

3745 Communication Controller Model A
3746 Nways Multiprotocol Controller
Models 900 and 950



Planning Series:

Management Planning Guide

3745 Communication Controller Model A
3746 Nways Multiprotocol Controller
Models 900 and 950



Planning Series:

Management Planning Guide

Note!

Before using this information and the product it supports, be sure to read the general information under “Notices” on page xiii.

Second Edition (September 2000)

This edition applies to the 3745 Communication Controller Models A and 3746 Nways® Multiprotocol Controller Models 900 and 950.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

A form for readers' comments appears at the back of this publication. If the form has been removed, address your comments to:

Department CGFA
Design & Information Development
IBM Corporation
PO Box 12195
Research Triangle Park NC 27709
U.S.A.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 1988, 2000. All rights reserved.

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

Contents

Figures	ix
Tables	xi
Notices	xiii
Electronic Emission Notices	xiv
Industry Canada Class A Emission Compliance Statement	xiv
Avis de conformité aux normes d'Industrie Canada	xiv
European Union (EU) Mark of Conformity Statement	xiv
Japanese Voluntary Control Council for Interference (VCCI) Statement	xv
Korean Communications Statement	xvi
Taiwanese Class A Warning Statement	xvi
New Zealand Radiocommunications (Radio) Regulations	xvi
Notice to UK Users	xvi
Trademarks	xvii
Year 2000 Statement	xviii
What Is New in This Book	xviii
 About this Guide	 xix
Who Should Use the 3745/3746 Planning Series	xxii
Where to Find More Information	xxii
Additional Information on the Web	xxiii
CD-ROM	xxiii
Accessing CD-ROM Information	xxiv
How to Use the 3745/3746 Planning Series	xxv
Finding Your Way Around in the New Planning Series	xxviii
 Chapter 1. 3746 Management Overview	 1
NetView for OS/390 Management of APPN Networks Overview	2
SNATAM Structural Overview	3
VTAM CMIP Services	4
SNATAM Topology Manager Overview	5
SNATAM Topology Data	5
NGMF Graphic Views of APPN	5
Topology Manager Functions	6
APPN Topology Integrator	8
How the Topology Manager and Integrator Work Together	8
NetView for OS/390 Management of IP Networks	10
Managing System	10
MultiSystem Manager Presentation Services	12
Manager-to-Agent Communication	12
RUNCMD	12
Alerts and Resolutions	12
Monitoring Resources	12
The MSM IP Tower	13
Example IP Views	14
The View Hierarchy	14
NetView for AIX V3-to-MultiSystem Manager Communication	17
NetView for MVS to AIX Service Point Communication	18
Performance Management	19

Reporting Service Processor and NNP CPU and Memory Use	19
The Need for Performance Monitoring	19
Present Performance Monitoring on SNA Networks	19
NetView Performance Monitor Support Details	20
APPN Resource Management Using NetView RUNCMD	20
NetView for AIX Management of IP Networks	21
Managing Your IP Resources with SNMP	22
Managers and Agents	22
Traps	22
NetView for AIX Examples	23
SNMP Management of APPN Networks	24
NetView Alerts	25
External Box Errors	25
Internal Box Errors	25
Focal Points	25
Paths for Reporting Alerts to NetView	26
Path for Reporting Network Node Processor Alerts	27
Paths for Reporting MOSS-E Alerts	27
Parameter Definitions for Reporting Alerts to NetView	28
Network Node Processor Alerts	29
MOSS-E Alerts: Mainstream Path Definitions for APPN/HPR Path	29
MOSS-E Alerts: Mainstream Path Definitions for SNA/Subarea Path	31
MOSS-E Alerts: Alternate Path Definition	33
Generate MOSS-E Alerts	34
To Generate MOSS-E Alerts	34
To Not Generate MOSS-E Alerts	34
To Locate the Generate Alerts Parameter	34
NetView V2R4 Alert Code Point Customizing	34
Service Processor and Network Node Processor	35
Do Not Use Service LAN for User Stations	35
Token-Ring LAN Bridges	35
Unplugged Cables and Stations	36
Controller Operations when the Service Processor is Not Available	36
Recommendations for Customer Operations	37
Save Configuration	37
Save Microcode	37
Backing Up Your Service Processor	38
Ordering and Setting Up a Backup Service Processor	38
Controller Operations when the Network Node Processor Is Not Available	39
APPN/HPR Network Node	39
IP Routing	39
Dual Network Node Processors	40
 Chapter 2. 3746 APPN/HPR Network Node Management	 41
NetView APPN/HPR Topology Management	41
Configuring APPN/HPR Topology Management	42
Host Definitions	42
CCM Definitions	42
NetView Graphic Monitor Facility Topology Examples	43
Local 3746 APPN/HPR Topology Management from the Service Processor	45
Local APPN Topology Examples	45
Definitions for Performance Monitoring on APPN/HPR	45
3746 Definitions for NPM	47
CCM Station Definitions on Port 2080	48

DLUR/DLUS Definitions	51
Host VTAM and NPM Definitions	51
Chapter 3. MAE APPN/HPR Network Node Management	53
APPN/HPR Alerts	53
Supported Message Units	54
Logging of APPN Alerts on the Router	54
Managing the Network Node Functions from an SNMP Manager	54
MIBs Provided by APPN	54
Providing Topology Information to the SNA Topology Manager	55
MAE (FC 3000) SNMP Configuration	56
Chapter 4. Performance Management with NetView Performance Monitor	59
The Need for Performance Monitoring	59
Current Performance Monitoring on SNA Networks	59
Migrating to APPN/HPR Performance Monitoring	60
Data Collected for the NetView Performance Monitor	61
Performance monitoring data	61
Accounting data	63
Chapter 5. Remote Customer Consoles	65
Using TME 10 Remote Control (DCAF)	65
Using Java Console	66
Customer Consoles	66
Minimum Workstation Configuration	68
DCAF Consoles	68
DCAF Hardware Requirements	69
Java Console	69
Telnet Access	69
Service Processor Parameters	69
For DCAF	70
For DCAF Consoles Using Communications Manager/2	70
For DCAF Consoles Using TCP/IP	71
For Java Console	72
Remote Access Program Installation and Configuration	73
TME 10 Remote Control (DCAF) Installation and Configuration	73
DCAF Remote Access Security	73
DCAF Secure	74
DCAF Non-secure	74
Disabling of Incoming Calls	75
Java Console Installation and Configuration	75
Chapter 6. Connecting to the IBM Remote Support Facility	77
Automatic Microcode Download	78
Parameter Definitions for RSF	79
Customer Information	79
RSF Authorization	79
Automatic/Microcode Download Option	80
RSF Modem	80
Chapter 7. 3746 IP Router Management	81
Managing Your 3746 IP Resources	81
3746-9x0 SNMP Functions	82
Management Information Base (MIB) Support for 3746 IP Router	82

3746-9x0 SNMP Agent Functions	82
3746-9x0 SNMP Relay	82
Distributed Agents	83
SNMP Traps	84
Definitions for SNMP Management	84
Setting the SNMP Information from CCM	86
Managing IP Resources via DCAF	87
Local IP Resource Management from the Service Processor	87
Supported RFCs	88
CDLC Protocol	89
 Chapter 8. X.25 Network Management	 91
Fault Management	91
Accounting and Performance Monitoring through NPM	91
SNMP	91
 Appendix A. MOSS-E Worksheets for Controller Installation	 93
Parameter Definitions for Reporting Alerts to NetView	93
Network Node Processor Alerts	93
MOSS-E Alerts: Mainstream Path Definition	93
APPN/HPR Network	93
SNA/Subarea Network	93
MOSS-E Alerts: Alternate Path Definition	93
Generate MOSS-E Alerts	93
Performance Management CM/2 Parameters (NPM)	94
Service Processor Parameters for DCAF using CM/2	94
For LAN-Attached Consoles	94
For SNA-Attached Consoles	94
For APPN/HPR-Attached Consoles	94
For IP-Attached Consoles	94
For Modem-Attached Consoles	94
Service Processor Parameters for Java Console	95
Choice of Remote Access	95
Remote Access Security	95
DCAF Security Choice	95
DCAF Non-Secure Remote Logon Password	95
Disable Incoming Calls (to Service Processor)	96
Parameter Definitions for RSF	96
Customer Information	96
Remote Support Facility Authorization	96
Set Automatic Microcode Download Option	96
 Appendix B. MOSS-E Service Processor Customization Function	 97
 Appendix C. ESCON MIB	 103
 List of Abbreviations	 113
 Glossary	 117
 Bibliography	 121
Customer Documentation for the 3745 (All Models), and 3746 (Model 900)	121
Additional Customer Documentation for the 3745 Models 130, 150, 160, 170, and 17A	127

Customer Documentation for the 3746 Model 950 128
Required Documentation 132
Related Documentation 132

Index 135

Figures

1.	3746 Management Options	1
2.	Structural Overview of SNATAM	4
3.	APPN Topology Example	7
4.	APPN Topology Integrator	9
5.	Detail of MultiSystem Manager and NetView Component Parts	11
6.	The MSM/IP Views at a Glance	15
7.	Domain Manager and IP Network Aggregation Object	15
8.	Display of Segment	16
9.	The Flow of Information between NetView for AIX V3 and NetView for MVS	17
10.	SNA (NCP) Performance Monitoring Activities (3745/3746-900)	20
11.	RUNCMD Path	21
12.	Example IP Network	23
13.	Example IP Segment	23
14.	Example RABM Display	24
15.	NetView Alert Paths over APPN	26
16.	NetView Alert Paths over Subarea	27
17.	Example of Switched Major Node Definition	30
18.	Example of NCP Generation for a Link to the Service LAN, Part 1	31
19.	Example of NCP Generation for a Link to the Service LAN, Part 2	32
20.	Example of Switched Major Node Definition	32
21.	Example of a NCP Generation for an SDLC Link to the NetView program	33
22.	Single Network View	43
23.	More Detailed View of a Network Node	44
24.	Example Management Window for APPN	45
25.	NPM Configuration	46
26.	Active Configuration	48
27.	Stations on Coupler/Port 2080	49
28.	Token-Ring Port Configuration	49
29.	Token-Ring Station Configuration	50
30.	APPN Parameters	51
31.	Example of Switched Major Node	51
32.	Example of Resource Resolution Table	52
33.	NPM Management Menu	52
34.	Navigation Window	56
35.	SNMP General Window	57
36.	SNMP Communities Window	57
37.	SNMP Communities (Details)	58
38.	Types of Traps	58
39.	NPM Data Collection	60
40.	APPN/HPR Performance Monitoring Activities (3746 Network Node)	61
41.	Console Attachments	66
42.	RSF Connections	77
43.	Managing IP Resources with SNMP (3746)	81
44.	3746-9x0 IP SNMP Implementation	82
45.	Distributed SNMP Agents	83
46.	3746-9x0 IP SNMP TRAPs	85
47.	Two SNMP Managers for One 3746 IP Router	85
48.	SNMP Read Access	86
49.	SNMP Traps	87

50.	Service Processor Customization	97
51.	Customer Information Customization	98
52.	SP Time and Date Customization	98
53.	Service LAN Addresses	99
54.	NetView Link(s)/Reporting Customization	99
55.	Token-Ring 3270 Session Customization	99
56.	CCM Remote Configuration	100
57.	Manage Passwords	100
58.	Retain Customization	100
59.	DCAF Customization	101
60.	Point-to-Point Protocol Configuration	101
61.	Console Configuration for Java	102

Tables

1.	Customer Tasks	xxv
2.	Location of Old Planning Guide Chapters in New Planning Guides . . .	xxviii
3.	Summary of Management Options	2
4.	For the PPP Server (Service Processor)	95
5.	For the PPP Client (Remote Station)	95
6.	Either DCAF or Java Console	95
7.	Customer Documentation for the 3745 Models X10 and X1A, and 3746 Model 900	121
8.	Additional Customer Documentation for the 3745 Models 130 to 17A .	127
9.	Customer Documentation for the 3746 Model 950	128

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.

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

Electronic Emission Notices

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Class A Emission Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité aux normes d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

European Union (EU) Mark of Conformity Statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 30. August 1995 (bzw. der EMC EG Richtlinie 89/336).

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach Paragraph 5 des EMVG ist die IBM Deutschland Informationssysteme GmbH, 70548 Stuttgart.

Informationen in Hinsicht EMVG Paragraph 3 Abs. (2) 2:

Das Gerät erfüllt die Schutzanforderungen nach EN 50082-1 und EN 55022 Klasse A.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

“Warnung: Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen.”

EN 50082-1 Hinweis:

“Wird dieses Gerät in einer industriellen Umgebung betrieben (wie in EN 50082-2 festgelegt), dann kann es dabei eventuell gestört werden. In solch einem Fall ist der Abstand bzw. die Abschirmung zu der industriellen Störquelle zu vergrößern.”

Anmerkung:

Um die Einhaltung des EMVG sicherzustellen, sind die Geräte, wie in den IBM Handbüchern angegeben, zu installieren und zu betreiben.

Japanese Voluntary Control Council for Interference (VCCI) Statement

This product is a Class A Information Technology Equipment and conforms to the standards set by the Voluntary Control Council for Interference by Technology Equipment (VCCI). In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korean Communications Statement

Please note that this device has been certified for business purpose with regard to electromagnetic interference. If you find this is not suitable for your use, you may exchange it for one of residential use.

A급 기기(업무용)

이 기기는 업무용으로 전자파적합등록을 받은 기기이오니
판매자 또는 이용자는 이점을 주의하시기 바라며, 만약
구입하였을 때에는 구입한 곳에서 가정용으로 교환하시기
바랍니다.

Taiwanese Class A Warning Statement

警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這種
情況下，使用者會被要求
採取某些適當的對策。

New Zealand Radiocommunications (Radio) Regulations

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Notice to UK Users

The IBM 3746 Model 900 and IBM 3746 Model 950 are manufactured according to the International Safety Standard IEC950 and, as such, is approved in the UK under the General Approval number NS/G/1234/J/100003.

The Active Remote Couplers (ARCs) and the X.21 Interface, housed within the 3746 Model 900 and 3746 Model 950, are approved separately, each having their own independent approval number. These interface adapters, supplied by IBM, do not contain excessive voltages. An excessive voltage is one which exceeds 42.4 V peak ac or 60 V dc. They interface with the 3746 Model 900 or 3746 Model 950, using Safe Extra Low Voltages only.

In order to maintain the independent approval of the IBM adapters, it is essential that other optional cards, not supplied by IBM, do not use mains voltages or any

other excessive voltages. Seek advice from a competent engineer before installing other adapters not supplied by IBM.

Trademarks

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

AIX	MVS/ESA
ACF/VTAM	MVS/XA
Advanced Peer-to-Peer Networking	Nways
APPN	Operating System/2
AS/400	OS/2
CICS	OS/390
DB2	Processor Resource/Systems Manager
Enterprise Systems Connection Architecture	RETAIN
Extended Services	RS/6000
ESCON	S/370
ESCON XDF	S/390
ES/3090	S/390 Parallel Enterprise Server
ES/9000	System/36
IBM	System/370
LPDA	System/390
Multiprise	SystemView
MVS	VM/ESA
	VSE/ESA
	VTAM

NetView and Tivoli are trademarks of Tivoli Systems, Inc. in the United States, or other countries, or both.

Freelance is a trademark of Lotus Development Corporation in the United States, or other countries, or both.

Java, all Java-based trademarks and logos, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation.

Intel and Pentium are registered trademarks of Intel Corporation in the U.S. and other countries.

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

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

Year 2000 Statement

This product is Year 2000 ready. When used in accordance with its associated documentation, it is capable of correctly processing, providing, and/or receiving date data within and between the 20th and 21st centuries, provided all other products (for example, software, hardware, and firmware) used with the product properly exchange accurate date data with it.

For more information, refer to:

<http://www.ibm.com/year2000>

The 3745 and 3746 controllers require a certain level of microcode to be Year 2000 ready. For more detailed information, access the URL listed above and click **Product Readiness**.

What Is New in This Book

This book has been revised to clarify and correct Network Performance Monitor (NPM) definitions.

The technical changes and additions are indicated by a vertical line (|) to the left of the change.

About this Guide

The *3745/3746 Planning Series* is designed to help you plan the installation and configuration of the IBM 3745 Communication Controller Models A and IBM 3746 Nways® Multiprotocol Controller Models 900 and 950. The *Planning Series* also describes the information you must gather to install and integrate 3746 Controllers into Advanced Peer-to-Peer Networking®/High-Performance Routing (APPN®/HPR) and Internet Protocol (IP) environments.

The *3745/3746 Planning Series* consists of a set of Planning Guides that replace, update and obsolete the *Planning Guide*.

Important:

1. If you already use the existing *Planning Guide*, IBM recommends that you read the new *Planning Series* to learn about new features and to become familiar with the new structure in which planning information is presented.
2. When planning the installation and configuration of 3746 controllers you must use the *IBM 3745 Communication Controller Models A, IBM 3746 Nways Multiprotocol Controller, Models 900 and 950: Overview* along with the *3745/3746 Planning Series* to have all required information.
3. The 3745/3746 documentation is updated periodically in response to your needs and to reflect product evolutions. Because of the time delay necessary to update hard media (books that are printed and available on CD-ROM), it is highly recommended that you check periodically the IBM 3745/3746 documentation on the Web for the latest versions of the documents (see “Additional Information on the Web” on page xxiii).

Refer to the appropriate Planning Guide for the parameters to be customized for the installation and operation of:

- 3745 Communication Controller Models A
- 3746 Nways Multiprotocol Controller Models 900 and 950
- Network Node Processor (NNP)
- Multiaccess Enclosure (MAE)
- Service processor
- Distributed Console Access Facility (DCAF) and TME® 10 remote consoles
- Java™ Console
- Network management

When you define 3746 resources controlled by NCP, record the information in the worksheets provided for the Controller Configuration and Management application.

The *3745/3746 Planning Series* consists of the following planning guides:

Overview, Installation, and Integration

Starts with a general overview of 3746 planning and then explains the various 3745 and 3746 installation and upgrade scenarios.

The guide also explains the options available for the basic integration of the controller and its service processor into your network. There are MOSS-E worksheets for these options, which are to be filled out for the IBM service representative who does the actual controller installation or upgrade. The appendixes:

- Shows the panels of the MOSS-E service processor customization function
- Support offered by each level of the 3746 Licensed Internal Code.

ESCON Channels

After an overview of ESCON® and the adapters, the guide explains the configuration and tuning. This can be done with either the ESCON Generation Assistant (EGA) tool or the Controller Configuration Management (CCM) tool.

The guide also includes examples of various types of ESCON configurations.

Note: For information about using ESCON adapters on the MAE, refer to the *Multiaccess Enclosure Planning* guide.

Token Ring and Ethernet

Helps you with the configuration and definitions of your 3746 Network Node token-ring adapters (TRAs) for APPN/HPR-, IP-, and NCP-controlled traffic.

There are MOSS-E worksheets for the token-ring information needed by the IBM service representative to install or update your machine.

Although no longer available from IBM, the guide explains 3746 Ethernet support and Ethernet adapter configuration.

The token-ring (IEEE 802.5) and Ethernet (IEEE 802.3) standards are discussed in the appendixes.

Note: For Multiaccess Enclosure Ethernet information, refer to the *Multiaccess Enclosure Planning* guide.

Serial Line Adapters

Starts with an overview of the serial line adapters. Next X.25, frame-relay, PPP, and SDLC support are covered.

The two ways that the 3746 supports ISDN (LIC16 adapter¹ and terminal adapters) are explained, including how ISDN lines can be used as backups for other types of lines.

There is an appendix that gives the frame-relay support in each NCP level since frame relay was introduced in NCP Version 6.

Note: For Multiaccess Enclosure ISDN information, refer to the *Multiaccess Enclosure Planning* guide.

Physical Planning

Gives information to help you plan the physical site used by the 3745/3746s frames, service processor, and network node processor: the physical dimensions, electrical characteristics, and so on. It also gives this information for the various components of the 3745/3646, such as the Multiaccess Enclosure, Controller Extension, LICs, LCBs, ARCs, and so on.

The cable descriptions include feature codes (FCs) and part numbers used when ordering them.

¹ No longer being manufactured

The guide includes and explains the controller installation sheets, which show what IBM has installed on your machines.

Plugging sheets for keeping track of your installed LICs, ARCs, and cables are provided along with examples and explanations of their use.

Note: This type of information for the Multiaccess Enclosure is in the *Multiaccess Enclosure Planning* guide.

Management Planning

Starts with a management overview covering:

- Tivoli® NetView®
- Performance Management
- Service processor
- Network Node Processor
- APPN Topology Integrator

Then there are chapters about:

- APPN/HPR Network Node management
- NetView Performance Monitor
- Remote console support
- IBM Remote Support Facility
- 3746 IP router management
- Multiaccess Enclosure APPN/HPR Network Node management
- X.25 network

There are MOSS-E worksheets for the network management parameters needed by the IBM service representative to install or upgrade your machine.

The guide explains the use of the MOSS-E Service Processor Customization.

There is an example of ESCON management information base (MIB) definitions.

Note: For Multiaccess Enclosure management information, refer to the *Multiaccess Enclosure Planning* guide.

Multiaccess Enclosure Planning

Provides information about the Multiaccess Enclosure and its adapters (ATM, ESCON, and so on) and how to configure them.

For information about:

- Multiaccess Enclosure APPN/HPR Network Node management, refer to the *3745/3746 Planning Series: Management Planning*
- Physical site planning and the cables, refer to the *3745/3746 Planning Series: Physical Planning*

Protocols Description

Is an in depth description of these protocols used by the 3746:

- APPN/HPR
- IP

The detailed discussions of how the 3746 and Multiaccess Enclosure support these protocols help you understand the purpose of the protocol parameter definitions and what types of information are needed for the most efficient operation of your 3745/3746-connected networks.

CCM Planning Worksheets, (Online)

These example worksheets for the 3746 and MAE can be used to plan the actual definitions of the many CCM parameters you need to configure your 3746.

This guides is available (in PDF format) on the Web at

<http://www.ibm.com/networking/did/3746bks.html#Customer>

Who Should Use the 3745/3746 Planning Series

The *3745/3746 Planning Series* is intended for network planners, network specialists, and system programmers responsible for collecting the information required for the installation and network integration of 3745 Communication Controller Models A and 3746 Expansion Unit Model 900 in an SNA environment, as well as the 3746-950 and 3746-900 as APPN/HPR network nodes and IP routers.

Where to Find More Information

While planning a migration, you must use the following documents in addition to the *3745/3746 Planning Series* guides:

- IBM *3745 Communication Controller Models A and 170, 3746 Nways Multiprotocol Controller Models 900 and 950: Overview*, GA33-0180
- IBM *3745 Communication Controller All Models, 3746 Nways Multiprotocol Controller Model 900: Console Setup Guide*, SA33-0158 (This guide contains information about remote console access to 3745/3746-900s via an SNA/subarea, APPN, or TCP/IP path and using a modem.)

Also, you may need to use the following additional documents:

- IBM *3746 Nways Multiprotocol Controller Model 900 and 950: Controller Configuration and Management: User's Guide*, SH11-3081 (IBM recommends that you prepare controller definitions before installing a 3746. To obtain a stand-alone version of the Controller Configuration and Management that runs on an OS/2® workstation, contact your IBM marketing representative.)
- *3746 Nways Multiprotocol Controller Model 950: User's Guide*, SA33-0356. (This guide contains information about routine operations, installing and testing the communication line adapters, service processor, and remote consoles.)
- *Planning for Integrated Networks*, SC31-8062.

Be sure to use the latest editions of these documents. This will ensure that you have up-to-date and complete information about the 3746 controllers.

The following *IBM International Technical Support Organization* redbooks provide useful information about 3746 implementation:

- *APPN Architecture and Product Implementations Tutorial*, GG24-3669
- *IBM 3746 Nways Multiprotocol Controller Model 950 and IBM Model 900: APPN Implementation Guide*, GG24-2536
- *Subarea Network to APPN Network Migration Guide*, SG24-4656
- *IBM 3746 Nways Multiprotocol Controller Model 950 and IBM Model 900: IP Implementation Guide*, SG24-4845 (an IBM redbook).

Be sure to see the other relevant documents listed in the bibliography at the back of this guide.

Additional Information on the Web

You can access the latest news and information about IBM network products, customer service and support, and information about microcode upgrades at:

<http://www.ibm.com/>

The latest versions of the *Planning Series* and other 3745/3746 documentation are available in PDF format at:

<http://www.ibm.com/networking/did/3746bks.html#Customer>

CD-ROM

Starting with engineering change F12380, the Licensed Internal Code (LIC) is shipped on a CD-ROM. The complete 3745/3746 documentation set is also included on the CD-ROM.

Examples: 3745 Models A and 3746 *Planning Series*, 3746 NNP and Service Processor Installation and Maintenance Guides, CCM *User's Guide*, 3746-950 *User's Guide*, and others. See the bibliography for the complete name and form number of the books.

3745/3746 documentation is in PDF format. Acrobat Reader for OS/2® is included on the CD-ROM to allow you to read the .PDF files and print all or part of a book.

Accessing CD-ROM Information

To access the CD-ROM from a service processor equipped with a CD-ROM drive, do the following:

- Step 1.** Install the CD-ROM in the service processor CD-ROM drive.
- Step 2.** In the MOSS-E main panel, open the **View** menu and select **Information**.
- Step 3.** Double-click **CD-ROM documentation**. Your browser automatically opens and displays the documentation home page.
- Step 4.** Click any highlighted text (blue and underlined) to go to the material that interests you:
- Click **Documentation** to access 3745/3746 books.
 - Click the icon marked PDF that corresponds to the item that interests you.

The Acrobat Reader automatically opens and displays the file in the full panel mode. Use the **Page Up** and **Page Down** keys to move through the document.

Press **Esc** to display the Reader menus that allow you to print all or part of the file.

When you close the Acrobat Reader, you return to the browser.

When you close the browser, you return to the MOSS-E Documentation menu.

Each document file has one or more of the following identifiers:

- Date
- Form number
- Engineering change level
- Revision code.

Check these identifiers on future releases of the CD-ROM to see if the documents that you use have been updated.

How to Use the 3745/3746 Planning Series

Your Responsibility as a Customer

You are responsible for performing the tasks listed in Table 1. These tasks are not performed by IBM personnel as part of the machine installation and basic operations. They can, however, be performed by IBM on a fee basis.

Table 1 (Page 1 of 3). Customer Tasks

Task	Where to Find Information
Network design:	Network design is not covered in this book. Refer to the following IBM books for SNA, APPN/HPR, and IP network planning guidance: <ul style="list-style-type: none">• <i>Planning for Integrated Networks</i>, SC31-8062• IBM redbooks:<ul style="list-style-type: none">– <i>Subarea Network to APPN Network Migration Guide</i>– <i>IBM 3746 Nways Multiprotocol Controller Model 950 and IBM Model 900: APPN Implementation Guide</i>– <i>IBM 3746 Nways Multiprotocol Controller Model 950 and IBM Model 900: IP Implementation Guide</i>– <i>IBM Nways 2216 Multiaccess Connector Description</i>– <i>IBM 2216 Multiaccess Connector ESCON Solutions</i>
Physical planning: Before the IBM service representative arrives to install your controller, make sure that you have met the necessary requirements for the following: <ul style="list-style-type: none">• Electric power• Floor space with service clearances• Space for the cables• The RSF switched line• The Controller Expansion (FC 5023)• Other components (such as the service processor).	"Physical Planning Details" chapter in the <i>3745/3746 Planning Series: Physical Planning</i>
Controller hardware configuration definitions: Decide what type of attachments (lines) and how many of each type you need.	This input is necessary for the IBM ordering system (CF3745). For more information, refer to the <i>3745/3746 Planning Series: Physical Planning</i> .

Table 1 (Page 2 of 3). Customer Tasks

Task	Where to Find Information
<p>Software definitions and tuning:</p> <ul style="list-style-type: none"> • ESCON port, host link, and station definitions; ESCON resource, TCP/IP, and VTAM® tuning • Token-ring port and station definitions; PU and LU maximum limits; port sharing with NCP-controlled traffic; duplicate addresses; token-ring APPN, IP, and/or NCP resource tuning and VTAM tuning • Serial line (SDLC, PPP, frame-relay, and X.25) port and station definitions; location of CLPs, LICs, LCBs, and ARCs; maximum CLA line connectivity; CLP backups • Multiaccess Enclosure: hardware planning and configuration; software configuration and tuning • Use of the Controller Configuration and Management (CCM) application. 	<p>Refer to:</p> <ul style="list-style-type: none"> • “ESCON Adapters” chapter in the <i>3745/3746 Planning Series: ESCON Channels</i> • “ESCON Channel Adapter” chapter in the <i>3745/3746 Planning Series: Multiaccess Enclosure Planning</i> • “ESCON Configuration Examples” chapter in the <i>3745/3746 Planning Series: ESCON Channels</i> • “Token-Ring Adapters” chapter in the <i>3745/3746 Planning Series: Token Ring and Ethernet</i> • “Serial Line Adapters” chapter in the <i>3745/3746 Planning Series: Serial Line Adapters</i> • “3746 SDLC Support” chapter in the <i>3745/3746 Planning Series: Serial Line Adapters</i> • <i>3745/3746 Planning Series: Multiaccess Enclosure Planning</i> • <i>3745/3746 Planning Series: Physical Planning</i> • <i>IBM Controller Configuration and Management User's Guide, SH11-3081.</i> <p>Also refer to:</p> <ul style="list-style-type: none"> • <i>IBM 3746 Nways Multiprotocol Controller Model 950 and IBM Model 900: APPN Implementation Guide</i> (an IBM redbook) • <i>IBM 3746 Nways Multiprotocol Controller Model 950 and IBM Model 900: IP Implementation Guide</i> (an IBM redbook).
<p>Filling out:</p> <ul style="list-style-type: none"> • 3746 plugging sheets To keep a record of the processors and couplers (and their addresses) installed in the 3746 frame. • <i>CCM User's Guide, SH11-3081</i> worksheets To plan the 3746 and MAE logical resource definitions. They can then be used when configuring the 3746 and MAE via the CCM. 	<p>Refer to:</p> <ul style="list-style-type: none"> • “Plugging Sheets for 3745 and 3746” chapter in the <i>3745/3746 Planning Series: Physical Planning</i> • <i>3745/3746 Planning Series: CCM Planning Worksheets</i>

Table 1 (Page 3 of 3). Customer Tasks

Task	Where to Find Information
<p>NetView definitions in VTAM, the MOSS-E, NPM, CCM, NetView/360, and Tivoli NetView® (formerly NetView for AIX) for:</p> <ul style="list-style-type: none"> • APPN traffic • IP traffic • NetView alert path. 	<p>Refer to:</p> <ul style="list-style-type: none"> • “3746 Management Overview” chapter in the <i>3745/3746 Planning Series: Management Planning</i> • “3746 APPN/HPR Network Node Management” chapter in the <i>3745/3746 Planning Series: Management Planning</i> • “3746 IP Router Management” chapter in the <i>3745/3746 Planning Series: Management Planning</i>.
<p>Controller, service processor, and network node processor definitions. For example:</p> <ul style="list-style-type: none"> • Link IPL port information • Password management • NetView alert reporting path definitions • DCAF LU definitions • Ethernet port definitions for SNMP • Service processor token-ring and IP LAN addresses. 	<p>Refer to “Controller and Service Processor Integration” chapter in the <i>3745/3746 Planning Series: Overview, Installation, and Integration</i>.</p> <p>Fill out the worksheets in the various <i>Planning Series</i> guides. These worksheets are used by the IBM service representative during installation.</p>
<p>Remote console definitions (using DCAF):</p> <ul style="list-style-type: none"> • Ensure that the necessary hardware and software is available for the type of console attachment chosen • Service processor definitions for DCAF • DCAF installation and configuration on the remote console. 	<p>Refer to:</p> <ul style="list-style-type: none"> • “Remote Customer Consoles” chapter in the <i>3745/3746 Planning Series: Management Planning</i> • For the 3746-900, refer to the <i>3745 Console Setup Guide</i> • For the 3746-950, refer to the <i>IBM 3746 Nways Multiprotocol Controller Model 950 User’s Guide</i>
<p>Connection to the IBM remote support facility (RSF):</p> <ul style="list-style-type: none"> • Service processor connection (modem) definitions • Customer definitions for RSF records. 	<p>Refer to the “Connecting to the IBM Remote Support Facility” chapter in the <i>3745/3746 Planning Series: Management Planning</i></p>
<p>Problem determination through the MOSS-E and NetView</p>	<p>For the 3746-900, refer to:</p> <ul style="list-style-type: none"> • <i>Problem Analysis Guide</i> accessed online from the MOSS-E • <i>3745 Models A: Alert Reference Guide</i> • <i>3745 All Models: Advanced Operators Guide</i>

Finding Your Way Around in the New Planning Series

If you are familiar with the layout of the old *3745 Communication Controller Models A and 3746 Models 900 and 950: Planning Guide*, GA33-0457, Table 2 should help you find which of the eight new books of the planning series contains the information that you need.

Note: Some of the chapters in the *Planning Guide* have been split into two or more new chapters in one or more new guides.

Table 2 (Page 1 of 2). Location of Old Planning Guide Chapters in New Planning Guides

Old Planning Guide		New Planning Series Book	
Chapter	Chapter Name	Chapter(s)	Guide Name
1	3745 and 3746 General Information	--	Not included in the new guides
2	APPN/HPR Overview	1	<i>Protocols Description</i>
3	Internet Protocol (IP) Overview	2	<i>Protocols Description</i>
4	3746 ATM Support	4	<i>Multiaccess Enclosure Planning</i>
5	Token-Ring/802.5	B	<i>Token-Ring and Ethernet</i>
6	Ethernet Overview	C	<i>Token-Ring and Ethernet</i>
7	Frame Relay Overview	4, 5	<i>Serial Line Adapters</i>
8	Point-to-Point Protocol (PPP) Overview	4	<i>Serial Line Adapters</i>
9	X.25 Overview	2, 3, 5, 7	<i>Serial Line Adapters</i> <i>Management Planning</i>
10	ISDN Adapters	8	<i>Serial Line Adapters</i>
11	ESCON Overview	1	<i>ESCON Channels</i>
12	3745 and 3746 Installation and Upgrade Scenarios	2	<i>Overview, Installation, and Integration</i>
13	Configuration Scenarios	6	<i>Multiaccess Enclosure Planning</i>
14	3746 Planning Overview	1	<i>Overview, Installation, and Integration</i>
15	ESCON Adapters	1, 2, 3	<i>ESCON Channels</i>
16	Token-Ring Adapters	1, 2, 3	<i>Token-Ring and Ethernet</i>
17	Ethernet Adapters	4, 5	<i>Token-Ring and Ethernet</i>
18	Serial Line Adapters	1	<i>Serial Line Adapters</i>
19	3746 SDLC Support	3, 4	<i>Serial Line Adapters</i>
20	Multiaccess Enclosure	1	<i>Multiaccess Enclosure Planning</i>
21	Multiaccess Enclosure Adapters Overview	2	<i>Multiaccess Enclosure Planning</i>
22	ESCON Channel Adapter	8	<i>Multiaccess Enclosure Planning</i>
23	Multiaccess Enclosure ISDN Support	5	<i>Multiaccess Enclosure Planning</i>
24	3746 Configuration Overview	--	Not included in the new guides
25	Welcome to the CCM	--	Not included in the new guides
26	Multiaccess Enclosure Configuration	7	<i>Multiaccess Enclosure Planning</i>
27	3746 Base Frame ESCON Configuration Examples	1	<i>ESCON Channels</i>
28	Configuring the MAE ESCON Channel Adapter	8	<i>Multiaccess Enclosure Planning</i>

Table 2 (Page 2 of 2). Location of Old Planning Guide Chapters in New Planning Guides

Old Planning Guide		New Planning Series Book	
Chapter	Chapter Name	Chapter(s)	Guide Name
29	3746 Management Overview	1	<i>Management Planning</i>
30	3746 APPN/HPR Network Node Management	2	<i>Management Planning</i>
31	3746 IP Router Management	6	<i>Management Planning</i>
32	MAE APPN/HPR Network Node Management	2	<i>Management Planning</i>
33	MAE IP Router Management	6	<i>Management Planning</i>
34	Controller and Service Processor	3	<i>Overview, Installation, and Integration</i>
35	Customer Consoles and DCAF	4 1 1	<i>Management Planning</i> <i>Overview, Installation, and Integration</i> <i>Token-Ring and Ethernet</i>
36	Connecting to the IBM Remote Support Facility	5	<i>Management Planning</i>
37	Performance Management with NetView Performance Monitor	3	<i>Management Planning</i>
37	3746 IP Router Management	6	<i>Management Planning</i>
38	MOSS-E Worksheets for Controller Installation (3745)	A A A	<i>Overview, Installation, and Integration</i> <i>Management Planning</i> <i>Token-Ring and Ethernet</i>
39	Parameter Cross-Reference Table	B	<i>Overview, Installation, and Integration</i>
40	CCM Worksheets for Controller Configuration Definitions	1	<i>CCM Planning Worksheets (online)</i>
41	Multiaccess Enclosure Worksheets	2	<i>CCM Planning Worksheets (online)</i>
42	Familiarizing Yourself with the Installation Sheets	2	<i>Physical Planning</i>
43	Plugging Sheets for the 3746 Nways Multiprotocol Controller	3	<i>Physical Planning</i>
44	Physical Planning Details	1	<i>Physical Planning</i>
A	3746-9x0 Microcode Levels (EC)	D	<i>Overview, Installation, and Integration</i>
B	ESCOM MIB	A	<i>Management Planning</i>
C	MOSS-E Service Processor Customization Function	C	<i>Overview, Installation, and Integration</i>

Chapter 1. 3746 Management Overview

This chapter gives an overview of network management relevant to the operation of the 3746 Network Node. The addition of the NNP to allow the 3746 to function as a stand-alone APPN network node and/or IP router, and the recent addition of the Multiaccess Enclosure (MAE) with its APPN and IP functions, gives a number of options for managing the hardware and software running in these platforms.

The management tasks associated with the 3746 are:

- Reporting hardware and software alerts
- APPN and IP Topology management
- Configuration management with the CCM (including MAE)
- Performance management with Network Performance Monitor (NPM).

Management can be divided up into local and remote management. Local management is carried out via the service processor (SP), but this can also be done from remote workstations by using DCAF. Remote management is carried out from different platforms, these may be distributed or centralized. Management information is forwarded from the SP, and the APPN and IP control points to management software running on a variety of hardware platforms, different protocols may be used to transport this data.

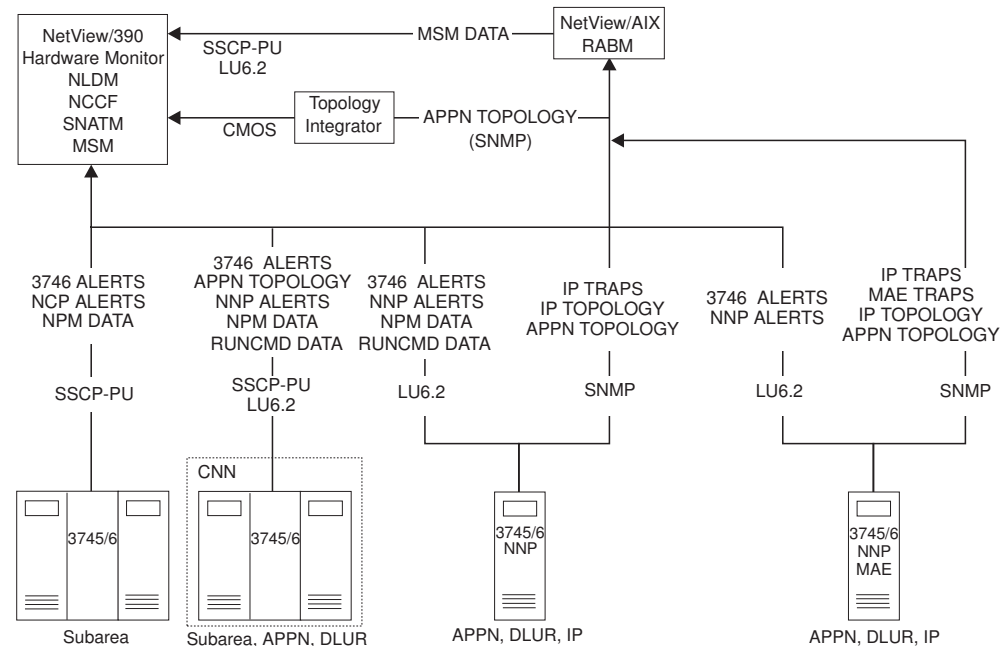


Figure 1. 3746 Management Options

Figure 1 shows the available hardware and software configurations reporting management data to different management platforms. Table 3 on page 2 gives an overview of the management options for each configuration. The options are discussed in greater detail in the following sections.

<i>Table 3. Summary of Management Options</i>				
Networking Architecture	Management Data Available	Management Software	Transport	Refer to:
Subarea SNA	3746 Alerts NCP Alerts NPM Data	NetView for OS/390 NetView for OS/390 NPM	SSCP-PU	Page 59
Subarea SNA APPN (CNN)	3746 Alerts NNP Alerts NPM Data RUNCMD Data	NetView for OS/390 NetView for OS/390 NPM NetView for OS/390	LU6.2 LU6.2 LU6.2 LU6.2 to SSCP-PU	Pages 2 and 59
APPN (NNP) DLUR	3746 Alerts NNP Alerts NPM Data RUNCMD Data	NetView for OS/390 NetView for OS/390 NPM NetView for OS/390	LU6.2	Pages 2 and 59
IP (NNP)	IP Traps IP Topology APPN Topology	NetView/AIX NetView/AIX, MSM RABM, SNATM	SNMP	Pages 10, 21, and 24
APPN (MAE) DLUR (MAE)	3746 Alerts NNP Alerts	NetView for OS/390 NetView for OS/390	LU6.2	"MAE APPN/HPR Network Node Management" chapter in the <i>3745/3746 Planning Series: Multiaccess Enclosure Planning</i>
IP (MAE)	IP Traps MAE Traps IP Topology APPN Topology	NetView/AIX NetView/AIX, MSM NetView/AIX, MSM RABM, SNATM	SNMP	Pages 2, 10, 21, and 24.
APPN (MAE)	SNMP Traps APPN Traps	NetView/AIX	SNMP	

NetView for OS/390 Management of APPN Networks Overview

Tivoli NetView V2R4 includes a feature for managing APPN networks called the NetView APPN Topology and Accounting Management (APPNTAM). This feature works with corresponding agent functions to gather and record data about APPN networks.

NetView V3R1 was enhanced to include functions for managing the topology and status of both subarea and APPN networks. For more information on SNA and APPN management, please refer to *Dynamic Subarea and APPN Management Using NetView V3R1*. For APPN, these enhancements include:

- Integration of the APPN Topology and Accounting Management (APPNTAM) feature into the Enterprise Option of NetView V3R1. It is now called the SNA Topology and Accounting Manager (SNATAM), and it provides support for both APPN and subarea topology.
- The CMIP services function is no longer part of NetView in V3R1. Instead, NetView utilizes the CMIP services function present in VTAM® V4R3 in order to communicate with agents.
- Support for the VTAM SNATAM agent shipped as a part of VTAM V4R3.
- The CM/2 agent is now shipped as part of NetView and has been renamed the APPN Topology and Accounting Agent (APPNTAA). This agent is also available for the IBM 2217 and 3746 NNP.

- Support for the dynamic topology and status of LUs. With the SNA topology manager in NetView Version 3, LU information is not automatically collected from the VTAM agent for all LUs. This choice was made in order to reduce the network traffic and the number of objects created and maintained in NetView's Resource Object Data Manager (RODM). Application LUs and APPN control points will automatically be reported by the VTAM agent to the SNA topology manager when local and network topology is being collected from the VTAM agent.

Note: The NetView RODM is an object-oriented data cache. Objects in RODM represent resources in the network. The data cache is located entirely in the memory of the host processor resulting in fast access to data and high transaction rates.

- Session monitor support for DLUR/S sessions, border nodes, and VR-TGs. The session monitor will be able to indicate whether the SSCP-PU and SSCP-LU sessions are using the Dependent LU Requester/Server (DLUR/S) pipe. The session monitor has also been enhanced to be able to indicate in the APPN route displays whether the APPN route for a session traverses VR-TGs or crosses APPN networks.

The Topology Management function provides the ability to obtain, monitor, control and graphically display the topology of your APPN networks:

- Collection and storage of APPN topology data, including real-time updates, in the RODM data cache
- Dynamic, graphical display of APPN topology, using the NGMF
- Control of SNA ports and links using commands on the NGMF pull-down menus, the operator console, and Command Tree/2.

The Accounting Management function provides the ability to centralize collection of LU 6.2 session and conversation accounting information. This information is logged to the system management facilities (SMF) or a user-defined external log.

You can automate these functions using the NetView automation facilities, such as command lists and the automation table. In addition, you can automate using methods and objects stored in RODM.

SNATAM Structural Overview

SNATAM provides APPN management functions according to a manager-agent relationship. This feature uses the Open System Interconnect (OSI) system management model. Management service is provided by one or more managing systems, which gather and correlate data from multiple managed systems. The managing systems provide this service through one or more management applications, called managers, which communicate using OSI Common Management Information Protocol (CMIP) with management applications at the managed systems, called agents.

The topology manager and accounting manager applications are separate entities that can be installed and initialized independently. You can install the topology manager application on a NetView central system. You can install the accounting manager application on a NetView central system and on a NetView distributed system.

The corresponding SNATAM agent applications reside on VTAM and on APPN NNs and ENs that use the OS/2® Communications Manager/2 platform. The SNATAM agent includes both the topology agent and the accounting agent applications that can be initialized independently.

In all cases, the CMIP services must be active to support the manager-agent communications. Communication between the manager and agent applications is over LU 6.2 sessions using OSI CMIP and the SNA multiple domain support (MDS), this is known as *CMIP Over SNA* (CMOS).

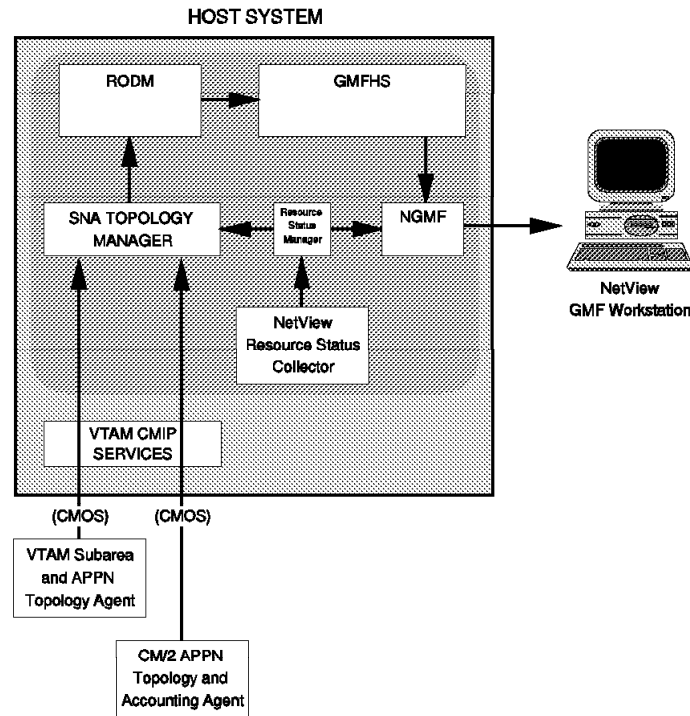


Figure 2. Structural Overview of SNATAM

Figure 2 illustrates the structure of the SNATAM feature. The topology agent on the OS/2 system is gathering and forwarding topology information to the topology manager. The accounting agent is gathering and forwarding accounting data to the accounting manager. Note that each manager application can gather information from multiple agent applications; each agent application can forward data to multiple manager applications.

VTAM CMIP Services

The VTAM CMIP services component allows communication between the SNATAM manager and agent applications using VTAM MS transport. MS transport uses LU 6.2 sessions for the actual communications between systems in the network. The CMIP data exchanged between the manager and agent applications is encapsulated in MDS-MUs and transported over these LU 6.2 sessions using the management services MDS-SEND and MDS-RECEIVE transaction programs. The CMIP services task or program comprises the OSI Layers 5 to 7 and other services, such as internal MIB API.

SNATAM Topology Manager Overview

The topology manager works with one or more topology agents to gather the APPN topology information of your APPN networks, as well as to monitor the networks for any topology or resource status changes. Agent applications can be on APPN network nodes (NNs) and end nodes (ENs). NNs provide network and local topology support; ENs provide local topology support.

The topology agent forwards APPN topology and status information upon request to the topology manager. The topology manager correlates and stores this data in RODM according to the SNATAM topology data model. It dynamically creates objects in RODM and updates the status of these objects as information is received from the topology agents in the network.

The topology manager allows you to manage APPN resources, namely logical links and ports, at the agent nodes. When you issue a command to start monitoring network or local topology, the topology manager sends a request to the agent. The agent sends the requested topology data to the manager, then continues to send status and configuration updates to the manager. The agent also activates and deactivates ports and links when it receives those commands from the manager. An agent can interact with one or more managers, each requesting the same or different data.

SNATAM Topology Data

The SNATAM topology manager gathers topology data from the topology agent nodes in the network. The two types of topology being collected and monitored are:

Network topology

That is, your APPN backbone topology. It contains information about NNs, virtual routing nodes (VRNs), and transmission groups (TGs) between nodes that are part of an APPN intermediate routing network. Topology manager should request network topology from at least one agent network node in each subnetwork.

Local topology

That is, local information about NNs, ENs, and low-entry networking nodes (LENs), the connections between nodes, and the ports and links that make up the connections. A node must have a topology agent installed to support local topology monitoring.

NGMF Graphic Views of APPN

The SNA topology manager uses the NGMF to provide the graphical interface for displaying and monitoring APPN resources stored in RODM. APPN views are updated dynamically as changes occur in the network. This ensures that the most current status and configuration are available to the operator. Operators can use the views to monitor the status of the APPN network, navigate through the network, locate failed resources, activate and deactivate links and ports, and control topology monitoring.

Topology Manager Functions

The functions available with the topology manager enable you to do the following:

- Monitor APPN network topology to view the connectivity between APPN network nodes. The views are updated dynamically with configuration and status changes of the network nodes and the TGs between them.
- Monitor APPN local topology to view agent nodes and their TGs, ports, and logical links. Local topology also displays adjacent NNs, ENs, and LENS. These views are updated dynamically with configuration and status changes to nodes, TGs, links, and ports.
- Control the status of ports and links (activate, deactivate, and recycle).
- Navigate from high-level aggregate views to real resources, using functions such as the More detail, Fast path to failing resource, and Locate resource pull-down menu selections.
- Display views of an APPN network, including views of:
 - All APPN subnetworks being monitored (with each subnetwork as an aggregate object)
 - An individual APPN subnetwork (an aggregate view representing NN domains and the TG circuits between NNs)
 - A particular domain of an NN
 - Local connections of a node (TG, links, ports, and adjacent nodes)
 - A particular connection (a TG or link and the adjacent node).
- Display information about resources such as CP and link names, TG numbers, and the NETID of a subnetwork.
- Identify which NNs, ENs, and TGs have additional capabilities and display what they are. For example, NN capabilities can include border node and directory server. TG capabilities can include support for CP-CP sessions.
- Use existing NGMF functions to navigate and edit views.
- Automate operations using RODM objects.
- Create user-defined objects and views in RODM for customized operation.

Figure 3 on page 7 gives an example of a subarea network topology displayed by SNATAM.

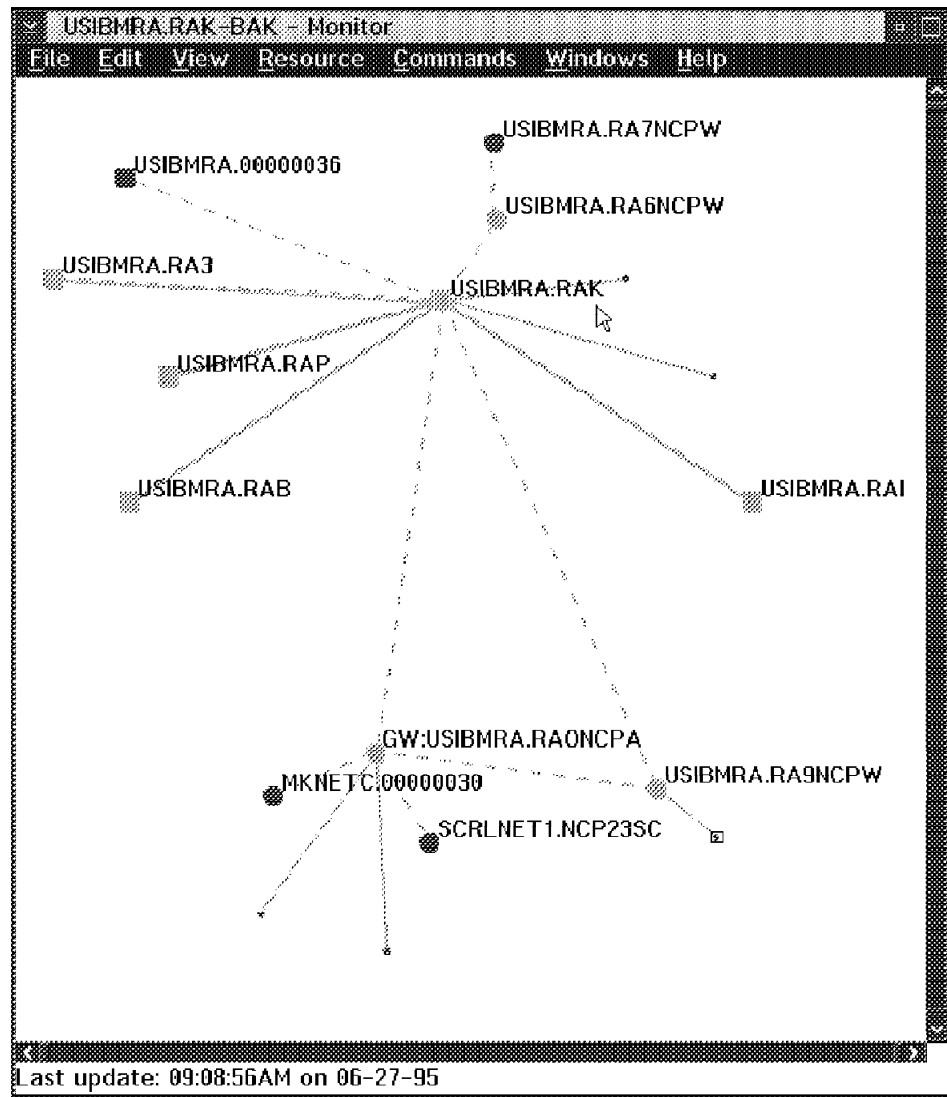


Figure 3. APPN Topology Example

APPN Topology Integrator

The APPN Topology Integrator (referred to as the *integrator*) is an application that runs on any OS/2 WARP® or WARP Connect workstation with Communications Manager/2 (CM/2) V1R1 or later and TCP/IP V3R0. The integrator enables the management of SNMP devices via CMIP. Together with the NetView SNA Topology and Accounting Manager (SNATAM) and the APPN Topology and Accounting Agent (APPNTAA), the integrator is part of a complete solution providing for the management of APPN topology.

SNATAM provides APPN management functions according to a manager-agent relationship. This relationship is defined by the International Organization for Standardization (ISO) in terms of a managing system and a managed system, respectively. The manager applications for APPN topology are NetView applications. Agent applications, including APPNTAA and the integrator, which collect information for transmission to NetView, reside on APPN network nodes and end nodes that use the CM/2 platform. Communication between the manager and agent applications is over APPC sessions using Open Systems Interconnection (OSI) Common Management Information Protocol (CMIP) and the Systems Network Architecture (SNA) Multiple-Domain Support (MDS). To support the CMIP Services, the integrator uses the Management Services (MS) transport.

The integrator is installed, started, and maintained entirely separately from the manager function (see “NetView for OS/390 Management of APPN Networks Overview” on page 2).

How the Topology Manager and Integrator Work Together

The Topology Manager application works with one or more integrators to gather topology from the SNA network. The integrator is needed to provide APPN topology information from SNMP devices. An integrator can be located on an APPN NN or EN.

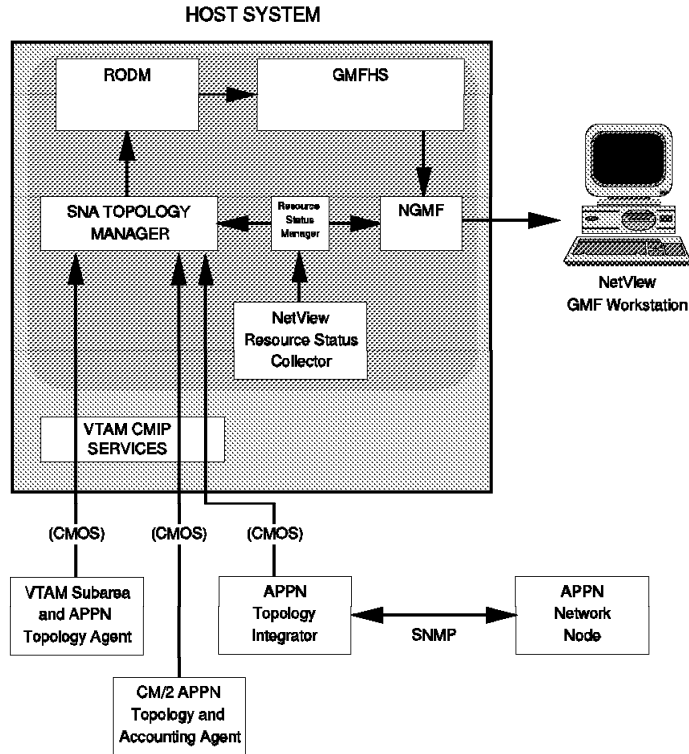


Figure 4. APPN Topology Integrator

When an operator issues a command to start monitoring topology at a node with an SNMP agent, the topology manager sends a request to the integrator. The integrator obtains the requested network or local topology data from the respective SNMP agent and sends the data to the manager. It continues to send status and configuration updates to the manager by polling the SNMP agent for topology changes. An integrator can support approximately 200 concurrent monitor requests.

Note: Each monitor request is handled in a separate OS/2 thread. Although OS/2 can handle a theoretical maximum of 4095 processes or threads, the system default value is 256.

The integrator can also activate and deactivate ports and links at an SNMP device upon receiving requests from the manager if these actions are supported by the SNMP agent at the device.

NetView for OS/390 Management of IP Networks

NetView provides a solution for the monitoring and control of IP resources under GMF. The IP resources can be displayed on the same screen as subarea and APPN SNA resources, and controlled in the same way. This product is called *MultiSystem Manager* (MSM).

MultiSystem Manager uses a manager-agent relationship to manage LAN and IP workgroups. This relationship consists of a managing system, from now on referred to as the topology manager, and managed systems, from now on referred to as topology agents.

MultiSystem Manager Release 2 enables management of the following IP resources:

- Networks
- Locations
- Subnets
- Segments
- Routers
- Hosts
- Bridges
- Hubs
- Interfaces

The MSM topology agents are supported for the following software platforms:

- NetView/6000
- NetView for AIX²
- LAN Network Manager Entry
- LAN Network Manager
- Novell NetWare

The role of the topology agents is to monitor all of the resources controlled by the workstation in which the agent resides and to dynamically communicate any changes in resource status to the topology manager. The NetView/6000 agent only retrieves topology information from the NetView/6000 database when requested by MSM. Resource status changes are sent to MSM by NetView/6000.

Managing System

MSM consists of a base component and features for the different environments. Figure 5 on page 11 provides more detail showing the components of the MSM base code.

² After NetView for AIX V4R0, the product is named Tivoli® NetView.

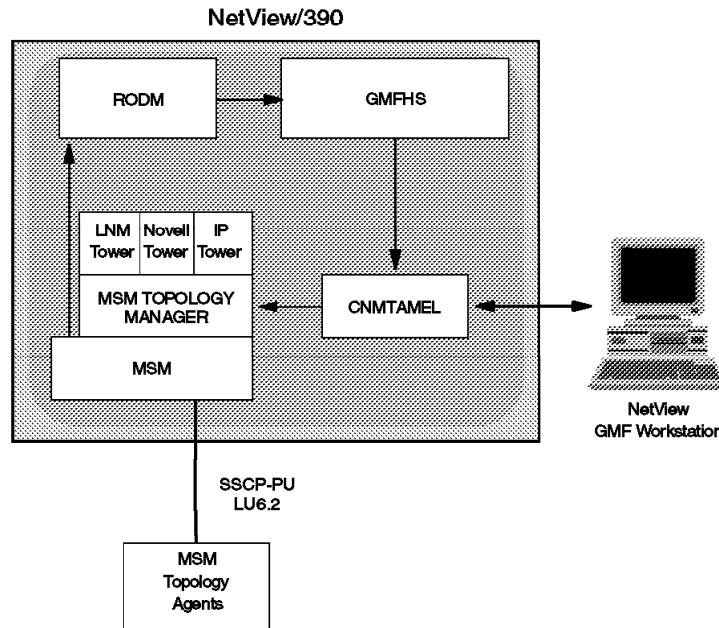


Figure 5. Detail of MultiSystem Manager and NetView Component Parts

MSM consists of the following components:

- NetView REXX command lists with a REXX alternative library

Note: With SAA REXX/370 installed, the command lists run compiled. Without the SAA REXX/370 installed, the command lists will run with the alternative library.

- NetView command processors
- NetView panels
- Load files for the MSM data model.

The command lists and command processors can run in one or several NetView autotasks (for load balancing).

The MSM topology manager performs the following tasks:

- Dynamically discovers the topology and status of the network.
- Stores this information in the NetView Resource Object Data Manager (RODM).
- Automatically processes topology and status updates from the topology agents.

Centralized and integrated LAN and IP management can be achieved, because status information about your networks and all LAN and IP resources is stored in RODM. The information in RODM relates to the information received from your topology agents. In addition MSM allows graphical management of LAN and IP resources by displaying the information on the NetView Graphic Monitor Facility (NGMF) workstation. Figure 5 shows you how MSM works in the NetView environment.

MultiSystem Manager Presentation Services

Using NGMF you can navigate through the views of your networks. Figure 6 on page 15 gives you an example of the IP views created by MultiSystem Manager.

As a result of the object-oriented approach used in the data repository (RODM), the IP objects/views created by MSM can easily be integrated with other types of objects/views in RODM (for example LAN adapter, NetWare requester or SNA objects).

Manager-to-Agent Communication

The MSM topology manager communicates with the topology agents by means of NetView RUNCMD commands across SNA sessions. Topology agents communicate with MSM through RUNCMD responses, alerts and resolutions.

RUNCMD

RUNCMD commands are SNA Network Management Vector Transports (NMVTs) that you send from NetView to a service point application. The workstation topology agent translates each NetView RUNCMD command into the specific workstation command. Command response NMVTs contain information about the workstation or about the result of a workstation command. After the workstation processes a command from NetView, the topology agent builds a command response, imbeds it in an SNA/MS NMVT and sends it to NetView.

Alerts and Resolutions

Alerts in this context are SNA/MS NMVTs sent from service point applications to NetView. The alerts from the service points will appear in the hardware monitor component of NetView.

The topology agent sends an alert when it wants to notify the topology manager of a topology or status change. When all of the problems associated with a resource are corrected, the topology agent sends a resolution notification to the topology manager indicating that the resource has now returned to a satisfactory status.

Monitoring Resources

Once the initial status for the managed resources is stored in RODM, the MSM agents can notify NetView of topology or status changes by sending alerts to NetView.

The NetView Automation Table routes the alerts to the topology manager and the GMFHS event manager. The topology manager queries RODM for the topology resources. If the resources that caused the topology change alert are not found in RODM, the topology manager will create them.

The MSM IP Tower

MSM utilizes functions of the following products to enable centralized management of IP network environments:

- AIX® NetView Service Point V1.2 or V1.2.1 (referred to hereafter as the service point)
- AIX SystemView® NetView/6000 V2.1 (referred to hereafter as NetView/6000) or NetView for AIX V3.³

MSM uses a manager-agent relationship to manage IP networks. This relationship consists of a managing system referred to as the topology manager and a managed system, referred to as the topology agent. MSM provides the topology manager that runs on the NetView for MVS® management platform. Each NetView for AIX V3 includes a topology agent that reports on all of the resources controlled by that IP manager.

The data collected by MultiSystem Manager from the managed NetView for AIX V3 systems is stored in a single high-speed data cache called the Resource Object Data Manager (RODM) and is presented on the NGMF workstation in graphical form. You still need to run NetView for AIX V3 on one or multiple workstations, all of them managing their own resources.

NetView/6000 is a comprehensive management tool for distributed heterogeneous, multivendor devices on TCP/IP networks. It provides an open network management platform that enables the integration of Simple Network Management Protocol (SNMP) and Common Management Information Protocol (CMIP) applications.

Most common is SNMP, which is a TCP/IP recommended standard that enables managers to ask agents to retrieve and change information about network objects. Those objects make up a collection called the Management Information Base (MIB). The MIB is not an actual database residing somewhere on the network: the individual pieces of information, called MIB objects, reside on the agent system, where they can be accessed (GET-command) and changed (SET-command) at the manager's request. This is how NetView/6000 manages network objects.

NetView/6000 is an AIX application; some of the functions it provides are as follows:

- Dynamic discovery and management of IP resources:
 - Networks
 - Segments
 - Routers
 - Hubs
 - Bridges
 - Hosts
 - Adapters
- Configuration, fault and performance management
- Threshold monitoring and automation facility
- Host communications with NetView for MVS using Service Point
- Alert filtering

³ After NetView for AIX V4R0, the product is named Tivoli® NetView.

- Interface with Ingres database
- Graphical user interface using OSF/Motif and X-Windows System standards
- SNMP and NetView/6000 command line commands.

NetView for AIX V3 adds the following functions:

- Enhanced database support to manage trap, topology and collected SNMP data using, additionally:
 - DB2/6000
 - Informix
 - Oracle
 - Sybase
- Enhanced event handling including trap-forwarding, multiple dynamic workspaces and operator-less event automation
- Integrated System Resource Monitoring Tool
- Distributed discovery and management using Systems Monitor V2
- Enhanced APIs
- Backup Manager function

Note: For further information on NetView for AIX V3, refer to the NetView for AIX V3 manuals.

Example IP Views

This section gives some examples of how IP resources are displayed by NGMF.

The View Hierarchy

Included in the following is a simple scenario in which the NGMF operator navigates down by double-clicking on resources to display IP Internet views. Details on the views are explained in the next chapter.

An overview of the view hierarchy is provided in Figure 6 on page 15 to illustrate how to click your way down to the IP Internet view.

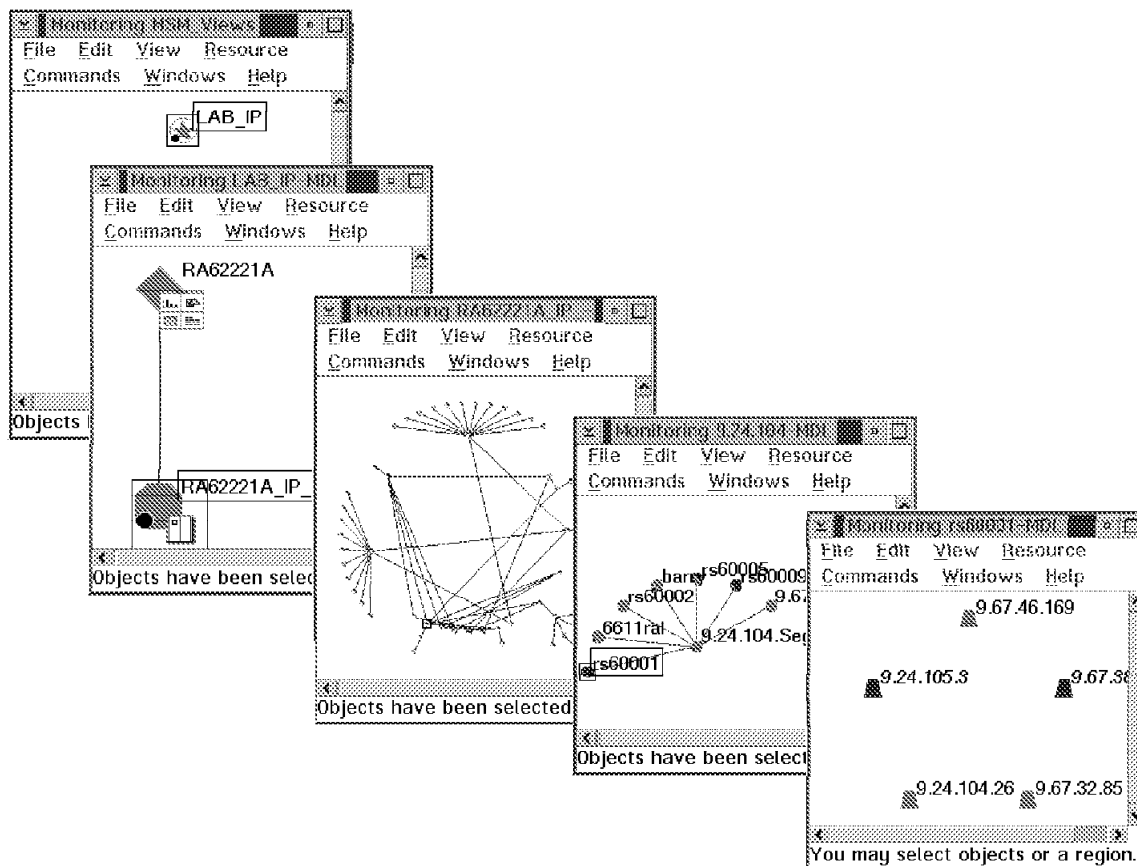


Figure 6. The MSM/IP Views at a Glance

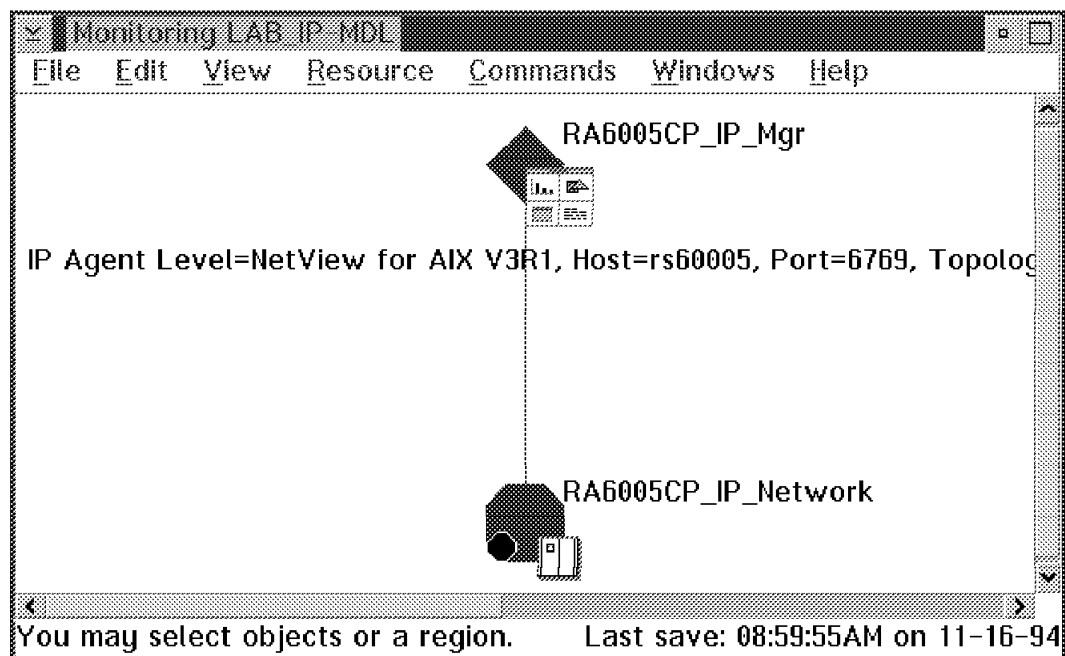


Figure 7. Domain Manager and IP Network Aggregation Object

In this example the managed IP network has a service point called RA6005CP. This is the CP name of our service point machine and has to be used in the RUNCMD, as shown later, if LU 6.2 is used for transport. This view includes also the IP network aggregate object (RA6005CP_IP_Network) and some helpful information about the domain manager including its IP agent level, host name and topology level (so-called "other data"), which is optional.

By double clicking on the network aggregate 9.24.104, which is our local IP network, we get a view containing the network with all attached routers. This view hierarchy corresponds to the view hierarchy NetView for AIX V3 uses.

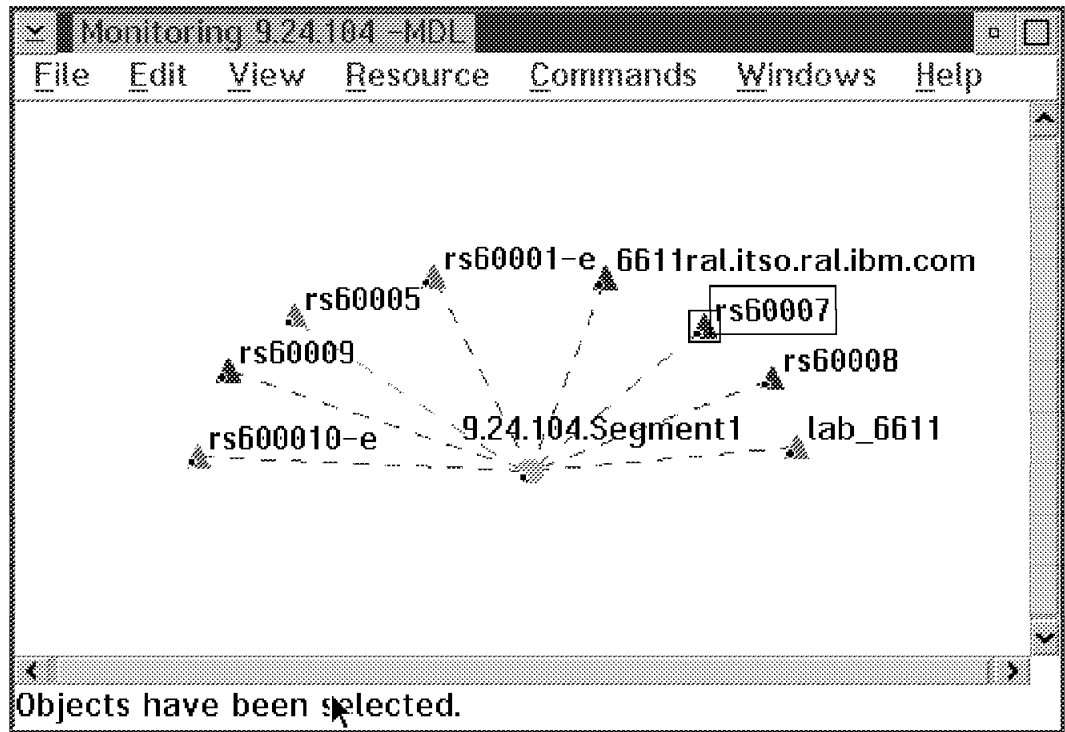


Figure 8. Display of Segment

NetView for AIX V3-to-MultiSystem Manager Communication

MultiSystem Manager communicates with NetView for AIX V3 using the following products on an AIX® workstation:

- AIX SNA Server V2
- AIX NetView Service Point V1.2.1.

or

- AIX SNA Services V1.2
- AIX NetView Service Point V1.2.

SNA Server/Services only provides a connection; the service point is a transport vehicle, moving data. The following applications that use the service point are provided in NetView for AIX V3:

- Trap-to-Alert Daemon (TRALERTD)
- Service-Point-Application Daemon (SPAPPLD).

The flow of information between NetView for AIX V3 and NetView for MVS (now referred to as Tivoli NetView for OS/390) is illustrated in Figure 9.

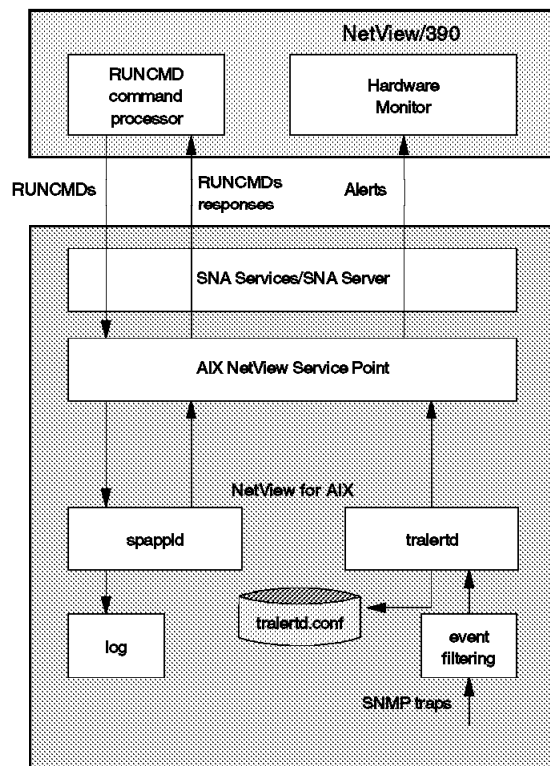


Figure 9. The Flow of Information between NetView for AIX V3 and NetView for MVS

Note: NetView for AIX V3 and Service Point have to run on the same physical machine to work with MSM.

The TRALERTD receives SNMP traps and converts them into NetView for MVS Alerts (NMVTs). There is a special filter function, that allows you to customize which traps are forwarded to NetView for MVS. The TRALERTD provides default trap to alert conversion rules and default filter. The conversion rules are stored in the tralertd.conf file.

The service point application daemon SPAPPLD receives commands that are sent from NetView for MVS and sends RUNCMD responses. It also logs all activities in the NV390.LOG logfile.

NetView for MVS to AIX Service Point Communication

NetView for MVS communicates with service point using one of the following SNA connections:

- An SSCP-PU session
- MDS Transport using LU 6.2 session.

Communication over an SSCP-PU Session: This is not supported for NetView/6000-MSM communication. We tried it and found that it worked, but you should consider using LU 6.2 for support and performance reasons. If your AIX service point and your NetView focal point VTAM are in different SNA networks, you will have to use an LU 6.2 session since this provides the required cross domain support.

Communication over an MDS Transport LU 6.2 Session: An LU 6.2 connection is required when the service point node is not in the same SNA network or VTAM domain as NetView MSM. It is also required for APPN networks, where the role of the PU is taken over by the APPN control point.

When using the SNA server, the control point takes the place of the LU and is used to address the service point with the RUNCMD command. This facility has two advantages:

- Definition is much easier, because you do not have to define any LUs.
- It is possible to change the focal point NetView used by service point, which means you can share one service point machine between two NetView for MVS (not at the same time). All you have to do is to send a NetView FOCALPT CHANGE command to the service point and the host partner LU is changed.

Note: If an LU 6.2 session is used with SNA services, the connection is dependent on the status of the partner LU, which in this case is NetView for MVS. The connection is reestablished by the first RUNCMD sent by NetView for MVS after the LU-LU session has become inactive. It is necessary to define an LU 6.2 logmode for this.

If you are using SNA server, there should be no problem if the host partner LU becomes inactive. SNA server tries to reestablish the session continuously and so the session becomes active shortly after the VTAM major node is activated. SNA server only has to be restarted when the connection has been down too long SNA server stops trying to reconnect after a maximum of 500 attempts.

The retry frequency and number of retries is controlled by fields in the SNA DLC profile. The default is 20 retries at one-minute intervals.

Note: When the VTAM switched major node is inactivated and activated, sometimes it might also be necessary to restart the SNA subsystem in addition to service point.

Performance Management

Except for “Reporting Service Processor and NNP CPU and Memory Use,” this section assumes you are familiar with NetView Performance Monitor (NPM). It describes NPM in a SNA subarea environment.

Reporting Service Processor and NNP CPU and Memory Use

The service processor and NNP CPU and memory use statistics can be displayed at the service processor. To do this, use the **Service Processor** menu, then:

1. Click on **Performance Management**.
2. Run the **Perform SP/NNP statistics** function.

The **SP/NNP(A/B) Performance Analysis** window opens.

The statistics are dynamically updated.

The Need for Performance Monitoring

Performance monitoring consists of three basic tasks:

- Collecting data as the events being monitored are happening.
- Sending the data collected to a central point.
- Analyzing the data to give the required picture of present performance against either:
 - A past situation
 - An ideal attainable situation.

The purpose of analysis depends on the requirement for monitoring. It could be:

- To offer the best throughput for the cost of the network
- Real-time traffic management
- Accounting and charging purposes.

Whatever the purpose, performance monitoring is a combination of host and 3746 Network Node activities.

Present Performance Monitoring on SNA Networks

Referring to Figure 10 on page 20, the present mix of activities is:

1. Individual DLCs (SDLC, CDLC, Token-Ring 802.2, frame relay, X.25, and ISDN) collect data according to keywords chosen at NCP generation time. The DLCs have algorithms onboard to watch data flowing through them and to collect the required information. Only that information chosen at generation time can be collected.
2. A task running in the same NCP to which the DLCs are connected, NPA (Network Performance Application) gathers data from the DLCs. This is running in an LU0-PU2.0 session.
3. The NPA in NCP is connected to the NPM running in the host via an LU-LU session. NPM receives the data from all the NPAs and displays or prints the required analysis.

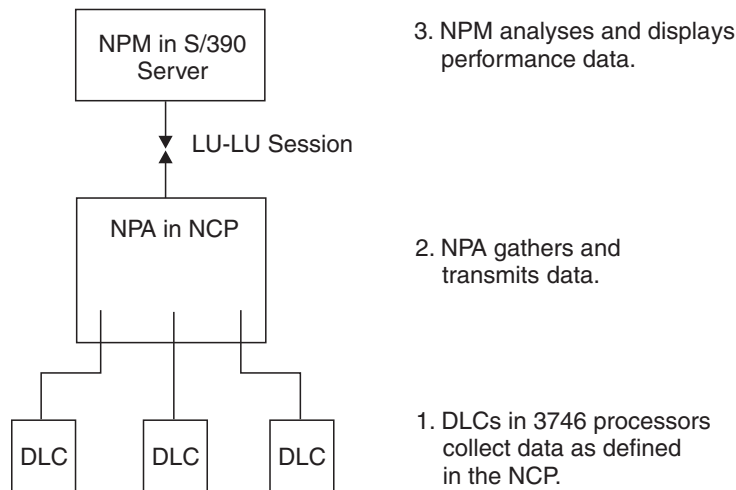


Figure 10. SNA (NCP) Performance Monitoring Activities (3745/3746-900)

NetView Performance Monitor Support Details

The NetView Performance Monitor (NPM) Version 2 Release 1 or Release 2, used in conjunction with NCP Version 7 Release 3 or Release 4, is required for performance monitoring of:

- X.25 lines connected to the 3746-900, supported by X.25 NPSI Version 3 Release 8 or by the X.25 ODLC function of NCP V7R4 requiring FC 5030 into the 3746-900. NPM must be installed with APAR number OW10583.
- TIC3 and 3746-900 processor (CLP, TRP, TRP2, ESCP, ESCP2, and CBSP or CBSP) utilization. NPM must be installed with APAR numbers OW08565 and OW10584.

Support for LAN counter data reporting for non-ERP traffic⁴ over a TIC3 requires NCP V7 R4 and one of the following:

- NPM V1 R6 with APAR OW17878
- NPM V2 R1 with APAR OW17876.

Support for the HPR LAN counter data reporting over a TIC3 requires NCP V7 R4 and NPM V2 R2 with APAR OW17876.

APPN Resource Management Using NetView RUNCMD

The Network Communication Control Facility (NCCF) RUNCMD allows you to manage your APPN network by sending commands to the service processor (and network node processor via the service processor) for the 3746 Network Node APPN resources.

After configuring the **Focal Point** via CCM for the service processor, it can respond to commands sent over SNA or APPN links from the VTAM specified as the Focal Point, see “Focal Points” on page 25. CM/2 in the service processor is the Service Point for the NetView Focal Point.

⁴ The 3746-900, operating as an APPN composite network node (CNN) with NCP V7 R4, supports HPR/ANR traffic, which does not require error recovery procedures (ERPs) with the adjacent HPR node.

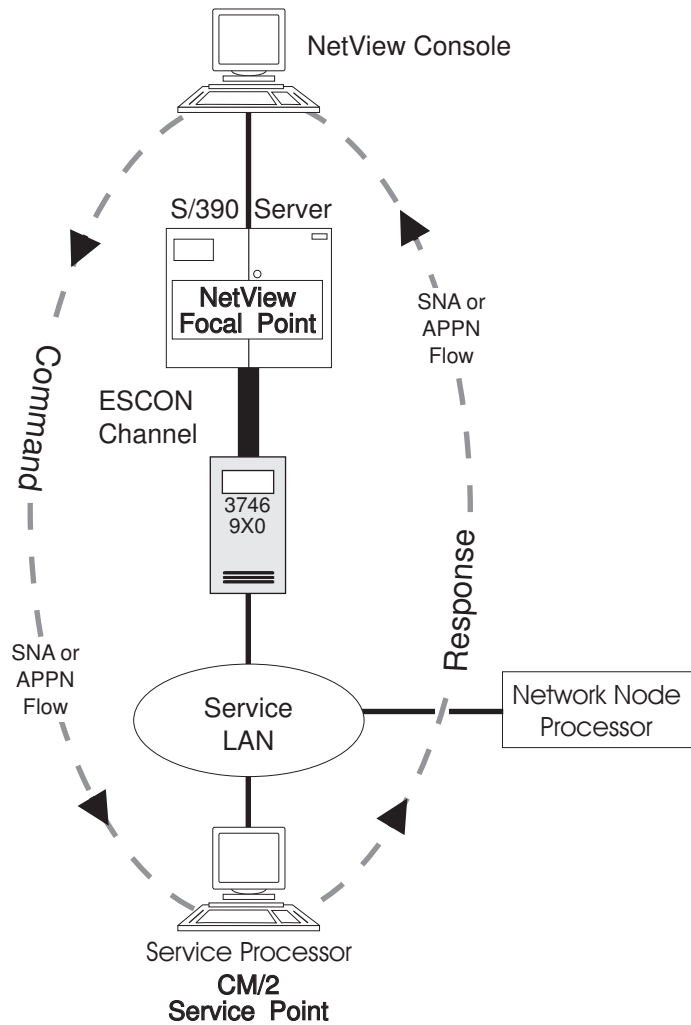


Figure 11. RUNCMD Path

Commands follow the path shown in Figure 11 between the service processor and the NetView console:

NetView console →
 VTAM in the S/390 server →
 ESCON channel to 3746 →
 Service LAN to CM/2 in service processor (→)
 (NNP, if necessary)

For information about all the available commands and how to configure the service processor, refer to the *3745 Models A and 3746 Models 900 and 950: NetView Console APPN Command Reference Guide*, GA33-0479.

NetView for AIX Management of IP Networks

The following describes NetView for AIX management of IP networks.

Managing Your IP Resources with SNMP

Your IP resources are managed with the Simple Network Management Protocol (SNMP), which is used to:

- Monitor and control network elements
- Communicate fault management information between the network management stations and agents in the network elements (hosts, gateways, and terminal servers).

Unsolicited messages (traps) inform network management stations of asynchronous events such as:

- Cold start
- Warm start
- Link down
- Link up
- Authentication failure
- Neighbor loss
- Enterprise specific.

Managers and Agents

SNMP operates with *agents* that monitor network resources and report events to their *manager* on a network management station. The relationship between a manager and its collection of agents is called a *community*, and is defined by three properties:

- Name of the community
- IP address of the manager within the community
- Access mode of the manager (also called *privilege*). The 3746 Network Node implements Read access which allows the manager to read information from a resource, but not to make changes to that information.

Traps

These are event notifications sent by agents to their managers. They consist of two parts:

- Name of the trap community
- IP address of the SNMP manager that is to receive the traps (alerts).

NetView for AIX Examples

The following figures show example NetView for AIX (NetView/6000) displays of IP networks. Figure 12 shows an example IP network; Figure 13 show an example of an Ethernet segment.

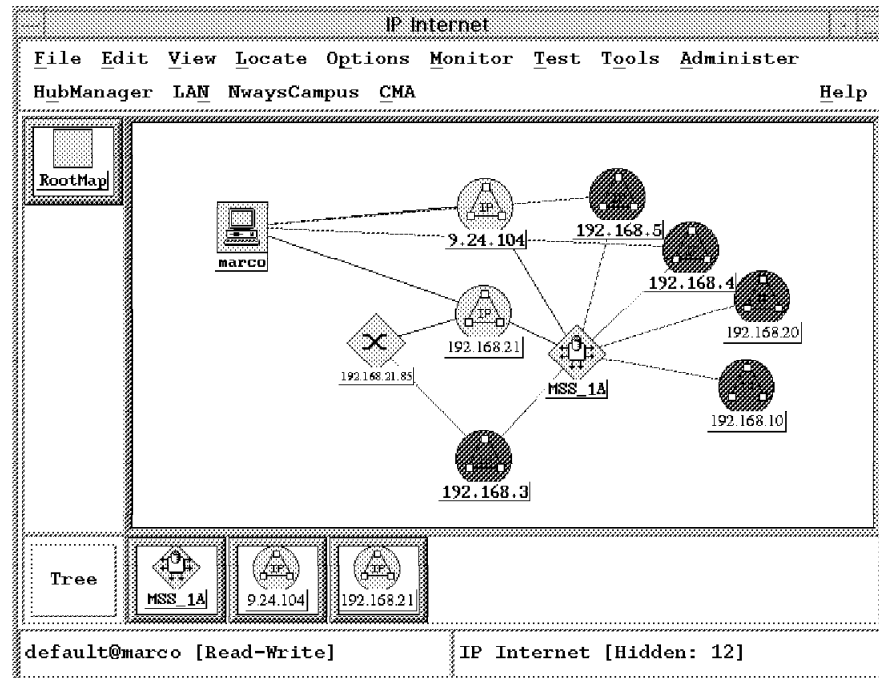


Figure 12. Example IP Network

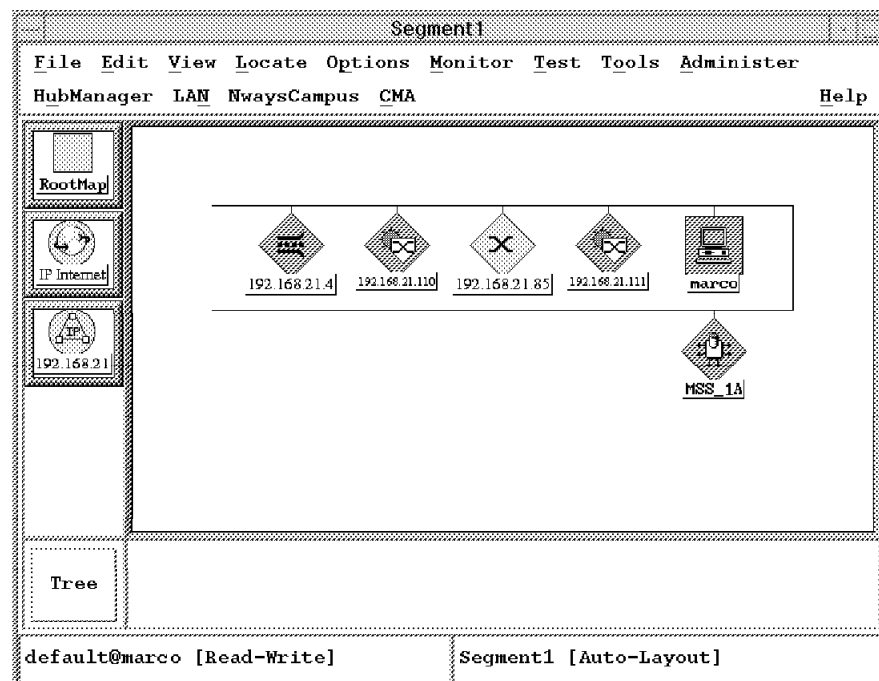


Figure 13. Example IP Segment

SNMP Management of APPN Networks

IBM Nways Campus Manager - LAN for AIX now includes the functions of IBM Router and Bridge Manager/6000 V1.2 (RABM). RABM is used to monitor the health and performance of bridges and routers in the campus network. Among support for other IBM and OEM devices through standard and enterprise-specific MIBs, it also supports APPN and DLSw MIBs. In addition, it includes Alert Manager, which enables SNA alerts that are enveloped in SNMP traps to be displayed correctly on the NetView for AIX Event Desk. Although this function was provided specifically for IBM 3746 and AS/400® devices, it can be used by any SNMP agent.

With the APPN Topology feature, it is possible to view APPN networks end-to-end. APPN resources are discovered automatically and can be viewed with their status as color-coded icons. APPN protocol performance and error events (data and graphs) are also provided.

A single NN RABM client provides details of the complete APPN backbone. For local topology of NNs and ENs, the RABM client must be installed in each NN.

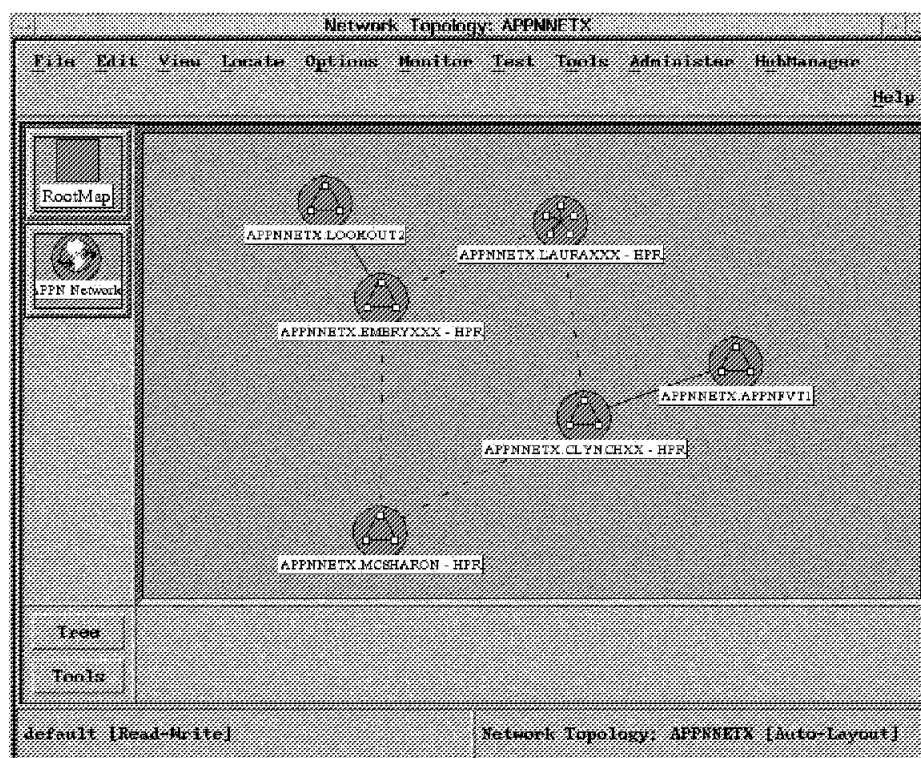


Figure 14. Example RABM Display

Figure 14 shows an example RABM display. It shows a network of six APPN nodes; the nodes with the suffix *-HPR* are HPR-capable. HPR links are shown as dotted lines, and APPN links are shown with solid lines.

NetView Alerts

If you are not going to use the NetView program, please go to “To Not Generate MOSS-E Alerts” on page 34.

External Box Errors

A network error detected by the network node processor is an external box error. It causes the network node processor to generate a network alert, which is sent to the NetView program via the session between the network node processor and the NetView program.

For external box errors, there is no MOSS-E intervention.

Internal Box Errors

An internal hardware or microcode problem in the 3746 Network Node (3746-900, 3746-950, network node processor, or service processor) is an internal box error. The 3746-900 or 3746-950 sends its hardware or microcode error data to the service processor (MOSS-E) and network node processor (control point) via the TIC3 on the CBSP. For MOSS-E microcode errors, the network node processor is not notified. The following happens after an internal box error has been detected:

- The network node processor generates a network alert for the 3746 Network Node resources that are affected by the internal box error. This alert is sent to the NetView program via the session between the network node processor and the NetView program.
- The MOSS-E:
 - Records a system reference code (SRC) on the service processor hard disk
 - Displays an alarm on the service processor
 - Generates a hardware alert that is sent to the NetView program via a session between the service processor and NetView
 - Automatically calls the IBM Remote Support Facility, if this function is enabled (see Chapter 6)

Note: To match the network alerts reported by the network node processor with the hardware alerts reported by the MOSS-E for the same problem, make sure that both the network node processor and the MOSS-E alerts are reported to the *same* NetView program (see “Path for Reporting Network Node Processor Alerts” on page 27 and “Paths for Reporting MOSS-E Alerts” on page 27).

Focal Points

Alerts are sent to a node’s *focal point* (FP) NetView (defined in CCM). When this FP is unavailable, alerts may then be sent to a *backup focal point* NetView.

If the connection to the primary focal point cannot be established, or an existing connection becomes inactive, the 3746 will attempt the following if:

Backup focal point is defined

The 3746 attempts to connect to the backup focal point.

No backup focal point defined

The 3746 attempts to reconnect to the primary focal point.

If the connection attempt to a focal point is not successful, then a timer is set and a retry is made when the timer expires. For each subsequent failure, the retry time is doubled up to an interval of one day. After that a retry is attempted once a day.

Paths for Reporting Alerts to NetView

Figure 15 shows the paths for reporting network node processor and MOSS-E alerts to NetView over an APPN network.

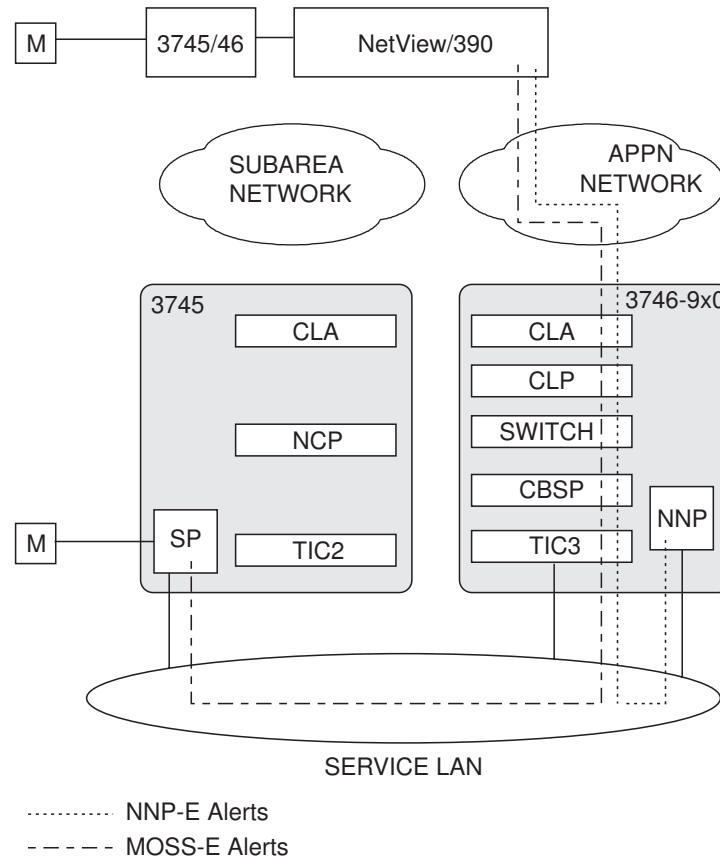


Figure 15. NetView Alert Paths over APPN

..... MOSS-E Alerts - Main Path

----- MOSS-E Alerts - Alternate Path

The network node processor reports the network alerts to NetView via the APPN/HPR network. The network alerts flow over from the NNP into the 3746 via the service LAN TIC3, and then over an APPN connection out of the 3746 to NetView (see Figure 15 on page 26).

Two paths can be used by the service processor (MOSS-E) for sending the hardware alerts to NetView. These are:

- Mainstream path
- Alternate path.

Mainstream Path: This is the normal path to the NetView program, generally flowing through the APPN/HPR network or, depending on the service LAN configuration, the SNA/subarea network. Either the APPN/HPR path or one of the SNA/subarea paths to NetView must be defined at installation time.

APPN/HPR Path: The MOSS-E alerts flow from the service processor to NetView over the same physical path (although using a different session) as the alerts reported by the network node processor. See Figure 15 on page 26.

The alerts flow from the service processor into the 3746 through the TIC3 connected to the service LAN, and from there via an APPN network to NetView.

Note: This path uses the DLUR support of the network node processor and requires a VTAM with the dependent LU server (DLUS) function at the other end of the DLUR pipe.

SNA/Subarea Path: The service processor can use an SNA/subarea path to NetView. This is via an NCP-controlled token-ring port operating as the gateway to the NetView program. One of the following 16-Mbps token-ring ports⁵ connected to the service processor LAN is used to send the MOSS-E-generated hardware alerts to the NetView program (see Figure 16 on page 27):

- The TIC3 of the 3746-900 that provides the communication between the CBSP and the service processor
- A TIC3 port of another token-ring adapter in the 3746-900
- A TIC2 port of a token-ring adapter in a 3745.

Note: If you select an SNA/subarea path, you can use any 3745 or 3746-900 that is connected to the service LAN.

Alternate Path: If the mainstream path is not available, the MOSS-E can be pre-configured to contact the NetView program host via the SDLC port on the service processor (see Figure 16 on page 27). This alternate path must be defined in the service processor. For more information, refer to the “MOSS-E Service Processor Customization Function” appendix in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

Alerts are sent via the service processor SDLC port to the SP modem, through a public switched network to another modem that is connected to a 374X that provides a subarea path to NetView.

You must provide a 3745 or 3746 switched port at the host site. This port must be equipped with a switched line modem to receive the dial connection. The modem must be compatible with the service processor modem. For more information about the type of modem needed, refer to the “Controller and Service Processor Integration” chapter in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

Host procedures must include the activation of the switched port to answer the call.

Parameter Definitions for Reporting Alerts to NetView

This section presents the parameters that you must define in the service processor for the NetView path. These parameters allow alerts originating from problems detected in the 3746 Network Node and the network to be reported. Use the “Parameter Definitions for Reporting Alerts to NetView” on page 93 worksheets on page 93 to record the values you assign to the parameters described in this section.

⁵ The token-ring port on the MOSS does not provide this path to the NetView program.

Network Node Processor Alerts

The network node processor reports network alerts to NetView according to the network management focal point defined via the *CCM User's Guide*, SH11-3081 (refer to the Network Node and DLUR Parameter worksheet in the *3745/3746 Planning Series: CCM Planning Worksheets*):

Network identifier

Identifies the APPN/HPR network to which the focal point node (running NetView) is connected.

IBM-registered networks identifiers should have an 8-byte name with the structure *cceeeenn*, where:

- *cc* is the country code (according to ISO 3166)
- *eeee* is the enterprise code (unique within a country)
- *nn* is the network suffix code (unique within one enterprise).

Control point name

Identifies the focal point node (running the NetView program) that is to receive the alerts.

Note: Up to eight backup focal points (running other NetView programs) can be defined via *CCM User's Guide*, SH11-3081. Use the Network Node Processor Alert worksheet in “MOSS-E Worksheets for Controller Installation” appendix in the *3745/3746 Planning Series: Overview, Installation, and Integration* to record the values you assign to the parameters described in this section.

MOSS-E Alerts: Mainstream Path Definitions for APPN/HPR Path

Use the MOSS-E Alert: Mainstream Path worksheet in the “MOSS-E Worksheets for Controller Installation” appendix in the *3745/3746 Planning Series: Overview, Installation, and Integration* to record the values you assign to the parameters described in this section. This APPN/HPR path (see “APPN/HPR Path” on page 27) uses the TIC3 of the CBSP. If you want to use it as the mainstream path for the MOSS-E alerts, the following MOSS-E and VTAM definitions are needed:

MOSS-E Parameters

LAN destination address

This is the MAC address (locally administered address) of the TIC3 on the CBSP (token-ring adapter used as the gateway to the NetView program). See Figure 15 on page 26.

This address must be defined with the same value used for the **token-ring local address (MAC address)** parameter in the “Controller and Service Processor Integration” chapter in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

This address has 12 digits and must be unique among all other network addresses (LAAs) on the service LAN. Specify this address in the IBM Token-Ring Network format (your network administrator should be able to help you with this format). This address will be used by your service representative when customizing your service processor. For more information, refer to the “MOSS-E Service Processor Customization Function” appendix in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

CCM User's Guide, SH11-3081 Parameters: The APPN/HPR path uses the DLUR support of the 3746 Network Node, which requires a VTAM with the DLUS function to be defined via the *CCM User's Guide, SH11-3081*. *CCM User's Guide, SH11-3081* allows you to define a primary DLUS and backup DLUSs.

Primary dependent LU server (DLUS)

Identifies the VTAM running the DLUS that you want to use.

Backup DLUS

Specifies whether there is a backup dependent LU server. If you select Yes, give the network identifier and the server name of the backup DLUSs.

Waiting Time Before Retry

Specifies the length of time, in tenths of a second, that the DLUR must wait before attempting to re-establish a broken path to the DLUS. The maximum value is 120 seconds.

The default value is -1, for no retry. Other values are:

- 0, for an immediate retry
- 1 second, for a short retry
- 3 seconds, for a long retry

VTAM Keywords: To report alerts to NetView, you must define the service processor as a switched major node (PU type 2.1) in VTAM with the following parameters:

CPNAME defined with the same value used for the **MOSS-E Local Node Name** parameter in the “Controller and Service Processor Integration” chapter in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

NETID defined with the same value used for the **Network ID** parameter in the “Controller and Service Processor Integration” chapter in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

```

*****
*      MAJNODE FOR CONNECTION :  MOSS-E  <==>  NETVIEW      *
*****
NTVMOSSE VBUILD TYPE=SWNET,MAXGRP=1,MAXNO=1
*-----*
MOSSE    PU      ADDR=04,PUTYPE=2,                          X
          NETID=Network ID,                                  X
          CPNAME=Local node name,                             X
          DISCNT=NO

```

Figure 17. Example of Switched Major Node Definition

Note: This PU definition can also be coded in the switched major node using the IDBLK and IDNUM parameters instead of NETID and CPNAME. Here, the service processor local node characteristics must be defined using the Communications Manager. Specifically, the two fields of the local node ID parameter are used:

- **IDBLK** has the value of first field (three digits)
- **IDNUM** has the value of second field (five digits).

MOSS-E Alerts: Mainstream Path Definitions for SNA/Subarea Path

If you use an NCP path for the MOSS-E alerts (see “SNA/Subarea Path” on page 28), the following MOSS-E, NCP, and VTAM definitions are needed:

MOSS-E Parameters

LAN destination address

This is the MAC address (locally administered address) of the token-ring port used as the gateway to the NetView program (See Figure 15 on page 26).

This address must be defined with the same value used for the **token-ring local address (MAC address)** parameter in the “Controller and Service Processor Integration” chapter in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

This address has 12 digits and must be unique among all other network addresses (LAAs) on the service LAN. Specify this address in the IBM Token-Ring Network format (your network administrator should be able to help you with this format).

NCP Keywords: The following NCP definitions must be planned if you use an SNA/subarea for the mainstream path:

1. A **Physical line** and a **physical unit (PU)**. You must define **A** with the same value used for the MOSS-E **token-ring local address (MAC address)** parameter in the “Controller and Service Processor Integration” chapter in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

```
*-----* FFA30320
* TIC          PORT 2080 ATT TO SERVICE PROCESSOR - PHYSICAL      * FFA30330
*-----* FFA30340
GP50C2080 GROUP ECLTYPE=(PHYSICAL, ANY),                          *
          ADAPTER=TIC3                                           *
K50C2080 LINE ADDRESS=(2080,FULL),PORTADD=0,LOCADD= A           *
          MAXTSL=16732,LSPRI=PU,PUTYPE=1,ANS=CONTINUE,          *
          ADAPTER=TIC3,TRSPEED=16,TRANSFR=254                   *
S50C2080 PU ADDR=01,                                           *
          INNPORT=NO
.
.
```

Figure 18. Example of NCP Generation for a Link to the Service LAN, Part 1.
The link passes through a 3746-900 (TIC3 of the CBSP).

2. A Logical group with at least one Line/PU.

These definitions apply to a TIC type 3 or 2.

```

***** FFA33180
*   TIC      GROUP L78G2080: LAN LOGICAL DEFINITIONS      * FFA33200
***** FFA33230
L50G2080 GROUP DIAL=YES,LNCTL=SDLC,TYPE=NCP,ECLTYPE=(LOGICAL,PER), *
              CALL=INOUT,PHYSRSC=S50C2080,                *
              LINEAUT=YES,                                *
              MAXPU=1,                                     *
              NPACOLL=NO,                                  *
              PUTYPE=2,                                    *
              RETRIES=(6,0,0,6)
R50A0001 LINE
Z50A0001 PU
.
.

```

Figure 19. Example of NCP Generation for a Link to the Service LAN, Part 2.
The link passes through a 3746-900 (TIC3 of the CBSP).

VTAM Keywords: To report alerts to NetView, you must define the service processor as a switched major node (PU type 2.1) in VTAM with the following parameters:

CPNAME defined with the same value used for the MOSS-E **Local Node Name** parameter in the “Controller and Service Processor Integration” chapter in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

NETID defined with the same value used for the MOSS-E **Network ID** parameter in the “Controller and Service Processor Integration” chapter in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

```

*****
*   MAJNODE FOR CONNECTION : MOSS-E <==> NETVIEW      *
*****
NTVMOSSE VBUILD TYPE=SWNET,MAXGRP=1,MAXNO=1
*-----*
MOSSE   PU   ADDR=04,PUTYPE=2,                          X
              NETID=Network ID,                          X
              CPNAME=Local node name,                     X
              DISCNT=NO

```

Figure 20. Example of Switched Major Node Definition

Note: This PU definition can also be coded in the switched major node using the IDBLK and IDNUM parameters instead of NETID and CPNAME. In this case, the service processor local node characteristics must be defined using the MOSS-E Communications Manager. Specifically, the two fields of the local node ID parameter are used:

- **IDBLK** has the value of first field (three digits)
- **IDNUM** has the value of second field (five digits).

MOSS-E Alerts: Alternate Path Definition

MOSS-E Parameters: If you plan to use an alternate path along with the mainstream path, you must supply the following:

Modem type

Select the type of the modem used and to what it is connected (MPA card or COM1 port). Refer to the “MOSS-E Service Processor Customization Function” appendix in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

Telephone number for alert reporting on the switched SDLC link

This is the telephone number used by the service processor and its modem for automatic dialing to the SNA port providing access to the NetView program via the public switched network. For more information, see:

- “Alternate Path” on page 28
- Figure 15 on page 26
- the “MOSS-E Service Processor Customization Function” appendix in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

Note: The Link type is SDLC, the default value, as the alternate path to the NetView program uses an SDLC link via the public switched network.

NCP Keywords: In the 37xx controller providing channel access to the host running NetView, the following NCP definition must be taken into consideration for your alternate path:

Note: Make sure that NRZI is the same, either YES or NO, in the MOSS-E Communications Manager and in the NCP.

```
*****
G23SIDES GROUP DIAL=YES,LNCTL=SDLC,TYPE=NCP,REPLYTO=3,XID=YES
K23C0004 LINE ADDRESS=(0004,FULL),DUPLEX=FULL,RING=YES,NEWSYNC=NO,      *
          V25BIS=(YES,DLSDLC),AUTO=YES,PAUSE=0.1,TRANSFR=71,          *
          NRZI=YES,CLOCKNG=EXT,RETRIES=(3,3,3),CALL=IN,ENBLT0=15
P23C0004 PU PUTYPE=2,ISTATUS=ACTIVE
*****
```

Figure 21. Example of a NCP Generation for an SDLC Link to the NetView program

Note: Remember to change your network operator procedures or CLIST to enable the activation of the SNA port called by the service processor. Use the Service Processor Parameter worksheet (see Appendix A, “MOSS-E Worksheets for Controller Installation” on page 93) to record values you assign to the parameters described in this section.

Generate MOSS-E Alerts

To Generate MOSS-E Alerts

If you use the NetView program, verify that the Configuration management parameter in the MOSS-E NetView/Link Operation function, Generate alerts, is checked (✓) and customized. For more information, refer to the “MOSS-E Service Processor Customization Function” appendix in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

To Not Generate MOSS-E Alerts

If you do not want to report alerts from the service processor to the NetView program, verify that the Configuration management parameter in the MOSS-E NetView/Link Operation function Generate alerts is **not** checked. If you are using the NetView program, but do not want MOSS-E alerts sent for a time, use this parameter to prevent alert generation and later to reenable the alerts.

Use the worksheet on page 93 to record values you assign to the parameters described in this section.

To Locate the Generate Alerts Parameter

To locate this parameter:

- Step 1. Open the Service Processor menu.
- Step 2. Open the Configuration Management menu.
- Step 3. Run the SP Customization function.
- Step 4. Check (✓) **NetView Link / Operations** and click **Next**.
- Step 5. Check (✓) **Generate Alerts** or remove the check mark next to **Generate Alerts** as needed.
- Step 6. If you enabled **Generate Alerts**, customize the NetView Links / Identification / LAN address / and Dial Phone number as required.
- Step 7. Click **Next** and customize the 3270 Session Information if required.
- Step 8. Click **Next** to exit the screen.
- Step 9. Click **Close**.
- Step 10. Select **Yes** to validate the changes, or **No** to cancel the changes.

Wait for the Service Processor Customization in Progress message to clear, this may take several minutes.
- Step 11. Click **OK** when Service Processor Customization Successful message is displayed.

NetView V2R4 Alert Code Point Customizing

The NetView Program, Version 3 Release 1, supports all the code points used by the service processor and network node processor in the alerts sent to the network operator.

NetView V2R4 does not support all the code points of the 3746 Network Node; new code points are used in the alerts related to APPN/HPR.

If you are using NetView V2R4, the code points listed in this section must be added to your NetView program with their messages. The procedure to customize the code points is found in the *NetView V2 R4: Customization Guide*, SC31-7091.

Generic Alert Data (X'92') Alert MS Subvector:

X'3122' APPN/HPR-DLUR PROTOCOL ERROR

Meaning: A product implementing the APPN/HPR dependent LU requester (DLUR) function has detected a protocol problem that may impact users.

X'800A' APPN/HPR-DLUR CONFIGURATION ERROR

Meaning: A product implementing the APPN/HPR dependent LU requester (DLUR) function has detected a configuration problem that may impact users.

Most Probable Cause (X'93') Alert MS Subvector:

X'2019' APPN/HPR COMMUNICATIONS

Meaning: Self-explanatory

Install Causes (X'95') Alert MS Subvector:

X'80B9' NODE WAS INCORRECTLY SPECIFIED AS DEPENDENT LU SERVER

Meaning: A network administrator has specified the name of a dependent LU requester instead of the name of a dependent LU server. The configuration must be corrected before the DLUR function can operate.

Failure Causes (X'96') Alert MS Subvector:

X'202C' APPN/HPR COMMUNICATIONS FAILURE

Meaning: Self-explanatory

Service Processor and Network Node Processor

The information in this section is useful for managing the service processor and network node processor (NNP).

Do Not Use Service LAN for User Stations

Attention!

Service LAN problems may disrupt 3746 Network Node operations.

Token-Ring LAN Bridges

If remote consoles are connected to your LAN, the communication with the service LAN must be done through a bridge:

1. The bridge **must** be configured with the proper **filters** to prevent unnecessary traffic, such as broadcast storms, from entering the service LAN. Such broadcast storms are usually produced by IP traffic.

The bridge must forward only those frames that are explicitly addressed (no broadcast frames) to the service processors.

2. An improperly configured bridge on the service LAN can interfere with the operation of the network node processor and service processor. Among possible effects, such interference could:
 - Prevent the 3746 from completing its IML.
 - Prevent the 3746 from performing the selective IML of a processor, for example, the IML of ESCON processors for which a host link (not a host link station) definitions has been modified or deleted.
 - Degrade the operation of the 3746 Network Node (as explained in “Unplugged Cables and Stations”).
3. If a hub is used for communication between remote consoles and the service processors, the service processor access unit (the SPAU, that forms the service LAN inside the controller expansion) must be connected to the hub with the proper filter protection.

Vital components of the 3746 Network Node (the CBSP2/TIC3, service processor, and network node processors) **must never be directly** connected to a hub because of the risk of accidental or unplanned disruption of the related cables. See “Unplugged Cables and Stations.”

Unplugged Cables and Stations

Beaconing (resulting from removing a station or bridge) or unplugging the network node processor cable from the service LAN for a short time does not interfere with 3746 operations. The NN automatically reestablishes communications between the 3746 adapters and the network node processor. However, if these conditions last for more than about two minutes, the network node processor cannot re-establish contact with the 3746 adapters. While established user sessions are not disturbed, NN operations degrade (see “Controller Operations when the Network Node Processor Is Not Available” on page 39). To re-establish normal operation of the network node processor, it is necessary to re-IPL the network node processor. During the IPL, all traffic and sessions on the NN are halted.

Controller Operations when the Service Processor is Not Available

If you have a problem with your service processor, switch to your backup service processor, if you have one (see “Backing Up Your Service Processor” on page 38), and call the IBM service representative.

Normal operation of the 3746 Network Node requires the service processor but once the controller is correctly configured and operating, it may not be necessary to use the service processor for extended periods of time.

This means that if the service processor fails, you may not notice any immediate degradation in controller operation. If the service processor is not operational, then:

- The Controller Configuration and Management functions are not available to the local and remote operators.
- All operations explained in the following chapters are no longer available:
 - “NetView Alerts.” No alerts are reported to NetView for the 3746 Network Node or the service processor.
 - Chapter 6, “Connecting to the IBM Remote Support Facility.” There are no calls to the RSF (RETAIN®).

- Chapter 5, “Remote Customer Consoles.” There is no remote access to the MOSS-E.
- The service processor operator cannot:
 - IPL or IML the 3746 Network Node from the service processor.
 - IML a specific adapter.
 - Power on or off the 3746 Network Node through the MOSS-E.
- NNP access is unavailable.
- Also unavailable are automatic IMLs of the 3746 adapters.
- MAE access is unavailable.

However, the 3746 adapter dumps and error records are saved in the adapter. When the service processor is operational again, the MOSS-E automatically detects any dumps or error messages available in the adapters.

Recommendations for Customer Operations

IBM recommends regular scheduled use of the service processor to ensure that it is operating correctly and to keep network operators proficient with its advanced functions.

Save Configuration

Depending on the microcode level installed on your service processor, the procedure is different.

- Up to D46130 microcode level, an optical disk is used to back up the configuration data.
- From the F12380 microcode level, a diskette is used to back up the configuration data.

It is recommended to save the configuration data each time the configuration changes. For further information about backing up the configuration data, refer to the *3746 Nways MultiProtocol Controller Model 950: User's Guide*, SA33-0356, or the *3745 All Models and 3746-900 Basic Operations Guide*, SA33-0177.

Save Microcode

Note: The following applies to the LIC delivered on an optical disk, but only for EC up to D46130.

The current level of the MOSS-E microcode in the MOSS-E *must* be saved after each of the following functions is used:

- Change Active Code
- Manage Microcode Changes
- Manage Microcode Fixes.

To back up all the microcode, you must re-IPL the service processor. Refer to the *3746-950 User's Guide* or the *3745/3746-900 Basic Operations Guide*.

Backing Up Your Service Processor

Note: The following applies to the LIC delivered on an optical disk, but only for EC up to D46130.

To provide a higher level of reliability, you can order a second service processor which will replace your active service processor if it fails.

During normal operations, the backup service processor *is not connected* to the service processor LAN and should remain powered off. Its hard disk will be a duplicate of the active service processor hard disk. If recovery is needed, the failing active service processor is disconnected from the LAN and replaced by the backup.

Backing up your service processor requires both:

- Ordering and setting up a backup service processor
- Saving either:
 - Configuration data of the active MOSS-E and copying it to the backup hard disk
 - All the microcode in the active service processor, including the configuration data, and copying it to the backup hard disk.

Ordering and Setting Up a Backup Service Processor

Note: The following applies to the LIC delivered on an optical disk, but only for EC up to D46130.

You can order a second service processor feature as a backup. It is delivered with the licensed internal code already loaded on the hard disk.

If the backup service processor is delivered after the first one, the microcode level of the backup might differ from the level of the first service processor⁶.

If the code levels are different, you can use either the microcode level of your:

- Active service processor by copying it onto the hard disk of the backup service processor⁶.
- Backup service processor by copying just the active configuration onto the hard disk of the backup service processor⁶.

⁶ For information on how to check the microcode levels, to back up the MOSS-E microcode and the configuration data, refer to the *3745/3746-900 Basic Operations Guide* or the *3746-950 User's Guide*.

Controller Operations when the Network Node Processor Is Not Available

APPN/HPR Network Node

The interruption of network node processor operations does not disturb the established user traffic (LU-LU sessions) until the network node processor comes up again and the control point is activated. However, the interruption of the 3746 control point results in a degradation of the following NN operations:

- Resources cannot be activated and deactivated.
- Sessions cannot be started or stopped.
- Network problems cannot be reported.
- Other NNs get no response from the network node processor. They then assume that the node has failed and remove it from their network topology map.

In order to recover from a failing situation and return to normal operations, you can either:

- Restart the APPN/HPR control point that runs in the network node processor.
- Shutdown and restart, that is re-IML the whole network processor.

In either case, *CCM User's Guide*, SH11-3081 provides the possibility to automatically activate the configuration by enabling the Automatic configuration activation option.

When this option is enabled, restarting the control point or re-IMLing the NN interrupts the 3746 operation, which results in the loss of data traffic flowing through the 3746 resources.

When this option is disabled, restarting the control point or re-IMLing the NN does not interrupt the 3746 operation and therefore preserves the traffic flowing through the 3746 resources, until you manually activate the configuration by clicking **Activate Configuration**.

IP Routing

The interruption of the network node processor does not disturb IP routing functions:

- IP datagrams are still forwarded based on the existing routing table and caches.
- OSPF/RIP/BGP are still able to exchange routing information thus allowing datagrams for new destinations to be routed.

However, the interruption of the network node processor results in a degradation of the IP router operations:

- IP resources cannot be activated, deactivated, nor displayed.
- No Telnet operations to the NNP are possible.
- SNMP flows are no longer handled. This could lead to a *router down* image in the Tivoli NetView displays.

Restarting the network node processor resets and activates all the 3746 interfaces and flushes all caches and dynamic routing table entries (that is, those *known* by OSPF/RIP/BGP). For IP users, this could lead to longer response times; some IP

packets are lost and retransmitted by the TCP end points during the restart of the interfaces. However, from the user's (end-to-end) point of view, the TCP connection is not disrupted.

Dual Network Node Processors

Each 3746 Network Node can have two network node processors:

- One is *active* and running the control point.
- The other is in *hot standby* and ready to take over in case the active network node processor should fail.

The first network node processor installed is identified as NNP-A, the second is NNP-B. (Refer to the "Physical Planning Details" chapter in the *3745/3746 Planning Series: Physical Planning* for the physical location of the two network node processors.) Dual NN processor operation can be enabled or disabled depending on whether or not the operator has selected the Enable CP/NNP Backup option. Both network node processors are monitored by the service processor.

When the active network node processor is failing, the service processor requests the standby network node processor to become active using the same configuration as the formerly active network node processor used. This can be either automatically or manually done:

- If the Enable CP/NNP Backup option is enabled, the standby NNP automatically takes over the failing active NNP.
- Otherwise, the operator manually starts or IMLs the standby NNP.

In either case, *CCM User's Guide*, SH11-3081 provides the possibility to automatically activate the configuration by enabling the Automatic configuration activation option.

- When this option is enabled, data traffic flowing through the 3746 resources is lost, reset, and started.
- When this option is disabled, established traffic stays running but no new connections are possible until the operator manually activates the configuration by clicking **Activate Configuration**, which is disruptive for the 3746 operation.

Chapter 2. 3746 APPN/HPR Network Node Management

This chapter describes aspects of network management relevant to the operation of the 3746 Network Node. It only deals with the management of APPN Resources connected to the 3746 native enclosures, and visible through the NNP control point. For information about APPN resources controlled by the MAE control point, see the “MAE APPN/HPR Network Node Management” chapter in the *3745/3746 Planning Series: Multiaccess Enclosure Planning*. This chapter covers the following subjects:

- Graphical APPN Topology management with NetView
- APPN Configuration management with the CCM
- Performance management with Network Performance Monitor, see Chapter 4, “Performance Management with NetView Performance Monitor” on page 59.

NetView APPN/HPR Topology Management

As explained in “NetView for OS/390 Management of APPN Networks Overview” on page 2, the Topology Manager of APPN/HPR is part of the NetView for MVS product, and allows you to graphically display and control APPN resources. The 3746 supports the SNATAM topology agent but does not support the Accounting Manager.

The Topology Manager of NetView and the Topology Agent of the 3746 Network Node exchange data over LU 6.2 sessions.

Topology Manager enables you to:

- Monitor APPN/HPR network topology to view the connectivity between APPN/HPR network nodes.
- Monitor APPN/HPR local topology to view a 3746 Network Node and its:
 - Transmission groups (TGs)
 - Ports
 - Logical links
 - Adjacent network nodes
 - End nodes
 - Low end networks.
- Control the status of ports and links, that is, to activate or deactivate them.
- Display views of:
 - An APPN/HPR network
 - APPN/HPR subnetworks
 - Particular domains of a network node.
- Display information about resources such as control points, link names, TG numbers and so on.
- Automate operations using NetView Resource Object Data Manager (RODM) objects.

Note: The APPNTAM TOPOSNA RECYCLE is not supported by the 3746.

Configuring APPN/HPR Topology Management

Host Definitions

To monitor the APPN topology of a network, the name of a network node must be declared to the NetView topology manager with the following command:

```
TOPOSNA MONITOR, NETWORK, NODE=Nodename
```

Where *Nodename* is the name of the network node.

To change the node monitoring the network, use the following commands:

```
TOPOSNA STOP, NETWORK, NODE=Nodename
```

```
TOPOSNA MONITOR, NETWORK, NODE=NewNodename
```

All APPN network nodes with a topology agent are capable of monitoring their local topology and sending the information to the NetView topology manager, including the 3746-9x0. To monitor local topology use the following commands:

```
TOPOSNA STOP, LOCAL, NODE=Nodename
```

```
TOPOSNA MONITOR, NETWORK, NODE=NewNodename
```

It is not recommended that the 3746 NN be used as the agent for monitoring the network topology of a large APPN network due to the extra load this creates on the NNP.

CCM Definitions

The topology agent runs continually on the 3746 NNP, and does not need to be explicitly started.

NetView Graphic Monitor Facility Topology Examples

NGMF topology presents a list of the topology displays available when the operator logs on to NGMF. The list of displays available depends upon the network being monitored and the number of agents that topology data is being collected from. Selecting one of these displays and navigating down through the data presented allows the operator to display a wealth of APPN information.

Figure 22 shows an example APPN network. As APPN network nodes all have the same representation of a network's topology, network topology need not be collected from every network node in an APPN network. The view shown displays APPN network nodes and the transmission groups connecting them.

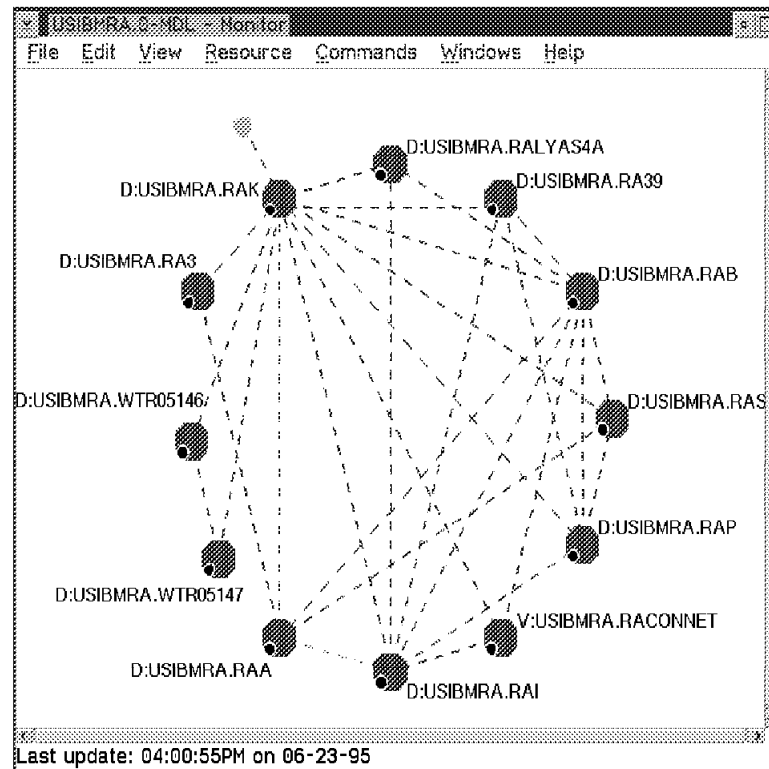


Figure 22. Single Network View

Selecting a more detailed view for node USIBMRA.WTR05147 brings up a more detailed logical view with information similar to that shown in Figure 23 on page 44.

In Figure 23, all nodes and TGs are shown that connect to USIBMRA.WTR05147. All resources shown can have commands issued against them.

When local topology is also connected for a 3746, then physical adapters and predefined or dynamic links can also be displayed.

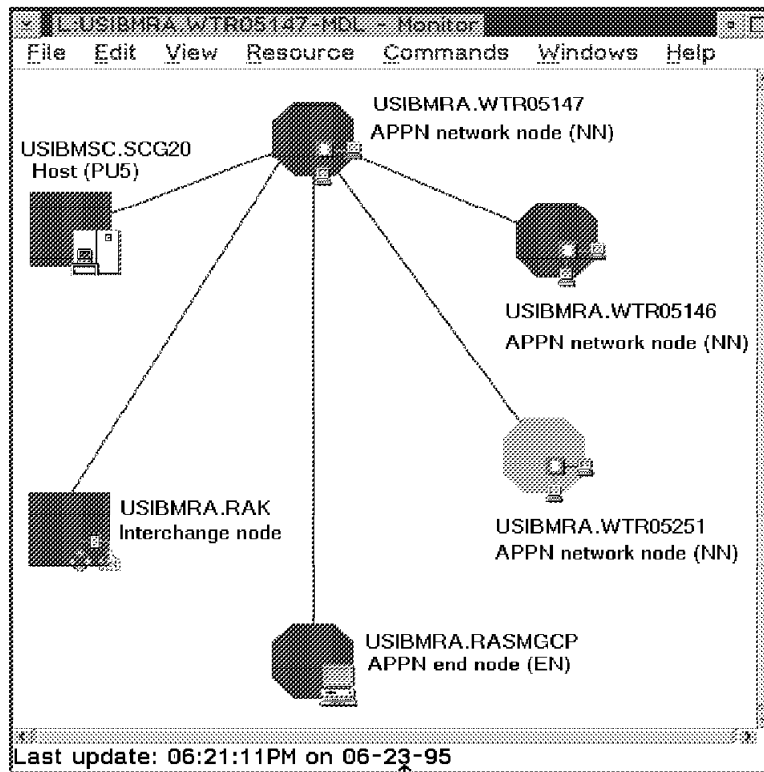


Figure 23. More Detailed View of a Network Node

Local 3746 APPN/HPR Topology Management from the Service Processor

To display the local topology of the 3746 APPN network nodes, (adjacent nodes, including dependent PUs), the *CCM User's Guide*, SH11-3081 tool must be used.

With DCAF running in the NGMF workstation (or an OS/2 workstation), the operator can remotely access 3746 Network Nodes and run the 3746 node configuration, local topology display, and network management functions of the CCM.

Local APPN Topology Examples

This section explains how to go to the windows where you can see details of the APPN resources running on the network, and activate or deactivate these resources.

Figure 24 shows the APPN-specific cascade menu.

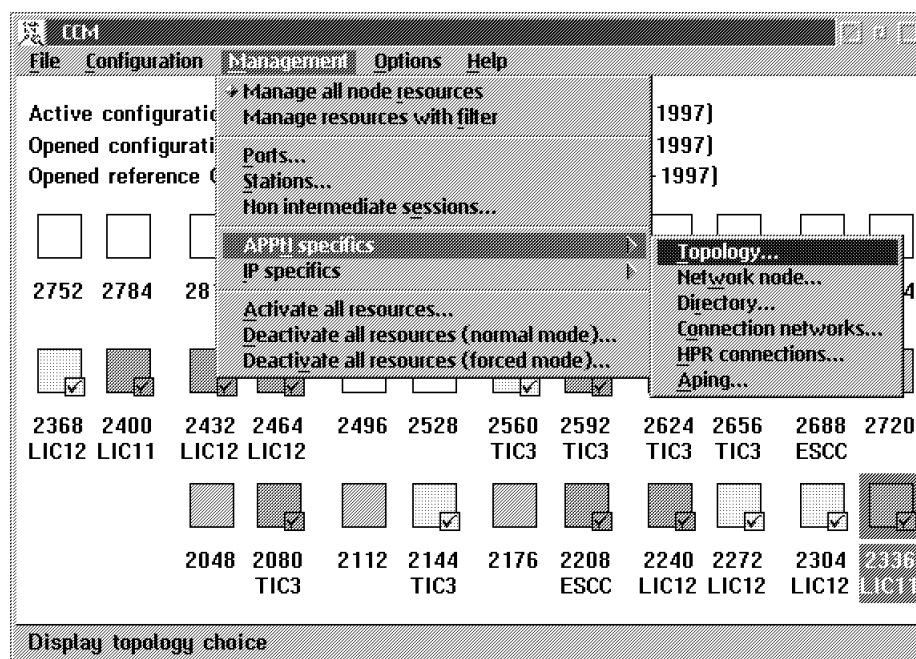


Figure 24. Example Management Window for APPN

Definitions for Performance Monitoring on APPN/HPR

For 3746-900 adapters running APPN that are not under NCP control, and 3746-950 adapters running APPN, the NPALU which runs in the NNP collects performance data.

If the 3746 is connected to the host NetView over an APPN network, then the NPALU session (LU type 0) must be transported over a DLUR/DLUS connection to the host. To support DLUS, the minimum level required for VTAM is Version 4, Release 2.

The following section explains how to activate NPM performance monitoring on the NNP, and then how to define a path to the host NetView for delivering the information collected to NPM over an APPN network.

In addition to these definitions, either at the port or station level, you must specify whether to collect NPM information or not for your resources.

Note: By default, *all* resources are defined with NPA eligible set to No. This means that if you want to collect data from a particular resource you should set NPA eligibility to Yes. In addition, setting NPA eligible set to Yes for a port, will enable data collection for all dynamically defined stations on that port.

Figure 25 shows the machine configuration that the following definition steps refer to.

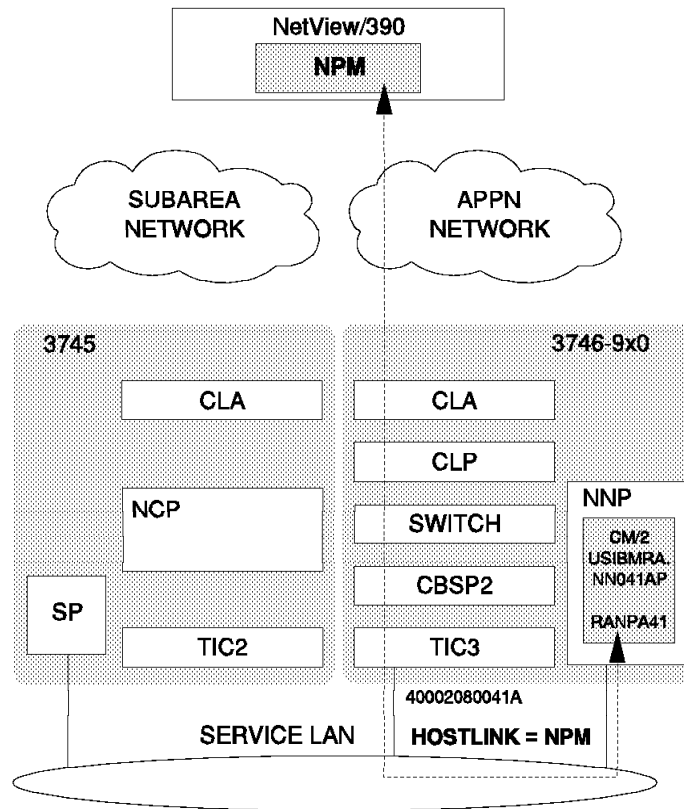


Figure 25. NPM Configuration

3746 Definitions for NPM

To create definitions for NPM on the 3746, you must:

1. Use CCM to allow port 2080 to automatically generate a station for the NPALU on the NNP.
2. Use CCM to define a DLUS/DLUR pipe to the VTAM that is the DLUS.
3. Create the host VTAM and NPM definitions.

These steps are described in the following sections.

Note: You must define the Network ID, local node name, and NPALU that the IBM service representative configured during the installation of the service processor. See the procedure for the definitions in the section about configuring the NetView Performance Monitor (NPM) in either of the following guides:

- *3746 Nways Multiprotocol Controller, Model 900: Installation Guide*
- *3746 Nways Multiprotocol Controller, Model 950: Installation Guide*

After creating the NPM definitions, be sure to fill out the NPM worksheet in the “MOSS-E Worksheets for Controller Installation” appendix in the *3745/3746 Planning Series: Overview, Installation, and Integration* with the following names:

- NETID of NPM
- PU running on the NNP for NPM
- NPA LU running on the NNP for NPM.

CCM Station Definitions on Port 2080

These CCM definitions allow the NPALU on the NNP to communicate with VTAM via PORT2080. Port 2080 does not allow link stations to be dynamically defined for incoming calls, therefore the link station for the NPALU must be manually defined.

Step 1. Select and open the active configuration on CCM.

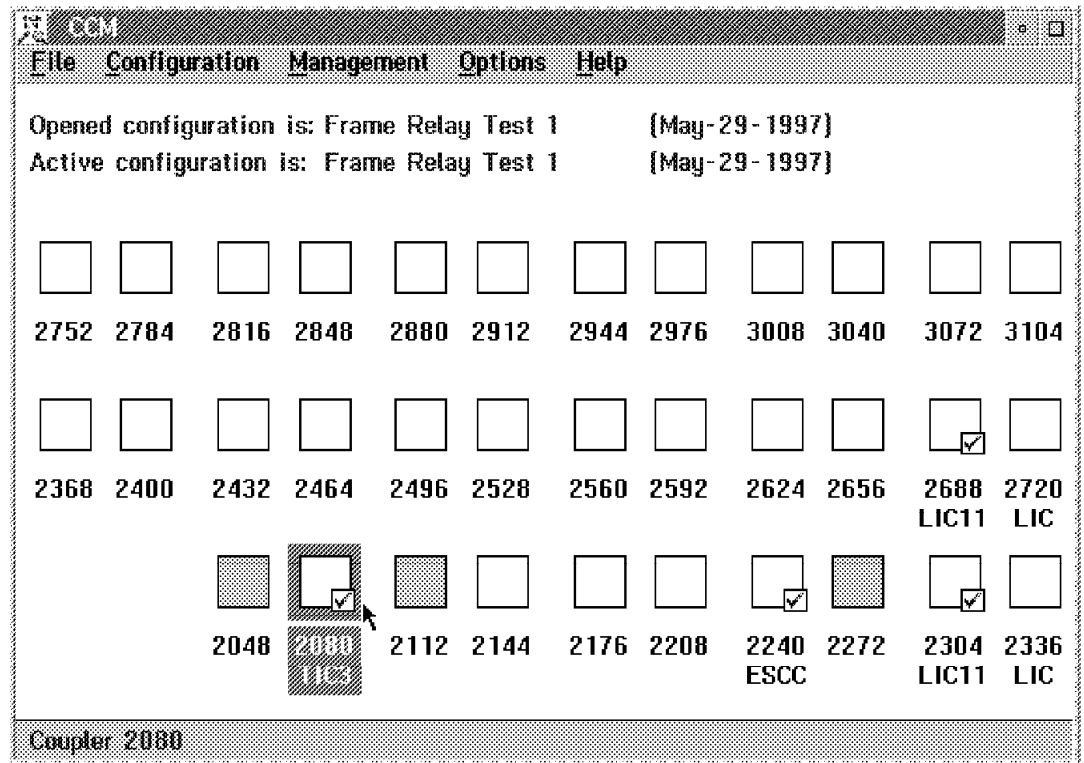


Figure 26. Active Configuration

Step 2. Select **port 2080**, this brings up a list box that asks you if you want to have automatic NPM definitions made on this port. Click **YES**.

Note: This is not possible on the stand-alone CCM.

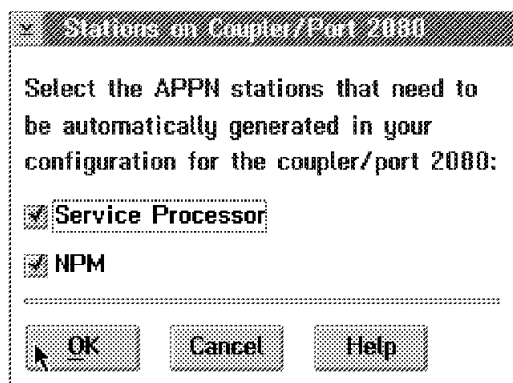


Figure 27. Stations on Coupler/Port 2080

Step 3. Make sure NPM and (if applicable) service processor are checked, then click **OK**.

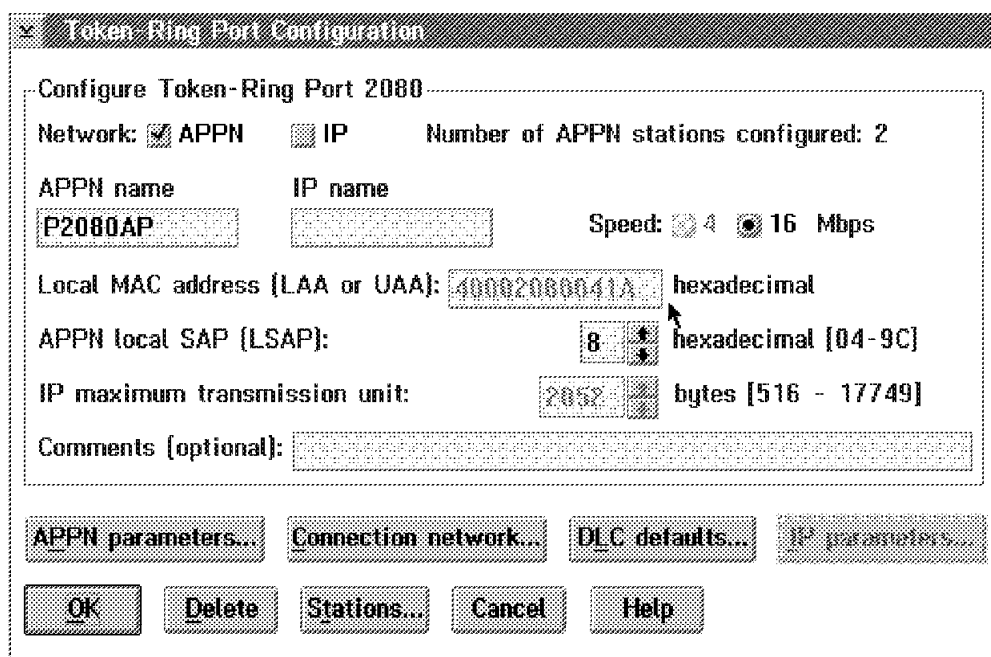
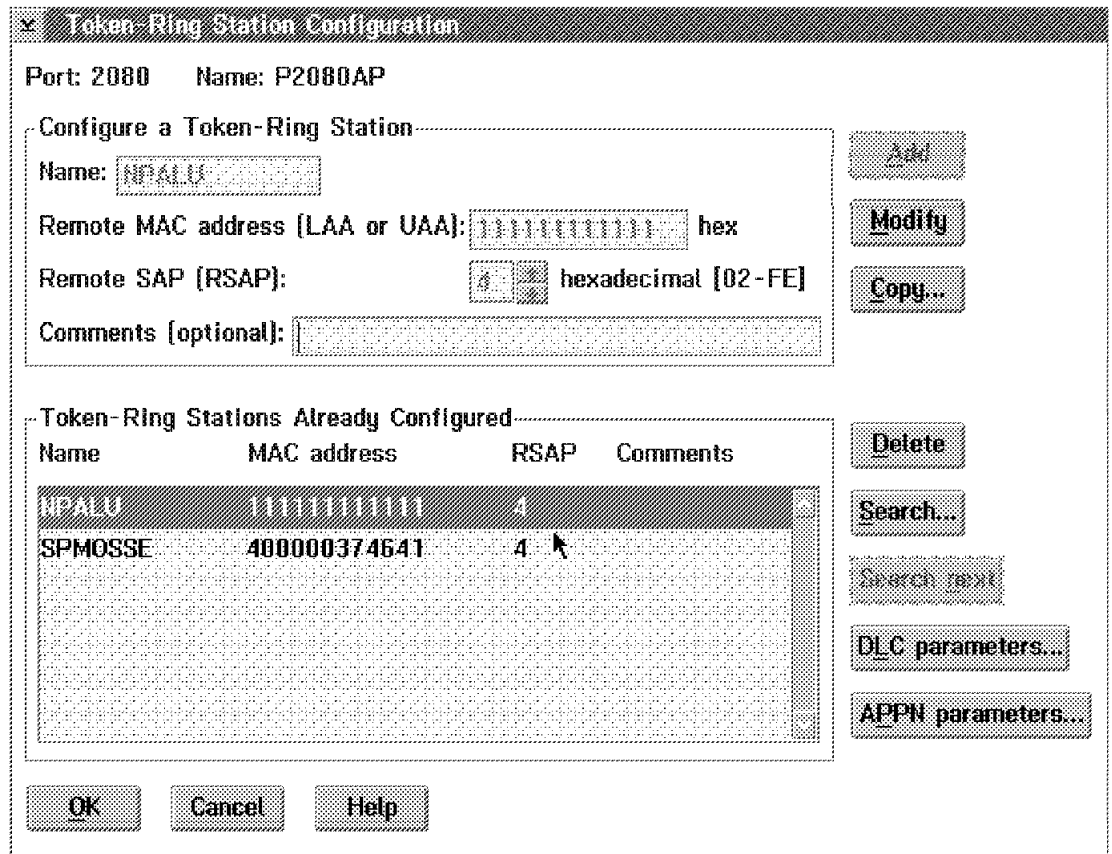


Figure 28. Token-Ring Port Configuration

Note: On this window, you can see the MAC address of this port, this must match the destination MAC address defined in CM/2 for the link called **NPM**.

Step 4. Click **Stations**.



The dialog box is titled "Token-Ring Station Configuration". It has a port number of 2080 and a name of P2080AP. It is divided into two main sections: "Configure a Token-Ring Station" and "Token-Ring Stations Already Configured".

Configure a Token-Ring Station:

- Name: NPALU
- Remote MAC address (LAA or UAA): 1111111111 hex
- Remote SAP (RSAP): 4 hexadecimal [02-FE]
- Comments (optional):

Token-Ring Stations Already Configured:

Name	MAC address	RSAP	Comments
NPALU	1111111111	4	
SPMOSSE	400000374641	4	

Buttons on the right side: Add, Modify, Copy, Delete, Search, Search next, DLC parameters..., APPN parameters... Buttons at the bottom: OK, Cancel, Help.

Figure 29. Token-Ring Station Configuration

Step 5. On this window, you can see the station which was automatically defined for the NPALU running on the NNP. The destination MAC address of 1111111111 does not match any real address. When this CCM configuration is activated, the NDF part is sent to the NNP. There, this MAC address is automatically updated to contain the correct MAC address for the NNP.

Step 6. Select **NPALU**, click **APPN parameters...**, and go to "DLUR/DLUS Definitions" on page 51.

DLUR/DLUS Definitions

Enter (or verify that) the information in Figure 30, for the primary DLU server **USIBMRA.RAK** has been defined.

Figure 30. APPN Parameters

In our case, the DLUS/R is needed because we only have an APPN path to RAK, where NetView and NPM are running. As the NPALU (TESTNPA) is a type 0 LU, DLUR provides the path through the APPN network to allow the PU TESTNOPD and its LU TESTNPA to be activated and have SSCP sessions to RAK.

Close the CCM windows by clicking **OK**, and the configuration can be activated when desired.

Host VTAM and NPM Definitions

To support NPM, the following host definitions must be made:

1. **Switched major node**, refer to the example given in Figure 31.
2. **Resource resolution table**, refer to the example given in Figure 32 on page 52.

In these tables the CP and LU names must be equal to the names previously defined in communications manager:

- CPNAME (TESTNOPD) = Local node name
- LUNAME (TESTNPA) = LU name.

```
DLUR41  VBUILD TYPE=SWNET,MAXGRP=1,MAXNO=1
-----*
* ERS4 : PU NNP                                     *
```

```
TESTNOPD PU  ADDR=04,PUTYPE=2,CPNAME= TESTNOPD
TESTNPA LU   LOCADDR=1
```

Figure 31. Example of Switched Major Node

```

*****
*   DESCRIPTIVE NAME : 3746 MODEL 900 VTAMLST DEFINITION   *
*****
*   BUILD STATEMENT - CONTROLLER INFO                       *
*****
*
TESTNOPD BUILD MODEL=3746-900,                                X
                        NETID=SYSTSTAP,                        X
                        NEWNAME=TESTNOPD,                      X
                        NPA=(YES,DR),                          X
                        VERSION=N/A
*
*****
*   NPM VIRTUAL RESOURCES                                   *
*****
M900NPA GROUP LNCTL=SDLC,                                     X
                        NPARSC=YES,                             X
                        VIRTUAL=YES,                             X
                        NPACOLL=YES,                             X
                        ISTATUS=ACTIVE
*
TESTNODL LINE
TESTNOPD PU
TESTNPA LU
*
*****
*   END OF GEN SOURCE                                     *
*****
*
GENEND GENEND
END

```

Figure 32. Example of Resource Resolution Table

Figure 33 displays the NPM management panel that allows you to define the NPM configuration for the NNP as mentioned in “3746 Definitions for NPM” on page 47.

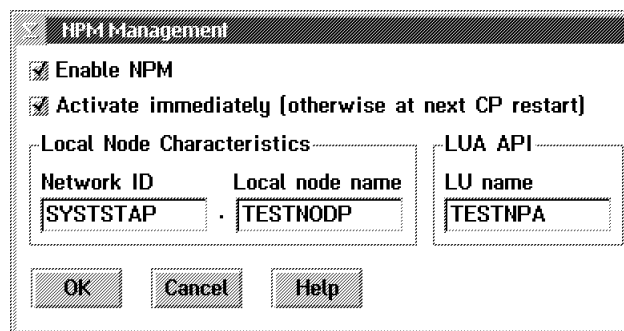


Figure 33. NPM Management Menu

Chapter 3. MAE APPN/HPR Network Node Management

You can manage the MAE network node as an APPN entry point, which forwards APPN-related alerts to an APPN focal point, or as an SNMP-managed node.

APPN/HPR Alerts

The MAE network node can serve as an APPN entry point for alerts related to APPN. As an entry point, the router is responsible for forwarding APPN and LU 6.2 generic alerts about itself and the resources in its domain to a *focal point* for centralized processing. A focal point is an entry point that provides centralized management and control for other entry points for one or more network management categories.

Note: If the focal point node is not available to receive an alert from the router network node, the alert is “held” (stored) by CPMS. APPN on the router can hold up to ten alerts.

Entry points, such as the MAE, that communicate with a focal point make up that focal point's *sphere of control*. If a focal point explicitly defines the entry points in its sphere of control and initiates communication with those entry points, it is an *explicit focal point*. If a focal point is designated by its entry points, which initiate communication with the focal point, the focal point is an *implicit focal point*. The focal point for the router is an explicit focal point.

An explicit focal point must define the router entry point node as being within its sphere of control and initiate a session, or *focal-point-to-entry-point relationship*, with the router. When this relationship is established, the focal point becomes the *primary focal point* for the router. The focal point also informs the router entry point about the existence of a *backup focal point*, if one has been designated.

If the session between the router entry point and its primary focal point fails, the router can initiate a session with a designated backup focal point, provided it has been informed by the primary focal point of the backup focal points it is to use. Before initiating a session with a backup focal point, the router entry point makes an attempt to re-establish communication with its primary focal point. If that attempt fails, the router switches to the backup focal point. The primary focal point is then responsible for re-establishing the focal point to entry-point relationship with the router.

The router entry point communicates with the focal point through an LU 6.2 session. Multiple-domain support (MDS) is the mechanism that controls the transport of management services requests and data between these nodes. The router network node does *not* support SSCP-PU sessions with focal points.

Management processes within the router's control point are handled by its control point management services (CPMS) component. The CPMS component within the router network node collects unsolicited problem management data from resources within the router's domain and forwards this data to the appropriate focal point.

Supported Message Units

The MAE network node uses the following message units for sending and receiving management services data, including alert messages from domain ENs:

Message unit	Description
CP-MSU	Control point management services unit. This message unit is generated by CPMS and contains alert information forwarded by the router entry point. CPMS passes CP-MSU message units to MDS.
MDS-MU	Multiple-domain support message unit. This message unit is generated by MDS. It encapsulates the CP-MSU for transport between nodes.

Logging of APPN Alerts on the Router

The MAE network node logs all APPN and LU 6.2 generic alerts using the Event Logging System (ELS). You can access these alerts by using the MAE error logging facility.

Managing the Network Node Functions from an SNMP Manager

The router network node can function as an SNMP-managed node. An operator or application at an SNMP network management station can query objects in the APPN MIBs (using the SNMP GET AND GET NEXT commands) to retrieve APPN status information and node statistics. A subset of APPN MIB objects can be modified using the SNMP SET command.

As an SNMP-managed node, the router can send unsolicited status and error information, in the form of traps to an SNMP manager.

MIBs Provided by APPN

The MIB support provided by APPN in MAS V1R1.0 on the MAE is:

- Support of GET, GET_NEXT, SET, AND TRAP
- APPN MIB
- APPN HPR MIB
- APPN DLUR MIB
- RPC 1666 - SNA NAU MIB.

The MIB support provided by APPN in the multiaccess enclosure is:

- Support of GET, GET_NEXT, SET, AND TRAP
- IETF Standard APPC MIB - RFC 2051
- IETF Standard APPN MIB
- IETF Standard APPN HPR MIB
- IETF Standard APPN DLUR MIB
- RPC 1666 - SNA NAU MIB
- Portions of the previously available private APPN MIB
 - DLC Trace, Memory, and Accounting
- Portions of the previously available private APPN HPR MIB
 - HPR NCL and Route Test.

Note that MIB information is also available for the underlying interfaces and protocols that APPN uses. APPN is just a logical protocol that sits above and uses the interfaces.

Providing Topology Information to the SNA Topology Manager

The SNA Topology Manager (SNATM) components of TME 10 NetView for OS/390 and NetView for MVS/ESA® V3R1 provide object-oriented management and control of SNA subarea and APPN networks. SNATM uses CMIP protocols over SNA transport to communicate with agents, which provide it with topology information. CMIP-based agents are provided for such products as VTAM V4R3, Communications Manager/2 and Communications Server/2, the 2217, and the 3746-9X0 Network Node Processor.

The MAE APPN implementation does not provide a CMIP over SNA agent, so its APPN topology cannot be managed directly, in a transparent way, from the mainframe NetView. The TME 10 NetView for OS/390 APPN Topology Integrator allows the MAE APPN topology to be managed by NetView.

MAE (FC 3000) SNMP Configuration

This section shows how to make SNMP definitions for the MAE (FC 300)⁷ using the MAE Configuration Program:

1. From the Navigation Window, select **General**, under the SNMP Config folder.

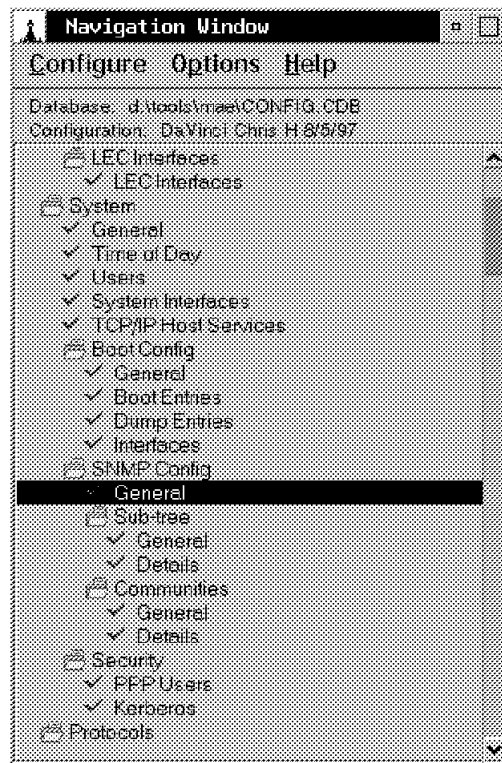


Figure 34. Navigation Window

⁷ For the MAE (FC 3001), the SNMP definitions are made through the CCM.

2. On the SNMP general window, SNMP can be enabled, and the UDP port for traps can be specified.

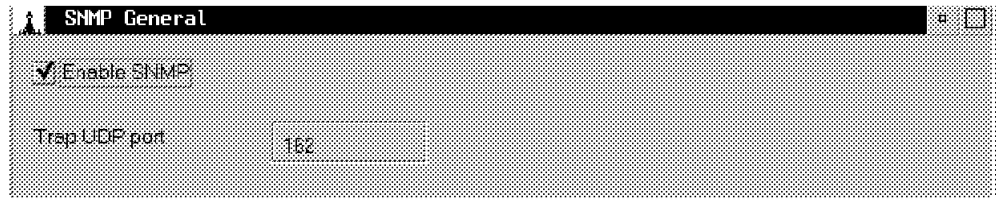


Figure 35. SNMP General Window

3. From the Navigation Window, select **General**, under the Communities folder. On the SNMP Communities screen, the names of SNMP communities can be defined, the type of access the community has to the MIB variables, and the view of the MIB that the community is presented.

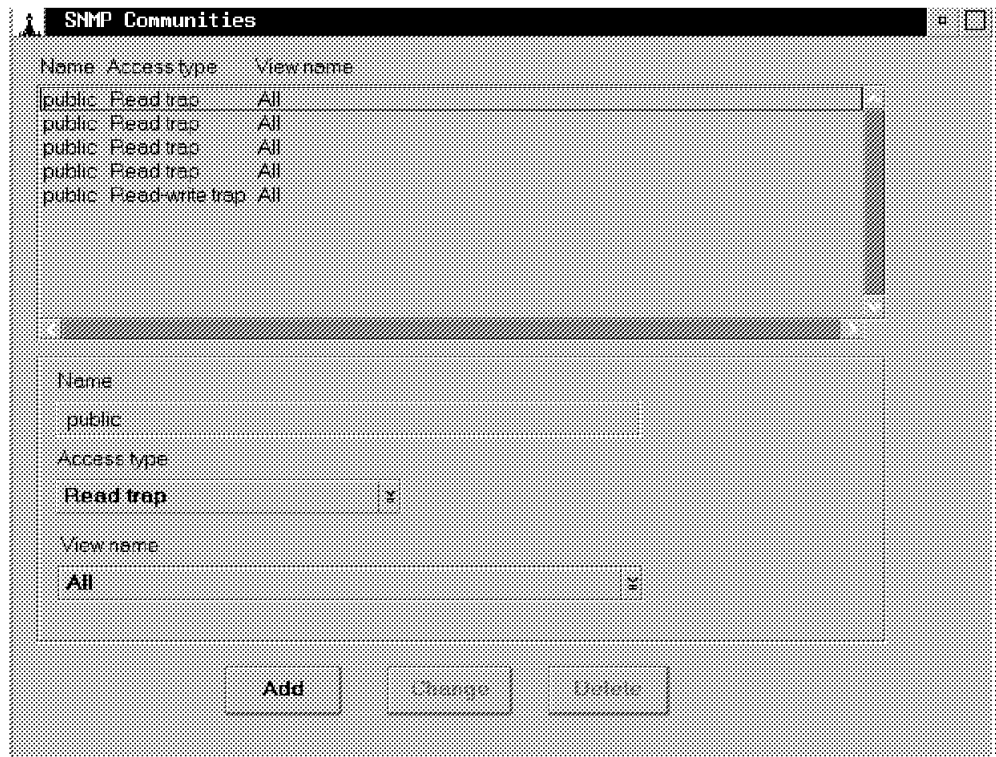


Figure 36. SNMP Communities Window

4. From the Navigation Window, select **Details**, under the Communities folder.
On the SNMP Communities (Details) screen, the names of SNMP communities defined on the Communities screen are listed, select **Addresses**. This gives you the possibility to define the IP addresses and subnet masks of members of the community.

The members will receive traps from the 3746 Multiaccess Enclosure, and can access the MIB variables allowed for their community.

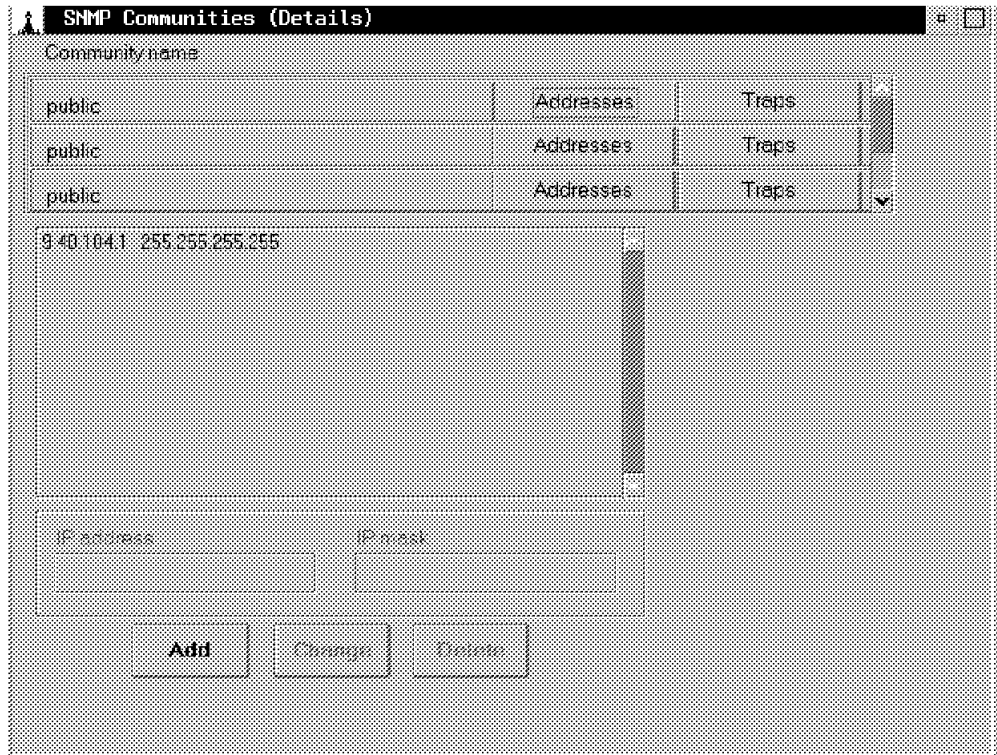


Figure 37. SNMP Communities (Details)

5. Select **Traps**. This allows you to define the types of traps that are sent to the members of the community. In this case, **All** was selected.

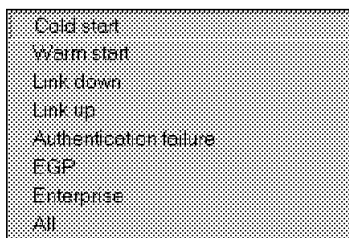


Figure 38. Types of Traps

Chapter 4. Performance Management with NetView Performance Monitor

This chapter describes the 3746 support of the NetView Performance Monitor (NPM) and the migration of performance monitoring using NPM from an SNA environment to an APPN/HPR environment. It assumes you are familiar with the NPM.

Note: For customers operating a 3746 Model 900 or 950 with NetView Performance Monitor (NPM), the installation of any one of the following requires at a **minimum** NPM V2R4 with APAR OW37743:

- 3746 and MAE Extended Functions 4 (FC 5810 or 5811)
- 3746 Extended Functions 2 (FC 5802)

The Need for Performance Monitoring

Performance monitoring consists of three basic tasks:

- Collecting data as the events being monitored are happening.
- Sending the data collected to a central point.
- Analyzing the data to give the required picture of present performance against either:
 - A past situation
 - An ideal attainable situation.

The purpose of analysis depends on the requirement for monitoring. It could be:

- To offer the best throughput for the cost of the network
- Real-time traffic management
- Accounting and charging purposes.

Whatever the purpose, performance monitoring is a combination of host and 3746 Network Node activities.

Current Performance Monitoring on SNA Networks

The Network Performance Application (NPA) in the NCP collects performance and accounting data from the 3745, and 3746 adapters that are under NCP control. Referring to Figure 39 on page 60, the present mix of activities is:

1. Individual DLCs (SDLC, channel CDLC, token-ring 802.2, frame relay, X.25, and ISDN) collect data according to keywords chosen at NCP generation time. The DLCs have algorithms onboard to watch data flowing through them and to collect the required information. Only that information chosen at generation time can be collected.
2. The task running in the NCP that controls the DLCs, NPA (Network Performance Application) gathers data from the DLCs.
3. The NPA in NCP has a LU0 logical unit called the NPALU. This is connected to the NPM running in the host via an LU-LU session.

The NPALU is connected either over a subarea path or over an APPN path to the host NPM via a DLUR/DLUS connection.

Figure 40 on page 61 shows these paths.

4. NPM receives the data from all the NPAs and displays or prints the required analysis.

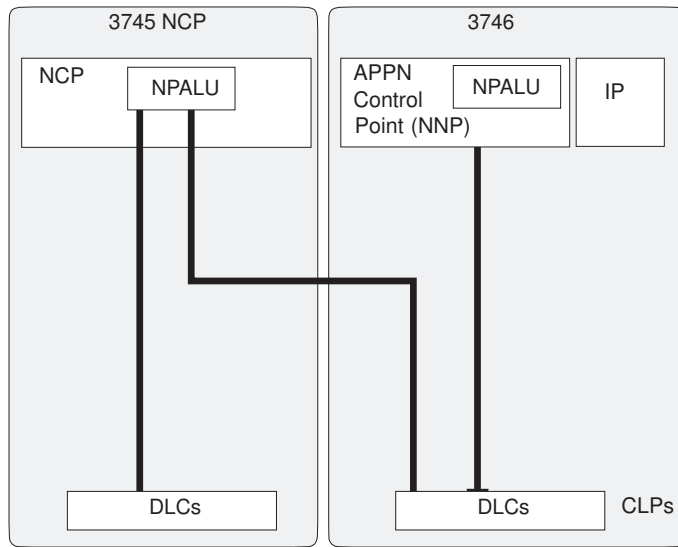


Figure 39. NPM Data Collection

Migrating to APPN/HPR Performance Monitoring

Under APPN/HPR there is a more dynamic situation, which allows you to perform the following actions:

- Define the data you want to collect using the CCM. The definitions are held in the Network Definition File (NDF).
- Establish a DLUR/DLUS connection to a VTAM that has subarea connectivity to the NPM that will collect the data (this VTAM must be V4R2 or later). The DLUR/DLUS session is needed to transport the LU0 session between the NPALU and NPM over the APPN network.

See “Definitions for Performance Monitoring on APPN/HPR” on page 45 for details of the definitions needed in the CCM and VTAM.

Once you have set up the collection environment, you can collect and analyze performance data:

1. Individual DLCs (SDLC, ESCON, CDLC, 802.2, frame relay, and X.25) collect data according to keywords defined in the CCM. Only that information defined in the NDF by the CCM can be collected.
2. NPA, running under the 3746 APPN/HPR control point gathers data from the DLCs.
3. NPA transfers the data to NPM via the NPALU (LU0), this LU is supported by CM/2 running on the NNP.
4. NPM receives the data from all the NPAs and displays or prints the required analysis.

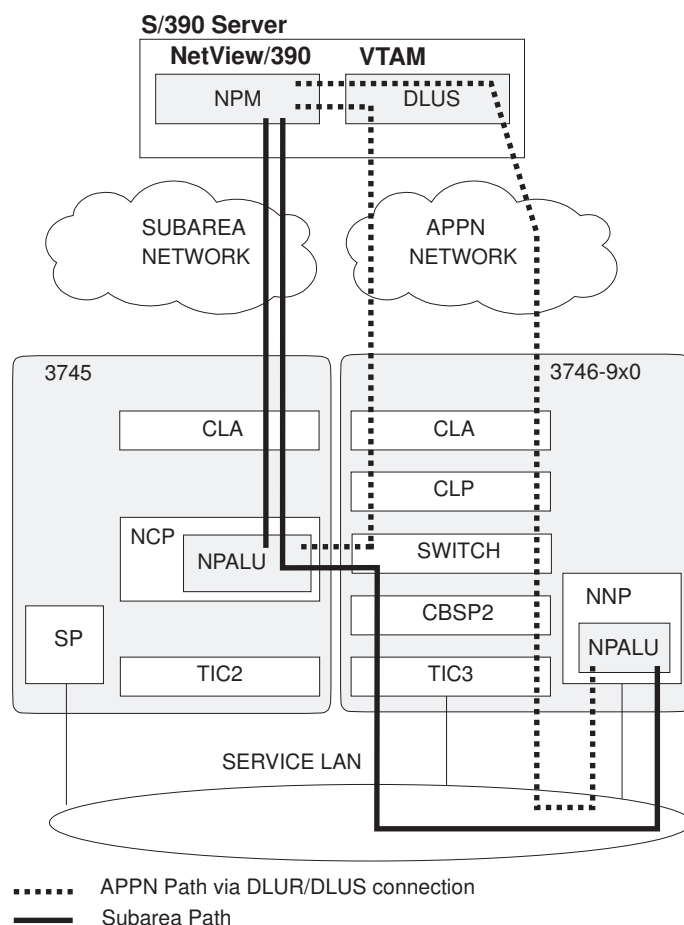


Figure 40. APPN/HPR Performance Monitoring Activities (3746 Network Node)

Note: Figure 40 shows NPM data being transmitted from the NNP over the service LAN to the 3746 or 3745. Although it is recommended that no stations use the service LAN for user data, using a path over the service LAN and PORT2080 for NPM data is acceptable.

Data Collected for the NetView Performance Monitor

No data is collected and sent to the NetView Performance Monitor (NPM) for an MAE resource.

Performance monitoring data

The 3746-900 and 3746-950 provide the NetView Performance Monitor (NPM) with many performance monitoring records, no matter how they are reported (through a 3746-900 via the NCP or NNP or through a 3746-950 via the NNP). The contents of these records depend on which resource is monitored.

Note: That for a given resource, a 3746-900 equipped with an NNP can forward the reports using both the NCP and the NNP if the resource is shared by both control points, and defined as NPA-eligible in both configurations.

Some examples of the performance data is given below. For the complete list and details of the performance data available, refer to the NPM documentation.

- Processor utilization

The following data is provided for each processor of the 3746-9x0:

- Processor type:

- x'51'** CBTRP : Controller Bus and Token-ring Processor. The CBTRP is a TRP equipped with a CBC in place of a TIC3 for attachment to the 3745 CCU B.

- x'52'** CLP : Communication Line Processor

- x'53'** ESCP : ESCON Processor

- x'54'** TRP : Token-Ring Processor

- x'55'** CBSP : Controller Bus and Service Processor

- Processor utilization (in percentage from 0 to 100)
 - Buffer storage utilization (SDS), that is, percentage of buffer storage in use
 - Program storage utilization (PDS), that is, percentage of program storage in use

For a 3746-900, NCP adds information about the 3745 CCU and buffer utilization to the above-mentioned data. Of course the corresponding fields are meaningless for a 3746-950.

Because a resource name is required to reference the processor utilization record, the NCP name is used for a 3746-900 and the network node name for a 3746-950.

Note: Monitoring of processor utilization requires the engineering change D46130I for a 3746-950.

- ESCON physical link

The following counters are provided to the NPM:

- I-frames sent
 - I-frames received
 - Bytes sent
 - Bytes received
 - Retransmitted I-frames
 - Retransmitted bytes
 - Total error count
 - Outbound queue length
 - Total poll count
 - Positive poll count
 - When one or more ESCON stations work in HPR mode, the following counters are also provided for the global HPR traffic flowing over the optical link:
 - HPR frames sent
 - HPR frames received
 - HPR bytes sent
 - HPR bytes received
 - HPR bytes queued for transmission
 - Transmit HPR frames discarded for exceeding the transmit queue threshold

- Received HPR frames discarded due to congestion in this node.

- ESCON station
- SDLC station
- Token-ring physical link
- Token-ring external user
- Token-ring station

Note: All the token-ring counters apply also to the service processor LAN attached to the CBSP.

- Frame-relay physical line
- Frame-relay FRTE
- Frame-relay FRFH
- Frame-relay LMI PU
- X.25 physical line
- X.25 physical PU
- X.25 Virtual Channel
- Point-to-Point Protocol

There is no NPM performance monitoring for a line or station running the Point-to-Point Protocol (PPP).

- ISDN

There is no performance monitoring for an ISDN D-channel of LIC16, because traffic on this channel is not high enough to require performance monitoring.

For an ISDN B-channel line, the same performance monitoring counters as for a physical frame-relay line are reported to the NPM, because this channel runs the frame-relay protocol.

For a logical ISDN line, the same performance monitoring counters as for a logical frame-relay line (FRTE) are reported to the NPM, because this channel runs the frame-relay protocol.

Note: ISDN performance monitoring requires the FC 5800.

Accounting data

Accounting reports can be used:

- To check the network charges.

In this case, remember that the way the network performs billing may be slightly different from the way the 3746-9x0 builds the accounting reports. So the checking can only be rough. The 3746-9x0 accounting reports can never be considered as a reference.

- To get detailed statistics data for each call.

As an example, accounting allows to compute the percentage of calls abnormally cleared by the network or remote equipment.

Accounting data is reported to the NPM only for X.25 and ISDN protocols. The latter does not apply to a 3746-950, because ISDN (LIC16) can flow only NCP traffic. X.25 accounting applies to a 3746-900 and 3746-950.

For the complete list and details of the accounting data available, refer to the NPM documentation.

Notes:

1. X.25 accounting requires the engineering change D46130I for a 3746-950. ISDN accounting requires the FC 5800.
2. Accounting data is reported on behalf of an X.25 physical line or ISDN D-channel (PU) resource.
3. For ISDN accounting, there are only three types of accounting report for ISDN. The intermediate accounting report does not exist because this type of report would normally be sent:
 - When an accounting counter overflows (unsolicited report). But there is no accounting counter for ISDN, because ISDN charges are not based on data volume.
 - When solicited by the NPM operator. But in this case, the report would be empty (only the time stamp) because there is no counter in the report.
4. Accounting data for X.25 is put within the control vector 81 (CV81).
5. Accounting data for ISDN is put within the control vector 83 (CV83).
6. There is no accounting report when the X.25 virtual circuit flows IP traffic.

Chapter 5. Remote Customer Consoles

PS/2® workstations (or equivalent) can be used to access the service processor remotely. These workstations access the service processor MOSS-E and *CCM User's Guide*, SH11-3081 using:

- Distributed Console Access Facility (DCAF), an IBM licensed program
- Java Console™
- Telnet

They allow the operator at a remote workstation to control the keyboard and mouse input and monitor the display output of the service processor or network node processor. For details on setting up your workstations for DCAF or the Java Console, refer to the *3746 Nways Multiprotocol Controller Model 950: User's Guide*, SA33-0356, or the *3745 Communication Controller All Models, 3746 Nways Multiprotocol Controller Model 900: Console Setup Guide*, SA33-0158.

Using TME 10 Remote Control (DCAF)

With DCAF, the remote PS/2 workstation operates as a DCAF controlling workstation and the service processor as a DCAF target workstation.

Once a connection is established between a workstation and the service processor or network node processor, the remote operator can perform MOSS-E and *CCM User's Guide*, SH11-3081 functions as if seated in front of the service processor.

Remotely controlling a service processor with DCAF blocks the operation of its keyboard and mouse except for the DCAF hot keys.

Notes:

1. Before concluding that the service processor is not working, make sure that it is not under the control of a DCAF remote console. Try the DCAF hot keys (the default keys are **Alt+T**). Refer to the *3746 Nways Multiprotocol Controller Model 950: User's Guide*, the *3745 and 3746 Model 900 Console Setup Guide*, or the DCAF documentation for hot key information.
2. Using DCAF, only one remote workstation can control the service processor at a time.
3. A remote workstation can be configured to have access to more than one service processor.
4. The service processor is shipped preconfigured as a DCAF target workstation.
5. DCAF is a separate product from the 3746 Network Node. Installation of DCAF on a PS/2 (or equivalent) workstation is a customer responsibility.

Using Java Console

Starting with microcode level F12720, you can access the service processor or network node processor to use the remote keyboard, mouse, and display like a DCAF connection, except that:

- In addition to the service processor, using the Java Console, you can connect directly to the network node processor.
- Java Console does not block keyboard and mouse on the service processor and network node processor.

Customer Consoles

Figure 41 shows the types console (PS/2 workstations) connections to the service processor.

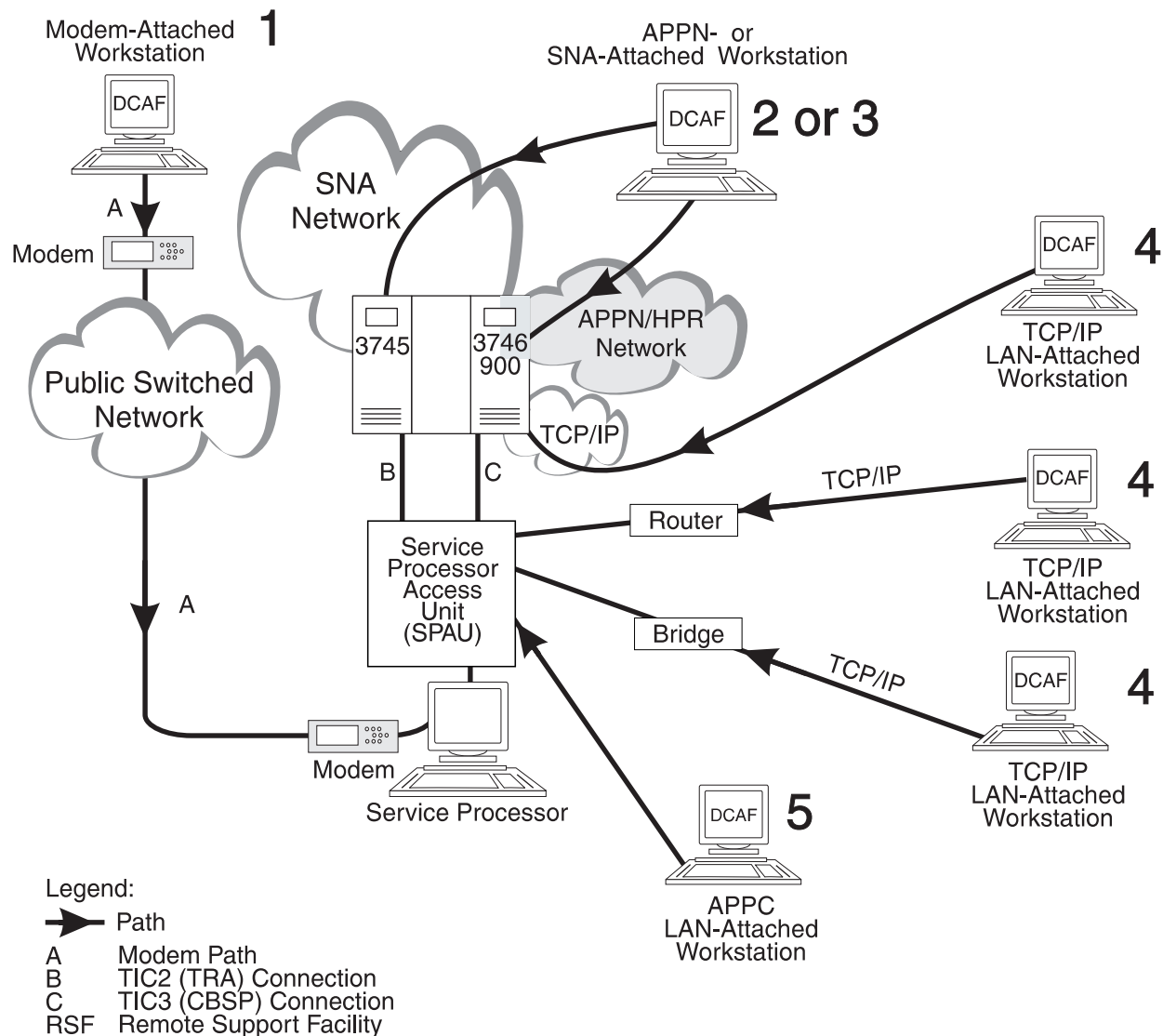


Figure 41. Console Attachments

The types of consoles are:

1. **Modem-attached**, which use the analog switched telephone network to access the service processor via its SDLC port and modem. The service processor modem is also used for RSF and RETAIN connections.

If the APPN/HPR or SNA path for the remote console is not available, a modem attached to the switched network would allow the remote console to access the service processor.

2. **APPN/HPR-attached**, which communicate with the service processor via an SNA LU 6.2 session over your APPN/HPR backbone.
3. **SNA-attached**, which communicate with the service processor via an SNA LU 6.2 session over your SNA backbone.
4. **TCP/IP LAN-attached**, which attach:
 - Directly to the same token-ring LAN as the service processor
 - Indirectly through LAN bridges or routers, with appropriate filtering, to the service processor LAN.

Communications Manager/2 or TCP/IP communications can be used.

Note: Service LAN Problems may disrupt 3746 Network Node operations. See page 35 for important information about token-ring LAN bridges and unplugged cables and stations on the service LAN.

5. **APPC LAN-attached**, which is attached directly to the Service Processor Access Unit (SPAUA) or indirectly through a token-ring LAN bridge.

Sending an alert to NetView via service processor SDLC port⁸ or calling RSF⁹ has a higher priority for the MOSS-E than remote console sessions using the SDLC port of the service processor. This means that should either of these needs arise during a DCAF session, the remote workstation operator using a modem-attached console may be asked to end the remote session to free the service processor SDLC port. See Chapter 6, "Connecting to the IBM Remote Support Facility."

A remote console can be configured for all types of access. This way, a single console at a central control site could be LAN-attached to a local service processor while providing SNA, APPN/HPR, and modem access to other (remote) service processors.

The NetView Graphic Monitor Facility (NGMF) workstation (or any workstation running DCAF) can also use the public switched network to access the service processor if the path through the user network is not available.

⁸ See "Alternate Path" on page 28.

⁹ See Chapter 6, "Connecting to the IBM Remote Support Facility" on page 77.

Minimum Workstation Configuration

An overview of the system requirements for remote workstations is given in this section. For more complete information, refer to *3745 and 3746 Model 900 Console Setup Guide*.

DCAF Consoles

You need the following minimum program levels in your workstations to remotely access the service processor in the:

Communications Manager environment:

- IBM OS/2, Version 2.1 operating system
- Communications Manager/2, Version 1.11 or Communication Server/2
- LAN Adapter Protocol Support (LAPS), Version 2.2 or later.

TCP/IP environment (for LAN-attached consoles):

- IBM OS/2, Version 2.1 operating system
- TCP/IP for OS/2, Version 2.0 and the corrective service diskette (CSD).

Common to both environments:

- TME 10 Remote Control 1.0 (Distributed Console Access Facility, Version 1.3 with CSD 1.3.1)
- TME 10 Remote Control 2.0 (Distributed Console Access Facility, Version 1.3 with CSD 1.3.3).

Notes:

1. Subsequent releases of the above programs can be used unless otherwise stated.
2. Network Transport Services/2 (NTS/2) should be installed for LAN-attached consoles and SNA-attached consoles connected to an SNA network via a LAN.
3. Accessing the service processor via an SNA or APPN/HPR network backbone requires the following:
 - TME 10 Remote Control remote workstations and gateway workstations configured as physical units type 2.1 (PU 2.1). If the TME workstation is downstream from a 3174 control unit, the 3174 must have either of the following support:
 - Configuration Support B plus 8Q0800 Programming Request for Price Quotation (PRPQ).
 - Configuration Support C (APPN feature).
 - When using 3725 Communication Controllers in the network backbone, the controllers must be loaded with NCP V4 R3 and operate under VTAM V3 R2 or later.
 - When using 3720 and 3745 communication controllers in the network backbone, the controllers must be loaded with NCP V5 R2 or later and operate under VTAM V3 R2 or later.

DCAF Hardware Requirements

The remote workstations must be IBM PS/2s (with an 80386 microprocessor or better) or the equivalent. A hard disk of at least 80 MB and at least 10 MB of storage (RAM) is recommended. If you have other applications besides OS/2 and DCAF, you may need more hard disk space and storage. For input/output, the console must have:

- A VGA display such as an IBM 8515 color display or equivalent.
- A mouse.
- A QWERTY keyboard. If this keyboard is not available, then the QWERTY equivalent keys must be used. For example, on an AZERTY keyboard you must use the "q" key when you want to type an "a."

To find the equivalent keys on an IBM non-QWERTY keyboard, refer to your OS/2 documentation for keyboard layouts or codes.

- For a LAN-attached console, an IBM Token-Ring Network Adapter/A operating at 16 Mbps.
- For a modem-attached console, a synchronous modem (compatible with the service processor modem, such as the IBM 7855 or 7857 modem) and a serial port (compatible with the synchronous modem).

To dial the service processor, the modem must either provide dialing capability (like the IBM 7855 and 7857) or be complemented with a telephone set.

For information about the characteristics of the service processor modem, refer to "Controller and Service Processor Integration" in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

- For an APPN/HPR- or SNA-attached console, an IBM Token-Ring Network Adapter or a serial port with a synchronous modem.

Java Console

The controlling workstation may be operated on any of the following platforms:

- OS/2, OS/2 Warp
- Windows® 95, Windows 98, and Windows NT®
- AIX, UNIX®

The minimum program levels required on your workstation to remotely access the service processor is a Web browser (for example, Internet Explorer 4.0, or Netscape 4.0) with Java 1.1 or later enabled.

Telnet Access

To remotely access NNP functions, make sure that your remote workstation runs an operating system that supports TCP/IP, including the Telnet Client program.

Service Processor Parameters

The following MOSS-E parameters should be supplied to the IBM service representative for installation of the service processor and are used when customizing the service processor (see Appendix B, "MOSS-E Service Processor Customization Function" on page 97).

For DCAF

This information about the service processor is necessary for the DCAF controlling workstations to know how to find the service processor in your network. This information should be available at installation time even if you do not plan to use DCAF to remotely access the service processor. Having these parameters already defined in the service processor will save a service representative visit and possible interruption of MOSS-E if you should decide in the future to use DCAF.

For DCAF Consoles Using Communications Manager/2

For CM/2 consoles, supply the following parameters:

Local LU name

The DCAF target running in the service processor must be defined in the service processor as a local LU. One LU name is required for each type of remote console that you plan to use:

- LAN-attached
- APPN/HPR- or SNA/subarea-attached
- Modem-attached

See “Customer Consoles” on page 66.

The LU names must be defined in the MOSS-E and be unique in the APPN/HPR or SNA/subarea network that contains the service processor. Enter the value of this parameter in the “Service Processor Parameters for DCAF using CM/2” worksheet on page 94 for each type of remote console used. Your service representative will use this parameter when configuring your service processor (refer to the “MOSS-E Service Processor Customization Function” appendix in the *3745/3746 Planning Series: Overview, Installation, and Integration*, GA27-4234).

In the DCAF controlling workstations, this LU name is used in the definitions of the partner LU. The LU name value is 1 to 8 characters long and can include:

- Upper case letters (A - Z)
- Digits (0 - 9), but it cannot start with a digit
- Dollar sign (\$)
- At sign (@)
- Number sign (#)

Destination address

This address is used only for SNA and APPN consoles attached. See Figure 41 on page 66, if the alert path to NetView is:

- **Not defined** or through **SNA**:
 - The DCAF SNA can be set for path: 1, 2, 3, or 4
 - The DCAF APPN can be set for path: 4
- Defined through **APPN**:
 - The DCAF SNA can be set for path: 1, 2, 3, or 4 with RSAP different than the TIC3 RSAP defined for the NetView link (refer to the “MOSS-E Service Processor Customization Function” appendix in the *3745/3746 Planning Series: Overview, Installation, and Integration*).

- The DCAF APPN can be set for path: 4 with the same RSAP defined for the NetView link (refer to the “MOSS-E Service Processor Customization Function” appendix in the *3745/3746 Planning Series: Overview, Installation, and Integration*).

Enter the value of this parameter in the “Service Processor Parameters for DCAF using CM/2” worksheet on page 94 for SNA and APPN remote consoles. Your service representative will use this parameter when configuring your service processor (refer to the “MOSS-E Service Processor Customization Function” appendix in the *3745/3746 Planning Series: Overview, Installation, and Integration*). The remaining values in this section have been already defined elsewhere.

Network ID

Identifies the APPN/HPR or SNA network to which the service processor node is connected. Refer to information about the **Network ID** parameter in the “Controller and Service Processor Integration” chapter and the “MOSS-E Service Processor Customization Function” appendix in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

Local node name

This identifies the service processor in the network. Refer to information about the **Local Node Name** parameter in the “Controller and Service Processor Integration” chapter and the “MOSS-E Service Processor Customization Function” appendix in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

Network adapter address

This is the locally administered address (LAA) of the service processor token-ring adapter. Refer to information about the **Network Adapter Address** parameter in the “Controller and Service Processor Integration” chapter and the “MOSS-E Service Processor Customization Function” appendix in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

There are definitions required in VTAM and NCP for SNA/subarea-attached consoles. There are no VTAM or NCP definitions for LAN-attached and modem-attached consoles.

APPN/HPR-attached consoles must not be defined in VTAM or NCP.

For detailed information about DCAF definitions in the CM/2 of the controlling workstation, refer to the *3746 Nways Multiprotocol Controller Model 950: User's Guide* or the *3745 and 3746 Model 900 Console Setup Guide*.

For DCAF Consoles Using TCP/IP

If your workstation running DCAF uses the TCP/IP protocols to communicate with the target service processor over the service LAN, or your IP network, you need to define the IP address and subnet mask of the service processor (defined via the MOSS-E) in your remote consoles.

For detailed information about the IP address of the service processor, refer to the “Controller and Service Processor Integration” chapter and the “MOSS-E Service Processor Customization Function” appendix in the *3745/3746 Planning Series: Overview, Installation, and Integration*.

For detailed information about DCAF definitions in TCP/IP of the controlling workstation, refer to the *3746 Nways Multiprotocol Controller Model 950: User's Guide* or the *3745 and 3746 Model 900 Console Setup Guide*.

For Java Console

The target service processor runs the Java Console server and runs the point-to-point protocol (PPP) server over COM 1 that is connected the asynchronous modem. This allows the remote controlling workstation to reach the service processor via the PPP server using a switched line.

Security for the Java Console includes passwords necessary to:

- Establish the PPP connection. The PPP link uses of Challenge Handshake Authentication Protocol (CHAP).
- To run Java Console.
- To logon to the MOSS-E, if the MOSS-E operator is not currently logged on.

The PPP configuration parameters are:

Accept incoming calls on SP?

Authorizes incoming calls from the remote Java Console workstation.
The default is Yes.

Local phone number

The number of the modem connected to the service processor.

PPP Server IP address

This is the address of the PPP server, which is run by the service processor. This IP address is different from the service processor IP address used for communication over the service LAN. It is reserved for the PPP connection between the remote PPP client controlling workstation and the service processor PPP server.

The PPP server address uses the same subnet network as the service processor service LAN subnet.

PPP Client IP address

This is the IP address assigned by the service processor PPP server to the remote calling workstation during the establishment of the server-workstation link. Any calling workstation is given this IP address by the PPP server.

The PPP client address uses the same subnet network as the service processor service LAN subnet.

DTE Speed

This is the speed of COM 1.

For the 7857 modem, set the DTE speed to 19200.

For the 7858 modem, keep the default value of 115200.

If you have a problem with your PPP connection, try a lower speed.

MRU Size

This is the size of the maximum request/reply unit (MRU) sent and received between the service processor PPP server and the workstation PPP client. The default is 1500.

Customer Password

This is the password you must use when remotely connecting to the service processor via the PPP server using a switched line.

The default password is **IBM3745C**.

IBM service password

This is the password the service representative uses when remotely connecting to the service processor via the PPP server using a switched line.

The default password is **IBM3745I**.

If you use the Java Console, enter these parameter values on page 95.

Remote Access Program Installation and Configuration

The two methods to remotely access the service processor (and network node processor) are mutually exclusive. If you want to use remote access, you must choose either:

- TME 10 Remote Control (DCAF)
- Java Console

Enter your choice on the service representative worksheet on page 95.

TME 10 Remote Control (DCAF) Installation and Configuration

In the *3746 Nways Multiprotocol Controller Model 950: User's Guide* and *3745 and 3746 Model 900 Console Setup Guide*, there are procedures for:

- Installing TME 10 Remote Control and starting a controlling session with a service processor.
- Installing Communications Manager/2 or TCP/IP, or both.
- Configuring customer consoles as one or more of the DCAF controlling workstations:
 - LAN-attached (APPC type)
 - LAN-attached (TCP/IP type)
 - APPN/HPR-attached
 - SNA-attached
 - Modem-attached.

The diskette supplied with the *3746 Nways Multiprotocol Controller Model 950: User's Guide* and *3745 and 3746 Model 900 Console Setup Guide* contains an example for each type of remote console attachment.

DCAF Remote Access Security

To log on to a service processor using a remote DCAF workstation, you must first establish a DCAF link between the remote workstation and the service processor. This link requires certain parameters that are unique to each service processor.

Refer to the "Remote Customer Consoles" chapter in the *3745/3746 Planning Series: Management Planning* for planning information about these parameters.

There are two types of DCAF connection to the service processor:

- Secure
- Non-secure

DCAF Secure

If you select to enable **Allow the target to be a secure target**¹⁰, very secure links¹¹ are setup between the controlling remote workstations and target service processors. Refer to the DCAF documentation for details about using DCAF Secure in your workstations.

Fill out the worksheet “Remote Access Security” on page 95 if you want the IBM service representative to set the service processor as DCAF Secure.

DCAF Non-secure

A non-secure DCAF link only uses a series of passwords to provide access security:

DCAF password

As part of the process of establishing the link between the remote workstation and the service processor, you are asked for the service processor DCAF password before you can have access to the service processor. This password can be unique for each service processor.

Once the DCAF password is entered and the link is established, you can monitor the display of the service processor.

To define or change this password, use the Customize DCAF Target Settings function which is in the MOSS-E Service Processor menu. The two parameters that you have to plan for are:

Enable DCAF password

Yes or no. The default is yes.

Password

1 to 8 alphanumeric characters.

Use the worksheet “Remote Access Security” on page 95 to record these parameters.

Note: There is no factory default password. If no password has been defined, the remote operator just presses **Enter** when asked for the password.

MOSS-E password

To remotely control the service processor, you must enter the MOSS-E password to log onto the MOSS-E. These passwords are explained in the “Controller and Service Processor Integration” chapter of the *3745/3746 Planning Series: Overview, Installation, and Integration*.

¹⁰ Once a service processor is specified as a secure target, the only way to make the service processor non-secure again is to reinstall the MOSS-E microcode.

¹¹ Using encryption, long passwords, and authentication.

Disabling of Incoming Calls

The service processor modem can be set not to accept any incoming calls. This is mainly used to isolate the service processor from remote modem-attached consoles (DCAF controlling and RSF console). The procedure is different depending on the type of modem used:

Integrated modem

Use the MOSS-E Disable incoming calls function and record this parameter on the worksheet "Disable Incoming Calls (for Service Processor)" on page 96.

This type of modem is no longer available from IBM.

External modem

Manually, using the modem buttons. Refer to the manual for your modem for this procedure.

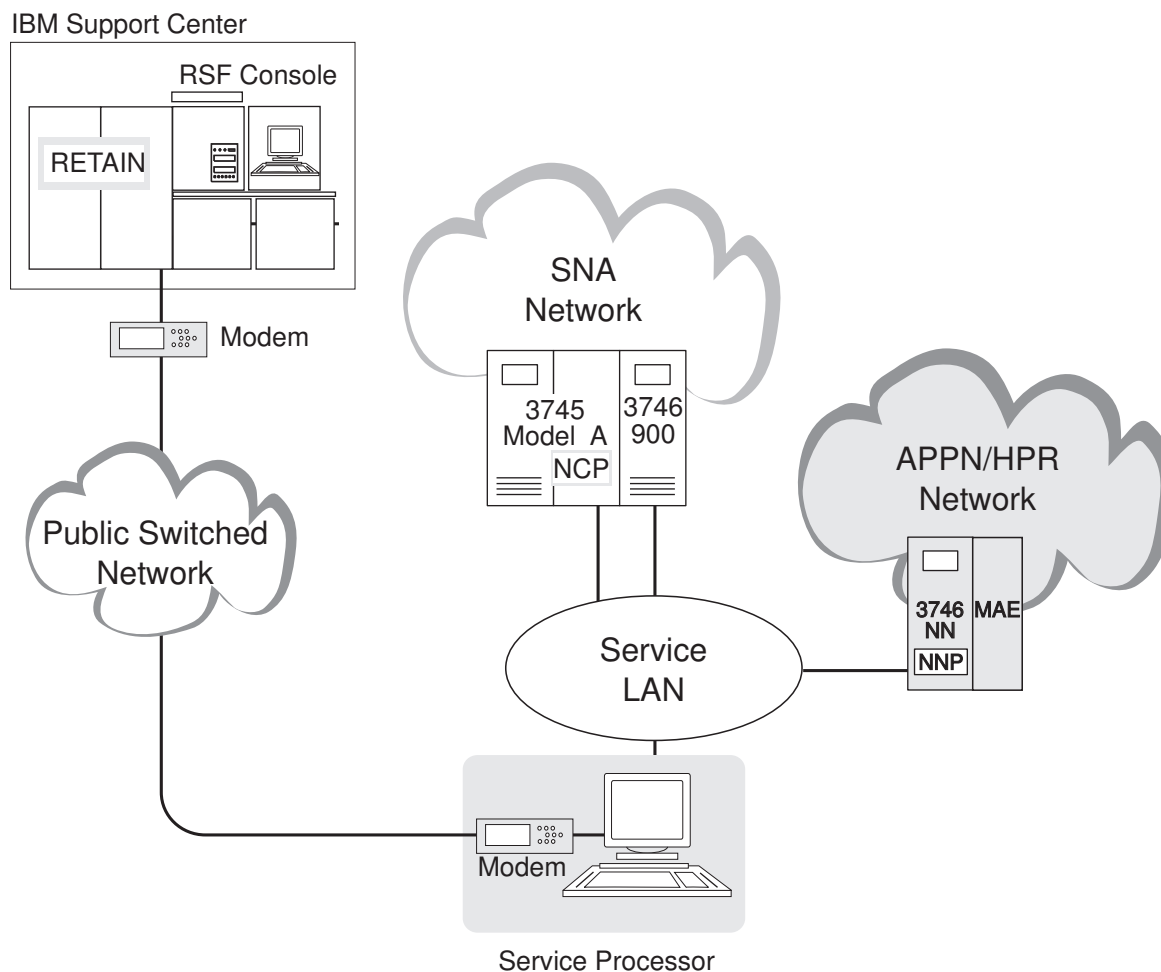
Java Console Installation and Configuration

In the *3746 Nways Multiprotocol Controller Model 950: User's Guide* and *3745 and 3746 Model 900 Console Setup Guide*, there are procedures for:

- Configuring Java Console on the service processor
- Installing Java Console as a program on the remote workstation
- Configuring Java Console on the remote workstation
- Connecting to the service processor and network node processor
- Downloading and uploading files to the service processor

Chapter 6. Connecting to the IBM Remote Support Facility

The 3746 Network Node service support is based on automatic problem reporting to and problem resolution from IBM RETAIN databases via the remote support facility (RSF).



Legend:

3746 NN A 3745/3746-900 with an NNP or a 3746-950
NNP Network Node Processor
MAE Multiaccess Enclosure

Figure 42. RSF Connections

When a critical problem is detected in the 3746 Network Node (3746-900, 3746-950, network node processor, or service processor):

1. The system reference code (SRC) of the problem is recorded in a MOSS-E event log.
2. An alarm is displayed at the service processor.

3. If you are using the IBM RSF and its authorization has been enabled:
 - a. An alert is sent to the NetView program informing the operator that the IBM RSF is being called.
 - b. Problem and error data are automatically reported to RETAIN.
 - c. A second alert is sent to the NetView program informing the NetView operator of the results of the call to RSF.
 - d. If there are any microcode changes, they will be downloaded from RETAIN to the service processor hard disk. It may be possible that the new level of microcode could solve the problem.
 - e. If further investigation is needed, the IBM support center can access the service processor from a remote console. If a hardware failure is suspected, an IBM service representative goes to your site with replacement parts.

The same sequence applies to problems detected in any 3745 or 3746-900 sharing the service processor with the 3746 Network Node. The MOSS event log is used to store information about 3745 problems.

Note: If you have a 3746-900 attached to a 3745 Model A, confirm with your service representative that the 3746-900 has been registered separately on the RETAIN database. If it is not, then a call from such a 3746-900 will fail.

If you have a problem not detected by the MOSS-E, you can manually report the problem to RETAIN using the MOSS-E Report Problem Using Remote Support Facility function in the Problem Management menu

Automatic Microcode Download

The microcode in the controller and the service processor may be updated by downloading microcode via the RSF link from the IBM RETAIN database. The microcode change levels (MCLs) are saved on the service processor hard disk in a temporary file and must be installed and activated before being operational.

If you are an RSF user, it is recommended that you select the automatic MCL download option to periodically receive the latest MCLs. The MOSS-E will automatically define the date and time of the download and will initiate the RSF connection when the day and time occur. The procedure for this option is explained in the *IBM 3745/3746-900 Connection and Integration Guide* or *IBM 3746-950 User's Guide*.

If you do not use RSF, you will (at your request) receive MCLs on an optical disk. This may mean delays in the correct operation of your network, if MCLs are needed to solve microcode problems. Therefore, IBM strongly recommends the use of RSF to minimize any such delays.

Note: Automatic microcode download is available only if the RSF authorization has been enabled.

Parameter Definitions for RSF

The parameters described in this section should be recorded on the RSF Parameter worksheets in on page 96. These parameters are stored in the service processor for use by your IBM service representative.

Customer Information

This information is used by IBM RSF and RETAIN to call you if there is a controller problem.

Company name

The name of your organization, up to 35 characters in length.

Address

The address of your organization. You can use up to three lines of up to 35 characters each.

System location

The physical location of the 3746 Network Node. You can use up to 35 characters in each line and up to two lines.

Contact person

The name of the person to contact at your central site responsible for activating and deactivating systems, and monitoring system problems. Enter up to 30 characters.

The following two telephone numbers can be up to 34 characters long. Include your area code in the telephone number that you specify.

Company telephone number for voice communications

The telephone number that you want IBM to use in normal situations. Use a telephone number other than the service processor modem telephone number.

Company service telephone number for RSF modem communications

The telephone number of the modem attached to the service processor SDLC port.

RSF Authorization

Remote support facility authorization

Enable This is necessary to allow automatic RSF calls by the MOSS-E.

Disable Default value. This prevents the 3746 Network Node from calling RSF; the operator must call IBM to report any problems detected by the 3746 Network Node.

Automatic/Microcode Download Option

This option is only available if the preceding RSF authorization value is set to ENABLE.

Set Automatic Microcode Download Option

- | | |
|------------|---|
| Yes | This allows periodic downloading from RETAIN via the RSF of any new MCLs that might be available from RETAIN. |
| No | Default value. This prevents automatic MCL downloads. |

RSF Modem

The modem attached to the service processor is used primarily to provide the RSF connection to the IBM support center, but it is also used for:

- Remote console access
- Sending alerts to the NetView program (alternate path).

For the characteristics of the modem used for RSF (and RETAIN), refer to “Physical Planning Details” in the *3745/3746 Planning Series: Physical Planning*, GA27-4238.

Chapter 7. 3746 IP Router Management

Managing Your 3746 IP Resources

..

This section describes how to manage the IP resources controlled by the 3746 IP Router. These are the IP functions running on the 3746 native adapters (referred to in this book as the 3746 IP Router). For information about how to manage MAE-controlled IP resources, refer to the MAE IP Router Management” chapter in the *3745/3746 Planning Series: Multiaccess Enclosure Planning*.

The 3746 provides the function of an SNMP agent and can communicate, using IP datagrams, with an SNMP manager such as Tivoli NetView. The Router and Bridge Management (RABM) application (which is available with the IBM Nways Enterprise Manager, program number 5777-AAK) is needed to display the following information:

- Alert and fault management information
- ESCON MIB information

The relationship between these elements is shown in Figure 43. The SNMP agent is supplied as part of the IP routing feature (FC 5033), which runs on the 3746 NNP feature (FC 5022).

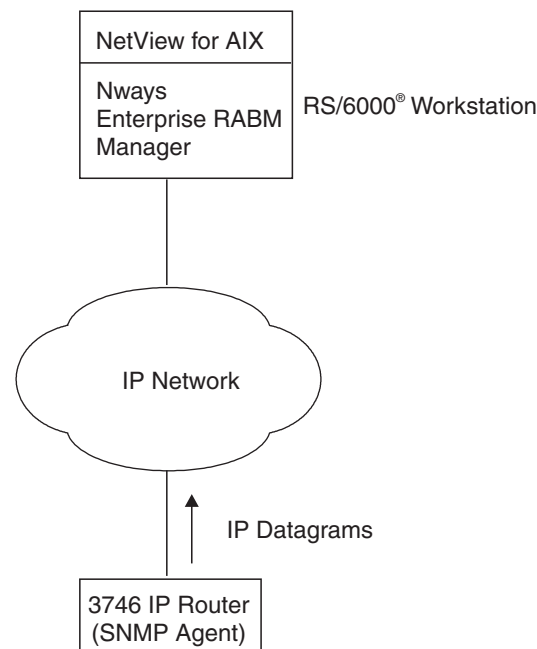


Figure 43. Managing IP Resources with SNMP (3746)

If you want to manage your IP resources centrally from a DCAF station, see “Managing IP Resources via DCAF” on page 87 for further information.

3746-9x0 SNMP Functions

Management Information Base (MIB) Support for 3746 IP Router

A *management information base (MIB)* defines which aspects of network communications are managed by SNMP. These are standard objects, and the following MIBs are supported by the 3746 Network Node:

- MIB 2 (standard MIB, RFC 1213)
- OSPF MIB (standard MIB, RFC 1253)
- Token-ring MIB (standard MIB, RFC 1231)
- Frame-relay MIB (standard MIB, RFC 1315)
- PPP MIB (standard MIB, RFC 1471)
- ESCON MIB (see Appendix C, “ESCON MIB” on page 103)
- X.25 MIB (Standard MIBs, RFC 1381, RFC 1382).

Problems detected in the 3746 Network Node are reported to Tivoli NetView as SNA alerts or CMIP alarms encapsulated in traps. Those traps are received by RABM, which translates them into a local trap to send them to the event desk of Tivoli NetView.

3746-9x0 SNMP Agent Functions

The 3746 IP router provides SNMP V1 agent support. The SNMP **GET**, **GET_NEXT**, and **TRAP** commands are supported. The SNMP **SET** command is not supported. Every SNMP network management station equipped with the appropriate MIB support can retrieve this information.

To configure the 3746 IP SNMP configuration (community names, TRAP receivers, and so on) requires CCM configuration. SNMP configuration via the Telnet configuration interface is not available.

3746-9x0 SNMP Relay

Figure 44 depicts the 3746 IP SNMP implementation. Two main components can be identified:

- SNMP relay code residing on the 3746-9x0
- SNMP agent code residing on the NNP

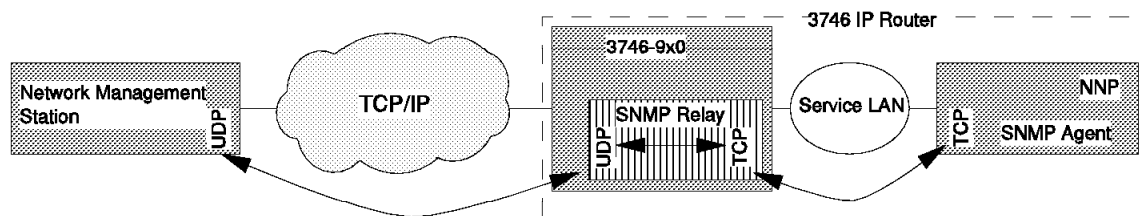


Figure 44. 3746-9x0 IP SNMP Implementation

The *SNMP relay* function on the 3746-9x0 enables an SNMP network management station to send its SNMP requests to any of the IP ports of the 3746-9x0 IP router. By relaying SNMP traffic, rather than forcing network stations to contact the NNP, the location of the SNMP agent is transparent to the network management station.

IP connectivity is required between the network management station and the 3746 IP router. The service LAN is used for the traffic between the 3746-9x0 and the NNP. Both 3746 IP and NNP must be operational to enable SNMP access. Note that the SNMP traffic between 3746-9x0 and network management station uses UDP (port 161), while the SNMP relay function uses TCP transport.

Distributed Agents

The NNP SNMP agent uses the distributed programming interface (DPI V2) described in RFC 1592. To retrieve the information that SNMP network management stations are soliciting, the SNMP agent interfaces with a number of subagents. As most of the SNMP MIB information required is maintained on the 3746-9x0, the subagents themselves interact with processes running on the 3746-9x0 processors.

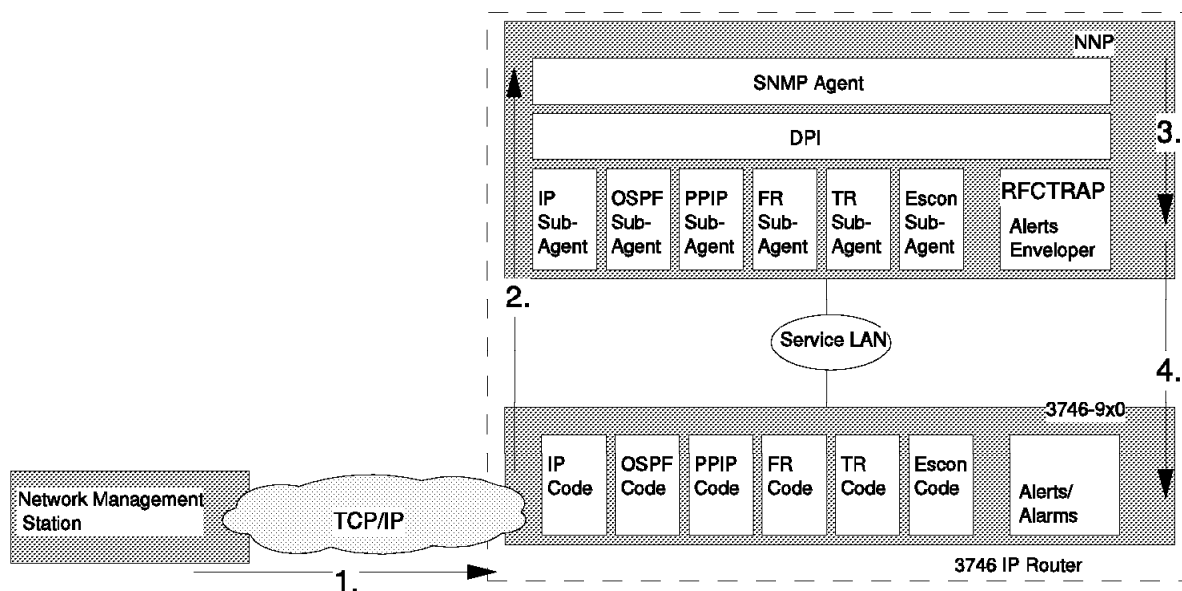


Figure 45. Distributed SNMP Agents

Figure 45 details the subagents concept. Network management stations soliciting SNMP information access (1) the 3746-9x0 which relays (2) the requests to the NNP. The NNP accepts the SNMP request and forwards it (3) to its appropriate subagent. The subagent decodes the ASN.1 format and interfaces (4) with its counterpart in the 3746-9x0.

Note: For performance reasons, the subagents retrieve whole tables that are cached to respond to successive SNMP requests.

The 3746 IP agent supports solicited and unsolicited SNMP traffic. Solicited data is sent in response to an SNMP query received from a network management station. Soliciting data requires read SNMP access on the 3746-9x0 IP routers. Figure 48 on page 86 depicts how the IP addresses and community names are set to enable read access. Unsolicited data is sent after errors have been detected. Unsolicited data is sent as TRAPs.

Figure 49 on page 87 depicts how the IP addresses and community names are set for network management stations that must receive TRAPs.

SNMP Traps

Errors detected by the 3746-9x0 are categorized as external or internal errors. 3746-9x0 external errors are due to protocol violations, cabling problems, and so on. 3746-9x0 internal errors are due to microcode and hardware problems.

Figure 46 on page 85 depicts how the 3746-9x0 IP router generates TRAPs.

- External error

When an external error is detected the 3746-9x0 generates an alert to the NNP control point (CP). The NNP CP decides if the error is IP related and invokes its RFCTRAP code. RFCTRAP generates the SNMP trap and hands it over to the SNMP agent. The latter forwards it to all SNMP network management stations that are configured to receive TRAPs.

- Internal error

When an internal error is detected the 3746-9x0 generates an alert to both NNP and service processor. The processing of the alert sent to the NNP is equivalent to an external error and results in SNMPs being sent. For the alert received by the service processor, configuration information is added before invoking RFCTRAP on the NNP and generating (a second) TRAP.

To handle the TRAPs on your network management station requires IBM's Router and Bridge Manager (RABM) available with the Nways Enterprise Manager. The Alert Manager within RABM is able to understand and convert the CMIP data that is contained within some of the TRAPs. For details on the information contained in the TRAPs, refer to the *3745/3746 Alert Reference Guide*.

Definitions for SNMP Management

The SNMP manager must be reachable on the IP network by the 3746 it manages. A 3746 IP Router may be managed by more than one SNMP manager, and may also report problems to more than one SNMP manager. The SNMP agent in the 3746 IP Router uses a simple authentication to determine which SNMP manager can access its MIB variables. This authentication scheme includes the specification of a *community name* that must be defined on both sides:

- 3746 SNMP agent
- SNMP manager

This relationship is shown in Figure 47 on page 85.

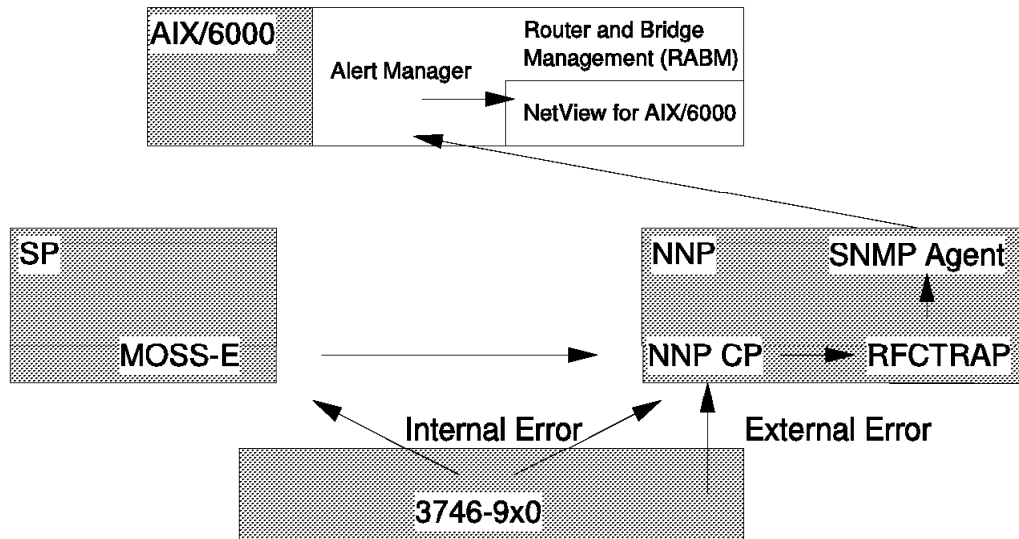


Figure 46. 3746-9x0 IP SNMP TRAPs

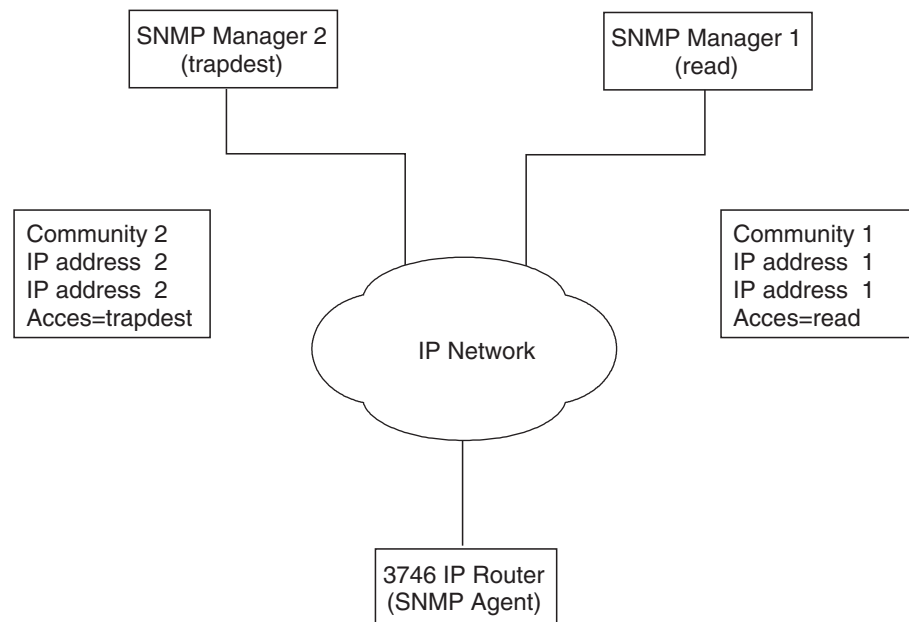


Figure 47. Two SNMP Managers for One 3746 IP Router

You create SNMP management definitions using CCM. Use one SNMP Configuration worksheet for *each* SNMP manager that you define, including:

- IP address of the SNMP manager.
- IP subnet mask of the SNMP manager.
- Community name that will be used. This must be the same community name defined for the SNMP manager.

- Access mode:
 - **Read** - allows SNMP manager to read 3746 MIB variables but not to change them.
 - **Trapdest** - allows SNMP manager to receive problem reports (traps) from the 3746 IP Router.

The CCM SNMP planning worksheet is in the *3745/3746 Planning Series: CCM Planning Worksheets* located on the Web at:

<http://www.ibm.com/networking/did/3746bks.html#Customer>

Note: For information about the access control parameters that you must define in order for SNMP manager to access the SNMP agent, refer to “Internet Protocol (IP) Overview” in the *3745/3746 Planning Series: Protocols Description*.

Setting the SNMP Information from CCM

Figure 48 shows how to allow all network management stations on network 9.24.104, using community name *PUBLIC*, to have read access to the 3746 SNMP IP variables.

The image shows a 'SNMP Configuration' dialog box. It has a title bar with a minus, maximize, and close button. The main area is divided into two sections. The top section is titled 'Configure a Set of SNMP Transport Information'. It contains three radio buttons for 'Access type': 'Read' (selected), 'Write', and 'Trapdest'. To the right of these are three buttons: 'Add', 'Modify', and 'Delete'. Below the radio buttons is a text field for 'Community name' containing 'PUBLIC'. Below that are two text fields: 'Network IP address' containing '9.24.104.0' and 'Network mask' containing '255.255.255.0'. The bottom section is titled 'SNMP Transport Information Sets Already Configured'. It contains a table with the following data:

Access	Community name	Network IP address/mask
Read	PUBLIC	9.24.104.0 255.255.255.0

At the bottom of the dialog box are three buttons: 'OK', 'Cancel', and 'Help'.

Figure 48. SNMP Read Access

Figure 49 shows how to configure the 3746 IP router to send its SNMP traps, using community name *IBM3746*, to the network management station 9.24.104.76.

The image shows a 'SNMP Configuration' dialog box. It has a title bar with a dropdown arrow and the text 'SNMP Configuration'. Inside, there are two main sections. The first section is titled 'Configure a Set of SNMP Transport Information'. It contains three radio buttons for 'Access type': 'Read', 'Write', and 'Trapdest'. The 'Trapdest' button is selected. Below these are three text input fields: 'Community name' (containing 'IBM3746'), 'Network IP address' (containing '9.24.104.76'), and 'Network mask' (containing '255.255.255.255'). To the right of these fields are three buttons: 'Add', 'Modify', and 'Delete'. The second section is titled 'SNMP Transport Information Sets Already Configured'. It contains a table with three columns: 'Access', 'Community name', and 'Network IP address/mask'. The table has two rows: one for 'Read' with 'PUBLIC' and '9.24.104.0 255.255.255.255', and one for 'Trapdest' with 'IBM3746' and '9.24.104.76'. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'. A mouse cursor is pointing at the 'OK' button.

Access	Community name	Network IP address/mask
Read	PUBLIC	9.24.104.0 255.255.255.255
Trapdest	IBM3746	9.24.104.76

Figure 49. SNMP Traps

Managing IP Resources via DCAF

If you want to manage your 3746 Network Node IP resources centrally via the DCAF (see Chapter 5, "Remote Customer Consoles" on page 65), you will need the following:

- An OS/2 station, running DCAF, with an SNA, APPN/HPR, or IP path to the service processor
- An RS/6000®, server running Tivoli NetView, for IP topology display and IP performance reporting, with an IP path to the service LAN of the 3746.

Local IP Resource Management from the Service Processor

You can manage IP network resources by issuing commands from either:

- The CCM IP Specifics menu.

If information is generated as the result of a CCM command being issued, it is displayed by CCM in the CCM IP Results Display window.

- The Telnet console

If you are using Telnet, refer to the publication *3746 Nways Multiprotocol Controller Model 950: User's Guide*.

Supported RFCs

The 3746 IP router supports the following RFCs:

RFC 768	UDP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826/1042	ARP
RFC 919/922	Broadcast including
RFC 925	ARP Subnet Routing
RFC 950	Subnetting
RFC 951/1542	BOOTP Relay Agents
RFC 1009	Internet Gateways
RFC 1027	Proxy ARP(Subnet Routing)
RFC 1058	RIP V1
RFC 1112	IP Multicast
RFC 1122	Requirements for Internet Hosts – Communication Layers
RFC 1144	TCP/IP header compression
RFC 1155	Structure of Management Information
RFC 1157	SNMP v2
RFC 1441 to 1450	SNMP v2
RFC 1452	SNMP v2
RFC 1191	Path MTU Discovery
RFC 1213	MIB-II for TCP/IP-based Internet
RFC 1231	Token-ring MIB
RFC 1253	OSPF V2 MIB
RFC 1315	Frame-relay MIB
RFC 1331/1332	PPP
RFC 1471	PPP IP MIB Support
RFC 1490	Frame relay
RFC 1583/1584	OSPF V2 and Multicast Extensions to OSPF
RFC 1592	DPI
RFC 1654	BGP V4
RFC 1716	Towards Requirements for IP Routers.

CDLC Protocol

For CDLC protocol used by the 3746, the buffer size used in the DEVICE statement must be at least 4 bytes larger than that used in the GATEWAY or BSDROUTINGPARMS statements. For example:

```
; device_name CDLC base_dev_addr r_bufs w_bufs read_size write_size
DEVICE DEVXA8C CDLC 967 200 200 4096 4096
```

```
GATEWAY
;net_number first_hop link packet_size subnet_mask subnet_value
193.9.200 = LINK1 4092 0
128.84 193.9.200.2 LINK1 4092 0.0.255.0 0.0.1.0
```

```
BSDROUTINGPARMS false
; link mtu metric subnet_mask dest_addr
LINK1 4092 0 255.255.255.0 0
LINK2 .....
LINK3 .....
ENDBSDROUTINGPARMS
```

Chapter 8. X.25 Network Management

Fault Management

Network Management Vector Transport (NMVT) alerts are sent to NetView/390 or Tivoli NetView, depending on which control point (NCP, 3746 APPN/HPR, or 3746 IP) activated the X.25 line. If activated by:

- NCP, the alerts are sent to NetView/390 via the NCP.
- 3746 APPN/HPR control point, the alerts are sent to NetView/390 via the APPN control point.
- 3746 IP control point, the alerts are sent to NetView for AIX¹² via the IP control point. In that case the NMVT alerts are enveloped within an SNMP trap.

If the line is shared between multiple control points, each activating control point sends its own alerts to NetView or NetView for AIX³. Therefore, the same problem might be reported by up to three alerts.

Accounting and Performance Monitoring through NPM

A 3746 Network Node can transfer accounting and performance monitoring data to the Network Performance Monitor (NPM) for:

- Data Link level (LAP-B) performance monitoring
- Packet level (PLP) performance monitoring
- Virtual circuit level accounting.

When and only when the X.25 line is activated by the 3746 APPN/HPR control point or NCP, the performance monitoring counters count the overall/traffic, including the IP traffic. When the X.25 line is activated by the 3746 IP control point only, there is no performance monitoring through the NPM.

Performance counters for IP are also reported to NetView for AIX³. See “SNMP.”

There is no virtual circuit accounting for IP traffic, even if the X.25 line has been activated by the APPN/NCP control point or NCP.

SNMP

Configuration parameters and performance counters can be displayed through SNMP, using the MIB Version II (described in RFC 1213). The 3746 IP router implements the SNMP MIBs described in the following RFC:

- RFC 1381 (MIB for LAP-B)
- RFC 1382 (MIB for PLP).

Each MIB element can be only read.

¹² . After NetView for AIX V4R0, the product is named Tivoli NetView.

For more information about SNMP, see “3746-9x0 SNMP Functions” on page 82.

Appendix A. MOSS-E Worksheets for Controller Installation

Complete these sheets and give them to:

- The IBM service representative (the MOSS-E parameters are needed during controller installation)
- The person doing additional controller configuration using the *IBM 3745 Communication Controller All Models, IBM 3746 Nways Multiprotocol Controller Connection and Integration Guide*.

When applicable, default parameter values are included (in parentheses) in the tables of this appendix.

Parameter Definitions for Reporting Alerts to NetView

Network Node Processor Alerts

The following parameters are discussed in on page 28.

Network identifier	(SYSTSTAP)
Control point name	

MOSS-E Alerts: Mainstream Path Definition

LAN destination address parameters are discussed on pages LAN destination address on page 29 and LAN destination address on page 31.

APPN/HPR Network

LAN destination address	
-------------------------	--

SNA/Subarea Network

LAN destination address	
-------------------------	--

MOSS-E Alerts: Alternate Path Definition

The following parameter is discussed on page 33.

Telephone number for alert reporting on the switched SDLC link	
--	--

Generate MOSS-E Alerts

The following parameter is discussed on page 34.

Problem management	(Generate alerts)
--------------------	-------------------

Performance Management CM/2 Parameters (NPM)

The following parameters are discussed on page 59.

NPM netid	
PU name for CM/2	
NPA LU name	

Service Processor Parameters for DCAF using CM/2

These parameters are defined in “For DCAF Consoles Using Communications Manager/2” on page 70.

For LAN-Attached Consoles

LU name	(DCAFLAN)
---------	-----------

For SNA-Attached Consoles

LU name	(DCAFSNA)
Destination address	(400000502080)

For APPN/HPR-Attached Consoles

LU name	(DCAFAPPN)
Destination address	(400000502080)

For IP-Attached Consoles

Service Processor IP Address	(192.9.200.1)
------------------------------	---------------

For Modem-Attached Consoles

LU name	(DCAFSDLC)
---------	------------

Service Processor Parameters for Java Console

The following parameters are discussed on page 72.

Access incoming calls on SP?	(Yes)
Local phone number	

Table 4. For the PPP Server (Service Processor)

IP address	(192.9.200.7)
Subnet mask	(255.255.255.240)

Table 5. For the PPP Client (Remote Station)

IP address	(192.9.200.8)
Subnet mask	(255.255.255.240)

DTE Speed	(115200)
MRU Size	(1500)
Customer password	(IBM3745C)
IBM service password	(IBM3745I)

Choice of Remote Access

This parameter is discussed on page 73.

Table 6. Either DCAF or Java Console

Enable DCAF Link/Operations	
Enable Console Link/Operations for Java	

Remote Access Security

The following parameters are discussed in “DCAF Remote Access Security” on page 73.

DCAF Security Choice

Allow the target to be a secure target	(No)
--	------

DCAF Non-Secure Remote Logon Password

Enable password	(Yes)
Password	

Disable Incoming Calls (to Service Processor)

The following parameter is discussed on page 75.

Enable/Disable Service Processor Incoming Calls	(Enable)
---	----------

Parameter Definitions for RSF

The following parameters are discussed in “Parameter Definitions for RSF” on page 79.

Customer Information

Company Name	
Address	
System location	
Contact person	
Company telephone number for voice communications	
Company telephone number for modem communications	

Remote Support Facility Authorization

The following parameters are discussed in “For Java Console” on page 72.

Enable/Disable Remote Support Facility	(Disable)
--	-----------

Set Automatic Microcode Download Option

Yes/No	(No)
--------	------

Appendix B. MOSS-E Service Processor Customization Function

When installing your service processor, the service representative will use the service processor customization function to setup your service processor according to your configuration. This function can also be used by the customer to add or modify existing parameters.

To access the function:

1. On the MOSS-E view primary window, double-click the **Service Processor** object icon.
2. Click **Configuration Management**.
3. Double-click **SP customization**.
4. If it is the first time that you invoke SP Customization, all the items are selected. If you want to select only one item, click on the corresponding check box to deselect the items that you do not want to modify the parameters, then click **Next>>** and follow the prompts.

The MOSS-E panels in Figure 50 to Figure 61 on page 102 appear during service processor customization.

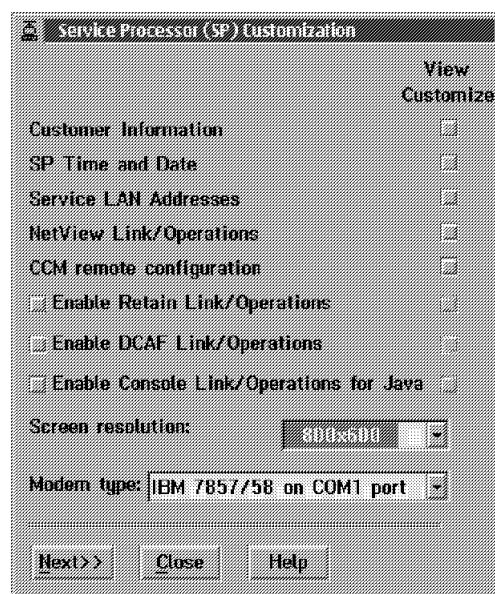
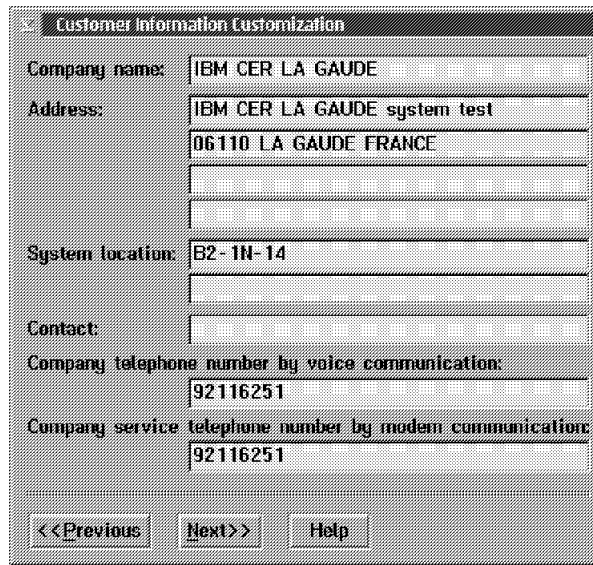


Figure 50. Service Processor Customization



Customer Information Customization

Company name: IBM CER LA GAUDE

Address: IBM CER LA GAUDE system test
06110 LA GAUDE FRANCE

System location: B2-1N-14

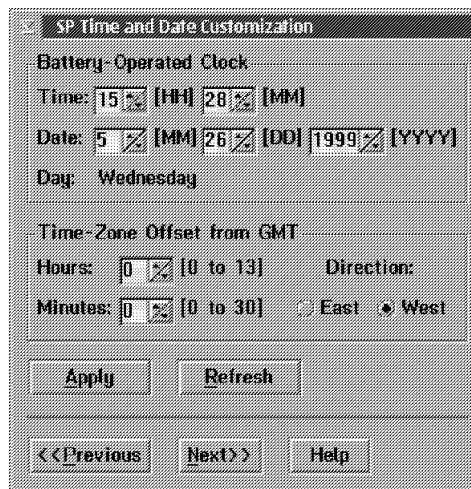
Contact:

Company telephone number by voice communication: 92116251

Company service telephone number by modem communication: 92116251

<<Previous Next>> Help

Figure 51. Customer Information Customization



SP Time and Date Customization

Battery-Operated Clock

Time: 15 [HH] 28 [MM]

Date: 5 [MM] 26 [DD] 1999 [YYYY]

Day: Wednesday

Time-Zone Offset from GMT

Hours: 0 [0 to 13] Direction:

Minutes: 0 [0 to 30] ☐ East ☒ West

Apply Refresh

<<Previous Next>> Help

Figure 52. SP Time and Date Customization

	IP address	Subnet mask	Hostname	UAA/LAA
Service Processor:	9.100.77.61	255.255.255.0	SP11111	400000781111
NNP-A:	9.100.77.62	255.255.255.0	CA134567	
NNP-B:	not installed			
TIC3 2080:	9.100.77.63	255.255.255.0		
SP default router:	9.100.77.1			
NAE:	not installed			

LAN Manager
Do you have a LAN manager? ☐ Yes ☒ No C&SM LAN ID: MOSSE

<<Previous Next>> Help

Figure 53. Service LAN Addresses

NetView Link(s)/Reporting Customization

☐ Generate alerts ☐ Enable Netview RUNCMD

NetView Link(s)
Link(s) through? ☐ SNA ☒ APPN
How many? ☐ 1 ☒ 2
Link type? ☒ LAN ☐ SDLC

Machine Identification
Machine type Model Serial number
3745 17A 12 34567

Local Node Characteristics
Network ID Local node name
SYSTSTAP MOSSNMVT

LAN Link
TIC2 or TIC3 LAA: 400000782080 hex
TIC3 RSAP: 08 hexadecimal [04-9C]
Customize 3270 sessions? ☒ Yes ☐ No

Switched SDLC Link Telephone Number
0492116251

<<Previous Next>> Help

Figure 54. NetView Link(s)/Reporting Customization

Token-Ring 3270 Session Customization

Host code page: 297 France

LU local/NAU address: 3 numerical [3-255]

Long session/LU name: B

Number of sessions: 4 numerical [1-4]

<<Previous Next>> Help

Figure 55. Token-Ring 3270 Session Customization

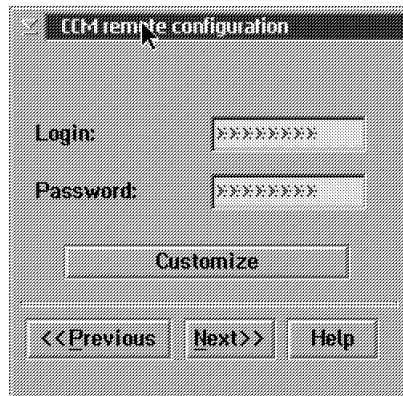


Figure 56. CCM Remote Configuration



Figure 57. Manage Passwords

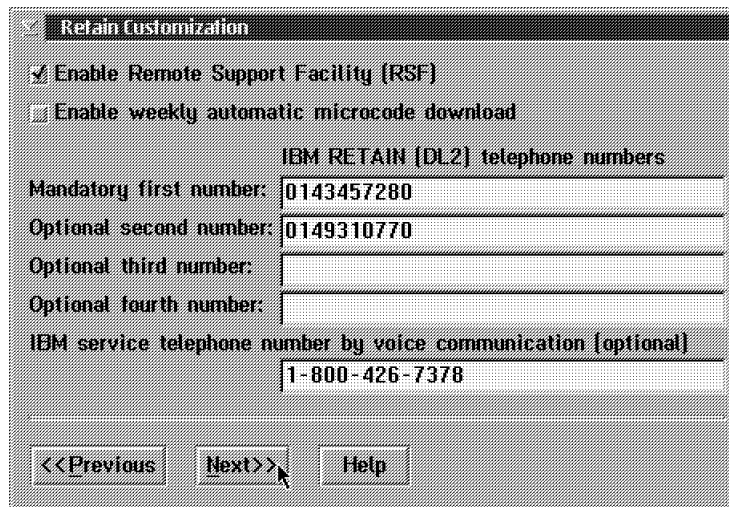


Figure 58. Retain Customization

DCAF Customization

Attached Consoles

	LU name	Destination address (hexadecimal)	RSAP (hex [04-9C])
<input type="checkbox"/> SNA	DCAFSNA	400000782000	04
<input type="checkbox"/> APPN	DCAFAPPN	400000782000	00
<input type="checkbox"/> LAN	DCAFLAN		

SDLC Attached Console

☐ SDLC DCAFS DLC

Accept any incoming calls on SP? ☒ Yes ☐ No

Local phone number: 1111111111

<<Previous Next>> Help

Figure 59. DCAF Customization

Point-to-Point Protocol Configuration

PPP Server Customization

Accept any incoming calls on SP? ☒ Yes ☐ No

Local phone number: 1111111111

	IP Address	Subnet mask	Hostname
PPP Server	9.100.77.67	255.255.255.0	SSP11111
PPP Client	9.100.77.68	255.255.255.0	

DTE Speed: 115200 MRU Size: 1500

PPP Client Login Customization

	Customer	IBM Service
User Name	CSP11111	ISP11111
Password	XXXXXXXX	XXXXXXXX

View/Change Passwords

<<Previous Next>> Help

Figure 60. Point-to-Point Protocol Configuration

	Login	Password
SP:	RENAULT	
NNP-A:	PEUGEOT	
NNP-B:		

View/Change Passwords

<<Previous Next>> Help

Figure 61. Console Configuration for Java

Appendix C. ESCON MIB

```

IBMESCON-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, enterprises, Counter32, OBJECT-TYPE
        FROM SNMPv2-SMI
    OBJECT-GROUP, MODULE-COMPLIANCE
        FROM SNMPv2-CONF
    ifIndex
        FROM RFC1213-MIB;

ibmESCON MODULE-IDENTITY
    LAST-UPDATED "9604150000Z"
    ORGANIZATION "IBM"
    CONTACT-INFO "Bob Moore (remoore @ ralvm6)
        IBM Corporation
        800 Park Offices Drive
        CNMA/664
        P.O. Box 12195
        Research Triangle Park, NC 27709, USA
        Tel: 1 919 254 4436
        E-mail: remoore@ralvm6.vnet.ibm.com

        John Rooney (rooney @ yktvmv)

        Valerie Zoccola (zoccolav @ lgeprofs)"

DESCRIPTION
    "MIB for managing activity on an ESCON channel from its
    secondary end.

    'ESCON' is a trademark of the IBM Corporation."

    ::= { ibmArchitecture 17 }

ibm OBJECT IDENTIFIER ::= { enterprises 2 }
ibmArchitecture OBJECT IDENTIFIER ::= { ibm 5 }

esconPortData OBJECT IDENTIFIER ::= { ibmESCON 1 }
esconLinkData OBJECT IDENTIFIER ::= { ibmESCON 2 }
esconStationData OBJECT IDENTIFIER ::= { ibmESCON 3 }
esconConformance OBJECT IDENTIFIER ::= { ibmESCON 4 }

-- This MIB contains three tables, for managing an ESCON configuration
-- as shown here:
--
--
-- Host 1                                     Host 2
-- -----
-- .d-1..d-y          d1...d-y.             .           .
-- .                   .                     .           .
-- .  PN-1      ...   PN-xx .               .           .
-- -----
-- HLA-1 .                                     HLA-2 .
-- .                                           .
--
-- -----
-- .                   ESCON Director         .
-- .                                           .
-- -----
-- CULA-1.                                     CULA-2.
-- .                                           .
--
-- -----
-- .           -----           .           .
-- .   .   ESCON   .           .   ESCON   .   .
-- .   .   port 1 .           .   port 2   .   .
-- .           -----           .           .
-- .                                           .
-- .                                           .
-- .                   Device supporting this MIB .

```

```

--
-- - ESCON port table represents an ESCON physical port. As shown,
--   a device may support more than one ESCON port. This table
--   is indexed by ifIndex from MIB-II. The entry for this port in
--   ifTable uses the ifType value 73 (ESCON).
--
--   Note that the Control Unit Link Address (CULA), identifying the
--   port on the ESCON Director to which an ESCON port is optically
--   connected, is a non-index object in this table.
--
-- - ESCON link table represents a link between an ESCON device
--   and a "logical host" within an actual host. This table has
--   a three-part index:
--
--     - ifIndex from MIB-II, identifying the ESCON port
--       supporting the link
--     - esconLinkHostLinkAddress (HLA), identifying the actual
--       host for the link.
--     - esconLinkPartitionNumber (PN), identifying the "logical
--       host" for the link, within the actual host identified
--       by esconLinkHostLinkAddress.
--
-- - ESCON station table represents a link station in an ESCON
--   device. This table has a four-part index:
--
--     - ifIndex from MIB-II, identifying the ESCON port
--       supporting the link
--     - esconStationHostLinkAddress (HLA), identifying the actual
--       host for the link.
--     - esconStationPartitionNumber (PN), identifying the "logical
--       host" for the link, within the actual host identified
--       by esconLinkHostLinkAddress.
--     - esconStationDeviceAddress (d-n in the figure), identifying
--       the device address by which the host knows the station.
--
-- *****
-- IBM ESCON port table
-- *****

esconPortTable OBJECT-TYPE
    SYNTAX SEQUENCE OF EsconPortEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table of objects that describe an ESCON channel port."

    ::= { esconPortData 1 }

esconPortEntry OBJECT-TYPE
    SYNTAX EsconPortEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table of objects that describe an ESCON channel port. This
        table is indexed by ifIndex from MIB-II."

    INDEX { ifIndex }

    ::= { esconPortTable 1 }

EsconPortEntry ::= SEQUENCE
{
    esconPortControlUnitLinkAddress OCTET STRING,
    esconPortInFiberStatus INTEGER,
    esconPortOutFiberStatus INTEGER
}

esconPortControlUnitLinkAddress OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE(2))
    MAX-ACCESS read-only
    STATUS current

```



```

DESCRIPTION
    "This address identifies the ESCON Director port to which the
    optical fiber from the ESCON device is attached."

::= { esconPortEntry 1 }

esconPortInFiberStatus OBJECT-TYPE
    SYNTAX INTEGER {
        inLoff(1),
        inOls(2),
        inIdle(3),
        inUnknown(4)
    }
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Status of the fiber into this device from the host:

        inLoff      = the light is off on the fiber into
                     this device from the host
        inOls       = the fiber into this device from the
                     host is in an intermediate state between
                     light-off and light-on
        inIdle      = the fiber into this device from the
                     host is in the light-on state, and is
                     ready to transfer data from the host to
                     this device
        inUnknown   = the agent cannot determine the status of
                     the fiber into this device from the host"

::= { esconPortEntry 2 }

esconPortOutFiberStatus OBJECT-TYPE
    SYNTAX INTEGER {
        outDisableReq(1),
        outDisableForced(2),
        outLoffForced(3),
        outOls(4),
        outOlsForced(5),
        outEnable(6),
        outError(7)
    }
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Status of the fiber out of this device to the host:

        outDisableReq  = out disable obtained; the fiber
                       out of this device into the host
                       is not in the light-on state
        outDisableForced = out ESCON emits OLS; the fiber
                       out of this device into the host
                       is not in the light-on state
        outLoffForced   = out ESCON forced light-off; the fiber
                       out of this device into the host
                       is not in the light-on state
        outOls          = the fiber out of this device into the
                       host is in an intermediate state
                       between light-off and light-on
        outOlsforced    = out ESCON forced OLS; the fiber
                       out of this device into the host
                       is not in the light-on state
        outEnable       = the fiber out of this device into the
                       host is in the light-on state, and is
                       ready to transfer data from this
                       device to the host
        outError        = the status of the fiber out of this
                       device to the host is none of those
                       listed above. This is a state that
                       should not occur"

::= { esconPortEntry 3 }

```

```

-- *****
-- IBM ESCON link table
-- *****

esconLinkTable OBJECT-TYPE
    SYNTAX SEQUENCE OF EsconLinkEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table of objects that describe an ESCON channel link."

    ::= { esconLinkData 1 }

esconLinkEntry OBJECT-TYPE
    SYNTAX EsconLinkEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table of objects that describe an ESCON channel link. This
        table is indexed by ifIndex from MIB-II, by host link address,
        and by (host) partition number."

    INDEX { ifIndex,
            esconLinkHostLinkAddress,
            esconLinkPartitionNumber }

    ::= { esconLinkTable 1 }

EsconLinkEntry ::= SEQUENCE
{
    esconLinkHostLinkAddress OCTET STRING,
    esconLinkPartitionNumber OCTET STRING,
    esconLinkStatus INTEGER
}

esconLinkHostLinkAddress OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE(1))
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "This address identifies the ESCON Director port to which the
        optical fiber between the ESCON Director and the host is
        attached."

    ::= { esconLinkEntry 1 }

esconLinkPartitionNumber OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE(1))
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "A number identifying a logical host within an actual host."

    ::= { esconLinkEntry 2 }

esconLinkStatus OBJECT-TYPE
    SYNTAX INTEGER {
        hlpNotEstab(1),
        hlpEstab(2),
        hlpError(3)
    }
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Gives the status of the link:

        hlpNotEstab = Host Logical Path not established
        hlpEstab = Host Logical Path established
        hlpError = Host Logical Path error"

```

```

 ::= { esconLinkEntry 3 }

-- *****
-- IBM ESCON station table
-- *****

esconStationTable OBJECT-TYPE
    SYNTAX SEQUENCE OF EsconStationEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table of objects that describe an ESCON channel station."

    ::= { esconStationData 1 }

esconStationEntry OBJECT-TYPE
    SYNTAX EsconStationEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table of objects that describe an ESCON channel station. This
        table is indexed by ifIndex from MIB-II, by host link address,
        by (host) partition number, and by ESCON device address."

    INDEX { ifIndex,
            esconStationHostLinkAddress,
            esconStationPartitionNumber,
            esconStationDeviceAddress }

    ::= { esconStationTable 1 }

EsconStationEntry ::= SEQUENCE
{
    esconStationHostLinkAddress OCTET STRING,
    esconStationPartitionNumber OCTET STRING,
    esconStationDeviceAddress OCTET STRING,
    esconStationState INTEGER,
    esconStationAttentionDelay INTEGER,
    esconStationAttentionTimeOut INTEGER,
    esconStationMaxBfru INTEGER,
    esconStationUnitSize INTEGER,
    esconStationMaxMsgSizeReceived INTEGER,
    esconStationMaxMsgSizeSent INTEGER,
    esconStationDataPacketsOkReceived Counter32,
    esconStationDataPacketsKoReceived Counter32,
    esconStationDataPacketsSent Counter32,
    esconStationTotalFramesSent Counter32,
    esconStationDataPacketsRetransmitted Counter32,
    esconStationPositiveAckDataPackets Counter32,
    esconStationSecondChanceAttentions Counter32,
    esconStationCommandsRetried Counter32
}

esconStationHostLinkAddress OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE(1))
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "This address identifies the ESCON Director port to which the
        optical fiber between the ESCON Director and the host is
        attached."

    ::= { esconStationEntry 1 }

esconStationPartitionNumber OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE(1))
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "A number identifying a logical host within an actual host."

```

```

        ::= { esconStationEntry 2 }

esconStationDeviceAddress OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE(1))
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "A unique hexadecimal number allocated to each station on the
        same host link."

        ::= { esconStationEntry 3 }

esconStationState OBJECT-TYPE
    SYNTAX INTEGER {
        idle(1),
        cpDefined(2),
        cpReset (3),
        cpActive(4),
        cpDelete(5),
        cpAbend(6),
        cldpWait(7),
        cldpDefined(8),
        cldpError(9),
        cldpLoad(10),
        cldpDump(11),
        deletePending(12),
        deleted(13),
        cpXidExpected(14)
    }
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The current state of the station."

        ::= { esconStationEntry 4 }

esconStationAttentionDelay OBJECT-TYPE
    SYNTAX INTEGER (0 .. 420)
    UNITS "seconds"
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Specifies the amount of time in seconds that elapses
        from the receipt of a packet at an ESCON station (when
        no other packets are queued) before that station sends
        buffered data to the Host.

        An update to this object takes effect the next time the station
        establishes communications with the host."

        ::= { esconStationEntry 5 }

esconStationAttentionTimeOut OBJECT-TYPE
    SYNTAX INTEGER (10 .. 840)
    UNITS "seconds"
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Specifies the amount of time in seconds that the station is to
        wait for a response to an attention signal it sent to the host
        before initiating channel disconnect.

        An update to this object takes effect the next time the station
        establishes communications with the host."

        ::= { esconStationEntry 6 }

esconStationMaxBfru OBJECT-TYPE
    SYNTAX INTEGER (1 .. 65535)
    MAX-ACCESS read-only
    STATUS current

```

```

DESCRIPTION
    "Number of buffers in the host buffer pool for receiving data
    from this station."

 ::= { esconStationEntry 7 }

esconStationUnitSize OBJECT-TYPE
    SYNTAX INTEGER (64 .. 4000)
    UNITS "bytes"
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Maximum size of a buffer, in bytes, that the host can receive
        from this station."

 ::= { esconStationEntry 8 }

esconStationMaxMsgSizeReceived OBJECT-TYPE
    SYNTAX INTEGER (0 .. 65535)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "The maximum length of a message that can be received on this
        station.

        An update to this object takes effect the next time the station
        establishes communications with the host."

 ::= { esconStationEntry 9 }

esconStationMaxMsgSizeSent OBJECT-TYPE
    SYNTAX INTEGER (0 .. 65535)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "The maximum length of a message that can be sent from this
        station to the host.

        An update to this object takes effect the next time the station
        establishes communications with the host."

 ::= { esconStationEntry 10 }

esconStationDataPacketsOkReceived OBJECT-TYPE
    SYNTAX Counter32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of data packets received from the host by this
        station without Data Check."

 ::= { esconStationEntry 11 }

esconStationDataPacketsKoReceived OBJECT-TYPE
    SYNTAX Counter32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of data packets received from the host by this station
        with Data Check."

 ::= { esconStationEntry 12 }

esconStationDataPacketsSent OBJECT-TYPE
    SYNTAX Counter32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of data packets sent to the host by this station."

 ::= { esconStationEntry 13 }

```

```

esconStationTotalFramesSent OBJECT-TYPE
    SYNTAX Counter32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of data packets and control packets sent to the host
        by this station."

    ::= { esconStationEntry 14 }

esconStationDataPacketsRetransmitted OBJECT-TYPE
    SYNTAX Counter32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of data packets retransmitted by this station"

    ::= { esconStationEntry 15 }

esconStationPositiveAckDataPackets OBJECT-TYPE
    SYNTAX Counter32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of data packets sent by this station to the host that
        the host has positively acknowledged. When the host sends a
        positive acknowledgement for a group of n data packets, this
        counter is incremented by n."

    ::= { esconStationEntry 16 }

esconStationSecondChanceAttentions OBJECT-TYPE
    SYNTAX Counter32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of times this station has sent a Second Chance
        Attention signal to the host."

    ::= { esconStationEntry 17 }

esconStationCommandsRetried OBJECT-TYPE
    SYNTAX Counter32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of times a command has been retried on this
        station"

    ::= { esconStationEntry 18 }

-- *****
-- IBM ESCON conformance
-- *****

esconMibCompliances OBJECT IDENTIFIER ::= {esconConformance 1 }

esconMibGroups OBJECT IDENTIFIER ::= {esconConformance 2 }

esconPortGroup OBJECT-GROUP
    OBJECTS {
        esconPortControlUnitLinkAddress,
        esconPortInFiberStatus,
        esconPortOutFiberStatus
    }
    STATUS current
    DESCRIPTION
        "Objects that describe an ESCON channel port."

    ::= { esconMibGroups 1 }

```

```

esconLinkGroup OBJECT-GROUP
    OBJECTS {
        esconLinkStatus
    }
    STATUS current
    DESCRIPTION
        "Objects that describe an ESCON channel link."

    ::= { esconMibGroups 2 }

esconStationGroup OBJECT-GROUP
    OBJECTS {
        esconStationState,
        esconStationAttentionDelay,
        esconStationAttentionTimeOut,
        esconStationMaxBfru,
        esconStationUnitSize,
        esconStationMaxMsgSizeReceived,
        esconStationMaxMsgSizeSent,
        esconStationDataPacketsOkReceived,
        esconStationDataPacketsKoReceived,
        esconStationDataPacketsSent,
        esconStationTotalFramesSent,
        esconStationDataPacketsRetransmitted,
        esconStationPositiveAckDataPackets,
        esconStationSecondChanceAttentions,
        esconStationCommandsRetried
    }
    STATUS current
    DESCRIPTION
        "Objects that describe an ESCON channel station."

    ::= { esconMibGroups 3 }

esconMibCompliance MODULE-COMPLIANCE
    STATUS current
    DESCRIPTION
        "The compliance statement for the SNMPv2 entities that
        implement the IBM ESCON MIB."

    MODULE -- this module
        MANDATORY-GROUPS {
            esconPortGroup,
            esconLinkGroup,
            esconStationGroup
        }

        OBJECT esconStationAttentionDelay
        MIN-ACCESS read-only
        DESCRIPTION
            "Write access is not required."

        OBJECT esconStationAttentionTimeOut
        MIN-ACCESS read-only
        DESCRIPTION
            "Write access is not required."

        OBJECT esconStationMaxMsgSizeReceived
        MIN-ACCESS read-only
        DESCRIPTION
            "Write access is not required."

        OBJECT esconStationMaxMsgSizeSent
        MIN-ACCESS read-only
        DESCRIPTION
            "Write access is not required."

    ::= { esconMibCompliances 1 }

END

```


List of Abbreviations

AB	area border	CLIST	command list
ACF	advanced communications function	CLA	communication line adapter
ACF/VTAM	advanced communications function for the virtual telecommunications access method	CLP	communication line processor
ANR	automatic network routing	CM	communications manager
APPN	advanced peer-to-peer networking	CNN	composite network node
ARB	adaptive rate-based flow/congestion control	CNM	communication network management
ARC	active remote connector	COS	cost of service
ARP	address resolution protocol	CP	control point
AS	autonomous system	CR	communications rate
ASB	autonomous system border	CSU	customer service unit
ASE	autonomous system external	DCAF	distributed console access facility
ASCII	american national standard code for information interchange	DCE	data circuit-terminating equipment
AUTO	automatic	DDS	digital data service
BAN	boundary access node	DE	discard eligibility
BECN	backward explicit congestion notification	DLC	data link control
BER	box event record	DLCI	data link connection identifier
BGP	border gateway protocol	DLSw	data link switching
BOOTP	bootstrap protocol	DLUR	dependent LU requester
bps	bits per second	DLUS	dependent LU server
BRS	bandwidth reservation system	DMUX	double multiplex circuit
BSC	binary synchronous communication	DSU	data service unit
C&SM	communications and system management	DTE	data terminal equipment
CBSP	control bus and service processor	DX	duplex
CCITT	comité consultative international télégraphique et téléphonique The international telegraph and telephone consultative committee	EBCDIC	extended binary-coded decimal interchange code
CCU	central control unit	EBN	extended border node
CD	carrier detector	EC	engineering change
CDF-E	configuration data file - extended	EMIF	ESCON multiple image facility
CE	customer engineer	EN	end node
CF3745	3745 and 3746 configurator and performance model	EP	emulation program
CHPID	channel path id	EPO	emergency power OFF
CIDR	classless inter-domain routing	ESCA	ESCON channel adapter
CIR	committed information rate	ESCC	ESCON channel coupler
		ESCD	ESCON Director
		ESCON	Enterprise Systems CONnection
		ESCP	ESCON processor
		FC	feature code
		FDX	full duplex
		FECN	forward explicit congestion notification

FRAD	frame-relay access device	LQ	line quality
FRFH	frame-relay frame handler	LU	logical unit
FRSE	frame-relay switching equipment	LSS	low-speed scanner
FRTE	frame-relay terminating equipment	MAC	medium access control
HCD	hardware configuration definition	MAU	medium attachment unit
HDX	half duplex	MB	megabyte (processor storage) 1MB = 2 ²⁰ bytes (1 048 576 bytes)
HI	high	Mbps	megabits per second (speed or communication volume per second) 1 Mbps = 1 000 000 (one million) bits per second
HLA	host link address	MCL	microcode change level
HONE	hands-on network environment	MES	miscellaneous equipment specification
HPR	high performance routing	MIB	management information base
HSS	high-speed scanner	MIH	missing interrupt handler
ICMP	internet control message protocol	MLC	machine level control
IML	initial microcode load	MLTG	multi-link transmission group
INN	intermediate network node or IBM information network	MOSS-E	maintenance and operator subsystem - extended
IOCP	Input/Output Configuration Program	MTP	multipoint
IP	internet, or internetwork, protocol	MUX	multiplex circuit
IPL	initial program load	MVS	multiple virtual storage
IPR	installation planning representative	NAU	network addressable unit
ITU-T	international telecommunications union - telecommunications (ex-CCITT)	NMBA	nonbroadcast multiaccess
KB	kilobyte (processor storage) 1KB = 2 ¹⁰ bytes (1 024 bytes)	NCP	Network Control Program
kbps	kilobits per second (speed or communication volume per second) 1 kbps = 1 000 (one thousand) bits per second	NDRS	non-disruptive route switching
LAA	locally administered address	NGMF	netView graphic monitor facility
LAN	local area network	NN	network node
LCB	line connection box	NNP	network node processor
LCBB	line connection box base	NPM	netView performance monitor
LCBE	line connection box expansion	NRZI	non-return-to-zero inverted
LCP	link control protocol	NVT	network virtual terminal
LDM	limited distance modem	ODLC	outboard data link control
LED	light emitting diode	OSPF	open shortest path first
LIB n	line interface board type n	PBN	peripheral border node
LIC n	line interface coupler type n	PCI	Peripheral component interconnect
LSA	link state advertisement	PEP	partitioned emulation program
LIU n	line interface coupler unit type n	PING	packet internet groper
LIV	link integrity verification	PN	peripheral node
LMI	local management interface	PPP	point-to-point protocol
LP	logical partition	PPPNCP	point-to-point network control protocol
LPDA®	link problem determination aid	PTP	point-to-point

PTT	post, telegraph, and telephone	SRC	service reference code
PU	physical unit	S/S	start-stop
PVC	permanent virtual circuit	SVC	switched virtual circuit
QUAL	quality	TC	test control
RCV	receive clock	TCM	trellis code modulation
RETAIN®	remote technical assistance information network	TCP	transmission control protocol
RFS	ready for sending	TG	transmission group
RIP	routing information protocol	THRES	threshold
RNR	receive not ready	TICn	Token-ring interface coupler type n
ROS	read-only storage	TIM	time services
RR	receive ready	TOS	type of service
RSF	remote support facility	TPF	transaction processing facility
RTP	rapid transport protocol	TRA	Token-ring adapter
RTS	request to send	TRP	Token-ring processor
SDLC	synchronous data link control	TSS	transmission subsystem
SMUX	single multiplex circuit	UDP	user datagram protocol
SNBU	switched network backup	UTP	unshielded twisted pair
SNI	SNA network interconnection	VTAM	virtual telecommunications access method
SNMP	simple network management protocol	XID	exchange station identification
SPAU	service processor access unit	XMIT	transmit

Glossary

This glossary defines new terms used in this manual.

adaptive rate-based flow and congestion control (ARB). A function of High Performance Routing (HPR) that regulates the flow of data over an RTP connection by adaptively changing the sender's rate based on feedback on the receiver's rate. It allows high link utilization and prevents congestion before it occurs, rather than recovering after congestion has occurred.

advanced communication function (ACF). A group of IBM licensed programs, principally VTAM programs, TCAM, NCP, and SSP, that use the concepts of Systems Network Architecture (SNA), including distribution of function and resource sharing.

advanced communications function for the virtual telecommunications access method (ACF/VTAM). An IBM licensed program that controls communication and the flow of data in an SNA network. It provides single-domain, multiple-domain, and interconnected network capability.

advanced peer-to-peer networking (APPN). Data communications support that routes data in a network between two or more advanced program-to-program communications (APPC) systems that do not need to be adjacent.

automatic network routing. A function of High Performance Routing (HPR) that provides a low-level routing mechanism that requires no intermediate storage.

channel adapter (CA). A communication controller hardware unit used to attach the controller to a host processor.

communication controller. A device that directs the transmission of data over the data links of a network; its operation may be controlled by a program executed in a processor to which the controller is connected or it may be controlled by a program executed within the device. For example, the IBM 3745 and 3746 Network Nodes.

communications manager. A function of the OS/2 Extended Edition program that lets a workstation connect to a host computer and use the host resources as well as the resources of the other personal computers to which the workstation is attached, either directly or through a host system. The communications manager provides application programming interfaces (APIs) so that users can develop their own applications.

configuration data file - extended (CDF-E). A 3746 Network Node MOSS-E file that contains a description

of all the hardware features (presence, type, address, and characteristics).

communications management configuration host node. The type 5 host processor in a communications management configuration that does all network-control functions in the network except for the control of devices channel-attached to a data host nodes. Synonymous with communications management host. See also data host node.

control panel. A panel that contains switches and indicators for the customer's operator and service personnel.

control program. A computer program designed to schedule and to supervise the execution of programs of the controller.

control subsystem. The part of the controller that stores and executes the control program, and monitors the data transfers over the channel and transmission interfaces.

customer engineer. See IBM service representative

data circuit-terminating equipment (DCE). The equipment installed at the user's premises that provides all the functions required to establish, maintain, and terminate a connection, and the signal conversion between the data terminal equipment (DTE) and the line. For example, a modem is a DCE.

Note: The DCE may be a stand-alone equipment or integrated in the 3745.

data terminal equipment (DTE). That part of a data station that serves as a data source, data link, or both, and provides for the data communication control function according to protocols. For example, the 3174 and PS/2s are DTEs.

data host node. In a communication management configuration, a type 5 host node that is dedicated to processing applications and does not control network resources, except for its channel adapter-attached or communication adapter-attached devices. Synonymous with data host. See also communications management configuration host node.

direct attachment. The attachment of a DTE to another DTE without a DCE.

ESCON channel. A channel having an Enterprise System Connection* channel-to-control-unit I/O interface that uses optical cables as a transmission medium.

ESCON channel adapter (ESCA). A communication controller hardware unit used to attach the controller to a host via ESCON fiber optics. An ESCA consists of an ESCON channel processor (ESCP) and an ESCON channel coupler (ESCC).

ESCON channel coupler (ESCC). A communication controller hardware unit which is the interface between the ESCON channel processor and the ESCON fiber optic cable.

ESCON channel processor (ESCP). A communication controller hardware unit which provides the channel data link control for the ESCON channel adapter.

distributed console access facility. (1) This program product provides a remote console function that allows a user at one programmable workstation (PS/2) to remotely control the keyboard input and monitor the display of output of another programmable workstation. The DCAF program does not affect the application programs that are running on the workstation that is being controlled. (2) An icon that represents the Distributed Console Access Facility.

enterprise systems connection (ESCON). A set of IBM products and services that provides a dynamically connected environment within an enterprise.

Host. See host processor

host processor. (1) A processor that controls all or part of a user application network. (2) In a network, the processing unit where the access method for the network resides. (3) In an SNA network, the processing unit that contains a system services control point (SSCP). (4) A processing unit that executes the access method for attached communication controllers.

High performance routing (HPR). An extension of APPN that provides faster traffic throughput, lower delays, and lower storage overheads.

IBM service representative. An individual in IBM who does maintenance services for IBM products or systems. Also called the IBM *Customer Engineer*.

initial microcode load (IML). The process of loading the microcode into an adapter, the MOSS, or the service processor.

internet. (1) A wide area network connecting disparate networks using the internetwork protocol (IP) (2) A public domain wide area network connecting thousands of disparate networks in industry, education, government and research. The Internet uses TCP/IP as the standard for transmitting information.

internet address. The numbering system used in IP internetwork communications to specify a particular

network, or a particular host on that network with which to communicate.

internet control message protocol (ICMP). A protocol used by a gateway to communicate with a source host, for example, to report an error in a datagram. It is an integral part of the Internetwork Protocol (IP).

internetwork protocol. A protocol that routes data from its source to its destination in an internet environment. It is also called the *Internet Protocol*.

internetwork. Any wide area network connecting more than one network.

initial program load (IPL). The initialization procedure that causes the 3745 control program (NCP) to begin operation.

LAN-attached console. A PS/2 attached to the token-ring LAN that has the service processor attached. It is used to operate remotely the MOSS and MOSS-E functions.

IP router. A device that enables an Internetwork Protocol (IP) host to act as a gateway for routing data between separate networks.

line interface coupler (LIC). A circuit that attaches up to four transmission cables to the controller (from DTEs, DCEs or telecommunication lines).

locally administered address. In a local area network, an adapter address that the user can assign to override the universally administered address.

maintenance and operator subsystem - extended (MOSS-E). The licensed internal code loaded on the service processor hard disk to provide maintenance and operator facilities to the user and IBM service representative.

microcode. A program that is loaded in a processor (for example, the MOSS processor) to replace a hardware function. The microcode is not accessible to the customer.

modem (modulator-demodulator). See DCE.

multiple virtual storage (MVS). Multiple Virtual Storage, consisting of MVS/System Product Version 1 and the MVS/370 Data Facility Product operating on a System/370™ processor.

NetView. An IBM licensed program used to monitor a network, manage it, and diagnose its problems.

nonswitched line. A connection between systems or devices that does not have to be made by dialing. The

connection can be point-to-point or multipoint. The line can be leased or private. Contrast with *switched line*.

ping. A simple IP application that sends one or more messages to a specified destination host requesting a reply. Usually used to verify that the target host exists, or that its IP address is a valid address.

remote console. A PS/2 attached to the 3746 Network Node either by a switched line (with modems) or by one of the communication lines of the user network.

remote technical assistance information network (RETAIN).

service processor. The processor attached to a 3745, 3746-900, and 3746-950 via a token-ring LAN.

remote support facility (RSF). RSF provides IBM maintenance assistance when requested via the public switched network. It is connected to the IBM RETAIN database system.

service representative. See IBM service representative

services. A set of functions designed to simplify the maintenance of a device or system.

switched line. A transmission line with which the connections are established by dialing, only when data transmission is needed. The connection is point-to-point and uses a different transmission line each time it is established. Contrast with *nonswitched line*.

synchronous data link control (SDLC). A discipline for managing synchronous, code-transparent, serial-by-bit information transfer over a link connection. Transmission exchanges may be duplex or half-duplex over switched or nonswitched links. The configuration of the link connection may be point-to-point, multipoint,

or loop. SDLC conforms to subsets of the Advanced Data Communication Control Procedures of the American National Standards Institute and High-Level Data Link Control (HDLC) of the International Standards Organization.

synchronous transmission. Data transmission in which the sending and receiving instruments are operating continuously at substantially the same frequency and are maintained, through correction, in a desired phase relationship.

Token-ring adapter (TRA) type 3. 3746-900 and 3746-950 line adapter for IBM Token-Ring Network, composed of one token-ring processor card (TRP2), and two Token-Ring interface couplers type 3 (TIC 3s).

Token-ring interface coupler type 2 (TIC2). A circuit that attaches an IBM Token-Ring network to the 3745.

Token-Ring Interface Coupler type 3 (TIC3). A circuit that attaches an IBM Token-Ring network to the 3746-900 or 3746-950.

user access area. A specific area in the controller where the customer can install, remove, change, or swap couplers and cables without IBM assistance.

universally administered address. In a local area network, the address permanently encoded in an adapter at the time of manufacture. All universally administered addresses are unique.

user application network. A configuration of data processing products, such as processors, controllers, and terminals, for data processing and information exchange. This configuration may use circuit-switched, packet-switched, and leased-circuit services provided by carriers or PTT. Also called a *user network*.

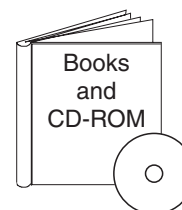
V.24, V.35, and X.21. ITU-T (ex-CCITT) recommendations on transmission interfaces.

Bibliography

Customer Documentation for the 3745 (All Models), and 3746 (Model 900)

Table 7 (Page 1 of 6). Customer Documentation for the 3745 Models X10 and X1A, and 3746 Model 900

This customer documentation has the following formats:

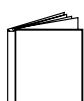


Finding Information

3745 Models A and 3746 Books

All of the books in the 3745 Models A and 3746 library are available on the CD-ROM that contains the Licensed Internal Code (LIC) for the machine.

Evaluating and Configuring



GA33-0092

IBM 3745 Communication Controller Models 210, 310, 410, and 610

Introduction

Gives an introduction of the IBM Models 210 to 610 capabilities.

For Models A, refer to the *Overview*, GA33-0180.



GA33-0180

IBM 3745 Communication Controller Models A and 170² IBM 3746 Nways Multiprotocol Controller Models 900 and 950

Overview

Gives an overview of connectivity capabilities within SNA, APPN, and IP networking.



GA27-4234

IBM 3745 Communication Controller Models A² IBM 3746 Nways Multiprotocol Controller Models 900 and 950

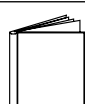
Planning Series:

Overview, Installation, and Integration

Provides information for:

- Overall 3746 planning
- Installation and upgrade scenarios
- Controller and service processor network integration
- Related MOSS-E and CCM worksheets for these tasks.

Table 7 (Page 2 of 6). Customer Documentation for the 3745 Models X10 and X1A, and 3746 Model 900



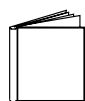
GA27-4235

IBM 3745 Communication Controller Models A²
IBM 3746 Nways Multiprotocol Controller
Models 900 and 950

Planning Series:
Serial Line Adapters

Provides information for:

- Serial line adapter descriptions
- Serial line adapter line weights and connectivity
- Types of SDLC support
- Configuring X.25 lines
- Performance tuning for frame-relay, PPP, X.25, and NCP lines.
- ISDN adapter description and configuration.



GA27-4236

IBM 3745 Communication Controller Models A²
IBM 3746 Nways Multiprotocol Controller
Models 900 and 950

Planning Series:
Token Ring and Ethernet

Provides information for:

- Token-ring adapter description and configuration
- Ethernet adapter description and configuration.



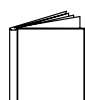
GA27-4237

IBM 3745 Communication Controller Models A²
IBM 3746 Nways Multiprotocol Controller
Models 900 and 950

Planning Series:
ESCON Channels

Provides information for:

- ESCON adapter descriptions
- ESCON configuration and tuning information
- ESCON configuration examples.



GA27-4238

IBM 3745 Communication Controller Models A²
IBM 3746 Nways Multiprotocol Controller
Models 900 and 950

Planning Series:
Physical Planning

Provides information for:

- 3746 and MAE physical planning details
- 3746 and MAE cable information
- Explanation of installation sheets
- 3746 plugging sheets.

Table 7 (Page 3 of 6). Customer Documentation for the 3745 Models X10 and X1A, and 3746 Model 900

	GA27-4239	IBM 3745 Communication Controller Models A² IBM 3746 Nways Multiprotocol Controller Models 900 and 950 Planning Series: Management Planning
		Provides information for: <ul style="list-style-type: none"> • Overview for 3746 • 3746 APPN/HPR, IP router, and X.25 • NetView Performance Monitor (NPM), remote consoles, and RSF • MAE APPN/HPR management.
	GA27-4240	IBM 3745 Communication Controller Models A² IBM 3746 Nways Multiprotocol Controller Models 900 and 950 Planning Series: Multiaccess Enclosure Planning
		Provides information for: <ul style="list-style-type: none"> • MAE adapters details • MAE ESCON planning and configuration • ATM and ISDN support.
	GA27-4241	IBM 3745 Communication Controller Models A² IBM 3746 Nways Multiprotocol Controller Models 900 and 950 Planning Series: Protocols Description
		Provides information for: <ul style="list-style-type: none"> • Overview and details about APPN/HPR and IP.
	On-line information	IBM 3745 Communication Controller Models A² IBM 3746 Nways Multiprotocol Controller Models 900 and 950 Planning Series: Controller Configuration and Management Worksheets
		Provides planning worksheets for ESCON, Multiaccess Enclosure, serial line, and token-ring definitions.
Preparing Your Site		
	GC22-7064	IBM System/360™, System/370™, 4300 Processor Input/Output Equipment Installation Manual-Physical Planning (Including Technical News Letter GN22-5490) Provides information for physical installation for the 3745 Models 130 to 610. For 3745 Models A and 3746 Model 900, refer to the <i>Planning Guide</i> , GA33-0457.
	GA33-0127	IBM 3745 Communication Controller Models 210, 310, 410, and 610 Preparing for Connection Helps for preparing the 3745 Models 210 to 610 cable installation. For 3745 Models A refer to the <i>Connection and Integration Guide</i> , SA33-0129.

Table 7 (Page 4 of 6). Customer Documentation for the 3745 Models X10 and X1A, and 3746 Model 900




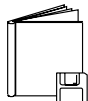



Preparing for Operation		
	GA33-0400	<p>IBM 3745 Communication Controller All Models³ IBM 3746 Nways Multiprotocol Controller Models 900 and 950</p> <p>Safety Information¹</p> <p>Provides general safety guidelines.</p>
	SA33-0129	<p>IBM 3745 Communication Controller All Models³ IBM 3746 Nways Multiprotocol Controller Model 900</p> <p>Connection and Integration Guide¹</p> <p>Contains information for connecting hardware and integrating network of the 3745 and 3746-900 after installation.</p>
	SA33-0416	<p>Line Interface Coupler Type 5 and Type 6 Portable Keypad Display</p> <p>Migration and Integration Guide</p> <p>Contains information for moving and testing LIC types 5 and 6.</p>
	SA33-0158	<p>IBM 3745 Communication Controller All Models³ IBM 3746 Nways Multiprotocol Controller Model 900</p> <p>Console Setup Guide¹</p> <p>Provides information for:</p> <ul style="list-style-type: none"> Installing local, alternate, or remote consoles for 3745 Models 130 to 610 Configuring user workstations to remotely control the service processor for 3745 Models A and 3746 Model 900 using: <ul style="list-style-type: none"> DCAF program Telnet Client program Java Console support.
Customizing Your Control Program		
	SA33-0178	<p>Guide to Timed IPL and Rename Load Module</p> <p>Provides VTAM procedures for:</p> <ul style="list-style-type: none"> Scheduling an automatic reload of the 3745 Getting 3745 load module changes transparent to the operations staff.
Operating and Testing		
	SA33-0098	<p>IBM 3745 Communication Controller All Models⁴</p> <p>Basic Operations Guide¹</p> <p>Provides instructions for daily routine operations on the 3745 Models 130 to 610.</p>
	SA33-0177	<p>IBM 3745 Communication Controller Models A² IBM 3746 Nways Multiprotocol Controller Model 900</p> <p>Basic Operations Guide¹</p> <p>Provides instructions for daily routine operations on the 3745 Models 17A to 61A, and 3746 Model 900 operating as an SNA node (using NCP), APPN/HPR Network Node, and IP Router.</p>

Table 7 (Page 5 of 6). Customer Documentation for the 3745 Models X10 and X1A, and 3746 Model 900

	SA33-0097	IBM 3745 Communication Controller All Models³ Advanced Operations Guide¹	<p>Provides instructions for advanced operations and testing, using the 3745 MOSS console.</p>
	On-line Information	Controller Configuration and Management Application	<p>Provides a graphical user interface for configuring and managing a 3746 APPN/HPR Network Node and IP Router, and its resources. It is also available as a stand-alone application, using an OS/2 workstation. Defines and explains all the 3746 Network Node and IP Router configuration parameters through its online help.</p>
	SH11-3081	IBM 3746 Nways Multiprotocol Controller Models 900 and 950 Controller Configuration and Management: User's Guide⁵	<p>Explains how to use CCM and gives examples of the configuration process.</p>
	GA33-0479	IBM 3745 Communication Controller Models A IBM 3746 Nways Multiprotocol Controller Models 900 and 950 NetView Console APPN Command Reference Guide	<p>Explains how to use the RUN COMMAND from the NetView S/390 Program and gives examples.</p>
Managing Problems			
	SA33-0096	IBM 3745 Communication Controller All Models³ Problem Determination Guide¹	<p>A guide to perform problem determination on the 3745 Models 130 to 61A.</p>
	On-line Information	Problem Analysis Guide	<p>An online guide to analyze alarms, events, and control panel codes on:</p> <ul style="list-style-type: none"> • IBM 3745 Communication Controller Models A² • IBM 3746 Nways Multiprotocol Controller Models 900 and 950.
	SA33-0175	IBM 3745 Communication Controller Models A² IBM 3746 Expansion Unit Model 900 IBM 3746 Nways Multiprotocol Controller Model 950 Alert Reference Guide	<p>Provides information about events or errors reported by alerts for:</p> <ul style="list-style-type: none"> • IBM 3745 Communication Controller Models A² • IBM 3746 Nways Multiprotocol Controller Models 900 and 950.

Table 7 (Page 6 of 6). Customer Documentation for the 3745 Models X10 and X1A, and 3746 Model 900

¹ Documentation shipped with the 3745.




² 3745 Models 17A to 61A.

³ 3745 Models 130 to 61A.

⁴ Except 3745 Models A.

⁵ Documentation shipped with the 3746-900.

Additional Customer Documentation for the 3745 Models 130, 150, 160, 170, and 17A

<i>Table 8. Additional Customer Documentation for the 3745 Models 130 to 17A</i>		
This customer documentation has the following format:		
		
Finding Information		
<p>3745 Models A and 3746 Books</p> <p>All of the books in the 3745 Models A and 3746 library are available on the CD-ROM that contains the Licensed Internal Code (LIC) for the machine.</p>		
Evaluating and Configuring		
	GA33-0138	<p>IBM 3745 Communication Controller Models 130, 150, 160, and 170</p> <p>Introduction</p> <p>Gives an introduction about the IBM Models 130 to 170 capabilities, including Model 160.</p> <p>For Model 17A refer to the <i>Overview</i>, GA33-0180.</p>
Preparing Your Site		
	GA33-0140	<p>IBM 3745 Communication Controller Models 130, 150, 160, and 170</p> <p>Preparing for Connection</p> <p>Helps for preparing the 3745 Models 130 to 170 cable installation.</p> <p>For 3745 Model 17A refer to the <i>Connection and Integration Guide</i>, SA33-0129.</p>
¹ Documentation shipped with the 3745.		

Customer Documentation for the 3746 Model 950

Table 9 (Page 1 of 4). Customer Documentation for the 3746 Model 950

This customer documentation has the following formats:



Finding Information

3745 Models A and 3746 Books

All of the books in the 3745 Models A and 3746 library are available on the CD-ROM that contains the Licensed Internal Code (LIC) for the machine.

Preparing for Operation



GA33-0400

IBM 3745 Communication Controller All Models¹
IBM 3746 Expansion Unit Model 900
IBM 3746 Nways Multiprotocol Controller Model 950

Safety Information²

Provides general safety guidelines.

Evaluating and Configuring



GA33-0180

IBM 3745 Communication Controller Models A and 170³
IBM 3746 Nways Multiprotocol Controller
Models 900 and 950

Overview

Gives an overview of connectivity capabilities within SNA, APPN, and IP networking.



GA27-4234

IBM 3745 Communication Controller Models A²
IBM 3746 Nways Multiprotocol Controller
Models 900 and 950

Planning Series: Overview, Installation, and Integration

Provides information for:

- Overall 3746 planning
- Installation and upgrade scenarios
- Controller and service processor network integration
- Related MOSS-E and CCM worksheets for these tasks.

Table 9 (Page 2 of 4). Customer Documentation for the 3746 Model 950

	GA27-4235	IBM 3745 Communication Controller Models A² IBM 3746 Nways Multiprotocol Controller Models 900 and 950
		Planning Series: Serial Line Adapters
		Provides information for: <ul style="list-style-type: none"> • Serial line adapter descriptions • Serial line adapter line weights and connectivity • Types of SDLC support • Configuring X.25 lines • Performance tuning for frame-relay, PPP, X.25, and NCP lines. • ISDN adapter description and configuration.
	GA27-4236	IBM 3745 Communication Controller Models A² IBM 3746 Nways Multiprotocol Controller Models 900 and 950
		Planning Series: Token Ring and Ethernet
		Provides information for: <ul style="list-style-type: none"> • Token-ring adapter description and configuration • Ethernet adapter description and configuration.
	GA27-4237	IBM 3745 Communication Controller Models A² IBM 3746 Nways Multiprotocol Controller Models 900 and 950
		Planning Series: ESCON Channels
		Provides information for: <ul style="list-style-type: none"> • ESCON adapter descriptions • ESCON configuration and tuning information • ESCON configuration examples.
	GA27-4238	IBM 3745 Communication Controller Models A² IBM 3746 Nways Multiprotocol Controller Models 900 and 950
		Planning Series: Physical Planning
		Provides information for: <ul style="list-style-type: none"> • 3746 and MAE physical planning details • 3746 and MAE cable information • Explanation of installation sheets • 3746 plugging sheets.

Table 9 (Page 3 of 4). Customer Documentation for the 3746 Model 950





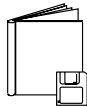





	GA27-4239	<p>IBM 3745 Communication Controller Models A² IBM 3746 Nways Multiprotocol Controller Models 900 and 950</p> <p>Planning Series: Management Planning</p>
	Provides information for:	<ul style="list-style-type: none"> • Overview for 3746 • 3746 APPN/HPR, IP router, and X.25 • NetView Performance Monitor (NPM), remote consoles, and RSF • MAE APPN/HPR management.
	GA27-4240	<p>IBM 3745 Communication Controller Models A² IBM 3746 Nways Multiprotocol Controller Models 900 and 950</p> <p>Planning Series: Multiaccess Enclosure Planning</p>
	Provides information for:	<ul style="list-style-type: none"> • MAE adapters details • MAE ESCON planning and configuration • ATM and ISDN support.
	GA27-4241	<p>IBM 3745 Communication Controller Models A² IBM 3746 Nways Multiprotocol Controller Models 900 and 950</p> <p>Planning Series: Protocols Description</p>
	Provides information for:	<ul style="list-style-type: none"> • Overview and details about APPN/HPR and IP.
	On-line information	<p>IBM 3745 Communication Controller Models A² IBM 3746 Nways Multiprotocol Controller Models 900 and 950</p> <p>Planning Series: Controller Configuration and Management Worksheets</p>
	Provides planning worksheets for ESCON, Multiaccess Enclosure, serial line, and token-ring definitions.	

Table 9 (Page 4 of 4). Customer Documentation for the 3746 Model 950

Operating and Testing		
	SA33-0356	<p>IBM 3746 Nways Multiprotocol Controller Model 950</p> <p>User's Guide²</p> <p>Explains how to:</p> <ul style="list-style-type: none"> • Carry out daily routine operations on Nways controller • Install, test, and customize the Nways controller after installation • Configure user's workstations to remotely control the service processor using: <ul style="list-style-type: none"> – DCAF program – Telnet client program – Java Console support.
	On-line information	<p>Controller Configuration and Management Application</p> <p>Provides a graphical user interface for configuring and managing a 3746 APPN/HPR network node and IP Router, and its resources. It is also available as a stand-alone application, using an OS/2 workstation. Defines and explains all the 3746 Network Node and IP Router configuration parameters through its on-line help.</p>
	SH11-3081	<p>IBM 3746 Nways Multiprotocol Controller Models 900 and 950</p> <p>Controller Configuration and Management: User's Guide²</p> <p>Explains how to use CCM and gives examples of the configuration process.</p>
	GA33-0479	<p>IBM 3745 Communication Controller Models A IBM 3746 Nways Multiprotocol Controller Models 900 and 950</p> <p>NetView Console APPN Command Reference Guide</p> <p>Explains how to use the RUN COMMAND from the NetView S/390 Program and gives examples.</p>
Managing Problems		
	On-line information	<p>Problem Analysis Guide</p> <p>An on-line guide to analyze alarms, events, and control panel codes on:</p> <ul style="list-style-type: none"> • IBM 3745 Communication Controller Models A³ • IBM 3746 Nways Multiprotocol Controller Models 900 and 950.
	SA33-0175	<p>IBM 3745 Communication Controller Models A³ IBM 3746 Expansion Unit Model 900 IBM 3746 Nways Multiprotocol Controller Model 950</p> <p>Alert Reference Guide</p> <p>Provides information about events or errors reported by alerts for:</p> <ul style="list-style-type: none"> • IBM 3745 Communication Controller Models A³ • IBM 3746 Nways Multiprotocol Controller Models 900 and 950.
<p>¹ Models 130 to 61A. ² Documentation shipped with the 3746-950 ³ 3745 Models 17A to 61A.</p>		

Required Documentation

The following documents are indispensable for planning for your 3745/3746 controllers:

- *3745 Communication Controller Models A and 170, 3746 Nways Multiprotocol Controller Models 900 and 950: Overview*, GA33-0180
- *3745 Communication Controller All Models, 3746 Nways Multiprotocol Controller Model 900: Console Setup Guide*, SA33-0158.

Be sure to use the latest editions of the above documents.

Related Documentation

The following documents are also helpful for **planning** for your 3745/3746 controllers:

- *Planning for Integrated Networks*, SC31-8062
- *Planning and Reference for NetView, NCP, and VTAM*, SC31-7122.
- *Virtual Telecommunications Access Method V3 R4: Resource Definition Reference*, SC31-6438

The following Enterprise Systems Connection (**ESCON**) documents may be helpful:

- *Introducing the Enterprise Systems Connection*, GA23-0383
- *Enterprise Systems Connection Migration*, GA23-0383
- *Planning for Enterprise Systems Connection Links*, GA23-0367
- *Introducing Enterprise Systems Connection Directors*, GA23-0363.

The following IBM International Technical Support Centers “redbooks” are generally very helpful:

- *Frame Relay Guide*, GG24-4463
- *3746-900 and NCP Version 7 Release 2*, GG24-4464.

The following Network Control Program (**NCP**) documents may be helpful:

- For NCP V6 R2:
 - *Network Control Program V6 R2: Migration Guide*, SC31-6216
 - *Network Control Program V6 R2, ACF/SSP V3 R8, EP R11: Resource Definition Guide*, SC31-6209-01
 - *Network Control Program V6 R2, ACF/SSP V3 R8, EP R11: Resource Definition Reference*, SC31-6210-01
 - *Network Control Program V6 R2: Planning and Implementation Guide*, GG24-4012
 - *Network Control Program V6 R2, ACF/SSP V3 R8, EP R11: Library Directory*, SC31-6215.
- For NCP V6 R3:
 - *Network Control Program V6 R3: Migration Guide*, SC31-6217
 - *Network Control Program V6 R3, ACF/SSP V3 R9, EP R11: Resource Definition Guide*, SC31-6209-02
 - *Network Control Program V6 R3, ACF/SSP V3 R9, EP R11: Resource Definition Reference*, SC31-6210-02 Guide,
 - *Network Control Program V6 R3, ACF/SSP V3 R9, EP R11: Library Directory*, SC31-6218.
- For NCP V7 R1:
 - *Network Control Program V7 R1: Migration Guide*, SC31-6219
 - *Network Control Program V7 R1, ACF/SSP V4 R1, EP R12: Resource Definition Guide*, SC31-6223-00
 - *Network Control Program V7 R1, ACF/SSP V4 R1, EP R12: Resource Definition Reference*, SC31-6224-00
 - *Network Control Program V7 R1, ACF/SSP V4 R1, EP R12: Library Directory*, SC31-6220.

- For NCP V7 R2:
 - *Network Control Program V7 R2, ACF/SSP V4 R2, EP R12: Generation and Loading Guide*, SC31-6221.
 - *Network Control Program V7 R2: Migration Guide*, SC31-6258-00
 - *Network Control Program V7 R2, ACF/SSP V4 R2, EP R12: Resource Definition Guide*, SC31-6223-01
 - *Network Control Program V7 R2, ACF/SSP V4 R2, EP R12: Resource Definition Reference*, SC31-6224-01
 - *Network Control Program V7 R2, ACF/SSP V4 R2, EP R12: Library Directory*, SC31-6259.
- For NCP V7 R3:
 - *Network Control Program V7 R3: Migration Guide*, SC31-6258-01
 - *Network Control Program V7 R3, ACF/SSP V4 R3, EP R12: Resource Definition Guide*, SC31-6223-02
 - *Network Control Program V7 R3, ACF/SSP V4 R3, EP R12: Resource Definition Reference*, SC31-6224-02
 - *Network Control Program V7 R3, ACF/SSP V4 R3, EP R12: Library Directory*, SC31-6262.
- For NCP V7 R4:
 - *Network Control Program V7 R4: Migration Guide*, SC30-3786
 - *Network Control Program V7 R4, ACF/SSP V4 R4, EP R12: Resource Definition Guide*, SC31-6223-03
 - *Network Control Program V7 R4, ACF/SSP V4 R4, EP R12: Resource Definition Reference*, SC31-6224-03
 - *Network Control Program V7 R4, ACF/SSP V4 R4, EP R12: Library Directory*, SC30-3785.
- For NCP V7 R5:
 - *Network Control Program V7 R5: Migration Guide*, SC30-3833
 - *Network Control Program V7 R5, ACF/SSP V4 R4, EP R12: Resource Definition Guide*, SC31-6223-04
 - *Network Control Program V7 R5, ACF/SSP V4 R4, EP R12: Resource Definition Reference*, SC31-6224-04
 - *Network Control Program V7 R5, ACF/SSP V4 R4, EP R12: Library Directory*, SC30-3832.
- For NCP V7 R6:
 - *Network Control Program V7 R6: Migration Guide*, SC30-3833-01
 - *Network Control Program V7 R6, ACF/SSP V4 R4, EP R14: Resource Definition Guide*, SC31-6223-06
 - *Network Control Program V7 R6, ACF/SSP V4 R4, EP R14: Resource Definition Reference*, SC31-6224-06
 - *Network Control Program V7 R6, ACF/SSP V4 R4, EP R14: Library Directory*, SC30-3785.
- For NCP V7 R7:
 - *Network Control Program V7 R7: Migration Guide*, SC30-3889
 - *Network Control Program V7 R7, ACF/SSP V4 R4, EP R14: Resource Definition Guide*, SC31-6223-07
 - *Network Control Program V7 R7, ACF/SSP V4 R4, EP R14: Resource Definition Reference*, SC31-6224-07
 - *Network Control Program V7 R7, ACF/SSP V4 R4, EP R14: Library Directory*, SC30-3971.

The following **OS/2** document may be of some help:

IBM Extended Services® for OS/2 Programming Services and Advanced Problem Determination for Communications, SO4G-1007.

For the Distributed Console Access Facility (**DCAF**) Version 1.3 the following documents are needed:

- *DCAF: Installation and Configuration Guide*, SH19-4068
- *DCAF: User's Guide*, SH19-4069
- *DCAF: Target User's Guide*, SH19-6839.

To learn more about the **APPN** architecture, including high-performance routing (HPR), adaptive rate based flow and congestion control (ARB), dependent LU requesters/servers (DLURs/DLUSs), and other subjects, refer to:

- *Inside APPN - The Essential Guide to the Next-Generation SNA*, SG24-3669.
- *APPN Architecture and Protocol Implementations Tutorial* SG24-3669.

The following Virtual Telecommunications Access Method (**VTAM**), may be helpful:

- *Virtual Telecommunications Access Method V4R3: Resource Definition Reference*, SC31-6438.

For help with **TCP/IP**, refer to:

- *TCP/IP for MVS: Performance Tuning Guide*, SC31-7188.

To learn about token-ring configurations and the **IEEE 802.2** standard, refer to:

- *Token-Ring Network Architecture Reference*, SC30-3374.

These latest NetView documents may be helpful:

- *TME 10 NetView for OS/390 Version 1: Planning Guide*, GC31-8226
- *TME 10 NetView for OS/390 Version 1: Tuning Guide*, SC31-8240.

The following NetView Performance Monitor (**NPM**) documents are available:

- *NetView Performance Monitor: Concepts and Planning V2R2*, GH19-6961-01
- *NetView Performance Monitor: Concepts and Planning V2R3*, GH19-6961-02
- *NetView Performance Monitor: Concepts and Planning V2R4*, GH19-6961-03
- *NetView Performance Monitor: Concepts and Planning V3R1*, GH19-4221-00.

Index

Numerics

3746 SNMP variable 86

A

accounting management, X.25 91
accounting manager
addresses, IP for remote consoles 71
agents (SNMP) 22
alerts 12
alternate alert reporting path 27, 28
APPN
 MIBs 24
 topology and accounting management (APPNTAM) 2
 topology feature 24
APPN/HPR
 mainstream alert reporting path definitions 29
 subarea mainstream definitions in VTAM 30

B

beaconing 36

C

CCM SNMP 86
CD-ROM Online documentation xxiii
changes since last edition xviii
CMIP 3, 4
CMIP services 2
code points
 code points supported by NetView 34
 customizing for alerts 34
command tree/2 3
community name 86
configuring DCAF 73
configuring Java Console 75
controller operations when the service processor is not available 36
customer
 consoles 66
 specific information 79, 96
customer tasks xxv

D

DCAF
 Communications Manager 70
 customer consoles 66
 DCAF non-secure 74
 defined 65

DCAF (*continued*)

 installation and configuration 73
 IP resources, managing 87
 remote logon password 95
 service processor (CM/2) parameters 94
 service processor parameters 70
 service processor security 73
 target logon password 74
 TCP/IP 71
DCAF console programming access 68
definitions
 APPN/HPR
 APPN/HPR mainstream path 27, 29
 for RSF 79, 96
 for SNA network in VTAM 32
 in VTAM for subarea mainstream path 30
 mainstream alert reporting path 27
 mainstream path
 APPN/HPR path 29
 SNA/subarea path 31
 NetView alternate path 33
 NetView path parameter 28
 network node processor alerts 29
disabling calls 75
distributed agent 83
DLSw MIBs 24
DLUR 3
DLUS 3

E

enterprise specific MIBs 24
external box errors 25

F

fault management, X.25 91

I

installing DCAF 73
internal box errors 25
IP
 DCAF, managing resources 87
 protocols, simple network management (SNMP) 22
 router management 21, 81

J

Java Console
 configuration 75
 programming requirements 69

L

- LAN bridge 35
- local topology 5
- locating Generate Alerts parameter 34
- locating netview link/operations parameter 34

M

- mainstream alert reporting path 27
- managers (SNMP) 22
- managing system 10
- MDS-MUs 4
- MDS-RECEIVE 4
- MDS-SEND 4
- microcode download, automatic 78, 96
- microcode levels required for year 2000 readiness xviii
- migration APPN/HPR performance management, to 60
- modem
 - disabling calls 75
 - external 75
 - integrated 75
- modem, RSF 80
- monitor APPN/HPR network topology 41
- MOSS-E
 - alternate alert reporting path 28
 - path for reporting MOSS-E alerts 27
 - SNA/subarea path 28

N

- NetView 20
 - alert focal point 25
 - alternate path 28
 - alternate path definition 33
 - backup alert focal point 25
 - code points customizing for alerts 34
 - code points supported 34
 - generate MOSS-E alerts 93
 - generate NetView alerts 34
 - mainstream path 27
 - not using NetView 34
 - path for reporting alerts 26
 - path for reporting network node processor alerts 27
 - path parameter definitions 28, 93
 - reporting MOSS-E alerts to 25
 - RUNCMD 20
 - topology management 41
- netview link/operations parameter 34
- NetView Performance Monitor 19, 59
- NetView Performance Monitor (NPM) 20
- network management, X.25 91
- network node
 - alert focal point 25
 - alternate alert reporting path 27, 28
 - external box errors 25
 - internal box errors 25

- network node (*continued*)

- mainstream alert reporting path 27
 - management 41
 - path for reporting alerts to NetView 26
 - path for reporting MOSS-E alerts 27
 - reporting MOSS-E alerts to NetView 25
 - SNA/subarea alert reporting path 28
- network node processor
 - alerts 29
 - unplugging network node processor from service LAN 36
- Network Performance Monitor 60
- network topology database 5
- network, APPN/HPR monitor 41
- NGMF 3
- NNP 19
 - reporting CPU and memory use 19
- no users on service LAN 35

O

- operator password, remote 74
- OSI 3

P

- parameter worksheets 93
- password
 - DCAF remote logon 95
 - remote operator 74
- path for reporting
 - alerts to NetView 26
 - MOSS-E alerts 27
- performance management 19, 59
- performance monitoring
 - APPN/HPR, definitions 45
 - CCM, definitions 47
- performance monitoring, X.25 91
- programming
 - requirements for Java Console 69
 - requirements for Telnet 69
- protocols, IP
 - simple network management (SNMP) 22

R

- remote
 - access security 73
 - operator password 74
- remote consoles
 - DCAF hardware requirements 69
 - minimum workstation configuration 68
- resolutions 12
- RODM 3
- router management (IP) 21, 81

RSF
 authorization 79, 96
 connecting to 77
 modem 80
 parameter definitions 79, 96
RUNCMD 12

S

security
 remote access 73
 remote operator password 74
 service processor 73
service processor 19
 CM/2 parameters for DCAF 94
 customization 97
 definitions for RSF 79, 96
 disable calls 75
 disable service processor incoming calls 96
 parameters for DCAF 70
 recommendations for operations 37
 reporting CPU and memory use 19
 security 73
service processor and NNP
 automatic activation, dual network node processor 40
 backup different levels of microcode 38
 broadcast storms 35
 dual Network Node Processors 40
 hot standby network node processor 40
 LAN bridge 35
 network node processor loss: effect on IP 39
 operations when the network node processor is not available 39
 recommendations for service processor operations 37
 redundant Network Node Processor 40
 saving microcode 37
 service processor backs 38
 service processor not available 36
session monitor 3
Simple network management protocol (SNMP) 22
 agents 22
 Definitions 84
 IP resources, managing 81
 managers 22
 traps 22
 X.25 91
SMF 3
SNA
 alert reporting path 28
 alert transport 24
 management services 4
 topology manager 2, 5
SNMP
 See also Simple network management protocol (SNMP)

SNMP (*continued*)
 agent 24
 traps 24
SNMP relay 82
SNMP trap 84
SNMP TRAPS 86

T

TCP/IP DCAF 71
telnet programming requirements 69
TME 10 remote control, installation and configuration 73
topology agent 5
topology and accounting agent (APPNTAA) 2
topology management 41
topology manager 3, 5, 6
Trap 84
traps (SNMP) 22

V

VR-TG 3
VTAM
 network definitions 30, 32

W

workstation configuration, TME 10 Remote Control 68

X

X.25
 accounting management 91
 fault management 91
 network management 91
 performance monitoring 91
 SNMP 91

Y

Year 2000
 microcode levels required xviii
 readiness xviii

Tell Us What You Think!

3745 Communication Controller Model A
3746 Nways Multiprotocol Controller
Models 900 and 950
Planning Series:

Management Planning Guide
Publication No. GA27-4239-01

We hope you find this publication useful, readable, and technically accurate, but only you can tell us! Your comments and suggestions will help us improve our technical publications. Please take a few minutes to let us know what you think by completing this form. If you are in the USA, you can mail this form postage free or fax it to us at 1-800-253-3520. Elsewhere, your local IBM branch office or representative will forward your comments or you may mail them directly to us.

Overall, how satisfied are you with the information in this book?	Satisfied	Dissatisfied
	<input type="checkbox"/>	<input type="checkbox"/>

How satisfied are you that the information in this book is:	Satisfied	Dissatisfied
Accurate	<input type="checkbox"/>	<input type="checkbox"/>
Complete	<input type="checkbox"/>	<input type="checkbox"/>
Easy to find	<input type="checkbox"/>	<input type="checkbox"/>
Easy to understand	<input type="checkbox"/>	<input type="checkbox"/>
Well organized	<input type="checkbox"/>	<input type="checkbox"/>
Applicable to your task	<input type="checkbox"/>	<input type="checkbox"/>

Specific comments or problems:

Please tell us how we can improve this book:

Thank you for your comments. If you would like a reply, provide the necessary information below.

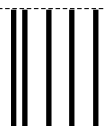
Name	Address
Company or Organization	
Phone No.	



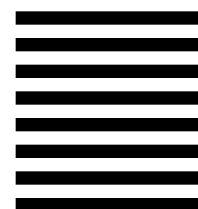
Fold and Tape

Please do not staple

Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Design & Information Development
IBM Corporation
Software Reengineering
Department G71A/ Bldg 503
P.O. Box 12195
Research Triangle Park, NC 27709-9990



Fold and Tape

Please do not staple

Fold and Tape



Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

GA27-4239-01

