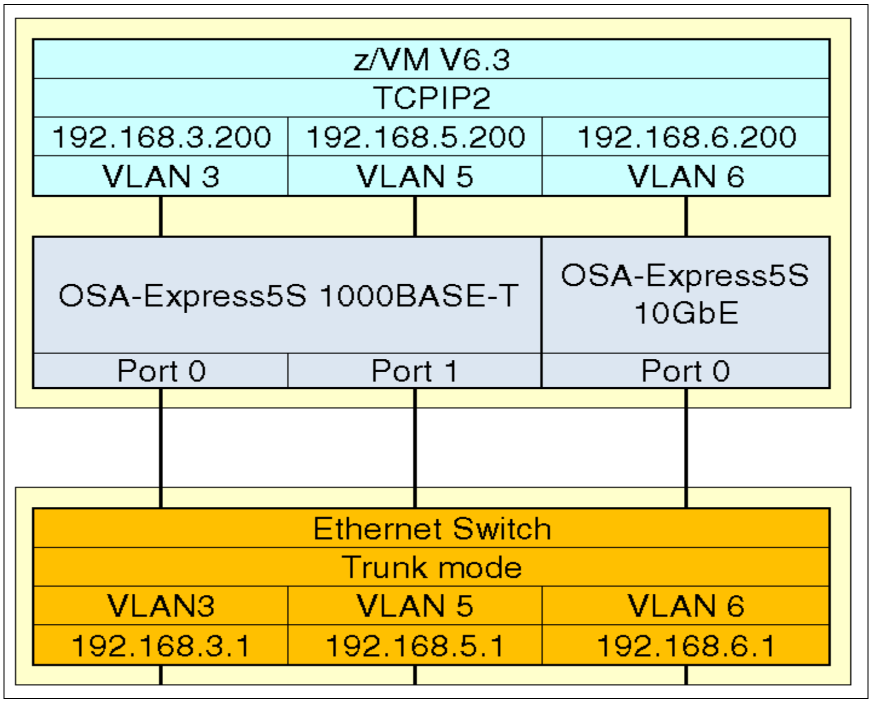


Figure 10-9 z/VM VLAN configuration

Ethernet switch configuration

We altered the configuration in the Ethernet switch to support the VLAN and the trunk port. We added VLAN 3 to port 1/0/13, VLAN 5 to port 1/0/15, and VLAN 6 to port1/0/26.

10.4.2 Verification

After activation, we used the **`netstat dev`** command to verify that the VLAN ID in our z/VM TCP/IP environment was defined correctly (see Example 10-8).

Example 10-8 Results of the netstat dev command on z/VM

```
Device OSA20C0                 Type: OSD           Status: Ready
  Queue size: 0     CPU: 0     Address: 20C0       Port name: UNASSIGNED
    Link OSA20C0               Type: QDIOETHERNET   Port number: 0
      Transport Type: Ethernet MAC: 02-00-00-00-00-9B
      Speed: 1000000000
      BytesIn: 0               BytesOut: 406
      Forwarding: Enabled      MTU: 1500            IPv6: Disabled
      IPv4 Path MTU Discovery: Disabled
      VLAN ID: 3                                    GVRP: Disabled
      IPv4 VIPA ARP
      Multicast Group                         Members
      ---------------                         -------
      224.0.0.1                                  1

Device OSA20C6                 Type: OSD           Status: Ready
  Queue size: 0     CPU: 0     Address: 20C6       Port name: UNASSIGNED
    Link OSA20C6               Type: QDIOETHERNET   Port number: 1
      Transport Type: Ethernet MAC: 02-00-00-00-00-9C
      Speed: 1000000000
      BytesIn: 0               BytesOut: 406
      Forwarding: Enabled      MTU: 1500            IPv6: Disabled
      IPv4 Path MTU Discovery: Disabled
      VLAN ID: 5                                    GVRP: Disabled
      IPv4 VIPA ARP
      Multicast Group                         Members
      ---------------                         -------
      224.0.0.1                                  1

Device OSA2160                 Type: OSD           Status: Ready
  Queue size: 0     CPU: 0     Address: 2160       Port name: UNASSIGNED
    Link OSA2160               Type: QDIOETHERNET   Port number: 0
      Transport Type: Ethernet MAC: 02-00-00-00-00-9D
      Speed: 10000000000
      BytesIn: 15068           BytesOut: 2444
      Forwarding: Enabled      MTU: 1500            IPv6: Disabled
      IPv4 Path MTU Discovery: Disabled
      VLAN ID: 6                                    GVRP: Enabled
      IPv4 VIPA ARP
      Multicast Group                         Members
      ---------------                         -------
      224.0.0.1                                  1
```

In Example 10-9 on page 106, we show the output of the **`netstat tap tcpip2 home`** command. This displays the home addresses of TCP/IP2.

Example 10-9 Output of netstat tcp tcpip2 home

```
VM TCP/IP Netstat Level 630       TCP/IP Server Name: TCPIP2

IPv4 Home address entries:

Address         Subnet Mask      Link             VSWITCH
-------         -----------      ------           -------
192.168.3.200   255.255.255.0    OSA20C0          <none>
192.168.5.200   255.255.255.0    OSA20C6          <none>
192.168.6.200   255.255.255.0    OSA2160          <none>

IPv6 Home address entries: None

Ready; T=0.01/0.01 01:23:00
```

We successfully tested the connection from z/OS SC30 to z/VM by using the **ping** command.

10.5 VLAN support for the z/VSE operating system

IBM z/VSE (Virtual Storage Extended) software provides VLAN support for OSA-Express CHPID types OSD and OSX and IBM HiperSockets devices.

In a Layer 3 configuration, VLANs can be transparently used by IPv6/VSE and TCP/IP for the IBM VSE/ESA (Virtual Storage Extended/Enterprise Systems Architecture) operating system. If you want to configure VLANs for OSA-Express (CHPID types OSD and OSX) devices in a Layer 2 configuration that carries IPv6 traffic, you require the IPv6/VSE from Barnard Software, Inc.

You can use one of the following ways to configure your system to use VLAN:

- Configure one or more VLANs in the TCP/IP stack of IPv6/VSE by using the **LINK** command. For details of IPv6/VSE commands, see *IPv6/VSE Installation Guide*, SC34-2616.
- Generate and catalog phase IJBOCONF containing the global VLANs to be used with your OSAX devices. z/VSE provides skeleton SKOSACFG to generate phase IJBOCONF. The VLANs contained in IJBOCONF can be transparently used for Layer 3 links by IPv6/VSE and TCP/IP for VSE/ESA. See *z/VSE Planning,* SC34-2635 for details.

Example 10-10 on page 107 shows a sample configuration that sets VLAN ID 200 for Device D00.

Example 10-10 Sample SKOSACFG configuration

```
* $$ JOB JNM=IJBOCONF,CLASS=A,DISP=D
// JOB IJBOCONF GENERATE IJBOSA MODULE CONFIGURATION PHASE
// LIBDEF *,CATALOG=PRD2.CONFIG
// LIBDEF *,SEARCH=PRD1.BASE
// OPTION ERRS,SXREF,SYM,NODECK,CATAL,LISTX
PHASE IJBOCONF,*
// EXEC ASMA90,SIZE=(ASMA90,64K)
IJBOCONF CSECT
IJBOCONF AMODE ANY
IJBOCONF RMODE ANY
*
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
* *
* GLOBAL VLAN DEFINITION *
* *
* DEFGVLAN DEVNO=<CUU>, VLAN_ID=<ID>, VLAN_PRIO=<PRIO> *
* <CUU> VSE DEVICE NUMBER IN HEX FORMAT *
* <ID> VLAN ID IN DECIMAL FORMAT (1 ... 4095) *
* <PRIO> VLAN PRIORITY (VALID VALUES 0 ... 7) *
* *
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
*
DEFGVLAN DEVNO=0D00,VLAN_ID=200
*
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
* *
* ONLY ONE GLOBAL VLAN CAN BE DEFINED PER SUBCHANNEL. *
* IF GLOBAL VLAN IS DEFINED, NO USUAL VLAN(S) MAY BE DEFINED *
* ON THE SAME SUBCHANNEL. *
* *
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
END
/*
// IF $MRC GT 4 THEN
// GOTO NOLINK
// EXEC LNKEDT,PARM='MSHP'
/. NOLINK
/&
* $$ EOJ
```

Note: The SKOSACFG job template s in ICCF library 59.

10.6 VLAN support for the Linux operating system

VLAN support was added to the Linux kernel in Version 2.4.19. If your Linux system is not running at this level or a later one, you need an updated kernel to load the IEEE 802.1Q VLAN module.

VLAN support is usually built as a module called 8021q.o. Use the **insmod** or **modprobe** command to load the module before you attempt to use VLAN support. To load the module by using the **modprobe** command, you enter:

```
# modprobe 8021q
```

When the module is loaded, you see the following messages in your system log or dmesg output:

```
802.1Q VLAN Support v1.7 Ben Greear <greearb@candelatech.com>
All bugs added by David S. Miller <davem@redhat.com>
```

10.6.1 VLAN implementation

In our environment (see Figure 10-10) we configured two VLANs, one for each Linux system. We enabled a connection between the two VLANs through an Ethernet switch, and defined the OSA connection in trunk mode. We also installed two workstations, one defined to each VLAN.

Note: If the OSA port is connected to an Ethernet switch port that is defined to run in access mode, then no VLAN definitions are required for the Linux TCP/IP stack.

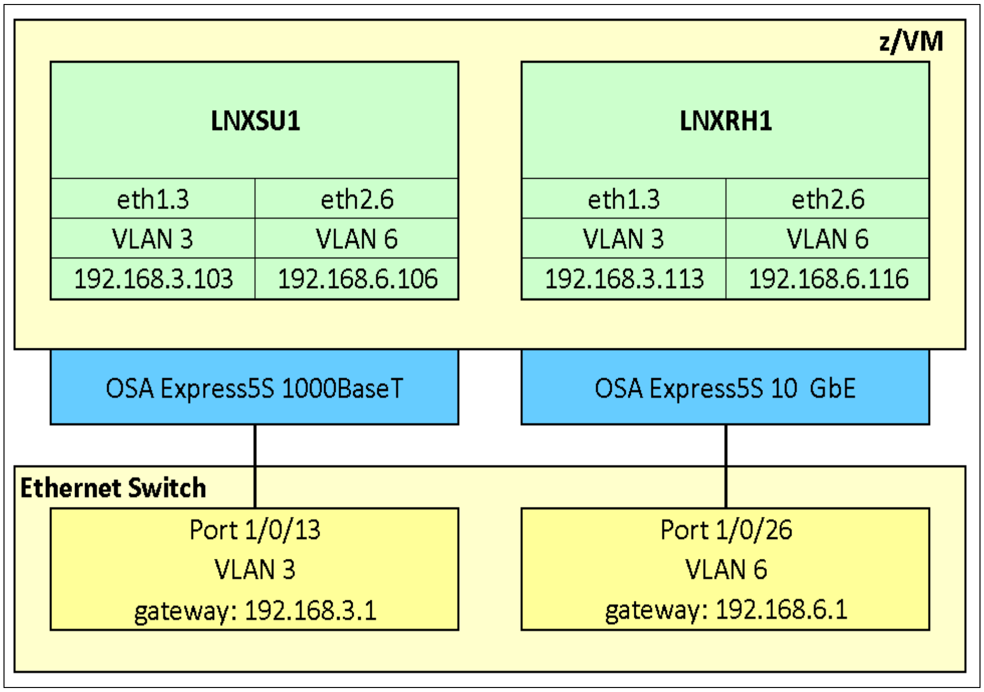


Figure 10-10 VLAN configuration - Linux on System z

A VLAN is defined for an existing Ethernet interface. The **vconfig** command is used to add or remove a VLAN configuration for a defined Ethernet interface.

Linux commands

On LNXSU1 and LNXRH1, we defined the VLAN configurations and brought up the interfaces by using the following commands:

- LNXSU1

```
vconfig add eth1 3
ifconfig eth1.3 192.168.3.103 netmask 255.255.255.0 up
```

- LNXRH1

```
vconfig add eth2 6
ifconfig eth2.6 192.168.3.113 netmask 255.255.255.0 up
```

After issuing the **vconfig add** commands on the respective systems, we received the following messages:

- LNXSU1

  ```
  Added VLAN with VID == 3 to IF -:eth1:-
  ```

- LNXRH1

  ```
  Added VLAN with VID == 6 to IF -:eth2:-
  ```

To remove a VLAN interface, you use the following commands:

```
ifconfig eth1.3 down
vconfig rem eth1.3
```

Startup configuration

Configuring VLANs is a manual process that must be scripted to take place when the Linux guests are booted. As VLAN use grows, you can expect Linux distributors to include VLAN boot-time configuration in their network scripts.

Ethernet switch configuration

We altered the configuration of the Ethernet switch to support the VLANs and the trunk port. We added VLAN ID 3 to port 1/0/13 and VLAN ID 6 to port 1/0/26.

10.6.2 Verification

We verified the VLAN definitions with the **ifconfig** command on LNXSU1 and LNXRH1. Example 10-11 shows the results from LNXRH1.

Example 10-11 Results of the ifconfig command

```
ifconfig
eth1.3    Link encap:Ethernet  HWaddr 02:00:00:00:01:9E
          inet addr:192.168.3.113  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::ff:fe00:7a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1492  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:468 (468.0 b
```

We successfully tested the connections from z/OS SC30 to LNXSU1 and to LNXRH1 by using the **ping** command.

11

z/VM virtual switch

The IBM z/VM operating system virtual switch (`VSWITCH`) is built on guest LAN technology and consists of a network of virtual adapters that can be used to interconnect guest systems. The virtual switch can also be associated with one or more IBM Open Systems Adapter-Express (OSA) ports. This capability allows access to external LAN segments without requiring an intermediate router between the external LAN and the internal z/VM guest LAN.

The virtual switch can operate at Layer 2 (the data link layer) or Layer 3 (the network layer) of the OSI model.

In this chapter, the following topics describe the elements and capabilities of the virtual switch with OSA Ethernet features and explain how to implement Layer 2 support, VLAN support, and port isolation:

11.1 Virtual switch description

The virtual switch bridges real hardware and virtualized LANs by using virtual Queued Direct I/O (QDIO) adapters. External LAN connectivity is achieved through OSA Ethernet features that are configured in QDIO mode. Like the OSA Ethernet features, the virtual switch supports the transport of Layer 2 (Ethernet frames) and Layer 3 (IP packets) traffic.

By default, the virtual switch operates in IP mode (Layer 3) and data is transported within IP packets. Each guest system is identified by one or more IP addresses for the delivery of IP packets. All outbound traffic that is destined for the physical portion of the LAN segment is encapsulated in Ethernet frames, with the MAC address of the OSA port as the source MAC address. With inbound traffic, the OSA port strips the Ethernet frame and forwards the IP packets to the virtual switch for delivery to the guest system, based on the destination IP address within each IP packet.

When operating in Ethernet mode (Layer 2), the virtual switch uses a unique MAC address for forwarding frames to each connecting guest system. Data is transported and delivered within Ethernet frames. This method can transport both TCP/IP and non-TCP/IP-based application data through the virtual switch. The address resolution process allows each guest system's MAC address to become known to hosts on the physical side of the LAN segment through an attached OSA port. All inbound or outbound frames that pass through the OSA port have the guest system's corresponding MAC address as the destination or source address.

The switching logic resides in the z/VM Control Program (CP), which owns the OSA port connection and performs all data transfers between guest systems that are connected to the virtual switch and the OSA port (see Figure 11-1).

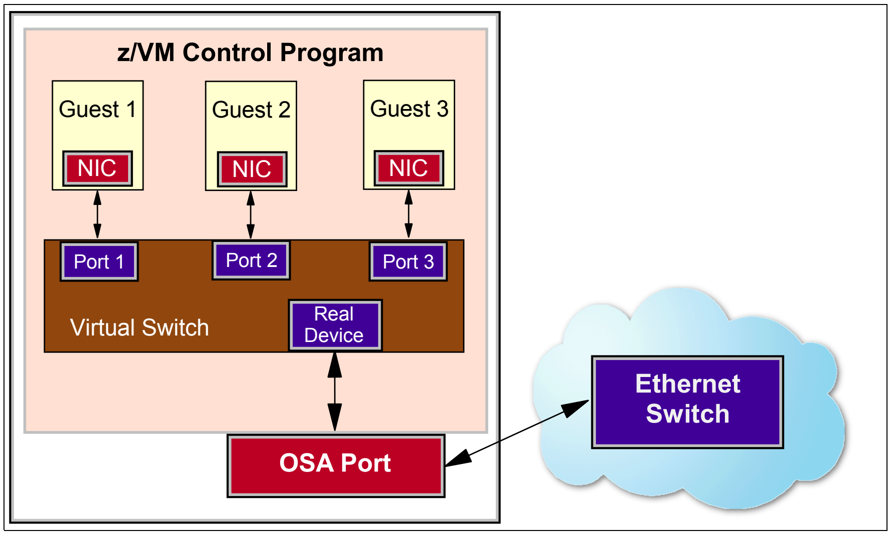


Figure 11-1 Virtual switching logic

In this chapter, we concentrate primarily on the OSA Layer 2 support. We highlight the Ethernet mode (Layer 2) capabilities of a z/VM virtual switch (VSWITCH) and the definitions that are required to implement such an environment.

In the remainder of this section, we describe the elements that make up the virtual switch and its capabilities.

11.1.1 VSWITCH controller

VSWITCH connectivity to an OSA device is managed through a *controller* virtual machine. The controller is responsible for the management of the OSA devices that are attached to the virtual switch. It handles the initialization of the device and communicates configuration information to the OSA port. In QDIO or OSA device terms, you can think of the controller as the manager of the control read and write devices and the Control Program (CP) as the manager of the data device. To enable this functionality, at least one TCP/IP virtual machine must be configured to act as a controller.

Two VSWITCH controllers (DTCVSW1 and DTCVSW2) come predefined with the base installation of z/VM Version 5, Release 3 and later releases. They are started during the IPL of the z/VM system through user AUTOLOG1. Both controllers are monitored by TCP/IP and get restarted if they become unresponsive.

Note: Unlike previous networking configurations that deployed a guest LAN with a router virtual machine TCP/IP stack, there is no requirement to define any IP addresses or devices in the TCP/IP stack for the VSWITCH controller virtual machines.

11.1.2 Network interface card

A network interface card (NIC) is a set of virtual I/O devices that simulate one of the following network adapters:

- OSA (in QDIO mode)
- IBM HiperSockets technology

Each guest system that is going to connect to a virtual switch needs to have at least one virtual NIC defined. After it is defined, this NIC can be connected to the virtual switch. To the guest operating system, the NIC devices look like a range of OSA devices. The NIC can be defined permanently with a z/VM user directory statement or temporarily (for the life of the guest system) by using CP commands. These CP commands are typically put into the guest system's PROFILE EXEC data set, along with the required COUPLE of the QDIO NIC to an existing VSWITCH, virtual HiperSockets LAN, or real HiperSockets LAN.

MAC addresses

A MAC address provides the identification for Ethernet frames that are transported across a LAN segment. A virtual NIC is assigned a locally defined MAC address by z/VM software when it is created. These locally generated MAC addresses are visible across the physical portion of the LAN segment through an OSA port when the VSWITCH is running in Layer 2 mode.

You can specify which MAC addresses are locally generated and assigned to each guest. system. This is done by using a combination of the `VMLAN` statement (in `SYSTEM CONFIG`) and the `NICDEF` statement (in the user directory).

The `VMLAN` statement contains a `MACPREFIX` parameter, which you can use to specify a 3-byte ID prefix for all MAC addresses in the z/VM system. The VMLAN parameter `MACIDRANGE` controls the range of identifiers that can be used by CP when generating the unique identifier component of a virtual NIC's MAC address.

In the user directory, a `NICDEF` statement is added for each guest that connects to the virtual switch. You can use the `MACID` parameter of `NICDEF` to specify a unique identifier that is appended to the `MACPREFIX` to form a unique MAC address for that guest system. If `MACID` is omitted, CP generates a unique identifier that is based on the range that is specified in the

`MACIDRANGE` parameter. If you specify a `MACID` value in the **`NICDEF`** that is already in use by another guest system, the virtual network adapter is not created. Therefore, a MACID value must be used to ensure that the guest systems maintain a consistent, predictable MAC address.

11.1.3 VSWITCH capabilities

In this section, we describe the key VSWITCH capabilities that are used with the OSA Ethernet features:

- Layer 2 and Layer 3 support
- VLAN support
- Port isolation support
- Link aggregation support

Layer 2 and Layer 3 support

Layer 2 and Layer 3 support relate to transport modes. A transport mode is a method that is used to identify, manage, and transport data through the virtual switch. The virtual switch supports two transport modes: IP mode and Ethernet mode. A virtual switch can operate in only one of the two transport modes at a time.

IP mode

In this mode, the virtual switch operates at Layer 3 (Network Layer) of the OSI model. IP addressing is used in IP mode to transport TCP/IP application data. The virtual switch works with the Layer 3 support of the OSA Ethernet features to communicate with hosts in an IP network. By default, the virtual switch operates in IP mode.

IP mode has these attributes:

- It supports IP for TCP/IP applications only.
- It supports IPv4 networks only.
- IP packets are transported on the LAN segment.
- All destinations are identified by IP addresses.
- IP address assignments are set by the TCP/IP stack in the guest virtual machine.
- Each TCP/IP stack can have more than one IP address.
- ARP processing is offloaded to the OSA adapter.
- VLAN tagging resides in internal QDIO headers.
- All TCP/IP stacks share the OSA burnt-in MAC address.

Ethernet mode

In this mode, the virtual switch operates at Layer 2 (data link layer) of the OSI model. Because Ethernet mode uses MAC addressing to forward frames, it is protocol-independent. This provides the ability to transport both TCP/IP and non-TCP/IP application data (such as SNA, DECnet, IPX, or NetBIOS). The virtual switch works with the Layer 2 support of the OSA Ethernet features to communicate with hosts on a physical LAN segment to which the OSA port is connected.

Ethernet mode has these key attributes:

- It supports all applications that deploy Ethernet (IEEE 802.2).
- Ethernet frames are transported on the LAN segment.
- All destinations are identified by MAC address.
- MAC addresses can be locally administered through z/VM CP commands or configuration statements.

- Each connection is identified by a single MAC address.
- TCP/IP stack maintains its own ARP cache.
- VLAN tagging resides within the Ethernet frames per IEEE 802.1Q specifications.
- IPv4 and IPv6 networks are supported.
- Required for deployment of link aggregation.

With Ethernet mode, the path length for transporting data is reduced because there is no need to traverse an extra layer up the protocol stack. For this reason and for the functional benefits, we suggest using the VSWITCH in Ethernet mode.

VLAN support

VLAN capability in the VSWITCH is based on IEEE standards 802.1p/Q and is supported by OSA Ethernet features that are running in QDIO mode. VLAN support works with both Layer 2 and Layer 3 transport modes in the VSWITCH.

The purpose of VLANs is to provide logical isolation. Therefore, VLANs behave like separate physical networks, even if they are within the same switch or VSWITCH. In order for devices in different VLANs to communicate, IP routing must occur.

The VLAN protocol uses additional information in the Ethernet header that is stored after the destination and source MAC address. The information marks the frame as one that contains a VLAN ID. This technique is known as *tagging*.

Delivery of frames that are tagged with a VLAN ID is controlled by the physical switch or VSWITCH, not by the devices that are connecting to the same infrastructure.

How the VSWITCH is defined (with or without the VLAN option) determines whether it is VLAN aware or VLAN unaware.

The VSWITCH supports two VLAN mode types: *access mode* and *trunk mode*. These modes specify whether the VSWITCH applies a VLAN tag (access mode) or expects the VLAN tag (trunk mode) to be applied by the connected guest system.

Ports in access mode

An *access port* is a type of connection in a VSWITCH that is used to transport data from a guest system that is VLAN-unaware. This port provides the guest system with connectivity through a VSWITCH that is VLAN-aware, without requiring the guest system to support VLAN tagging.

Access port definitions work with a Layer 2 or a Layer 3 VSWITCH. Only one VLAN ID can be used for each access port.

Ports in trunk mode

A *trunk port* is a type of connection in a VSWITCH that is used to transport data from a guest system that is VLAN-aware. Generally, all frames that flow through this port are VLAN tagged. The exception to this is when a trunk port is granted access to the untagged VLAN set.

Trunk port definitions work with a Layer 2 and a Layer 3 VSWITCH. Multiple VLAN IDs can be assigned to each trunk port.

Port isolation support

Through the port-sharing capabilities of the OSA feature and VSWITCH, systems that are operating in separate z/VM images or logical partitions (LPARs) can communicate directly through the same OSA feature or VSWITCH without sending data to the physical network. In some cases, this can pose a security threat, which can be eliminated with the use of VLANs. However, VLANs might not satisfy all requirements for complete isolation.

Port isolation minimizes the security risk by separating and isolating frames within the VSWITCH and preventing guest systems that share the VSWITCH from communicating with each other.

When port isolation is turned on, traffic is also blocked between those guest systems that share the VSWITCH and OSA port. All network traffic is forced to pass through the physical OSA port. Only routing outside of the IBM System z server allows connectivity to the VSWITCH. This is also true for multiple VSWITCHes that share OSA port and for connections to other logical partitions that share OSA port.

Link aggregation support

Link aggregation support allows up to eight dedicated OSA ports to appear as a single logical link for data transmissions with a physical LAN. This capability provides load balancing and failover for a VSWITCH.

In the z/VM operating system, these links are OSA ports that are grouped on a VSWITCH that is operating in Ethernet mode (Layer 2) and given a group name. From the VSWITCH perspective, the group is treated as a single link for external connectivity. A port group on the VSWITCH conforms to the Link Aggregation Group (LAG) defined by IEEE 802.3ad.

When OSA ports are grouped into a LAG, they can no longer be share with other operating systems or LPARs. After an OSA port is removed from the group, it can be shared again.

Link aggregation in the VSWITCH works only in ETHERNET mode and has the following requirements:

- All OSA ports in the LAG must be connected to the same external Ethernet switch.
- The external Ethernet switch must support the IEEE 802.3ad standard.
- All ports must run in full duplex mode and use the same speed setting.
- For single port per CHPID (OSA features), all defined devices must be inactive on all LPARs. This includes the z/VM LPAR where the VSWITCH is running.
- For multiport per CHPID (OSA- features), if only one port is used for link aggregation, then the other ports can be used for other VSWITCHs or TCP/IP stacks.

For more information about these topics and z/VM communication services and concepts, see *z/VM Connectivity Version 6 Release 3*, SC24-6174.

11.2 Our VSWITCH environment

Figure 11-2 on page 117 shows our VSWITCH environment, which consisted of a z/VM Version 6, Release 3 LPAR and a z/OS Version 2, Release 1 LPAR that share two OSA-Express5S 1000BASE-T and two OSA-Express4S 1000BASE-T ports. The four OSA ports were connected to ports on an Ethernet switch that were defined as trunk ports. The OSA ports were defined to our System zEC12 server as channel type OSD (QDIO), which is a requirement for Layer 2 support.

Two virtual switches were configured in the z/VM LPAR with two virtual controllers (primary and backup). The OSA ports were attached to the virtual switches to provide connectivity from the guest systems to the external LAN.

Note: VSWITCH administration is a dynamic process. It allows you to change access authorizations dynamically. However, for changes to the attributes of the VSWITCH (such as transport mode or VLAN aware or unaware), the VSWITCH must be redefined.

Under z/VM, two Linux guest systems were configured, as Figure 11-2 shows:

- LNXSU1 (SUSE Linux Enterprise Server [SLES] 11 SP2)
- LNXRH1 (Red Hat Enterprise Linux Server release 6.4)

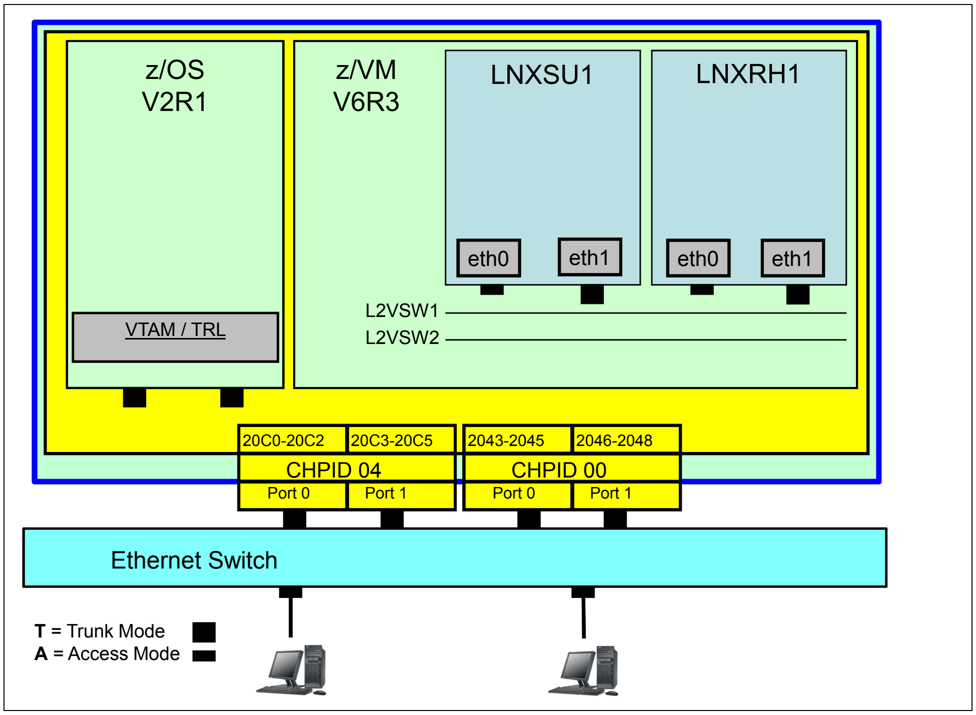


Figure 11-2 The VSWITCH environment

Note: Figure 11-2 is a multipurpose diagram that is used throughout the remainder of this chapter.

The purpose of our VSWITCH environment is to show the following functionality:

1. Layer 2 within the VSWITCH, Linux guest systems, and OSA ports
2. VLAN support across the VSWITCH, Linux guest systems, z/OS environment, and the clients that are connected to the Ethernet switch
3. Port isolation across the Ethernet switch between the VSWITCH, Linux guest systems, and z/OS environment
4. Link aggregation across the VSWITCH, the OSA ports, and Ethernet switch

Tip: Check the appropriate Preventive Service Planning buckets (PSP) buckets for required APARs and PTFs before implementing the VSWITCH in your environment.

We provide setup and verification examples in the following sections:

- Configuring a Layer 2 VSWITCH
- Configuring VLAN support
- Enabling port isolation

To validate our VSWITCH environment, we used OSA/SF and various system commands. You will find examples of their use in the subsequent sections of this chapter.

11.3 Configuring a Layer 2 VSWITCH

In this section, we explain how our VSWITCH was configured in Ethernet mode to support Layer 2 traffic and how this environment was verified.

Figure 11-3 shows our Layer 2 virtual switch configuration.

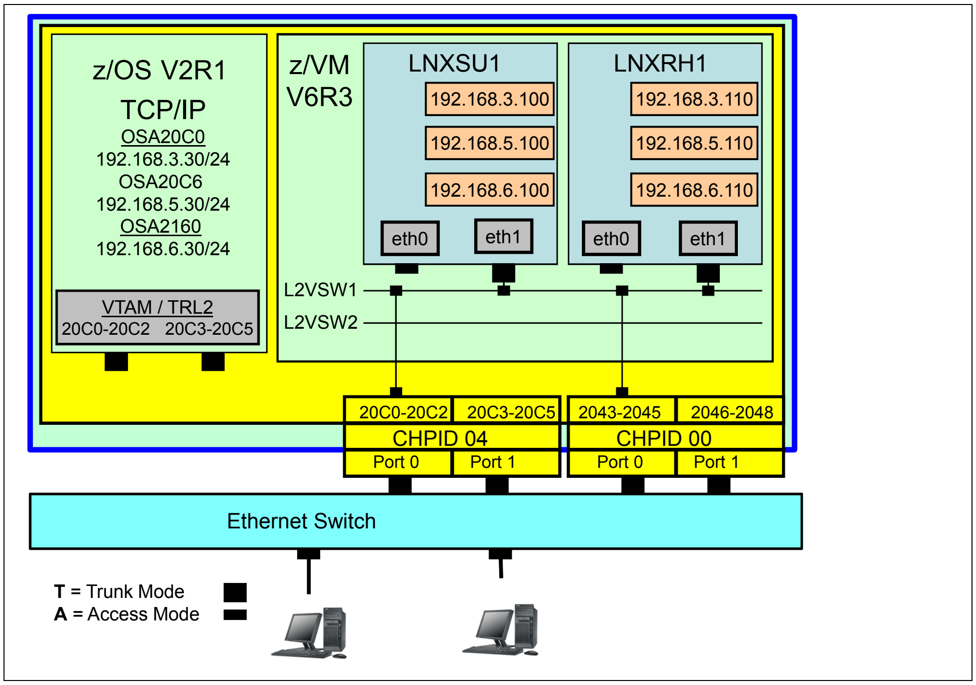


Figure 11-3 Layer 2 virtual switch configuration

We show how to do the following tasks:

- Configure a Layer 2 virtual switch environment by using OSA ports.
- Verify the Layer 2 virtual switch environment.
- Verify connectivity between guests and clients that are connected through the virtual switch and OSA port.

11.3.1 Define the virtual switch environment

These are the steps that we followed to implement our Layer 2 VSWITCH environment:

1. Defined a virtual switch to provide network connectivity between guest systems and clients over the OSA port.
2. Authorized access for each guest system to the virtual switch.

3. Created a simulated network interface controller (NIC) on each guest system to be connected to the virtual switch.
4. Verified the configuration.

Note: Definitions that are made in the z/VM `SYSTEM CONFIG` file can be added to the `PROFILE EXEC` of the user `AUTOLOG1`. The `AUTOLOG` virtual machine is automatically logged on as part of the z/VM IPL sequence and is a convenient way to make definitions permanent.

A virtual switch is created by using the CP **`DEFINE VSWITCH`** command from any z/VM Class B user (such as MAINT, TCPMAINT, or AUTOLOG1), or by adding the following definition to the `SYSTEM CONFIG` file:

```
DEFINE VSWITCH L2VSW1 RDEV 20C0 2043 ETHERNET
DEFINE VSWITCH L2VSW2 RDEV 2046 20C3 ETHERNET
```

The `ETHERNET` parameter indicates that the virtual switch operates in Ethernet mode and provides Layer 2 functionality. The virtual switch is connected to two OSA port, CHPID `04` (devices `20C0-20C2`) and CHPID `00` (devices `2043-2045`).

Devices `2043-2045` are for a secondary interface to be used if there is a problem with the primary interface (devices `20C0-20C2`).

The syntax of the `DEFINE VSWITCH` statement is as follows:

```
DEFINE VSWITCH switchname [ operands ]
```

The *switchname* is the name of the virtual switch, and the *operands* define the attributes of the virtual switch.

Add VMLAN

In addition, you can add a `VMLAN` statement to the CP `SYSTEM CONFIG` file, which overrides the system-wide MAC address definitions that are used when generating local MAC addresses for the individual NIC devices the guest systems use. We used the default system generated MAC address settings because we had only a single z/VM system in our environment.

The syntax of the `VMLAN` statement is as follows:

```
VMLAN [ operands ]
```

In this statement, *operands* means the attributes to be set for all z/VM guest LANs in the system. The definitions in Example 11-1 can be used to modify the default VMLAN values.

Example 11-1 VMLAN definition

```
VMLAN MACPREFIX 02EEEE
VMLAN MACIDRANGE SYSTEM 100000-1FFFFF
```

Tip: If you run multiple z/VM systems on a System z server, change the `MACPREFIX` of each system to avoid MAC address duplication.

See *CP Commands and Utilities Reference*, SC24-6081 for all operands accepted by the commands that are used in the chapter.

11.3.2 Authorize the guest system access to the virtual switch

To authorize guest system access to a VSWITCH, statements need to be added to the `SYSTEM CONFIG` file on MAINT disk CF1. We added `MODIFY VSWITCH` statements (see Example 11-2) to grant access to the virtual switch. You can also use **`SET VSWITCH`** commands to achieve the same results.

Example 11-2 MODIFY VSWITCH statement in SYSTEM CONFIG file

```
MODIFY VSWITCH L2VSW1 GRANT LNXSU1
MODIFY VSWITCH L2VSW2 GRANT LNXSU1
MODIFY VSWITCH L2VSW1 GRANT LNXRH1
MODIFY VSWITCH L2VSW2 GRANT LNXRH1
```

To add, change, or remove authorizations of guest systems, the z/VM CP provides the Class B command **`SET VSWITCH`** ***`switchname`***.

Example 11-3 Add user authorization by using CP commands

```
SET VSWITCH L2VSW1 GRANT LNXSU1
SET VSWITCH L2VSW2 GRANT LNXSU1
SET VSWITCH L2VSW1 GRANT LNXRH1
SET VSWITCH L2VSW2 GRANT LNXRH1
```

Example 11-4 Revoke a user authorization by using CP commands

```
SET VSWITCH L2VSW1 REVOKE LNXSU1
```

This function can also be performed by an external security manager (ESM), such as the IBM Resource Access Control Facility (RACF®). For more information about the use of an ESM, see Appendix K, “Authorization in the IBM z/VM operating system” on page 251.

11.3.3 Connect the guest systems to the VSWITCH

To connect guest systems to the VSWITCH, you need virtual NICs. To create a virtual NIC that will remain permanently defined to a guest system (after initial program loads, or IPLs, of the guest system or the z/VM operating system), a `NICDEF` statement needs to be added to the z/VM user directory.

Alternative: To dynamically link your guest systems to the virtual switch, use the **`DEFINE NIC`** and **`COUPLE`** commands. See “Defining and coupling a NIC using CP commands” on page 187.

The *NICDEF* statement defines virtual OSA devices, which are fully simulated by the VM CP. Example 11-5 shows a sample user directory entry for our Linux guests that connect to the VSWITCH (`L2VSW1`).

Example 11-5 NICDEF statements for Linux guests that are connecting to L2VSW1

```
USER LNXSU1 LNX4ITSO  2G 4G  G
   NICDEF 8000 TYPE QDIO LAN SYSTEM L2VSW1

USER LNXRH1 LNX4ITSO  2G 4G  G
   NICDEF 8000 TYPE QDIO LAN SYSTEM L2VSW1
```

Note: We could have added a `MACID` parameter to the `NICDEF` statement. Instead, we chose to let the system generate the MAC address for us.

This is the syntax of the `NICDEF` statement for a virtual NIC:

`NICDEF` *`vdev`* `TYPE QDIO [` *`operands`* `]`

In this statement, *vdev* specifies the base virtual device address for the adapter, and *operands* defines the characteristics of the virtual NIC.

11.3.4 Verify the virtual switch configuration

We performed an initial program load (IPL) of our z/VM LPAR and checked to ensure that the changes we made were correct by querying the controller, VSWITCH, NIC, VMLAN, and access authorizations.

Note: We could have made all of our changes dynamically by issuing the configuration commands directly from MAINT or any other Class B user ID. Dynamic changes are useful when you are unable to do an IPL of z/VM software or if the changes are only temporary.

Check the controller

To check whether the VM TCP/IP stacks are recognized as controller virtual machines, the **`QUERY CONTROLLER`** command can be used (see Example 11-6).

Example 11-6 QUERY CONTROLLER output

```
QUERY CONTROLLER
Controller DTCVSW1   Available: YES   VDEV Range: 0600-F000 Level 630
  Capability: IP ETHERNET VLAN_ARP GVRP    LINKAGG    ISOLATION
              NO_ENSEMBLE NO_INMN BRIDGE_CAPABLE    VEPA
   SYSTEM L2VSW1     Active           Controller: *         RDEV: 20C0
   SYSTEM L2VSW2     Active           Controller: *         RDEV: 2046

Controller DTCVSW2   Available: YES   VDEV Range: 0600-F000 Level 630
  Capability: IP ETHERNET VLAN_ARP GVRP    LINKAGG    ISOLATION
              NO_ENSEMBLE NO_INMN BRIDGE_CAPABLE    VEPA
   SYSTEM L2VSW1     Backup           Controller: *         RDEV: 2043
   SYSTEM L2VSW2     Backup           Controller: *         RDEV: 20C3
```

Check the VSWITCH

To check the state of the virtual switch, the **QUERY VSWITCH** command can be used (see Example 11-7).

Example 11-7 QUERY VSWITCH

```
Q VSWITCH L2VSW1
VSWITCH SYSTEM L2VSW1   Type: QDIO    Connected: 2    Maxconn: INFINITE
  PERSISTENT  RESTRICTED    ETHERNET                  Accounting: OFF
  USERBASED
  VLAN Unaware
  MAC address: 02-00-00-00-00-76    MAC Protection: Unspecified
  IPTimeout: 5         QueueStorage: 8
  Isolation Status: OFF        VEPA Status: OFF
 Uplink Port:
  State: Ready
  PMTUD setting: EXTERNAL   PMTUD value: 8992
  RDEV: 20C0.P00 VDEV: 0630 Controller: DTCVSW1  ACTIVE
  RDEV: 2043.P00 VDEV: 062A Controller: DTCVSW2  BACKUP
```

Check the VMLAN

If you choose to change the default system-wide MAC addresses rather than the system default MAC addresses, use the **QUERY VMLAN** command to check whether the VMLAN changes are applied (see Example 11-8).

Example 11-8 QUERY VMLAN

```
QUERY VMLAN
VMLAN maintenance level:
  Latest Service: Base
VMLAN MAC address assignment:
  System MAC Protection: OFF
  MACADDR Prefix: 020000 USER Prefix: 020000
  MACIDRANGE SYSTEM: 000001-FFFFFF
             USER:   000000-000000
VMLAN Unified Resource Manager status:
  Hypervisor Access: NO        Status: UNAVAILABLE
  ID: NONE
  MAC Prefix: 000000
VMLAN default accounting status:
  SYSTEM Accounting: OFF       USER Accounting: OFF
VMLAN general activity:
  PERSISTENT Limit: INFINITE   Current: 5
  TRANSIENT  Limit: INFINITE   Current: 0
```

Check authorization

To check the access list of the authorized user IDs for the virtual switch, use the **QUERY VSWITCH switchname** application control command (ACC) command (see Example 11-9 on page 123).

Example 11-9 QUERY VSWITCH command

```
QUERY VSWITCH L2VSW1 ACC
VSWITCH SYSTEM L2VSW1   Type: QDIO    Connected: 2    Maxconn: INFINITE
  PERSISTENT  RESTRICTED    ETHERNET                  Accounting: OFF
  USERBASED
  VLAN Unaware
  MAC address: 02-00-00-00-00-76    MAC Protection: Unspecified
  IPTimeout: 5        QueueStorage: 8
  Isolation Status: OFF        VEPA Status: OFF
    Authorized userids:
      LNXRH1   LNXSU1
 Uplink Port:
  State: Ready
  PMTUD setting: EXTERNAL   PMTUD value: 8992
  RDEV: 20C0.P00 VDEV: 0630 Controller: DTCVSW1  ACTIVE
  RDEV: 2043.P00 VDEV: 062A Controller: DTCVSW2  BACKUP
```

Check the NICs

To check the NIC for each guest system, enter the **QUERY NIC DETAILS** command from the guest system's z/VM user ID (see Example 11-10).

Example 11-10 QUERY NIC details (LNXSU1)

```
QUERY NIC DETAILS
Adapter 8000.P00 Type: QDIO      Name: UNASSIGNED  Devices: 3
  MAC: 02-00-00-00-00-72         LAN: * None
      RX Packets: 0          Discarded: 0          Errors: 0
      TX Packets: 0          Discarded: 0          Errors: 0
      RX Bytes: 0                    TX Bytes: 0
  Unassigned Devices:
      Device: 8000  Unit: 000   Role: Unassigned
      Device: 8001  Unit: 001   Role: Unassigned
      Device: 8002  Unit: 002   Role: Unassigned
```

Notice that the default MAC address, 02-00-00-00-00-72, was assigned by the system.

11.3.5 Creating definitions for Layer 2 support: SUSE and Red Hat Linux

For Layer 2 support, an OSA QDIO device must be attached and defined to the Linux version that is running on a System z. We used a virtual NIC with addresses 8000, 8001, and 8002 that were coupled or attached to the VSWITCH L2VSW1.

To verify the virtual NIC already defined to the Linux, you can use **the lscss** command (see Example 11-11)

Example 11-11 lscss command

```
lnxsu1:~ # lscss
Device   Subchan.  DevType CU Type Use  PIM PAM POM  CHPIDs
----------------------------------------------------------------------
0.0.8000 0.0.000c  1732/01 1731/01      80  80  80   05000000 00000000
0.0.8001 0.0.000d  1732/01 1731/01      80  80  80   05000000 00000000
0.0.8002 0.0.000e  1732/01 1731/01      80  80  80   05000000 00000000
```

To activate the interface, you echo the addresses of the OSA devices (real or virtual) to the `sysfs` structure (see Example 11-12).

Example 11-12 Echo command

```
echo 0.0.8000,0.0.8001,0.0.8002 > /sys/bus/ccwgroup/drivers/qeth/group
```

The `/var/log/messages` file contains entries that show the status of the OSA devices (see Example 11-13).

Example 11-13 Contents of /var/log/messages file

```
Nov 13 10:00:38 lnxsu1 kernel: qeth.e9767c: register layer 2 discipline
Nov 13 10:00:38 lnxsu1 kernel: qdio: 0.0.8002 OSA on SC e using AI:1 QEBSM:0 PCI:1
TDD:1 SIGA:RW A
Nov 13 10:00:38 lnxsu1 kernel: qeth.980814: 0.0.8000: MAC address
02:00:00:00:00:72 successfully registered on device eth1
Nov 13 10:00:38 lnxsu1 kernel: qeth.7c6a37: 0.0.8000: Device is a Guest LAN QDIO
card (level: V630)
Nov 13 10:00:38 lnxsu1 kernel: with link type GuestLAN QDIO (portname: )
Nov 13 10:00:38 lnxsu1 ifup:     eth1      name: ITSO OSA Express5S Network card
(0.0.8000)
```

The interface name is `eth1` and should be online. Use the following command to check:

```
cat /sys/bus/ccwgroup/drivers/qeth/0.0.8000/online
```

The output should be `1` if the device is online. If the output is `0`, you must issue the following command to bring it online:

```
echo 1 > /sys/bus/ccwgroup/drivers/qeth/0.0.8000/online
```

After the interface is registered successfully, the network definitions can be created by using this command:

```
ifconfig eth1 192.168.3.100 netmask 255.255.255.0 up
```

On the z/VM side, we verified the connection by using the **`QUERY VSWITCH`** command, as shown in Example 11-14 on page 125.

Example 11-14 Query VSWITCH detail - output

```
VSWITCH SYSTEM L2VSW1   Type: QDIO    Connected: 2    Maxconn: INFINITE
  PERSISTENT  RESTRICTED   ETHERNET                   Accounting: OFF
  USERBASED
  VLAN Unaware
  MAC address: 02-00-00-00-00-76    MAC Protection: Unspecified
  IPTimeout: 5        QueueStorage: 8
  Isolation Status: OFF       VEPA Status: OFF
 Uplink Port:
  State: Ready
  PMTUD setting: EXTERNAL   PMTUD value: 8992
  RDEV: 20C0.P00 VDEV: 0630 Controller: DTCVSW1  ACTIVE
    Uplink Port Connection:
      RX Packets: 0         Discarded: 0         Errors: 0
      TX Packets: 16        Discarded: 0         Errors: 0
      RX Bytes: 0                   TX Bytes: 1320
      Device: 0630  Unit: 000   Role: DATA       Port: 2049
      Partner Switch Capabilities: No_Reflective_Relay
  RDEV: 2043.P00 VDEV: 062A Controller: DTCVSW2  BACKUP
 Adapter Connections:                           Connected: 2
    Adapter Owner: LNXRH1   NIC: 8000.P00 Name: UNASSIGNED  Type: QDIO
      RX Packets: 0         Discarded: 0         Errors: 0
      TX Packets: 6         Discarded: 0         Errors: 0
      RX Bytes: 0                   TX Bytes: 468
      Device: 8002  Unit: 002   Role: DATA       Port: 0001
      Options: Ethernet Broadcast
        Unicast MAC Addresses:
          02-00-00-00-00-74
        Multicast MAC Addresses:
          01-00-5E-00-00-01
          33-33-00-00-00-01
          33-33-FF-00-00-74
    Adapter Owner: LNXSU1   NIC: 8000.P00 Name: UNASSIGNED  Type: QDIO
      RX Packets: 0         Discarded: 0         Errors: 0
      TX Packets: 6         Discarded: 0         Errors: 0
      RX Bytes: 0                   TX Bytes: 468
      Device: 8002  Unit: 002   Role: DATA       Port: 0002
      Options: Ethernet Broadcast
        Unicast MAC Addresses:
          02-00-00-00-00-72
        Multicast MAC Addresses:
          01-00-5E-00-00-01
          33-33-00-00-00-01
          33-33-FF-00-00-72
```

Notice that both `LNXSU1` and `LNXRH1` are connected to the virtual switch (`L2VSW1`). Also, you can see the system-generated MAC addresses.

We used the **`ping`** command to verify connectivity between `LNXSU1` and `LNXRH1` over the virtual switch.

11.3.6 Setting up Layer 2 for the guest systems

We chose to configure a static IP address for each Linux guest, LNXSU1 (192.168.3.100) and LNXRH1 (192.168.3.110), using the following commands:

```
ifconfig eth1 192.168.3.100 netmask 255.255.255.0 up
ifconfig eth1 192.168.3.110 netmask 255.255.255.0 up
```

To test our environment, we issued **ping** commands between LNXSU1, LNXRH1, and the workstations connected through an OSA port that were attached to an Ethernet switch.

> **Alternative:** We could define the Linux guests as Dynamic Host Configuration Protocol (DHCP) clients to request IP addresses from a DHCP server that is running on the LAN. This works because the Linux guests' MAC addresses are visible to both the internal and external segments of the LAN.

Configuring a Linux device has changed from using /etc/chandev.conf to the use of the sysfs structure. Scripts in /etc/sysconfig/hardware and /etc/sysconfig/network/ for SUSE, along with /etc/sysconfig/network-scripts/ for Red Hat, configure the qeth devices and network definitions.

In addition to making permanent definitions by using the appropriate scripts, those definitions can also be made dynamically. See *Device Drivers, Features, and Commands*, SC33-8289 for details.

11.3.7 Making permanent device and network definitions

SUSE and Red Hat provide a set of GUI tools and shell scripts to configure network devices and network settings. However, depending on the distribution, different members are created.

Create permanent Layer 2 definitions for SUSE

To make all of the definitions from the previous section permanent, we coded the required information into the distribution-specific configuration member.

SUSE SLES 11 has two locations where the final hardware-related and network-related configuration files are stored. These locations will not change.

- Hardware-related definitions are stored in this path:

  ```
  /etc/sysconfig/hardware
  ```

- Network interface definitions are stored in this path:

  ```
  /etc/sysconfig/network
  ```

You must decide whether to use one of the existing interfaces or create a new interface.

In our environment, we created a new member for device address 8000. SUSE uses file names that are created from the type of hardware, combined with the hardware address. OSA QDIO devices are named hwcfg-qeth-bus-ccw-0.0.8000.

If you plan to implement Layer 2 support, insert a QETH_LATER2_SUPPORT='1' statement.

On our SUSE system, we created the hardware configuration member in Example 11-15 on page 127 for the NIC 8000 device.

Example 11-15 /etc/sysconfig/hardware/hwcfg-qeth-bus-ccw-0.0.8000

```
CCW_CHAN_IDS='0.0.8000 0.0.8001 0.0.8002'
CCW_CHAN_MODE=''
CCW_CHAN_NUM='3'
LCS_LANCMD_TIMEOUT=''
MODULE='qeth'
MODULE_OPTIONS=''
QETH_IPA_TAKEOVER='0'
QETH_LAYER2_SUPPORT='1'
QETH_OPTIONS=''
SCRIPTDOWN='hwdown-ccw'
SCRIPTUP='hwup-ccw'
SCRIPTUP_ccw='hwup-ccw'
SCRIPTUP_ccwgroup='hwup-qeth'
STARTMODE='auto'
```

The network definition file for NIC device 8000 is shown in Example 11-16.

Example 11-16 /etc/sysconfig/network/ifcfg-eth1

```
BOOTPROTO='static'
IPADDR='192.168.3.100'
BROADCAST=''
STARTMODE='auto'
NAME='ITSO OSA Express5S Network card (0.0.8000)'
USERCONTROL='no'
NETMASK='255.255.255.0'
```

Create permanent Layer 2 definitions for Red Hat

Red Hat RHEL 6 has one location where both network- and hardware-related interface information is stored. This location is fixed and will not change:

```
/etc/sysconfig/network-scripts
```

We created a configuration file for the new device with address x'8000'. Red Hat Enterprise Linux (RHEL) uses file names that start with ifcfg- concatenated with the Linux interface name. For example, OSA QDIO devices are called:

```
ifcfg-eth1
```

RHEL puts hardware-related and network definitions in one configuration file.

On our Red Hat system, we created the configuration file for the NIC 8000 device, as shown in Example 11-17 on page 128.

Example 11-17 /etc/sysconfig/network-scripts/ifcfg-eth1

```
# IBM QETH
DEVICE=eth1
VSWITCH=1
OPTIONS="layer2=1"
BOOTPROTO=none
IPADDR=192.168.3.110
NETMASK=255.255.255.0
NETTYPE=qeth
ONBOOT=yes
SUBCHANNELS=0.0.8000,0.0.8001,0.0.8002
TYPE=Ethernet
USERCTL=no
IPV6INIT=no
PEERDNS=yes
```

11.4 Configuring VLAN support

To demonstrate Layer 2 functionality across the virtual switch and OSA ports, we extended our Layer 2 configuration to include the z/OS TCP/IP stacks. Connectivity to the z/OS systems is provided through an Ethernet switch. The steps described previously to configure and implement a virtual switch environment remain the same, except for the VLAN-specific changes that are highlighted in the following text. As mentioned previously, the configuration changes can be made dynamically, depending on your circumstances, but to make them permanent, you must add them to your system configuration files.

Previously, our configuration traversed the virtual switch fabric without the use of VLAN IDs. These are the next objectives:

- Add VLAN functionality to the environment (z/VM and z/OS)
- Verify the VLAN environment
- Show VLAN connectivity between the virtual switch, Linux guest systems, and the z/OS TCP/IP stacks

Figure 11-4 illustrates our VSWITCH environment with VLANs.

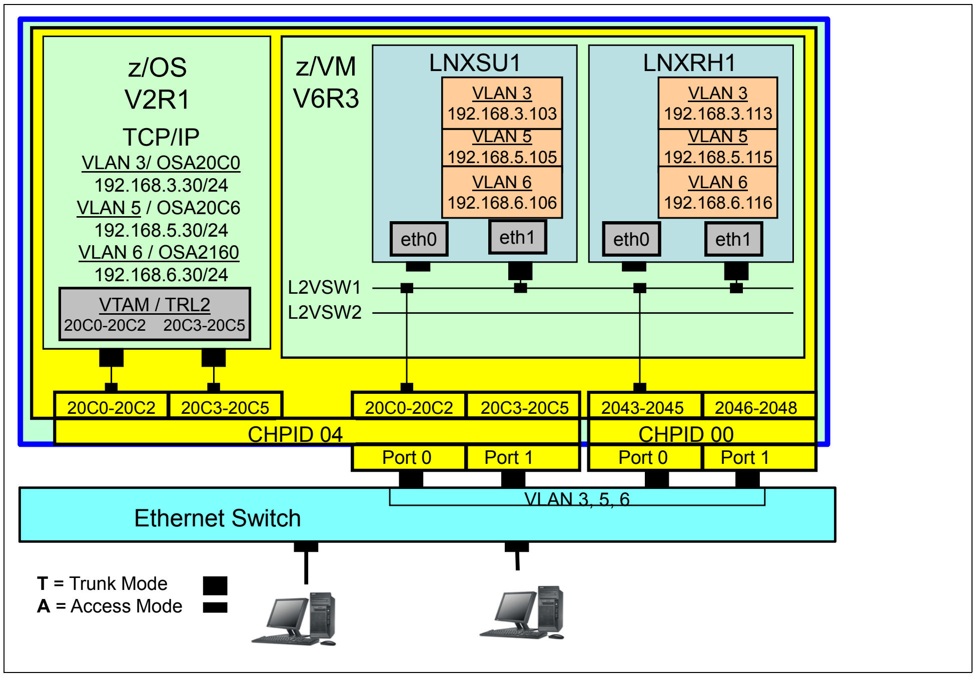


Figure 11-4 Our VSWITCH environment with VLANs

To add VLAN capability to our VSWITCH environment, we followed these steps:

1. Define VLAN capabilities to the virtual switch
2. Authorize Linux guests access to the virtual switch with VLAN IDs
3. Add VLANs to the guest systems
4. Add VLAN support to the z/OS TCP/IP stacks
5. Configure trunk mode in the Ethernet switch for the OSA connections
6. Verify the LAN.

11.4.1 Define VLAN capabilities to the virtual switch

When configuring a virtual switch with VLAN capabilities, you can select whether the VSWITCH provides access mode or trunk mode. We configured our environment in trunk mode to show the Layer 2 and VLAN capabilities of the virtual switch with the OSA port and Ethernet switch. For more information about VLAN support and access or trunk mode, see Chapter 10, “VLAN support” on page 89.

For assistance with the VLAN configuration process, see the flowchart shown in Figure 11-5.

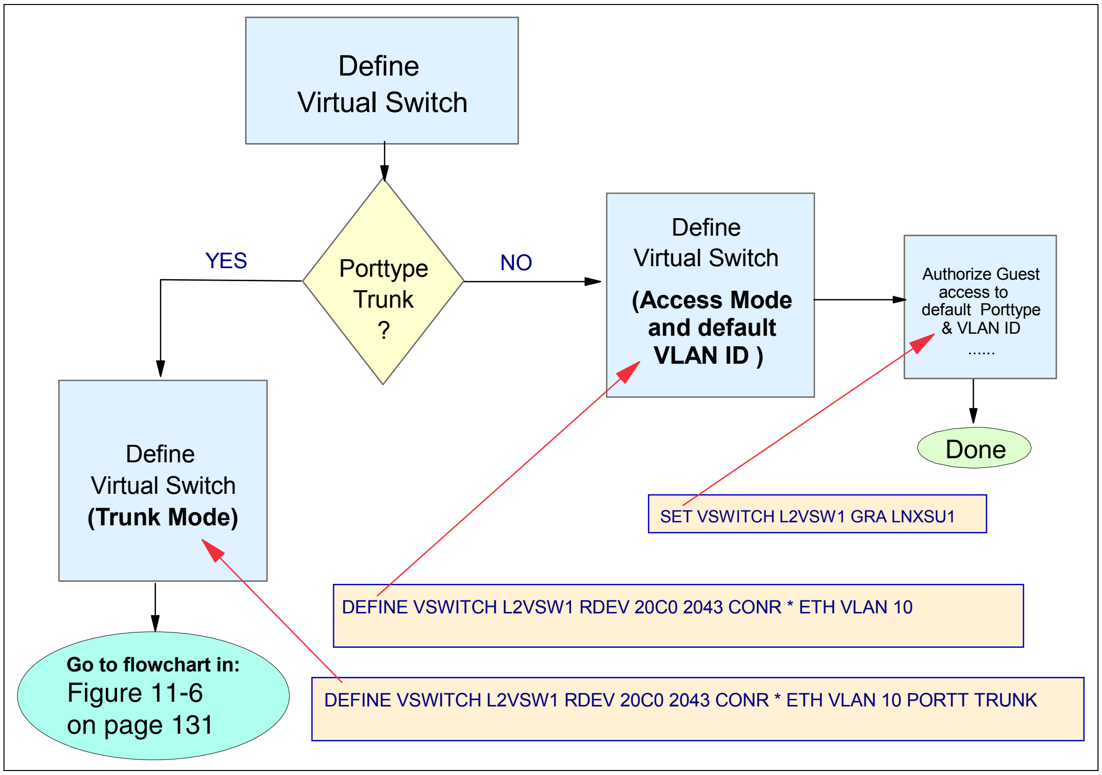


Figure 11-5 Virtual switch: VLAN configuration

The VLAN ID and port type values that are used in the **DEFINE VSWITCH** command are inherited by the guest systems when it is attaching to the virtual switch.

To add VLAN support to the virtual switch, add parameters on the **DEFINE VSWITCH** command. We configured our virtual switch as a trunk port with a default VLAN ID of 10 as shown in Example 11-18. For more information about VLAN standards and support, see Chapter 10, “VLAN support” on page 89.

Example 11-18 Defining the trunk port type

```
DEFINE VSWITCH L2VSW1 RDEV 20C0 2043 ETH VLAN 3 PORTT TRUNK
```

Another operand that can be specified when you defining a VLAN-aware virtual switch is NATive. This keyword and value specifies the native VLAN ID to be associated with untagged frames received and transmitted by the virtual switch. If this option is omitted, the default VLAN is used as the native VLAN ID. Usually, the same native VLAN ID as your real switch must be used. The default for most Ethernet switches is 1.

11.4.2 Authorize Linux guests access to the virtual switch with VLAN IDs

You must update the access authorization for the Linux guests to include VLAN capabilities. With the **set vswitch** command, you can authorize access for guests and change the default values for a virtual switch that is defined as a trunk port. For assistance with the VLAN port type configuration options and granting access, see the flowchart shown in Figure 11-6 on page 131.

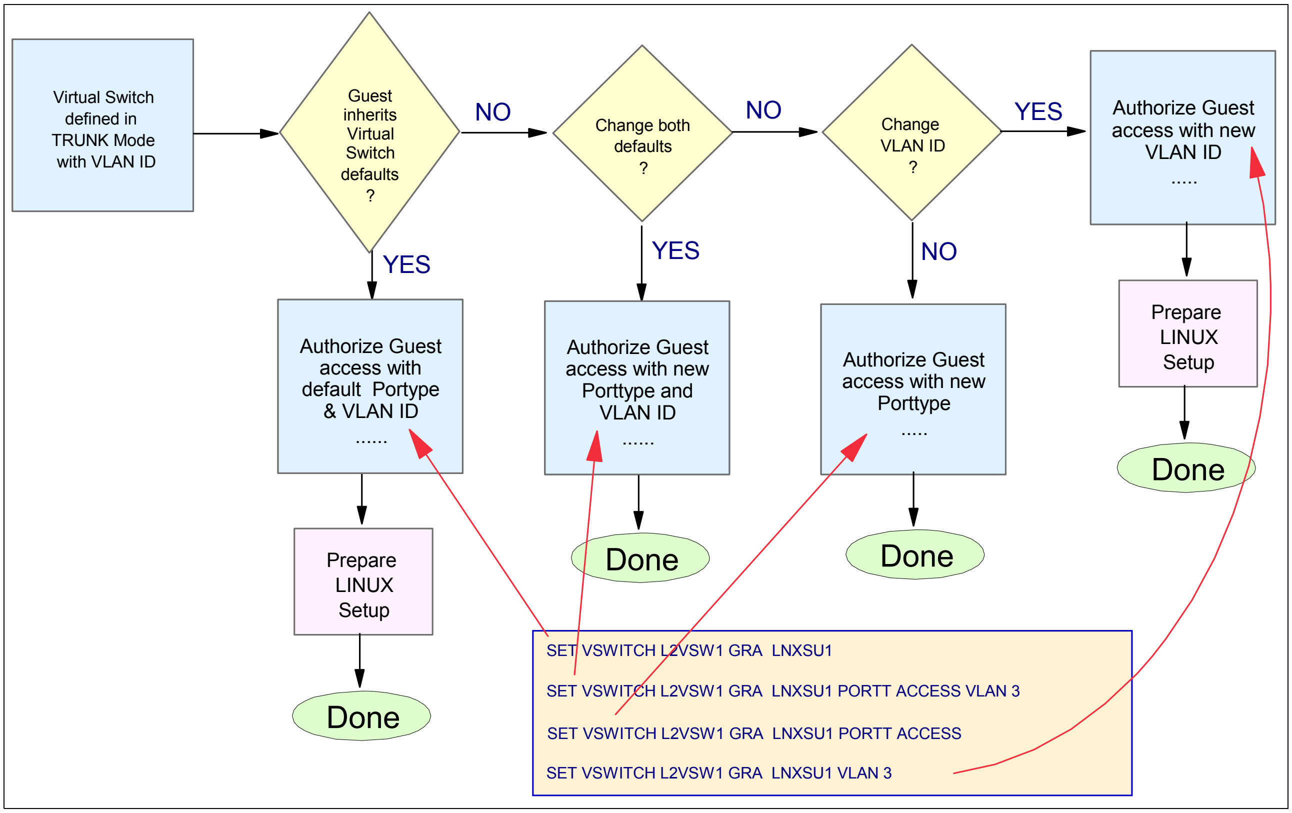

Virtual Switch defined in TRUNK Mode with VLAN ID
Guest inherits Virtual Switch defaults ?
NO
Change both defaults ?
NO
Change VLAN ID ?
YES
Authorize Guest access with new VLAN ID .....
YES
YES
NO
Authorize Guest access with default Portype & VLAN ID ......
Authorize Guest access with new Porttype and VLAN ID ......
Authorize Guest access with new Porttype .....
Prepare LINUX Setup
Done
Done
Done
Prepare LINUX Setup
Done
SET VSWITCH L2VSW1 GRA LNXSU1
SET VSWITCH L2VSW1 GRA LNXSU1 PORTT ACCESS VLAN 3
SET VSWITCH L2VSW1 GRA LNXSU1 PORTT ACCESS
SET VSWITCH L2VSW1 GRA LNXSU1 VLAN 3

Figure 11-6 Virtual switch - VLAN port type configuration options

For our environment, we revoked all access and then authorized each guest to have access to the virtual switch by using the SET VSWITCH command (see Example 11-19). Notice the VLAN parameters and absence of the PORTTYPE parameter. The port type was determined in the VSWITCH definition (from Example 11-18 on page 130).

Example 11-19 Authorizing the guests

```
SET VSWITCH L2VSW1 GRA LNXSU1 VLAN 3-6
SET VSWITCH L2VSW1 GRA LNXRH1 VLAN 3-6
```

11.4.3 Add VLANs to the guest systems

To enable VLAN support on the Linux guests, changes must be made to the interface that represents the virtual switch. In our case, this is `eth1`. We applied an IP address of `0.0.0.0` to eth1 to eliminate any IP address conflicts, then we added the VLAN IDs with the corresponding IP address.

> **Important:** For the virtual switch to identify the correct VLAN and IP address that is allocated to the Linux guest, it is important to define eth'x' with an IP address of `0.0.0.0` using the `ifconfig eth'x' 0.0.0.0 up` command. Failure to do so results in the virtual switch incorrectly associating the VLAN ID with the eth'x' interface IP address. By specifying an IP address of zero, the eth'x' interface presents the appropriate VLAN interface IP address to the virtual switch.

Define VLAN support for SUSE and Red Hat versions of Linux

Previous steps to configure and implement a virtual switch environment remain the same, except for the VLAN-specific values.

The VLAN configuration changes can be made dynamically depending on your circumstances. However, to make them permanent, you must add them to your system configuration files.

> **Important:** Ensure that your Linux guest system is at the appropriate kernel version. See 10.4, “VLAN support in the IBM z/VM operating system” on page 104, for details.

When configuring a virtual switch with VLAN capabilities, you can select either access mode or trunk mode. We configured our environment in trunk mode to show the Layer 2 and VLAN capabilities of the virtual switch with the OSA ports and Ethernet switch. For more information about VLAN support and access mode and trunk mode, see Chapter 10, “VLAN support” on page 89.

For the shell scripts to define a VLAN interface, see *Device Drivers, Features, and Commands*, SC33-8289. You can download it from this web page:

http://download.boulder.ibm.com/ibmdl/pub/software/dw/linux390/docu/l26cdd03.pdf

The scripts work the same way in SUSE and Red Hat versions of Linux. See Example 11-20 for the SUSE results and Example 11-21 for the Red Hat results.

Example 11-20 SUSE defining VLAN ID 3 on Interface eth1

```
lnxsu1:~ # vconfig add eth1 3
Added VLAN with VID == 3 to IF -:eth1:-
lnxsu1:~ # ifconfig eth1.3 192.168.3.103 netmask 255.255.255.0
lnxsu1:~ # ifconfig eth1.3
eth1.3    Link encap:Ethernet  HWaddr 02:00:00:00:00:72
          inet addr:192.168.3.103  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::ff:fe00:7a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1492  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:328 (328.0 b)
```

Example 11-21 Red Hat defining VLAN ID 3 on Interface eth1

```
[root@lnxrh1 ~]# vconfig add eth1 3
Added VLAN with VID == 3 to IF -:eth1:-
[root@lnxrh1 ~]# ifconfig eth1.3 192.168.3.113 netmask 255.255.255.0
[root@lnxrh1 ~]# ifconfig eth1.3
eth1.3    Link encap:Ethernet  HWaddr 02:00:00:00:00:74
          inet addr:192.168.3.113  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::ff:fe00:74/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1492  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:956 (956.0 b)
```

After defining a VLAN interface, for example VLAN `3`, the name of the interface for SLES 11 and RHEL 6 is `eth1.3`.

Permanent definitions for VLAN support: SUSE Linux

To make all of the definitions from 11.4.3, “Add VLANs to the guest systems” on page 131 permanent, you need to code the information in the distribution-specific configuration member.

To create the VLAN definition member for the VLAN ID, copy one of the QDIO Ethernet definition files, and name the new member `ifcfg-ethx`, concatenated with the VLAN ID. Remove definitions from the file that relate to hardware, keeping only the statements that are network-related (see Example 11-22). Add your network definitions and the `ETHERDEVICE=’`*`interface name`*`’` statement to the file. The `ETHERDEVICE` statement links the definition file to the actual network interface.

Example 11-22 SUSE member /etc/sysconfig/network/ifcfg-eth1.3

```
ETHERDEVICE='eth1'
BOOTPROTO='static'
STARTMODE='auto'
IPADDR='192.168.3.103'
NETMASK='255.255.255.0'
NETWORK='192.168.3.0'
BROADCAST='192.168.3.255'
PREFIXLEN=''
```

Permanent definitions for VLAN support: Red Hat Linux

To make all of the definitions from 11.4.3, “Add VLANs to the guest systems” on page 131 permanent, you need to code the information in the distribution-specific configuration member.

To create the VLAN definition member for the VLAN ID, copy one of the QDIO Ethernet definition files and name the new member `ifcfg-ethx`, concatenated with the VLAN ID. Remove definitions from the file that relate to hardware, keeping only the statements that are network-related (Example 11-23). Add your network definitions, the `DEVICE=’`*`interface name`*`’` statement, and `VLAN=yes` to the file. The `DEVICE` statement links this definition file to the actual network interface.

Example 11-23 Red Hat member /etc/sysconfig/network-scripts/ifcfg-eth1.3

```
# Please read /usr/share/doc/initscripts-*/sysconfig.txt
# for the documentation of these parameters.
TYPE=Ethernet
DEVICE=eth1.3
VLAN=yes
BOOTPROTO=none
NETMASK=255.255.255.0
IPADDR=192.168.3.113
ONBOOT=yes
USERCTL=no
IPV6INIT=no
PEERDNS=yes
NETTYPE=qeth
```

11.4.4 Add VLAN support to the z/OS TCP/IP stacks

To enable VLAN support for the z/OS TCP/IP stacks, we add the VLAN ID parameter to the LINK statements in the PROFILE member for the OSA port. Example 11-24 shows the configuration that we used to define the VLANs in the z/OS environment.

Example 11-24 z/OS TCPI/IP VLAN configuration

```
z/OS LPAR (SC30):

DEVICE OSA20C0  MPCIPA   ; OSD Devices on CHPID 04
LINK   OSA20C0LNK  IPAQENET OSA20C0  VLANID 3

DEVICE OSA20C6  MPCIPA  ; OSD Devices on CHIPD 04
LINK   OSA20C6LNK  IPAQENET OSA20C6 VLANID 5

DEVICE OSA2160  MPCIPA  ; OSD Devices on CHPID 07
LINK   OSA2160LNK  IPAQENET OSA2160  VLANID 6
```

11.4.5 Configure trunk mode in the Ethernet switch for the OSA connections

In the Ethernet switch, we defined trunk mode for port 2/7, which was directly connected to the OSA port (CHPID 04) on the z/VM LPAR (Example 11-25). Port 1/2 was connected to the OSA port (CHPID 04) on the z/OS LPAR, which was previously set to trunk mode.

Example 11-25 Ethernet switch configuration

```
SET TRUNK 2/7 ON DOT1Q 1-2005,1025-4094
```

Important: In a production environment, multiple OSA ports should be connected to at least two different Ethernet switches to avoid single points of failure.

11.4.6 Verify the VLAN

After completing the configuration tasks, we verified the VLAN environment.

We checked the virtual switch to see the list of authorized user IDs. In Example 11-26 on page 135, notice the VLAN-specific information that is displayed.

Example 11-26 Authorized user IDs for virtual switch

```
QUERY VSWITCH L2VSW1 ACC
VSWITCH SYSTEM L2VSW1   Type: QDIO    Connected: 2    Maxconn: INFINITE
  PERSISTENT  RESTRICTED    ETHERNET                  Accounting: OFF
  USERBASED
  VLAN Aware  Default VLAN: 0003    Default Porttype: Trunk   GVRP: Enabled
              Native  VLAN: 0001    VLAN Counters: OFF
  MAC address: 02-00-00-00-00-76    MAC Protection: Unspecified
  IPTimeout: 5         QueueStorage: 8
  Isolation Status: OFF        VEPA Status: OFF
  Authorized userids:
      LNXRH1   Porttype: Trunk  VLAN: 0003-0006
      LNXSU1   Porttype: Trunk  VLAN: 0003-0006
      TCPIP2   Porttype: Trunk  VLAN: 0003
 Uplink Port:
  State: Ready
  PMTUD setting: EXTERNAL   PMTUD value: 8992
  RDEV: 20C0.P00 VDEV: 0636 Controller: DTCVSW1  ACTIVE
  RDEV: 2043.P00 VDEV: 0630 Controller: DTCVSW2  BACKUP
```

Next, we displayed the virtual switch to verify that our new VLAN information was defined correctly (see Example 11-27). Notice the VLAN and the Porttype information. Toward the bottom of the display under the Adapter Owner sections, the Linux guests now show a `Trunk` port type.

Example 11-27 Virtual switch display with VLAN capability

```
QUERY VSWITCH L2VSW1 DET
VSWITCH SYSTEM L2VSW1   Type: QDIO    Connected: 2    Maxconn: INFINITE
  PERSISTENT  RESTRICTED    ETHERNET                  Accounting: OFF
  USERBASED
  VLAN Aware  Default VLAN: 0003    Default Porttype: Trunk   GVRP: Enabled
              Native  VLAN: 0001    VLAN Counters: OFF
  MAC address: 02-00-00-00-00-76    MAC Protection: Unspecified
  IPTimeout: 5         QueueStorage: 8
  Isolation Status: OFF        VEPA Status: OFF
 Uplink Port:
  State: Ready
  PMTUD setting: EXTERNAL   PMTUD value: 8992
  RDEV: 20C0.P00 VDEV: 0636 Controller: DTCVSW1  ACTIVE
    Uplink Port Connection:
      RX Packets: 0         Discarded: 0          Errors: 0
      TX Packets: 75        Discarded: 0          Errors: 0
      RX Bytes: 0                    TX Bytes: 6442
      Device: 0636  Unit: 000   Role: DATA       Port: 2049
      Partner Switch Capabilities: No_Reflective_Relay
  RDEV: 2043.P00 VDEV: 0630 Controller: DTCVSW2  BACKUP
 Adapter Connections:                            Connected: 2
    Adapter Owner: LNXRH1   NIC: 8000.P00 Name: UNASSIGNED  Type: QDIO
      Porttype: Trunk
      RX Packets: 0         Discarded: 0          Errors: 0
      TX Packets: 21        Discarded: 0          Errors: 14
      RX Bytes: 0                    TX Bytes: 1542
      Device: 8002  Unit: 002   Role: DATA       Port: 0002
      VLAN: 0003 0005 0006
      Options: Ethernet Broadcast
        Unicast MAC Addresses:
          02-00-00-00-00-74
        Multicast MAC Addresses:
          01-00-5E-00-00-01
          01-80-C2-00-00-21
          33-33-00-00-00-01
          33-33-00-00-02-02
          33-33-FF-00-00-74
    Adapter Owner: LNXSU1   NIC: 8000.P00 Name: UNASSIGNED  Type: QDIO
      Porttype: Trunk
      RX Packets: 6         Discarded: 0          Errors: 0
      TX Packets: 18        Discarded: 0          Errors: 18
      RX Bytes: 276                 TX Bytes: 1476
      Device: 8002  Unit: 002   Role: DATA       Port: 0001
      VLAN: 0003 0005 0006
      Options: Ethernet Broadcast
        Unicast MAC Addresses:
          02-00-00-00-00-72
        Multicast MAC Addresses:
          01-00-5E-00-00-01
          01-80-C2-00-00-21
          33-33-00-00-00-01
          33-33-FF-00-00-72
```

We looked at the interface configuration for LNXSU1 and LNXRH1, respectively. The changes in these displays are the absence of IP addresses on the eth1 interface. Only the VLAN interfaces (subinterfaces) are associated with a valid IP address. The VLAN interfaces (IDs) use the real interface (eth1) to communicate with the LAN over the virtual switch. During this process, the eth1 interface adopts the IP address of the VLAN interface to establish connectivity to the virtual switch and beyond.

The configurations were displayed on the Linux guests with the **ifconfig** command. Example 11-28 shows the results for LNXSU1.

Example 11-28 Interface display for LNXSU1

```
lnxsu1:/ # ifconfig
eth1.3    Link encap:Ethernet  HWaddr 02:00:00:00:00:72
          inet addr:192.168.3.103  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::ff:fe00:7a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1492  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:468 (468.0 b)
```

We then issued **ping** commands from LNXSU1 and LNXRH1 to the IP addresses assigned to the appropriate VLAN IDs for the z/OS LPAR. In all cases, we received a positive response, which indicates a working infrastructure between the systems.

Lastly, we tried to ping the IP addresses that were not defined to the individual VLANs and vice versa. As expected, they were unsuccessful, verifying the intended isolation of the environment.

11.5 Enabling port isolation

Port isolation prevents guest systems from sending data to other guests on the same virtual switch. Packets that are destined for another guest port on the VSWITCH are discarded. In addition, no direct LPAR-to-LPAR communication over a shared OSA port is permitted with guest ports on the VSWITCH. This is a very important security option; it forces all IP traffic to pass through a connected OSA port to the external LAN environment. After reaching an external Ethernet switch, packet filtering or other security-related actions can take place.

Port isolation works with a VSWITCH that is either in IP mode (Layer 3) or Ethernet mode (Layer 2). If a VSWITCH has isolation set to *on*, guest systems that have a NIC connected to it cannot exchange data with each other. That is also true for two or more VSWITCHs with isolation set on that are sharing OSA port or ports.

In this section, we verified that the following actions occur when VSWITCH port isolation is set to *on*:

1. Packets between guest systems that are attached to the VSWITCH are dropped.
2. Packets that are destined for the VSWITCH guest ports from any LPAR that is sharing the connected OSA ports are dropped.
3. Packets from the VSWITCH that are destined for any LPAR that is sharing the connected OSA ports are dropped.

Figure 11-7 depicts the environment that we used to verify port isolation. Our VSWITCH is VLAN-aware only because we specified VLANs in our TCP/IP stacks, but this is not a prerequisite. We also added IP routing to our external Ethernet switch to allow connectivity between the VLANs.

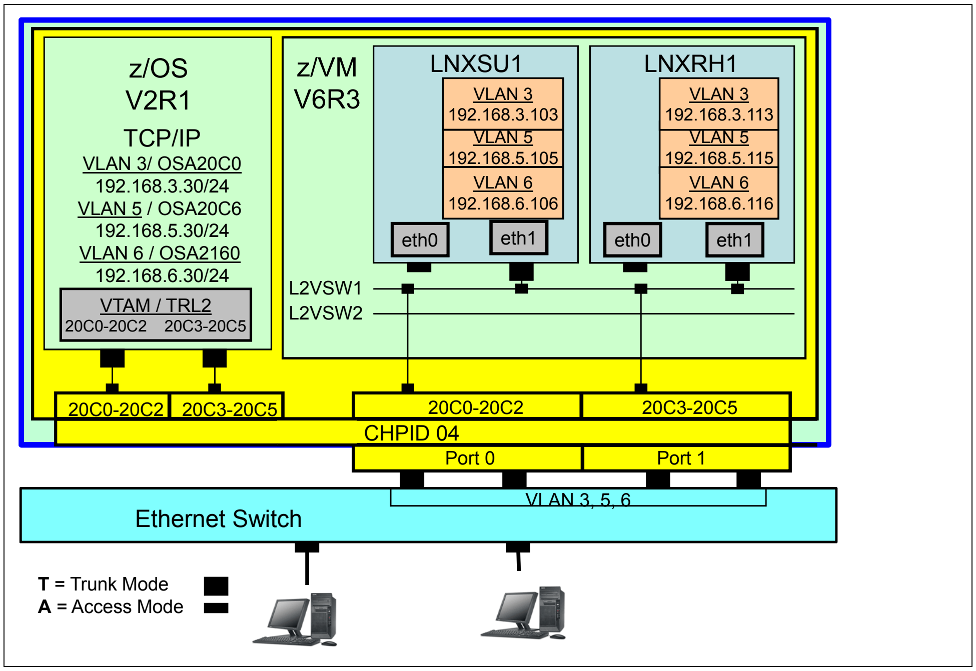


Figure 11-7 Our VSWITCH environment with port isolation

Important: To provide support for VSWITCH port isolation, you can check the appropriate PSP bucket for your environment. See PSP Buckets - How to find them on Web:

http://www.ibm.com/support/docview.wss?uid=swg21201593

All of the definitions for this environment are described in 11.3, “Configuring a Layer 2 VSWITCH” on page 118 and 11.4, “Configuring VLAN support” on page 128.

New feature for port isolation: See 11.6, “VEPA mode” on page 139 for more about the new feature called Virtual Ethernet Port Aggregator (VEPA).

11.5.1 Port isolation *off*, systems sharing VSWITCH and OSA

Example 11-29 shows a query of virtual switch L2VSW1 with port isolation set to *off* (default). LNXSU1 and LNXRH1 were sharing L2VSW1, which was connected to an OSA port.

The **SET VSWITCH L2VSW1 ISOL OFF** command can be used to disable port isolation.

Example 11-29 Query L2VSW1 - VSWITCH with port isolation off

```
QUERY VSWITCH L2VSW1 DET
VSWITCH SYSTEM L2VSW1   Type: QDIO    Connected: 2    Maxconn: INFINITE
  PERSISTENT  RESTRICTED    ETHERNET                  Accounting: OFF
  USERBASED
  VLAN Aware  Default VLAN: 0003    Default Porttype: Trunk    GVRP: Enabled
              Native  VLAN: 0001    VLAN Counters: OFF
  MAC address: 02-00-00-00-00-76    MAC Protection: Unspecified
  IPTimeout: 5         QueueStorage: 8
  Isolation Status: OFF        VEPA Status: OFF
```

We used the **ping** command to verify connectivity between the z/OS LPAR, LNXSU1, and LNXRH1 (by using the virtual switch). All pings were successful, as expected.

11.5.2 Port isolation *on*, systems sharing VSWITCH and OSA

Example 11-30 shows a query of virtual switch L2VSW1 with port isolation set to *on*. LNXSU1 and LNXRH1 were sharing L2VSW1, which was connected to an OSA port. The OSA port was also shared by a z/OS LPAR. We used the **SET VSWITCH L2VSW1 ISOL ON** command to enable port isolation on L2VSW1.

Example 11-30 Query L2VSW1 - VSWITCH with port isolation on

```
QUERY VSWITCH L2VSW1 DET
VSWITCH SYSTEM L2VSW1   Type: QDIO    Connected: 2    Maxconn: INFINITE
  PERSISTENT  RESTRICTED    ETHERNET                  Accounting: OFF
  USERBASED
  VLAN Aware  Default VLAN: 0003    Default Porttype: Trunk    GVRP: Enabled
              Native  VLAN: 0001    VLAN Counters: OFF
  MAC address: 02-00-00-00-00-76    MAC Protection: Unspecified
  IPTimeout: 5         QueueStorage: 8
  Isolation Status: ON VEPA Status: OFF
```

We used the **ping** command to test connectivity between the z/OS LPAR, LNXSU1, and LNXRH1 through the virtual switch. As expected, all pings failed.

11.6 VEPA mode

The Virtual Ethernet Port Aggregator (VEPA) is part of the IEEE 802.1Qbg standard to reduce the complexities that are associated with highly virtualized deployments, such as hypervisor virtual switches that bridge many virtual machines. VEPA can take all virtual machine traffic that is sent by the server and send it to an adjacent network switch. This mode of operation moves all frame relay-switching from the hypervisor virtual switch to the (external) adjacent switch. With the adjacent switch handling the frame relay for VSWITCH guest port-to-guest port communications, embedded network-based appliances in the adjacent switch such as firewalls, access control lists (ACLs), quality of service (QoS), and port mirroring, are available to be deployed for this guest port-to-reflective relay guest port switching.

VEPA eliminates the need to provide and support these network-based appliances in the hypervisors and LPARs. The IEEE 802.1Qbg standard includes a way for an adjacent (Layer 2) switch to support a VEPA mode with a virtual switch through a *reflective relay* (also known as a *hairpin turn*). This enables packets that are received on the switch port to be “reflected” back on the same switch port.

The `VEPA ON` option in the **SET VSWITCH** command can be used to place the virtual switch into VEPA mode. Similar to `ISOLATION ON`, VEPA mode affects all internal guest-to-guest communications (unicast, broadcast, and multicast traffic), along with the virtual switch’s Uplink RDEV data connection. Figure 11-8 illustrates a VEPA environment.

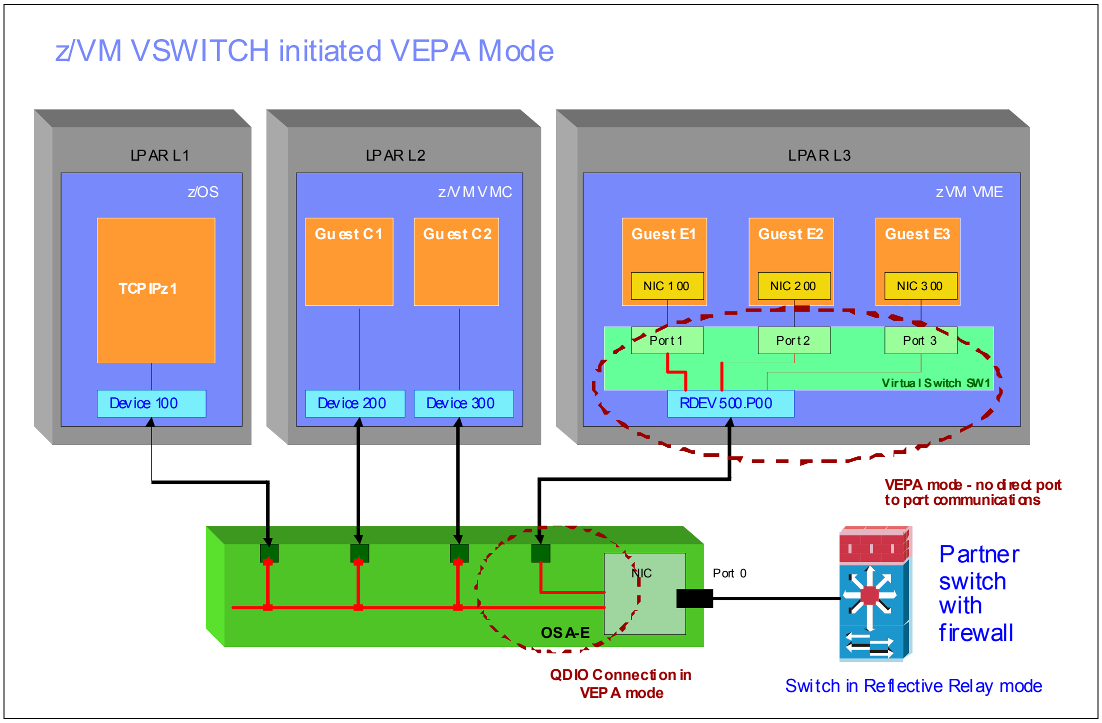


Figure 11-8 z/VM VSWITCH-initiated VEPA mode

In VEPA mode, there are no direct communications between guests that are coupled to the VSWITCH (E1, E2, E3). All communication is forwarded to the partner switch. Also, there are no direct communications between sharing connections on the OSA feature and the

VSWITCH Uplink RDEV. All direct communications from and to the VSWITCH Uplink connection are sent to the partner switch. In each of these cases, the partner switch determines whether the frames are sent back for delivery to the destination through the reflective relay capability.

VEPA ON requires an Ethernet virtual switch (without a Bridge port) with OSA uplinks that support VEPA, and the partner switch must support reflective relay.

11.6.1 Promiscuous mode

Promiscuous mode (passing on all traffic received) on an individual guest system is not affected by the virtual switch isolation or VEPA modes. Promiscuous guests still receive a copy of the guest-to-guest internal traffic when the virtual switch is operating in either of the two isolation modes.

11.6.2 Link aggregation

A virtual switch that is operating with a Link Aggregation group already has segregated RDEV QDIO connections. Each RDEV in the port group is a connected to an OSA port that is in exclusive use mode. An OSA port operating in this mode has no other LPARs or hosts that are sharing the OSA port. Essentially, the virtual switch has exclusive use of the OSA port.

If guest port isolation is also required, you must use the **SET VSWITCH ISOLATION ON** command. This command does not attempt to isolate the RDEV connections within the port group, but it ensures that the backup RDEV connection is isolated when it is activated during a failover incident. Similarly, **SET VSWITCH VEPA ON** must be configured if policy enforcement is to be provided by the physical switch.

A

Open Systems Adapter-Express features by version

This appendix lists the OSA-Express5S and OSA-Express4S features that are available on these mainframe systems:

- IBM zEnterprise System BC12 (zBC12), Business Class
- IBM zEnterprise System EC 12 (zEC12), Enterprise Class
- IBM zEnterprise System 114 (z114)
- IBM zEnterprise System 195 (z196)

The information covers the following versions:

- “OSA-Express5S 1000BASE-T Ethernet features” on page 143
- “OSA-Express5S 10-Gigabit Ethernet Long Reach (10GbE LR) features” on page 144
- “OSA-Express5S 10 Gigabit Ethernet Short Reach (10GbE SR) features” on page 145
- “OSA-Express5S Gigabit Ethernet long wavelength (GbE LX) features” on page 145
- “OSA-Express5S Gigabit Ethernet short wavelength (GbE SX) features” on page 146
- “OSA-Express4S 1000BASE-T Ethernet features” on page 147
- “OSA-Express4S 10 Gigabit Ethernet Long Reach (10GbE LR) features” on page 148
- “OSA-Express4S 10 Gigabit Ethernet Short Reach (10GbE SR) features” on page 148
- “OSA-Express4S Gigabit Ethernet long wavelength (GbE LX) features” on page 149
- “OSA-Express4S Gigabit Ethernet short wavelength (GbE SX) features” on page 149

OSA-Express feature descriptions by version

Table A-1 lists the OSA-Express5S and OSA-Express4S (OSA) features that are supported on System z systems, along with the maximum number of OSA ports that each system supports. For all optical links, the connector type is LC duplex unless otherwise specified. The electrical Ethernet cable for OSA connectivity has an RJ 45 jack. Subsequent sections list details about each feature that is supported on zEC12, zBC12, z196, and z114 systems.

Table A-1 System z OSA features

Feature name	Feature code	Cable type	Maximum unrepeated distance[a]	System
OSA-Express5S GbE LX	0413	SM 9 µm	5 km	zEC12, zBC12
		MCP[b]	550 m (500)	
OSA-Express5S GbE SX	0414	MM 50 µm	550 m (500)	zEC12, zBC12
		MM 62.5 µm	220 m (166) 275 m (200)	
OSA-Express5S 10GbE LR	0415	SM 9 µm	10 km	zEC12, zBC12
OSA-Express5S 10GbE SR	0416	MM 50 µm	550 m (500)	zEC12, zBC12
		MM 62.5 µm	220 m (166) 275 m (200)	
OSA-Express5S 1000BASE-T	0417	UTP Cat5 or 6	100 m	zEC12, zBC12
OSA-Express4S GbE LX	0404	SM 9 µm	5 km	zEC12, z196, z114
		MCP[b]	550 m (500)	
OSA-Express4S GbE SX	0405	MM 50 µm	550 m (500)	zEC12, z196, z114
		MM 62.5 µm	275 m (200) 220 m (160)	
OSA-Express4S 10GbE LR	0406	SM 9 µm	10 km	zEC12, z196, z114
OSA-Express4S 10GbE SR	0407	MM 50 µm	300 m (2000) 82 m (500)	zEC12, z196, z114
		MM 62.5 µm	33 m (200)	
OSA-Express4S 1000BASE-T	0408	UTP Cat5 or 6	100 m	zEC12

a. Minimum fiber bandwidths in MHz/km for multimode fiber optic links are included in parentheses, where applicable.

b. MCP cables enable the 1 Gbps single mode features to connect to multimode fiber.

Important: On a zEC12 system, the maximum number of OSA-Express3 and OSA-Express4S cards depends on the mix of those cards. The maximum number of OSA-Express3 cards is 24 (carry forward only). The maximum number of OSA-Express4S cards alone is 48 cards. The maximum number of OSA-Express3 and OSA-Express4S that are mixed is determined based on a maximum of 48 PCHIDs.

On a zBC12 system, the maximum OSA-Express3 features is 8 (carry forward only), or 16 with RPQ 8P2733 for second I/O drawer (carry forward only). The maximum OSA-Express4S (carry forward only) and OSA-Express5S features is 48

Table A-2 shows the numbers of I/O features that are supported on zEC12 systems.

Table A-2 zEC12 supported I/O features

I/O feature	Ports per feature	Ports per CHPID	Max.number[a] of		CHPID definition
			Ports	I/O slots	
OSA-Express3 10GbE LR/SR	2	1	48	24	OSD, OSX
OSA-Express3 GbE LX/SX	4	2	96	24	OSD, OSN
OSA-Express3 1000BASE-T	4	2	96	24	OSE, OSD, OSC, OSN, OSM
OSA-Express4S GbE LX/SX	2	2	96	48	OSD
OSA-Express4S 10GbE LR/SR	1	1	48	48	OSD, OSX
OSA-Express4S 1000BASE-T	2	2	96	48	OSE, OSD, OSC, OSN, OSM
OSA-Express5S 10GbE LR/SR	1	1	48	48	OSD, OSX
OSA-Express5S GbE LX/SX	2	2	96	48	OSD
OSA-Express5S 1000BASE-T	2	2	96	48	OSE, OSD, OSC, OSN, OSM

[a] The maximum number of OSA-Express3 and OSA-Express4S features that are mixed is determined based on a maximum of 48 PCHIDs.

OSA-Express5S 1000BASE-T Ethernet features

Feature code 0417 is exclusive to the zEC12 and zBC12 and can be installed only in the Peripheral Component Interconnect Express (PCIe) I/O drawer. It occupies one slot in the PCIe I/O drawer and has two ports that connect to a 1000-Mbps (1 Gbps) or 100-Mbps Ethernet LAN. Each port has a Small Form Factor Pluggable (SFP) transceiver with an RJ-45 receptacle for cabling to an Ethernet switch. The SFP allows a concurrent repair or replace action on each SFP. The RJ-45 receptacle must be attached by using EIA/TIA category 5 or 6 unshielded twisted pair (UTP) cable with a maximum length of 100 meters (328 feet).

The two ports of the OSA-Express5S 1000BASE-T feature have one CHPID assigned, so the two ports share one CHPID number. Use of both ports on a two-port CHPID requires operating system support.

The OSA-Express5S 1000BASE-T Ethernet feature supports auto-negotiation when it is attached to an Ethernet router or switch. If you allow the LAN speed to default to auto-negotiation, the OSA port and the attached router or switch auto-negotiate the LAN speed between them and connect at the highest common performance speed of interoperation. If the attached Ethernet router or switch does not support auto-negotiation, the OSA port examines the signal that it is receiving and connects at the speed and full-duplex mode of the device at the other end of the cable.

You can choose either of these settings for the OSA-Express5S 1000BASE-T Ethernet feature port:

- Auto-negotiate
- 100 Mbps full-duplex

If you are not using auto-negotiate, the OSA port attempts to join the LAN at the specified speed. If this does not match the speed and duplex mode of the signal on the cable, the OSA port does not connect.

LAN speed can be set by using the OSA Advanced Facilities function of the Hardware Management Console (HMC). The explicit settings override the OSA feature port's ability to auto-negotiate with its attached Ethernet switch.

Each OSA-Express5S 1000BASE-T CHPID can be defined as CHPID types OSD, OSE, OSC, OSN, or OSM. See 1.1.1, "Operating modes" on page 3, for details about modes of operation and supported traffic types. The following Ethernet standards are applicable for this feature:

- 1000BASE-TX (standard transmission scheme)
  - IEEE 802.3u
- 1000BASE-T (standard transmission scheme)
  - IEEE 802.1p
  - IEEE 802.1q
  - IEEE 802.3ab
  - IEEE 802.3ac
  - IEEE 802.3u
  - IEEE 802.3x
  - DIX Version 2

Statement of direction: The zEC12 and zBC12 are planned to be the last System z servers to support IEEE 802.3 Ethernet frame types. All OSA-Express features on future System z servers are planned to support DIX Version 2 (V2) exclusively.

OSA-Express5S 10-Gigabit Ethernet Long Reach (10GbE LR) features

Feature code 0415 is supported on the zEC12 and zBC12 and can be installed only in the PCIe I/O drawer. It occupies one slot and has one port with a SFP transceiver and an LC duplex receptacle that connects to a 10 Gbps Ethernet LAN over a 9-micron single mode fiber optic cable that terminates with an *LC duplex* connector. It supports an unrepeated maximum distance of 10 km (6.2 miles). The SFP allows a concurrent repair or replace action.

The OSA-Express5S 10GbE LR feature does not support auto-negotiation to any other speed and runs in full duplex mode only. OSA-Express5S 10GbE LR supports 64B/66B encoding, whereas GbE supports 8B/10 encoding, making auto-negotiation to any other speed impossible.

The one port of the OSA-Express5S 10GbE LR feature has one CHPID assigned and can be defined as type OSD or OSX. See 1.1.1, “Operating modes” on page 3, for details about modes of operation and supported traffic types.

The following Ethernet standards are applicable for the 10GBASE-LR (standard transmission scheme) feature:

- IEEE 802.3ae
- IEEE 802.1q
- IEEE 802.3x - flow control
- DIX Version 2

Statement of direction: The zEC12 and zBC12 are planned to be the last System z servers to support IEEE 802.3 Ethernet frame types. All OSA-Express features on future System z servers are planned to support DIX Version 2 (V2) exclusively.

OSA-Express5S 10 Gigabit Ethernet Short Reach (10GbE SR) features

Feature code 0416 is supported on the zEC12 and zBC12 and can be installed only in the PCIe I/O drawer. It occupies one slot and has one port with an SFP transceiver and an LC duplex receptacle that connects to a 10 Gbps Ethernet LAN over a 62.5-micron or 50-micron multimode fiber optic cable that terminates with an LC duplex connector. The maximum supported unrepeated distance is 33 meters (108 feet) on a 62.5-micron multimode (200 MHz) fiber optic cable, 82 meters (269 feet) on a 50-micron multimode (500 MHz) fiber optic cable, and 300 meters (984 feet) on a 50-micron multimode (2000 MHz) fiber optic cable. The SFP allows a concurrent repair or replace action.

The OSA-Express5S 10GbE SR feature does not support auto-negotiation to any other speed and runs in full duplex mode only. OSA-Express5S 10GbE SR supports 64B/66B encoding, whereas GbE supports 8B/10 encoding, making auto-negotiation to any other speed impossible.

The one port of the OSA-Express5S 10GbE SR feature has one CHPID assigned and can be defined as type OSD or OSX. See 1.1.1, “Operating modes” on page 3, for details about modes of operation and supported traffic types.

The following Ethernet standards are applicable for the 10GBASE-SR (standard transmission scheme) feature:

- IEEE 802.3ae
- IEEE 802.1q
- IEEE 802.3x - flow control
- DIX Version 2

Statement of direction: The zEC12 and zBC12 are planned to be the last System z servers to support IEEE 802.3 Ethernet frame types. All OSA-Express features on future System z servers are planned to support DIX Version 2 (V2) exclusively.

OSA-Express5S Gigabit Ethernet long wavelength (GbE LX) features

Feature code 0413 is supported on the zEC12 and zBC12 and can be installed only in the PCIe I/O drawer. It occupies one slot and has two ports with an SFP transceiver and an LC duplex receptacle that connect to a 1 Gbps Ethernet LAN over a 9-micron single mode fiber optic cable that terminates with an LC duplex connector. It supports an unrepeated maximum distance of 5 km (3.1 miles). A multimode (62.5 or 50 micron) fiber optic cable can be used with these features. Use of these multimode cable types requires a mode-conditioning patch (MCP) cable at each end of the fiber optic link (see the “Mode-conditioning patch cables” table in Appendix B of the *IBM System z Connectivity Handbook*, SG24-5444). Use of the single mode to multimode MCP cables reduces the supported distance of the link to a maximum of 550 meters (1084 feet). The SFP allows a concurrent repair or replace action.

The two ports of the OSA-Express5S GbE LX (long range) feature share a channel path identifier (CHPID type OSD, exclusively). The use of both ports on a two-port CHPID requires support by the operating system. See 1.1.1, “Operating modes” on page 3, for details about modes of operation and supported traffic types.

The OSA-Express5S GbE LX feature does not support auto-negotiation to any other speed and runs in full duplex mode only

The following Ethernet standards are applicable for the 1000BASE-LX (standard transmission scheme) feature:

- IEEE 802.3ac
- IEEE 802.1q
- IEEE 802.3x
- IEEE 802.3z
- DIX Version 2

> **Statement of direction:** The zEC12 and zBC12 are planned to be the last System z servers to support IEEE 802.3 Ethernet frame types. All OSA-Express features on future System z servers are planned to support DIX Version 2 (V2) exclusively.

OSA-Express5S Gigabit Ethernet short wavelength (GbE SX) features

Feature code 0414 is supported on the zEC12 and zBC12 systems and can be installed only in the PCIe I/O drawer. It occupies one slot and has two ports with an SFP transceiver and an LC duplex receptacle that connect to a-1 Gbps Ethernet LAN over a 50-micron or 62.5-micron multimode fiber optic cable that terminates with an LC duplex connector over an unrepeated distance of 550 meters (for 50 µm fiber) or 220 meters (for 62.5 µm fiber). The SFP allows a concurrent repair or replace action.

The two ports of the OSA-Express5S GbE SX feature share a channel path identifier (CHPID type OSD exclusively). The use of both ports on a two-port CHPID requires support by the operating system. See 1.1.1, “Operating modes” on page 3, for details about modes of operation and supported traffic types.

The OSA-Express5S GbE SX feature does not support auto-negotiation to any other speed and runs in full duplex mode only.

The following Ethernet standards are applicable for the 1000BASE-SX (standard transmission scheme) feature:

- IEEE 802.3ac
- IEEE 802.1q
- IEEE 802.3x
- IEEE 802.3z
- DIX Version 2

Statement of direction: The zEC12 and zBC12 are planned to be the last System z servers to support IEEE 802.3 Ethernet frame types. All OSA-Express features on future System z servers are planned to support DIX Version 2 (V2) exclusively.

OSA-Express4S 1000BASE-T Ethernet features

Feature code 0408 is exclusive to the zEC12 and can be installed only in the PCIe I/O drawer. It occupies one slot in the PCIe I/O drawer and has two ports that connect to a 1000 Mbps (1 Gbps) or 100 Mbps Ethernet LAN. Each port has an RJ-45 receptacle for cabling to an Ethernet switch. The RJ-45 receptacle must be attached by using EIA/TIA category 5 or 6 unshielded twisted pair (UTP) cable with a maximum length of 100 meters (328 feet).

The two ports of the OSA-Express4S 1000BASE-T feature have one CHPID assigned, so the two ports share one CHPID number. The use of both ports on a two-port CHPID requires support by the operating system.

The OSA-Express4S 1000BASE-T Ethernet feature supports auto-negotiation when attached to an Ethernet router or switch. If you allow the LAN speed and duplex mode to default to auto-negotiation, the OSA port and the attached router or switch auto-negotiate the LAN speed and duplex mode settings between them. They connect at the highest common performance speed and duplex mode of operation. If the attached Ethernet router or switch does not support auto-negotiation, the OSA port examines the signal that it is receiving and connects at the speed and duplex mode of the device at the other end of the cable.

You can choose any one of the following settings for the OSA-Express4S 1000BASE-T Ethernet feature port:

- Auto-negotiate
- 100 Mbps half-duplex
- 100 Mbps full-duplex
- 1000 Mbps full-duplex

Statement of direction: The OSA-Express4S 1000BASE-T Ethernet feature is the last copper Ethernet feature to support half- duplex operation. Any future 1000BASE-T Ethernet feature will support only full-duplex operation and auto-negotiation to 100 or 1000 Mbps exclusively.

If you are not using auto-negotiate, the OSA port attempts to join the LAN at the specified speed and duplex mode. If this does not match the speed and duplex mode of the signal on the cable, the OSA port does not connect.

LAN speed and duplex mode can be set explicitly by using OSA/SF or the OSA Advanced Facilities function of the Hardware Management Console (HMC). The explicit settings overrides the OSA feature port’s ability to auto-negotiate with its attached Ethernet switch.

Each OSA-Express4S 1000BASE-T CHPID can be defined as CHPID type OSD, OSE, OSC, OSN, or OSM. See 1.1.1, “Operating modes” on page 3, for details about modes of operation and supported traffic types. The following Ethernet standards are applicable for this feature:

- 10BASE-T (standard transmission scheme)
  - IEEE 802.2
  - IEEE 802.3
  - ISO/IEC 8802-3
  - DIX Version 2
- 1000BASE-TX (standard transmission scheme)
  - IEEE 802.3u
- 1000BASE-T (standard transmission scheme)
  - IEEE 802.1p
  - IEEE 802.1q
  - IEEE 802.3ab
  - IEEE 802.3ac
  - IEEE 802.3u
  - IEEE 802.3x

OSA-Express4S 10 Gigabit Ethernet Long Reach (10GbE LR) features

Feature code 0406 is supported on the zEnterprise CPCs and can be installed only in the PCIe I/O drawer. It occupies one slot and has one port that connects to a 10 Gbps Ethernet LAN over a 9-micron single mode fiber optic cable that terminates with an LC duplex connector and supports an unrepeated maximum distance of 10 km (6.2 miles).

The OSA-Express4S 10GbE LR feature does not support auto-negotiation to any other speed and runs in full duplex mode only. OSA-Express4S 10GbE LR supports 64B/66B encoding, whereas GbE supports 8B/10 encoding, which makes auto-negotiation to any other speed impossible.

The one port of the OSA-Express4S 10GbE LR feature has one CHPID assigned and can be defined as type OSD or OSM. See 1.1.1, “Operating modes” on page 3, for details about modes of operation and supported traffic types.

The following Ethernet standards are applicable for the 10GBASE-LR (standard transmission scheme) feature:

- IEEE 802.3ae
- IEEE 802.1q
- IEEE 802.3x - flow control
- DIX Version 2

OSA-Express4S 10 Gigabit Ethernet Short Reach (10GbE SR) features

Feature code 0407 is supported on the zEnterprise CPCs and can be installed only in the PCIe I/O drawer. It occupies one slot and has one port that connects to a 10 Gbps Ethernet LAN over a 50-micron or 62.5-micron multimode fiber optic cable that terminates with an LC duplex connector. The maximum supported unrepeated distance is 33 meters (108 feet) on a 62.5-micron multimode (200 MHz) fiber optic cable, 82 meters (269 feet) on a 50-micron multimode (500 MHz) fiber optic cable, and 300 meters (984 feet) on a 50-micron multimode (2000 MHz) fiber optic cable.

The OSA-Express4S 10GbE SR feature does not support auto-negotiation to any other speed and runs in full duplex mode only. OSA-Express4S 10GbE SR supports 64B/66B encoding, whereas GbE supports 8B/10 encoding, which makes auto-negotiation to any other speed impossible.

The one port of the OSA-Express4S 10GbE SR feature has one CHPID assigned and can be defined as type OSD or OSM. See 1.1.1, “Operating modes” on page 3, for details about modes of operation and supported traffic types. The following Ethernet standards are applicable for the 10GBASE-SR (standard transmission scheme) feature:

- IEEE 802.3ae
- IEEE 802.1q
- IEEE 802.3x - flow control
- DIX Version 2

OSA-Express4S Gigabit Ethernet long wavelength (GbE LX) features

Feature code 0404 is supported on the zEnterprise CPCs and can be installed only in the PCIe I/O drawer. It occupies one slot and has two ports that connect to a 1 Gbps Ethernet LAN over a 9-micron single mode fiber optic cable that terminates with an LC duplex connector. It supports an unrepeated maximum distance of 5 km (3.1 miles). A multimode (62.5 or 50 micron) fiber optic cable can be used with these features. Use of these multimode cable types requires an MCP cable at each end of the fiber optic link (see the “Mode-conditioning patch cables” table in Appendix B of the IBM Redbooks publication, *IBM System z Connectivity Handbook*). Use of the single mode to multimode MCP cables reduces the supported distance of the link to a maximum of 550 meters (1084 feet).

The two ports of the OSA-Express4S GbE LX feature share a channel path identifier (CHPID type OSD exclusively). The use of both ports on a two-port CHPID requires support by the operating system. See 1.1.1, “Operating modes” on page 3, for details about modes of operation and supported traffic types.

The OSA-Express4S GbE LX feature does not support auto-negotiation to any other speed and runs in full duplex mode only.

The following Ethernet standards are applicable for the 1000BASE-LX (standard transmission scheme) feature:

- IEEE 802.3ac
- IEEE 802.1q
- IEEE 802.3x
- IEEE 802.3z
- DIX Version 2

OSA-Express4S Gigabit Ethernet short wavelength (GbE SX) features

Feature code 0405 is supported on the zEnterprise CPCs and can be installed only in the PCIe I/O drawer. It occupies one slot and has two ports that connect to a 1 Gbps Ethernet LAN over a 50-micron or 62.5-micron multimode fiber optic cable that terminates with an LC duplex connector over an unrepeated distance of 550 meters (for 50 µm fiber) or 220 meters (for 62.5 µm fiber).

The two ports of the OSA-Express4S GbE SX feature share a channel path identifier (CHPID type OSD exclusively). The two ports of the OSA-Express5S 1000BASE-T feature have one CHPID assigned, so the two ports share one CHPID number. The use of both ports on a two-port CHPID requires support by the operating system. See 1.1.1, “Operating modes” on page 3, for details about modes of operation and supported traffic types.

The OSA-Express4S GbE SX feature does not support auto-negotiation to any other speed and runs in full duplex mode only.

The following Ethernet standards are applicable for the 1000BASE-SX (standard transmission scheme) feature:

- IEEE 802.3ac
- IEEE 802.1q
- IEEE 802.3x
- IEEE 802.3z
- DIX Version 2

B

Network Traffic Analyzer

The Network Traffic Analyzer (NTA) trace facility runs in IBM z/OS operating system software. It is a diagnostic method for reviewing frames that are flowing to and from an IBM Open Systems Adapter-Express (OSA) feature. You can use the NTA statement to collect frames as they enter or leave an OSA feature for an attached host.

The information covers the following topics:

- “Setting up the Network Traffic Analyzer” on page 152
- “Using the Network Traffic Analyzer feature” on page 159
- “Network Management Interface API for diagnosing problems” on page 166
- “References” on page 167

Setting up the Network Traffic Analyzer

When data problems occur in a LAN environment, multiple traces are usually required. A sniffer trace might be required to see the data as it was received from or sent to the network. An OSA hardware trace might be required if the problem is suspected in the OSA, and z/OS Communications Server traces are required to diagnose Virtual Telecommunications Access Method (VTAM) or TCP/IP problems.

To help problem diagnosis, the Network Traffic Analyzer (NTA) function provides a way to trace inbound and outbound frames for OSA-Express5S and OSA-Express4S features. The NTA trace function is controlled and formatted by the z/OS Communications Server, but data is collected in the OSA at the network port.

Note: To enable the OSA-Express Network Traffic Analyzer, you must be running at least an IBM System z10® or IBM System z9 server with OSA features in Queued Direct I/O (QDIO) mode (channel path identifier, or CHPID, type OSD). See the Preventive Service Planning (PSP) buckets for more information:

- IBM zEnterprise EC12, see 2827DEVICE (Enterprise Class) and 2828DEVICE (Business Class)
- IBM zEnterprise 196 system, see the 2817DEVICE (Enterprise Class)
- IBM zEnterprise 114 system, see the 2818DEVICE (Business Class)

This section describes the steps for setting up the Network Traffic Analyzer feature:

- Determine the microcode level for OSA/OSAExpress5S
- Define TRLE definitions
- Check TCPIP definitions
- Customize Network Traffic Analyzer (NTA)
- Define a resource profile in RACF
- Allocate a VSAM linear data set

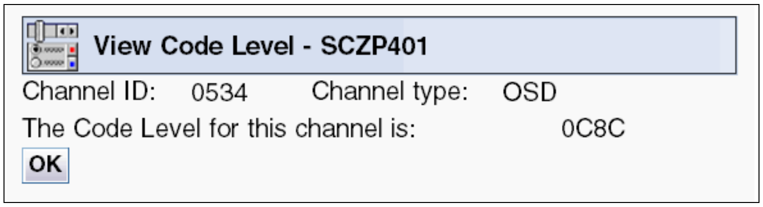
Determine the microcode level for OSA

There are many ways to determine the OSA microcode level: from the Hardware Management Console (HMC) or by issuing the `D NET,TRL,TRLE=OSA20COP` command. The two possible steps here show you how to use the VTAM TRL command in the Hardware Management Console (HMC).

From the HMC, complete these steps:

1. Select your system.
2. Double-click **OSA Advanced Facilities**.
3. Select the appropriate PCHID.
4. Select **View code leve**l.

Figure B-1 on page 153 shows the microcode level that is installed in one of our OSA-Express5 features.



View Code Level - SCZP401

Channel ID: 0534 Channel type: OSD

The Code Level for this channel is: 0C8C

Figure B-1 View code level

Or, you can issue the **D NET,TRL,TRLE=OSA20C0P** command; Example B-1 shows the output.

Example B-1 Output Display TRL

```
D NET,TRL,TRLE=OSA20C0P
IST097I DISPLAY ACCEPTED
IST075I NAME = OSA20C0P, TYPE = TRLE 727
IST1954I TRL MAJOR NODE = OSA20C0
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = LEASED            , CONTROL = MPC , HPDT = YES
IST1715I MPCLEVEL = QDIO       MPCUSAGE = SHARE
IST2263I PORTNAME = OSA20C0    PORTNUM =   0   OSA CODE LEVEL = 0C8C
IST2337I CHPID TYPE = OSD      CHPID = 04  PNETID = ITSOPNET0
IST1577I HEADER SIZE = 4096 DATA SIZE = 0 STORAGE = ***NA***
IST1221I WRITE DEV = 20C1 STATUS = ACTIVE     STATE = ONLINE
IST1577I HEADER SIZE = 4092 DATA SIZE = 0 STORAGE = ***NA***
IST1221I READ  DEV = 20C0 STATUS = ACTIVE     STATE = ONLINE
IST1221I DATA  DEV = 20C2 STATUS = ACTIVE     STATE = N/A
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST1717I ULPID = TCPIPF ULP INTERFACE = OSA20C0
```

Define TRLE definitions

Use the **D U,,,20C0,16** command to ensure that you defined enough devices. See Example B-2 on page 154.

Example B-2 Verifying the number of OSA devices

```
D U,,,20C0
IEE457I 11.31.57 UNIT STATUS 734
UNIT TYPE STATUS        VOLSER     VOLSTATE
20C0 OSA  A-BSY
20C1 OSA  A
20C2 OSA  A-BSY
20C3 OSA  O
20C4 OSA  O
20C5 OSA  O
20C6 OSA  O
20C7 OSA  O
20C8 OSA  O
20C9 OSA  O
20CA OSA  O
20CB OSA  O
20CC OSA  O
20CD OSA  O
20CE OSA  O
20CF OSAD O-RAL
```

The OSA port needs another `DATAPATH` statement on the TRL (see Example B-3).

Example B-3 TRL definition

```
OSA20C0  VBUILD TYPE=TRL
OSA20C0P TRLE  LNCTL=MPC,                                               *
               READ=20C0,                                               *
               WRITE=20C1,                                              *
               DATAPATH=(20C2-20C5),                                    *
               PORTNAME=OSA20C0,                                        *
               PORTNUM=0,                                               *
               MPCLEVEL=QDIO
```

Check TCPIP definitions

An excerpt of the TCP/IP profile, which is displayed in Example B-4, shows the information that is needed when starting the NTA trace in a later step. Keep this information handy.

Example B-4 TCP/IP definitions

```
;OSA DEFINITION
DEVICE OSA20C0  MPCIPA
LINK   OSA20C0LNK  IPAQENET      OSA20C0
HOME
   192.168.3.30 OSA20C0LNK
START OSA20C0
```

After TCP/IP is started, you can also see the OAT entries by using the HMC. See Chapter 9, “IBM z/OS virtual MAC support” on page 79 for more information.

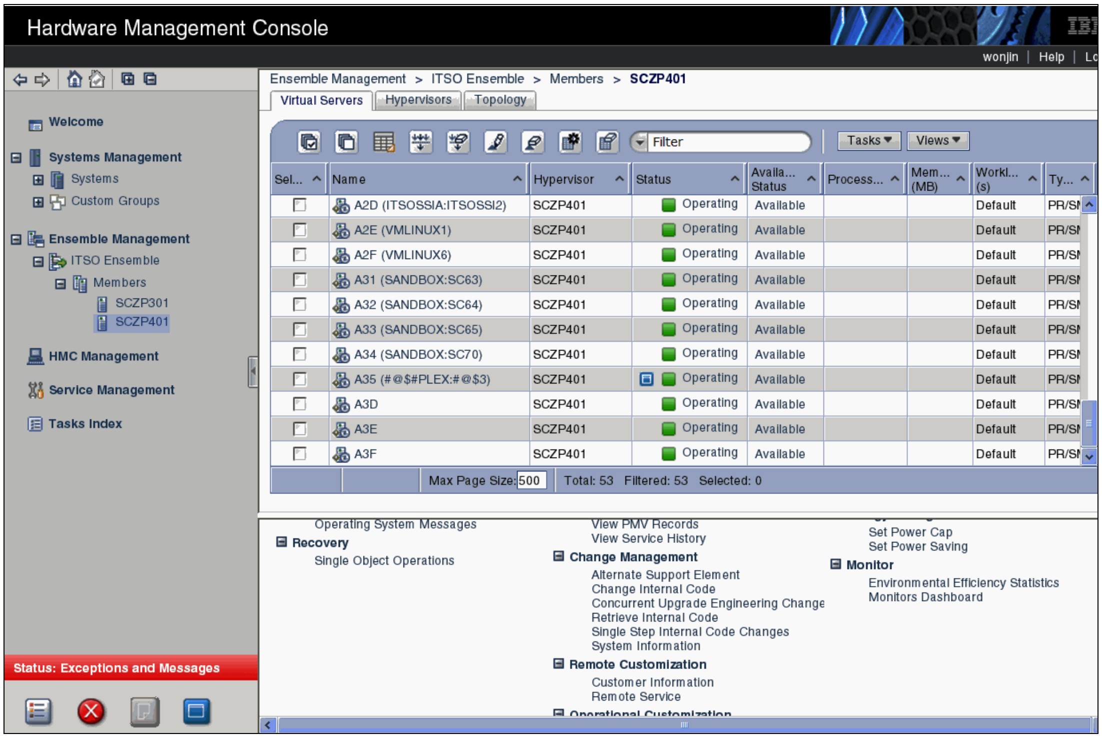
Customize Network Traffic Analyzer (NTA)

Use this task to select Network Traffic Analyzer or to check the current OSA-Express Network Traffic Analyzer authorization.

1. Log on to the Support Element (SE) on the Hardware Management Console (HMC) through Single Object Operations (SOO).

> **Important:** Enabling the NTA support could allow tracing of sensitive information. Therefore, the user ID that will handle the following steps must have the Access Administrator Tasks role assigned.

2. Select the CPC you want to work with, as shown in Figure B-2.

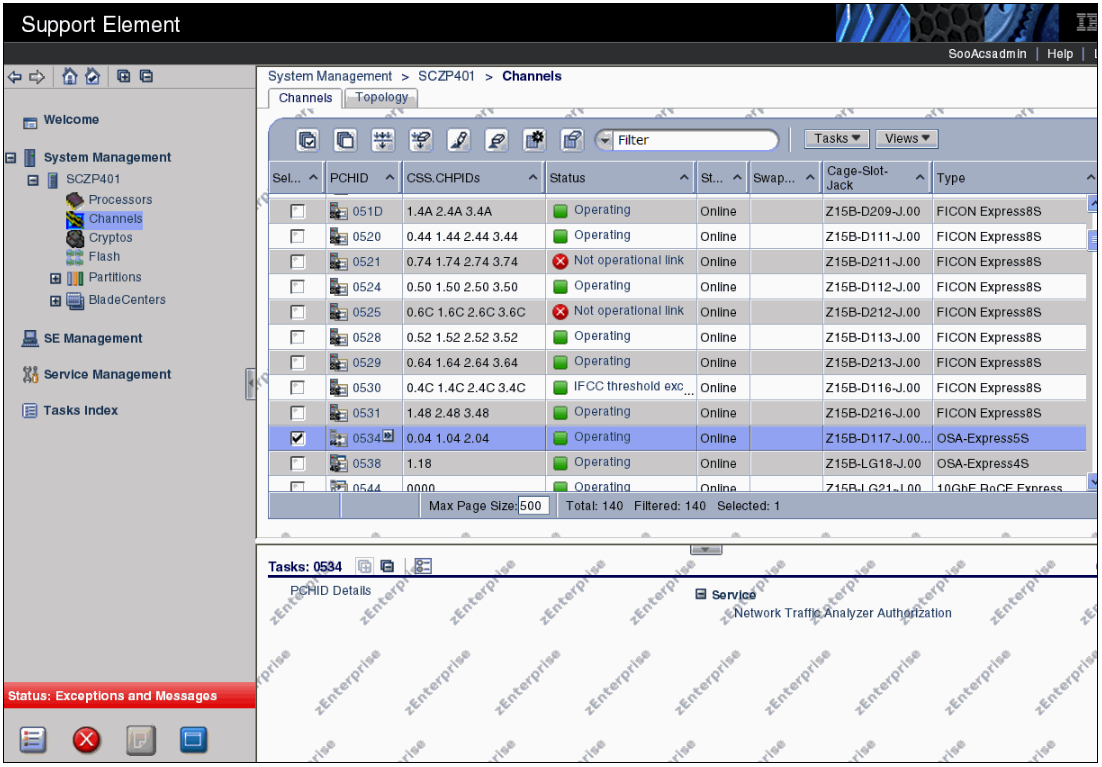


Sel...	Name	Hypervisor	Status	Availa... Status	Process...	Mem... (MB)	Workl... (s)	Ty...
□	A2D (ITSOSSIA:ITSOSSI2)	SCZP401	🟩 Operating	Available			Default	PR/SI
□	A2E (VMLINUX1)	SCZP401	🟩 Operating	Available			Default	PR/SI
□	A2F (VMLINUX6)	SCZP401	🟩 Operating	Available			Default	PR/SI
□	A31 (SANDBOX:SC63)	SCZP401	🟩 Operating	Available			Default	PR/SI
□	A32 (SANDBOX:SC64)	SCZP401	🟩 Operating	Available			Default	PR/SI
□	A33 (SANDBOX:SC65)	SCZP401	🟩 Operating	Available			Default	PR/SI
□	A34 (SANDBOX:SC70)	SCZP401	🟩 Operating	Available			Default	PR/SI
□	A35 (#@$#PLEX:#@$3)	SCZP401	🟩 Operating	Available			Default	PR/SI
□	A3D	SCZP401	🟩 Operating	Available			Default	PR/SI
□	A3E	SCZP401	🟩 Operating	Available			Default	PR/SI
□	A3F	SCZP401	🟩 Operating	Available			Default	PR/SI

Max Page Size: 500 Total: 53 Filtered: 53 Selected: 0

Figure B-2 From the HMC, log on to SE

3. Select and open the Service task list; see Figure B-3.

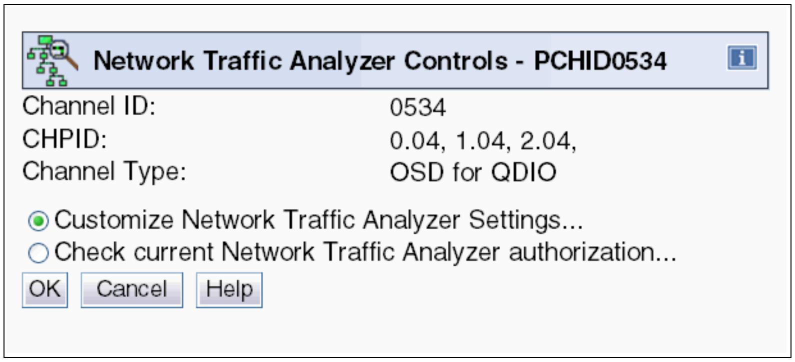


Sel...	PCHID	CSS.CHPIDs	Status	St...	Swap...	Cage-Slot-Jack	Type
□	051D	1.4A 2.4A 3.4A	🟩 Operating	Online		Z15B-D209-J.00	FICON Express8S
□	0520	0.44 1.44 2.44 3.44	🟩 Operating	Online		Z15B-D111-J.00	FICON Express8S
□	0521	0.74 1.74 2.74 3.74	☒ Not operational link	Online		Z15B-D211-J.00	FICON Express8S
□	0524	0.50 1.50 2.50 3.50	🟩 Operating	Online		Z15B-D112-J.00	FICON Express8S
□	0525	0.6C 1.6C 2.6C 3.6C	☒ Not operational link	Online		Z15B-D212-J.00	FICON Express8S
□	0528	0.52 1.52 2.52 3.52	🟩 Operating	Online		Z15B-D113-J.00	FICON Express8S
□	0529	0.64 1.64 2.64 3.64	🟩 Operating	Online		Z15B-D213-J.00	FICON Express8S
□	0530	0.4C 1.4C 2.4C 3.4C	🟩 IFCC threshold exc...	Online		Z15B-D116-J.00	FICON Express8S
□	0531	1.48 2.48 3.48	🟩 Operating	Online		Z15B-D216-J.00	FICON Express8S
☑	0534	0.04 1.04 2.04	🟩 Operating	Online		Z15B-D117-J.00...	OSA-Express5S
□	0538	1.18	🟩 Operating	Online		Z15B-LG18-J.00	OSA-Express4S
□	0544	0000	🟩 Operating	Online		Z15B-LG21-J.00	10GbE RoCE Express

Max Page Size: 500 Total: 140 Filtered: 140 Selected: 1

Figure B-3 Network Analyzer Authorization

4. Click the Network Traffic Analyzer Authorization task; see Figure B-4.



Network Traffic Analyzer Controls - PCHID0534

Channel ID: 0534
CHPID: 0.04, 1.04, 2.04,
Channel Type: OSD for QDIO

● Customize Network Traffic Analyzer Settings...
○ Check current Network Traffic Analyzer authorization...

Figure B-4 Network Traffic Analyzer controls

5. Select the control to work with:

   a. Customize Network Traffic Analyzer Settings. Allows the selection of the level of authorization for Host Network Traffic Analyze. There are three menus to work with:

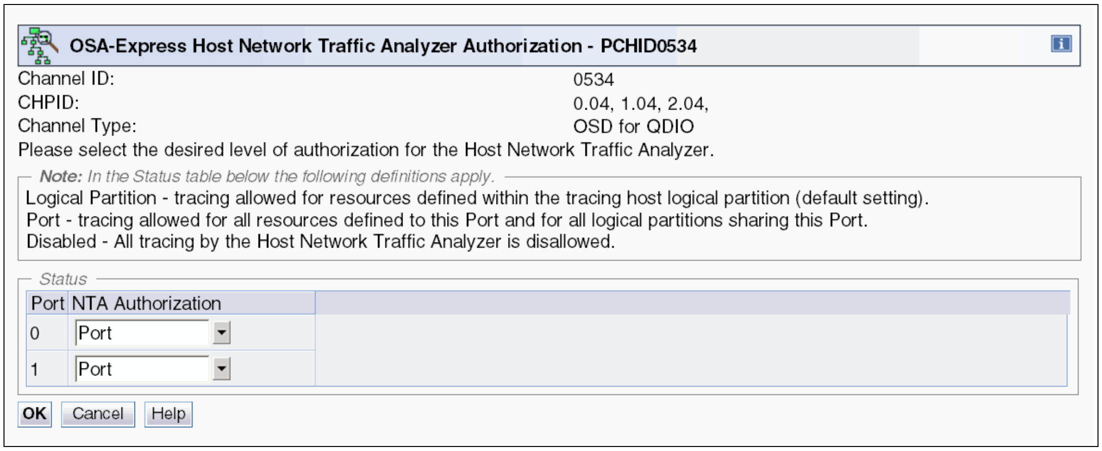
      i. Logical partition: Tracing allowed for resources that are defined within the tracing host logical partition (default setting).

      ii. Port: Tracing allowed for all resources that are defined to those ports and for all logical partitions that are sharing Port.

      iii. Disabled: All tracing by Host Network Traffic Analyzer is disallowed.

   b. Check current Network Traffic Analyzer authorization. Allows the support element to scan all the OSAs and report back which OSAs are authorized for NTA to trace outside its own partition.

6. Select **Network Traffic Analyzer Settings**, and then click **OK** (see Figure B-5).



OSA-Express Host Network Traffic Analyzer Authorization - PCHID0534

Channel ID: 0534
CHPID: 0.04, 1.04, 2.04,
Channel Type: OSD for QDIO

Please select the desired level of authorization for the Host Network Traffic Analyzer.

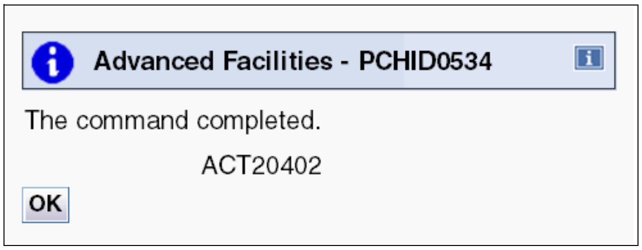
Note: *In the Status table below the following definitions apply.*
Logical Partition - tracing allowed for resources defined within the tracing host logical partition (default setting).
Port - tracing allowed for all resources defined to this Port and for all logical partitions sharing this Port.
Disabled - All tracing by the Host Network Traffic Analyzer is disallowed.

Status

Port	NTA Authorization
0	Port
1	Port

Figure B-5 NTA Authorization

7. If your CHPID is shared between several LPARs, we suggest you select the option PORT as shown in Figure B-5, then click **OK**. Figure B-6 shows the results.



Advanced Facilities - PCHID0534

The command completed.

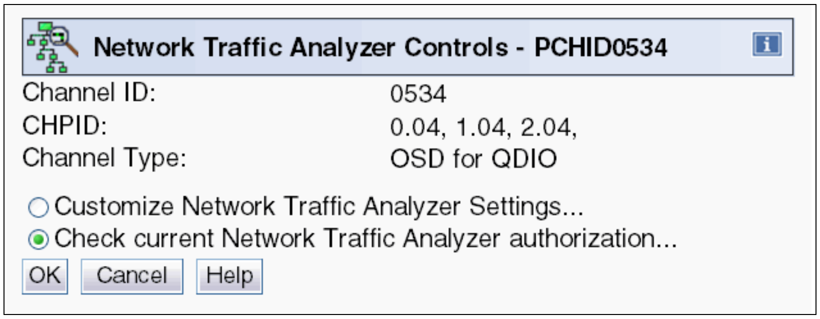
ACT20402

Figure B-6 Command completed

8. Use these steps to verify whether the command has been set, as required:
   - Log off from using the SYSPROG user ID.
   - Log on to the SE on the HMC through SOO (see Figure B-2 on page 155).

> **Important:** For checking the authorization of NTA support, the Access Administrator Tasks role must be assigned to the user ID.

   - Select **Check current Network Traffic Analyzer Authorization**, as shown in Figure B-4 on page 156.
   - Click **OK** (see Figure B-7).



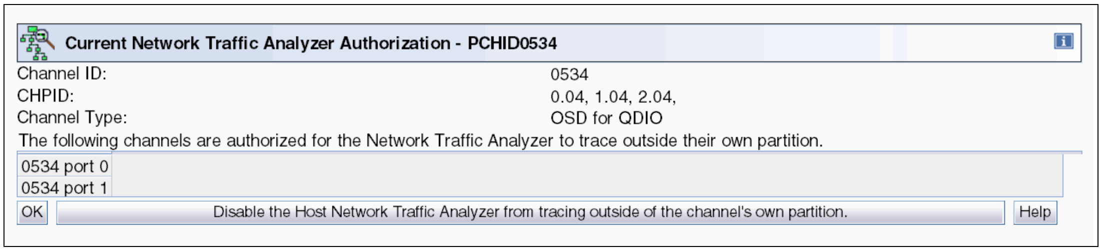
Network Traffic Analyzer Controls - PCHID0534

Channel ID: 0534
CHPID: 0.04, 1.04, 2.04,
Channel Type: OSD for QDIO

○ Customize Network Traffic Analyzer Settings...
● Check current Network Traffic Analyzer authorization...

Figure B-7 Network Traffic Analyzer controls

Figure B-8 shows that PCHID 0534 is authorized to be traced.



Current Network Traffic Analyzer Authorization - PCHID0534

Channel ID:	0534
CHPID:	0.04, 1.04, 2.04,
Channel Type:	OSD for QDIO

The following channels are authorized for the Network Traffic Analyzer to trace outside their own partition.

0534 port 0
0534 port 1

OK
Disable the Host Network Traffic Analyzer from tracing outside of the channel's own partition.
Help

Figure B-8 PCHID NTA Authorization

Define a resource profile in RACF

See Example B-5 for the RACF commands to allow users to issue the VARY TCPIP command.

Example B-5 RACF commands

```
RDEFINE OPERCMDS MVS.VARY.TCPIP.OSAENTA UACC(NONE)
PERMIT MVS.VARY.TCPIP.OSAENTA ACCESS(CONTROL) CLASS(OPERCMDS) ID(CS03)
SETR GENERIC(OPERCMDS) REFRESH
SETR RACLIST(OPERCMDS) REFRESH
```

Allocate a VSAM linear data set

Example B-6 shows how to create the VSAM linear data set. This VSAM linear data set is optional; however, we advocate its use.

Example B-6 Allocate VSAM linear data set

```
//DEFINE EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
DELETE +
(CS03.CTRACE.LINEAR) +
CLUSTER
DEFINE CLUSTER( +
NAME(CS03.CTRACE.LINEAR) +
LINEAR +
MEGABYTES(10) +
VOLUME(CPDLBO) +
CONTROLINTERVALSIZE(32768) +
) +
DATA( +
NAME(CS03.CTRACE.DATA) +
)
LISTCAT ENT(USER41.CTRACE.LINEAR) +
ALL
```

Using the Network Traffic Analyzer feature

This section provides information on how to set up and run the NTA feature.

Setting up the trace

The OSAENTA statement dynamically defines a QDIO interface to the OSA port that is being traced, which is called an *OSAENTA* interface. This interface is used exclusively for capturing OSA-Express Network Traffic Analyzer traces.

The OSAENTA statement enables an installation to trace data from other hosts that are connected to the OSA port.

> **Important:** The trace data that is collected should be considered confidential, and TCP/IP system dumps and external trace files that contain this trace data should be protected.

To see the complete syntax of the **OSAENTA** command, see *z/OS Communications Server: IP Configuration Reference*, SC31-8776.

Components involved in z/OS CTRACE

The CTRACE (component trace) service for collecting NTA trace data is called SYSTCPOT. The member in SYS1.PARMLIB is named CTINTA00. This member is used to define the size of the buffer space in the TCPIPDS1 data space that is reserved for OSAENTA CTRACE. The size range is 1 - 624 MB, with a default of 64 MB.

> **Note:** Update CTINTA00 to set the CTRACE buffer size. Keep in mind that this uses auxiliary page space storage.

Using the OSAENTA command

An internal interface is created when PORTNAME is defined on the OSAENTA statement. The dynamically defined interface name is EZANTA, concatenated with the port name. These EZANTA interfaces are displayed at the end of the **NETSTAT DEV** output.

When the ON keyword of the OSAENTA parameter is used, VTAM allocates the next available Transport Resource List Element (TRLE) data path that is associated with the port. This data path is used only for inbound trace data.

When the OFF keyword of the OSAENTA parameter is used (or the trace limits of the TIME, DATA, or FRAMES keyword are reached), the data path is released.

Set the OSAENTA traces

You can set the OSAENTA trace in either of two ways:

- By coding the OSAENTA statement in the profile TCP/IP
- By issuing a z/OS command

These methods are explained in this section.

Coding the statement in the profile TCP/IP

To code the OSAENTA statement in the profile TCP/IP, see Example B-7 on page 160.

Example B-7 TCP/IP profile

```
; set up the filters to trace for TCP packets on PORT 2323 with a source
;or destination
OSAENTA PORTNAME=OSA20C0 PROT=TCP IP=192.168.3.30 PORTNUM=2323
OSAENTA PORTNAME=OSA20C0 MAC=6CAE8B480B84
; activate the tracing (the trace will self-deactivate after 20,000 frames)
OSAENTA PORTNAME=OSA20C0 ON FRAMES=20000
; deactivate the tracing
OSAENTA OFF PORTNAME=OSA20C0
```

In this case, `OSAENTA` traces the `OSA20C0` port name only for traffic that matches the following filters:

- Protocol = `TCP`
- IP address = `192.168.3.30`
- Port number = `2323`

There are seven filters available to define the packets to capture:

- MAC address
- VLAN ID
- Ethernet frame type
- IP address (or range)
- IP protocol
- Device ID
- TCP/UDP

> **Note:** Use filters to limit the trace records to prevent overuse of the OSA processor resources, the LPAR processor resources, the TCPIPDS1 trace data space, memory, auxiliary page space, and the I/O subsystem that is writing the trace data to disk.

Using z/OS commands

Issue the following command in the z/OS software:

```
V TCPIP,TCPIPF,OSAENTA,ON,PORTNAME=OSA20C0,IP=192.168.3.30,PORTNUM=2323
```

The message that you receive in response to this command is shown in Figure B-9.

```
EZZ0060I PROCESSING COMMAND: VARY TCPIP,TCPIPF,OSAENTA,ON,PORTNAME=OSA
20C0,IP=192.168.3.30,PORTNUM=2323
EZZ0053I COMMAND VARY OSAENTA COMPLETED SUCCESSFULLY
```

Figure B-9 OSAENTA results

> **Important:** If you receive ERROR CODE 0003, it means that an attempt was made to enable Network Traffic Analyzer (NTA) tracing for a specified OSA port but the current authorization level does not permit it. See “Network Traffic Analyzer controls” in Figure B-4 on page 156 for directions about how to change the authorization to allow NTA to be used on this specified OSA.
>
> Also, read the *Support Element Operations Guide,* SC28-6860, for complete information about this topic.

The **NETSTAT DEVLINKS** command has been enhanced to show the NTA definition (see Example B-8).

Example B-8 Netstat Devlinks command output

```
OSA-EXPRESS NETWORK TRAFFIC ANALYZER INFORMATION:
  OSA PORTNAME: OSA20C0           OSA DEVSTATUS:     READY
    OSA INTFNAME: EZANTAOSA20C0   OSA INTFSTATUS:    READY
    OSA SPEED:    1000            OSA AUTHORIZATION: CHPID
    OSAENTA CUMULATIVE TRACE STATISTICS:
      DATAMEGS:   0                     FRAMES:          0
      DATABYTES:  0                     FRAMESDISCARDED: 0
      FRAMESLOST: 0
    OSAENTA ACTIVE TRACE STATISTICS:
      DATAMEGS:   0                     FRAMES:          0
      DATABYTES:  0                     FRAMESDISCARDED: 0
      FRAMESLOST: 0                     TIMEACTIVE:      0
    OSAENTA TRACE SETTINGS:           STATUS: ON
      DATAMEGSLIMIT: 1024               FRAMESLIMIT:     2147483647
      ABBREV:        224                TIMELIMIT:       10080
      DISCARD:       EXCEPTION
    OSAENTA TRACE FILTERS:            NOFILTER: NONE
      DEVICEID: *
      MAC:      *
      VLANID:   *
      ETHTYPE:  *
      IPADDR:   192.168.3.30/32
      PROTOCOL: *
      PORTNUM:  * 02323
```

The **NETSTAT** display for devices shows the Network Traffic Analyzer interfaces. The INTFName parameter has prefixed the OSA port name with `EZANTA` (as described in the next paragraph).

To display a specific NTA interface, use the `INTFName=EZANTAosaportname` keyword.

Traces are placed in an internal buffer, which can then be written by using a CTRACE external writer. The **MVS TRACE** command must also be issued for the `SYSTCPOT` component to activate the NTA trace.

Attention: If you receive ERROR CODE 0005, it means that an attempt was made to enable Network Traffic Analyzer tracing for a specified OSA that already has NTA tracing enabled elsewhere on the system for this OSA. Only one active tracing instance at a time is permitted on the system for a specified OSA.

When the trace starts, you can see that another device has been allocated to trace. Using the **D NET,TRL,TRLE=OSA20COP** command, as shown in Example B-9, that device is highlighted in the last line.

Example B-9   Output Display TRLE

```
IST1954I TRL MAJOR NODE = OSA20C0P
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = LEASED            , CONTROL = MPC , HPDT = YES
IST1715I MPCLEVEL = QDIO       MPCUSAGE = SHARE
IST2263I PORTNAME = OSA20C0    PORTNUM =   0   OSA CODE LEVEL = 0C8C
IST2337I CHPID TYPE = OSD      CHPID = 04  PNETID = ITSOPNET0
IST1577I HEADER SIZE = 4096 DATA SIZE = 0 STORAGE = ***NA***
IST1221I WRITE DEV = 20C1 STATUS = ACTIVE     STATE = ONLINE
IST1577I HEADER SIZE = 4092 DATA SIZE = 0 STORAGE = ***NA***
IST1221I READ  DEV = 20C0 STATUS = ACTIVE     STATE = ONLINE
IST1221I DATA  DEV = 20C2 STATUS = ACTIVE     STATE = N/A
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST1717I ULPID = TCPIPF ULP INTERFACE = OSA20C0
IST2310I ACCELERATED ROUTING DISABLED
IST1221I DATA  DEV = 20C2 STATUS = ACTIVE     STATE = N/A
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST1717I ULPID = TCPIPF ULP INTERFACE = OSA20C0
IST2310I ACCELERATED ROUTING DISABLED
IST2331I QUEUE   QUEUE     READ             QUEUE
IST2332I ID      TYPE      STORAGE          STATUS
IST2333I RD/1    PRIMARY   4.0M(64 SBALS)   ACTIVE
IST2305I NUMBER OF DISCARDED INBOUND READ BUFFERS = 0
IST2386I NUMBER OF DISCARDED OUTBOUND WRITE BUFFERS = 0
IST1757I PRIORITY1: UNCONGESTED PRIORITY2: UNCONGESTED
IST1757I PRIORITY3: UNCONGESTED PRIORITY4: UNCONGESTED
IST2190I DEVICEID PARAMETER FOR OSAENTA TRACE COMMAND = 01-01-00-02
IST1801I UNITS OF WORK FOR NCB AT ADDRESS X'25F25010'
IST1802I P1 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P2 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P3 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P4 CURRENT = 0 AVERAGE = 1 MAXIMUM = 1
IST1221I TRACE DEV = 20C3 STATUS = ACTIVE     STATE = N/A
```

Starting the CTRACE

1. Start the external writer (CTRACE writer) by using this command:

   ```
   TRACE CT,WTRSTART=CTWTR
   ```

2. Start the CTRACE and connect to the external writer by using this command:

   ```
   TRACE CT,ON,COMP=SYSTCPOT,SUB=(TCPIPF)
   ```

   ```
   R xx,WTR=CTWTR,END
   ```

3. Display the active component trace options with this command:

   ```
   DISPLAY TRACE,COMP=SYSTCPOT,SUB=(TCPIPF)
   ```

   Example B-10 on page 163 shows the output of this command.

Example B-10   Display Trace output

```
IEE843I 17.29.36  TRACE DISPLAY 979
        SYSTEM STATUS INFORMATION
 ST=(ON,0001M,00002M) AS=ON  BR=OFF EX=ON  MO=OFF MT=(ON,024K)
  TRACENAME
  =========
  SYSTCPOT
                      MODE BUFFER HEAD SUBS
                      =====================
                      OFF         HEAD    2
     NO HEAD OPTIONS
  SUBTRACE            MODE BUFFER HEAD SUBS
 -------------------------------------------------------------
  TCPIPF              MIN  0128M
     ASIDS      *NONE*
  JOBNAMES   *NONE*
  OPTIONS    MINIMUM
  WRITER     CTWTR
```

4. To display information about the status of the component trace for all active procedures, issue the following command:

   ```
   DISPLAY TRACE,COMP=SYSTCPOT,SUBLEVEL,N=8
   ```

   Example B-11 displays the output.

Example B-11   Status of Component Trace

```
IEE843I 17.31.49  TRACE DISPLAY 981
        SYSTEM STATUS INFORMATION
 ST=(ON,0001M,00002M) AS=ON  BR=OFF EX=ON  MO=OFF MT=(ON,024K)
  TRACENAME
  =========
  SYSTCPOT
                      MODE BUFFER HEAD SUBS
                      =====================
                      OFF         HEAD    2
        NO HEAD OPTIONS
     SUBTRACE            MODE BUFFER HEAD SUBS
    -------------------------------------------------------------
     TCPIPF              MIN  0128M
        ASIDS      *NONE*
        JOBNAMES   *NONE*
        OPTIONS    MINIMUM
        WRITER     CTWTR
--------------------------------------------------------------
  TCPIP               MIN  0128M
     ASIDS      *NONE*
     JOBNAMES   *NONE*
     OPTIONS    MINIMUM
     WRITER     *NONE*
```

5. Reproduce the problem.
    a. Disconnect the external writer:

    ```
    TRACE CT,ON,COMP=SYSTCPOT,SUB=(TCPIPF)
    R xx,WTR=DISCONNECT,END
    ```

    b. Stop the component trace:

    ```
    TRACE CT,OFF,COMP=SYSTCPOT,SUB=(TCPIPF)
    ```

    c. Stop the external writer:

    ```
    TRACE CT,WTRSTOP=CTWTR
    ```

Analyzing the trace

There are two ways to format the CTRACE:

- Use the Interactive Problem Control System (IPC)
- Use a batch job

In this section, we explain how to use each method.

Using IPCS to format CTRACE

You can format component trace records by using IPCS panels or a combination of IPCS panels and the CTRACE command, either from a dump or from external writer files.

From the IPCS PRIMARY OPTION MENU, select: **0 DEFAULTS - Specify default dump and options**. See Example B-12 for details.

Example B-12 IPCS default value

```
------------------------- IPCS Default Values ---------------------------------
 Command ===>

   You may change any of the defaults listed below. The defaults shown before
   any changes are LOCAL. Change scope to GLOBAL to display global defaults.

   Scope   ==> LOCAL   (LOCAL, GLOBAL, or BOTH)

   If you change the Source default, IPCS will display the current default
   Address Space for the new source and will ignore any data entered in
   the Address Space field.

   Source  ==> DSNAME('SYS1.SC30.CTRACE')
   Address Space   ==>
   Message Routing ==> NOPRINT TERMINAL
   Message Control ==> CONFIRM VERIFY FLAG(WARNING)
   Display Content ==> NOMACHINE REMARK REQUEST NOSTORAGE SYMBOL
```

Modify the DSNAME and OPTIONS to match your environment, and then select these options:

2 ANALYSIS	Analyze dump contents
7 TRACES	Trace formatting
1 CTRACE	Component trace
D DISPLAY	Specify parameters to display CTRACE entries

Fill in the parameters necessary as shown in Example B-13 on page 165 to format the OSAENTA trace.

Example B-13 CTRACE parameters

```
-------------------- CTRACE DISPLAY PARAMETERS  ------------------------
COMMAND ===>

  System      ===>          (System name or blank)
  Component   ===> SYSTCPOT (Component name (required))
  Subnames    ===> TCPIPF

  GMT/LOCAL   ===> G                       (G or L, GMT is default)
  Start time  ===>                         (mm/dd/yy,hh:mm:ss.dddddd or
  Stop time   ===>                          mm/dd/yy,hh.mm.ss.dddddd)
  Limit       ===> 0        Exception ===>
  Report type ===> SHORT    (SHort, SUmmary, Full, Tally)
  User exit   ===>          (Exit program name)
  Override source ===>
  Options         ===>

  To enter/verify required values, type any character
  Entry IDs ===>   Jobnames ===>   ASIDs ===>   OPTIONS ===>   SUBS ===>

  CTRACE COMP(SYSTCPOT) SUB((TCPIPA)) SHORT


  ENTER = update CTRACE definition.  END/PF3 = return to previous panel.
  S = start CTRACE.  R = reset all fields.
```

On the command line, entering the **S** command will show the trace formatted by the IPCS.

Using a batch job to format CTRACE

We used a batch job to generate the TRACE file, as shown in Example B-14.

Example B-14 CTRACE batch job format

```
//PKT2SNIF JOB (999,POK),'CS03',NOTIFY=&SYSUID,
//    CLASS=A,MSGCLASS=T,TIME=1439,
//    REGION=0M,MSGLEVEL=(1,1)
//    SET INDUMP='SYS1.SC30.CTRACE'
//IPCSBTCH EXEC PGM=IKJEFT01,DYNAMNBR=30
//IPCSDDIR DD DISP=SHR,DSN=SYS1.DDIR
//IPCSDUMP DD *
//SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//INDMP    DD DISP=SHR,DSN=&INDUMP.
//IPCSPRNT DD DSN=WCHUNG.CTRACE.SHORT,UNIT=SYSDA,
//    DISP=(NEW,CATLG),LRECL=133,SPACE=(CYL,(10,1)),RECFM=VBS,DSORG=PS
//IPCSTOC  DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SYSTSIN  DD *
 PROFILE MSGID
  IPCS NOPARM
  SETD PRINT NOTERM LENGTH(160000) NOCONFIRM FILE(INDMP)
  DROPD
 CTRACE COMP(SYSTCPOT) SUB((TCPIPF)) SHORT
 END
```

Network Management Interface API for diagnosing problems

IBM and other vendors have developed tools to assist in diagnosing problems in the network from the z/OS perspective. The tools often run as GUIs on a workstation but retrieve their problem diagnosis information by using data from SNMP, the z/OS System Management Facilities (SMF), and Multiple Virtual Storage (MVS) control blocks. Some of these tools also interface with the Network Management Interface API, which is provided by IBM.

Figure B-10 depicts a high-level view of the Network Management Interface (NMI) API and its interfaces to network management products.

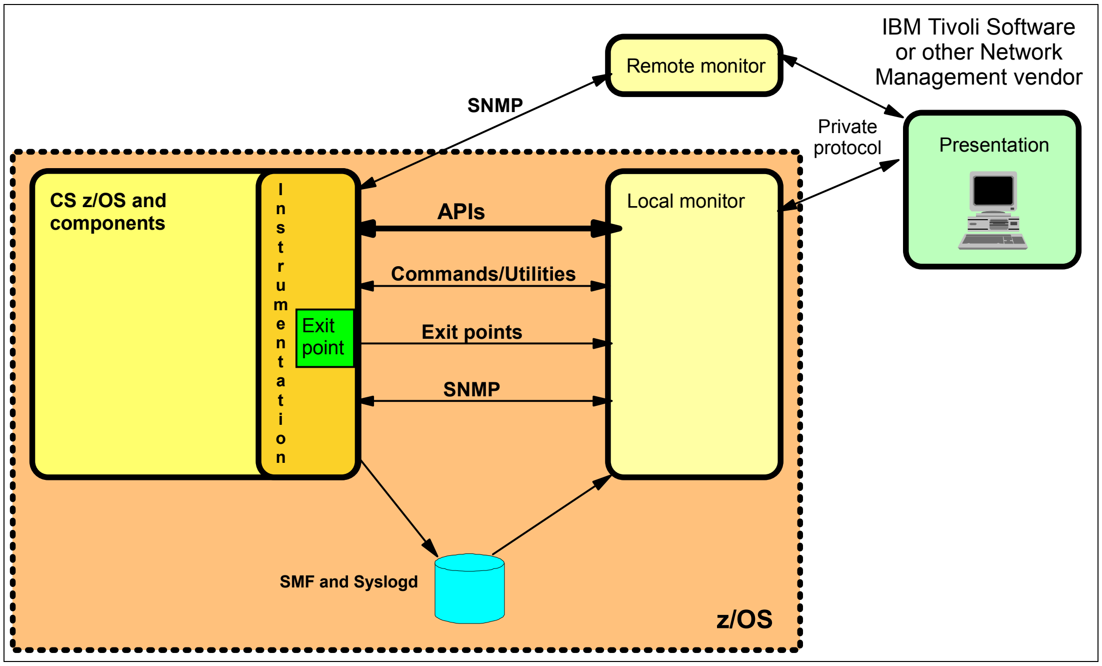


Figure B-10 Network Management Interface Architecture

The NMI API can interface with IBM Tivoli® OMEGAMON® XE for Mainframe Networks (or other products) to provide the following types of functions:

- Trace assistance
  - Real-time tracing and formatting for packet and data traces
- Information gathering
  - TCP connection initiation and termination notifications
  - API for real-time access to TN3270 server and FTP event data and to IPSec
  - APIs to poll information about currently active connections
  - TCP listeners (server processes)
  - TCP connections (detailed information about individual connections and UDP endpoints)
  - CS storage use
  - API to receive and poll for Enterprise Extender management data
  - Information and statistics for IP filtering and IPSec security associations on the local TCP/IP stacks.

  - Information and statistics for IP filtering and IPSec security associations on remote Network Security Services (NSS) clients when using the NSS server.
- Control activities
- Control the activation and inactivation of IPSec tunnels
- Loading policies for IP filtering and IPSec security associations on the local TCP/IP stacks
  - Loading policies for IP filtering and IPSec security associations on remote Network Security Services (NSS) clients when using the NSS server
  - Drop one or multiple TCP connections or UDP endpoints

References

See the following publications for more information about the use of logs, standard commands, tools, and utilities:

- *z/OS Communications Server: IP System Administrator's Commands*, SC31-8781
- *z/OS Communications Server: IP Diagnosis Guide*, GC31-8782
- *z/OS Communications Server: IP Configuration Reference*, SC31-8776
- *z/OS MVS Diagnosis: Tools and Service Aids*, GA22-7589
- *z/OS Communications Server: SNA Diagnosis Vol. 1, Techniques and Procedures,* GC31-6850
- *z/OS Communications Server: SNA Operation*, SC31-8779
- *MVS Installation Exits*, SA22-7593
- *Support Element Operations Guide,* SC28-6860

See the z/OS Communications Server web page for support and downloads:

https://ibm.biz/BdRCji

See the Tivoli Information Center for information on IBM Tivoli OMEGAMON XE for Mainframe Networks:

https://ibm.biz/BdRCj4

C

Hardware Management Console and Support Element tasks

This appendix describes the tools that you can use from a Hardware Management Console (HMC) or the Support Element (SE) for IBM zEnterprise EC12 (zEC12), IBM zEnterprise BC12 (zBC12), IBM zEnterprise 196 (z196), or IBM zEnterprise (z114) servers. First, we describe the advanced facilities for Open Systems Adapter-Express (OSA) channels, which are now available directly on the HMC as a task under the central processor complex (CPC) Operational Customization options. Then, we offer guidance for channel path identifier (CHPID) On/Off setting.

The information covers the following topics:

- “HMC advanced facilities for OSA” on page 170
- “View code level” on page 178
- “Configuring OSA channels on/off” on page 178

HMC advanced facilities for OSA

The following advanced facilities of the Open Systems Adapter Support Facility (OSA/SF) are available on the HMC.

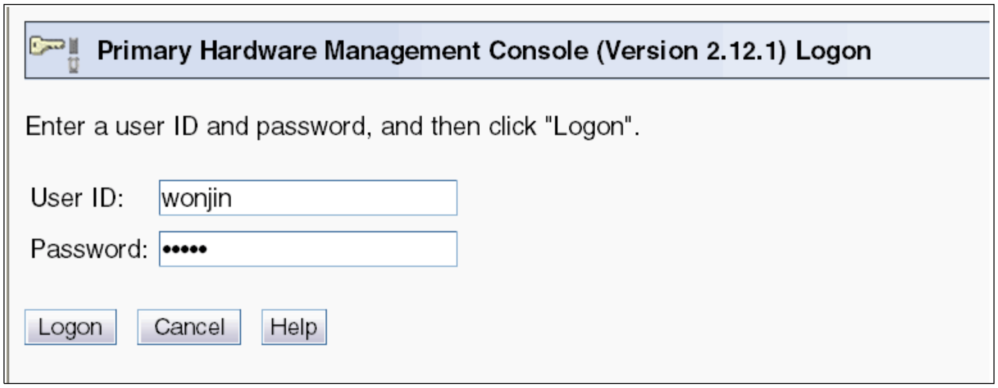
> **Note:** These functions are used for troubleshooting under the guidance of IBM Product Engineering.

- Set trace buffer
- Read trace buffer
- Export trace/dump file to diskette
- Card-specific advanced facilities, with the following subdivisions:
  - Enable or disable ports
  - Query port status
  - Run port diagnostics
  - View port parameter
  - Display or alter MAC address
  - Set Ethernet mode (only for FENET/1000BASE-T)

Online help is available for each function on the HMC or the SE. You can activate the online help in two ways:

- By clicking **Help** on the active window
- By pressing F1 on the keyboard

To gain access to the advanced facilities, log on to the HMC in system programmer mode (Figure C-1).



Primary Hardware Management Console (Version 2.12.1) Logon

Enter a user ID and password, and then click "Logon".

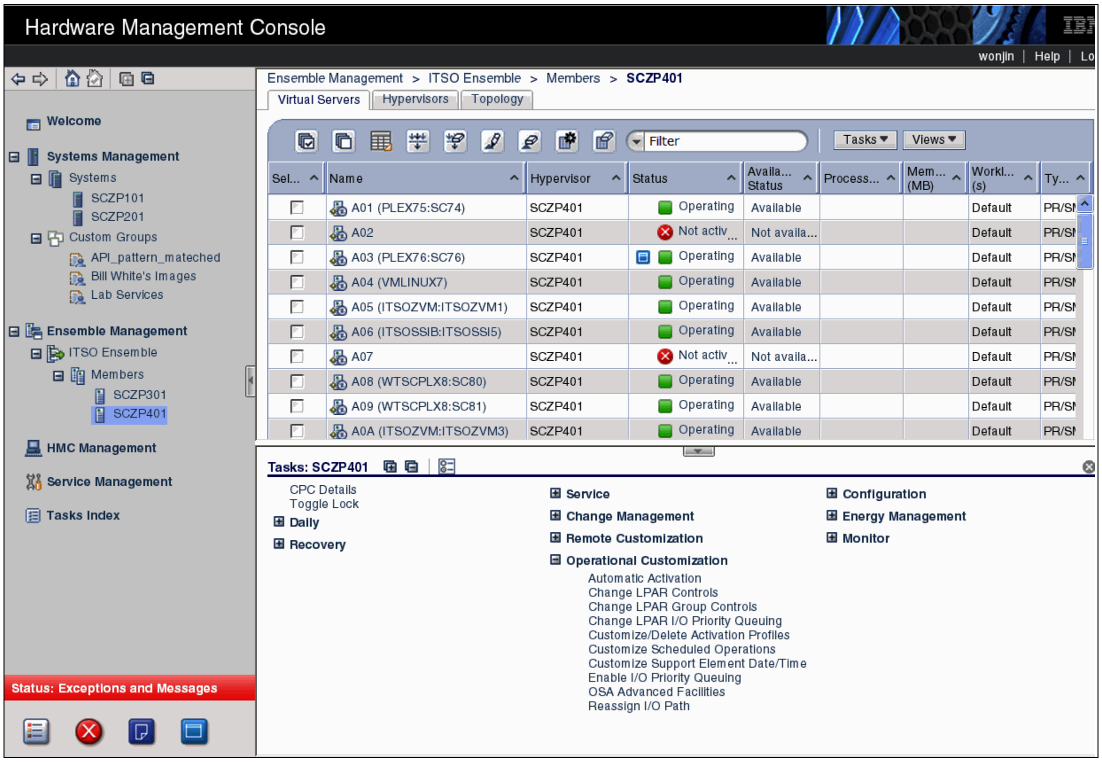
User ID: wonjin

Password: •••••

Figure C-1 Console logon

Then, follow these steps to start the individual functions:

1. Open System Management or Ensemble Management.
2. In the Hardware Management Console Workplace window (Figure C-2 on page 171), select the appropriate CPC and click **OSA Advanced Facilities** in the lower part of the window.

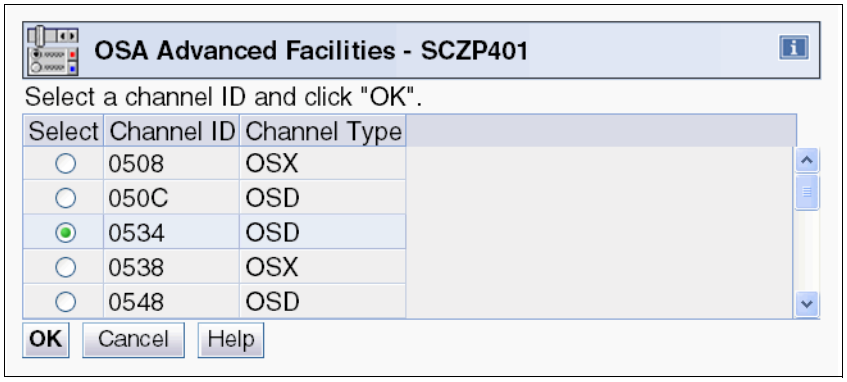


Sel...	Name	Hypervisor	Status	Availa... Status	Process...	Mem... (MB)	Workl... (s)	Ty...
□	A01 (PLEX75:SC74)	SCZP401	🟩 Operating	Available			Default	PR/SI
□	A02	SCZP401	☒ Not activ...	Not availa...			Default	PR/SI
□	A03 (PLEX76:SC76)	SCZP401	🟩 Operating	Available			Default	PR/SI
□	A04 (VMLINUX7)	SCZP401	🟩 Operating	Available			Default	PR/SI
□	A05 (ITSOZVM:ITSOZVM1)	SCZP401	🟩 Operating	Available			Default	PR/SI
□	A06 (ITSOSSIB:ITSOSSI5)	SCZP401	🟩 Operating	Available			Default	PR/SI
□	A07	SCZP401	☒ Not activ...	Not availa...			Default	PR/SI
□	A08 (WTSCPLX8:SC80)	SCZP401	🟩 Operating	Available			Default	PR/SI
□	A09 (WTSCPLX8:SC81)	SCZP401	🟩 Operating	Available			Default	PR/SI
□	A0A (ITSOZVM:ITSOZVM3)	SCZP401	🟩 Operating	Available			Default	PR/SI

Tasks: SCZP401
CPC Details
Toggle Lock
Daily
Recovery
Service
Change Management
Remote Customization
Operational Customization
Automatic Activation
Change LPAR Controls
Change LPAR Group Controls
Change LPAR I/O Priority Queuing
Customize/Delete Activation Profiles
Customize Scheduled Operations
Customize Support Element Date/Time
Enable I/O Priority Queuing
OSA Advanced Facilities
Reassign I/O Path
Configuration
Energy Management
Monitor

Figure C-2 HMC Workplace

3. The OSA Advanced Facilities window (Figure C-3) opens in the HMC console. Select the OSA CHPID that you want to work with and click **OK**.

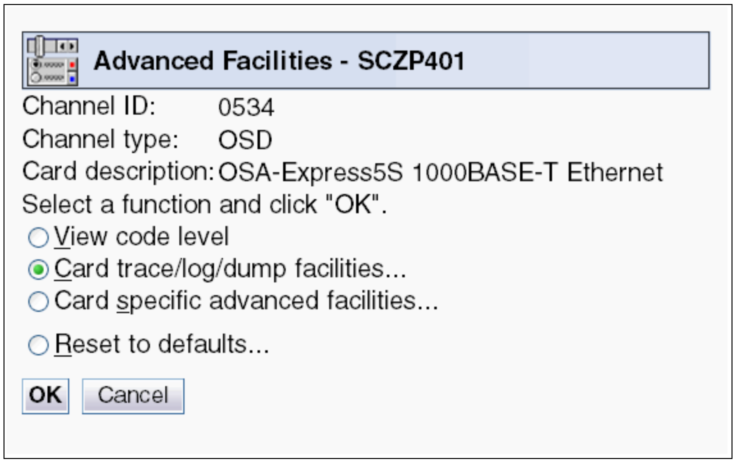

OSA Advanced Facilities - SCZP401

Select a channel ID and click "OK".

Select	Channel ID	Channel Type
○	0508	OSX
○	050C	OSD
●	0534	OSD
○	0538	OSX
○	0548	OSD

Figure C-3 HMC OSA Advanced Facilities window

The standard channel Advanced Facilities window (Figure C-4) opens.



Advanced Facilities - SCZP401

Channel ID: 0534
Channel type: OSD
Card description: OSA-Express5S 1000BASE-T Ethernet
Select a function and click "OK".

○ View code level
● Card trace/log/dump facilities...
○ Card specific advanced facilities...
○ Reset to defaults...

Figure C-4 Advanced Facilities window

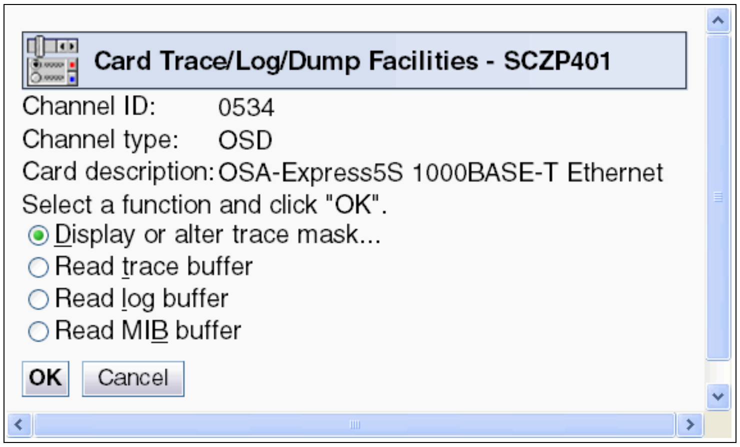
Trace functions for OSA

These trace functions are used to troubleshoot under the guidance of IBM Product Engineering.

Set the Trace Mask on the OSA card

Follow these steps to set the trace options:

1. In the OSA Advanced Facilities window, select **Card Trace/Log/Dump facilities**.
2. In the Card Trace/Log/Dump Facilities window (Figure C-5), select **Display and or alter trace mask** and click **OK**.



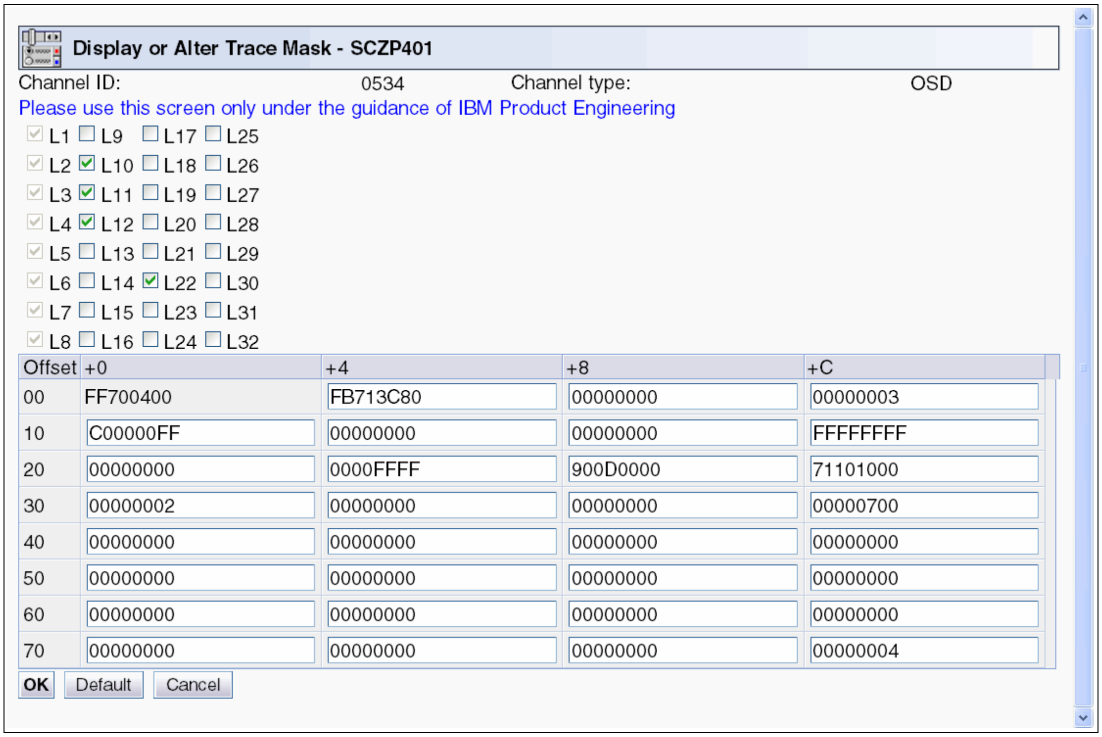
Card Trace/Log/Dump Facilities - SCZP401

Channel ID: 0534
Channel type: OSD
Card description: OSA-Express5S 1000BASE-T Ethernet
Select a function and click "OK".

● Display or alter trace mask...
○ Read trace buffer
○ Read log buffer
○ Read MIB buffer

Figure C-5 Card Trace/Log/Dump Facilities window

With guidance from the IBM representative, complete the fields that are shown in the Display or Alter Trace Mask window (Figure C-6).



Display or Alter Trace Mask - SCZP401

Channel ID: 0534 Channel type: OSD

Please use this screen only under the guidance of IBM Product Engineering

☑ L1	□ L9	□ L17	□ L25
☑ L2	☑ L10	□ L18	□ L26
☑ L3	☑ L11	□ L19	□ L27
☑ L4	☑ L12	□ L20	□ L28
☑ L5	□ L13	□ L21	□ L29
☑ L6	□ L14	☑ L22	□ L30
☑ L7	□ L15	□ L23	□ L31
☑ L8	□ L16	□ L24	□ L32

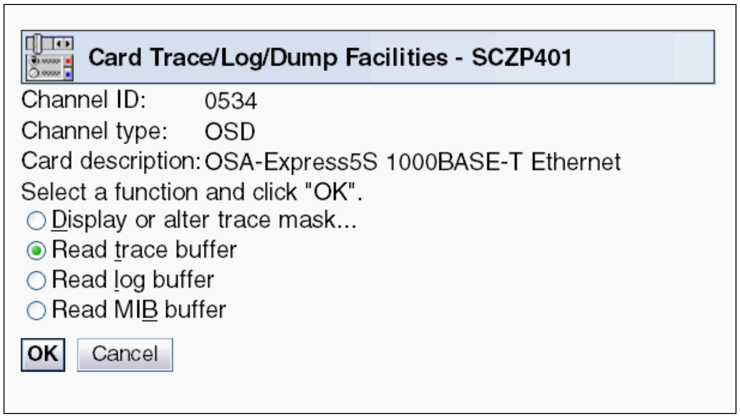
Offset	+0	+4	+8	+C
00	FF700400	FB713C80	00000000	00000003
10	C00000FF	00000000	00000000	FFFFFFFF
20	00000000	0000FFFF	900D0000	71101000
30	00000002	00000000	00000000	00000700
40	00000000	00000000	00000000	00000000
50	00000000	00000000	00000000	00000000
60	00000000	00000000	00000000	00000000
70	00000000	00000000	00000000	00000004

Figure C-6 Display or Alter Trace Mask window

Read the Trace Buffer on the OSA card

Follow these steps to read the trace buffer:

1. In the OSA Advanced Facilities window (Figure C-4 on page 172), select **Card Trace/Log/Dump facilities**.
2. In the Card Trace/Log/Dump Facilities window (Figure C-7), select **Read Trace Buffer** and click **OK**.



Card Trace/Log/Dump Facilities - SCZP401

Channel ID: 0534

Channel type: OSD

Card description: OSA-Express5S 1000BASE-T Ethernet

Select a function and click "OK".

○ Display or alter trace mask...

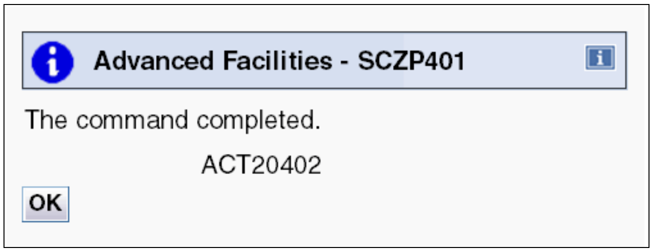
● Read trace buffer

○ Read log buffer

○ Read MIB buffer

Figure C-7 Read trace buffer confirmation window

The Read Trace Buffer function collects all data necessary for troubleshooting and writes a file on the HMC when the command is completed. Then, you see the command completed message that is shown in Figure C-8.



Advanced Facilities - SCZP401

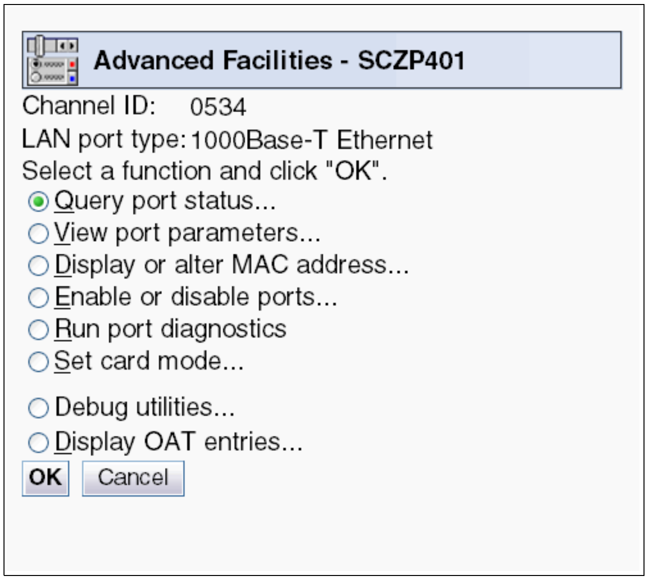
The command completed.

ACT20402

Figure C-8 Read trace buffer command completed notice

Hardware functions for OSA

1. In the OSA Advanced Facilities window as shown in Figure C-4 on page 172, select **Card specific advanced facilities**.
2. Then, select the **Advanced Facilities - SCZP401** window, which is shown in Figure C-9. The sections that follow explain the options.



Advanced Facilities - SCZP401

Channel ID: 0534

LAN port type: 1000Base-T Ethernet

Select a function and click "OK".

● Query port status...
○ View port parameters...
○ Display or alter MAC address...
○ Enable or disable ports...
○ Run port diagnostics
○ Set card mode...

○ Debug utilities...
○ Display OAT entries...

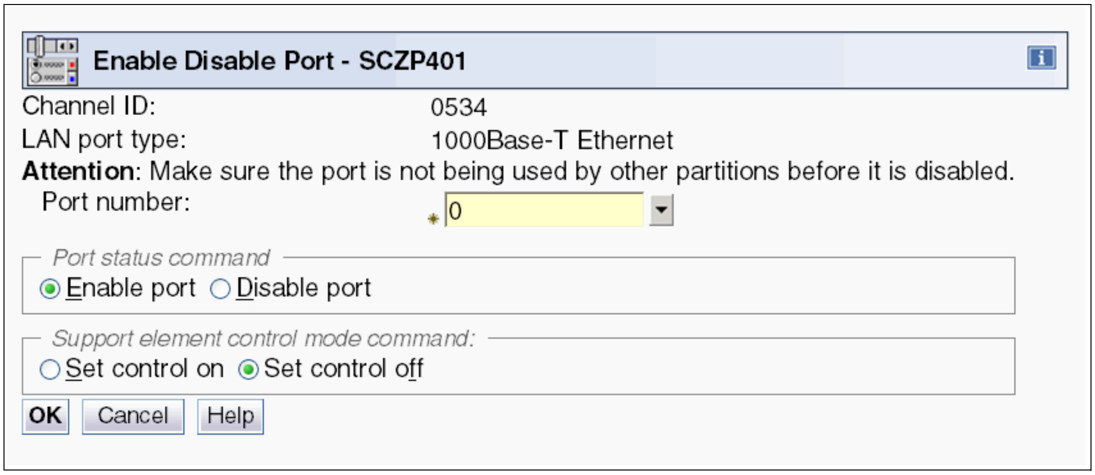
Figure C-9 Card-specific advanced facilities list

(The bottom two options are beyond the scope of this book.)

Enable or disable ports

In the Advanced Facilities window shown in Figure C-9, select **Enable or disable ports** and click **OK** to open the Enable or Disable ports window (Figure C-10 on page 175).

> **Note:** Enabling or disabling the port is also possible with an OSA/SF function.


Enable Disable Port - SCZP401

Channel ID: 0534

LAN port type: 1000Base-T Ethernet

Attention: Make sure the port is not being used by other partitions before it is disabled.

Port number: 0

Port status command

● Enable port ○ Disable port

Support element control mode command:

○ Set control on ● Set control off

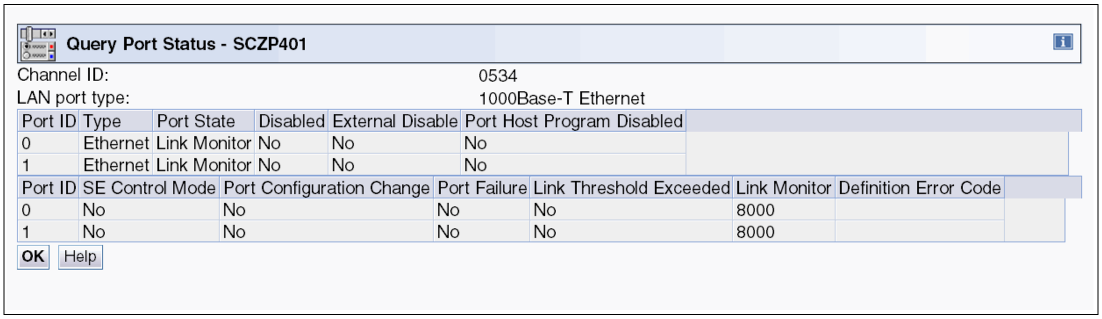
Figure C-10 Enable or Disable Ports window

Two tasks are related to the enable or disable port function:

- The first task enables or disables the port.
- The second task sets the control of enabling and disabling the port either to its Support Element (SE) or to both the SE and Open Systems Adapter Support Facility (OSA/SF).

Query port status

1. In the Advanced Facilities window (Figure C-9 on page 174), select **Query port status** and click **OK**. The Query port status window (Figure C-11) opens.
2. To exit the window, simply click **OK**.


Query Port Status - SCZP401

Channel ID: 0534

LAN port type: 1000Base-T Ethernet

Port ID	Type	Port State	Disabled	External Disable	Port Host Program Disabled
0	Ethernet	Link Monitor	No	No	No
1	Ethernet	Link Monitor	No	No	No

Port ID	SE Control Mode	Port Configuration Change	Port Failure	Link Threshold Exceeded	Link Monitor	Definition Error Code
0	No	No	No	No	8000	
1	No	No	No	No	8000	

Figure C-11 Query Port Status window

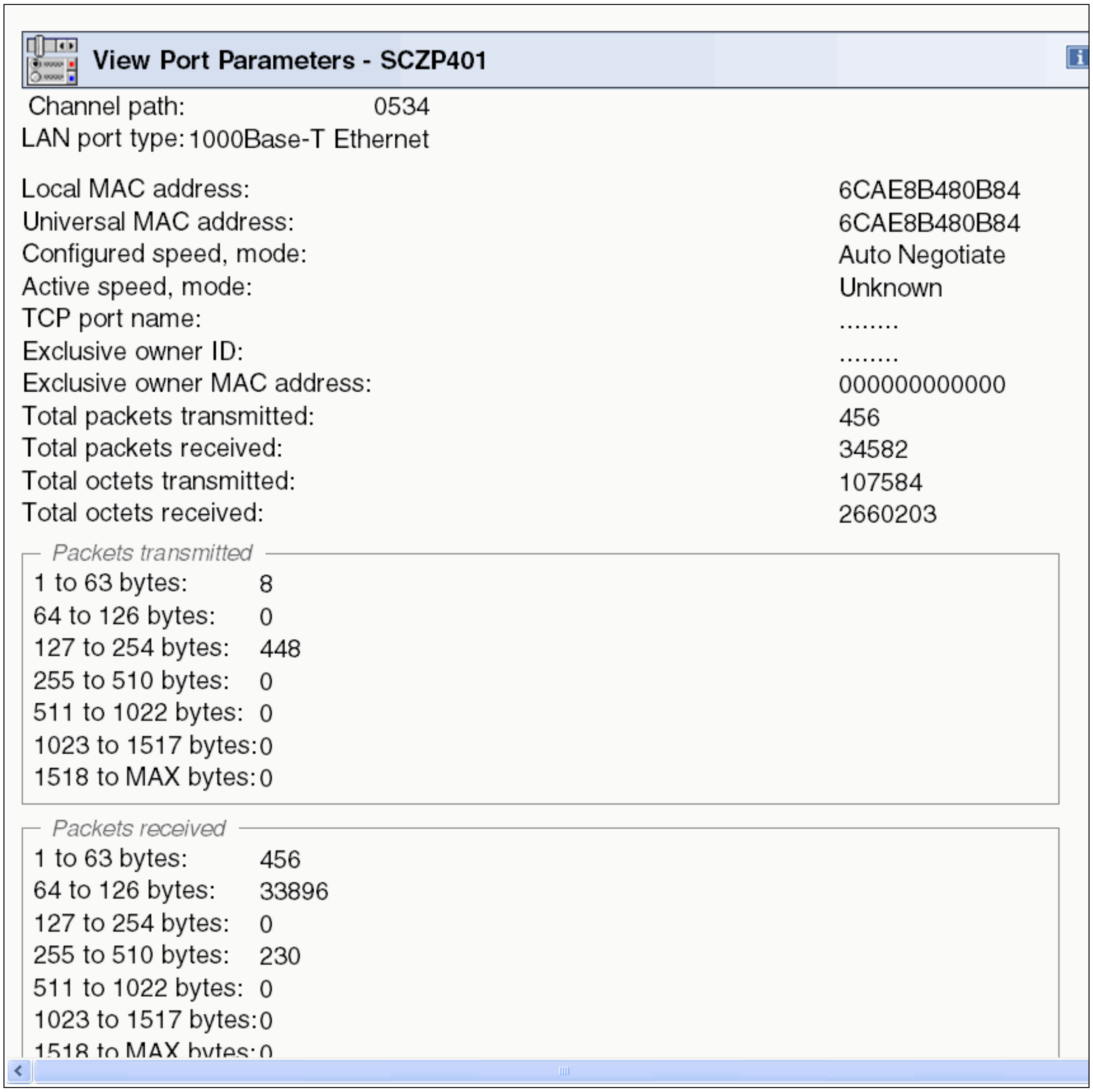
Run port diagnostics

In the Advanced facilities window (Figure C-9 on page 174), select **Run port diagnostics** and then click **OK**.

Note: You can run port diagnostics only if the port is disabled.

View port parameters

1. In the Advanced Facilities window (see Figure C-4 on page 172), select **View port parameters** and then click **OK**. For OSA-Express5S multi-port cards, select port 0 or 1.
2. In the View Port Parameters window that opens ((Figure C-12 on page 176), you can scroll to view all port parameters.
3. To exit the window, click **OK**.


View Port Parameters - SCZP401

Channel path: 0534
LAN port type: 1000Base-T Ethernet

Local MAC address:	6CAE8B480B84
Universal MAC address:	6CAE8B480B84
Configured speed, mode:	Auto Negotiate
Active speed, mode:	Unknown
TCP port name:	....
Exclusive owner ID:	....
Exclusive owner MAC address:	000000000000
Total packets transmitted:	456
Total packets received:	34582
Total octets transmitted:	107584
Total octets received:	2660203

Packets transmitted

1 to 63 bytes:	8
64 to 126 bytes:	0
127 to 254 bytes:	448
255 to 510 bytes:	0
511 to 1022 bytes:	0
1023 to 1517 bytes:	0
1518 to MAX bytes:	0

Packets received

1 to 63 bytes:	456
64 to 126 bytes:	33896
127 to 254 bytes:	0
255 to 510 bytes:	230
511 to 1022 bytes:	0
1023 to 1517 bytes:	0
1518 to MAX bytes:	0

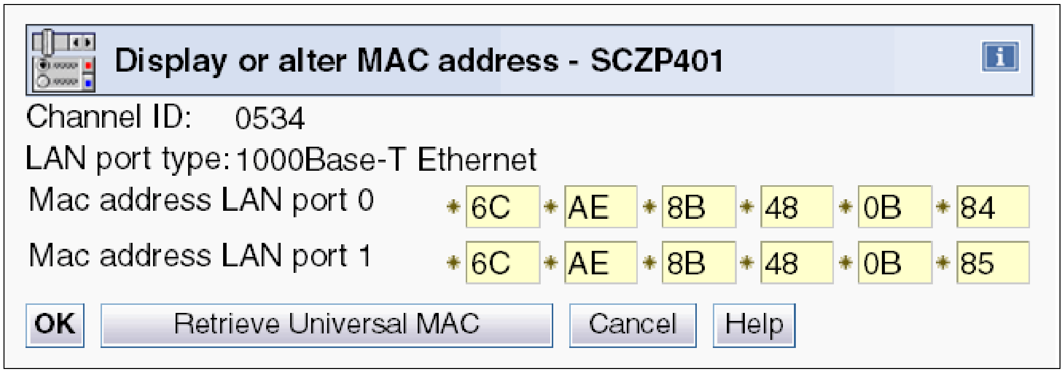
Figure C-12 View Port Parameters window

Display or alter MAC address on an OSA-Express card

1. In the Advanced Facilities window (Figure C-4 on page 172), select **Display or alter MAC address** and click **OK**.

2. In the Display or Alter MAC address window (Figure C-13 on page 177), change the MAC address, and click **Apply** to activate the change.

   To close the window without any changes, click **Cancel**.


Display or alter MAC address - SCZP401

Channel ID: 0534

LAN port type: 1000Base-T Ethernet

Mac address LAN port 0: 6C AE 8B 48 0B 84

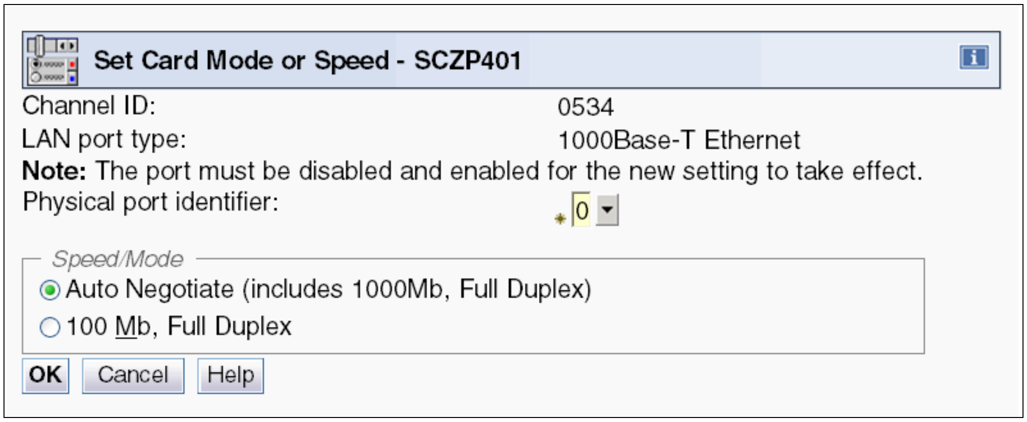
Mac address LAN port 1: 6C AE 8B 48 0B 85

Figure C-13 Display or alter MAC address window

Set card mode or speed

1. In the Advanced Facilities window (Figure C-4 on page 172), select **Set card mode** and then click **OK**.
2. In the Set Card Mode or Speed window (Figure C-14), set or change the settings that are shown. Click **Apply** to make the new settings active.
3. To exit the window without any changes, click **Cancel**.

Note: These settings override the OSA 1000BASE-T auto-negotiation facility.


Set Card Mode or Speed - SCZP401

Channel ID: 0534

LAN port type: 1000Base-T Ethernet

Note: The port must be disabled and enabled for the new setting to take effect.

Physical port identifier: 0

Speed/Mode

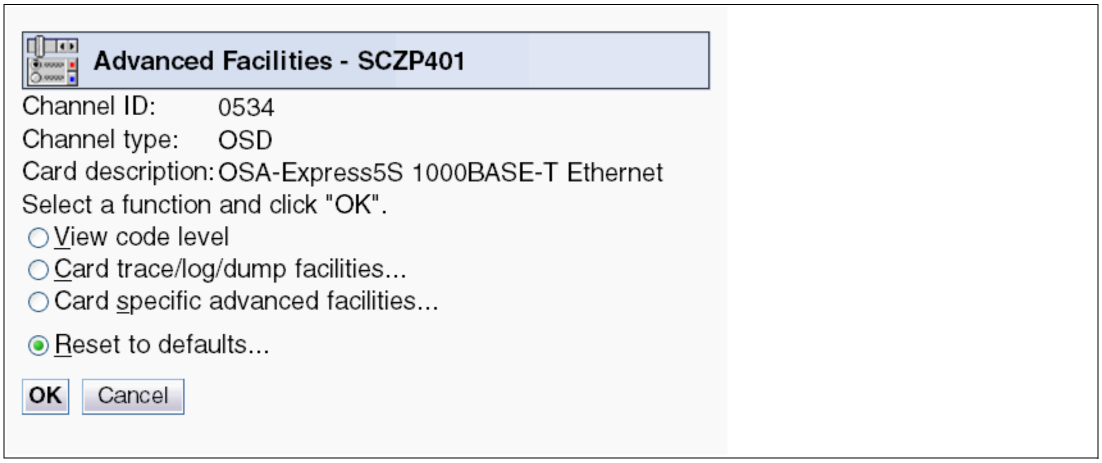
● Auto Negotiate (includes 1000Mb, Full Duplex)

○ 100 Mb, Full Duplex

Figure C-14 Set Card Mode or Speed window

OSA reset to defaults

Back in the OSA Advanced Facilities window (Figure C-15 on page 178), select **Reset to defaults** and click **OK**. You can use this function to reset all of your customized entries in the OSA card to the default settings, including the OSA address table (OAT).


Advanced Facilities - SCZP401

Channel ID: 0534

Channel type: OSD

Card description: OSA-Express5S 1000BASE-T Ethernet

Select a function and click "OK".

○ View code level

○ Card trace/log/dump facilities...

○ Card specific advanced facilities...

● Reset to defaults...

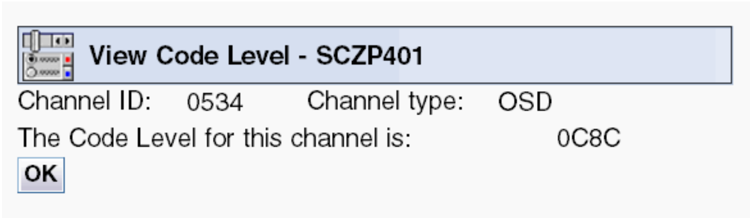
Figure C-15 Advanced Facilities window in the Support Element

View code level

The view code level task queries the OSA microcode level that is active in an OSA card. The code level is a four-digit number that relates to a specific microcode engineering change (EC) and microcode patch level (MCL).

This information can be useful in the diagnosis of an OSA-related problem. You might be asked by the IBM Remote Technical Support Center or your IBM Systems Services Representative for the OSA code level as part of information that they need to analyze a problem.

1. In the OSA Advanced Facilities, select **View Code Level**, and then click **OK** to see the View Code Level panel (Figure C-16).


View Code Level - SCZP401

Channel ID: 0534 Channel type: OSD

The Code Level for this channel is: 0C8C

Figure C-16 View Code Level panel

The four-digit code that is displayed varies, depending on the specific microcode EC and MCL levels that are active in the OSA card. The code changes as microcode maintenance updates are applied to your IBM zEnterprise EC 12 (zEC12), zEnterprise BC 12 (zBC12), zEnterprise 196 (z196), or zEnterprise 114 (z114) system by your IBM service representatives.

2. In the View Code Level panel, click **OK** to return to the Advanced Facilities window.

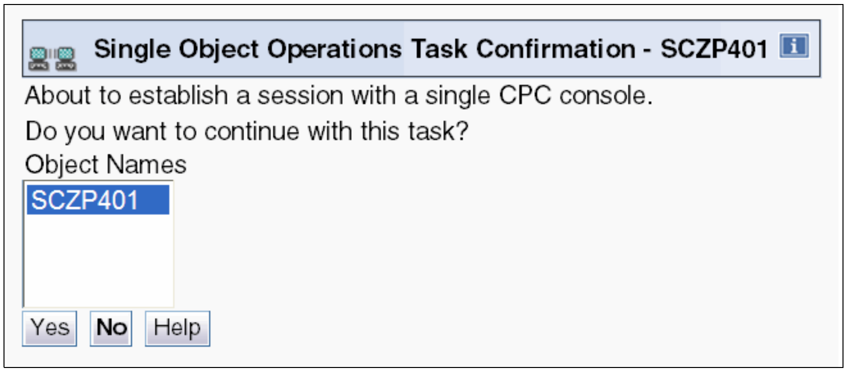
Configuring OSA channels on/off

With the current design of the OSA cards, there is no longer a need to configure the OSA CHPID offline and online to activate an OAT after changing it. However, for recovery reasons, it still might be necessary. Normally, you use IBM z/OS commands on the operator console to configure a channel On or off.

You cannot configure channels offline to the whole system with one command from an operator console when you are running in logical partition (LPAR) mode. We explain the HMC procedure that is used to configure a CHPID On or Off for all LPARs.

Log on to the Support Element

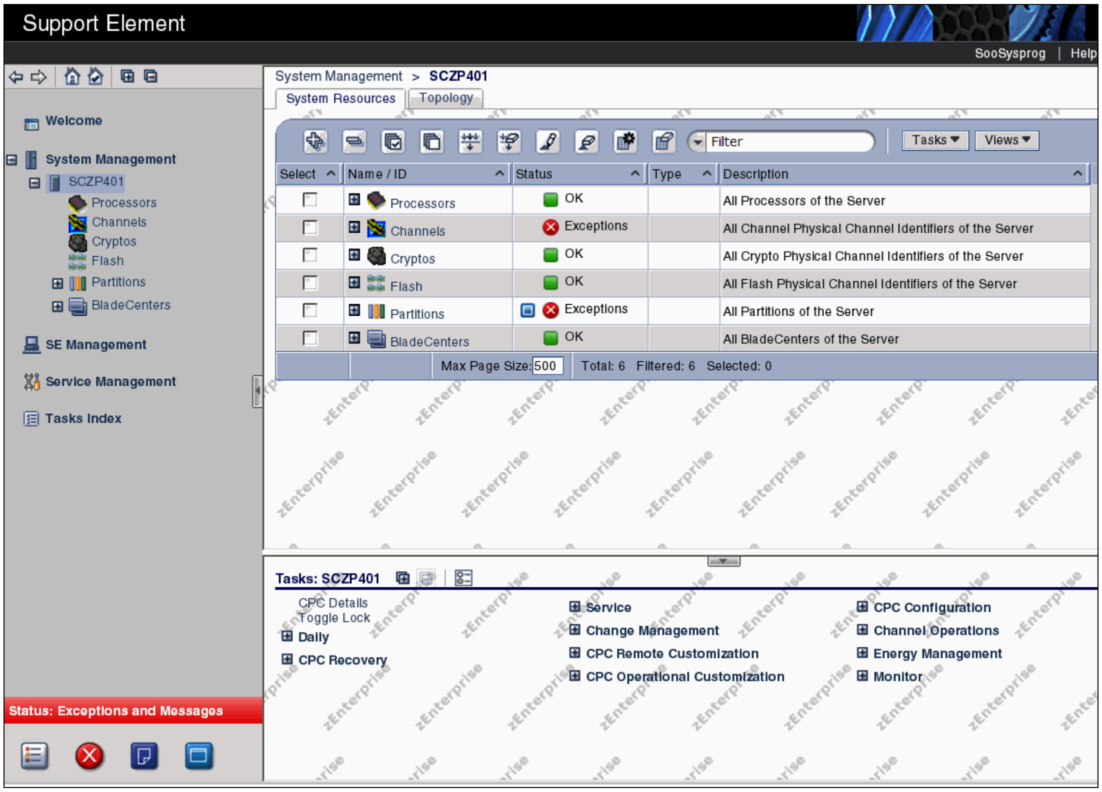
1. To gain access to all channel functions, follow these steps to start a session from the HMC to the SE.
2. From the HMC, complete these steps:
   a. Select the appropriate CPC Object and click **Single Object Operations** from the Recovery section in the bottom window.
   b. In the Single Object Selection window, select the CPC, and then click **OK**.
   c. In the confirmation window (Figure C-17), click **Yes**.



About to establish a session with a single CPC console.
Do you want to continue with this task?
Object Names
SCZP401

Figure C-17 Single Object selection

3. After a short time, the HMC displays the Support Element Workplace. Figure C-18 on page 180 shows an example of that window. The zEnterprise background of the workplace indicates that you are working in the SE.



Select	Name / ID	Status	Type	Description
☐	Processors	🟩 OK		All Processors of the Server
☐	Channels	☒ Exceptions		All Channel Physical Channel Identifiers of the Server
☐	Cryptos	🟩 OK		All Crypto Physical Channel Identifiers of the Server
☐	Flash	🟩 OK		All Flash Physical Channel Identifiers of the Server
☐	Partitions	☒ Exceptions		All Partitions of the Server
☐	BladeCenters	🟩 OK		All BladeCenters of the Server

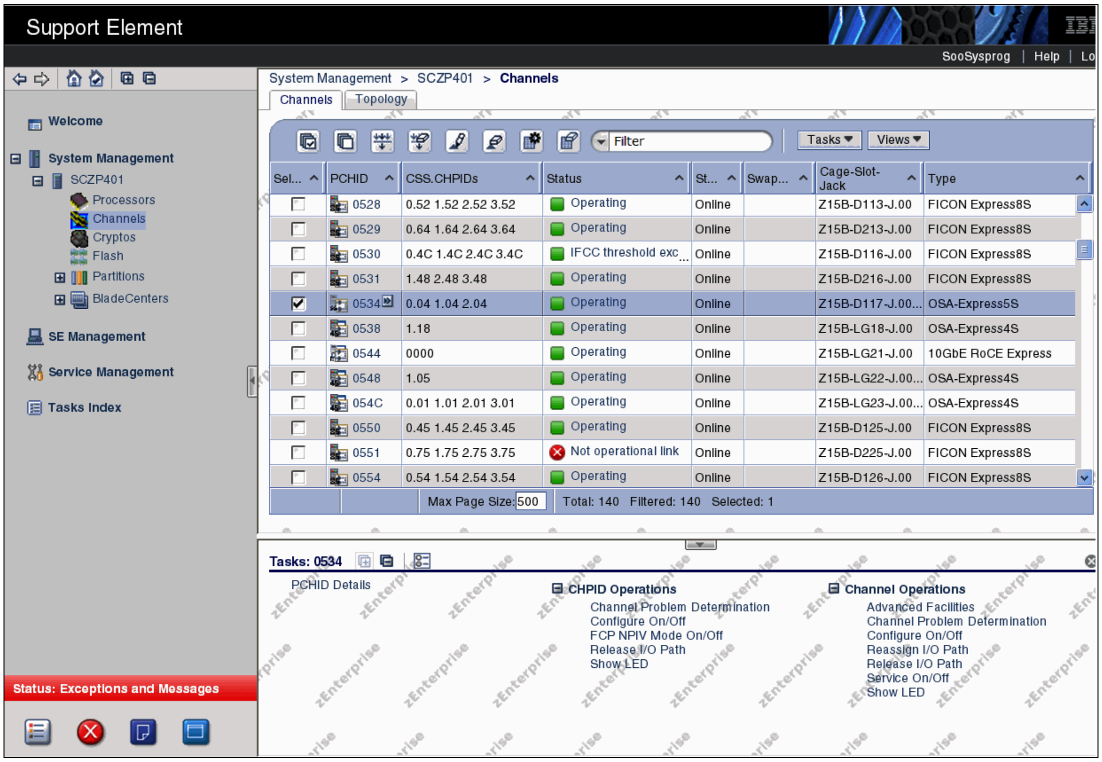
Max Page Size: 500 Total: 6 Filtered: 6 Selected: 0

Figure C-18 Support Element Workplace window

Set the CHPID to On or Off

Set the OSA CHPID to On or Off by following these steps:

1. In the SE, click the **CPC object** and click the **Channels**.
2. The CHPIDs are displayed in upper panel (see Figure C-19 on page 181). Use the scroll bar to display the required CHPID object.
3. Select CHPID to show the CHPID Operations list in the lower panel.



Sel...	PCHID	CSS.CHPIDs	Status	St...	Swap...	Cage-Slot-Jack	Type
☐	0528	0.52 1.52 2.52 3.52	🟩 Operating	Online		Z15B-D113-J.00	FICON Express8S
☐	0529	0.64 1.64 2.64 3.64	🟩 Operating	Online		Z15B-D213-J.00	FICON Express8S
☐	0530	0.4C 1.4C 2.4C 3.4C	🟩 IFCC threshold exc...	Online		Z15B-D116-J.00	FICON Express8S
☐	0531	1.48 2.48 3.48	🟩 Operating	Online		Z15B-D216-J.00	FICON Express8S
☑	0534	0.04 1.04 2.04	🟩 Operating	Online		Z15B-D117-J.00...	OSA-Express5S
☐	0538	1.18	🟩 Operating	Online		Z15B-LG18-J.00	OSA-Express4S
☐	0544	0000	🟩 Operating	Online		Z15B-LG21-J.00	10GbE RoCE Express
☐	0548	1.05	🟩 Operating	Online		Z15B-LG22-J.00...	OSA-Express4S
☐	054C	0.01 1.01 2.01 3.01	🟩 Operating	Online		Z15B-LG23-J.00...	OSA-Express4S
☐	0550	0.45 1.45 2.45 3.45	🟩 Operating	Online		Z15B-D125-J.00	FICON Express8S
☐	0551	0.75 1.75 2.75 3.75	☒ Not operational link	Online		Z15B-D225-J.00	FICON Express8S
☐	0554	0.54 1.54 2.54 3.54	🟩 Operating	Online		Z15B-D126-J.00	FICON Express8S

Max Page Size: 500   Total: 140   Filtered: 140   Selected: 1

Figure C-19   Support Element CHPIDs work area

4. In CHPID Operations, click **Configure On/Off**.
5. In Configure On/Off window (Figure C-20 on page 182), the Status column shows the status of the channel for each logical partition.

> **Note**: The Standby state indicates an offline CHPID to the LPAR.

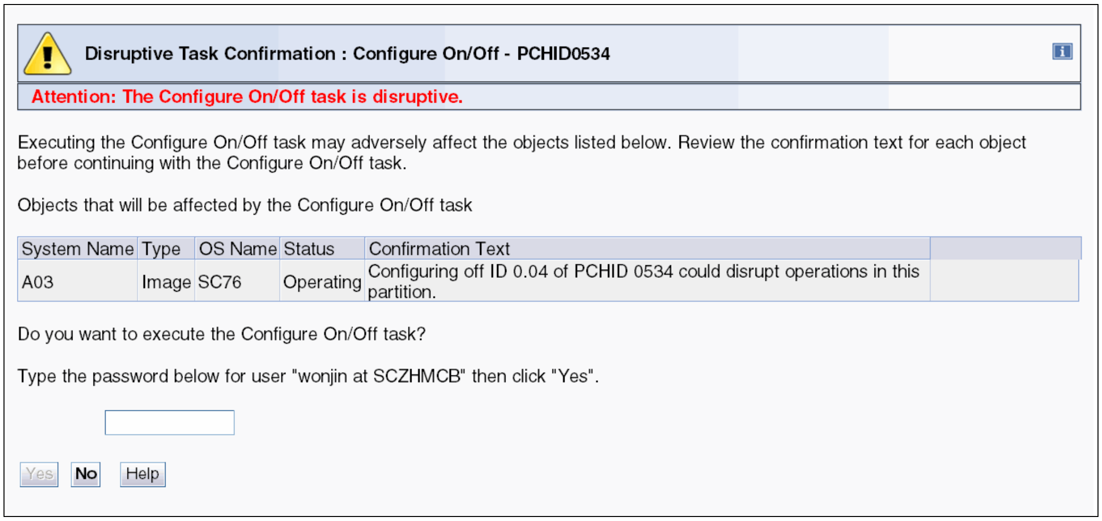
a. Read the warning information about configuring channels from the Support Element function rather than from an available operating system, and then type your password for confirmation.

   Toggle the CHPID if you cannot configure it offline and online from the operating system in each of the LPARs to which the CHPID is assigned.

   - If the channel should be set to Off for all partitions, use **Toggle all off**.
   - If the channel should be set to On for all partitions, use **Toggle all on**.
   - If the channel should *not* be changed in all partitions, then select the affected partitions. Clicking Toggle changes the state of the channel.

   > **Note:** Before you click **Apply** in the next step, ensure that only the CHPID or CHPIDs that you want toggled are highlighted.

b. In all cases, click **Apply** to immediately change the channel state to what you want.



Disruptive Task Confirmation : Configure On/Off - PCHID0534

Attention: The Configure On/Off task is disruptive.

Executing the Configure On/Off task may adversely affect the objects listed below. Review the confirmation text for each object before continuing with the Configure On/Off task.

Objects that will be affected by the Configure On/Off task

System Name	Type	OS Name	Status	Confirmation Text
A03	Image	SC76	Operating	Configuring off ID 0.04 of PCHID 0534 could disrupt operations in this partition.

Do you want to execute the Configure On/Off task?

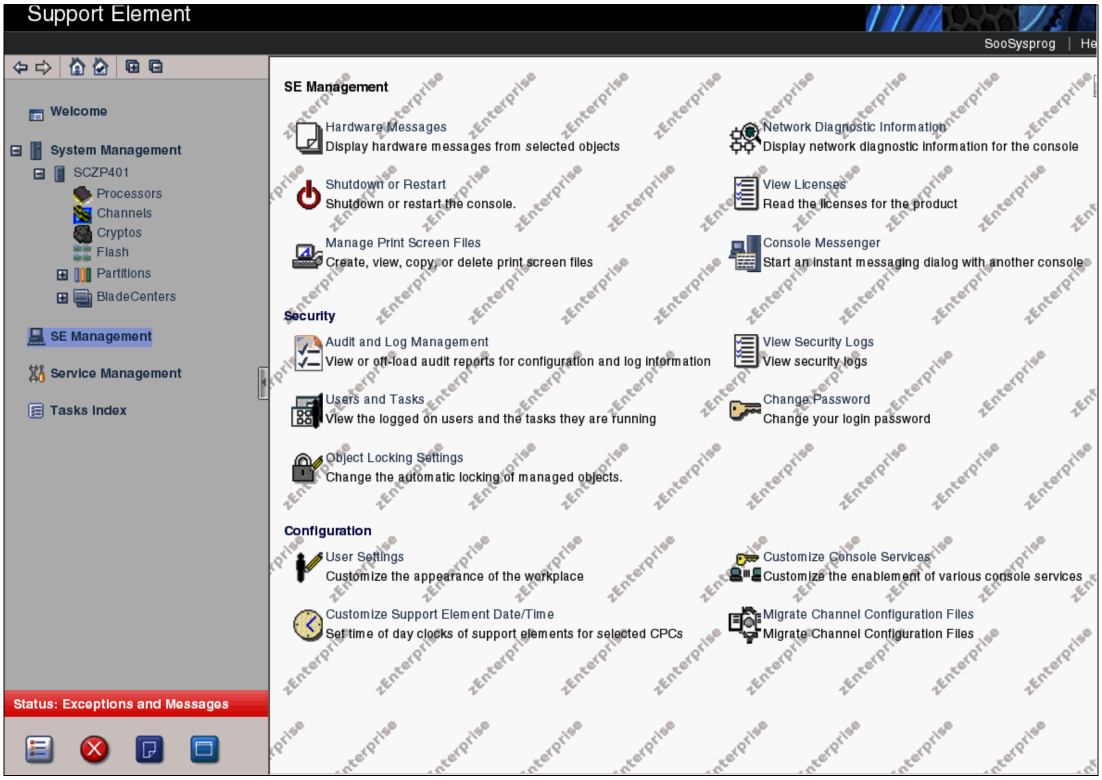
Type the password below for user "wonjin at SCZHMCB" then click "Yes".

Figure C-20 Configure On/Off window

6. The Configure On/Off Progress window briefly displays the `In progress` message. When the message changes to `Complete`, click **OK**.

Close the Support Element session

When the work with the channels is finished, click **Logoff** in the SE (Figure C-21) to end the Support Element session.



SE Management

Hardware Messages
Display hardware messages from selected objects

Network Diagnostic Information
Display network diagnostic information for the console

Shutdown or Restart
Shutdown or restart the console.

View Licenses
Read the licenses for the product

Manage Print Screen Files
Create, view, copy, or delete print screen files

Console Messenger
Start an instant messaging dialog with another console

Security

Audit and Log Management
View or off-load audit reports for configuration and log information

View Security Logs
View security logs

Users and Tasks
View the logged on users and the tasks they are running

Change Password
Change your login password

Object Locking Settings
Change the automatic locking of managed objects.

Configuration

User Settings
Customize the appearance of the workplace

Customize Console Services
Customize the enablement of various console services

Customize Support Element Date/Time
Set time of day clocks of support elements for selected CPCs

Migrate Channel Configuration Files
Migrate Channel Configuration Files

Figure C-21 Logging off from the Support Element

D

Useful setup and verification commands

This appendix lists the commands that we used to set up and verify the various local area network (LAN) environments that we describe in this book.

The information covers the following topics:

- “IBM z/OS commands” on page 184
- “z/VM commands” on page 186
- “Defining and coupling a NIC using CP commands” on page 187
- “Linux on System z TCP/IP commands” on page 188

IBM z/OS commands

We use the following IBM z/OS operating system commands in this publication. For a complete list and description of TCP/IP Console and TSO commands, see *IP Systems Administrator's Commands*, SC31-8781.

Table D-1 z/OS TCP/IP operator commands

Command	Description
D U,,,*dddd*[a],*nnn*	Gives the status of the device or devices
D U,,ALLOC,*dddd*,*nnn*[b]	Shows where the device or devices are allocated
D M=DEV(*dddd*)	Shows status of paths that are defined to a device
D M=CHP	Gives the status and type of all channel path identifiers (CHPIDs) that are defined to the z/OS
D M=CHP(*cc*[c])	Gives the status of the path to the defined devices
D A,L	Lists the jobs running in the system
D IOS,MIH	Missing-interrupt handler (MIH) values for all devices
SETIOS MIH,DEV=*dddd*,TIME=*mm:ss*	Sets the MIH time for a specified device
V *dddd-dddd*,ONLINE	Varies a device online
V *dddd-dddd*,OFFLINE	Varies a device offline
CF CHP(*cc*),ONLINE	Configures a CHPID online
CF CHP(*cc*),OFFLINE	Configures a CHPID offline
D TCPIP	Lists TCP/IP stacks that have started since the last initial program load (IPL) and stack status
D TCPIP,*tcpproc*,NETSTAT,ARP	Displays the contents of Address Resolution Protocol (ARP) cache for the TCP/IP stack
D TCPIP,*tcpproc*,NETSTAT,DEV	Shows the status of a device or devices or interface or interfaces that are defined in TCP/IP stack profile
D TCPIP,*tcpproc*,NETSTAT,HOME	Displays the home IP address or addresses that are defined in the TCP/IP stack profile
D TCPIP,*tcpproc*,NETSTAT,ND	Displays the contents of the IPv6 neighbor cache
D TCPIP,*tcpproc*,NETSTAT,ROUTE	Displays the routing information for the TCP/IP stack
D TCPIP,*tcpproc*,OSAINFO,INTFN=	Displays information for an active IPAQENET/IPAQENET6 interface.
V TCPIP,*tcpproc*,PURGECACHE,*linkname*	Purges ARP cache for the specified adapter (linkname or intfname [IPv6] from **NETSTAT,DEV**)
V TCPIP,*tcpproc*,START,*tcpipdev*	Starts a device or interface (IPv6) that is defined in a TCP/IP stack
V TCPIP,*tcpproc*,STOP,*tcpipdev*	Stops a device or interface (IPv6) that is defined in a TCP/IP stack

a. *dddd* indicates the device number.
b. *nnn* indicates the number of devices to be displayed.
c. *cc* indicates the CHPID number.

Table D-2 TCP/IP TSO commands

Command	Description
`NETSTAT ?`	Displays Netstat options
`NETSTAT ARP ALL`	Displays ARP cache
`NETSTAT DEV`	Displays the TCP/IP devices and links
`NETSTAT HOME`	Displays the TCP/IP Home IP addresses
`NETSTAT GATE`	Displays the TCP/IP Gateway addresses
`PING` *ipaddress*	Performs one PING to specified address
`TRACERTE` *ipaddress*	Traces router hops to a specified address
`OBEYFILE`	Executes selected TCP/IP profile statements

Table D-3 lists some of the Virtual Telecommunications Access Method (VTAM) commands in z/OS. For a complete list and description, see *SNA Operation*, SC31-8779.

Table D-3 VTAM commands

Command	Description
`D NET,VTAMOPTS`	Displays the current VTAM start options
`F` *vtamname*`,VTAMOPTS,` *optionname*=*value*	Modifies the current VTAM options (vtamname is the STC name; optionname is from VTAMOPTS.)
`D NET,MAJNODES`	Displays the VTAM major nodes
`D NET,ID=`*mnodename*`,E`	Displays information about a specified ID (for example, a Line, PU, or LU)
`D NET,TRL`	Displays the list of TRLEs
`D NET,TRL,TRLE=`*trlename*	Displays the status of a TRLE
`V NET,ID=ISTTRL,ACT,UPDATE=ALL`	Deletes inactive TRLEs from the TRL list
`V NET,ID=`*mnodename*`,ACT`	Activates a major node
`V NET,ID=`*mnodename*`,INACT`	Deactivates a major node

Important: If your static Transport Resource List Element (TRLE) definition is incorrect, remember that an active TRLE entry *cannot* be deleted. In such cases, you can use these steps:

1. Vary activate the TRL node with a blank TRLE to delete previous entries.
2. Code the correct TRL with correct TRLE entries and definitions.
3. *Vary* activate this corrected TRL and TRLE node.

z/VM commands

Tables Table D-4, Table D-5, and Table D-6 on page 187 list some of the central processor commands and TCP/IP commands in the IBM z/VM operating system. For information about other z/VM CP commands, see *z/VM CP Commands and Utilities Reference*, SC24-6175.

Table D-4 z/VM CP commands

Command	Description
`Q MITIME`	Displays MIH times for devices
`Q OSA ACTIVE|ALL`	Displays the status of Open Systems Adapter (OSA) devices
`Q` *rdev|rdev-rdev*	Displays the status of real devices
`Q PATHS` *rdev|rdev-rdev*	Displays the path status to real devices (PIM, PAM, LPM)
`Q CHPID` *cc*	Displays the real CHPID status
`SET MITIME` *rdev|rdev-rdev mm:ss*	Sets the MIH time for device or devices
`VARY OFF|ON` *rdev|rdev-rdev*	Varies devices online or offline
`VARY OFF|ON PATH` *cc* `FROM|TO` *rdev|rdev-rdev*	Changes the status of a path to devices
`VARY OFF|ON CHPID` *cc*	Configures a CHPID Off or On to both hardware and software

Table D-5 z/VM TCP/IP commands

Command	Description
`NETSTAT ?`	Displays **`NETSTAT`** options
`NETSTAT ARP`	Displays the Address Resolution Protocol (ARP) cache
`NETSTAT DEV`	Displays the TCP/IP devices and links
`NETSTAT HOME`	Displays the TCP/IP Home IP addresses
`NETSTAT GATE`	Displays the TCP/IP Gateway addresses
`NETSTAT OBEY START|STOP DEV`	Starts or stops the device name that is identified in **`NETSTAT DEV`** output
`IFCONFIG (z/VM6.3)`	Displays the TCP/IP devices and links (similar to the **`NETSTAT DEV`** command, but has other uses; see note)
`PING` *ipaddress*	Performs one **`ping`** to a specified address
`TRACERTE` *ipaddress*	Traces router hops to a specified address
`OBEYFILE`	Executes selected TCP/IP profile statements
Note: The IFCONFIG command can help to temporarily modify network interfaces in the current TCP/IP stack. See *z/VM TCP/IP Planning and Customization*, SC24-6238 for detailed uses. For more information about the other z/VM TCP/IP commands, see the *z/VM TCP/IP User's Guide*, SC24-6240.	

Table D-6 z/VM Virtual Switch CP commands

Command	Description
`DEFINE VSWITCH`	Defines the virtual switch and attributes
`DEFINE NIC`	Defines the simulated network interface card (NIC)
`COUPLE`	Helps to connect the NIC to the virtual switch
`SET VSWITCH`	Controls the attributes of an existing virtual switch
`QUERY CONTROLLER`	Displays the controller service machines
`QUERY VSWITCH`	Displays information about the virtual switch
`QUERY VSWITCH DETAILS`	Displays detail information about the virtual switch
`QUERY VSWITCH` *name* `ACCESS`	Displays authorized user IDs
`QUERY VMLAN`	Displays system-wide MAC addresses

Defining and coupling a NIC using CP commands

Tip: You may choose to use the **DEFINE NIC** and **COUPLE** approach rather than the NICDEF z/VM user directory statement. In this case, consider adding these two commands into your guest’s PROFILE EXEC file so they run automatically at IPL time or whenever the guest logs on.

To create a virtual NIC, use the following command syntax:

```
DEFINE NIC vdev [ operands ]
```

In this syntax, *vdev* specifies the base virtual device address for the adapter, and *operands* defines the characteristics of the virtual NIC. Operands accepted by the **DEFINE NIC** command are listed in Table D-7.

Table D-7 Operands for the DEFINE NIC command

Operands	Description
`TYPE`	This operand specifies the type of NIC adapter to be created, specifically the hardware and protocol that the adapter is to emulate. This is an optional keyword that you can specify with IBM HiperSockets or Queued Direct I/O (QDIO).
`HIPERsockets`	This operand defines this adapter as a simulated HiperSockets NIC. This adapter functions similar to the IBM HiperSockets internal adapter. A HiperSockets NIC can function without a z/VM guest LAN connection or can be coupled to a HiperSockets guest LAN.
`QDIO`	This operand defines this adapter as a simulated QDIO NIC. This adapter functions similarly to the OSA-Express (QDIO) adapter. A QDIO NIC is functional only when it is coupled to a QDIO guest LAN.
`IEDN`	This operand defines this adapter as a simulated intraensemble data network (IEDN) NIC. This adapter functions like an OSA-Express CHPID type OSX adapter (device model 1732-02) that is connected to an IEDN internal network that is managed by the Unified Resource Manager. An IEDN NIC is functional only when it is coupled to an IEDN virtual switch.

Operands	Description
`INMN`	This operand defines this adapter as a simulated intranode management network (INMN) NIC. This adapter functions like an OSA-Express CHPID type OSM adapter (device model 1732-03) that is connected an INMN internal network that is managed by the Unified Resource Manager. An INMN NIC is only functional when it is coupled to an INMN virtual switch.
`DEVices` *`devs`*	This determines the number of virtual devices that are associated with this adapter. For a simulated HiperSockets adapter, *devs* must be a decimal value between 3 and 3072 (inclusive). For a simulated QDIO, IEDN, or INMN adapter, *devs* must be a decimal value between 3 and 240 (inclusive). The **`DEFINE NIC`** command creates a range of virtual devices from *vdev* to *vdev + devs -1* to represent this adapter in your virtual machine. The default value is 3.
`CHPID` *`nn`*	A two-digit hexadecimal number that represents the CHPID number that the invoker wants to allocate for this simulated adapter. If the requested CHPID number is available, all of the virtual devices that belong to this adapter share the same CHPID number. This option is useful only if you need to configure a virtual environment with predictable CHPID numbers for your simulated devices.

After the NIC is installed, use the **`COUPLE`** CP command to connect the adapter to a guest LAN or virtual switch. This is the syntax of the **`COUPLE`** command for this scenario:

```
COUPLE vdev TO [ operands ]
```

In this syntax, *vdev* specifies the base virtual device address for the adapter, and *operands* defines where to connect the NIC. Table D-8 lists the operands that are accepted by the **`COUPLE`** command for the purpose of connecting a virtual NIC to a guest LAN.

Table D-8 Operands for the Couple command

Operands	Description
vdev	This is the base address (hex) of the network adapter.
ownerid lanname	The *ownerid* is the name of the owner of the guest LAN (such as SYSTEM). The *lanname* is the name of the guest LAN.

Remember that a virtual NIC can be coupled only to a *compatible* guest LAN. For example, a QDIO NIC cannot be coupled to a guest LAN of type HiperSockets.

For Red Hat Enterprise Linux systems, after you define the virtual NICs and couple it to a vswitch, you need to use the following syntax to issue **`cio_ignore`** command to remove the network channels from the list of ignored devices and make them visible to Linux:

```
cio_ignore -r read_device_bus_id,write_device_bus_id,data_device_bus_id
```

Replace *read_device_bus_id*,*write_device_bus_id*,*data_device_bus_id* with the three device bus IDs that represent network devices. For our example, the *read_device_bus_id* is `0.0.8000`, the *write_device_bus_id* is `0.0.8001`, and the *data_device_bus_id* is `0.0.8002`, so the command looks like this:

```
cio_ignore -r 0.0.8000,0.0.8001,0.0.8002
```

Linux on System z TCP/IP commands

When using the Linux commands listed in Table D-9, enter them in lowercase, as shown.

Table D-9 TCP/IP commands

Command	**Description**
arp	Displays ARP cache; use -? for options
dmesg | more	Display device assignments (and more) at kernel initialization
netstat -i	Displays an interface table
netstat -r	Displays host routes
ifconfig	Displays network interfaces (L0, eth0, tr0, and so on)
ifconfig interface up|down	Starts or stops a network interface
ping *hostnamelipaddress*	Performs one **ping** to a specified address
route	Displays routes
traceroute *hostnamelipaddress*	Traces router hops to a specified address

E

Using the Open Systems Adapter Support Facility

The Open Systems Adapter Support Facility (OSA/SF) is an application that helps you to customize and manage your OSA features. You can also use it to get status and operational information about the OSA ports that are defined in the Hardware Control Definition (HCD), which helps you in problem determination.

Note: This operating system-based version of OSA/SF does not support OSA-Express5S or newer devices. For information on those, see *Open Systems Adapter/Support Facility on the Hardware Management Console*, SC14- 7580.

OSA/SF includes a graphical user interface (GUI) and a Restructured Extended Executor (REXX) interface. The OSA/SF GUI runs on the Microsoft Windows 7 and Linux software platforms that have graphics and Java 1.6 support. For more information about using the REXX interface, see Appendix F, “Using the OSA/SF operating system-based interface” on page 211.

From a single OSA/SF GUI, you can establish connections to all server images (logical partitions (LPARs)) that have OSA/SF running. You do not need to have OSA/SF running on each server image. This gives you centralized control of OSA features that span server boundaries, as shown in Figure E-1 on page 192. You can have GUI instances in each server image that has OSA/SF, so you can monitor your OSA features locally.

This chapter provides instructions to help you set up and use OSA/SF. It covers the following topics:

- “Setup requirements and overview” on page 192
- “Setting up OSA/SF in the z/OS environment” on page 193
- “Installing OSA/SF GUI on a workstation” on page 195
- “Using the OSA/SF GUI” on page 197

Setup requirements and overview

OSA/SF is *required* when the OSA feature is configured for shared non-Queued Direct I/O (non-QDIO) mode and Systems Network Architecture/Advanced Peer-to-Peer Networking/High-Performance Routing (SNA/APPN/HPR) definitions, other than for Enterprise Extender (EE).

OSA/SF is not required for OSA features that are configured in QDIO mode or when the default IP Passthru (non-QDIO mode) is used. However, it is very useful for monitoring, problem determination, and simple performance analysis.

Note: OSA/SF is not supported on CHPID types OSC, OSM, and OSX.

Figure E-1 shows the communication path between the user interfaces and OSA features.

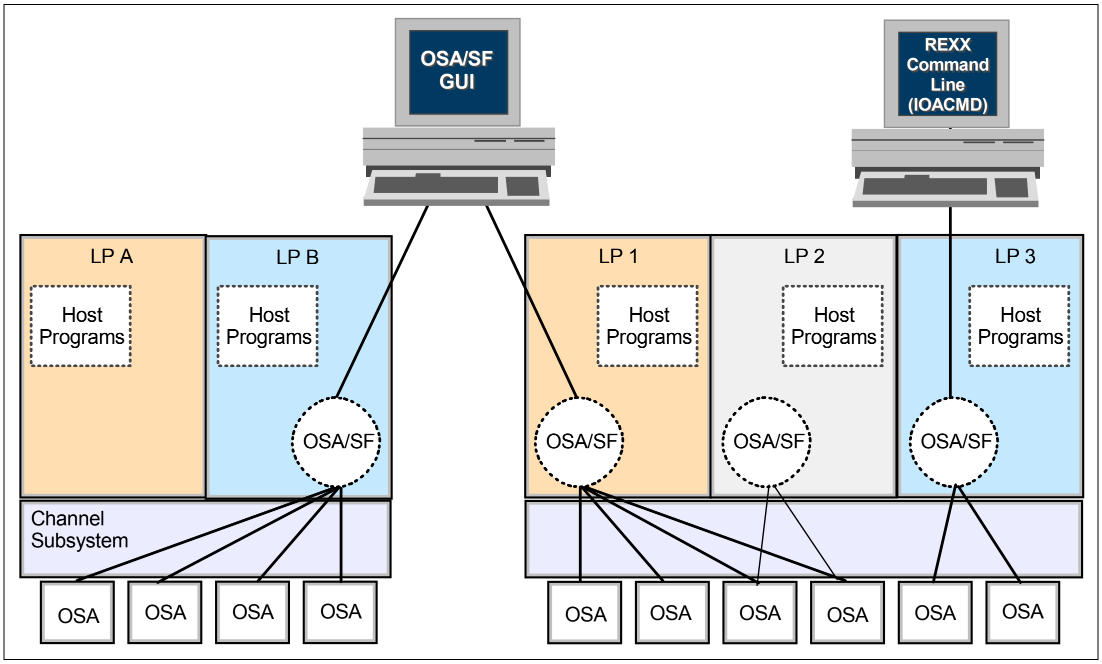


Figure E-1 OSA/SF communication path

This integrated version of OSA/SF is applicable to the in-service releases of IBM z/OS, IBM z/VM, and IBM z/VSE operating systems.

In the z/OS environment, the integrated version of OSA/SF can coexist with OSA/SF 2.1 and does not overlay it. The integrated version of OSA/SF for z/VM 5.4 replaces OSA/SF 2.1. In currently supported versions or releases of z/VM and z/VSE, this version is delivered as a program temporary fix (PTF) and overlays OSA/SF 2.1. The OSA/SF GUI supports only TCP/IP connections.

The OSA/SF GUI is common across z/OS, z/VM, and z/VSE operating systems. You can find examples of how the GUI is used in “Using the OSA/SF GUI” on page 197.

In addition to this book, you can find information about how to set up OSA/SF on z/OS, z/VM, and z/VSE in the *Open Systems Adapter-Express Customer's Guide and Reference*, SA22-7935.

There is also a version of OSA/SF that runs on the Hardware Management Console (HMC). It is exclusive to the IBM zEnterprise EC 12 (zEC12) and IBM zEnterprise BC 12 (zBC12) systems. The latest driver is *required*.

OSA/SF on the HMC is required for the OSA-Express5S features. Either OSA/SF on the HMC or the OSA/SF operating system component can be used for the OSA-Express4S features. The OSA/SF operating system component must be used for the OSA-Express3 features.

OSA/SF on the HMC can be used to configure CHPID type OSE. It can also be used to manage (query or display) CHPID types OSD, OSE, and OSN.

If you need more information about OSA/SF on the HMC, see *Open Systems Adapter/Support Facility on the Hardware Management Console*, SC14-7580.

Setting up OSA/SF in the z/OS environment

This section explains how to set up OSA/SF on the z/OS operating system. For information about setting up OSA/SF on z/VM or z/VSE systems and for access control to OSA/SF through Resource Access Control Facility (RACF), see *Open Systems Adapter-Express Customer's Guide and Reference*, SA22-7935.

Reminder: The OSAD device must be defined in the Hardware Configuration Definition (HCD) or input/output configuration program (IOCP) to the OSA CHPID for OSA/SF-to-OSA communication to work. For an HCD setup example, see 3.2.4, "Generating the IOCDS input from the HCD" on page 27. For an IOCDS input example, see Figure 3-1 on page 16.

Set up APPC and VTAM

Before using OSA/SF to manage your OSA features, you must configure Advanced Program-to-Program Communication (APPC) communication, regardless of the connection type used. We used the following steps to set up the APPC environment:

1. Define the Virtual Telecommunications Access Method (VTAM) APPL statement for OSA/SF. In our example, we create VTAM major node member `APPCOSA` in the `SYS1.VTAMLST` and add the statements shown in Example E-1.

   Example E-1 APPCOSA from SYS1.VTAMLST

   ```
   IOASERV  APPL  ACBNAME=IOASERV,                                   X
                  APPC=YES,AUTOSES=0,DDRAINL=NALLOW,                 X
                  DMINWNL=5,DMINMNR=5,DRESPL=NALLOW,                 X
                  DSESLIM=10,LMDENT=19,MODETAB=MTAPPC
   ```

2. Define an APPC local LU for OSA/SF by editing member `APPCPMxx` in the `SYS1.PARMLIB` and adding the statements that are shown in Example E-2 on page 194.

   Note: There is no dependency on the APPC scheduler for OSA/SF.

Example E-2 APPCPM00 from SYS1.PARMLIB

```
LUADD ACBNAME(IOASERV)     /* Specify the name of the LU to be    */
                           /* added                               */
      NOSCHED              /* Specify that the APPC/MVS           */
                           /* transaction scheduler is associated */
                           /* with this LU name                   */
      TPDATA(SYS1.APPCTP)  /* Specify that VSAM data set          */
                           /* SYS1.APPCTP is the permanent        */
                           /* repository for the TP profiles      */
                           /* for this LU                         */
```

> **Note:** `SYS1.APPCTP` is a VSAM data set. It must be allocated by using job `ATBTPVSM`, which is included in `SYS1.SAMPLIB`.

3. Add the `APPC` procedure to the `SYS1.PROCLIB`, as shown in Example E-3.

Example E-3 APPC from SYS1.PROCLIB

```
//APPC PROC APPC=00
//APPC EXEC PGM=ATBINITM,PARM='APPC=&APPC',REGION=0K
```

4. For automatic startup of the APPC environment, add the parameters that are shown in Example E-4 to your `COMMNDxx` member of `SYS1.PARMLIB`.

Example E-4 COMMND00 from SYS1.PARMLIB

```
COM='S APPC,SUB=MSTR'
```

Set up OSA/SF

To set up OSA/SF, use the following steps:

1. Create a started task (STC):
   a. Copy the sample procedure from `IOA.SIOASAMP(IOAOSASF)` to `SYS1.PROCLIB`.
   b. Edit the procedure and change the name to `OSASF`.
   c. Verify that the data set names in the `STEPLIB` and `IOALIB` DD statements match your environment.
2. Create a startup profile for OSA/SF:
   a. Allocate a sequential data set.
   b. Copy the sample that is provided in `IOA.SIOASAMP(IOASPROF)` into the sequential data set that you allocated before.
   c. Edit the profile and change `SYSNAME` and `CECNAME` to suit your installation (verify `UNIT` and `VOLSER`).
3. Set up the OSA configuration and master profile:
   a. Allocate sequential data set `IOA.&CECNAME.OSAS.CONFIG`, and copy the sample that is provided in `IOA.SIOASAMP(IOACFG)` into it.
   b. Allocate sequential data set `IOA.&CECNAME.MASTER.INDEX`, and copy the sample in `IOA.SIOASAMP(IOAINX)` into it.
4. Set up a REXX executable data set for use under TSO. Copy member `IOACMD` from `IOA.SIOASAMP` to your local lists or executable data sets.

5. To start the APPC and OSASF procedure, issue the following commands from the System Display and Search Facility (SDSF) log:

```
/s appc,sub=mstr
/s osasf
```

Communicate with OSA/SF by using TCP/IP

We used TCP/IP as the connection type for communicating with OSA/SF from a workstation. To set up TCP/IP, we performed the following steps:

1. Update the TCP/IP profile with the following data.
   a. Add the server to the AUTOLOG statement, as shown in Example E-5.

Example E-5 IOASRV from TCP/IP profile

```
 AUTOLOG
   .
   IOASRV
   .
```

   b. Add the port statement, as shown in Example E-6.

Example E-6 Port number from TCP/IP profile

```
PORT
.
2000 TCP IOASRV             ; OSA/SF Server
.
```

2. Create a procedure in SYS1.PROCLIB(IOASRV), as shown in Example E-7.

Example E-7 IOASRV from SYS1.PROCLIB

```
//IOASRV   PROC
//IOASRV   EXEC PGM=IOAXTSRV,PARM='2000',REGION=0M,TIME=NOLIMIT
//STEPLIB  DD  DISP=SHR,DSN=SYS1.SIOALMOD
//IOALIB   DD  DISP=SHR,DSN=SYS1.SIOALMOD
//SYSTCPD  DD  DISP=SHR,DSN=SYS1.TCPPARMS(PROF&SYSCLONE.)
//SYSPRINT DD  SYSOUT=*,DCB=(RECFM=FBA,LRECL=121,BLKSIZE=121)
//*SYSUDUMP DD  SYSOUT=*
```

3. Restart TCP/IP or use the **obeyfile** TCP/IP subcommand to make these modifications active.

Installing OSA/SF GUI on a workstation

We used the following steps to install and set up the OSA/SF GUI on a Microsoft Windows workstation after we installed and set up OSA/SF on the host system.

Check the hardware configuration

To use the OSA/SF GUI interface, a workstation with the following minimum hardware features is required:

- A Pentium 200 MHz (or equivalent) with 32 MB of RAM
- An SVGA display with a resolution of 1024 by 768 with 16-bit colors
- A communications adapter that supports the TCP/IP communications protocol

Check the software configuration

To use the GUI with z/OS, z/VM, or z/VSE software, you must have a workstation with either of the following versions:

- Microsoft Windows or Windows 8, plus these elements:
  - A IP network connection
  - Java 1.4 or later
  - JavaHelp 1.1.2 or later
- Linux kernel Version 2.4 or later with these elements:
  - A IP network connection
  - Java 1.4 or later
  - JavaHelp 1.1.2 or later

Download and install the Java runtime and JavaHelp files

Follow the installation instructions for downloading the latest Java runtime files (Java 1.4 or later) and JavaHelp files (JavaHelp 1.1.2 or later) from the Internet.

Download the code from z/OS by using FTP

Before you download the `IOAJAVA` GUI code, create a directory on your Windows workstation where you can place the code for the GUI (`ioajava.jar`).

To download the OSA/SF GUI to the workstation, follow these steps:

1. Open a DOS (command prompt) session on your workstation.
2. Change to the directory where you want the executable file stored by using **cd** command.
3. Enter the FTP command, using the IP address of your host (for example, `ftp 192.168.14.32`) or the hostname if a hostname resolution technique has been set up in your environment.
4. Enter your user ID and password.
5. Enter the following command to set the FTP transfer to binary:

   ```
   bin
   ```

6. Enter the following command (the z/OS data set name in single quotes):

   ```
   cd ‘ioa.sioajava’
   ```

7. Enter the following command:

   ```
   get ioajava ioajava.jar
   ```

8. When the download has completed successfully, enter the **bye** command.

Define the CLASSPATH environment variable

After you download the GUI code, define the `CLASSPATH` environment variable for Windows.

1. In Windows, go to the Control Panel, and double-click **System**.
2. In the System Properties window, click the **Advanced** tab. In that window, click **Environment Variables**.
3. In the Environment Variables window, define the `CLASSPATH` environment variable for Windows. Select **CLASSPATH** and click **Edit**. If you do not find `CLASSPATH` listed, click **New** to create it.
   a. For CLASSPATH Variable Value, specify the directories where you stored the Java help files *and* the OSA/SF GUI code that you transferred, separated by a semicolon. For example, you might have the following CLASSPATH definitions for Variable Value:

   ```
   C:\Program Files\Java\jh2.0\javahelp\lib\jh.jar;C:\Documents and
   Settings\Administrator\osasf\ioajava.jar
   ```

   b. If you are creating this variable, specify `CLASSPATH` for Variable Name.

   c. Click **OK**.

Start the OSA/SF GUI

Complete the following actions before you start the GUI:

1. Set up an OSA/SF GUI TCP/IP connection for your workstation.
2. Start an OSA/SF `IOASRV` task on the host system.

To start the GUI on a Microsoft Windows system, and follow these steps:

1. Open a new **Command Prompt** (DOS) window.
2. Change to the directory where the `ioajava` code resides.
3. Enter the following command from the C:\> command prompt:

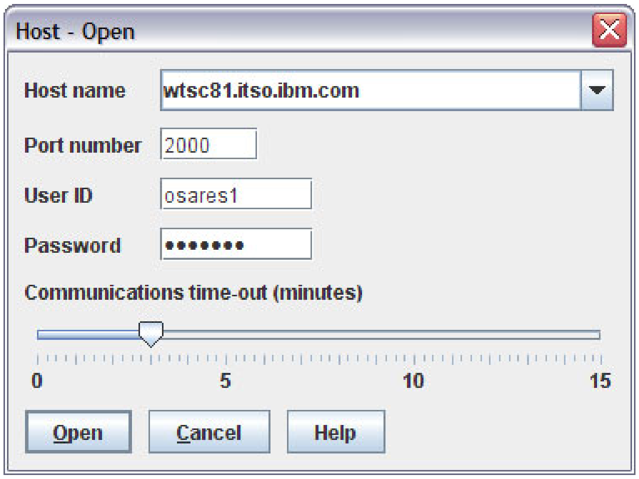
   ```
   java ioajava
   ```

Using the OSA/SF GUI

After you complete the steps for setting up the OSA/SF GUI, you can use the command windows to configure an OSA channel path identifier (CHPID). The Help panels that are part of the GUI provide information for each window.

> **Note:** This appendix uses the steps from the previous version of this book, because they have not changed. Also, this GUI is optional for OSA-Express4S and does not work for OSA-Express5S, both of which use the HMC version.

The Host - Open window (Figure E-2 on page 198) allows you to connect to the OSA/SF host. When you start the OSA/SF GUI, enter the name of the OSA/SF host system. Although the window allows access to only a single host system, you can open multiple windows on your workstation for other host systems.


Host - Open

Host name: wtsc81.itso.ibm.com

Port number: 2000

User ID: osares1

Password: •••••••

Figure E-2 OSA/SF Host - Open logon

OSA/SF Commands entries

The following sequence explains how to access the OSA/SF Commands window by using the Host - Open window. It also explains the functions that you can perform from the OSA/SF Commands window.

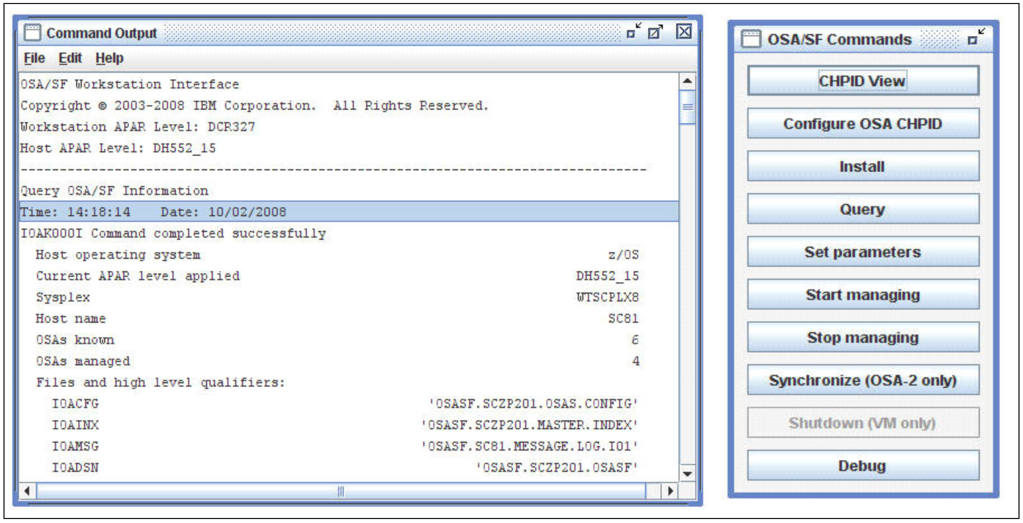
1. In the Host - Open window (Figure E-2), complete these tasks:
   a. Enter the following information:
      - Host name or IP address of the host system
      - Port as specified in the TCP/IP profile (see Example E-6 on page 195)
      - User ID and password for the system

   b. Click **Open**.

When the connection is established, you see the Workstation Interface window (Figure E-3 on page 199). Two panels open when the interface is displayed:

- Command Output: This panel shows the result of any command that you entered.
- OSA/SF Commands: This GUI is where you enter most REXX commands.

2. Click **CHPID View**.

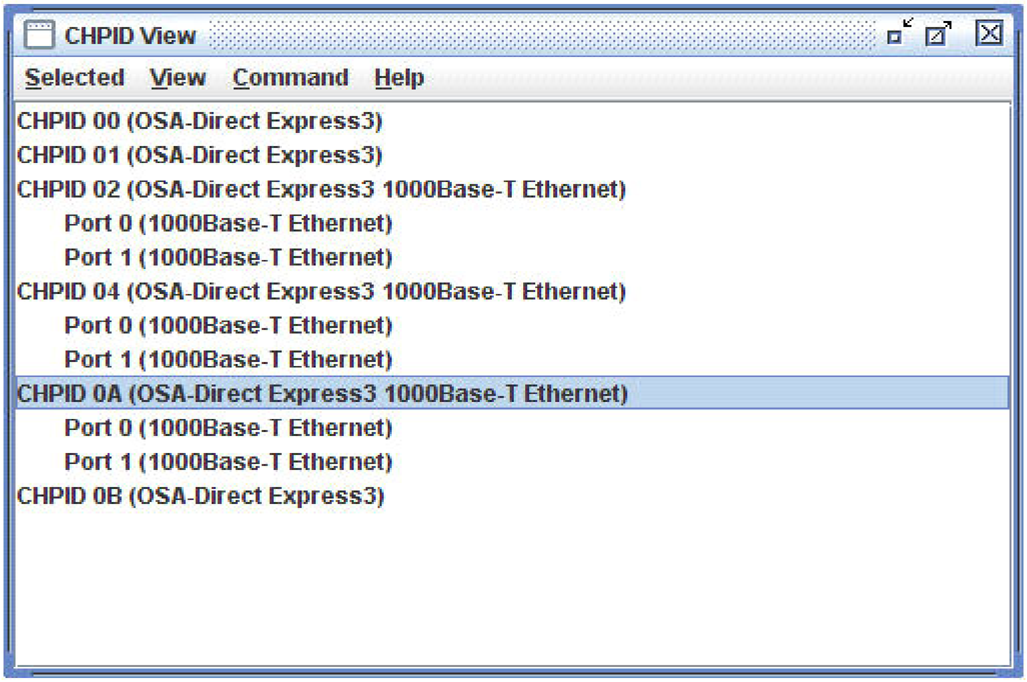


```
OSA/SF Workstation Interface
Copyright © 2003-2008 IBM Corporation.  All Rights Reserved.
Workstation APAR Level: DCR327
Host APAR Level: DH552_15
-------------------------------------------------------------------------------
Query OSA/SF Information
Time: 14:18:14    Date: 10/02/2008
IOAK000I Command completed successfully
  Host operating system                                                    z/OS
  Current APAR level applied                                           DH552_15
  Sysplex                                                              WTSCPLX8
  Host name                                                                SC81
  OSAs known                                                                  6
  OSAs managed                                                                4
  Files and high level qualifiers:
    IOACFG                                       'OSASF.SCZP201.OSAS.CONFIG'
    IOAINX                                      'OSASF.SCZP201.MASTER.INDEX'
    IOAMSG                                      'OSASF.SC81.MESSAGE.LOG.IO1'
    IOADSN                                             'OSASF.SCZP201.OSASF'
```

Figure E-3 OSA/SF Workstation Interface window

3. When the CHPID View window opens, it shows the CHPIDs that are managed by OSA/SF. Select the one that you want to work with.

   For our example, we double-clicked **CHPID 0A** (highlighted in (Figure E-4).



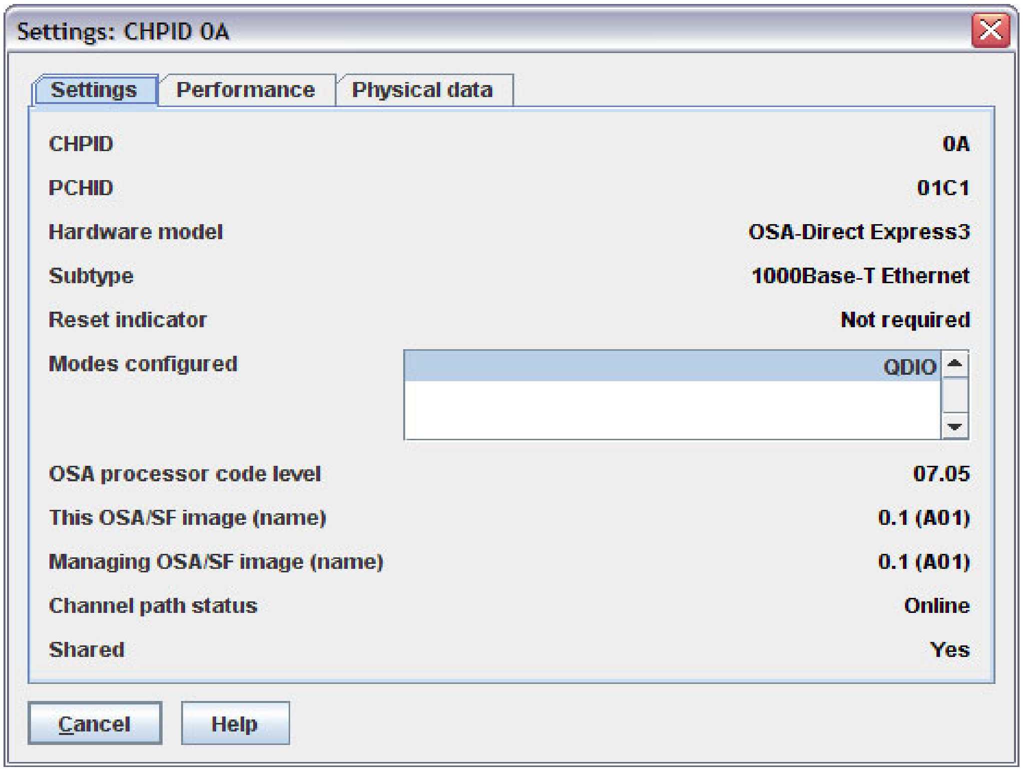
```
CHPID 00 (OSA-Direct Express3)
CHPID 01 (OSA-Direct Express3)
CHPID 02 (OSA-Direct Express3 1000Base-T Ethernet)
    Port 0 (1000Base-T Ethernet)
    Port 1 (1000Base-T Ethernet)
CHPID 04 (OSA-Direct Express3 1000Base-T Ethernet)
    Port 0 (1000Base-T Ethernet)
    Port 1 (1000Base-T Ethernet)
CHPID 0A (OSA-Direct Express3 1000Base-T Ethernet)
    Port 0 (1000Base-T Ethernet)
    Port 1 (1000Base-T Ethernet)
CHPID 0B (OSA-Direct Express3)
```

Figure E-4 CHPID view

Now you see the settings for that CHPID, shown in Figure E-5 on page 200. This window shows, among others things, the following information:

- The physical channel path identifier (PCHID) related to CHPID (in our example, 1C1)
- The hardware model of OSA (in our example, an OSA-Express3)
- The type of OSA (in our case, 1000BASE-T Ethernet)
- The mode that is configured (in our example, QDIO)
- The OSA processor code level (in our example, 07.05)
- The Channel Path status (in our example, the OSA CHPID is online)

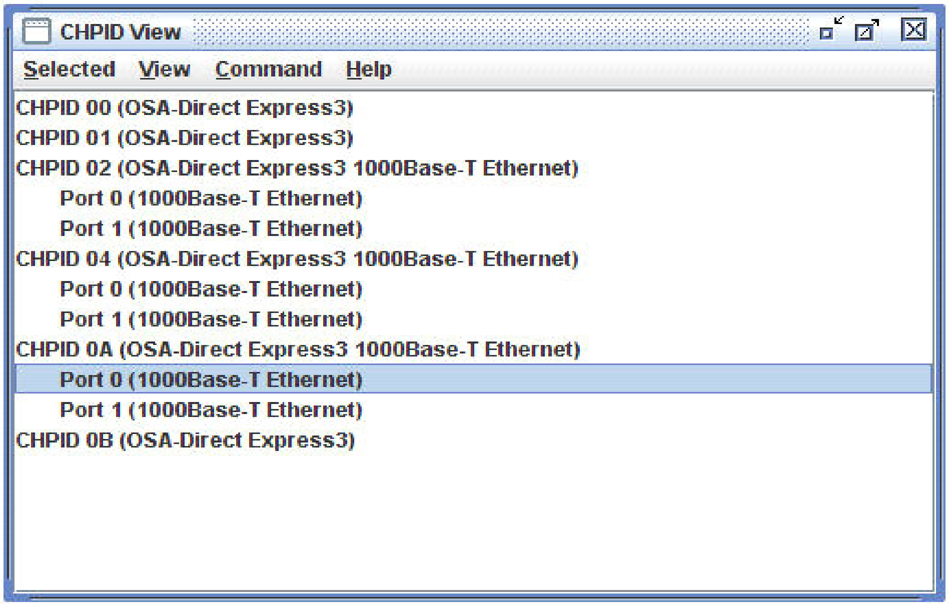
4. Return to the CHPID View window.



CHPID	0A
PCHID	01C1
Hardware model	OSA-Direct Express3
Subtype	1000Base-T Ethernet
Reset indicator	Not required
Modes configured	QDIO
OSA processor code level	07.05
This OSA/SF image (name)	0.1 (A01)
Managing OSA/SF image (name)	0.1 (A01)
Channel path status	Online
Shared	Yes

Figure E-5 CHPID settings

5. For our example, we double-clicked **Port 0** for CHPID 0A, as shown in Figure E-6 on page 201.



CHPID 00 (OSA-Direct Express3)
CHPID 01 (OSA-Direct Express3)
CHPID 02 (OSA-Direct Express3 1000Base-T Ethernet)
    Port 0 (1000Base-T Ethernet)
    Port 1 (1000Base-T Ethernet)
CHPID 04 (OSA-Direct Express3 1000Base-T Ethernet)
    Port 0 (1000Base-T Ethernet)
    Port 1 (1000Base-T Ethernet)
CHPID 0A (OSA-Direct Express3 1000Base-T Ethernet)
    Port 0 (1000Base-T Ethernet)
    Port 1 (1000Base-T Ethernet)
CHPID 0B (OSA-Direct Express3)

Figure E-6 CHPID View

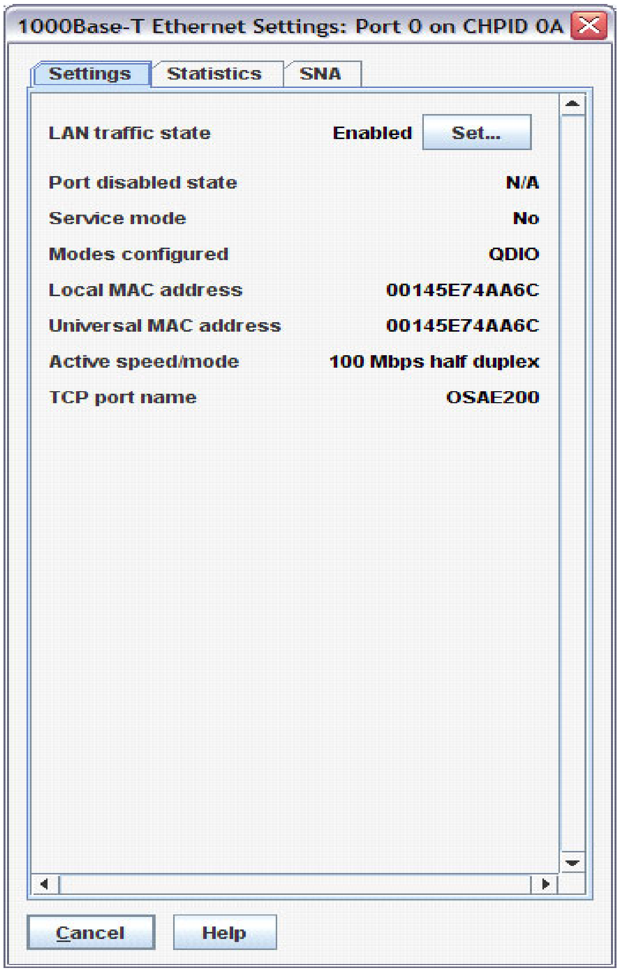
Note: As shown in Figure E-6, CHPID 0A has two OSA ports, Port 0 and Port 1.We have OSA-Express 1000BASE-T cards installed. Those features are 4-port dual-density cards and allow the configuration and operating of two ports per CHPID.

Now you see the settings that are shown in Figure E-7 on page 202. This window shows the following information:

- The LAN traffic state (enable)
- The MAC address
- The active speed mode (100 Mbps)
- The TCP port name (OSAE200)

Note: The reason that this window shows a speed of 100 Mbs is that this is the maximum speed that our switch supports. Both the OSA port and the switch negotiate the speed according to their attributes.

6. To view the packets that are transmitted and received and the error counters, select the **Statistics** tab.

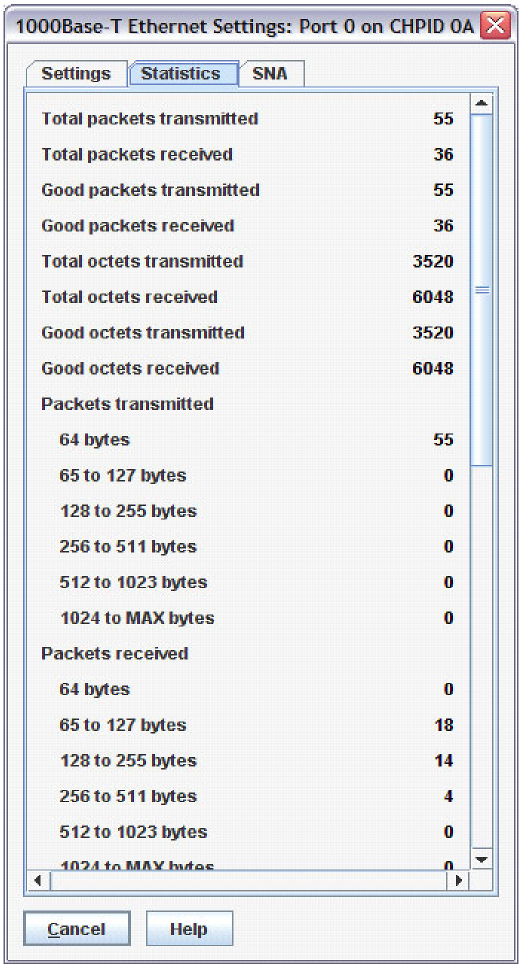


LAN traffic state	Enabled
Port disabled state	N/A
Service mode	No
Modes configured	QDIO
Local MAC address	00145E74AA6C
Universal MAC address	00145E74AA6C
Active speed/mode	100 Mbps half duplex
TCP port name	OSAE200

Figure E-7 Port settings

7. Figure E-8 on page 203 shows the details of the Statistics tab. Use the scroll bar to see more statistics.

> **Note:** The SNA tab is not applicable in QDIO mode.



Total packets transmitted	55
Total packets received	36
Good packets transmitted	55
Good packets received	36
Total octets transmitted	3520
Total octets received	6048
Good octets transmitted	3520
Good octets received	6048
Packets transmitted	
64 bytes	55
65 to 127 bytes	0
128 to 255 bytes	0
256 to 511 bytes	0
512 to 1023 bytes	0
1024 to MAX bytes	0
Packets received	
64 bytes	0
65 to 127 bytes	18
128 to 255 bytes	14
256 to 511 bytes	4
512 to 1023 bytes	0
1024 to MAX bytes	0

Figure E-8 Port Statistics tab

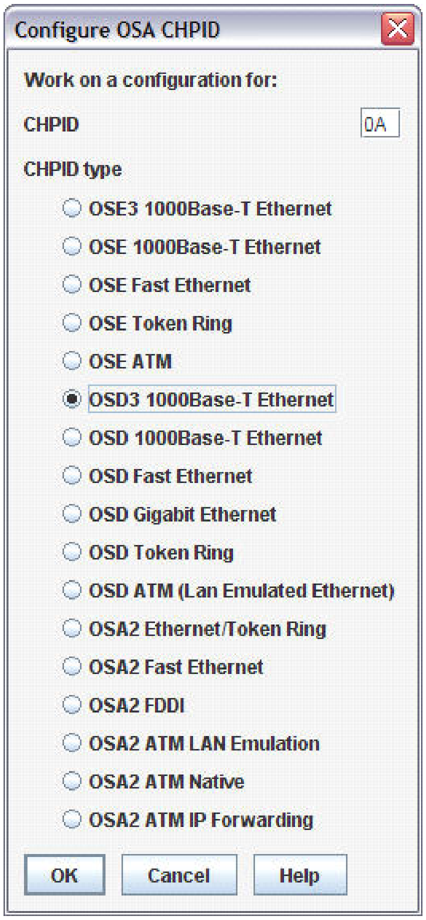
8. From the OSA/SF Commands panel that is shown in Figure E-3 on page 199, select **Configure OSA CHPID**.

9. In the Configure OSA CHPID window shown in Figure E-9, complete the following steps:

   a. Type the CHPID number. In our case, that is `0A`.

   b. Select the proper CHPID type. For our example, we choose **OSD3 1000Base-T Ethernet** because we are using an OSA-Express3 1000BASE-T card configured in QDIO mode.

   c. Press **ENTER**.



Configure OSA CHPID

Work on a configuration for:

CHPID 0A

CHPID type

○ OSE3 1000Base-T Ethernet
○ OSE 1000Base-T Ethernet
○ OSE Fast Ethernet
○ OSE Token Ring
○ OSE ATM
● OSD3 1000Base-T Ethernet
○ OSD 1000Base-T Ethernet
○ OSD Fast Ethernet
○ OSD Gigabit Ethernet
○ OSD Token Ring
○ OSD ATM (Lan Emulated Ethernet)
○ OSA2 Ethernet/Token Ring
○ OSA2 Fast Ethernet
○ OSA2 FDDI
○ OSA2 ATM LAN Emulation
○ OSA2 ATM Native
○ OSA2 ATM IP Forwarding

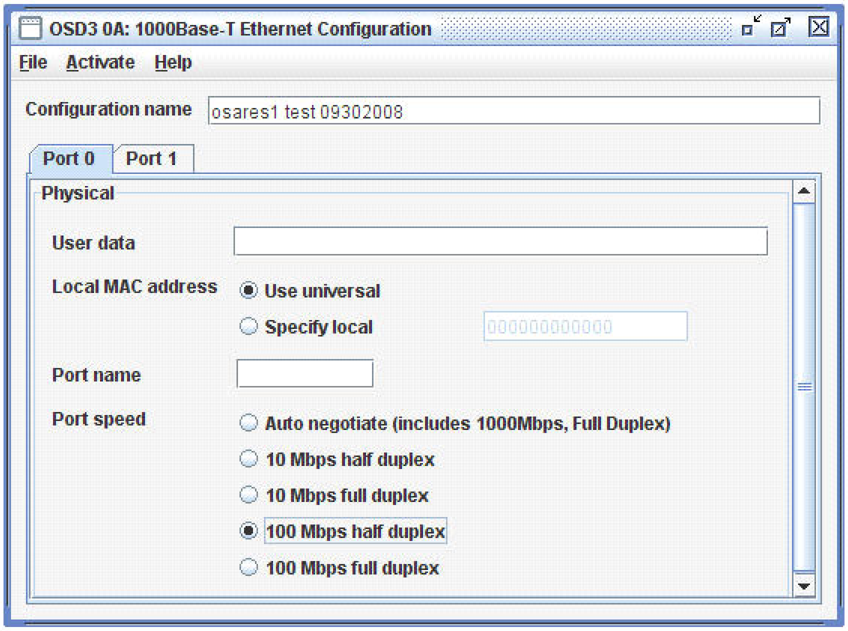
Figure E-9 Configure OSA CHPID

   d. Here you can apply changes for the configuration of CHPID 0A, as shown in Figure E-10 on page 205.

> **Note:** When configuring or changing OSA-Express3 features with four ports, make sure that you select the correct port in the CHPID (such as Port 0 or Port 1).

For example, you could choose these actions:

- Select **Specify local** (address) rather than the universal MAC.
- Change the LAN speed from 100 Mbps full duplex to 100 Mbps half duplex.



OSD3 0A: 1000Base-T Ethernet Configuration

Configuration name: osares1 test 09302008

Physical

User data:

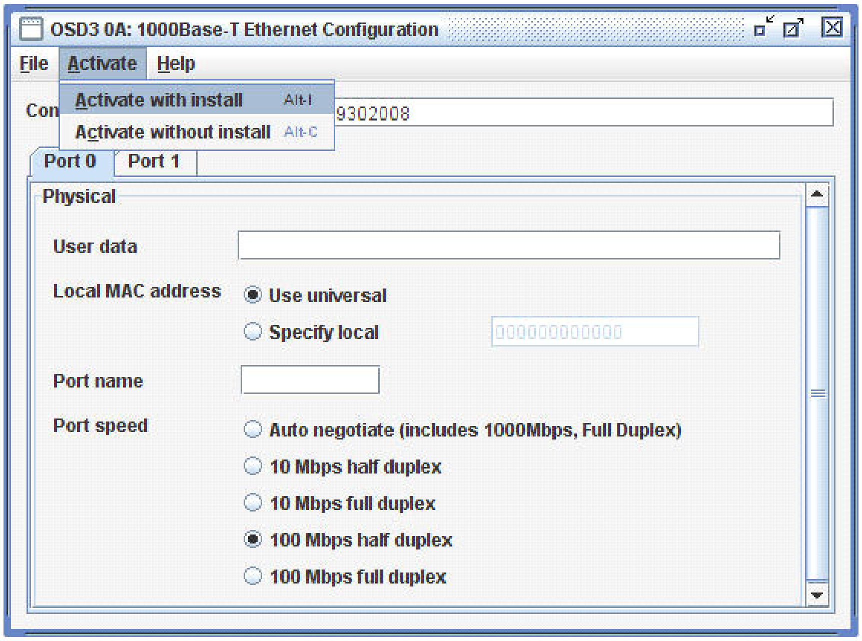
Local MAC address: ● Use universal ○ Specify local 000000000000

Port name:

Port speed:
○ Auto negotiate (includes 1000Mbps, Full Duplex)
○ 10 Mbps half duplex
○ 10 Mbps full duplex
● 100 Mbps half duplex
○ 100 Mbps full duplex

Figure E-10 1000Base-T Ethernet Configuration settings

10. Save your changes now by selecting **File** and then **Save Configuration**.
11. To perform the initial configuration, select **Activate with install** as shown in Figure E-11.



OSD3 0A: 1000Base-T Ethernet Configuration

Con 9302008

Physical

User data:

Local MAC address: ● Use universal ○ Specify local 000000000000

Port name:

Port speed:
○ Auto negotiate (includes 1000Mbps, Full Duplex)
○ 10 Mbps half duplex
○ 10 Mbps full duplex
● 100 Mbps half duplex
○ 100 Mbps full duplex

Figure E-11 Activate 1000BASE-T Ethernet configuration

Note: The `Install` command, from the OSA/SF Commands panel (Figure E-3 on page 199), can be used to load an existing configuration onto an OSA when you replace the OSA feature. It is *not* for the initial installation of an OSA feature.

12. Back in the OSA/SF Commands display (Figure E-3 on page 199), select **Query**.

13. You can use the Query window (Figure E-12) to display various information. Type the CHPID number (for our example, `0A`), and then select **One OSA**.

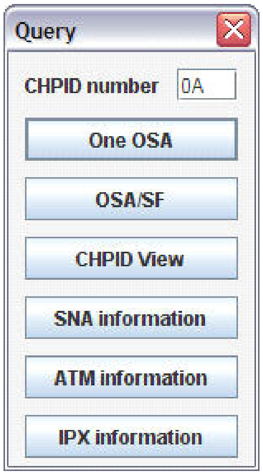
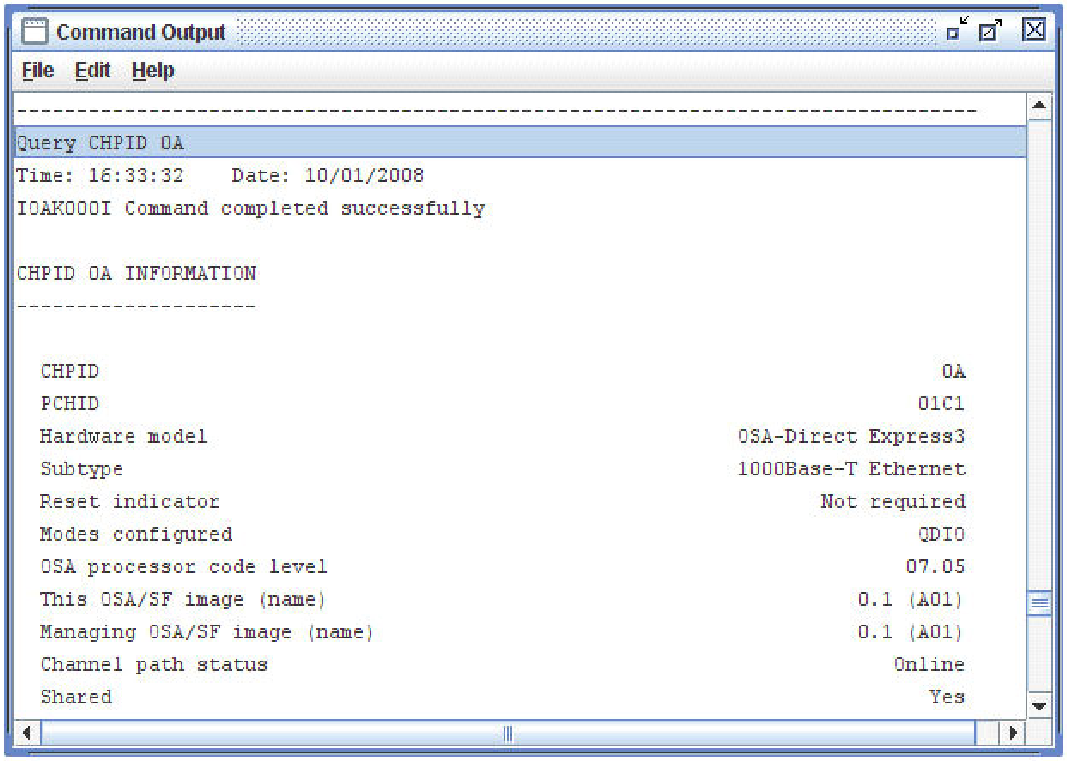


Figure E-12 Query window

The result of your Query command appears in the Command Output window (Figure E-13).



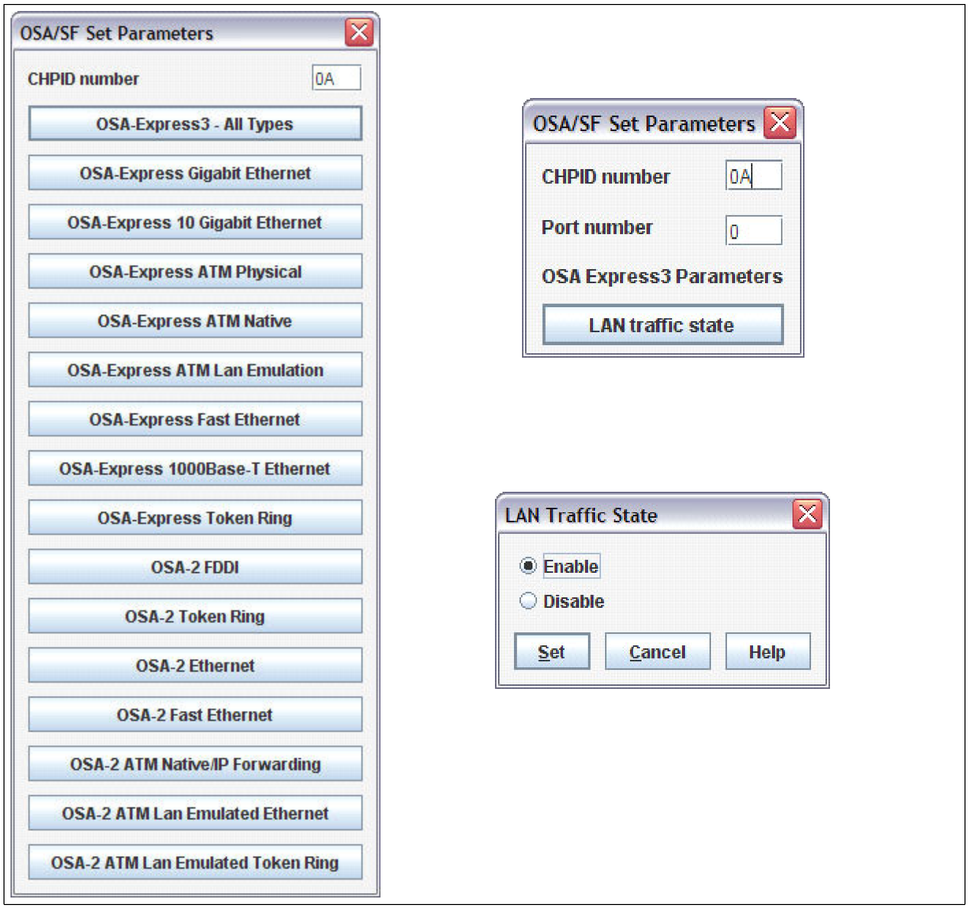
```
--------------------------------------------------------------------------------
Query CHPID 0A
Time: 16:33:32    Date: 10/01/2008
IOAK000I Command completed successfully

CHPID 0A INFORMATION
--------------------


  CHPID                                                                       0A
  PCHID                                                                     01C1
  Hardware model                                               OSA-Direct Express3
  Subtype                                                      1000Base-T Ethernet
  Reset indicator                                                     Not required
  Modes configured                                                          QDIO
  OSA processor code level                                                 07.05
  This OSA/SF image (name)                                            0.1 (A01)
  Managing OSA/SF image (name)                                        0.1 (A01)
  Channel path status                                                     Online
  Shared                                                                     Yes
```

Figure E-13 Command output of query One OSA

14. From the OSA/SF Commands panel (Figure E-3 on page 199), select **Set Parameters**.

15. In the OSA/SF Set Parameters window (Figure E-14 on page 207), depending on the type of feature, you can now set some parameters. We enter the CHPID number as 0A and select **OSA-Express3 - All Types**, because we are working with an OSA-Express3 1000BASE-T feature. The only valid action for our 1000BASE-T feature running in QDIO mode here is to check for the LAN traffic state and do an Enable/Disable command.

16. Complete the field Port number by typing a 0 or 1 and select **Enable** under LAN traffic state.



CHPID number 0A

CHPID number 0A

Port number 0

● Enable

○ Disable

Figure E-14 Set Parameters

Other tasks in the Commands window

From the OSA/SF Commands window (Figure E-3 on page 199), you can also perform the following tasks:

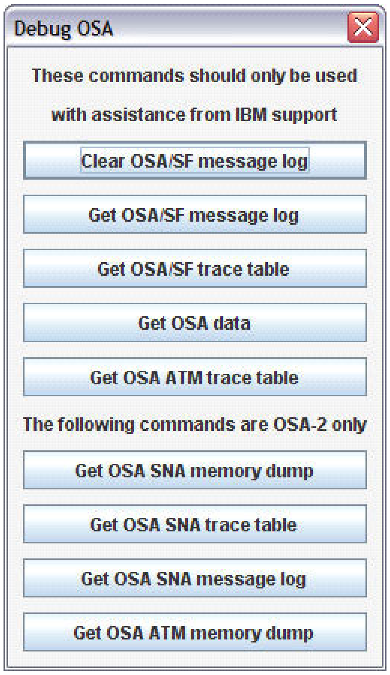
Start managing

This causes the copy of OSA/SF that runs in the image where the command is issued to take over management of the specified CHPID (OSA). If the CHPID is currently managed by a copy of OSA/SF that is running in another image, you must set the **Force** indicator (z/OS and z/VM only).

When this command completes, another copy of OSA/SF that is running on another image is limited to executing commands to this CHPID that do not change the CHPID’s environment.

Debug

This function of the OSA/SF GUI helps you to troubleshoot OSA problems. As stated in the Debug OSA window (Figure E-15 on page 208), use these Debug OSA commands only with assistance from IBM support.



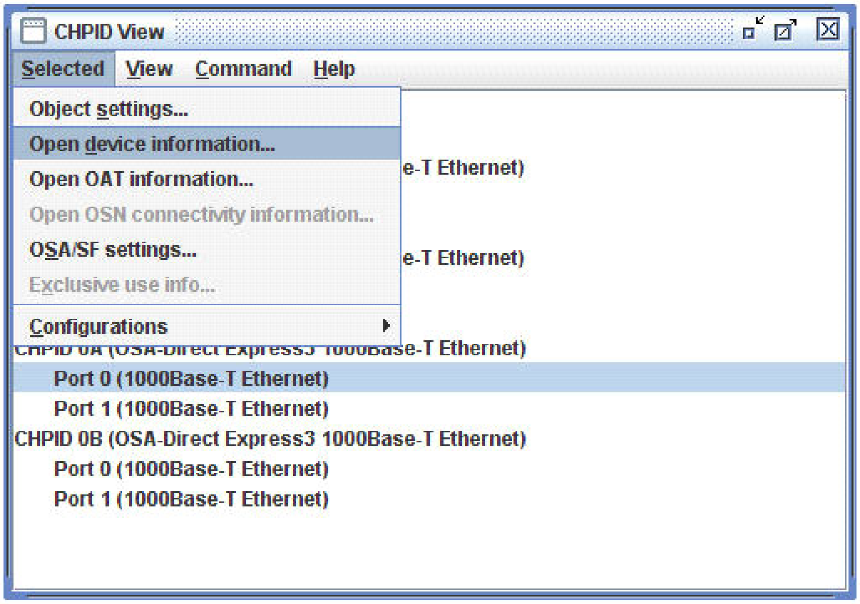
These commands should only be used with assistance from IBM support

The following commands are OSA-2 only

Figure E-15 Debug OSA

When debugging OSA problems, follow these steps under the guidance of IBM Support:

1. From the OSA/SF Commands window (Figure E-3 on page 199), select **CHPID View**.
2. From the CHPID View window, click **Selected** → **Open Device Information** to view device information, as shown in Figure E-16.

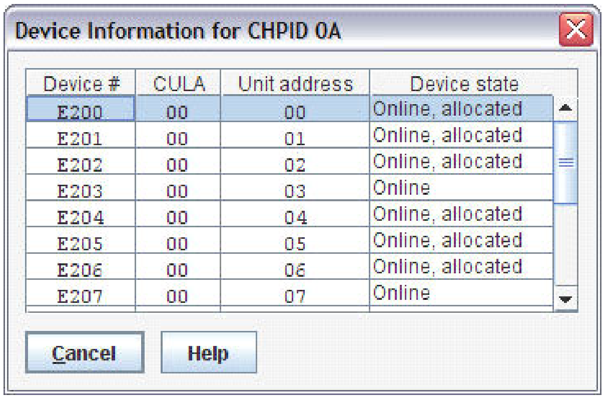


CHPID View
Selected
View
Command
Help
Object settings...
Open device information...
Open OAT information...
Open OSN connectivity information...
OSA/SF settings...
Exclusive use info...
Configurations
e-T Ethernet)
e-T Ethernet)
CHPID 0A (OSA-Direct Express3 1000Base-T Ethernet)
Port 0 (1000Base-T Ethernet)
Port 1 (1000Base-T Ethernet)
CHPID 0B (OSA-Direct Express3 1000Base-T Ethernet)
Port 0 (1000Base-T Ethernet)
Port 1 (1000Base-T Ethernet)

Figure E-16 CHPID View ("Open device information" selected in drop-down menu)

Figure E-17 shows the device information for CHPID 0A. You can see that unit addresses for Port 0, E200 to E202, are online and allocated. Port 1 (E204 to E206) is also. This indicates two things:

- VTAM TRL is active.
- TCP/IP is up, and our OSA port has been started.



Device #	CULA	Unit address	Device state
E200	00	00	Online, allocated
E201	00	01	Online, allocated
E202	00	02	Online, allocated
E203	00	03	Online
E204	00	04	Online, allocated
E205	00	05	Online, allocated
E206	00	06	Online, allocated
E207	00	07	Online

Figure E-17 Device Information

Note: Remember that to be able to use the OSA-Express Network Analyzer function, we defined an additional unit address during the HCD process. Also, in the VTAM TRLE, we added a data path (for CHPID 0A, Port 0 the device E203, and Port 1 the device E207). Both devices are online.

3. From the CHPID View window (Figure E-16 on page 208), click **Selected** → **Open OAT Information**.

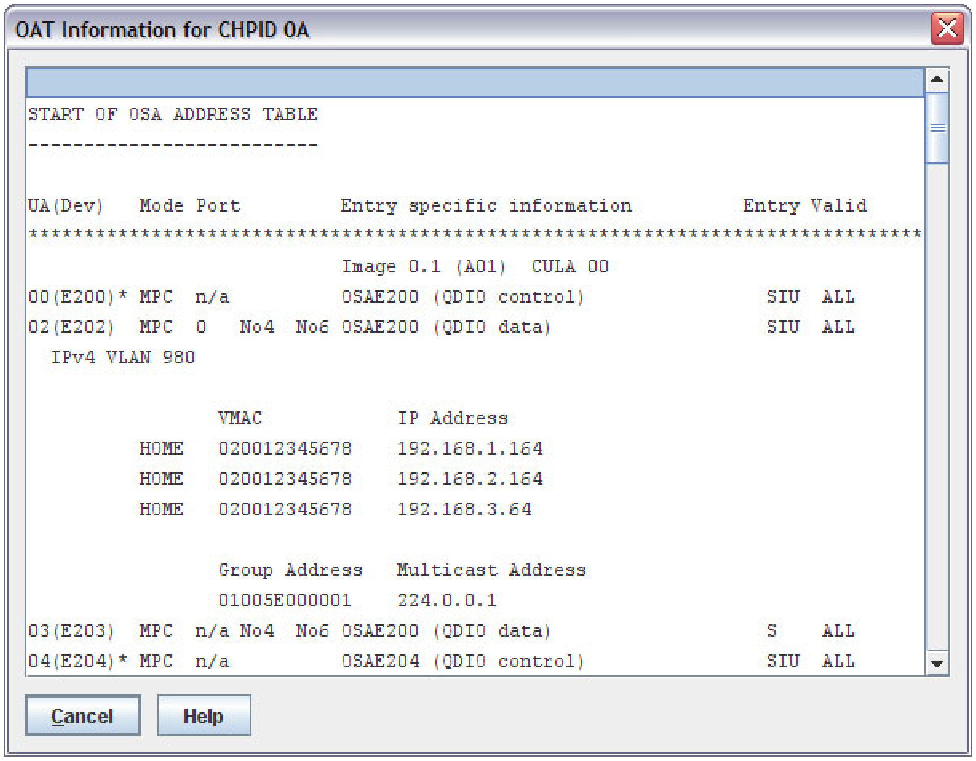
   The OAT Information for CHPID 0A window (Figure E-18 on page 210) shows the following information:

   – The LPAR number

   – The OSA port

   – The devices that are associated with the IP address. In our example, it shows 192.168.1.64 of our OSA Port 0 and 192.168.1.164 as the associated source virtual IP address (VIPA).

   Furthermore, you see the MAC address of this OSA port that is used by the Layer 3 VMAC function, which is described in Chapter 9, “IBM z/OS virtual MAC support” on page 79. Use the scroll bar to see the remaining OAT information for OSA Port 1 of CHPID 0A.



```
START OF OSA ADDRESS TABLE
--------------------------

UA(Dev)   Mode Port        Entry specific information         Entry Valid
********************************************************************************
                            Image 0.1 (A01)  CULA 00
00(E200)* MPC  n/a          OSAE200 (QDIO control)              SIU  ALL
02(E202)  MPC  0   No4  No6 OSAE200 (QDIO data)                 SIU  ALL
  IPv4 VLAN 980

                 VMAC            IP Address
          HOME   020012345678    192.168.1.164
          HOME   020012345678    192.168.2.164
          HOME   020012345678    192.168.3.64

                 Group Address   Multicast Address
                 01005E000001    224.0.0.1
03(E203)  MPC  n/a No4  No6 OSAE200 (QDIO data)                 S    ALL
04(E204)* MPC  n/a          OSAE204 (QDIO control)              SIU  ALL
```

Figure E-18 OAT Information

F

Using the OSA/SF operating system-based interface

This appendix describes the steps that are required to configure an Open Systems Adapter-Express (OSA) channel path identifier (CHPID) by using the TSO OS-based interface for the non-Queued Direct I/O (non-QDIO) modes. It does not apply to OSA-Express 5 devices, which run Open Systems Adapter Support Facility (OSA/SF) on the Hardware Management Console (HMC).[1]

The information covers the following topics:

[1] See *Open Systems Adapter/Support Facility on the Hardware Management Console*, SC14- 7580

Creating the OSA configuration

The Open Systems Adapter (OSA) configuration in the TSO environment is built with two z/OS sequential data sets. They contain statements that describe the OSA configuration and the OSA Address Table (OAT).

To build the OSA CHPID configuration, follow these steps:

1. Create two skeleton definitions:
   a. One skeleton definition for the configuration file

      You can get the sample of configuration files from IOA.SIOASAMP. Note the following points:

      - The sample asynchronous transfer mode (ATM) configuration file is named IOAATME.
      - The sample IOAFENET is used to configure Fast Ethernet and 1000BASE-T cards.
      - The sample token-ring configuration file is named IOATR.
      - The sample Gigabit configuration file is named IOAGIGA.

   b. One skeleton definition with the OAT entries (see “Creating the OAT file”)

      To ensure the correct format of the files, use the **`GET_CONFIG`** commands to retrieve the current files into sequential data sets.
2. Copy the skeleton definitions to work data sets.
3. Update, delete, or create the configuration and OAT entries as required.
4. Use the **`CONFIG_OSA`** command to activate your changes.

Creating the OAT file

Complete the following steps:

1. Create a skeleton OAT by using the OSA/SF **`GET_OAT`** command or by using the sample OAT file from the `IOA.SIOASAMP` data set.

   These are the names of the sample OAT files:

   IOAOSHRT: TCP/IP shared port (Example F-1 on page 213)
   IOAOSHRS: SNA shared port (Example F-2 on page 213)
   IOAOSHRA: TCP/IP SNA MPC shared port (Example F-3 on page 214)
   IOAENTR: Default OAT with two ports

> **Note:** If you retrieve the OAT from the OSA card, the OAT might contain several unneeded entries, especially if it is the default OAT file.

Example F-1   Sample TCP/IP OAT File (IOAOSHRT)

```
* This OAT template is a sample for setting up TCP/IP passthru mode
*   with port sharing between two Images running on an IBM zEnterprise 990 (z990)
system, which supports
*   logical channel subsytems.
* Image 0.5 and Image 0.7 are sharing port 0.
* Each OAT entry has more than one IP address that is associated with it.
********************************* Top of Data **********************************
* This OAT template is a sample for setting up TCP/IP passthru mode
*   with port sharing between two images that are running on a z990, which
supports
*   logical channel subsytems.
* Image 0.5 and Image 0.7 are sharing port 0.
* Each OAT entry has more than one IP address that is associated with it.
************************************************************************
* UA(Dev) Mode     Port     Entry specific information      Entry  Valid
************************************************************************
                               Image 0.5
00(1800)* passthru  00  Pri 105.001.005.005                  SIU    ALL
                            105.001.005.015
************************************************************************
                               Image 0.7
00(1800)* passthru  00  Sec 107.001.007.007                  SIU    ALL
                            107.001.005.017
```

Example F-2   Sample SNA OAT File (IOAOSHRS)

```
* This OAT template is a sample for setting up SNA mode with port
*   with port sharing between two images that are running on a z990, which
supports
*   logical channel subsytems.
* Image 0.5 and Image 0.7 are sharing port 0.
************************************************************************
* UA(Dev) Mode     Port     Entry specific information      Entry  Valid
************************************************************************
                               Image 0.5
0A(180A)  SNA       00                                       SIU    ALL
                               Image 0.7
0A(180A)  SNA       00                                       SIU    ALL
```

2. Copy the required parts of the OAT entry into a new data set.

Note: Only the *even* unit address entries are required for TCP/IP Passthru entries.

3. Update the OAT records for your logical partitions (LPARs) with the unit address, port mode and port number, default entry indicator, and IP address for each required device.
   - **Image/Partition:** Enter the channel subsystem (CSS) ID and partition number (*cssid.partitionnumber*) that is used for that entry. If you are running in basic mode or if the CHPID is dedicated, the partition number is 0.

- **UA:** The unit address can be any even address for TCP/IP Passthru, but unit address `00` is associated with OSA port 0 in the default OAT. Unit address `0A` is usually associated with OSA port 0 in Systems Network Architecture (SNA) mode.

  The OSA port unit address was used in the hardware configuration definition (HCD) when defining the OSA devices.

- **Mode:**
  - For TCP/IP Passthru, the port mode is `passthru`.
  - For SNA mode, the port mode is `SNA`.

- **Port:** Enter the port number that you want to associate with this unit address.

- **Default:** Enter `PRI` or `SEC` to make this the primary or secondary entry for this port, or enter `no` if it is neither the primary nor secondary entry.

  The entry that is designated as primary receives any datagram that is not specifically addressed to any of the home IP addresses that are associated with this OSA port. The secondary entry overtakes that function if the primary entry is not running.

- **IP Address:** Enter the home IP address for the port and unit address. Any time an OSA port (in TCP/IP Passthru mode) is shared, each partition's TCP/IP home IP address must also be added to the OAT. This allows the OSA to forward the received datagram to the appropriate partition.

4. Update the OAT records for your other LPARs with the unit address, port mode, port number, partition number, default entry indicator, and IP address for all devices. Do this in the way that was described for the first partition except, this time, substitute the appropriate addressing for your partitions.

Example F-3 shows an OAT file that is running in two partitions: `5` and `7`. One TCP/IP stack is running in each partition. `UNITADD` is defined in both partitions with a value of `00`. Shared SNA mode is defined for both partitions by using `UNITADD 0A`.

Example F-3 Sample OAT, shared port (IOAOSHRA)

```
This OAT template is a sample for setting up TCP/IP and SNA modes
With port sharing between two images that are running on a z990, which supports
logical channel subsytems.
Image 0.5 and Image 0.7 are sharing port 0.
************************************************************************
* UA(Dev) Mode     Port     Entry specific information      Entry  Valid
************************************************************************
                               Image 0.5
00(1800)* passthru  00  Pri 105.001.005.005                  SIU    ALL
                            105.001.005.015
                            105.001.005.025
                            105.001.005.035
02(1802)* passthru  00  No  100.100.100.100                  SIU    ALL
0A(180A)  SNA       00                                       SIU    ALL
************************************************************************
                               Image 0.7
00(1900)* passthru  00  No  107.001.075.075                  SIU    ALL
                            107.100.075.085
02(1902)* passthru  00  Sec 107.005.035.035                  SIU    ALL
0A(180A)  SNA       00                                       SIU    ALL
```

Activating the OSA configuration

IOACMD **CONFIG_OSA** performs the following functions:

- The OAT information from the specified data set is reformatted and saved on the z/OS host in the OSA configuration file. The OSA/SF configuration file (also defined in the startup profile) is updated to point to any code files that are required to support this configuration, and that are downloaded to the feature during any OSA/SF installation.
- An OSA/SF Install action downloads the OAT that is in the OATFILE data set.

See *Open Systems Adapter-Express Customer's Guide and Reference,* SA22-7935, for details about using OSA/SF.

Important: OSA configuration changes are disruptive, so all applications that are running through OSA devices must *not* have active sessions. Also, the OSAD device must be online to the host on which OSA/SF is running.

1. **Vary** all OSA devices offline (except the OSAD device) or at least those devices that have active sessions to all partitions that are sharing this OSA port.
2. Log on to TSO from the system on which OSA/SF is running.

Note: The TSO user ID must be set up to use the OSA/SF TSO interface.

3. Enter the **TSO IOACMD** command.
4. You see the choices shown in Figure F-1. Select option **2** to load a configuration.

```
IOACMD: Enter the command to be issued

IOACMD: 0 - End IOACMD
IOACMD: 1 - Clear Debug
IOACMD: 2 - Configure OSA CHPID
IOACMD: 3 - Convert OAT
IOACMD: 4 - Get Configuration File
IOACMD: 5 - Get Debug
IOACMD: 6 - Get OSA Address Table
IOACMD: 7 - Install
IOACMD: 8 - Put OSA Address Table (OSA-2 only)
IOACMD: 9 - Query
IOACMD:10 - Set Parameter
IOACMD:11 - Shutdown (VM only)
IOACMD:12 - Start Managing
IOACMD:13 - Stop Managing
IOACMD:14 - Synchronize (OSA-2 only)
```

Figure F-1 IOACMD menu

5. Select the OSA features that you want to configure by entering the number shown in the list (Figure F-2 on page 216), or just press Enter to get a list of valid OSA CHPIDs in your system.

```
IOACMD: Enter 'quit' to end IOACMD
IOACMD: Enter 0 for help
IOACMD: Enter 1 to configure an OSA-2 ATM CHPID
IOACMD: Enter 2 to configure an OSA-2 FDDI, ENTR, fast Ethernet CHPID
IOACMD: Enter 3 to configure an OSA-Express gigabit Ethernet CHPID
IOACMD: Enter 4 to configure an OSA-Express ATM CHPID
IOACMD: Enter 5 to configure an OSA-Express fast Ethernet or
                   an OSA-Express 1000Base-T Ethernet CHPID
IOACMD: Enter 6 to configure an OSA-Express token ring CHPID
IOACMD: Enter 7 to configure a non-QDIO (OSE) OSA-Express3 Ethernet CHPID
IOACMD: Enter a blank line to get a list of valid OSA CHPIDs
```

Figure F-2 IOACMD configure list

6. You are prompted through these configuration steps:

   a. Select the OSA feature type, and you will get the message in Figure F-3.

```
IOACMD: Enter CHPID -OR- 'quit' to end IOACMD
```

Figure F-3 IOACMD configuration message (1)

   b. Enter the OSA CHPID number to which the `CONFIG` file and OAT are to be downloaded. You will get the message in Figure F-4. Respond to that message (select `N` if you want to configure OSE, instead).

```
IOACMD: Is CHPID 0 of type OSD (QDIO)? (y/N)
```

Figure F-4 IOACMD configuration message (2)

   c. Enter the fully qualified data set name that contains the `CONFIG` definitions (Figure F-5)

```
IOACMD: Enter the name of the configuration file containing
IOACMD: the OSA-Express fast Ethernet/1000Base-T parameters.
IOACMD: -OR-
IOACMD: 'quit' to end IOACMD
```

Figure F-5 IOACMD configuration message (3)

   d. Enter the fully qualified data set name that contains the OAT definitions (Figure F-6)

```
IOACMD: Enter the name of the data set containing the OAT you
IOACMD:   want to put on the OSA
IOACMD:   (This should be in the same format that is returned by Get OAT)
IOACMD: -OR-
IOACMD: Enter 0 to exit this EXEC
```

Figure F-6 IOACMD configuration message (4)

   e. Enter the activation option, as shown in Figure F-7 on page 217. Note the following points:

      - **`Activate`** creates the OAT, updates the index data set, and downloads the OAT.
      - **`Activate, no Install`** creates the OAT and updates the index data set but does not download the OAT. **`IOACMD INSTALL`** must be done later.

```
IOACMD: 0 - Quit

IOACMD: 1 - Activate
IOACMD:     Sets up all the files and transfers the data to the CHPID
IOACMD:     If there are any 'in use' OAT entries, 'activate' will fail

IOACMD: 2 - Activate, no Install
IOACMD:     Only sets up the files, but does not transfer them to the CHPID
IOACMD:     You must issue the Install command at a later time
IOACMD:     to complete the activation
```

Figure F-7 IOACMD configuration message (5)

f. Press Enter to confirm the activation (Figure F-8), because it is disruptive to the OSA feature.

```
IOACMD: To end 'activate' processing, enter 'QUIT'
IOACMD: To proceed with processing, enter anything else
```

Figure F-8 IOACMD configuration message (6)

G

TCP/IP Passthru mode

This appendix describes the process to configure an OSA-Express3 1000BASE-T port for TCP/IP Passthru mode by using the default OSA Address Table (OAT). We did not have an Open Systems Adapter available for non-Queued Direct I/O (non-QDIO) testing, so this appendix was not updated for either OSA-Express4S or OSA-Express5S.

The information covers the following topics:

- “Default mode” on page 220
- “Hardware configuration definition requirements” on page 220
- “Displaying the default OAT” on page 221
- “Customizing z/OS TCP/IP” on page 224
- “Activation” on page 226

Default mode

Figure G-1 shows a functional view of the TCP/IP in Passthru mode connectivity that is described in this chapter.

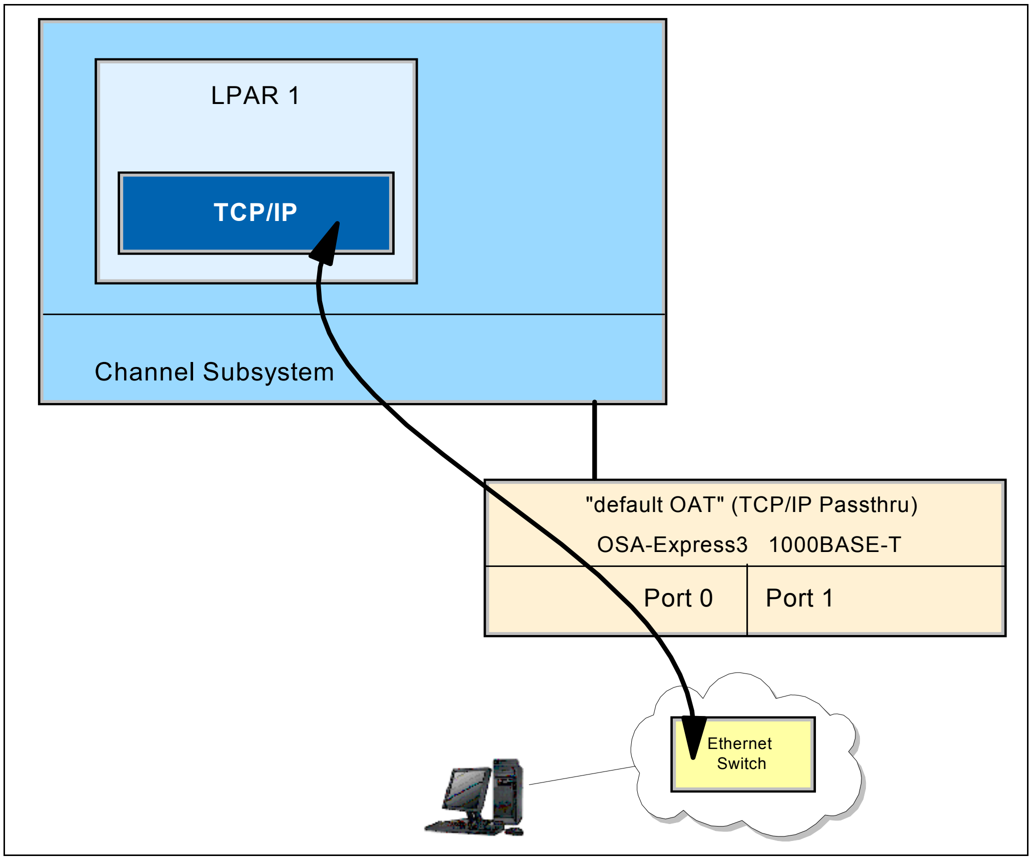


Figure G-1 TCP/IP in Passthru mode

For this example, we use the OSA-Express3 1000BASE-T card, channel path identifier (CHPID) type OSE, in *default* mode. When an OSA-Express feature is manufactured, a basic configuration is installed that permits some functions without the need to build and load an OSA Address Table.

The default mode permits “passthru” functionality only. One use for this mode is in a new installation, where you can establish that hardware configuration definitions (HCDs) and network connections are correct without the added complication or concern of whether there is a configuration error in the OAT.

The IBM zEnterprise z10 or z9 server sees the OSA-Express3 1000BASE-T port as a LAN Channel Station (LCS) device. An LCS device handles data traffic in either direction for any TCP/IP partition that has an OSA-Express port defined.

Hardware configuration definition requirements

The OSA-Express CHPID, the control unit, and the OSA devices must be defined in HCDs and activated. See Chapter 3, “Hardware configuration definitions” on page 15, for the procedure to create the definitions. Example G-1 on page 221 shows the necessary definitions for the input/output configuration data set (IOCDS) that we used for examples in this chapter. For future purposes, we use 31 OSA devices, although only two are needed in our configuration.

If you plan to use Open Systems Adapter Support Facility (OSA/SF), we suggest that you share your OSA-Express port among all partitions where OSA/SF is running. This is why we included the definition for the OSAD (Unit FE) device.

Example G-1 IOCDS input for CHPID 0C example

```
ID    MSG1='IODF29',MSG2='SYS6.IODF29 - 2008-10-08 12:04',    *
      SYSTEM=(2098,1),LSYSTEM=SCZP202,                        *
      TOK=('SCZP202',00800006991E2094120450420108282F00000000,*
      00000000,'08-10-08','12:04:50','SYS6','IODF29')
RESOURCE PARTITION=((CSS(0),(A01,1),(*,2),(*,3),(*,4),(*,5),(**
      ,6),(*,7),(*,8),(*,9),(*,A),(*,B),(*,C),(*,D),(*,E),(*,F*
      )),(CSS(1),(A11,1),(A12,2),(*,3),(*,4),(*,5),(*,6),(*,7)*
      ,(*,8),(*,9),(*,A),(*,B),(*,C),(*,D),(*,E),(*,F)))
CHPID PATH=(CSS(0),0C),SHARED,PARTITION=((A01),(=)),PCHID=230,*
      TYPE=OSE
CNTLUNIT CUNUMBR=2E40,PATH=((CSS(0),0C)),UNIT=OSA
IODEVICE ADDRESS=(2E40,031),UNITADD=00,CUNUMBR=(2E40),UNIT=OSA
IODEVICE ADDRESS=2E5F,UNITADD=FE,CUNUMBR=(2E40),UNIT=OSAD
```

Displaying the default OAT

Although we do not need to use OSA/SF for the activities in this chapter, we thought it would be instructive to view the default OAT.

The OSA/SF GUI must be connected to an IBM z/OS host that has OSA/SF running. In addition, the OSA CHPID must be defined by HCD, and the HCD must be activated. This step does not require the CHPID to be installed or online. It simply creates and saves an OSA-Express configuration.

1. Start the OSA/SF GUI program:
   a. Open a DOS command window.
   b. Enter the following command:

      ```
      java IOAJAVA
      ```

   c. At the prompt, type your password to make a connection.
2. In the Workstation Interface window, in the right panel under OSA/SF Commands, select **CHPID View** and select the CHPID (in our example: **0C**).

3. In the CHPID View window (Figure G-2), click **Selected** → **Object settings**.

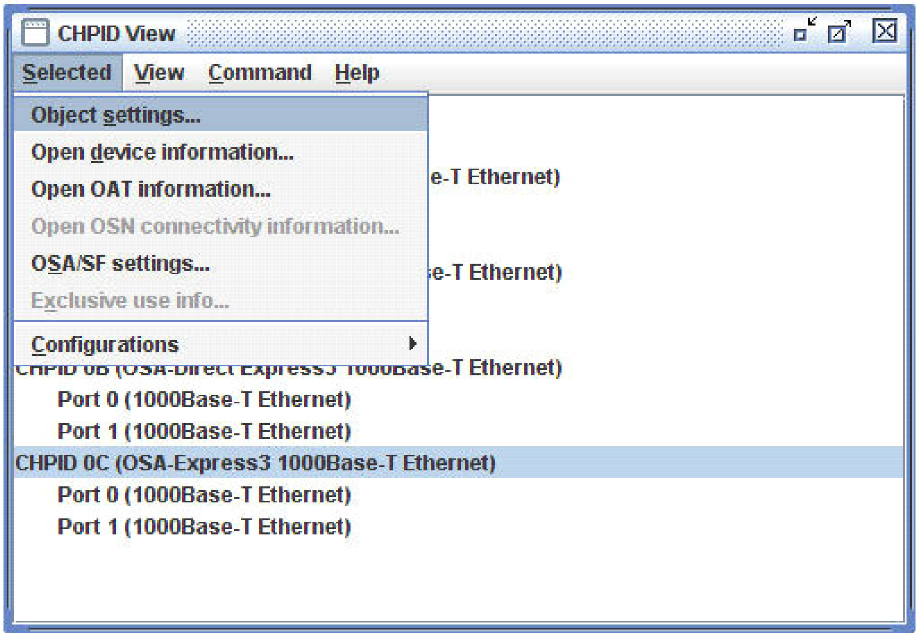
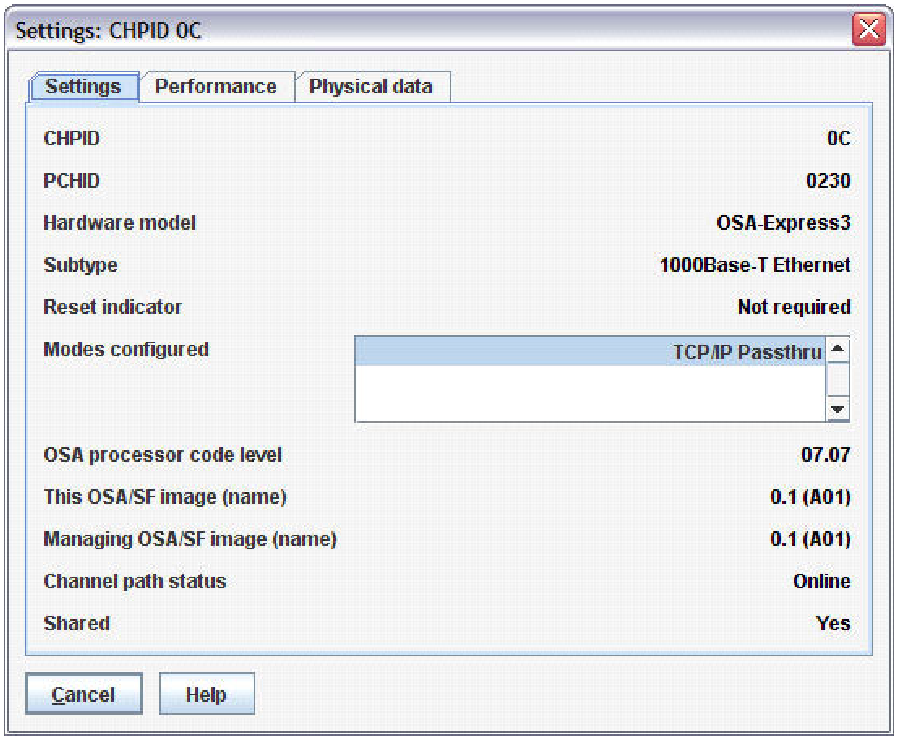

CHPID View
Selected
View
Command
Help
Object settings...
Open device information...
Open OAT information...
Open OSN connectivity information...
OSA/SF settings...
Exclusive use info...
Configurations
e-T Ethernet)
e-T Ethernet)
CHPID 0B (OSA-Direct Express3 1000Base-T Ethernet)
Port 0 (1000Base-T Ethernet)
Port 1 (1000Base-T Ethernet)
CHPID 0C (OSA-Express3 1000Base-T Ethernet)
Port 0 (1000Base-T Ethernet)
Port 1 (1000Base-T Ethernet)

Figure G-2 CHPID View, Object setting selected on drop-down menu

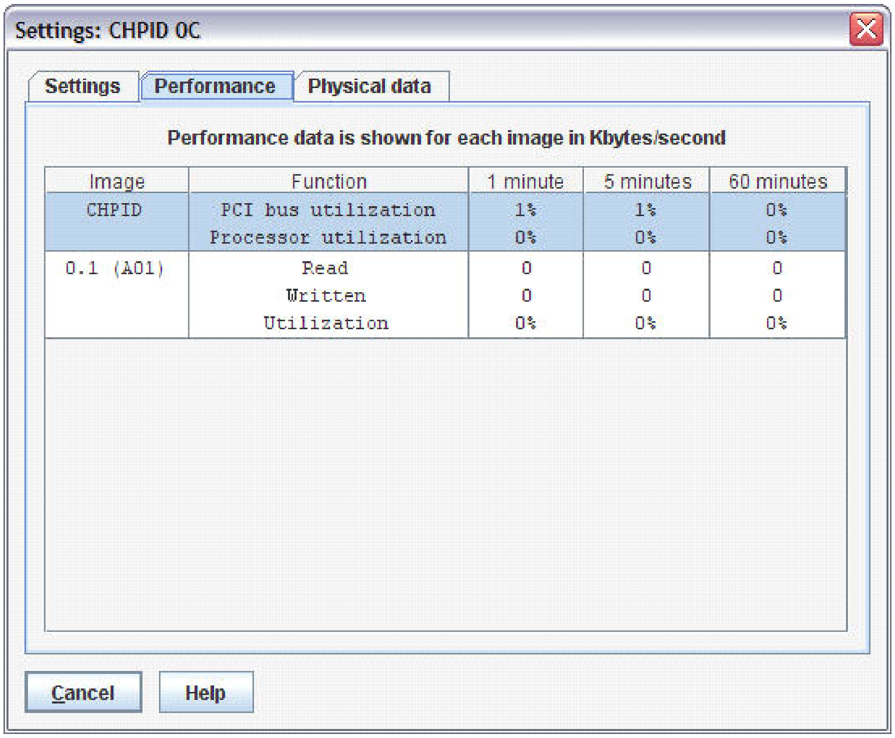
a. In the **Settings** tab (Figure G-3), you see that the CHPID is TCP/IP Passthru (OSE), online, shared, and the processor code level is displayed (07.07).



CHPID	0C
PCHID	0230
Hardware model	OSA-Express3
Subtype	1000Base-T Ethernet
Reset indicator	Not required
Modes configured	TCP/IP Passthru
OSA processor code level	07.07
This OSA/SF image (name)	0.1 (A01)
Managing OSA/SF image (name)	0.1 (A01)
Channel path status	Online
Shared	Yes

Figure G-3 Settings: CHPID 0C

b. Select the **Performance** tab (Figure G-4) to see performance data, such as the Peripheral Component Interconnect (PCI) bus use for all partitions that share the CHPID.

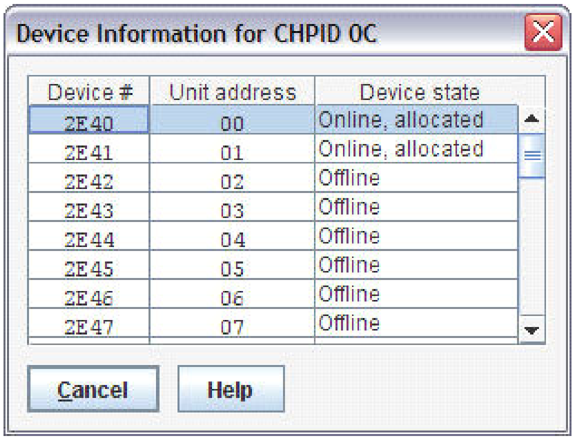


Performance data is shown for each image in Kbytes/second

Image	Function	1 minute	5 minutes	60 minutes
CHPID	PCI bus utilization	1%	1%	0%
	Processor utilization	0%	0%	0%
0.1 (A01)	Read	0	0	0
	Written	0	0	0
	Utilization	0%	0%	0%

Figure G-4 Performance data display

4. Return to the CHPID View window, and click **Selected** → **Open Device Information**. Now the unit addresses are displayed with their own status indications, as shown in Figure G-5.

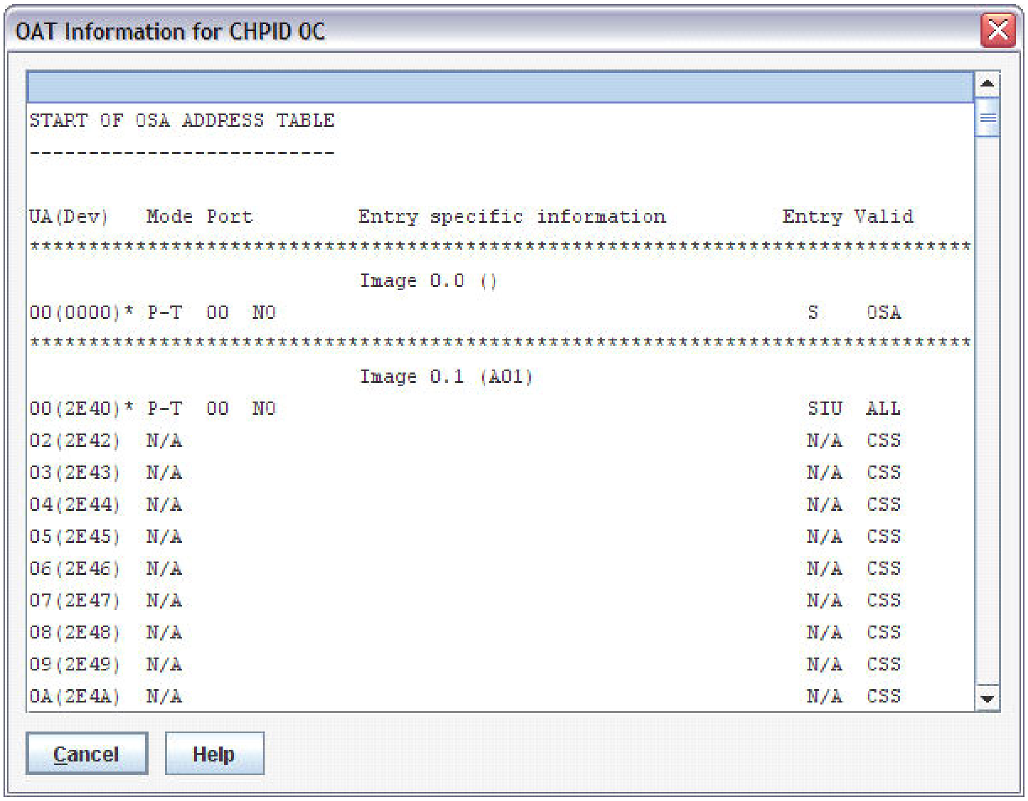


Device #	Unit address	Device state
2E40	00	Online, allocated
2E41	01	Online, allocated
2E42	02	Offline
2E43	03	Offline
2E44	04	Offline
2E45	05	Offline
2E46	06	Offline
2E47	07	Offline

Figure G-5 Device information

5. Again return to the CHPID View window. This time, click **Selected** → **Open OAT Information**.

   As shown in Figure G-6, it shows image A01 with devices 2E40 and 2E41 online and the status of SIU (started and in use). This display shows an example of an OSA-Express CHPID shared with multiple partitions.



```
START OF OSA ADDRESS TABLE
--------------------------

UA(Dev)   Mode Port         Entry specific information          Entry Valid
********************************************************************************
                            Image 0.0 ()
00(0000)* P-T  00  NO                                             S    OSA
********************************************************************************
                            Image 0.1 (A01)
00(2E40)* P-T  00  NO                                             SIU  ALL
02(2E42)  N/A                                                     N/A  CSS
03(2E43)  N/A                                                     N/A  CSS
04(2E44)  N/A                                                     N/A  CSS
05(2E45)  N/A                                                     N/A  CSS
06(2E46)  N/A                                                     N/A  CSS
07(2E47)  N/A                                                     N/A  CSS
08(2E48)  N/A                                                     N/A  CSS
09(2E49)  N/A                                                     N/A  CSS
0A(2E4A)  N/A                                                     N/A  CSS
```

Figure G-6 OAT Information

When the CHPID is dedicated to only one partition, LPAR 0 is unique in that this value is used to identify that an OSE CHPID is dedicated. Regardless of the LPAR to which the OSE CHPID is dedicated, the LPAR number that is used is always 0.

Customizing z/OS TCP/IP

Definitions are required in TCP/IP for the OSA-Express3 1000BASE-T in TCP/IP Passthru mode. For Passthru mode, you define one `LINK` statement for its related `DEVICE` statement.

Non-QDIO OSA-Express ports are defined to TCP/IP as LCS devices. You must assign an IP address by coding an entry for the LINK name in the `HOME` statement. Depending on your network design, you also need to code a route entry. OSA-Express can be activated in the TCP/IP profile by using a `START` statement.

Figure G-7 shows the network and the connections of our configuration example.

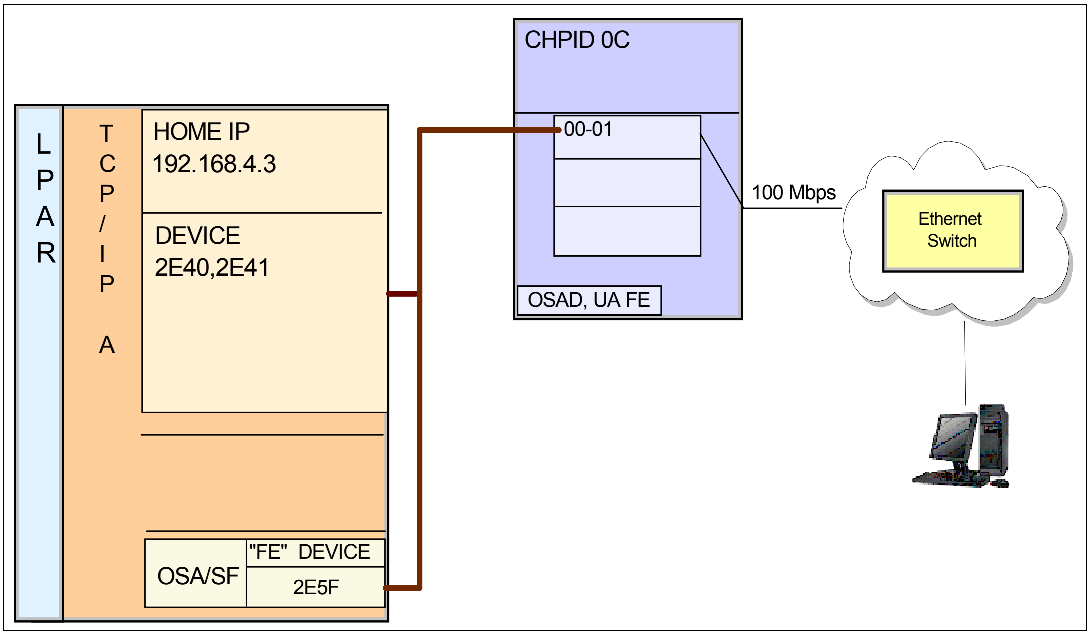


Figure G-7 TCP/IP Passthru mode with non-shared port

TCP/IP definitions

The z/OS device addresses used for port 0 are 2E40 and 2E41.

We defined:

- One `DEVICE` statement per OSA-Express Port, with the *even* device number of the two device addresses assigned to the hardware for the port

  Note the following considerations:

  – Even though you define only one port, you use two device numbers per OSA-Express Port for TCP/IP Passthru mode. One device is used by TCP/IP for reading, and the other device is used for writing.

  – Using the `DEVICE` statement, you define the DEVICE name, the DEVICE type (LCS) for the OSA-Express Port, and the DEVICE number (the read device number, which is the even device number).

- One `LINK` statement per OSA TCP/IP DEVICE statement

  Using the `LINK` statement, you define the LINK name, the LINK type (in our example, ETHERNET), the PORT number, and the DEVICE name.

  Although the OSA-Express port is known by the device number, the port number in the `LINK` statement *must* match the actual OSA-Express port number.

> **Note:** If you are using a OSA-Express3 1000 BASE-T multi-port card with two ports per CHPID, the port number that is specified on the `LINK` statement must relate to your OSA port, either port 0 or port1

- A HOME IP address (in our example, we used IP address 192.168.4.3)

  The HOME statement relates an IP address to the OSA described in the `DEVICE` and `LINK` statement pair.

- Routes using static routes through the `BEGINROUTES` statement

  > **BEGINROUTES statement:** If you are migrating your TCP/IP profile from an earlier release, the profile might use the GATEWAY statement to define static routes instead of the BEGINROUTES - ENDROUTES statements. GATEWAY is recognized and used, but consider replacing it with BEGINROUTES for the following reasons:
  >
  > - It is compatible with UNIX standards.
  > - It is easier to code than GATEWAY.
  > - It accepts both IPv4 and IPv6 addresses.
  > - It has enhanced functionality.
  >
  > Future static route enhancements will be available only with the BEGINROUTES statement.

  Dynamic routing can be accomplished by using the `OMPROUTE` daemon, or the `BSDROUTINGPARMS` statement can be used with the `RouteD` daemon. We do not recommend the use of the `BEGINROUTES` statement (static routes) with the *OMPROUTE* or `OROUTED` routing daemons.

- One `START` statement per OSA device

  The `START` device statement entry uses the `DEVICE` statement name.

Figure G-8 shows the TCP/IP profile definitions that we used to define OSA to TCP/IP A.

```
DEVICE OSA2E40  LCS 2E40
LINK   OSA2E40LNK  ETHERNET  0   OSA2E40

HOME
   192.168.4.3 OSA2E40LNK

BEGINROUTES
ROUTE 192.168.4.0/24           = OSA2E40LNK  MTU 1492
ENDROUTES

START OSA2E40
```

Figure G-8   TCP/IP profile definitions

Activation

Activation includes the following tasks, among others:

- Ensure that the devices are online
- Activate an OSA/SF configuration
- Activate VTAM resources
- Activate TCP/IP

Because the OSA-Express port is used in default mode, little needs to be done in our case. We need to ensure only that the devices are online and then activate TCP/IP.

Verifying that devices are online

To verify that the required devices are online, enter the z/OS Console Display command:

```
D U,,,2E40,2
IEE457I 11.08.20 UNIT STATUS 632
UNIT TYPE STATUS        VOLSER     VOLSTATE
2E40 OSA  A-BSY
2E41 OSA  A
```

If the devices are not online, enter the z/OS console Vary command:

```
V (2E40-2E41),ONLINE
```

Activating TCP/IP

There are three ways to make the added definitions to the TCP/IP profile effective:

- You can create an `obeyfile` by using the definition statements that are listed in this chapter.
- You can restart the TCP/IP stack.
- You can issue the following z/OS command:

  ```
  V TCPIP,TCPIPA,START,OSA2E40
  ```

We confirm the status of the TCP/IP devices by using the **`NETSTAT DEV`** command, as shown in Figure G-9 on page 228. Notice that both the device and the link are in `READY` status.

```
DEVNAME: OSA2E40           DEVTYPE: LCS       DEVNUM: 2E40
 DEVSTATUS: READY
 LNKNAME: OSA2E40LNK        LNKTYPE: ETH         LNKSTATUS: READY
   NETNUM: 0    QUESIZE: 0
   IPBROADCASTCAPABILITY: YES
   MACADDRESS: 00145E74A950
   ACTMTU: 1500
   SECCLASS: 255                  MONSYSPLEX: NO
 BSD ROUTING PARAMETERS:
   MTU SIZE: N/A               METRIC: 00
   DESTADDR: 0.0.0.0           SUBNETMASK: 255.255.255.0
 MULTICAST SPECIFIC:
   MULTICAST CAPABILITY: YES
   GROUP             REFCNT      SRCFLTMD
   -----             ------      --------
   224.0.0.1         0000000001  EXCLUDE
     SRCADDR: NONE
 LINK STATISTICS:
   BYTESIN                           = 1536
   INBOUND PACKETS                   = 24
   INBOUND PACKETS IN ERROR          = 0
   INBOUND PACKETS DISCARDED         = 0
   INBOUND PACKETS WITH NO PROTOCOL  = 0
   BYTESOUT                          = 1536
   OUTBOUND PACKETS                  = 24
   OUTBOUND PACKETS IN ERROR         = 0
   OUTBOUND PACKETS DISCARDED        = 2
```

Figure G-9 TCP/IP device, link status, and statistics

For a summary of related commands, see Appendix D, “Useful setup and verification commands” on page 183.

H

Our configuration definitions

This appendix lists configuration definitions that we used for examples in this book for TCP/IP in various operating systems environments. It also includes Virtual Telecommunications Access Method (VTAM) definitions that are used in the IBM z/OS operating system.

The information covers the following topics:

- “Sample environment” on page 230
- “z/OS definitions” on page 230
- “z/VM TCP/IP profile” on page 234

Sample environment

Figure H-1 is a logical representation of the environment that we used for the examples.

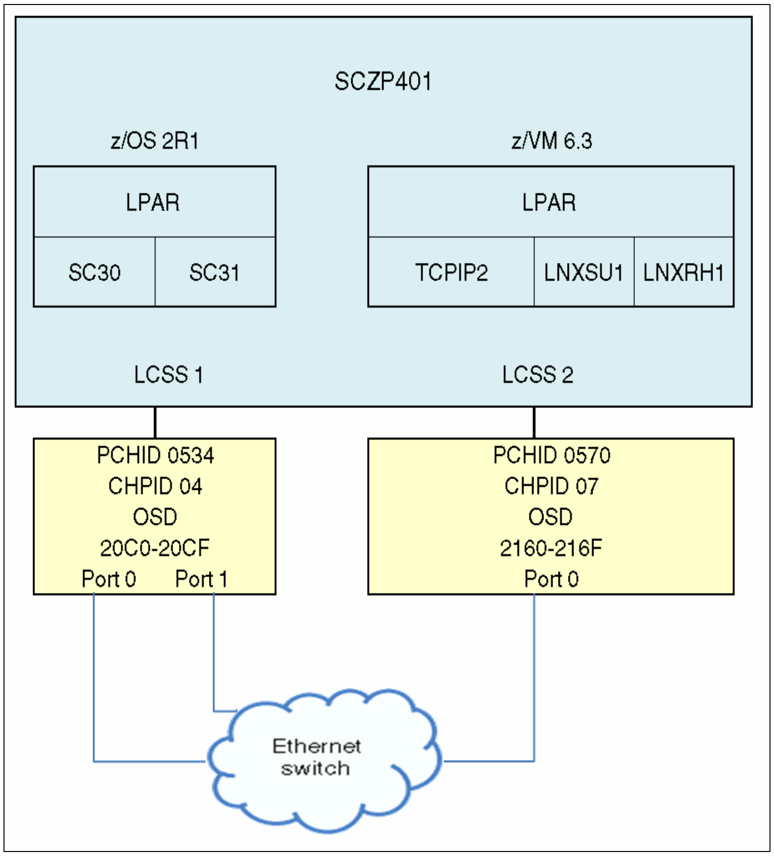
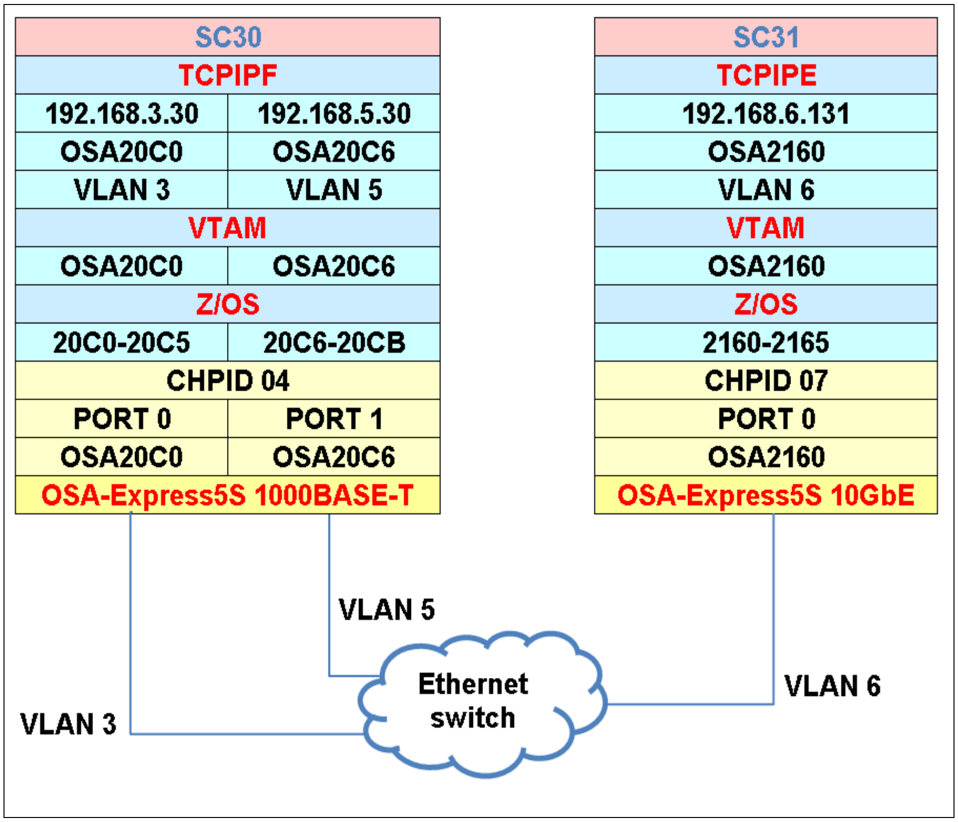


Figure H-1 Our hardware environment

z/OS definitions

This section includes examples of the definitions that we used in our z/OS logical partitions (LPARs), starting with a diagram. Figure H-2 on page 231 shows the IBM International Technical Support Organization (ITSO) lab environment from a z/OS perspective.



SC30	
TCPIPF	
192.168.3.30	192.168.5.30
OSA20C0	OSA20C6
VLAN 3	VLAN 5
VTAM	
OSA20C0	OSA20C6
Z/OS	
20C0-20C5	20C6-20CB
CHPID 04	
PORT 0	PORT 1
OSA20C0	OSA20C6
OSA-Express5S 1000BASE-T	

SC31
TCPIPE
192.168.6.131
OSA2160
VLAN 6
VTAM
OSA2160
Z/OS
2160-2165
CHPID 07
PORT 0
OSA2160
OSA-Express5S 10GbE

Figure H-2 Our z/OS environment

TCP/IP profiles

The TCP/IP profile for SC30 (Example H-1) shows only the lines that we added or changed.

Example H-1 Profile of TCPIPF

```
DEVICE OSA20C0  MPCIPA   ; OSD Devices on CHPID 04
LINK   OSA20C0LNK  IPAQENET OSA20C0  VLANID 3
;
DEVICE OSA20C6  MPCIPA  ; OSD Devices on CHIPD 04
LINK   OSA20C6LNK  IPAQENET OSA20C6 VLANID 5
;
HOME
  192.168.3.30  OSA20C0LNK
  192.168.5.30  OSA20C6LNK
;
BEGINROUTES
 ROUTE DEFAULT             192.168.3.1     OSA20C0LNK    MTU 1492
 ROUTE 192.168.3.0 255.255.255.0 =         OSA20c0LNK    MTU 1492
 ROUTE 192.168.5.0 255.255.255.0 =         OSA20C6LNK    MTU 1492
ENDROUTES
;
START OSA20C0
START OSA20C6
```

The TCP/IP profile for SC31 (Example H-2) shows only the lines that we added or changed.

Example H-2 Profile TCPIPE

```
INTERFACE OSA2160LNK
   DEFINE IPAQENET
   PORTNAME OSA2160
   IPADDR 192.168.6.131/24
   VLANID 6
   VMAC ROUTEALL
;
BEGINROUTES
 ROUTE DEFAULT              192.168.6.1     OSA2160LNK    MTU 8992
 ROUTE 192.168.6.0 255.255.255.0 =          OSA2160LNK    MTU 8992
ENDROUTES
;
START OSA2160LNK
```

VTAM definitions

This section presents examples of VTAM definitions for the channel path identifier (CHPID) OSD type and Enterprise Extender.

VTAM Transport Resource List definitions

We used the same Transport Resource List (TRL) definitions on both SC30 and SC31. Example H-3 shows port 0.

Example H-3 TRL for CHPID 04 - OSA-Express5S 1000BASE-T Port 0

```
OSA20C0  VBUILD TYPE=TRL
OSA20C0P TRLE  LNCTL=MPC,                                              *
               READ=20C0,                                              *
               WRITE=20C1,                                             *
               DATAPATH=(20C2-20C5),                                   *
               PORTNAME=OSA20C0,                                       *
               MPCLEVEL=QDIO

```

Example H-4 shows port 1.

Example H-4 TRL for CHPID 04 - OSA-Express5S 1000BASE-T Port 1

```
OSA20C6  VBUILD TYPE=TRL
OSA20C6P TRLE  LNCTL=MPC,                                              *
               READ=20C6,                                              *
               WRITE=20C7,                                             *
               DATAPATH=(20C8-20CD),                                   *
               PORTNAME=OSA20C6,                                       *
               PORTNUM=1,                                              *
               MPCLEVEL=QDIO
```

Example H-5 shows the 10GbE definition.

Example H-5   TRL for CHPID 07 - OSA-Express5S 10GbE

```
OSA2160  VBUILD TYPE=TRL
OSA2160P TRLE  LNCTL=MPC,                                              *
               READ=2160,                                              *
               WRITE=2161,                                             *
               DATAPATH=(2162-2165),                                   *
               PORTNAME=OSA2160,                                       *
               MPCLEVEL=QDIO
```

Example H-6 shows the external communication adapter (XCA) major node.

Example H-6   XCA Majornode XCAOSAX3 - used for non-QDIO configuration

```
XCAOSA   VBUILD TYPE=XCA
OSAX3    PORT  MEDIUM=CSMACD,                                          X
               ADAPNO=0,                                               X
               CUADDR=2E4A,                                            X
               TIMER=60,                                               X
               SAPADDR=04
***********************************************************************
OSAX3G   GROUP DIAL=YES,                                               X
               DYNPU=YES,                                              X
               ANSWER=ON,                                              X
               AUTOGEN=(3,L,P),                                        X
               CALL=INOUT,                                             X
               ISTATUS=ACTIVE

```

Example H-7 shows the switched major node.

Example H-7   Switched Majornode - used for our non-QDIO configuration

```
VBUILD TYPE=SWNET
OSASW    PU    ADDR=02,                                                X
               IDBLK=05D,                                              X
               IDNUM=12863,                                            X
               CPNAME=OSANT,                                           X
               IRETRY=YES,                                             X
               MAXOUT=7,                                               X
               MAXPATH=1,                                              X
               MAXDATA=1024,                                           X
               PACING=0,                                               X
               VPACING=0,                                              X
               PUTYPE=2,                                               X
               DISCNT=(NO),                                            X
               ISTATUS=ACTIVE,                                         X
               MODETAB=NEWMTAB,                                        X
               DLOGMOD=DYNTRN,                                         X
               USSTAB=USSLDYN,                                         X
               SSCPFM=USSSCS
OSASWL0  LU    LOCADDR=0,MODETAB=MTAPPC,DLOGMOD=APPCMODE
OSASWL1  LU    LOCADDR=1                                3270 SESSIONS
OSASWL2  LU    LOCADDR=2
```

z/VM TCP/IP profile

This section includes examples of the definitions that we used in our IBM z/VM LPAR. Figure H-3 shows our z/VM environment.

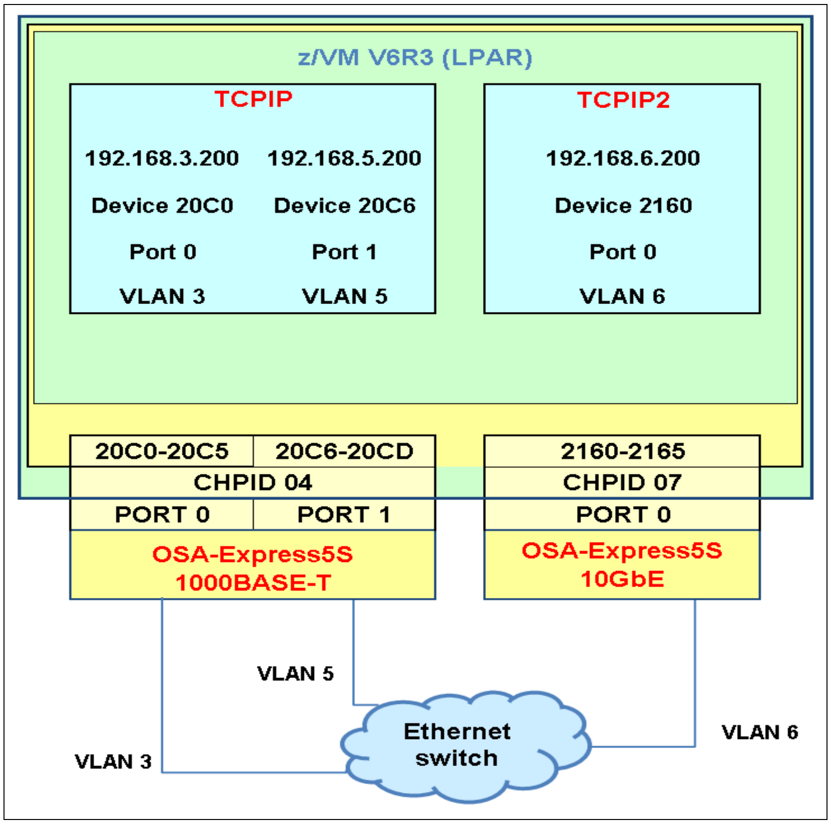


Figure H-3 Our z/VM environment

The TCP/IP profile in Example H-8 on page 235 shows only the statements that are related to OSA-Express5S 1000BASE-T and OSA-Express5S 10GbE.

Example H-8 Sample z/VM TCPIP profile

```
DEVICE OSA20C0 OSD 20C0 PORTNUMBER 00
LINK OSA20C0 QDIOETHERNET OSA20C0 MTU 1500 ETHERNET VLAN 3
;
DEVICE OSA20C6 OSD 20C6 PORTNUMBER 01
LINK OSA20C6 QDIOETHERNET OSA20C6 MTU 1500 ETHERNET VLAN 5
; (End DEVICE and LINK statements)
; ----------------------------------------------------------------------
HOME
192.168.3.200 255.255.255.0 OSA20C0
192.168.5.200 255.255.255.0 OSA20C6
; (End HOME Address information)
; ----------------------------------------------------------------------
GATEWAY
; Network       Subnet          First           Link             MTU
; Address       Mask            Hop             Name             Size
; ------------- --------------- --------------- ---------------- -----
DEFAULTNET                      192.168.3.1     OSA20C0          1500
; (End GATEWAY Static Routing information)
; ----------------------------------------------------------------------
START OSA20C0
START OSA20C6
; (End START statements)
```

Example H-9 shows the 10GbE definition for TCPIP2.

Example H-9 Sample z/VM TCPIP2 profile

```
DEVICE OSA2160 OSD 2160 PORTNUMBER 00
LINK OSA2160 QDIOETHERNET OSA2160 MTU 1500 ETHERNET VLAN 6
;
; (End DEVICE and LINK statements)
; ----------------------------------------------------------------------
HOME
192.168.6.200 255.255.255.0 OSA2160
; (End HOME Address information)
; ----------------------------------------------------------------------
GATEWAY
; Network       Subnet          First           Link             MTU
; Address       Mask            Hop             Name             Size
; ------------- --------------- --------------- ---------------- -----
DEFAULTNET                      192.168.3.1     OSA20C0          1500
; (End GATEWAY Static Routing information)
; ----------------------------------------------------------------------
START OSA2160
; (End START statements)
```

I

Address Resolution Protocol takeover

This appendix describes Address Resolution Protocol (ARP) takeover, including the definition requirements and verification procedures. The information covers the following topics:

- "ARP takeover description" on page 238
- "ARP takeover definitions" on page 239
- "Verifying ARP takeover" on page 241

ARP takeover description

ARP takeover is a function that allows traffic to be redirected from a failing Open Systems Adapter (OSA) connection to another OSA connection. This function is supported by IPv4 and IPv6 OSA interfaces.

When an OSA DEVICE or INTERFACE that is defined in a TCP/IP stack is started, all of the IP addresses with that OSA port in Queued Direct I/O (QDIO) mode (which is device type MPCIPA in the TCP/IP profile) are dynamically downloaded to the OSA.

> **Note:** If you want to use ARP takeover function, use your OSA-Express ports in QDIO mode. If the port is defined in non-QDIO mode (device type LCS in TCP/IP profile), you must use OSA Address Table (OAT) entries on the Hardware Management Console (HMC) for OSA-Express5S and OSA-Express4S or OSA/SF for OSA-Express4S to build and activate a configuration that identifies the multiple IP address that *might* be used with the adapter. In a dynamic virtual IP address (dynamic VIPA) environment (or a simple OSA takeover environment), use of QDIO mode simplifies setup and management.

To take advantage of ARP takeover, the following conditions must be met:

- If this is an *OSD* type CHPID, IP addresses are dynamically downloaded to the feature. If this is an *OSE* type CHPID, instead, a configuration must be activated that includes all of the IP addresses that are used by this feature.
- TCP/IP must have connections to at least two similar OSAs.
- The TCP/IP profile must be defined properly.

If an OSA port fails while there is a backup OSA port available on the same subnetwork, TCP/IP informs the backup adapter which IP address (real or VIPA) is to take over, and network connections are maintained. After it is set up correctly, the fault tolerance that is provided by the ARP takeover function is automatic.

Figure I-1 on page 239 illustrates our test environment for ARP takeover. We defined CHPID 03 and 05 as OSD type CHPIDs.

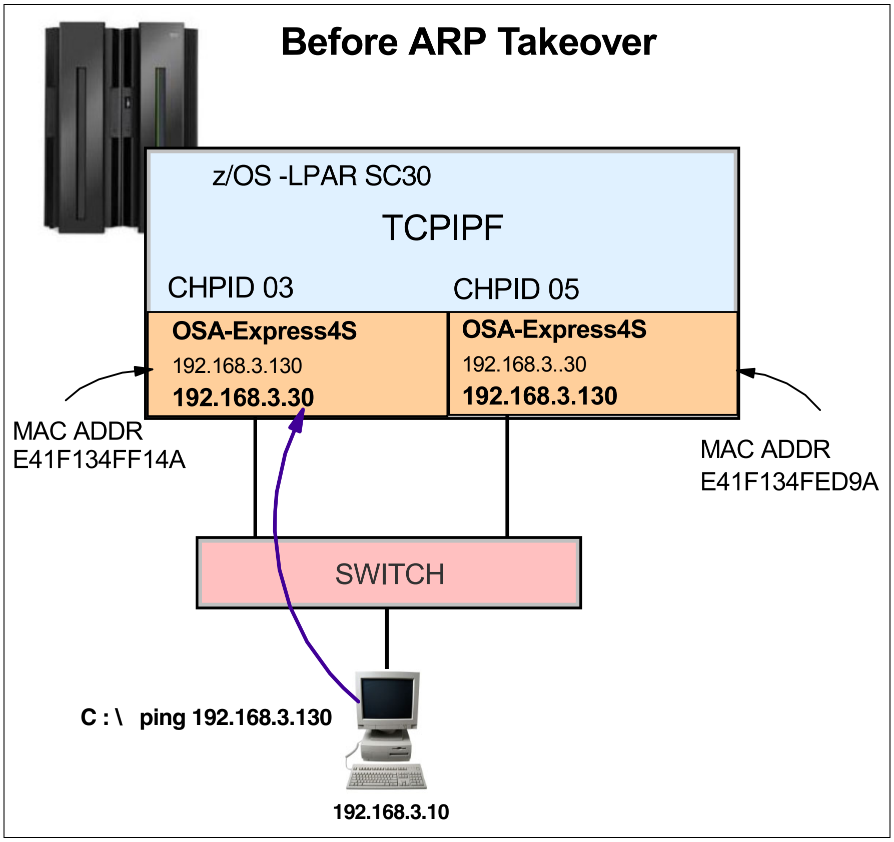


Figure I-1 Test environment before ARP takeover

Note: For demonstration purposes, these examples show a single-switch environment. However, to avoid single points of failure, always separate your OSA connections across multiple switches.

ARP takeover definitions

We updated the TCP/IP profile to support ARP takeover. We also modified the switch configuration to support ARP takeover.

TCP/IP definitions

Example I-1 on page 240 shows the items that we changed or added in our TCP/IP profile for ARP takeover support.

Example I-1   OSA TCP/IP profile

```
IPCONFIG MULTIPATH DATAGRAMFWD

 DEVICE OSA20A0 MPCIPA                    ; OSD Devices on CHPID 03
 LINK OSA20A0LNK  IPAQENET  OSA20A0

 DEVICE OSA20E0 MPCIPA                    ; OSD Devices on CHPID 05
 LINK OSA20E0LNK  IPAQENET OSA20E0
HOME
   192.168.3.30 OSA20A0LNK
   192.168.3.130 OSA20E0LNK

BEGINROUTES
ROUTE 192.168.3.0 255.255.255.0 =     OSA20A0LNK     MTU 1492
ROUTE 192.168.3.0 255.255.255.0 =     OSA20E0LNK     MTU 1492
ROUTE DEFAULT    192.168.3.1 OSA20A0LNK MTU 1492
ROUTE DEFAULT    192.168.3.1 OSA20E0LNK MTU 1492
ENDROUTES

START OSA20A0
START OSA20E0
```

In the `IPCONFIG` statement, we added `MULTIPATH` to allow multiple path definitions to the same network (or subnetwork). A `DEVICE` and `LINK` statement were needed for each of the two OSA ports that we switch between for the test. Notice the `ROUTE` statements that define two paths to get to the same network.

Normal status

Example I-2 shows the status of `LANGROUP` and `VIPAOWNER` before a failure.

Example I-2   Display result of a NETSTAT,DEV command before takeover

```
D TCPIP,TCPIPF,N,DEV
LANGROUP: 00002 1
LANGROUP: 00002
   NAME             STATUS      ARPOWNER          VIPAOWNER
   ----             ------      --------          ---------
   OSA20A0LNK       ACTIVE      OSA20A0LNK        YES
   OSA20E0LNK       ACTIVE      OSA20E0LNK        NO
```

In this example, the numbers correspond to the following information:

1. `OSA20A0LNK` and `OSA20E0LNK` belong to `LANGROUP: 00002`.

Ethernet switch definitions

We used the **`set port host`** command to do this because it accomplishes all of the tasks that are required to define a port as an end-station port. This command handles the following settings:

- `channel mode` to off
- `trunk mode` to off
- `port fast start` to enabled

Example I-3 shows an example of executing the command.

Example I-3 Set port host

```
6500-top> (enable) set port host 1/1
Jan 15 04:01:32 %SYS-6-CFG_CHG:Module 1 block changed by Console//
Port(s) 1/1 channel mode set to off.

Warning: Spantree port fast start should be enabled only on ports that are
connected to
a single host. Connecting hubs, concentrators, switches, bridges, and so on, to a
fast start port can cause temporary spanning tree loops. Use with caution.

Spantree port 1/1 fast start enabled.
Port(s) 1/1 trunk mode set to off.
```

Verifying ARP takeover

> **Note:** The results that are documented here are for our test with a specific switch. Consult the documentation that is provided by the manufacturer of your switch to determine the requirements to support ARP takeover.

We verified that ARP takeover worked by performing two different tasks:

- Pulling the CAT5/6 cable from the OSA port
- Stopping the device in the TCP/IP stack

Pulling the CAT5 cable

Figure I-2 on page 242 shows our environment after pulling the CAT5/6 cable and the route that the **ping** takes as a result of this.

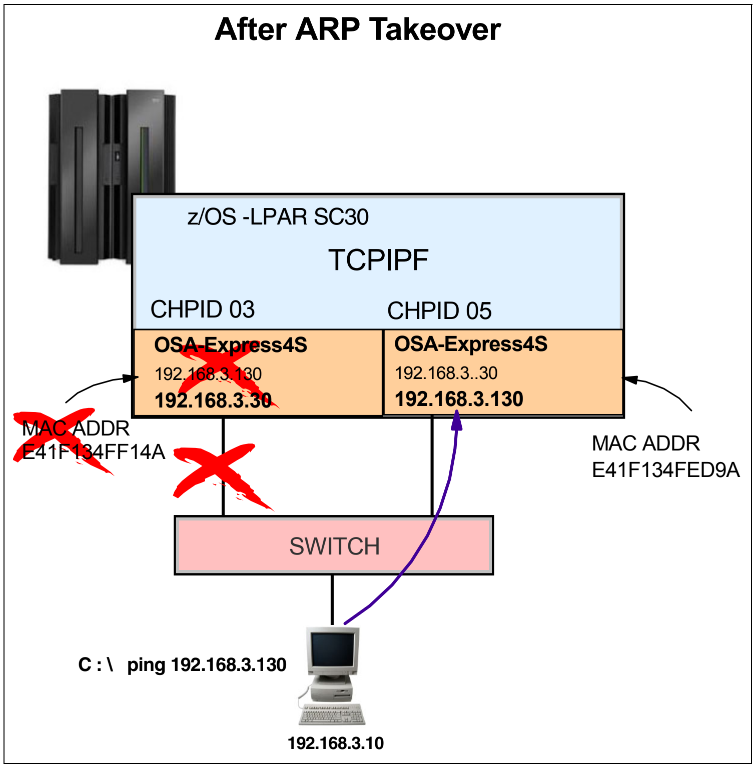


Figure I-2 Test environment after pulling the CAT5/6 cable

Figure I-3 shows the contents of the ARP cache on a Microsoft Windows workstation after pinging each of IP addresses that are defined in TCPIPF before any error condition was introduced.

```
C:\>arp -a

Interface: 192.168.3.10 on Interface 0x3000004
  Internet Address      Physical Address      Type
  192.168.3.130 e4-1f-13-4f-ed-9a dynamic
  192.168.3.30 e4-1f-13-4f-f1-4a dynamic
```

Figure I-3 Windows workstation APR cache (normal)

Notice that `192.168.3.130` is currently assigned to the MAC address associated with CHPID 05. Also `192.168.3.30` is assigned to the MAC address associated with CHPID 03.

Figure I-4 on page 243 shows the contents of the ARP table from the OSA before any error condition was introduced.

```
EZD0101I NETSTAT CS V2R1 TCPIPF
Querying ARP cache for address 192.168.3.130
INTERFACE: OSA20E0LNK      ETHERNET: E41F134FED9A

Querying ARP cache for address 192.168.3.30
INTERFACE: OSA20A0LNK      ETHERNET: E41F134FF14A

Querying ARP cache for address 192.168.3.10
INTERFACE: OSA20A0LNK      ETHERNET: 001641EDB69C
```

Figure I-4 ARP table from OSA TCPIPD (normal)

We pulled the CAT5 cable that connects the OSA port of CHPID 03 from the switch. Figure I-5 shows the resulting messages from the IBM z/OS console.

```
EZD0040I INTERFACE OSA20E0LNK HAS TAKEN OVER ARP RESPONSIBILITY FOR
INACTIVE INTERFACE OSA20A0LNK
EZZ4399I INTERFACE OSA20A0I FAILED - ADAPTER SIGNAL RECEIVED
EZZ4311I LINK OSA20A0LNK HAS FAILED ON DEVICE OSA20A0
```

Figure I-5 z/OS console messages after pulling the CHPID 03 CAT5/6 cable

Figure I-6 shows the contents of the ARP cache of the workstation after pulling the cable for CHPID 03.

```
C:\>arp -a

Interface: 192.168.3.10 on Interface 0x3000004
  Internet Address      Physical Address      Type
  192.168.3.130 e4-1f-13-4f-ed-9a dynamic
  192.168.3.30 e4-1f-13-4f-ed-9a dynamic
```

Figure I-6 Workstation ARP cache after pulling the CHPID 03 CAT5/6 cable

Notice that both IP addresses now point to the same MAC address, which is associated with CHPID 05. Nothing had to be done at the workstation to update the ARP cache. The TCP/IP that is running on z/OS initiated a gratuitous ARP to all hosts on the LAN when it was notified that the connection on CHPID 03 was lost.

Figure I-7 shows the contents of the ARP table on z/OS immediately after pulling the CAT5/6 cable for CHPID 03.

```
EZD0101I NETSTAT CS V2R1 TCPIPF
Querying ARP cache for address 192.168.3.30
INTERFACE: OSA20A0LNK      ETHERNET: E41F134FF14A

Querying ARP cache for address 192.168.1.10
INTERFACE: OSA20A0LNK      ETHERNET: 001641EDB69C

Querying ARP cache for address 192.168.3.130
INTERFACE: OSA20E0LNK      ETHERNET: E41F134FED9A
```

Figure I-7 z/OS TCP/IP ARP table after CAT5/6 cable for CHPID 03 pulled

Notice that there is no change yet in the MAC addresses in this ARP table. After a few minutes, the ARP table contained entries that associated the same IP address with both MAC addresses, as shown in Figure I-8.

```
EZD0101I NETSTAT CS V2R1 TCPIPF
Querying ARP cache for address 192.168.3.10
INTERFACE: OSA20A0LNK      ETHERNET: 001641EDB69C

Querying ARP cache for address 192.168.3.130
INTERFACE: OSA20E0LNK      ETHERNET: E41F134FED9A

Querying ARP cache for address 192.168.3.30
INTERFACE: OSA20A0LNK      ETHERNET: E41F134FED9A
```

Figure I-8   z/OS TCP/IP ARP table minutes after CAT5/6 cable for CHPID 03 pulled

Example I-4 shows the status after takeover.

Example I-4   Display results of a show ARP command after takeover

```
D TCPIP,TCPIPF,N,DEV
LANGROUP: 00002
LANGROUP: 00002
   NAME             STATUS      ARPOWNER          VIPAOWNER
   ----             ------      --------          ---------
   OSA20A0LNK       NOT ACTIVE  OSA20E0LNK        NO 1
   OSA20E0LNK       ACTIVE      OSA20E0LNK        YES
```

1. The interface `OSA20A0LNK` is inactive and is no longer `ARPOWNER`.

Then we cleaned up the ARP table with the **purgecache** command that is available in z/OS Version 2.1. Figure I-9 shows an example of the command.

```
V TCPIP,TCPIPF,PURGECACHE,OSA20A0LNK
EZZ0060I PROCESSING COMMAND: VARY TCPIP,TCPIPD,PURGECACHE,OSA20A0LNK
EZZ9786I PURGECACHE PROCESSED FOR LINK OSA20A0LNK
EZZ0053I COMMAND PURGECACHE COMPLETED SUCCESSFULLY
```

Figure I-9   z/OS PURGECACHE command

When the CAT5/6 cable was plugged back into the switch, we received the messages that are shown in Figure I-10 at the z/OS operator’s console.

```
EZD0041I INTERFACE OSA20A0LNK HAS TAKEN BACK ARP RESPONSIBILITY FROM INTERFACE
OSA20E0LNK
EZZ4313I INITIALIZATION COMPLETE FOR DEVICE OSA20A0
EZZ4340I INITIALIZATION COMPLETE FOR INTERFACE OSA20A0I
```

Figure I-10   CAT5 cable for CHPID 09 plugged into switch

Another gratuitous ARP was issued by TCPIPF to the hosts on the LAN that updated the ARP cache with the correct MAC addresses. On our Windows workstation, the gratuitous ARP updated only existing entries in the ARP cache. It did not create entries for IP addresses that were not currently in ARP cache.

Then, we could verify the result after takeback (see Example I-5).

Example I-5 Display result of a NETSTAT, DEV command after takeback

```
D TCPIP,TCPIPF,N,DEV
LANGROUP: 00002
LANGROUP: 00002
   NAME              STATUS      ARPOWNER          VIPAOWNER
   ----              ------      --------          ---------
   OSA20A0LNK        ACTIVE      OSA20A0LNK        NO 1
   OSA20E0LNK        ACTIVE      OSA20E0LNK        YES
```

In this example, the number **1** indicates that the `OSA20A0LNK` is now active and has its own `ARPOWNER` status back. However, the `OSA20E0LNK` keeps the `VIPAOWNER`. This is because a VIPA belongs to a stack and not to a particular interface; therefore, it does not matter which OSA is the `VIPAOWNER`.

Stopping the device in the TCP/IP stack

In this test, we created an error condition by stopping the device in the TCP/IP stack. Figure I-11 shows the command that was issued and the resulting messages.

```
V TCPIP,TCPIPF,STOP,OSA20A0
EZZ0060I PROCESSING COMMAND: VARY TCPIP,TCPIPF,STOP,OSA20A0
EZZ0053I COMMAND VARY STOP COMPLETED SUCCESSFULLY
EZZ4315I DEACTIVATION COMPLETE FOR DEVICE OSA20A0
EZD0040I INTERFACE OSA20E0LNK HAS TAKEN OVER ARP RESPONSIBILITY FOR
INACTIVE INTERFACE OSA20A0LNK
```

Figure I-11 Induced error by stopping the device in TCPIPF

A gratuitous ARP was sent, and the changes to the ARP tables were identical to those shown in Figure I-6 on page 243 and Figure I-7 on page 243.

We started the device again, as shown in Figure I-12.

```
V TCPIP,TCPIPF,START,OSA20A0
EZZ0060I PROCESSING COMMAND: VARY TCPIP,TCPIPF,START,OSA20A0
EZZ0053I COMMAND VARY START COMPLETED SUCCESSFULLY
EZZ4313I INITIALIZATION COMPLETE FOR DEVICE OSA20A0
```

Figure I-12 Starting the device in TCPIPF

Once again, the gratuitous ARP was sent to update existing ARP cache entries to the correct MAC addresses.

J

Resource Measurement Facility in an OSA environment

The IBM Resource Measurement Facility™ (IBM RMF™) in IBM z/OS software measures and reports on the performance and availability of such system resources as processors, channel paths, devices, and storage. RMF has extended the supported channel types to include the Open Systems Adapter (OSA). It also provides statistics about the bus use and the transfer rate for both the read and write operations in the Channel Activity Report.

The information covers the following topics:

RMF for the Open Systems Adapter

The following RMF reports are associated with the OSA:

- Monitor II Channel Path Activity Report
- Monitor I/Postprocessor Channel Path Activity Report
- Postprocessor Overview Reporting/Recording

Measurements are contained in System Management Facilities (SMF) Record Type 79(13) and are available through the ERBSMFI interface. SMF has been implemented with the field R79CACR, which contains the channel path acronym.

For OSA channel path identifiers (CHPIDs, with device types of OSD, OSE, OSX, and OSM), performance information is provided for three main components:

- Processor use
- Physical PCI bus use
- The bandwidth per port (both read and write directions)

The Channel Path Measurement Facility (CPMF) provides information about CHPIDs on a per-image basis. The Extended CPMF offers the enhancements that supply more data about the channel types.

RMF Monitor II output

The support for OSA CHPIDs (device types OSD, OSE, OSX, and OSM) can be found in an RMF monitor report called the *Channel Activity Report*. Figure J-1 on page 249 shows an example of that report. RMF must be defined with the `DEVICE(COMM)` option in the `ERBRMFxx` member from `SYS1.PARMLIB`.

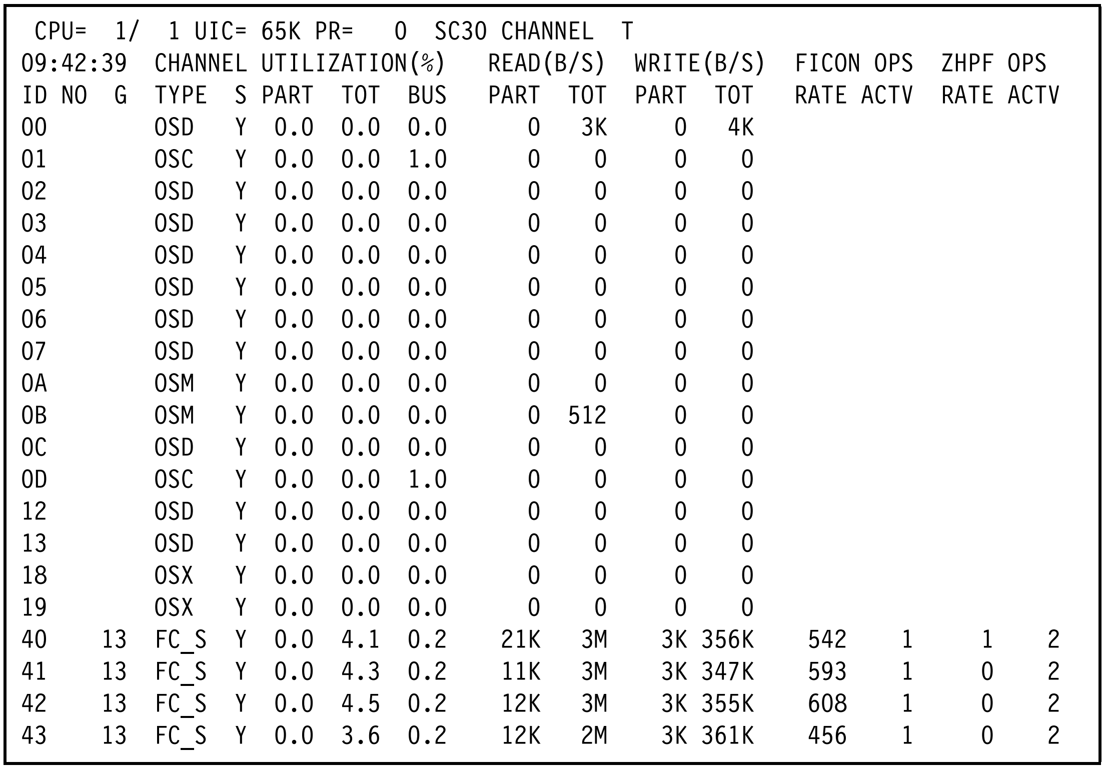
For more information, see the *Resource Measurement Facility User's Guide*, SC33-7990.

The Channel Activity Report

To view the OSA channel activity, complete these steps:

1. In the TSO ISPF Primary Option menu, enter `6` (Command).
2. In the TSO ISPF Command Shell, enter `RMFMON 2`, and then press **Enter**.
3. In the RMF Display menu, press **F4**.

   Figure J-1 shows an example of the Channel Activity Report.



```
 CPU=  1/  1 UIC= 65K PR=   0  SC30 CHANNEL  T
09:42:39  CHANNEL UTILIZATION(%)   READ(B/S)  WRITE(B/S)  FICON OPS  ZHPF OPS
ID NO  G  TYPE  S PART  TOT  BUS   PART  TOT  PART  TOT   RATE ACTV  RATE ACTV
00        OSD   Y  0.0  0.0  0.0      0   3K     0   4K
01        OSC   Y  0.0  0.0  1.0      0    0     0    0
02        OSD   Y  0.0  0.0  0.0      0    0     0    0
03        OSD   Y  0.0  0.0  0.0      0    0     0    0
04        OSD   Y  0.0  0.0  0.0      0    0     0    0
05        OSD   Y  0.0  0.0  0.0      0    0     0    0
06        OSD   Y  0.0  0.0  0.0      0    0     0    0
07        OSD   Y  0.0  0.0  0.0      0    0     0    0
0A        OSM   Y  0.0  0.0  0.0      0    0     0    0
0B        OSM   Y  0.0  0.0  0.0      0  512     0    0
0C        OSD   Y  0.0  0.0  0.0      0    0     0    0
0D        OSC   Y  0.0  0.0  1.0      0    0     0    0
12        OSD   Y  0.0  0.0  0.0      0    0     0    0
13        OSD   Y  0.0  0.0  0.0      0    0     0    0
18        OSX   Y  0.0  0.0  0.0      0    0     0    0
19        OSX   Y  0.0  0.0  0.0      0    0     0    0
40     13 FC_S  Y  0.0  4.1  0.2    21K   3M    3K 356K    542    1     1    2
41     13 FC_S  Y  0.0  4.3  0.2    11K   3M    3K 347K    593    1     0    2
42     13 FC_S  Y  0.0  4.5  0.2    12K   3M    3K 355K    608    1     0    2
43     13 FC_S  Y  0.0  3.6  0.2    12K   2M    3K 361K    456    1     0    2
```

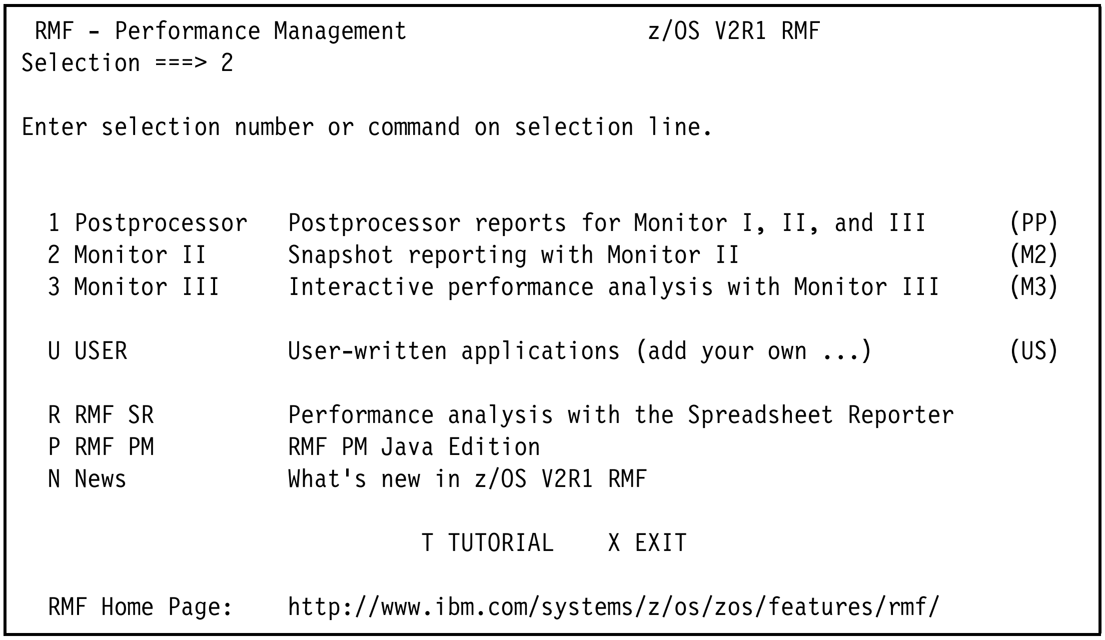
Figure J-1   Channel Activity Report

4. To exit the report, enter `QUIT`.

Alternative method of viewing the report

You can also use the RMF panel to get the Channel Activity Report that is shown in Figure J-1. From the RMF panel (Figure J-2 on page 249), follow these steps:

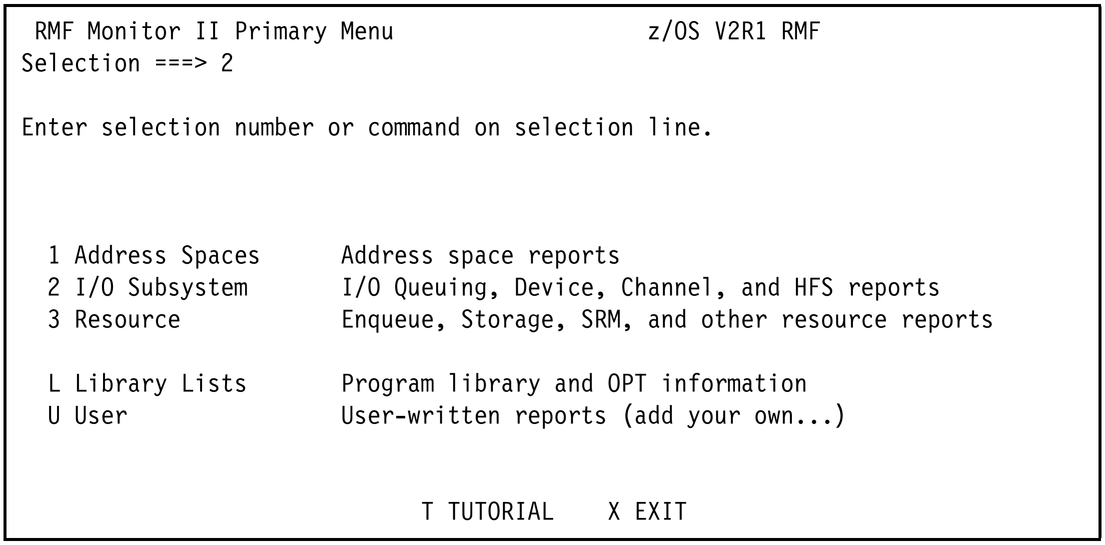
1. From the RMF main panel (Figure J-2 on page 249), enter `2` (Monitor II).



```
 RMF - Performance Management                 z/OS V2R1 RMF
Selection ===> 2

Enter selection number or command on selection line.



  1 Postprocessor   Postprocessor reports for Monitor I, II, and III      (PP)
  2 Monitor II      Snapshot reporting with Monitor II                    (M2)
  3 Monitor III     Interactive performance analysis with Monitor III     (M3)

  U USER            User-written applications (add your own ...)          (US)

  R RMF SR          Performance analysis with the Spreadsheet Reporter
  P RMF PM          RMF PM Java Edition
  N News            What's new in z/OS V2R1 RMF

                              T TUTORIAL    X EXIT

  RMF Home Page:    http://www.ibm.com/systems/z/os/zos/features/rmf/
```

Figure J-2   RMF Main panel

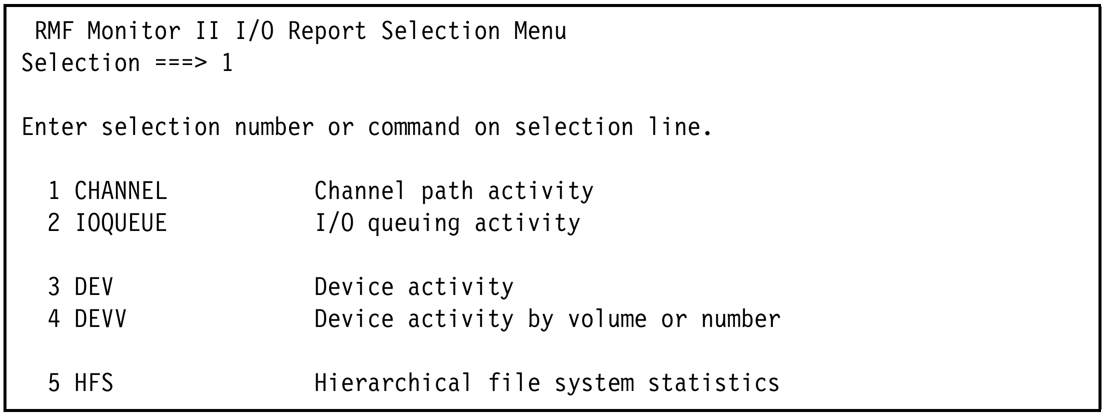
2. At the RMF Monitor II Primary Menu (Figure J-3), enter 2 (I/O Subsystem)



```
 RMF Monitor II Primary Menu                   z/OS V2R1 RMF
Selection ===> 2

Enter selection number or command on selection line.



  1 Address Spaces      Address space reports
  2 I/O Subsystem       I/O Queuing, Device, Channel, and HFS reports
  3 Resource            Enqueue, Storage, SRM, and other resource reports

  L Library Lists       Program library and OPT information
  U User                User-written reports (add your own...)


                              T TUTORIAL    X EXIT
```

Figure J-3 RMF Monitor II Primary Menu

3. At the RMF Monitor II I/O Report Selection Menu (Figure J-4 on page 250), enter 1 (Channel)



```
 RMF Monitor II I/O Report Selection Menu
Selection ===> 1

Enter selection number or command on selection line.

  1 CHANNEL           Channel path activity
  2 IOQUEUE           I/O queuing activity

  3 DEV               Device activity
  4 DEVV              Device activity by volume or number

  5 HFS               Hierarchical file system statistics
```

Figure J-4 RMF Monitor II I/O Report selection menu

4. Press Enter to get the snapshot of the report.

For more information, see *z/OS Resource Measurement Facility Report Analysis,* SC33-7991.

K

Authorization in the IBM z/VM operating system

This appendix describes the topics that are related to the authorization commands that are used in the chapters related to the IBM z/VM operating system. The information focuses on the following topic:

- “z/VM virtual switch authorization” on page 252

z/VM virtual switch authorization

You can restrict the access to the virtual switch function of z/VM software by using native control program (CP) security or an external security manager (ESM), such as Resource Access Control Facility (RACF).

> **Important:** If an ESM is in place, the security definitions that are made by the SET VSWITCH command are overridden by the ESM definitions.

Figure K-1 shows the authorization flow of the **COUPLE** logic.

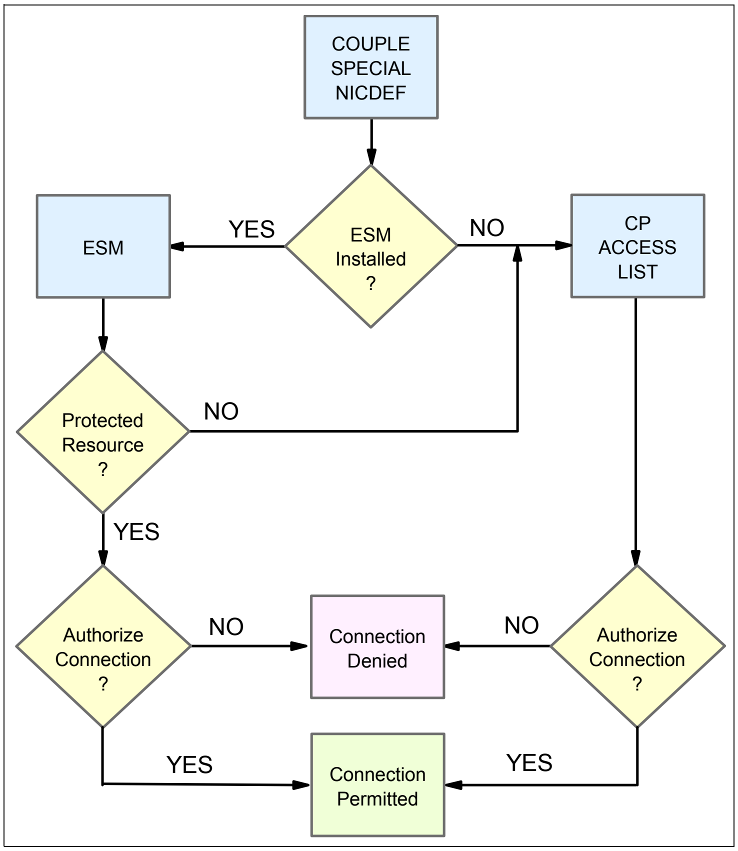


Figure K-1 Authorization flow for COUPLE logic

Running with control program authorization

If you do not have an ESM in place, you can use the CP access authorization function in z/VM. You can control the access to the virtual switch by using the **SET VSWITCH** command. You can see the complete syntax of **SET VSWITCH** command in Chapter 2 of the *z/VM CP Commands and Utilities Reference,* SC24-6175.

To check who has access to a virtual switch, use the **QUERY VSWITCH** command with the **ACCESS** option. In Example K-1 on page 253, you can see the authorized list of user IDs that can connect to VSWITCH L2VSW1.

Example K-1 Query of the authorization list for L2VSW1

```
QUERY VSWITCH L2VSW1 ACC
VSWITCH SYSTEM L2VSW1   Type: QDIO    Connected: 2    Maxconn: INFINITE
  PERSISTENT  RESTRICTED    ETHERNET                  Accounting: OFF
  USERBASED
  VLAN Unaware
  MAC address: 02-00-00-00-00-6E    MAC Protection: Unspecified
  IPTimeout: 5         QueueStorage: 8
  Isolation Status: OFF        VEPA Status: OFF
    Authorized userids:
      LNXRH1   LNXSU1
 Uplink Port:
  State: Ready
  PMTUD setting: EXTERNAL   PMTUD value: 8992
  RDEV: 20C0.P00 VDEV: 0630 Controller: DTCVSW1  ACTIVE
  RDEV: 2043.P00 VDEV: 062A Controller: DTCVSW2  BACKUP
```

To grant access to a virtual switch, use the **`SET VSWITCH GRANT`** command (see Example K-2).

Example K-2 Granting access to L2VSW1

```
SET VSWITCH L2VSW1 GRANT LNXSU1
Command complete
```

If you want to prevent a user from connecting to a virtual switch, use the **`SET VSWITCH REVOKE`** command (see Example K-3).

Example K-3 Revoking access to L2VSW1

```
SET VSWITCH L2VSW1 REVOKE LNXSU1
Command complete
```

You can also grant or revoke access to virtual local area networks (VLANs) that are identified by a VLAN ID. This means that you can determine which VLANs the user can connect to.

Running with Resource Access Control Facility authorization

Since z/VM Version 5.1, an additional resource class called VMLAN has been available. This class is used to protect the **`COUPLE`** function to virtual switches and VLANs. To establish RACF security for virtual switch, you must perform the following actions on your system:

1. Define RACF profiles for each virtual switch.
2. Permit access to guest systems.
3. Activate the VMLAN class.

Defining profiles for each virtual switch

To protect a virtual switch with RACF, it is important to define a RACF profile for each virtual switch in your system. Example K-4 shows our definition for the virtual switch called `L2VSW1`.

Example K-4 Defining a RACF profile for a virtual switch

```
RAC RDEFINE VMLAN SYSTEM.L2VSW1 UACC(NONE)
```

Important: If you do not have a profile for your virtual switch, the CP **ACCESS LIST** command determines the access. See "Running with control program authorization" on page 252, for more information.

Furthermore, you can restrict access to a virtual switch that is being used with VLANs. In Example K-5, we defined a RACF profile for virtual switch L2VSW1 and VLAN ID 0001. This means that virtual guest machines that connect to VLAN ID 0001 must have at least a permission UPDATE for the profile that is shown in Example K-5.

Example K-5 Defining a RACF profile for VLAN restrictions

```
RAC RDEFINE VMLAN SYSTEM.L2VSW1.0001 UACC(NONE)
```

Permitting access to guest systems

To allow a guest system to establish a connection to a virtual switch, you must grant RACF permission to the appropriate profile. In our environment, the guest system that is connected to virtual switch L2VSW1. Example K-6 shows the appropriate RACF command.

Example K-6 Permitting access to a virtual switch

```
RAC PERMIT SYSTEM.L2VSW1 CLASS(VMLAN) ACCESS(UPDATE) ID(LNXSU1)
```

Once the RACF permission is done, the virtual machine can use the CP COUPLE command to connect to the virtual switch. Otherwise, you see an error message as shown in Example K-7.

Example K-7 Failed access to a virtual switch

```
COUPLE 8000 SYSTEM L2VSW1
HCPNDF6011E You are not authorized to COUPLE to SYSTEM L2VSW1
```

If you want to revoke user access to a virtual switch, use the command that is shown in Example K-8.

Example K-8 Revoking access to a virtual switch

```
RAC PERMIT SYSTEM.L2VSW1 CLASS(VMLAN) ACCESS(UPDATE) ID(LNXSU1) DELETE
```

Activating the RACF VMLAN class

After you define the RACF profile for your virtual switch, you must activate the RACF class (VMLAN). Example K-9 shows the activation command.

Example K-9 Activating the VMLAN class

```
RAC SETROPTS CLASSACT(VMLAN)
```

Important: Before you activate the VMLAN class, you must define a profile for each virtual switch. Otherwise, the guests are unable to contact the virtual switch.

You can find more information about RACF commands in *Security Server RACF Command Language Reference*, SA22-7687.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed description of the topics that are covered in this IBM Redbooks publication.

IBM Redbooks

For information about ordering these publications, see "How to get IBM Redbooks" on page 256. Some of the publications cited here might be available in softcopy only.

- *IBM Communication Controller for Linux on System z V1.2.1 Implementation Guide*, SG24-7223
- *Enterprise Extender Implementation Guide*, SG24-7359
- *IBM System z Connectivity Handbook*, SG24-5444
- *OSA-Express Integrated Console Controller Implementation Guide*, SG24-6364
- *IBM zEnterprise System Technical Introduction*, SG24-8050
- *IBM zEnterprise BC12 Technical Guide*, SG24-8138
- *IBM zEnterprise EC12 Technical Guide*, SG24-8049
- *IBM zEnterprise System Technical Introduction*, SG24-7832
- *Enhanced Networking on IBM z/VSE*, SG24-8091
- *Introduction to the New Mainframe: z/VSE Basics*, SG24-7436
- *IBM z/OS V2R1 Communications Server TCP/IP Implementation Volume 4: Security and Policy-Based Networking*, SG24-8099.

Other publications

These publications are also relevant as further information sources:

- *Open Systems Adapter-Express Customer's Guide and Reference*, SA22-7935
- *Open Systems Adapter/Support Facility on the Hardware Management Console*, SC14- 7580
- *Resource Measurement Facility User's Guide*, SC33-7990
- *Resource Measurement Facility Report Analysis,* SC33-7991
- *Device Drivers, Features and Commands*, SC33-8289
- *Communications Server: IP Systems Administrator's Commands*, SC31-8781
- *Communications Server: IP Configuration Guide*, SC31-8775
- *Communications Server: IP Configuration Reference,* SC31-8776
- *Communications Server: IP Diagnosis Guide*, GC31-8782
- *Communications Server: SNA Diagnosis Vol. 1, Techniques and Procedures,* GC31-6850
- *Communications Server SNA Resource Definition Reference*, SC31-8778
- *Communications Server: SNA Operation*, SC31-8779

- *Communications Server: SNA Network Implementation Guide,* SC31-8563
- *Communications Server: IPv6 Network and Application Design Guide*, SC31-8885
- *z/OS MVS Diagnosis: Tools and Service Aids*, GA22-7589
- *MVS Installation Exits*, SA22-7593
- *Support Element Operations Guide,* SC28-6860
- *Security Server RACF Command Language Reference*, SA22-7687.
- z/VM Connectivity Version 6 Release 3, SC24-6174
- *z/VM CP Commands and Utilities Reference*, SC24-6175
- *z/VM TCP/IP User's Guide*, SC24-6240
- *z/VM TCP/IP Planning and Customization*, SC24-6019
- *z/VSE Planning*, SC33-8301
- *z/VSE Administration*, SC33-8304
- *z/VSE Operation*, SC33-8309
- *z/VSE V5R1 e-business Connectors User's Guide*, SC34-2629
- *z/VSE V5R1 TCP/IP Support*, SC34-2640
- *IP6VSE Installation Guide*, SC34-2616

Online resources

These websites and pages are also relevant as further information sources:

- System z networking

  http://www.ibm.com/servers/eserver/zseries/networking/

- System z networking white papers

  http://www.ibm.com/servers/eserver/zseries/networking/wpapers.html

- z/VM virtual networking

  http://www.vm.ibm.com/virtualnetwork/

- IBM Resource Link

  http://www.ibm.com/servers/resourcelink/

- OSA/SF on the Hardware Management Console

  http://www.ibm.com/support/docview.wss?uid=isg24ee3e5124568369385257ba600527f12

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

IBM

Redbooks

OSA-Express Implementation Guide

(0.5" spine)
0.475"<->0.873"
250 <-> 459 pages

OSA-Express Implementation Guide

Product, planning, and quick start information

Realistic examples and considerations

Hardware and software setup definitions

This IBM Redbooks publication will help you to install, tailor, and configure the Open Systems Adapter (OSA) features that are available on IBM zEnterprise servers. It focuses on the hardware installation and the software definitions that are necessary to provide connectivity to LAN environments. This information will help you with planning and system setup. This book also includes helpful utilities and commands for monitoring and managing the OSA features.

This information will be helpful to systems engineers, network administrators, and system programmers who plan for and install OSA features. The reader is expected to have a good understanding of IBM System z hardware, Hardware Configuration Definition (HCD) or the input/output configuration program (IOCP), Open Systems Adapter Support Facility (OSA/SF), Systems Network Architecture/Advanced Peer-to-Peer Networking (SNA/APPN), and TCP/IP protocol.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

SG24-5948-06 ISBN 0738439436