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

Planning Series:

Protocols Description

GA27-4241-01

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

Planning Series:

Protocols Description

GA27-4241-01

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.

Contents

Figures

Tables

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 Richlinie 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.

Trademarks

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

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

NetView, TME, 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 Edition

This book has been revised to include the following changes and enhancements:

- Support of the Branch Extender (BEX) function, reducing the Network Node (NN) load on large APPN networks. BEX support includes the following two new parameters:
  - APPN Branch Extender, which indicates whether the BEX function is activated on this node
  - Permit Search for Unregistered LUs, which indicates whether this node (when acting as an end node) can be searched for LUs even if the LUs were not registered with the network node server of the BEX.
  - Dynamic discover of low entry networking (LEN) nodes and network nodes (NN) without control sessions.

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 adapter[1] 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*.

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:

a. Click **Documentation** to access 3745/3746 books.

b. 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: • *Planning for Integrated Networks* • IBM redbooks: – *Subarea Network to APPN Network Migration Guide* – *IBM 3746 Nways Multiprotocol Controller Model 950 and IBM Model 900: APPN Implementation Guide* – *IBM 3746 Nways Multiprotocol Controller Model 950 and IBM Model 900: IP Implementation Guide* – *IBM Nways 2216 Multiaccess Connector Description* – *IBM 2216 Multiaccess Connector ESCON Solutions*
Physical planning: Before the IBM service representative arrives to install your controller, make sure that you have met the necessary requirements for the following: • 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 *3745/3746 Planning Series: Physical Planning*
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 *3745/3746 Planning Series: Physical Planning*.

Table 1 (Page 2 of 3). Customer Tasks	
Task	**Where to Find Information**
Software definitions and tuning: • ESCON port, host link, and station definitions; ESCON resource, TCP/IP, and VTAM® tuning	Refer to: • "ESCON Adapters" chapter in the *3745/3746 Planning Series: ESCON Channels* • "ESCON Channel Adapter" chapter in the *3745/3746 Planning Series: Multiaccess Enclosure Planning* • "ESCON Configuration Examples" chapter in the *3745/3746 Planning Series: ESCON Channels*
• 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	• "Token-Ring Adapters" chapter in the *3745/3746 Planning Series: Token Ring and Ethernet*
• 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	• "Serial Line Adapters" chapter in the *3745/3746 Planning Series: Serial Line Adapters* • "3746 SDLC Support" chapter in the *3745/3746 Planning Series: Serial Line Adapters*
• Multiaccess Enclosure: hardware planning and configuration; software configuration and tuning	• *3745/3746 Planning Series: Multiaccess Enclosure Planning* • *3745/3746 Planning Series: Physical Planning*
• Use of the Controller Configuration and Management (CCM) application.	• *IBM Controller Configuration and Management User's Guide*, SH11-3081. Also refer to: • *IBM 3746 Nways Multiprotocol Controller Model 950 and IBM Model 900: APPN Implementation Guide* (an IBM redbook) • *IBM 3746 Nways Multiprotocol Controller Model 950 and IBM Model 900: IP Implementation Guide* (an IBM redbook).
Filling out: • 3746 plugging sheets To keep a record of the processors and couplers (and their addresses) installed in the 3746 frame.	Refer to: • "Plugging Sheets for 3745 and 3746" chapter in the *3745/3746 Planning Series: Physical Planning*
• *CCM User's Guide*, SH11-3081 worksheets To plan the 3746 and MAE logical resource definitions. They can then be used when configuring the 3746 and MAE via the CCM.	• *3745/3746 Planning Series: CCM Planning Worksheets*

Table 1 (Page 3 of 3). Customer Tasks	
Task	**Where to Find Information**
NetView definitions in VTAM, the MOSS-E, NPM, CCM, NetView/360, and Tivoli NetView® (formerly NetView for AIX) for: • APPN traffic • IP traffic • NetView alert path.	Refer to: • "3746 Management Overview" chapter in the *3745/3746 Planning Series: Management Planning* • "3746 APPN/HPR Network Node Management" chapter in the *3745/3746 Planning Series: Management Planning* • "3746 IP Router Management" chapter in the *3745/3746 Planning Series: Management Planning*.
Controller, service processor, and network node processor definitions. For example: • 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.	Refer to "Controller and Service Processor Integration" chapter in the *3745/3746 Planning Series: Overview, Installation, and Integration*. Fill out the worksheets in the various *Planning Series* guides. These worksheets are used by the IBM service representative during installation.
Remote console definitions (using DCAF): • 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.	Refer to: • "Remote Customer Consoles" chapter in the *3745/3746 Planning Series: Management Planning* • For the 3746-900, refer to the *3745 Console Setup Guide* • For the 3746-950, refer to the *IBM 3746 Nways Multiprotocol Controller Model 950 User's Guide*
Connection to the IBM remote support facility (RSF): • Service processor connection (modem) definitions • Customer definitions for RSF records.	Refer to the "Connecting to the IBM Remote Support Facility" chapter in the *3745/3746 Planning Series: Management Planning*
Problem determination through the MOSS-E and NetView	For the 3746-900, refer to: • *Problem Analysis Guide* accessed online from the MOSS-E • *3745 Models A: Alert Reference Guide* • *3745 All Models: Advanced Operators Guide*

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

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

Chapter 1. APPN / HPR Overview

This chapter gives you a short introduction to Advanced Peer-to-Peer Networking® (APPN®) and HPR, serving as a conceptual base to understand the 3746-900 and the Nways® Controller in an APPN network. In order to have an in-depth knowledge of the APPN and HPR architecture and to know about the details of specific subjects, we strongly recommend that you read *APPN Architecture and Product Implementations Tutorial*.

For ACF/VTAM® and NCP implementations of HPR, refer to:

- *ACF/VTAM V4R3 HPR Early User Experiences*
- *ACF/NCP V7R3: New Functions*

Introduction

With the advancements in client/server and peer-to-peer technologies associated with the increasing power of workstations and midrange computers, it became essential to extend the Systems Network Architecture (SNA) in order to address these new networking requirements. That is why Advanced Peer-to-Peer Networking (APPN) was created.

Basing APPN on SNA protocols gives APPN a set of important characteristics, such as:

- Class of service: depending on the nature of data (interactive, batch, file transfer, and so on), APPN will select a physical path and assign the corresponding traffic priorities.
- Segmenting: A message can be divided in several smaller units. This allows the application to be independent of the characteristics of the network, such as the maximum blocksize of a line. This also helps provide fairness among the various sessions sharing one physical link.
- Flow control: pacing mechanisms prevents one node from flooding another one with excessive data.

When using SNA, customers were required to configure networks in a hierarchical design. Such topology often lacks the flexibility to address varying network geographies, sizes, and work group relationships. Moreover, the application's design has changed; instead of having code running in just one central processor, now there can be many processors running code.

APPN provides the flexibility to meet modern requirements for various dynamic topologies users need in their networks. For example, each networked computer can be directly connected to every other computer (known as a *mesh*) or they can all connect through a single routing network node. Alternatively, some customers will choose to continue to use a hierarchical network design. Mesh, network node, hierarchical networks, as well as mixtures of these, are all possible using APPN.

Advanced Program-to-Program Communication (APPC) is usually provided as system software. The APPC software provides two interfaces. The first, a programming interface "at the top," responds to requests from application programs that need to communicate. One example of such an interface is the CPI-C. The

second interface, "at the bottom," exchanges data with the communications hardware.

To determine where partner LUs are located in the network, the nodes in an APPN network exchange different types of messages, known as APPN control information. At each node in an APPN network, there is a control point (CP) that is responsible for managing its resources. Each node that has a CP establishes CP-CP with its *adjacent nodes* for both data and control traffic.

In the following sections, we give a description of each node type showing the differences between them.

Node Types

Each node type in the APPN architecture has a specific function set. Following, you have a description of how each node type works. Table 12 on page 72 and Table 13 on page 75 summarize all the option sets defined in the APPN architecture, and shows their implementation in the 3746.

APPN Network Node

An APPN network node provides distributed directory and routing services for all LUs that it controls. These LUs may be located on the APPN network node itself or on one of the adjacent LEN or APPN end nodes for which the APPN network node provides network node services. Jointly, with the other active APPN network nodes, an APPN network node is able to locate all destination LUs known in the network.

A facility known as *central resource registration* allows an APPN network node to register its resources at a central directory server. Once a resource is registered, APPN network nodes can locate the resource by querying the central directory server instead of using a broadcast search, thus improving network search performance during session establishment.

After the LU is located, the APPN network node is able to calculate the route between origin and destination LU according to the required class of service. All network nodes exchange information about the topology of the network. When two adjacent network nodes establish a connection, they exchange information about the network topology as they know it. In turn, each network node broadcasts this network topology information to other active and adjacent network nodes with which it has CP-CP sessions.

Alternatively, if the connection between network nodes is deactivated, then each network node broadcasts this change to all other, active and adjacent, network nodes. An APPN network node that is taken out of service will be declared inactive and, after some time, removed from the topology information in all network nodes, together with its routing capabilities to other nodes.

The APPN network node is also capable of routing LU-LU sessions through its node from one adjacent node to another adjacent node. This function is called *intermediate session routing*.

APPN End Node

An APPN end node provides limited directory and routing services for LUs local to it. The APPN end node can select an adjacent APPN network node and request this network node to be its *network node server*. If accepted by the network node, the APPN end node may register its local resources at the network node server. This allows the network node server to intercept Locate search requests for resources that are located on the APPN end node and pass the request on to the APPN end node for verification.

Without a network node server, an APPN end node can function as a LEN end node and establish LU-LU sessions with a partner LU in an adjacent APPN or LEN node.

The APPN end node sends Locate search requests, for resources unknown to the APPN end node, to its network node server. The APPN network node uses its distributed directory and routing facilities to locate the LU (via directed, central directory, or broadcast searches) and calculates the optimal route starting at the APPN end node toward the destination LU.

The APPN end node may have active connections to multiple adjacent network nodes; however, only one of these network nodes at a time can act as its network node server. The APPN end node selects its network node server by establishing CP-CP sessions with an adjacent APPN network node.

On APPN network nodes, the APPN end nodes are categorized as either *authorized* or *unauthorized*. An authorized APPN end node may send registration requests to register local network accessible resources at a network node server, a facility known as *end node resource registration*, and might, in addition, request that these resources be registered with the central directory server. If during session establishment a network node server does not know where an LU is located, the network node server queries authorized APPN end nodes within its domain that have indicated they are willing to be queried for unknown resources. Network accessible resources on unauthorized nodes require explicit definition at the network node server as part of its system definition or dynamically by the network node server's operator. To avoid explicitly defining resources of authorized nodes at their network node server, the APPN end node should either register its resources or allow the network node server to query the APPN end node for unknown resources.

An APPN end node can attach to any LEN or APPN node regardless of its network ID.

LEN End Node

A LEN end node provides peer-to-peer connectivity to other LEN end nodes, APPN end nodes, or APPN network nodes. A LEN end node requires that all network-accessible resources, either controlled by the LEN end node itself or on other nodes, be defined at the LEN end node. LUs on adjacent nodes need to be defined with the control point name of the adjacent node. LUs on non-adjacent nodes need to be defined with the control point name of an adjacent network node, as LEN end nodes assume that LUs are either local or reside on adjacent nodes.

Unlike APPN end nodes, the LEN end node cannot establish CP-CP sessions with an APPN network node; therefore, a LEN end node cannot register resources at a

network node server, nor can it request its network node server to search for a resource, or to calculate the route between the LEN end node and the node containing a destination resource.

However, indirectly a LEN end node uses the distributed directory and routing services of an adjacent network node by predefining remote LUs, owned by non-adjacent nodes, with the CP name of an adjacent APPN network node. The session activation (BIND) request for that remote LU is sent by the LEN end node to the adjacent network node. The network node, in turn, automatically acts as the LEN end node's network node server, locates the actual destination of the LU, calculates the route to it, and uses this route to send the BIND to its final destination.

A LEN end node can attach to any LEN or APPN node regardless of its network ID.

Enhanced Support for LEN End Nodes

After migrating from a VTAM® and NCP composite node configuration and replacing the NCPs with 3746-900 network nodes (900 NNs), networks experience VTAM-to-branch session failures. Sessions can be activated from the branch to the central VTAM, but not from VTAM to the branch because VTAM can no longer find the branch LUs. The following sections explain the cause of these session failures and the enhanced support solutions.

Before Migration: In the VTAM and NCP composite node configuration, the network has all devices and their LUs predefined in VTAM switched major node decks. Most devices are defined to VTAM as LEN end nodes, and their LUs are defined as independent LUs associated with the particular device. When VTAM activates a connection to one such device, it finds the device predefinition (the PU statement) and the associated LU statements. The PU statement tells VTAM to treat this device as a LEN end node, even though the device actually is configured as an APPN network node. In this way, if any application or other LU wants to establish a session with any of those independent LUs, VTAM knows where to send the session request (BIND) and which device can successfully process it.

After Migration: After migrating to the 900 NN configuration, the branch boxes are no longer connected to VTAM; they are connected to the 900 NN control point. This means that all the switched major node PU and LU definitions in VTAM are now useless (the PUs remain connectable forever, and the LUs remain undefined). Because the branch LU definitions in the VTAM switched major node deck are not usable and the branch LUs are not predefined in the 900 NNs, VTAM can no longer find the branch LUs to set up VTAM-to-branch sessions, with the exception of VTAM-to-branch-initiated sessions when the adjacent node is a network node with no CP-CP sessions. In those cases, predefinition in the 900 NN of all the LUs residing in the branch network nodes is still mandatory.

Functional Enhancements: The following enhancements have been made to a address this migration issue:

1. The first enhancement enables the 900 NN to learn some of the names of the LUs in a LEN end node without predefining them. The 900 NN obtains the PLU names from the BINDs that the LEN end node sends in and then defines a directory entry for each of those LUs. The LU directory entries enable the 900 NN to answer a received Locate, Find (PLU_name_from_BIND) with a Found, allowing sessions toward the LEN end node LU to succeed after that LU has sent a BIND.

Note: Once the 900 NN creates an LU definition, it keeps the directory entry as long as the connection to the LEN end node is alive. This might result in multiple network nodes having the same definition for a given LEN end node LU. If the LEN end node has multiple links to different network nodes and sends a blind BIND for the same PLU name on each of the links, each of the network nodes will respond Found to a Locate for that LU name. The same situation can occur if the LEN end node is actually an APPN end node that has no network node server (which is the only reason that it would send a BIND with no RSCV) and has some links predefined with CP-CP sessions disabled.

Unfortunately, this solution addresses only a part of the problem. Some branch LUs never send a BIND until being prompted by receipt of a BIND from VTAM.

2. The second enhancement addresses the inability of the 900 NN to respond to Locates on behalf of branch network nodes.

   When the branch device connects to the 900 NN, the 900 NN sees this device as another APPN network node that is configured not to support CP-CP sessions on the link. Architecturally, one network node does not respond to Locates for LUs that are located on another network node. So, even if all the branch LUs are predefined in each 900 NN, because the 900 NN will not respond on behalf of the branch device (as a network node), VTAM is still not able to find the branch LUs.

   The purpose of this second enhancement is to have the 900 NN respond to Locates on behalf of the branch network nodes. Predefinition in the 900 NN of all the LUs residing in the branch network nodes is **still mandatory** for VTAM-to-branch-initiated sessions, when the adjacent node is a network node with no CP-CP sessions as well as when it is a LEN end node.

   A branch-to-VTAM BIND from a LEN end node will always create an LU predefinition, but it will NOT cause an LU predefinition to be created if the BIND is received from a network node unless there is some other DEFINE_PARTNER_LU_LOCATION already defined which tells the 900 NN to respond to Locates on behalf of that network node.

Other Node Types

Additionally, there are some other node types that will be used in this publication. They are synonyms for nodes as seen from a subarea network, represent a specific junction in the network, or represent an APPN node with additional functions:

- Boundary and peripheral node
- Composite node
- Interchange node
- Virtual routing node
- Border node
- Extended border node

Boundary and Peripheral Node

Within traditional subarea SNA, the resources in a domain of a subarea SNA network are controlled through a hierarchical structure. The nodes that play a role in these networks are categorized as subarea and peripheral nodes. An example of such an SNA network is an S/390® server running VTAM and a 3745 Communication Controller running the network control program (NCP). Both VTAM and NCP are referred to as subarea nodes. The VTAM subarea node includes the control point function, hereafter called the System Services Control Point (SSCP).

Like the APPN control point, the SSCP controls all the resources that are in its domain.

Attached to these subarea nodes, or *boundary nodes*, are the *peripheral nodes*. The peripheral node is either a PU T2.0 or an APPN or LEN node. The PU T2.0 node is a traditional hierarchical node that requires the support of an SSCP to establish sessions. Traditional subarea SNA allowed LEN connections only; CP-CP sessions could not be established between VTAM and the APPN nodes.

With the introduction of APPN VTAM, a VTAM or a composite network node (subarea network consisting of one VTAM and one or more NCPs) is able to present an APPN image to other APPN nodes. APPN VTAM allows CP-CP sessions with APPN nodes attached to the VTAM or NCP boundary function, to get full APPN connectivity. The term “peripheral” node has lost its value in a network that is truly peer-to-peer.

Composite Node

The term *composite node* is used in some publications to represent a group of nodes that appear as ***one*** APPN or LEN node to other APPN or LEN nodes in an APPN network. For example, a subarea network that consists of one VTAM host and one or more NCPs consists of multiple nodes, but when connected to an APPN node, appears as ***one*** logical APPN or LEN node.

A subarea composite node may appear as either a LEN end node or as an APPN network node. In the former case, the term composite LEN node is used; in the latter case the term composite network node (CNN) is used.

Interchange Node

A VTAM host acting as an interchange node (ICN) can be a stand-alone APPN VTAM node or a composite network node. The ICN routes sessions from APPN nodes into and through the subarea network using subarea routing, without exposing the subarea implementation to the APPN part of the network. This is accomplished by making the APPN VTAM node, plus all its owned resources, appear to other nodes as a single APPN network node with multiple connections. At the same time the ICN, and the NCPs it owns, will maintain their subarea appearance to other subarea nodes.

The ICN supports SSCP-SSCP sessions with other VTAM nodes as well as CP-CP sessions with adjacent APPN network nodes and end nodes. This support allows the ICN to use both APPN and subarea data flows to locate LUs and to provide the best route between nodes. APPN session setup protocols, which flow on CP-CP sessions, are converted to the corresponding subarea protocols that flow on SSCP-SSCP sessions, and conversely.

To an ICN multiple VTAMs and NCPs may connect using subarea protocols (see for example VTAM1/NCP in Figure 1 on page 7). Session establishment is possible between any LU in the subarea network and any LU in the APPN network. The VTAM host to which APPN nodes attach, or the VTAM host owning the NCPs to which APPN nodes attach, must have implemented APPN VTAM, as it is responsible (as an “interchange node”) for the conversion of subarea to APPN protocols and vice versa; other VTAMs within the subarea network may be back-level VTAMs. From the viewpoint of the APPN nodes, LUs owned by VTAMs (for example, VTAM2 or VTAM3) other than the VTAM providing the interchange function, are considered to reside on APPN end nodes.

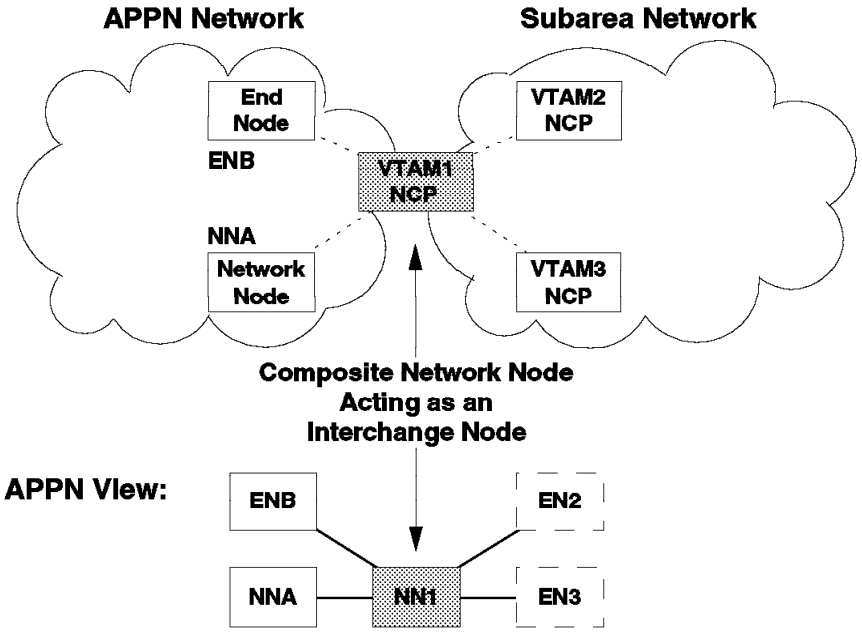


Figure 1. Composite Network Node Acting As an Interchange Node

Note: Figure 1 shows the basic form of connecting APPN and subarea networks using a composite network node acting as an interchange node.

Virtual Routing Node

APPN allows APPN nodes to reduce the addressing information stored at each node connected to a shared-access transmission facility (SATF), such as a token-ring, by allowing each node to define a virtual routing node (VRN) to represent its connection to the shared facility and all other nodes similarly configured. The SATF and the set of nodes that have defined a connection to a common virtual routing node constitute a *connection network*.

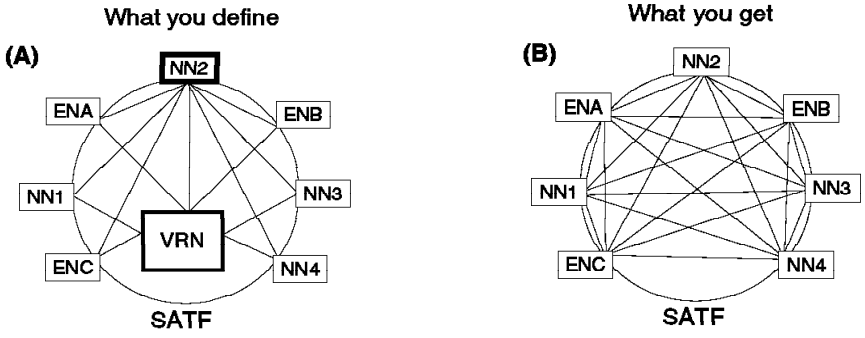


Figure 2. Virtual Routing Node

A virtual routing node (VRN) is not a node, but it is a way to define an APPN node's attachment to a shared-access transport facility. It reduces end node definition requirements by relying on the network node server to discover the common connection and supply necessary link-level signaling information as part of the regular Locate search process; LU-LU session data can then be routed directly, without intermediate node routing, between APPN nodes attached to the SATF.

Border Node

Base APPN architecture does not allow two adjacent APPN network nodes to connect and establish CP-CP sessions when they do not have the same network ID. The border node is an optional feature of an APPN network node that overcomes this restriction.

A border node can connect to an APPN network node with a different network ID, establish CP-CP sessions with it, and allow session establishment between LUs in different network ID *sub-networks*. Topology information is not passed between the sub-networks. Similarly a border node can also connect to another border node. A particular type of border node that is mentioned in this publication is the extended border node.

Extended Border Node

The extended border node allows the connection of network nodes with different network IDs and session establishment between LUs in different network ID sub-networks that need not be adjacent.

An extended border node provides directory session setup and route selection services across the boundary between paired or cascaded non-native network ID sub-networks. An extended border node can also partition a single network ID sub-network into two or more clusters or topology sub-networks with the same network ID, thus isolating one from the topology of the other.

Branch Extender

The Branch Extender Network Node (BrNN) is designed to optimize the connection of a branch office to an APPN WAN backbone network. The BrNN isolates all the end nodes on one or more branch office LANs from the backbone WAN. The domain of a BrNN might contain only end nodes and cascaded BrNNs. The domain of a BrNN does not contain network nodes or nodes with DLUR. The link on which the BEX is seen as an EN is called the *uplink*. The link on which the BEX is seen as an NN is called the *downlink*.

When configuring a BrNN, configure link stations to the backbone to be uplinks. This causes the BrNN to appear as a conventional end node to the backbone. From the perspective of the backbone, all resources in the domain of the BrNN appear to be owned by the BrNN, hiding the topology of the BrNN's domain from the backbone and reducing the number of broadcast locates in the backbone.

A BrNN presents a conventional network node interface over downlinks. End nodes in the domain of the BrNN register their resources with the BrNN and use the BrNN as a conventional network node server.

A BrNN accomplishes:

- Reduction of the number of network nodes in a large APPN network
- Hidden branch office topology from the WAN and hidden WAN topology from the BrNN
- Direct, peer-to-peer communication between defined branches connected to the same connection network
- Reduction in CP-CP session traffic on the WAN link

The following items are limitations of Branch Extender:

- Network nodes are allowed to connect only over links that a BrNN defines as uplinks.
- Only end nodes or cascaded BrNNs can be attached to a BrNN downlink.
- Border nodes acting as end nodes and DLUR nodes cannot be attached to a BrNN downlink.
- A node cannot connect to a Branch Extender over an uplink and a downlink at the same time.
- A BrNN can have CP-CP sessions with only one network node at a time.

The following CCM parameters have been added to configure BEX:

APPN Branch Extender
A node level parameter to enable the function.

Permit Search for Unregistered LUs
A branch extender normally registers all its LUs with its network node server, and indicates to the network node server that it should ***not*** be searched when the network node server is performing a domain broadcast search for an unknown LU.

Setting this parameter to YES causes the BEX to indicate to the network node server that it ***should*** be searched. You can set it to YES if the BEX node will be the network node server for an EN that does not register its LUs, so that searches can be propagated down to that EN. You can also set it to YES when the BEX node is DLUR and your network node server does not allow registration of DLUS-served dependent LUs.

Branch Uplink
This parameter allows you to define on which upstream link your node shows an EN appearance. You can define more than one link.

Link to Preferred Network Node
This parameter allows you to define which adjacent node will be your network node server. You can define more than one network node server

If the preferred network node server goes down and there is no other preferred network node server available, CP-CP sessions will be established with any available NN. As soon as a link to a preferred network node server is reestablished, the CP-CP sessions on the non-preferred network node server are forced down and then brought back up with the preferred network node server.

APPN Node Structure

This section briefly describes the structure and components of APPN network nodes, end nodes, and LEN nodes. An overview of each is presented in Figure 3 on page 14.

Node Operator

This component defines all information required by the node (for example, on links to adjacent nodes, and on LUs within its domain) and causes activation and deactivation of the node and its resources (for example, links). It may also query the status of a node's resources.

A node operator can be any of the following entities:

- A person using a system-specific dialog manager, which converts the information entered by the individual into node operator commands that are passed to the ***node operator facility***.
- A command file whose records are read and converted into node operator commands that are passed to the node operator facility.
- A transaction program. In this case, a remote transaction program communicates with a local transaction program and this local program converts the information received into node operator commands.

All three types of node operators use a program within the system to interact with the node operator facility.

Node Operator Facility

The function of this component is to allow communication between the node operator and the control point (CP), intermediate session routing (ISR), and LUs. Node Operator Facility (NOF) initializes the CP and ISR components when the node is started. It also performs functions such as the following when requested to do so by the node operator:

- Defining (creating) and deleting (destroying) LUs
- Activating and deactivating links
- Querying the CP and ISR for database and status information

Application Transaction Program

These programs communicate with other local or remote application transaction programs (TPs) to perform user-defined functions. Communication is accomplished by establishing conversations between TPs. Data is then exchanged between the TPs using an LU verb interface such as CPI-C. These verbs facilitate the task of writing a transaction program by isolating the programs from the protocol levels.

No matter what the verbs are, the tasks performed by them in a transaction program are the following:

- Allocate a conversation
- Accept a conversation
- Send data
- Receive data
- Grant permission to send
- Request a confirmation
- Grant or reject a confirmation
- End a conversation

Control Point

The function of the Control Point (CP) is to manage the resources of the node. It creates the path control (PC) and data link control (DLC) components. The CP also manages session resources and provides facilities such as directories and topology information. The CP is created by NOF when the node is started and is composed of several functions.

The following is a brief description of the CP components:

Configuration Services

Configuration Services (CS) manages the node's local resources such as links to adjacent nodes. It is responsible for the definition of ports, types of data link control (DLC), adjacent link stations, adjacent nodes and attached connection networks. In addition, the following functions are performed: link activation (including XID exchange), non-activation XID exchange (SSCP takeover, for example), link deactivation, link queries and connection networks capabilities (not supported in LEN end node). The NOF initializes, starts, stops and queries the configuration services. As it manages the local resources, it interacts with the other components of the CP, described below, and with the path control (PC) and the data link control (DLC).

Topology and Routing Services

On LEN end nodes and APPN end nodes, topology and routing services (TRS) collects information on links and adjacent nodes. In APPN network nodes, additionally, TRS collects and exchanges information on other network nodes and links between them. Furthermore, it provides the optimum route for LU-LU sessions.

Directory Services

Directory services (DS) is responsible for locating network resources throughout the APPN network. On APPN end nodes, it searches network resources in its local database first, and if the resource cannot be located, uses the services provided by the network node server that this APPN end node has a CP-CP session with. On LEN end nodes, it only searches resources in its local database, since it cannot keep CP-CP sessions with a network node.

Session Services

Session Services (SS) is responsible for activating and deactivating CP-CP sessions used by the CP components to exchange network information. Also, SS is responsible for assigning unique session identifiers to sessions, and to assist LUs in activating and deactivating sessions.

Address Space Manager

Address Space Manager (ASM) administers address space information that is used by path control to identify each individual session on a given link. This address space is a set of binary numbers, each one being 17 bits long. These numbers are used to uniquely identify a session between two adjacent nodes and are called the local form session identifier (LFSID). The LFSID, for a session being established through a intermediate node, is assigned by the ASM and passed to the session connector manager (SCM) that is a component of the intermediate session routing (ISR) function described in the next item. Also, ASM interacts with LUs and ISR at BIND/RSP(BIND) and UNBIND/RSP(UNBIND).

Management Services

Management services (MS) monitors and controls resources of a node. It can generate alerts to the network operator.

Intermediate Session Routing

The intermediate session routing (ISR) component is present only in an APPN network node. The primary function of ISR is to route session traffic received from one node and destined to another node. So, its node does not contain a destination LU. ISR is created by NOF when the node is started.

The components of the ISR are:

Session Connector Manager

Session Connector Manager (SCM) interfaces with the ASM to obtain the LFSID and the transmission group in the direction of the destination LU. Perform intermediate BIND processing.

Session Connector

Session Connector (SC) connects two stages of a session. The ISR must receive a frame and forward it to another node that can be the destination or another intermediate node. This is performed using a table that associates a source address in an incoming frame with an address on which the frame must be forwarded. These addresses are based on the LFSID of each session and are carried in the TH field of the SNA frame (specifically in the origin and destination address fields).

Logical Unit

The logical unit (LU) serves as a port into the network for one or more application transaction programs. It establishes sessions with other LUs. Conversations are allocated on these sessions that allow communication between TPs. Also, the session-level pacing is done by the SC.

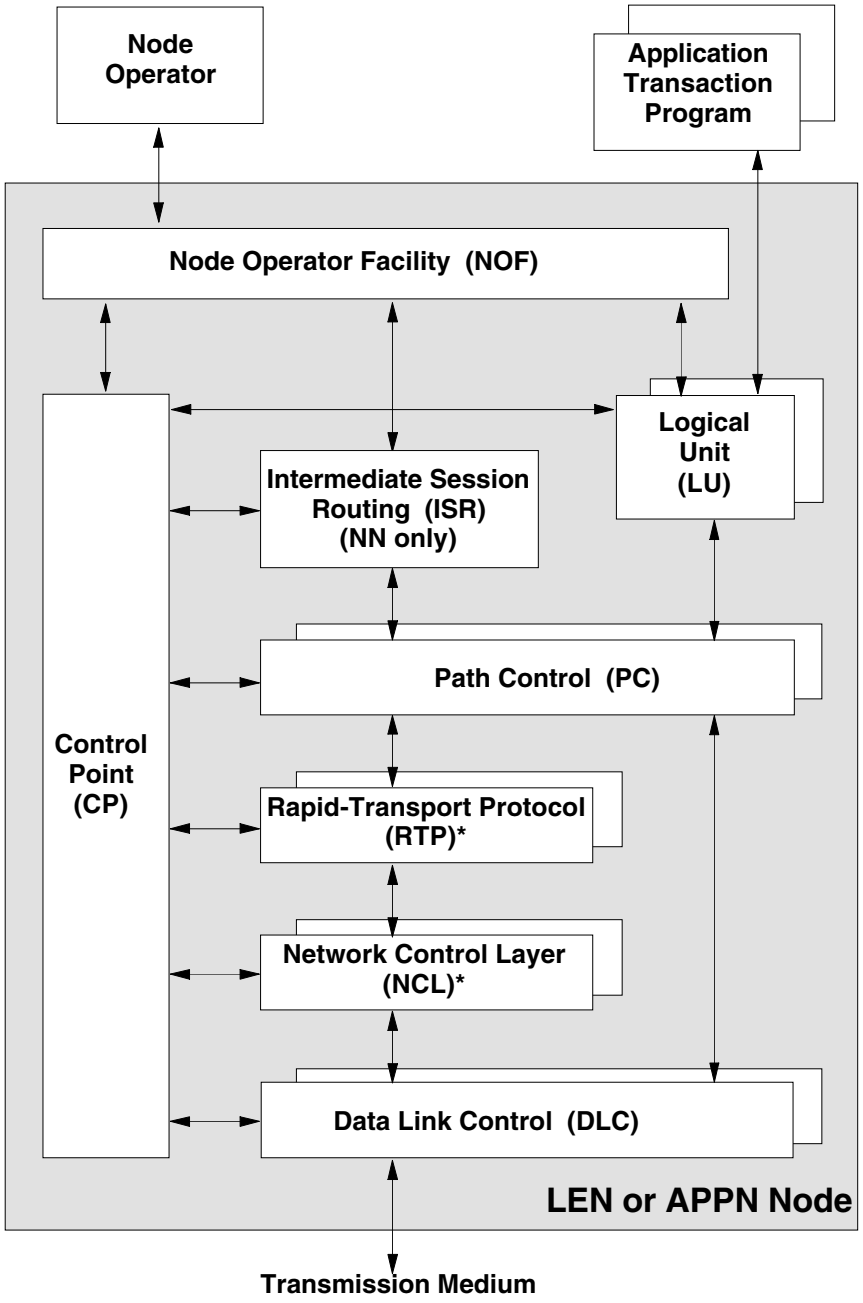
Path Control

The Path Control (PC) component routes message units from LUs, ISR, and CP within the node to DLC for transmission to adjacent nodes. Messages received by path control from DLC are routed to the appropriate component (CP, LU, or ISR). PC also routes message units between LUs within the local node.

Additionally, it performs segment generation, handles transmission priorities and performs error checking on TH.

Data Link Control

Data Link Control (DLC) provides the protocols necessary to ensure reliable delivery of messages between link stations in adjacent nodes attached to a common transmission medium. DLC also controls the node attachment to various types of transmission media.




```
Legend:
 *  =  APPN Node only
```

Figure 3. Structure of an APPN or LEN Node

Names

Resource naming is important because it allows end users to start a session without knowing the exact location of different resources within the network.

The Network Accessible Unit

In an APPN network, all components that can establish sessions with one another are called network-accessible units. Examples are CPs and LUs. The term NAU was previously used as an abbreviation for network addressable units. The terminology has changed with APPN, and now NAUs are represented by names rather than by addresses.

Within an APPN network, the names of network accessible units must be unique. To ensure the uniqueness of names within the network, a consistent naming convention is required. To make the administering of resource names easier, the network can be divided into partitions.

Network Identifiers

A partition of the network may be given a unique network identifier (net ID). Net IDs are 1 to 8 bytes long. The net ID is used throughout SNA, both in the subarea and the APPN part of a network. Because names of LUs and CPs have to be unique only within the scope of a net ID, they can be assigned and administered independently for each distinct partition of the network.

Network Names

A network name is an identifier of a network resource. Each CP, LU, link, and link station in an SNA network has a network name. The network names are assigned through system definition. In an APPN node, the system definition is done using the node operator facility (NOF).

Network-Qualified Names

A network-qualified name identifies both the resource and the network in which the resource is located. It is a concatenation of the network ID and the network name of the resource; for example, the names NETA.LUA and NETB.LUA refer to different entities.

Addresses

Network addresses uniquely identify a resource throughout the subarea network. Local addresses uniquely identify a session on a link. APPN uses local addresses. Traditional SNA subarea networking uses local ***and*** network addresses. Local addresses are used between peripheral nodes and the boundary functions of VTAM and NCP; network addresses are used when routing data between subarea nodes and bear no relation to specific sessions.

The address used in an APPN transmission header is an identifier unique on the given link for a particular session rather than the address of the NAU.

Addresses are used for routing. Routing in an SNA network uses a combination of two things:

- Information carried in the transmission header of the message
- Information stored in the intermediate node

In an APPN network, routing information is session oriented. The transmission header carries session identifiers that are locally defined for each pair of adjacent routing nodes and are only ***temporarily*** assigned. They are assigned at session

initiation, and released when the session ends. The session initiation request (BIND) carries routing information about the full session path that determines the sequence of links used from origin to destination. The local session identifier stored in each intermediate node in a session path is contained in a session connector and kept for the life of the session only.

The session identifier is associated with:

- A particular session
- A transmission group (link) between two nodes

Figure 4 shows a session between two LUs, LU1 and LU2, residing on two non-adjacent APPN end nodes. The session data is routed through two intermediate network nodes. The session can be thought of as a sequence of three session stages or "hops" with a distinct session identifier assigned to each session stage.

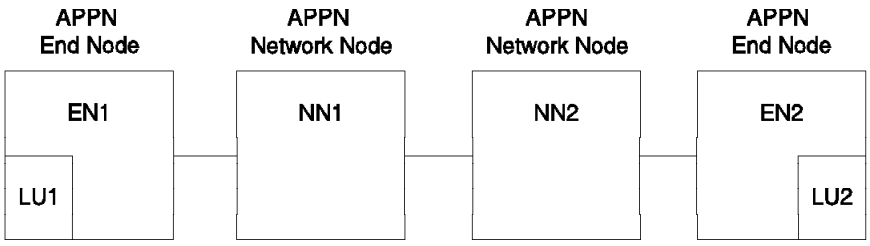


Figure 4. Session with Several Session Stages

Session identifiers vary at different session stages, which is why they are called local form session identifiers (LFSID). The LFSID is set up during session establishment by the address space manager component of the CP and assigned for the "lifetime" of an LU-LU (or CP-CP) session.

Each session is uniquely identified by a network-unique identifier, the fully qualified procedure correlation ID (FQPCID).

Domains

A domain is an area of control. A domain in an APPN network consists of the control point in a node and the resources controlled by the control point. Consequently, all APPN networks are multi-domain networks.

Although all APPN nodes are peers with respect to session initiations and do not rely on other nodes to control their resources, APPN end nodes and LEN end nodes use the services of network nodes. The domain of an APPN end node or LEN end node contains the node's own (local) resources. The domain of an APPN network node contains its local resources ***and*** the resources of those nodes that use the network node's services. Thus, the domains of the APPN end nodes and LEN end nodes are included in the domains of their respective network node servers.

Note: In traditional subarea networking, a domain is the part of the network managed by a VTAM system services control point (SSCP). Within this Redbook,

when using the term domain, we refer to an APPN domain unless explicitly stated otherwise.

High-Performance Routing

High-Performance Routing (HPR) is an extension to the APPN architecture. It can be implemented on an APPN end node or an APPN network node and does not change the basic functions of the architecture. It is intended that HPR will be implemented by making software upgrades to existing APPN products, without needing to change the hardware platform.

HPR enhances the routing mechanisms used by APPN to provide the following functions:

- HPR improves the performance over existing APPN routing, especially when using high-speed links.
- It can nondisruptively route sessions around links or nodes that have failed.
- It provides a new mechanism for congestion control that can improve traffic throughput.
- It reduces the amount of storage required in APPN intermediate nodes.

In an HPR network, a new form of routing is used, which is called automatic network routing or ANR. ANR is a source-routing protocol, which means the sender of a packet provides the information about the physical path the packet will use through the network in the network header. As HPR provides the ability to do nondisruptive path switching, the HPR architecture handles the case where the route changes in mid-session.

ANR uses a new form of addressing to identify the route through an HPR network. However, unlike the APPN session-oriented addresses (LFSIDs), the addresses in ANR are based purely on the links which make up the route. The network header contains a list of ANR labels which identify the route through the network. Each ANR label describes a link which is to be taken to exit a node.

In addition to the ANR labels, there are still addresses which are associated with sessions in HPR. Each session will have a pair of unique session addresses, one for each direction. Unlike the LFSID which identifies each stage of the APPN session, the HPR session addresses are used only on an (HPR) end-to-end basis. These are known as enhanced session addresses.

The process of supporting the end-to-end sessions across the HPR network is known as Rapid Transport Protocol (RTP).

In a network that is supporting both existing APPN nodes and HPR nodes, both the APPN and the HPR methods of addressing are used.

HPR Base and Towers

In order to facilitate implementations across a wide range of products, the following (optional) portions of HPR have been identified:

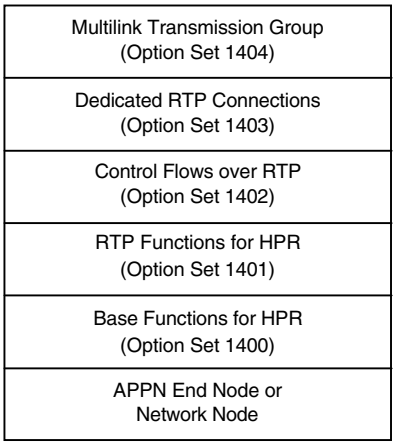


Figure 5. HPR Base and Towers

Base Functions (Option set 1400)

The primary function of the HPR base is to provide ANR routing. Products that only implement the base can participate as intermediate nodes for RTP connections. Nodes that do not support the RTP Tower cannot be the end points of RTP connections. The main function in the base is the *Intermediate ANR Routing*.

A new packet format, called a network layer packet (NLP), is used to transport data in the HPR subnet.

NLPs flowing over RTP connections may be efficiently routed through intermediate nodes using ANR routing. The CP-CP session traffic flows still use FID2 PIUs and APPN LU-LU session traffic not flowing over RTP connections will also use FID2 PIUs. Both FID2 PIUs, and NLPs may flow over a single link and are distinguished from one another by the first 4 bits in the packet.

Prior to establishing an RTP connection, a route setup protocol is done over the desired path. Link and node APPN topology update information indicates the appropriate level of HPR support by means of a new HPR control vector. Base-level nodes participate by adding the appropriate ANR information for the inbound and outbound links. When the route setup messages are exchanged between two nodes where one or both are base-level nodes, they flow in a FID2 PIU.

RTP Functions for HPR (Option set 1401)

Nodes that support the RTP functions for HPR Tower are able to transport LU-LU session traffic across HPR networks over RTP connections, thus enabling the use of HPR's high-speed ANR routing and non-disruptive path switch functions. An RTP connection can only be made between nodes that support the RTP Tower so it is essential that there be such nodes in the network. If all the HPR nodes in the network support only the base, there will be no advantages over APPN (in fact, pure APPN protocols will be used). All data flowing over an RTP connection is carried in a network layer packet (NLP). The following functions are included in the RTP Tower:

- Rapid Transport Protocol (RTP)

  This is the transport protocol used in HPR for transporting data across HPR subnets.

- Non-disruptive Path Switch

  If the current path being used by an RTP connection fails, the connection may be switched to a new path automatically. Sessions that are being transported by the RTP connection are not disrupted.

- APPN/HPR Boundary Function Support

  APPN (FID2) traffic is mapped to HPR (NLP) traffic and vice versa.

  When setting up a search for an LU, and the session to the LU over an RTP connection, the search reply will contain the ANR label of the network connection endpoint (NCE) at the end of the RTP associated with that LU.

  If the current path being used for an RTP connection fails, the RTP connection is switched to a new path (whenever possible). Sessions transported over the RTP connection are not disrupted.

  The APPN/HPR boundary function provides the mapping of APPN (FID2 PIU) traffic to HPR (network layer packet) traffic and vice versa.

Control Flows Over RTP Tower (Option set 1402)
Nodes supporting the HPR control flows over the RTP option use RTP connections (if both adjacent nodes support this option) for CP-CP sessions. When a link connecting two nodes that both support this option is activated, a long-lived RTP connection is established that is used to forward route setup messages.

Dedicated RTP Connections (Option set 1403)
See “Rapid Transport Protocol” on page 20.

Multilink Transmission Group (Option set 1404)
See “Multilink Transmission Groups” on page 23.

HPR Link Support

Since HPR is an enhancement of APPN it will operate over links supported by today’s APPN, supporting both APPN and HPR traffic on the same link. That means that existing hardware adapters and DLCs currently being used for APPN communications can continue to be used for HPR.

During link activation, DLCs are used by HPR in the same manner as by APPN. That is, XID3s are exchanged and the appropriate set mode signals are sent when the exchange is complete. For HPR, a new control vector is included in the negotiation-proceeding XID3 that contains additional HPR-specific information. If both sides include the new control vector, the link is referred to as an HPR link. If both nodes indicate support for the HPR transport option, then HPR transport option protocols are used; otherwise, HPR base protocols are used.

CP-CP sessions are established in the same manner as in APPN when the link is activated.

Immediately after an HPR link is activated and both nodes support the HPR control flows over RTP option, a long-lived RTP connection is established across the link for route setup and CP-CP control flows. This RTP connection remains active as long as the link remains active (hence the “long-lived” RTP connection).

To avoid the necessity to segment the transport layer header, the minimum "maximum packet size" that has to be supported for an HPR link is 768 bytes. For performance reasons it might be advisable to support larger packet sizes.

Automatic Network Routing

Automatic network routing (ANR) mode is a low-level routing mechanism that minimizes cycles and storage requirements for routing packets through intermediate nodes. ANR routing is significantly faster than current APPN routing. No intermediate node storage is required (APPN requires 200-300 bytes per session) and no precommitted buffers are necessary, which APPN recommends should be used.

HPR uses the ANR routing mode to route session traffic, including binds and unbinds, through an HPR network between nodes supporting the high-performance routing transport option.

HPR employs a route setup protocol in order to obtain ANR and RTP connection information of the selected path.

Each packet is routed through the network as a self-contained unit and is independent of all other packets. There is no table lookup or processing necessary at transit nodes such as the LFSID swapping procedure used by APPN. Any processing of packets required at the network connection and transport connection sub-layers is the responsibility of the origin and destination end points of the packets. End point processing includes flow control, segmentation and reassembly, and recovery of lost packets.

ANR is designed to be simple enough so high-performance switching can be accomplished. A major goal is to optimize the design for hardware implementation to get the appropriate performance level that is required by the new generation of high-speed networks.

Rapid Transport Protocol

Rapid Transport Protocol (RTP) is a connection-oriented, full-duplex protocol designed to transport data in a high-speed network. HPR uses RTP connections to transport LU-LU and optionally CP-CP session traffic.

Rapid transport protocol provides end-to-end error recovery with selective retransmission, non-disruptive path switch and adaptive rate-based (ARB) flow control. RTP may be implemented on network nodes or end nodes.

The physical path utilized by the RTP must satisfy the class of service (COS) associated with the session traffic it is carrying. Session traffic is carried over the RTP connection in such a way that intermediate nodes are not aware of the SNA sessions, or even the transport connection itself. Traffic from many sessions may be carried by a single RTP connection, provided they all use the same COS. An RTP connection provides two important advantages:

1. It transports data at very high speeds by using low-level intermediate routing and by minimizing the number of flows over the links for error recovery and flow control protocols. The flows are minimized by performing these functions at the RTP connection endpoints rather than at each hop (link) along the path. Data resequencing takes place at the RTP end points.

2. An RTP connection's path may automatically be switched to reroute data around a failed node or link without disrupting the sessions. The new path for the RTP connection is selected that best fits the same class of service as the failed connection. Higher layer protocols are not even notified of the rerouting.

The end points of an RTP connection must support the RTP transport option, whereas intermediate nodes need only support HPR base functions. APPN session end points can be in APPN or HPR nodes.

Class of Service

RTP connections are used to transport session data between HPR nodes operating within an HPR sub-network. They provide a full-duplex logical connection or *pipe* between two HPR nodes over a specific path through the HPR sub-network.

Each RTP connection transports session data between two RTP-capable end points for a single class of service (COS) as specified in the BIND. An RTP connection is not used for more than one COS, in order to simplify the route selection process during path switching. A node may activate multiple RTP connections (using different paths) to the same partner node for the same COS in order to distribute the traffic over multiple physical paths.

The same RTP connection that was activated by a node to carry sessions to the remote node may be used for the remote node to establish its sessions along. All traffic from an individual session flows over a single RTP connection, but many sessions may be multiplexed over a single RTP connection. All sessions requesting the same COS and following the same path through the HPR sub-network are transported over a single RTP connection between the HPR nodes containing the session end points.

ARB Flow Control and Congestion Control

In HPR, sessions with the same COS are multiplexed over a single RTP connection. The ARB flow control mechanism, used by RTP, addresses the fairness issue among multiple RTP connections through the network. It does not address the fairness issue among multiple sessions using one RTP connection.

In order to provide this fairness, we not only use the ARB mechanism for RTP connections but also use the existing session pacing over an RTP connection to prevent one session from monopolizing buffers in the two RTP components. In an APPN sense, the RTP connection can be seen as one stage (hop) on the session path.

The APPN hop-by-hop Windows-based flow control protocol, known as adaptive session pacing, is inadequate for high-speed data routing. HPR uses a protocol suitable for high-speed routing called adaptive rate-based (ARB) flow/congestion control. It regulates the flow of data over an RTP connection by adaptively changing the sender's rate based on feedback on the receiver's rate. This protocol allows for high-link utilization and prevents congestion before it occurs.

The input traffic entering the network is regulated by the ARB algorithm based on the conditions in the network and the partner RTP end point. An increased delay and decreased throughput indicates that congestion is occurring, and so input traffic is reduced. When the capacity of the network or partner RTP end point increases, input traffic is increased.

The ARB algorithm is designed to ensure that maximum throughput is attained. The ARB algorithm has the following properties:

- It adapts to network conditions in such a way as to maximize throughput and minimize congestion. It therefore operates within the operating region.
- It smooths the input traffic into the network, avoiding bursts when the physical capacity of the access link to the network is larger than the allowed input rate. This prevents long queues from developing in the network and helps minimize oscillation in the network traffic patterns.
- It provides end-to-end flow control between the RTP end points so that one end point does not flood the other.
- It requires minimum overhead in both processor cycles and network bandwidth.
- It provides equal access, or fairness, to all RTP connections.

The ARB algorithm is implemented on the RTP end points of a connection. There are two components at the RTP end points, an ARB sender and ARB receiver. The intermediate nodes have no awareness of the ARB protocol and therefore do not participate in it.

The sender continually queries the receiver by sending a *rate request* along with the data in order to determine the state of the network and state of the receiver node. The sender may reduce or increase its send rate depending upon the information it gets in the *rate reply* received from the receiver. Fixed characteristics, such as speed of the slowest link in the path and transmission time, are factored into the algorithm when the RTP connection is set up. These path characteristics are communicated by using an ARB *setup* message. Either RTP end point may send a setup message as a result of a path switch.

RTP Alive Timer

The RTP *Alive* timer is used to make sure that both the partner end point of the RTP connection and the path between the end points are operational after a period of inactivity. When this timer expires and no packet has arrived from the partner since it was last set, a packet with a status indicator will be sent and the SHORT_REQ timer is started. Should a status segment be received from the partner, the SHORT_REQ timer is stopped. Otherwise, when the SHORT_REQ timer expires the status request is retransmitted. After a predetermined number of retries and no response, an attempt will be made by the sender to find a new path for the connection. If the partner is not operational or there is no suitable path to the partner, the sender will eventually terminate the connection.

The purpose of the Alive timer is as follows:

- Keep limited resource links active, where limited resource links are automatically deactivated in HPR when no traffic flows over the link for a specified period of time. So when there is no session traffic, RTP sends *liveliness* messages at intervals set by the Alive timer.
- If the partner RTP end point or a link on the path fails, and the RTP end point is idle awaiting session traffic from the partner, then the RTP connection is “hung.” The Alive timer triggers a liveliness message that is used to detect this condition. Such a detection triggers a path switch.

Nondisruptive Path Switch

The HPR path switch function is used to automatically route data around a failed link or node. This function only operates within an HPR sub-network and is supported by all HPR network nodes and end nodes. When a failure occurs and an alternate path exists that satisfies the class of service for the failed RTP connection, a new RSCV is calculated and the RTP connection is switched; session traffic will be rerouted over the new path without disrupting the existing sessions.

Multilink Transmission Groups

A multilink transmission group (MLTG) consists of multiple DLC-level connections between two nodes made to appear to higher layers as a single connection. An MLTG is available for service as long as one or more of its constituent links are available.

Multilink transmission groups are supported in traditional subarea SNA networks and in APPN HPR networks, but not in base APPN.

Although superficially similar to multilink transmission groups in subarea networks, MLTGs in APPN HPR networks are significantly different in operation. This section describes HPR MLTGs.

HPR MLTG Requirements

Multilink transmission groups (MLTGs) have advantages over single-link TGs and parallel TGs in a number of cases:

Where the traffic demand can exceed existing TG capacity

Traffic demand can exceed existing TG capacity when a single session reaches the point at which it needs more bandwidth than the TG can provide. Aggregate available bandwidth can be raised simply by the addition of more links dynamically. If the demand subsequently falls, the extra bandwidth can be taken back by deletion of the extra links, saving network charges. Parallel TGs cannot help in this circumstance.

The need may also arise because of varying loads placed on a TG by a collection of sessions, rather than any single session. In this instance, adding parallel TGs ***might*** be an alternative solution, or not, depending on class-of-service and route selection implementations. But a single session could not use more capacity than the link offers that carries this session.

Where multiple lower-speed links are less expensive than a single higher-speed link

There are cases where multilink transmission groups prove less expensive than single-link TGs. In certain countries circuit capacities of 64 kbps and 2 Mbps are available, but nothing in between. If you live in one of these countries and have to provide 100 kbps of bandwidth, for example, you may find it costs less to put two 64-kbps links into a multilink transmission group than to have a single 2-Mbps link.

Where individual links are unreliable

Although HPR provides a fast nondisruptive path switch capability, not even this will be necessary if your TGs never fail. If you are considering MLTGs to avoid TG failures, however, you must plan for the potential effects of temporarily reduced TG capacity. When one of several active

links in an MLTG fails, effective capacity will be reduced even though the TG does not itself fail.

Where you have a subarea network including multilink transmission groups
If you have grown used to having the multilink transmission group facility in subarea networks you may feel more comfortable about migration to APPN HPR, knowing a similar facility is there.

Additional design objectives of the MLTG architecture include:

- The need to support mixed link types within MLTGs

  All supported SNA link types are also supported in HPR MLTGs.
- The need to support mixed link speeds within MLTGs
- The need to minimize system definition.

HPR MLTG Overview

The critical parameter determining whether two links belong to one MLTG or to two parallel TGs is TG number (given of course that the links connect the same pair of nodes). If the links share the same TG number, then they belong to an MLTG; if they have different TG numbers, then they belong to parallel TGs. In this regard, subarea SNA and HPR do not differ.

One of the architectural problems with subarea multilink transmission groups was the need for resequencing of packets. Higher layers required DLC to guarantee delivery of packets, hop-by-hop, and to guarantee FIFO order. This dictated, among other things, that SNA subarea nodes had to act as *store-and-forward* switches, being unable to make forward routing decisions until entire packets had been safely received. It could easily happen that two packets, transmitted on different links within a multilink transmission group, would reach this point in reverse order of their initial order. The receiving node would have to buffer the second packet, pending the arrival of the first. This TG resequencing function could impose large processing overheads, especially where there were widely varying line speeds, propagation delays, or packet lengths, or where there were significant line error rates. In today's high-speed networks, resequencing delays en route would be unacceptable.

HPR eliminates the need for TG resequencing and for hop-by-hop error recovery by shifting these functions to RTP end points. When a VR-based transmission group (VR-TG) crossing the subarea network includes a subarea multilink transmission group, resequencing is not done for HPR network layer packets transported over that subarea MLTG.

In the HPR MLTG architecture, error recovery on individual links is optional, and TG resequencing in route is absent. Because FID2 packets have to be transmitted reliably and in sequence, HPR MLTGs do not support any FID2 traffic. HPR MLTGs must carry ANR network layer packets exclusively. This means, in turn, that RTP connections must be used for CP-CP sessions and route setup flows. Both nodes connected by an HPR MLTG must hence support the control flows over RTP option.

As regards routing and ANR labels, MLTGs are treated the same as single-link TGs. See "Automatic Network Routing" on page 20. An MLTG is assigned one ANR label for each direction.

MLTGs and single-link TGs are also considered alike by TRS when it comes to the generalities of topology databases, TDUs, and route calculations. Differences show up when an MLTG's characteristics change ***in flight***; for instance, when a new link is added. Such circumstances cannot arise in single-link TGs. When MLTG characteristics do change, topology database records are modified and TDUs generated.

Some functions are not supported in HPR MLTG:

- Limited resource
- Connection networks
- Non-activation XID.

Much of the HPR MLTG architecture revolves around the handling of TG number and other characteristics governed by XID3 exchanges during link activation. In particular, it deals with the exceptions that can occur when differently defined links are put together.

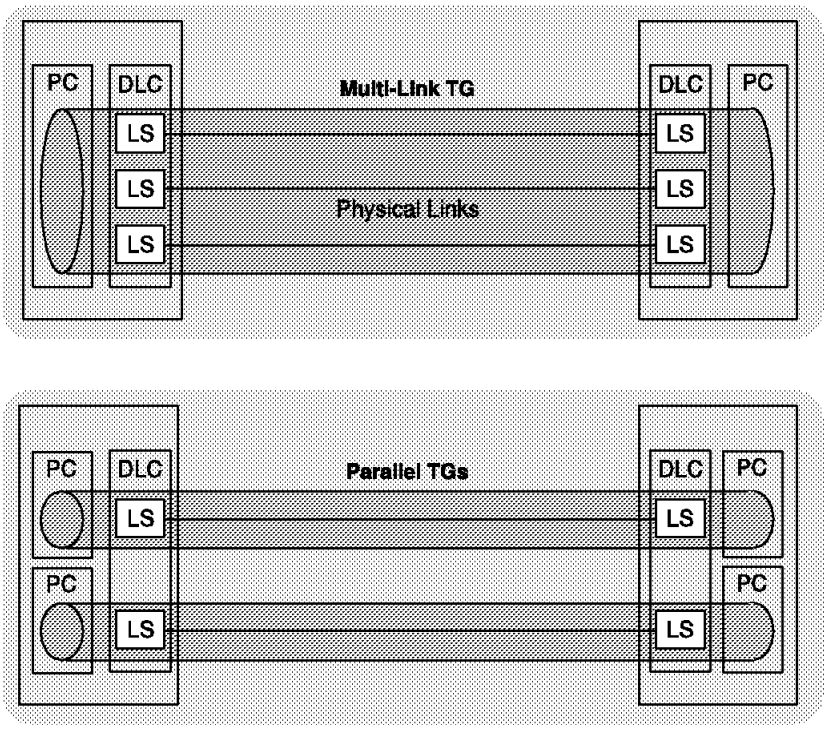


Figure 6. Multilink and Parallel TGs

Priority

HPR uses the same transmission priorities as the base APPN architecture (low, medium, high, and network). Transmission priority is associated with a class of service (COS). APPN has a set of architecturally defined COSs, each having a specified transmission priority. For example, the CPSVCMG COS, used by CP-CP sessions, has a transmission priority of network (the highest). COSs that are not architecturally defined may be used for LU-LU sessions; these COSs are associated with the priority of the session, either high, medium, or low.

APPN intermediate network nodes provide priority queues to allow higher-priority traffic to be routed before lower-priority traffic. The transmission priority function is also provided for packets flowing on RTP connections. Each RTP connection is associated with a COS and, therefore, has an assigned transmission priority.

Route Calculation

The APPN route calculation algorithm is used by HPR. HPR links are marked in the topology database, and the routes (paths) within HPR networks are specified with ANR labels instead of transmission group (TG) numbers and CP names. Nonetheless, the algorithm to compute these paths is unchanged.

The APPN architecture provides various means that could be used to make HPR links preferred to regular APPN links. Here are two examples:

- HPR links can be made to have better characteristics in terms of cost, delay, and so on, than APPN links even if the physical link characteristics are the same.
- Another possibility would be to use the user-defined fields in the COS tables and link characteristics to give HPR links smaller weights. The route calculation algorithm is then more likely to choose HPR links than APPN links.

However, as the routing decision is not a local optimization (within a node), but rather a global one (within the network), a small change in a link's characteristics may change the whole network's distribution of traffic. As a result, by artificially lowering the weight of an HPR link, the network could route all its traffic through that link causing a network collapse.

Therefore, when a node activates an HPR link, the link characteristics, which is broadcast as part of the topology function, should accurately characterize the link, and the node should not artificially modify the link characteristics.

To take full advantage of the HPR function:

- Adjacent APPN nodes should be upgraded. HPR-HPR-APPN routes are better than HPR-APPN-HPR routes.
- Links with the heaviest traffic, for example backbone links, should be added to the HPR network first.

In summary, this architecture allows seamless migration from an APPN network to an HPR network.

HPR-Only Route For Path Switch

When a time-out is detected while attempting to transmit data or Alive messages, RTP requests a new path from route selection services (RSS). If the new path between the two RTP end points contains one or more APPN links, that is, supporting only ISR function, the path switch will fail and the sessions traversing that RTP connection will be deactivated. This is not the case if there is a path between the two nodes that uses only HPR links. Because of the importance of session availability, a best-fit, HPR-only path is used, even if it does not match the required COS weight.

Timers

HPR uses timers to ensure that non-operational paths do not consume useless bandwidth to the detriment of other traffic. The timers are:

- Alive timer
- Short_req timer
- Path switch timer.

Each is described in more detail below.

Alive Timer

This user-defined timer ensures that both end points of an RTP connection and the path between them are still operational after a period of inactivity. When this timer expires and no packet has arrived from the partner since it was last set, an are_you_there packet is sent to the partner and a short_req timer is started. There are then two possible actions:

- If a response is received, the short_req timer is stopped.
- If the short_req timer expires, the are_you_there packet is resent.

If no response is received after a specified number of retries, a path switch is attempted.

Note: Both the Alive time and number of retries can be configured via CCM.

Short_req Timer

This timer is used for error recovery by RTP. Each RTP end point periodically "tags" a frame with a "request status" and waits for a response from the other end point. If no response is received with the time set in this timer, another frame is tagged and the wait starts again. This tag and wait cycle is repeated until a response is received or specified number of tags have been attempted.

The initial value of Short_req is 1 second (not configurable) and is computed regularly by RTP based on the round trip delay [old name: Round Trip Time (RTT)]:

```
Short_Req = (0.9 x Previous_Short_Req) + (1.8 x RTT).
```

Path Switch Timer

This timer is used to monitor the length of time that RTP should attempt a path switch for a connection before failing the patch switch.

Three path switch timers can be configured in the 3746 via CCM, one per transmission priority (high/medium/low). This improves the detection time of path switch failures for high-priority connections.

Migration

The following features of HPR ease migration from APPN:

- Inter-operation with existing APPN nodes
- No configuration restrictions (*drop-in* migration)
- Use existing APPN Control Point protocols and algorithms
- Shared topology.

Each is described in more detail below.

Inter-operation with Existing APPN Nodes

Transforming APPN protocols into HPR and vice versa is done by the *APPN/HPR boundary function*. This function provides all the necessary transformations to allow APPN-level nodes and HPR-level nodes to inter-operate seamlessly.

No Configuration Restrictions

New HPR nodes may be added and existing APPN nodes may be upgraded to HPR in any manner desired. There are no configuration restrictions whatsoever (drop-in migration). However, the benefits of HPR do not appear until contiguous clusters of HPR nodes, *HPR subnets*, are formed.

HPR Uses APPN Control Point Protocols and Algorithms

HPR uses the control point (CP) protocols of APPN (directory, topology, CP capabilities, and so on). CP-CP sessions are employed, just as in APPN, to transport these protocols. The APPN route selection algorithm, with a modification to calculate HPR-only paths for the path switch, is also used by HPR. Using existing APPN control flows significantly reduces the amount of code required for migration, that is, to implement the APPN/HPR boundary function.

Shared Topology

All nodes and links are reflected in every APPN and HPR network node's topology to facilitate migration and network management.

Migration Planning

The benefits appear when you have at least one HPR subnet operating, see "Route Calculation" on page 26. You could start by nominating for HPR operation either:

- The longest chain of HPR capability.
  1. List all HPR-capable stations and nodes.
  2. Starting from a VTAM host, work outwards to the furthest HPR-capable unit. That becomes your first HPR subnet, or chain of subnets.
  3. Using *CCM User's Guide*, SH11-3081, define all the required 3746 Network Nodes and stations as HPR-capable.
- The links with the heaviest traffic, either by current or predicted performance, then work outwards to adjacent APPN nodes.

Dependent LU Requester/Server

Figure 7 on page 29 is used as reference in this section.

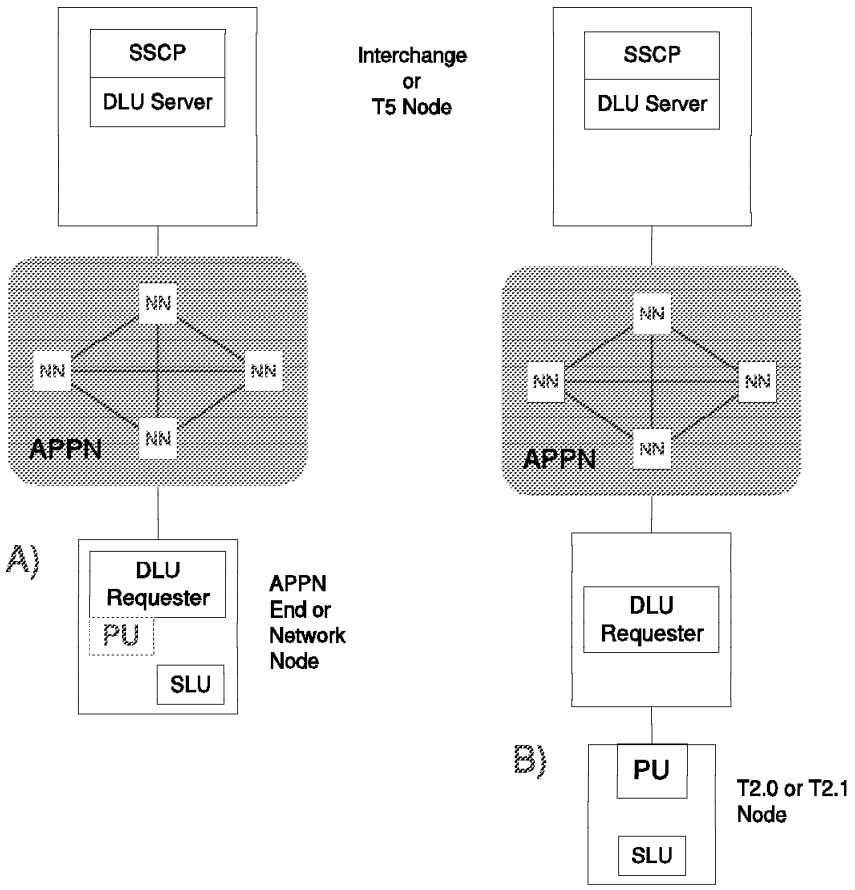


Figure 7. Dependent LU Requester/Server.

A) The dependent LU requester in the same node as the dependent LU(s).
B) The dependent LU requester in an APPN end node or network node directly connected to the PU T2.0 or APPN or LEN node containing the dependent LU(s).

The dependent LU requester (DLUR) and dependent LU server (DLUS) functions allow SSCP-PU and SSCP-LU data to flow through an APPN network. The session establishment data for dependent LUs flows on top of two APPN LU6.2 sessions. (For each one of DLUR and DLUS, there is one *contention winner* session and one *contention loser* session.) From the DLUR function to the dependent PU, the flow is the same of the NCP or VTAM boundary function to a PU (ACTPU, ACTLU, BIND, and so on).

The dependent LU server function (option set 1066) is a product feature of an interchange node or a T5 network node supporting session services extensions. This function provides server support for dependent LU requester clients in which SSCP-PU and SSCP-LU flow to a PU T2.0 or APPN or LEN node externally attached to the requester, or a PU T2.0 or APPN or LEN node image within the requester, are encapsulated within LU 6.2 sessions.

The dependent LU requester function (option set 1067) is an enhancement to an APPN end node or network node. This function is the client side of the dependent LU server function in which SSCP-PU and SSCP-LU flows to a PU T2.0 or APPN

or LEN node attached to the requester are encapsulated within LU 6.2 sessions as mentioned previously.

The requester function provides a remote boundary function for dependent LUs. This option set relieves the restriction that PU T2.0 nodes be directly attached (or bridged, or data link switched, or frame relayed) to the VTAM or NCP boundary function. The dependent LU requester function may reside in the same node as the secondary LU or be provided by a node adjacent to and upstream from the secondary LU (see Figure 7 on page 29).

For a more detailed discussion of the DLUR function see *Inside APPN with HPR: The Essential Guide to New SNA* SG24-3669, and *Subarea to APPN Network Migration Experiences*, SG24-4656.

Note: Bisynchronous (BSC) 3270 sessions are not supported over APPN links. If BSC sessions are required, you must maintain subarea paths to all potential session partners.

3746-9x0 APPN/HPR Network Node Implementation

This section describes details of the APPN features implemented by the 3746-9x0 APPN/HPR Network Node.

Terminology and Implementation Specifics

The 3746 NN is composed of a 3746 frame connected via a dedicated token-ring LAN to its service processor (SP) and network node processor (NNP). The token-ring LAN used for communication between the NNP and the service processor is referred to as the service LAN. The SP and NNP each contains a token-ring adapter attaching them to the same service LAN. MOSS-E traffic travels over the SP adapter onto the service LAN. Likewise APPN traffic session establishment traffic travels over the NNP adapter onto the service ring. Note that APPN user traffic does ***not*** flow on the service ring.

Figure 8 on page 31 depicts how the APPN functions are split up between the network node processor (NNP) and the adapters within the 3746 frame.

Note: Adapter means the CLP, TRP2, ESCP2, or CBSP2 processor and the associated line interface (LIC), token-ring interface (TIC3), Ethernet interface (TIC3 bridged), or ESCON® (ESCC) couplers.

Node Operator Facility (NOF) functions (for example, port and link activation), APPN topology and routing services, and session establishment tasks are executed in the NNP, while intermediate session routing (user traffic) is done within the 3746 adapter.

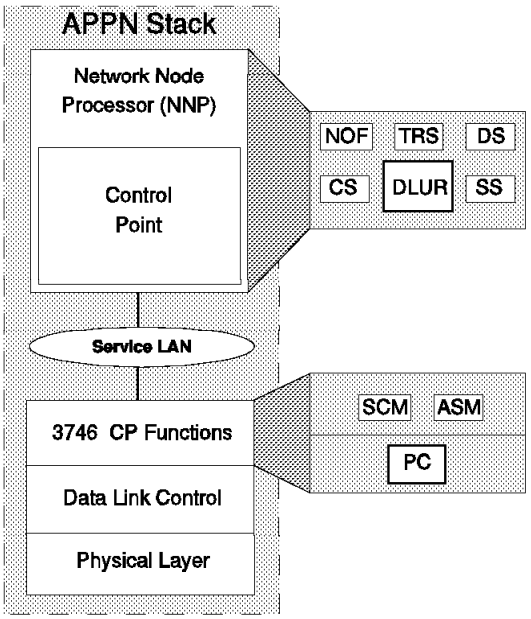


Figure 8. 3746 NN Structure. A full APPN stack is composed of functions performed on the network node processor (NNP) and within the 3746-9x0.

The APPN functions that run on the network node processor are:

- NOF - Node Operator Facility
- TRS - Topology and Routing Services
- DS - Directory Services
- CS - Configuration Services
- SS - Session Services
- DLUR - Dependent LU Requester

APPN functions performed within the 3746 adapters are:

- DLC - Data Link Control
- PC - Path Control
- ASM - Address Space Manager
- SCM - Session Connector

The following section details how these components inter-operate during session establishment and routing for APPN (independent LU 6.2) sessions.

Session Establishment and Routing

During APPN session establishment, CP functions on the NNP participate in locating session partners and are responsible for APPN route calculation. Figure 9 on page 32 depicts how CP-CP session data flows between the NNP and the control points of adjacent nodes.

Irrespective of the coupler the node is connected to, CP-CP data will always traverse:

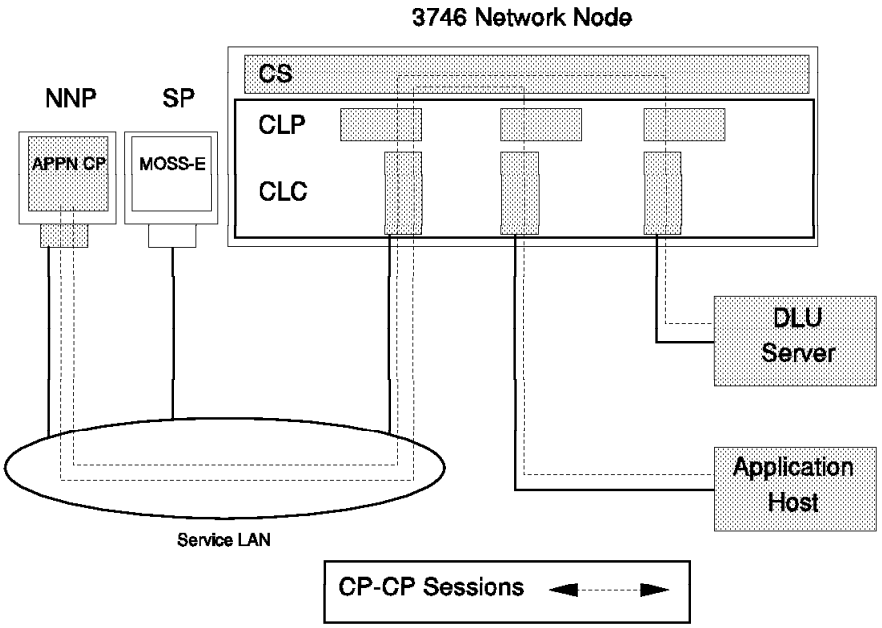
- The adapter (coupler and processor) that the APPN node is attached to
- The connectivity switch (CS)
- CBSP2
- Token-ring port 2080
- Service LAN

Note: In only two cases CP-CP session data will not traverse the connectivity switch:

1. When APPN nodes connect via token-ring port 2080

   However, with the introduction of the APPN NN functions the attachment of user equipment via the service LAN is no longer supported.

2. When using an internal APPN link between the 3746-900 NN and any of the CCUs of the attached 3745 Models A




```
Legend:
CS   =  Connectivity Switch
CLP  =  Communications Line Processor
CLC  =  Communications Line Coupler
NNP  =  Network Node Processor
SP   =  Service Processor
```

Figure 9. CP-CP Sessions

The BIND, which is the first SNA request unit flowing on the newly calculated route between two session partners, will trigger the address space manager (ASM) function running on the 3746 processors to assign LFSIDs. In addition, a session connector (SC) will be generated to enable intermediate session routing on the 3746 NN. The SC can be an intra-processor (within the same 3746 processor), or an inter-processor (between two different processors connected via the 3746 connectivity switch [CS]). See Figure 10 on page 33.

Figure 11 on page 34 illustrates the data flows during and after session establishment. End node A (EN A) is token-ring-connected to 3746 NN, while end node C (EN C) is SDLC-connected. In both cases the 3746 NN (NN B) is providing the network node server function, having CP-CP sessions with both end nodes.

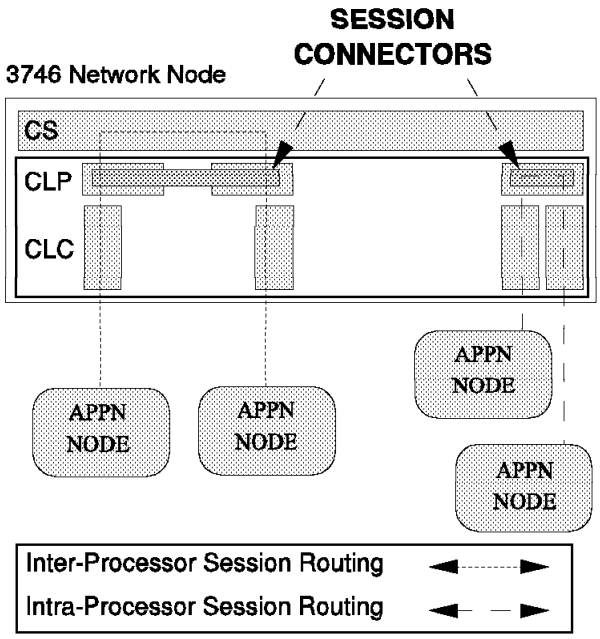


Figure 10. Intermediate Session Routing

To locate the session partner and calculate the best session path, APPN functions within the NNP are invoked. Initiated by the BIND, CP functions available on the 3746 processors will assign local form session identifiers (LFSIDs) for this session and generate a session connector (SC). Note that for this session an inter-processor SC applies. If both EN A and EN C were connected to couplers controlled by the same processor, an intra-processor SC would result.

When the 3746 NN is performing intermediate session routing, the session connector manager (SCM) performs the LFSID swapping required to forward session data.

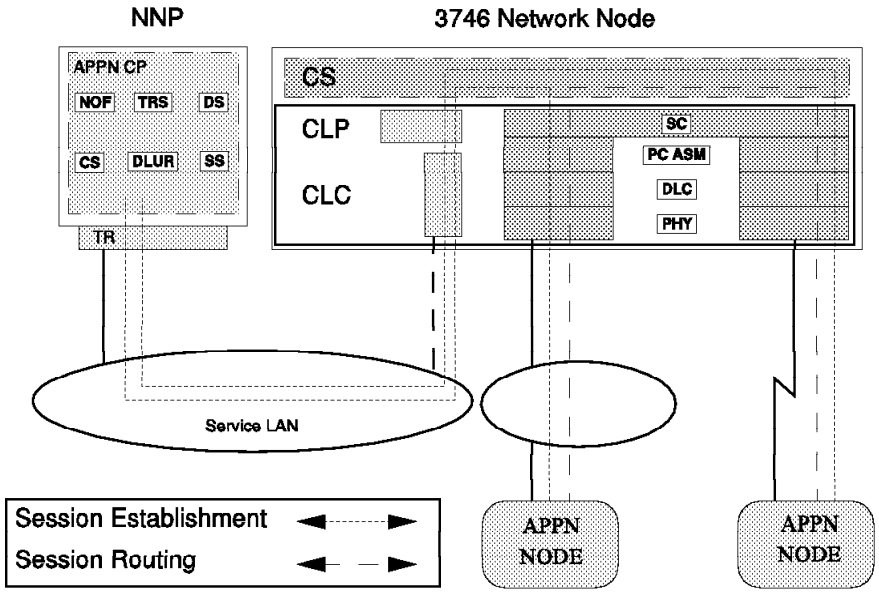


Figure 11. 3746 NN Intermediate Session Routing. All shaded components are involved in session setup. The dark-shaded components are also involved in intermediate session routing.

In order to provide the network node function in the 3746-9X0, the network node processor feature is used. This provides the network node processor (NNP) hardware resources and the licensed internal code required to support the APPN network node functions.

The NN processor feature includes the APPN CP and the APPN NN configuration control and management software (CCM) along with the hardware and token-ring interface. A keyboard and a display are not required on the network node processor; access is provided from facilities available on the service processor (SP).

Functions running on the control point can be accessed from the service processor. To allow configuration and management of the APPN NN functions the configuration control and management (CCM) tool, which runs on the SP, is used.

3746 Network Node Processor Backup

To provide additional resilience a second network node processor can be installed. The backup control point also attaches to the service LAN and can take over the functions from the primary control point. This process is controlled from the service processor; the CP backup can be done either manually or automatically. In case of a malfunctioning primary control point no new sessions can be established. To allow new session establishment, either the primary CP needs to be restarted, or the backup CP must take over. Once the original failing NNP again becomes available, it will be regarded as the backup network node processor.

Network Node Connectivity

Refer to the *3745 Communication Controller Models A and 170, 3746 Nways Multiprotocol Controller Models 900 and 950: Overview*, GA33-0180 for information about:

- The number of PUs, frame-relay DLCIs, and sessions available on the 3746-9x0
- The total number of PUs, APPN and dependent LU sessions, and lines that a 3746 network node can handle (no matter what type 2 adapter configuration is used)

DLC Support of Error Recovery

Network layer packets (NLPs) may be sent over an HPR link using link-level error recovery procedures or not. (Note that FID2 PIUs always use the link-level error recovery procedures, just as in APPN.) Whether or not error recovery is used on NLPs is determined during the initial exchange between adjacent nodes:

- Using link-level error recovery

  NLPs are transmitted in the same manner as in APPN where the LLC elements of procedure provide full error recovery. For HPR, this is recommended for links with high error rates.

- Not using link-level error recovery

  NLPs are transmitted in a manner such that the LLC will not perform any error recovery for it. This mode of operation is recommended for low error rate reliable links. The method for bypassing the link-level error recovery mechanisms varies depending on the link type (see descriptions of each link type below).

The following sections describe the link types currently supported by the 3746.

Token-Ring: Both *link-level error recovery* and ***no error recovery*** are supported in the 3746, but you are recommended to use *no error recovery*. HPR provides the capability to bypass error recovery for NLPs on LANs using 802.2. From an architecture point of view, a separate service access point (SAP), different from the SAP currently used to transmit APPN traffic, could be used to transmit NLPs with no link level error recovery. NLPs requiring link-level error recovery use the same SAP as existing APPN traffic. However, in the 3746, HPR SAP (error recovery or no error recovery) is identical to the APPN SAP for this port. All traffic, both error recovery and non-error recovery ones, travel over the same physical path. And, if that physical path is switched (due to link-level switching) to a new one, the new path is then used for all traffic.

Frame Relay: Both link-level error recovery and no error recovery are supported in the 3746, but you are recommended to use no error recovery especially on good quality lines. In the 3746, HPR SAP (error recovery or no error recovery) is identical to the APPN SAP for this port).

SDLC: There are no changes required in order to run HPR over SDLC. SDLC is run exactly as it is run without HPR, that is, ***only link-level error recovery*** is supported in the 3746.

X.25: The X.25 protocol always provides error recovery between a DTE and a DCE using the LAPB procedure. HPR runs over X.25 using the same QLLC protocol as the regular APPN traffic.

Neither the X.25 standard protocol nor the IBM QLLC protocol have been modified to transport HPR traffic.

ESCON: Only link-level error recovery is supported in the 3746.

Dependent LU Requester Implementation

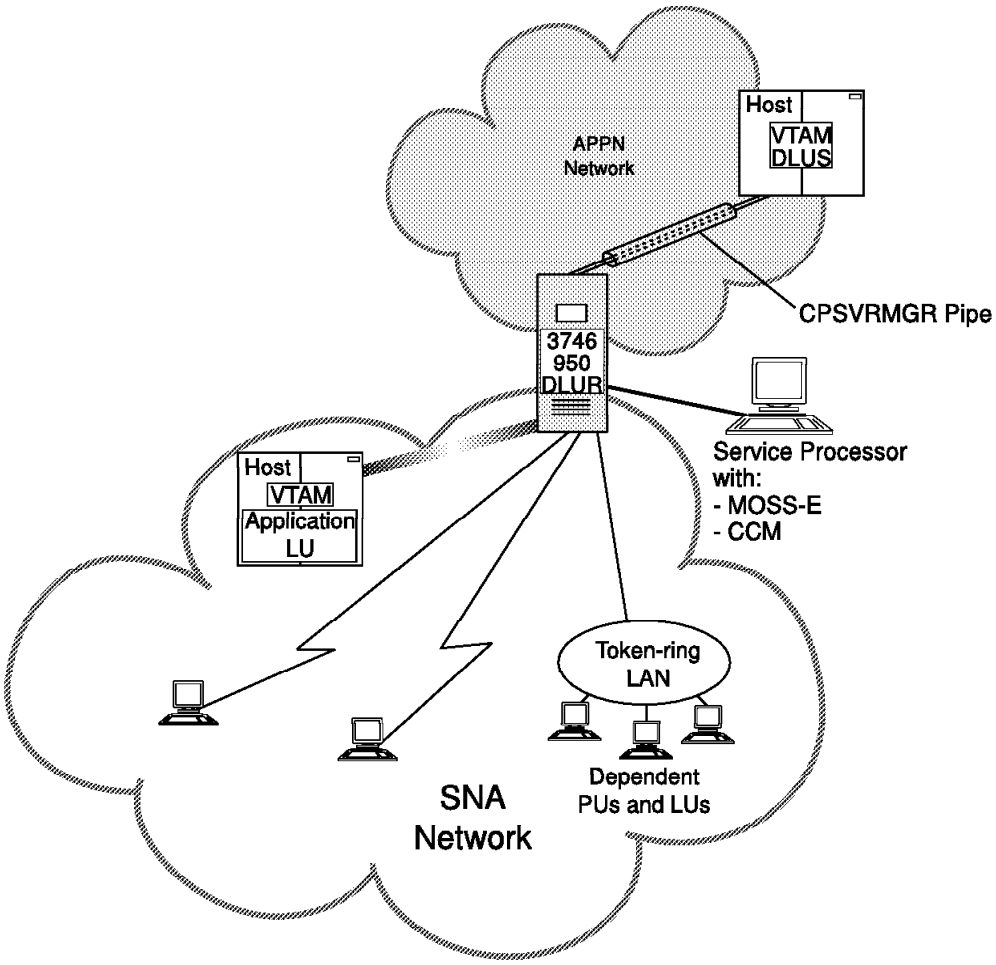


Figure 12. 3746 Network Node DLUR Connectivity

The Dependent LU Requester (DLUR) function facilitates conversion from a subarea environment to an APPN environment, allowing you to maintain central management of remote dependent LUs while benefiting from APPN throughout a network.

Two LU 6.2 sessions (one inbound, one outbound) are established between a DLUR and a Dependent LU Server (DLUS). These LU 6.2 sessions are collectively known as the CPSVRMGR pipe. SSCP-PU and SSCP-LU session flows use the CPSVRMGR pipe. An SSCP-PU session is established between a VTAM network node and the PU that owns the dependent LU, and an SSCP-LU session is established between VTAM and the dependent LU. Session initiation flows for the

dependent LU are sent over the SSCP-LU session, and VTAM can use a subarea or APPN path to initiate a session between the dependent LU and the primary LU (the application). BIND and session data are then routed directly between the primary LU and the dependent LU. To implement a DLUS/DLUR environment, consider the following:

- For the DLUR to initiate activation, via a call-in (to VTAM), no system definitions are required for existing token-ring LANs. Refer to “Token-Ring Configuration” chapter in the *3745/3746 Planning Series: Token Ring and Ethernet*.

  For SDLC lines, new definitions are needed in VTAM. Even if the SDLC line is leased, it must be referenced via a switched major node definition. Refer to “3746 SDLC Support” chapter in the *3745/3746 Planning Series: Serial Line Adapters*.

  The dynamic switched definition facility can be used to define the PU. For information about using the ISTEXCCS exit routine for dynamic definitions, refer to "Dynamically Defining Switched Resources" and related topics in the VTAM *Network Implementation Guide* that corresponds to your level of VTAM.

- For VTAM to initiate activation, via a call-out (from VTAM), of a PU, define the dependent LU requester by including the `DLURNAME` and `DLCADDR` operands on the PATH definition statement in the switched major node. `DLURNAME` specifies the CP name of the DLUR that owns the PU, and `DLCADDR` includes data link control (DLC) information used by the DLUR to locate the PU. Also include the `MAXDLUR` operand on the VBUILD definition statement to indicate the maximum number of unique DLURs defined for this switched major node.

  Note: If the `DLURNAME` is not fully qualified, the NETID of the DLUS is used.

- A DLUR may be served by multiple DLUS VTAMs simultaneously. It is possible for each of up to five downstream PUs on a DLUR to use a different DLUS, but this is not practical.

  Normally, a 3746 DLUR has a SSCP VTAM as its generic primary DLUS (and possibly, another VTAM as its generic back-up DLUS). One or more downstream PUs can grouped to use a different SSCP VTAM as its generic primary DLUS (with a different generic backup DLUS).

- Multiple DLURs may support the same PU, but only one at a time. The SSCP-PU session is through only one DLUR at any given time.

- Redial occurs as follows for DLUS supported PUs:

  – When a DLUS initiates the activation of a PU but receives a negative response, VTAM attempts to redial over each valid path statement for the PU until successful or until all valid paths have been tried. Redial does not occur if the negative response indicates that the PU is already active, or that the fully qualified procedure correlation identification (PCID) is not unique. If the fully qualified PCID is not unique, the DLUS attempts to redial the PU over the same path with a newly generated PCID.

  – Redial does not occur if PU activation was initiated by the DLUR.

  - When a protocol violation, topology database update (TDU) error, or CPSVRMGR session outage signal is received for a particular DLUR, VTAM attempts to redial every active or pending-active PU served by that DLUR for which a valid PATH statement is found. If the PU is already active, then VTAM performs the following:
    - If the PU was defined with `ANS=CONT` and the DLUR supports this function, giveback processing is performed prior to attempting redial.
    - If the PU was defined with `ANS=STOP` or the DLUR does not support `ANS=CONT`, the PU is deactivated prior to attempting redial.

- When a CP-CP session between a DLUS and DLUR fails, the CPSVRMGR session is inactivated, enabling reactivation of this CP-CP session.
- Information regarding DLUR-attached resources can be processed by the configuration services XID exit. This exit routine can be coded so that VTAM processes or denies requests for contact from known switched devices or so that VTAM processes or denies requests for PU activation from a DLUR. For details, refer to the *VTAM Customization*, LY43-0063. (Available to IBM licensed customers only).

VTAM DLCADDR Keyword in PATH Statement

The value of the DLCADDR keyword in the VTAM PATH definition statement is used when the DLUS attempts to establish a connection to a PU attached through a DLUR. As there is no direct connection to the DSPU, VTAM sends the information to the DLUR specified (DLURNAME), which then uses the information to establish a connection to the DSPU. You must code a DLCADDR keyword for each element of the information needed used to connect to a DSPU.

The format of the DLCADDR keyword is:

DLCADDR=(element,data_format,element_value)

- The first sub-operand indicates the element you are defining. A value between 1 and 96 can be specified.
- The second sub-operand indicates the format of the third sub-operand value, when transmitted to DLUR:

```
BCD:= Binary coded decimal
C:  = Any EBCDIC character
D:  = Decimal
X:  = Hexadecimal
I:  = Any ASCII character.
```

  Note: To be able to use the ASCII format, the following PTFs are required for:

  VTAM V4 R2, PTF UW28497
  VTAM V4 R3, PTF UW28498.

- The third sub-operand defines the value of the element.

An example of DLCADDR encoding is given below:

```
CP900DPT PATH  PID=1,                                              X
               DLURNAME=NETNODE1,              CPname of DLUR      X
               DLCADDR=(1,C,TR),               Type of attachment  X
               DLCADDR=(2,X,504F525432313434), PORT2144            X
               DLCADDR=(3,D,04),               DSAP of downstream CM/2 X
               DLCADDR=(4,X,400052005160),     MAC  of downstream CM/2 X
               USE=YES                  INITIALLY ACTIVE
```

The CP name of the 3746 DLUR is ***NETNODE1***, the DSPU is attached via the token-ring on port 2144 of the 3746. The DSAP and MAC address of the DSPU are specified in parameters 3 and 4.

Migration of SNI Connections to 3746 Models 900 and 950

SNA Network Interconnection (SNI) is a function of NCP which allows the interconnection of two SNA/subarea networks. Peripheral Border Node (PBN) and Extended Border Node (EBN) are functions that allow the interconnection of two APPN/HPR networks. They are provided by VTAM and NCP using 3745/3746-900 Composite Network Nodes (CNNs):

- A peripheral border node (PBN) allows access to adjacent APPN/HPR networks.
- An extended border node (EBN) allows access to non-adjacent APPN/HPR networks.

You cannot connect an SNA/subarea SNI node to an APPN/HPR node; once you migrate from a 3745/3746-900 to a 3746-900 network node or a 3746-950, the connections with the other nodes must use APPN/HPR flows.

Therefore, if your “partners” do not migrate to APPN but keep using SNI, you must keep a 3745/NCP that will handle your SNI traffic, while the coupled 3746-900 Network Node handles your APPN traffic. As shown in Figure 13 on page 40, the SNI traffic may flow over 3746 adapters to the NCP.

One exception to the above statement is when an SNI network is connected to a 3745 which is part of a CNN. Figure 29 on page 56 shows such a configuration. The 3745/NCP handles the SNI flows and routes these flows via an internal APPN link to the 3746-900 network node (Figure 25 on page 52 shows an example of how an internal APPN link works). The TRP2 which handles the APPN link also contains the HPR/RTP function. RTP converts APPN (ISR) flows from the SNI connection to HPR flows, which can then be routed through the APPN network as any other HPR flows.

Use the following procedure to migrate SNI nodes to APPN nodes:

Step 1. Add APPN/HPR Network Node support to the 3746-900 (NN).

This does not affect the SNI connections on the 3746-900; they stay under control of the NCP running in the 3745 CCU. See Figure 13 on page 40.

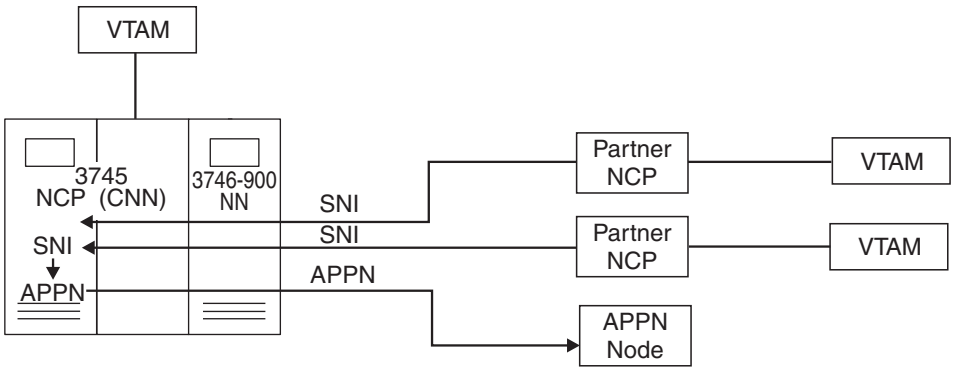


Figure 13. Example Network: Adding APPN Before SNI-to-APPN Migration

If there is a need to route traffic between an SNI port (or any SNA/subarea port of the 3745/3746-900) and an APPN port controlled by the 3746-900 network node, then the NCP must be defined as part of a Composite Network Node (CNN). NCP does the SNI-to-APPN and APPN-to-SNI conversions for the communication with the 3746-900 network node. This communication uses the coupling between the 3745 and the 3746-900, see "Internal APPN Connection between a 3745 and a 3746-900" on page 51.

Step 2. Progressively upgrade each partner network to support APPN connectivity to the 3746-900.

The minimum requirement is that the partner NCP becomes part of a Composite Network Node (VTAM plus one or more NCPs). This supports the APPN border node connection to the 3746-900 network node.

In the partner NCP, the connection is border node and in the 3746-900, the line will be defined in the 3746-900 network node instead of NCP. See Figure 14.

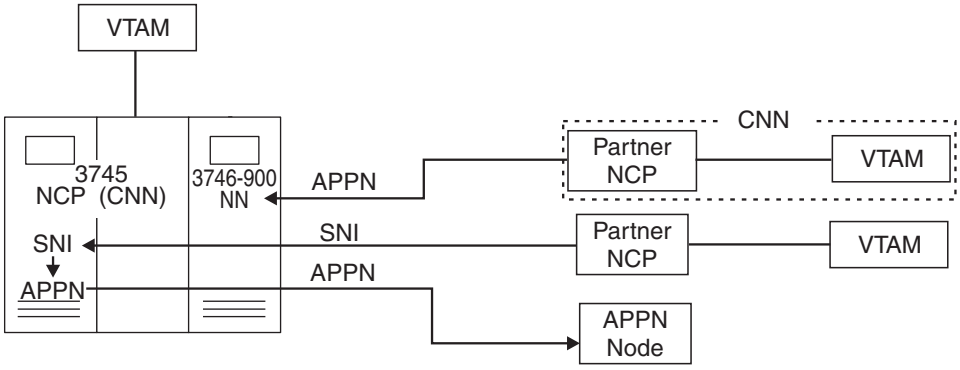


Figure 14. Example Network: SNI-to-APPN Migration

During this migration, the "partner" link stays physically attached to the same port of the 3746-900. The Controller Configuration and Management (CCM) is used to define this link in the 3746-900 network node.

Step 3. Upgrade the 3746-900 to a 3746-950.

This can be accomplished when there are no more SNI links or other need for NCP. See Figure 15 on page 41.

Note: Without Session Services Extension (SSE) support in the 3746 NN, this configuration supports independent sessions across the network boundary between the 3746 NN and a CNN providing the Extended Border Node (EBN) function. Dependent sessions across this boundary are not supported. The support of dependent sessions requires the 3746 NN directly adjacent to the CNN to support SSE. This is supported by the 3746 and VTAM (which has SSE support) acting together as a CNN.

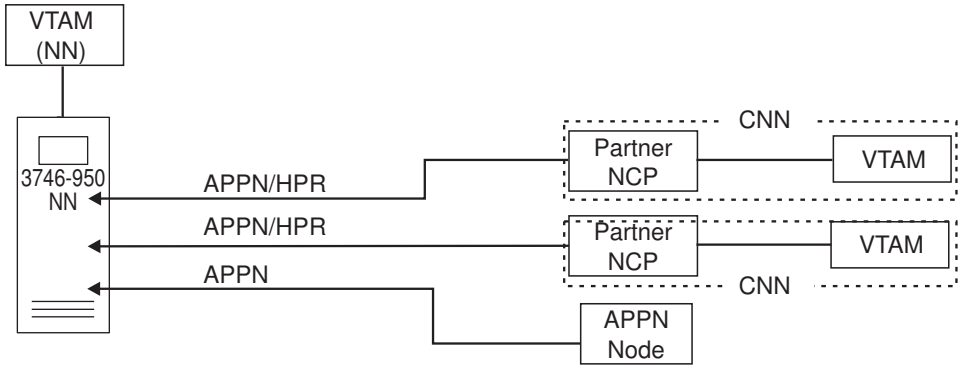


Figure 15. Example Network: Upgrading 3746-900 to a 3746-950

During this step, the 3745/NCP is removed from the controller configuration.

EBN/SSE Usage Rules

This section gives examples of independent and dependent connections across subnetwork boundaries using the extended border node (EBN) function.

VTAM, the IBM 2216 Nways Multiaccess Controller, and the IBM 3746 Multiaccess Enclosure support all of EBN.

The 3746 only supports the Session Services Extension (SSE) part of EBN.

Networks with DLURs: PLU, DLUS, and DLUR in Three Different Subnetworks

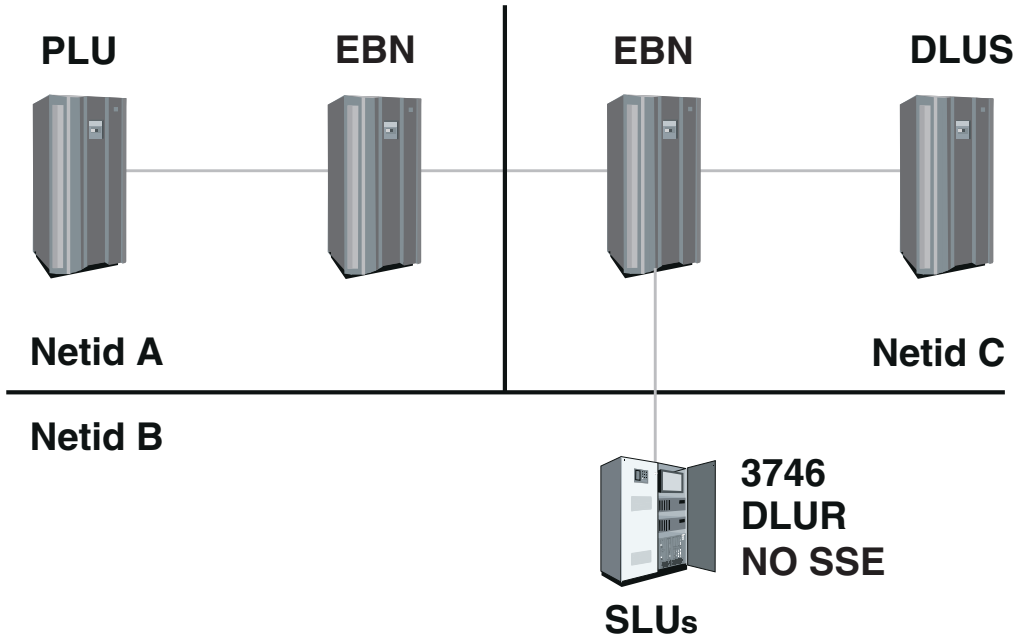


Figure 16. PLU and DLUS in Same Subnetwork

Table 3. PLU and DLUS in Same Subnetwork		
Path	**Required Nodes**	**Comments**
DLUS-PLU	1 EBN on *each side*	
DLUS-DLUR	1 EBN on *dependent logical unit server (DLUS) side*	SSE not needed on dependent logical unit requester (DLUR) side.
PLU-DLUR	1 EBN on *primary logical unit (PLU) side*	SSE not needed on DLUR side.
	An *extended boundary* connection is needed between networks A and C.	More than one extended boundary is allowed.
	A *peripheral boundary* connection is needed between networks B and C.	Only *one* peripheral boundary is allowed: when one boundary (peripheral or extended) exists, a second boundary (peripheral or extended) is not allowed. is not allowed between networks A and B.

Networks with DLURs: DLUS and DLUR in Same Subnetwork

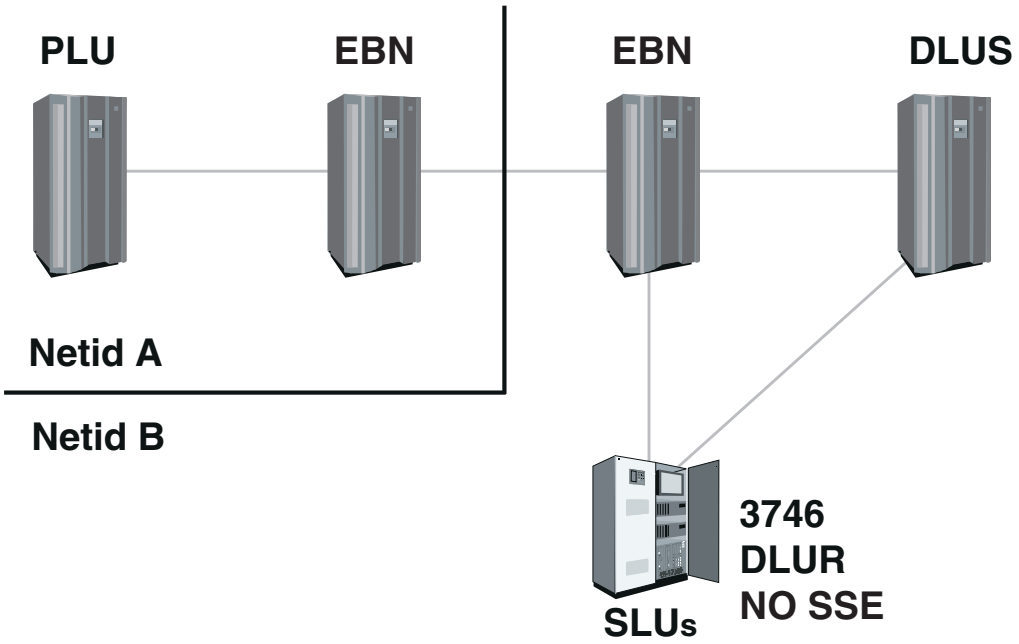


Figure 17. PLU and DLUR in Same Subnetwork

Table 4. PLU and DLUR in Same Subnetwork		
Path	**Required Nodes**	**Comments**
DLUS-PLU	1 EBN on *each side*	
DLUS-DLUR		SSE not needed, both DLUS and DLUR are in same network.
PLU-DLUR	1 EBN on *PLU side*	SSE not needed on DLUR side.
	An *extended boundary* needed between networks A and B.	A peripheral boundary is not allowed between networks A and B in this case.

Networks with DLURs: PLU and DLUS in Same Subnetwork

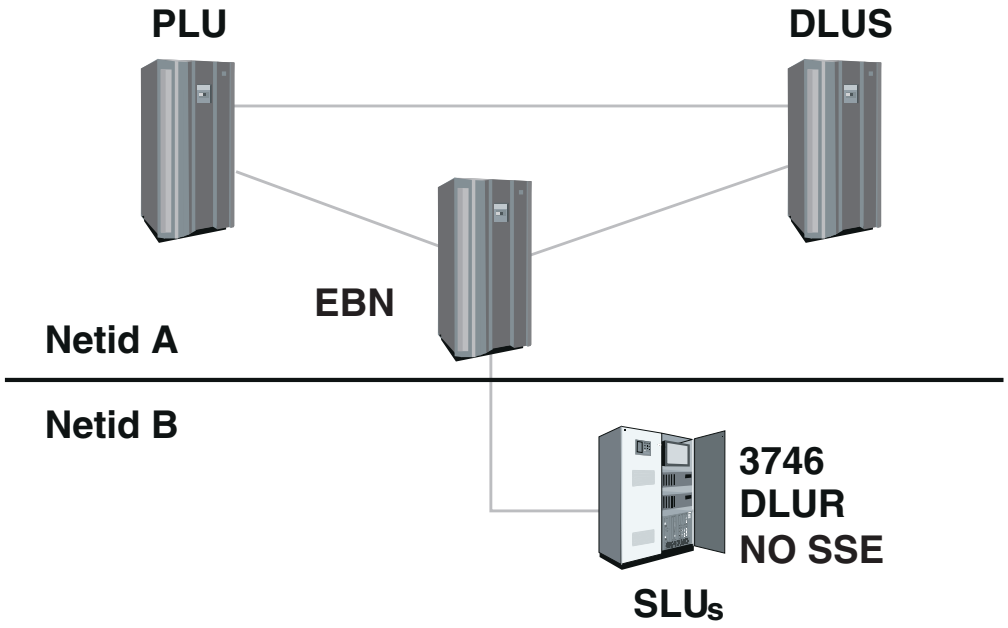


Figure 18. PLU and DLUS in Same Subnetwork

Table 5. PLU and DLUS in Same Subnetwork

Path	Required Nodes	Comments
DLUS-PLU		SSE in DLUS and PLU only needed for: • Secondary logical unit (SLU)-initiate sessions • Sessions requiring queuing (initiate-only, initiate-or-queue, and queue-only queuing) • Third Party Initiate (TPI) sessions • Auto-logon (initiate-or-notify initiate).
DLUS-DLUR	1 EBN on *DLUS side*	SSE not needed on DLUR side.
PLU-DLUR	1 EBN on *PLU side*	SSE not needed on DLUR side.

Networks with DLURs: PLU and DLUR in Same Subnetwork

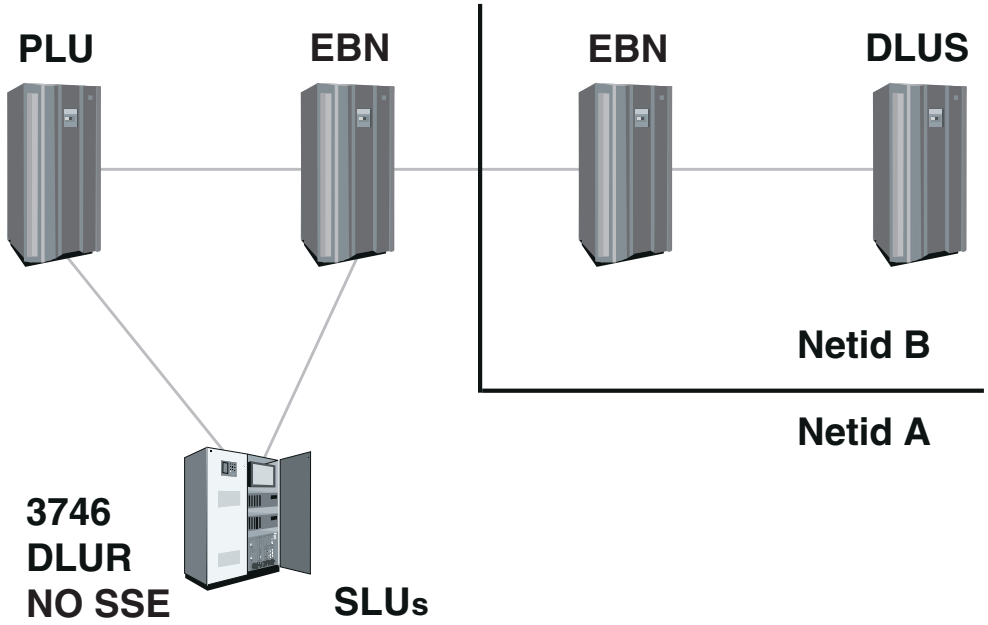


Figure 19. PLU and DLUR in Same Subnetwork

Table 6. PLU and DLUR in Same Subnetwork		
Path	**Required Nodes**	**Comments**
DLUS-PLU	1 EBN on *each side*	
DLUS-DLUR	1 EBN on *DLUS side*	SSE not needed on DLUR side.
PLU-DLUR		SSE not needed, both PLU and DLUR are in same network.
	An *extended boundary* needed between networks A and B.	A peripheral boundary is not allowed between networks A and B in this case.

Networks with DLURs: PLU in Subarea Network, DLUS and DLUR in Same APPN Network

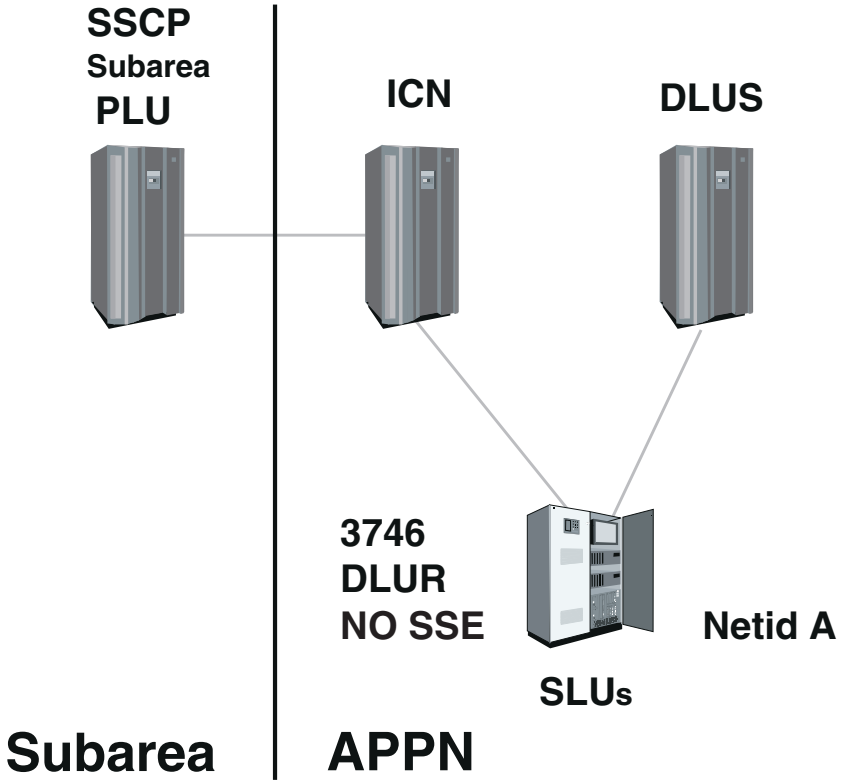


Figure 20. PLU in Subarea Network, DLUS and DLUR in Same APPN Network

Table 7. PLU in Subarea Network, DLUS and DLUR in Same APPN Network		
Path	**Required Nodes**	**Comments**
DLUS-PLU **PLU-DLUR**	The subarea VTAM, interchange node (ICN), and DLUS must support SSE.	The "owning" control point (CP) and network node server (NNS) of *both must* support SSE. In this example, the CP (PLU) is a Subarea VTAM and the NNS (PLU) is the ICN. The DLUS is both the CP and NNS for the SLU. The DLUR does not need a SSE.
DLUS-DLUR		SSE not needed as both are in same network.
	No EBNs needed.	There are no APPN subnetwork boundaries.
		Subarea resources appear to other network nodes as if they are APPN end nodes (ENs) served by the ICN in the path to that resource. In other words, the PLU looks like it is on an EN served by the ICN.

APPN Networks: 3746-9X0 Used as NNS of VTAM ENs

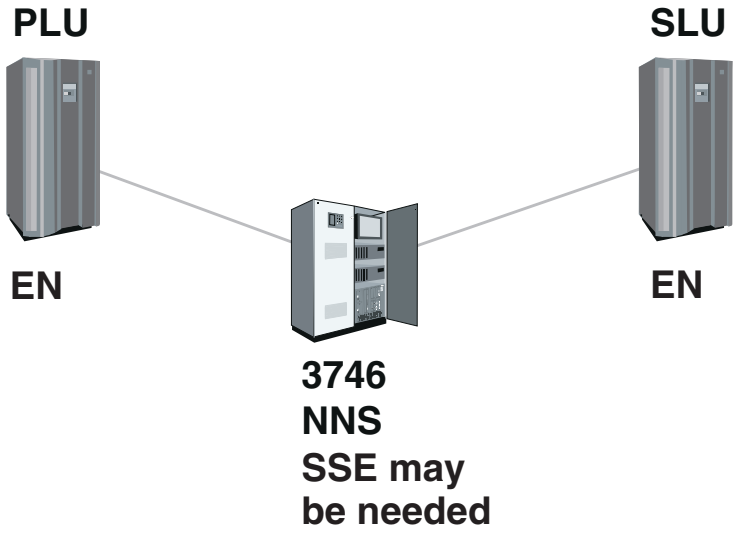


Figure 21. 3746-9X0 Used as NNS of VTAM ENs

Table 8. 3746-9X0 Used as NNS of VTAM ENs

Path	Required Nodes	Comments
	By default, CP-CP sessions not set up by VTAM.	VTAM assumes that it has a NNS that supports SSE. To have CP-CP sessions set up, define a NETSERVR list in the VTAM EN and code SLUINIT=OPT for every 3746 in the list.
	Only *PLU-initiated sessions* can be set up through the 3746 without SSE. SSE required for: • Secondary logical unit (SLU)-initiate sessions • Sessions requiring queuing (initiate-only, initiate-or-queue, and queue-only queuing) • Third Party Initiate (TPI) sessions • Auto-logon (initiate-or-notify initiate).	

APPN Networks: 3746-9X0 Connected to a VTAM EBN

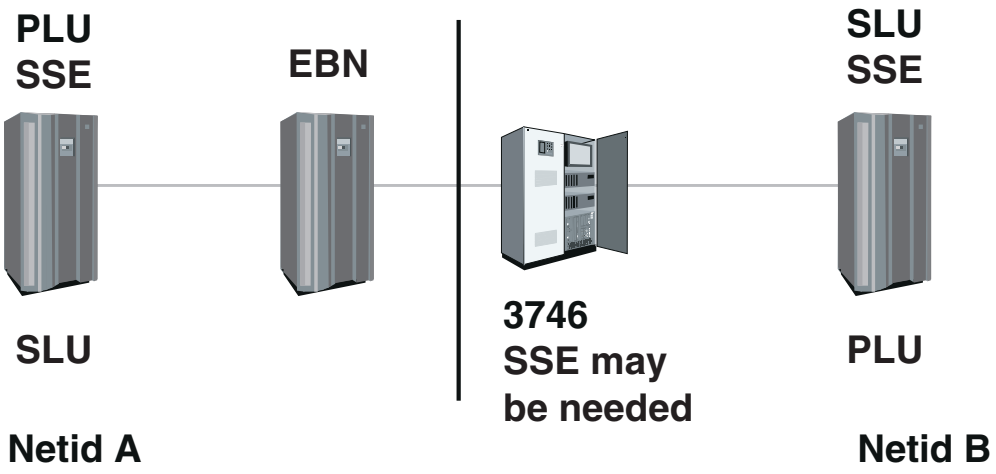


Figure 22. 3746-9X0 Connected to a VTAM EBN

Table 9. 3746-9X0 Connected to a VTAM EBN

Path	Required Nodes	Comments
PLU (subnetwork A)→ SLU (subnetwork B)	If the 3746 is *not SSE capable*, EBN changes 'Search/Find' to 'Search Only' before sending it to the 3746.	
PLU (subnetwork B)→ SLU (subnetwork A)	If the 3746 is *not SSE capable*, EBN should change 'Search/Find' to 'Search Only' before sending it to the PLU.	
	Only *PLU-initiated sessions* can be set up through the 3746 without SSE. SSE required for: • Secondary logical unit (SLU)-initiate sessions • Sessions requiring queuing (initiate-only, initiate-or-queue, and queue-only queuing) • Third Party Initiate (TPI) sessions • Auto-logon (initiate-or-notify initiate).	

Mixed APPN and Subarea Networks: 3746-9X0 between EBN and NCP/Subarea (with SLU)

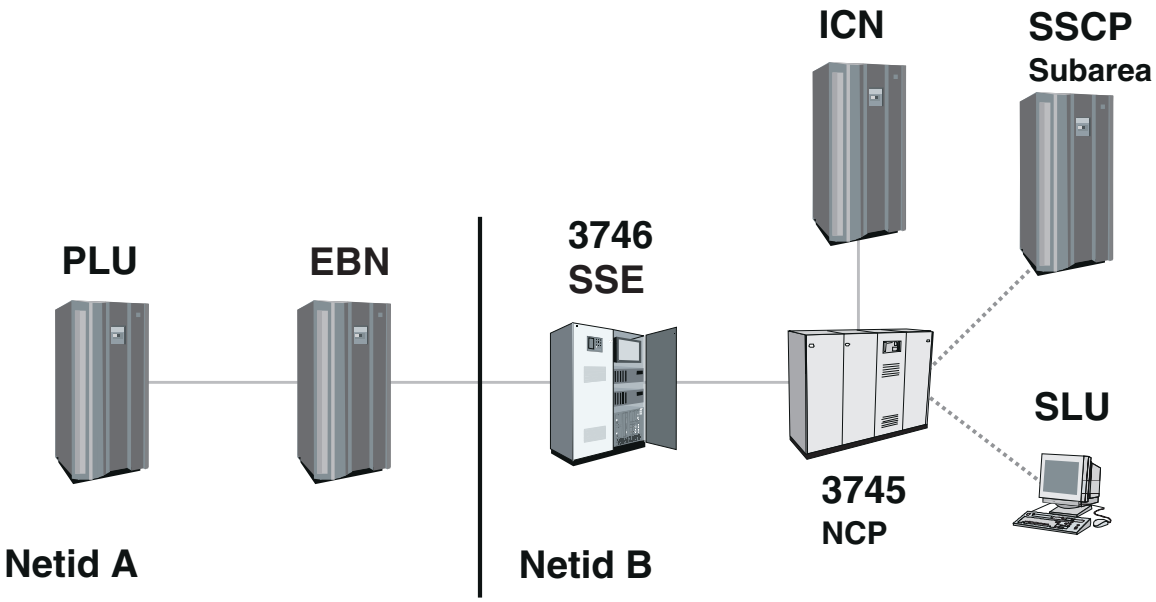


Figure 23. 3746-9X0 between EBN and NCP/Subarea (with SLU)

Table 10. 3746-9X0 between EBN and NCP/Subarea (with SLU)

Path	Required Nodes	Comments
SLU-SSCP		Subarea path has a NNS that supports SSE.
SSCP-PLU **PLU-SLU**	1 EBN on *either side* SSE required for (the 3746 is the NNS of DLU for sessions that originate in network A): • Secondary logical unit (SLU)-initiate sessions • Sessions requiring queuing (initiate-only, initiate-or-queue, and queue-only queuing) • Third Party Initiate (TPI) sessions • Auto-logon (initiate-or-notify initiate).	

Mixed APPN and Subarea Networks: 3746-9X0 between EBN (with SLU) and NCP/Subarea

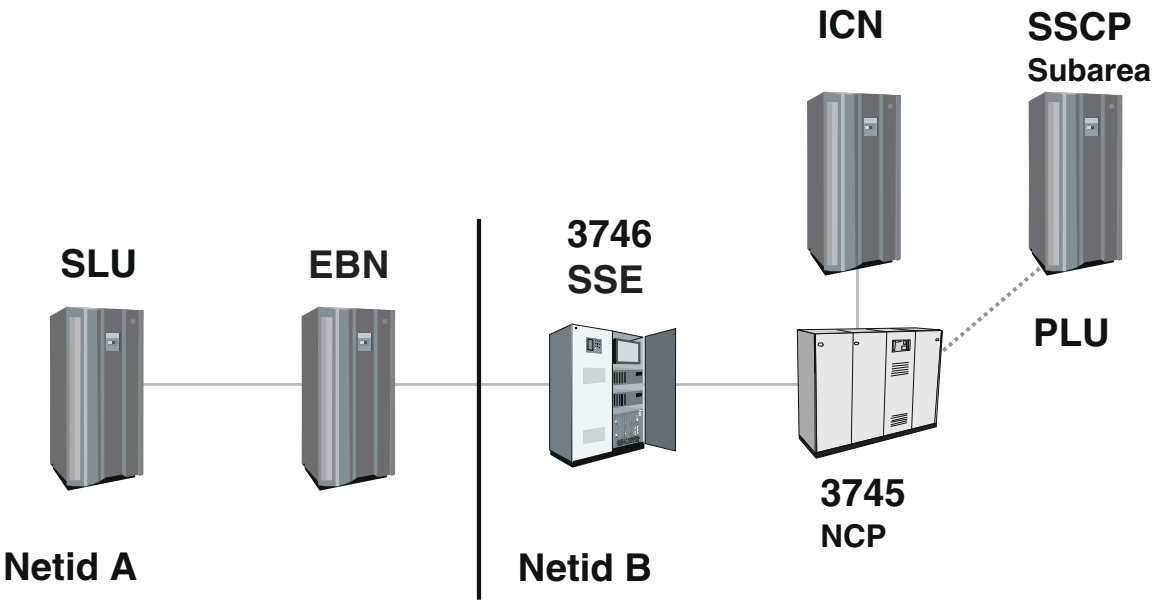


Figure 24. 3746-9X0 between EBN (with SLU) and NCP/Subarea

Table 11. 3746-9X0 between EBN (with SLU) and NCP/Subarea

Path	Required Nodes	Comments
SSCP-PLU **PLU-SLU**	1 EBN on *either side* *SSE required* in 3746. The 3746 is the NNS originating logical unit [OLU] for sessions the originate in network A. SSE required for: • Secondary logical unit (SLU)-initiate sessions • Sessions requiring queuing (initiate-only, initiate-or-queue, and queue-only queuing) • Third Party Initiate (TPI) sessions • Auto-logon (initiate-or-notify initiate).	

Internal APPN Connection between a 3745 and a 3746-900

On a 3745/3746-900, the controller bus coupler (CBC) provides an internal connection (an APPN transmission group) between the 3746-900 network node and the 3745 (NCP) operated as a composite network node (CNN). This internal APPN link is set up using a 3746-900 token-ring port. Any token-ring port, except the TIC3 port of the CBSP2 (port address 2080), can be used (see Figure 25 on page 52). The TRP2 for this TIC3 performs the APPN routing between the CBC link and the other ports of the 3746 Network Node.

Although data transmitted between the 3746 Network Node and the CNN does not actually pass through the token-ring port, a TIC3 must be present. To enable the activation of the token-ring port, a LAN must be connected to this TIC3. If this TIC3 port is used by the stations connected to the LAN, all the LAN traffic over this port must use a single point of control. For example, all the LAN stations that use this TIC3 as a destination address must be defined with the same destination SAP (for either NCP or the 3746 Network Node). However, this may not be practical as the TRP2 may already be loaded to its capacity by the internal APPN traffic.

Example of an Internal APPN Link

Figure 25 on page 52 shows an example of a 3745/3746-900 configuration using the internal APPN communication between the 3746 Network Node and the CNN. The components are:

- User workstation (PU/node) with a dependent or independent logical unit (LU) communicating with an application running in the host.
- CNN consisting of a host with VTAM, and a 3745 with a single NCP (one CCU). NCP communicates with VTAM via a parallel channel.
- 3746 Network Node.

The figure shows how the data flows between the user and the application.

3746-900 Configuration Requirements

The token-ring hardware required for the internal APPN link to the 3745 depends on the configuration of the 3745 and its mode of operation:

- 3745 with a single CCU (Models 17A, 21A, and 31A)

  One TIC3 on a TRP2 must be available.

- 3745 with two CCUs (Models 41A, and 61A):
  - If only **one** NCP communicates with the 3746 Network Node at a time (for example, in the “3745 twin-standby mode”), one TIC3 on a TRP2 must be available, for example, on of the TRP2 connecting CCU B.
  - If **two** NCPs communicate at the same time with the 3746 Network Node, two TIC3s must be available. For load distribution and backup reasons, they should preferably be on two different TRP2s. For example, the internal APPN link to CCU B could use a TIC3 on the TRP2 connecting CCU B and the APPN internal link CCU A could use a TIC3 on another TRP2.

Definitions Required for the Internal APPN Link

From a definition perspective, the internal link appears as a token-ring connection with the same token-ring address defined in the 3746 Network Node and the CNN:

- **Important**

  The CNN SAP value must be different from the NCP SAP (default X'04').

- **3746 Network Node (CCM Definitions)**

  One token-ring port definition is required for each CCU/3746 Network Node link. Figure 25 is a single link example.

  To allow simultaneous communication between the 3746 Network Node and both CCU A and CCU B, two port definitions are required. Each port definition must use a different TIC3 address.

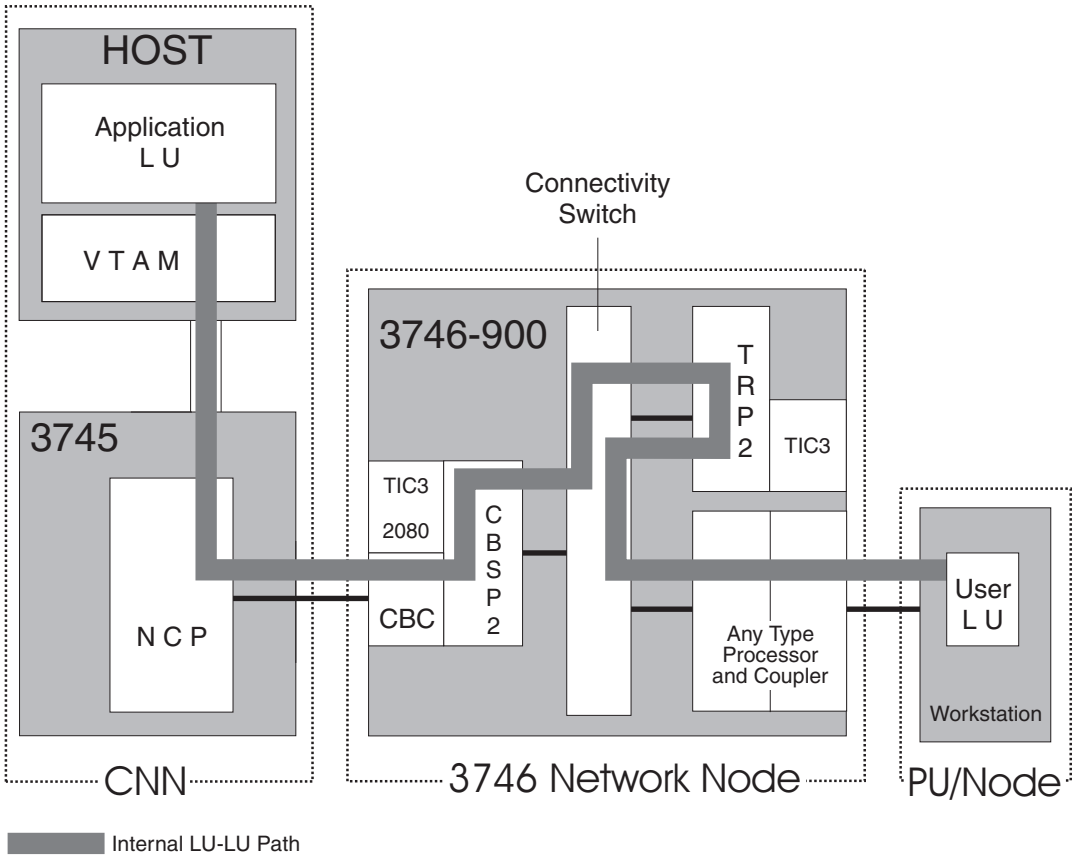


Figure 25. Internal APPN Link (3746-900)

The link station definition depends on who controls the TIC3:

1. If the TIC3 port connects LAN stations controlled ***only by the 3746 Network Node and these stations do not need to be defined in the 3746 Network Node***, then, using the Controller Configuration and Management (*CCM User's Guide*, SH11-3081) application:
   - Define the TIC3 port with the option “Accept any incoming calls” set to YES.
   - Do not make a link station definition for this TIC3 port.

2. If the TIC3 port connects LAN users controlled ***only by NCP in the CNN***, then, using *CCM User's Guide*, SH11-3081:
   – Define the TIC3 port with the option “Accept any incoming calls” set to NO.
   – For this TIC3 port define NCP as a link station:
     - The locally administered address (LAA) of the station must have the same value as the port LAA.
     - The destination service access point of the station must be set X‘04’ (the default value for the NCP service access point).
3. If the TIC3 port connects LAN users controlled ***only by the 3746 Network Node and defined in the 3746 Network Node***, then, using *CCM User's Guide*, SH11-3081:
   – Define the TIC3 port with the option “Accept any incoming calls” set to NO.
   – For this TIC3 port define NCP as a link station:
     - The locally administered address (LAA) of the station must have the same value as the port LAA.
     - The destination service access point of the station must be set X‘04’ (the default value for the NCP service access point).

- **CNN (VTAM and NCP Definitions)**
  – token-ring (port) definitions in NCP.

    The token-ring port address is the address of the TIC3 defined in the 3746 Network Node (using the *CCM User's Guide*, SH11-3081). The locally administered address must be the same in the NCP keyword `LOCADD` as in *CCM User's Guide*, SH11-3081.

    When using a dual CCU Model 3745, this port can be defined in both NCPs, but only one NCP is able to activate the port at a time. This means that the internal APPN link can be active via either CCU A or CCU B, but not both at the same time.

    To allow simultaneous communication between the 3746 Network Node and both CCU A and CCU B, two port definitions are required. Each port definition must use a different TIC3 address.

  – Link station definitions in VTAM.

    To represent the 3746-900 network node, a link station definition is required in VTAM. The local service access points value for the 3746 Network Node must be used (the default is X‘08’).

    VTAM dynamics can be used to generate the appropriate switched major node definitions.

3746 Network Nodes in APPN/HPR Networks: Examples

This section contains three examples of 3746 Network Nodes in APPN/HPR networks as:

- ANR node, see Figure 26
- APPN/RTP Node with Boundary function, see Figure 27 on page 55
- DLUR/RTP Node with Boundary function, see Figure 28 on page 55.

Each example shows the active path, end-to-end, and the network layers involved in the 3746, assuming that the traffic routing involves two adapters (ADP#1 and ADP#2). The legend for the examples is:

ADP	=	adapter
ANR	=	automatic network routing
APPN	=	APPN
DLC	=	data link control
DLUS	=	dependent LU server
HPR	=	High Performance Routing
ISR	=	intermediate session routing
RTP	=	rapid transport protocol.

Example 1: ANR Node

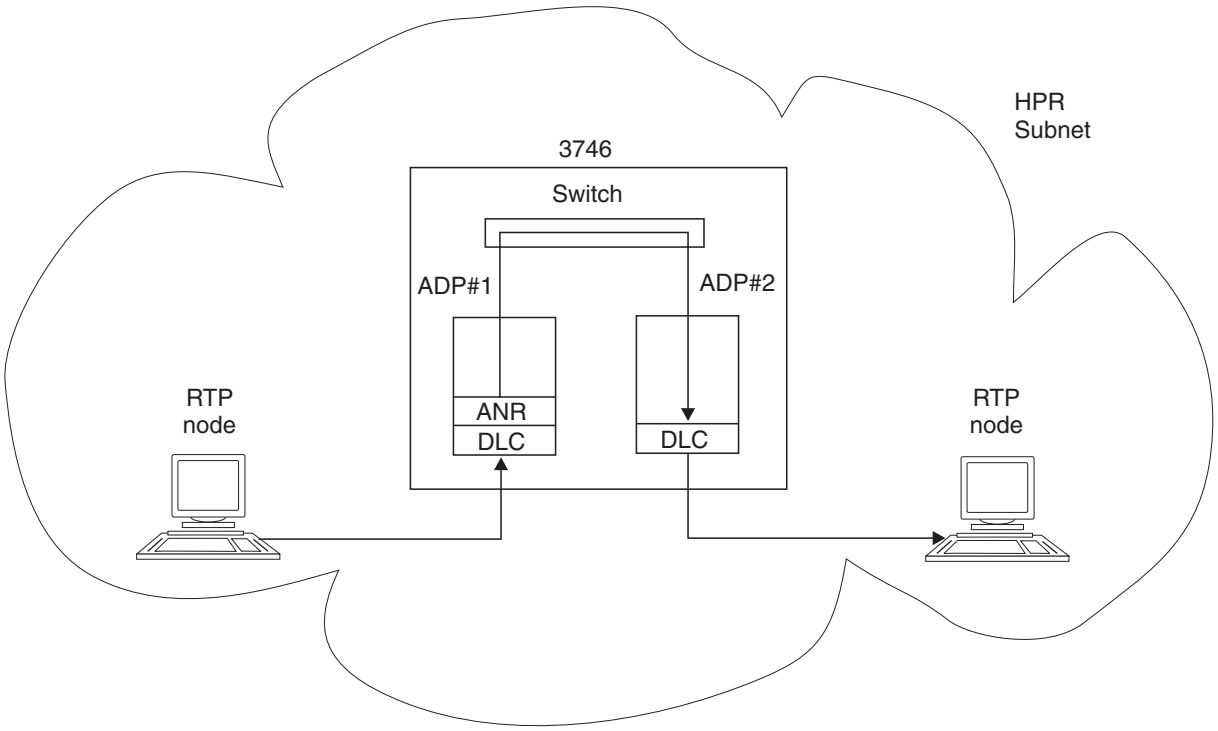


Figure 26. 3746 as an ANR Node

Example 2: APPN/RTP Node with Boundary Function

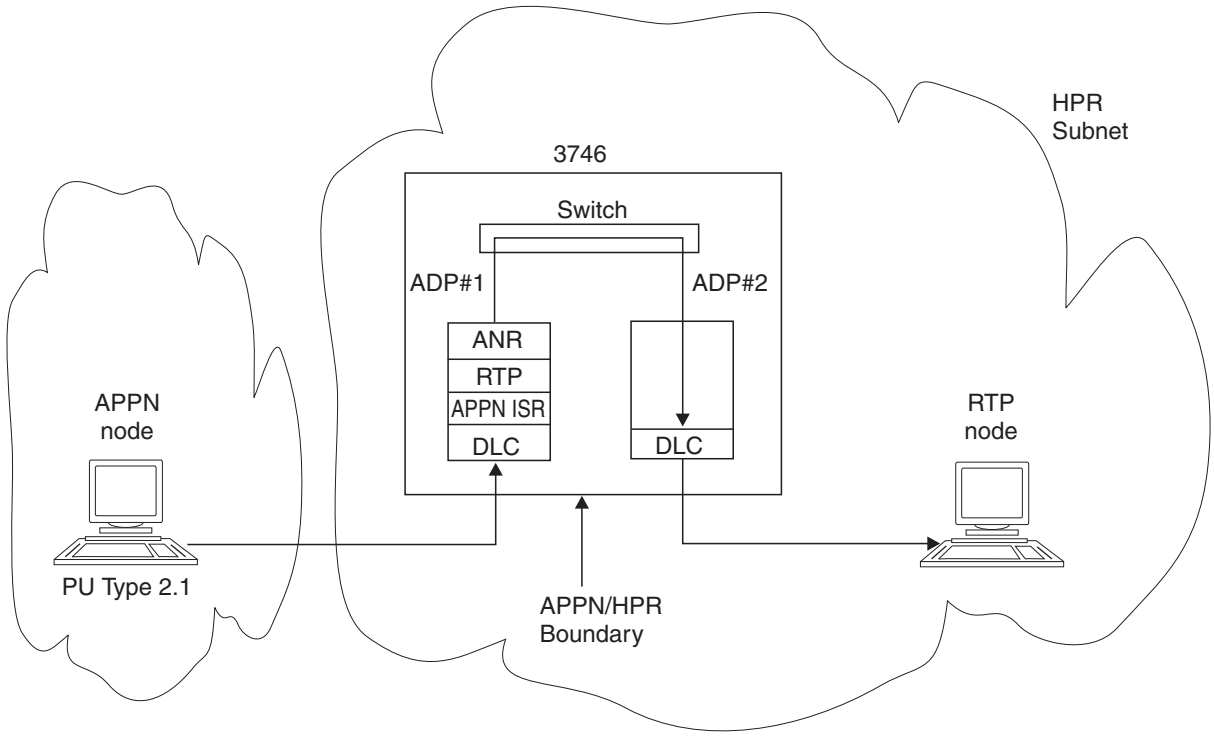


Figure 27. 3746 as an APPN/RTP Node (with Boundary Function)

Example 3: DLUR/RTP Node with Boundary Function

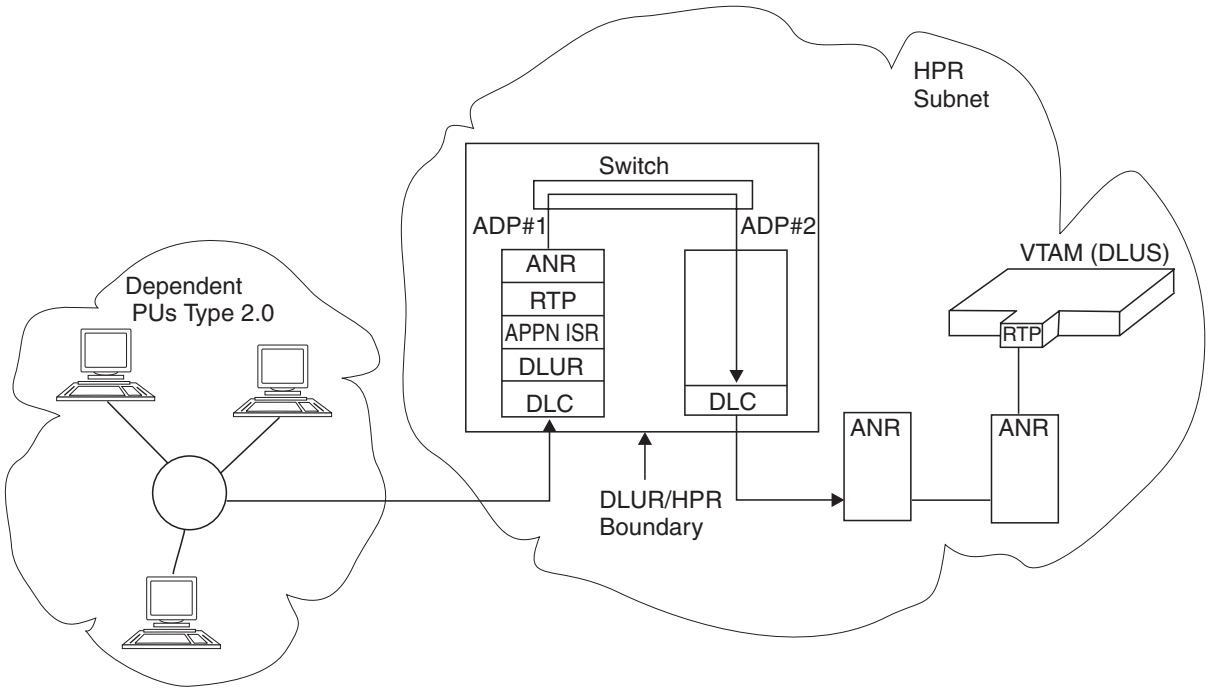


Figure 28. 3746 as a DLUR/RTP Node (with Boundary Function)

Example 4: APPN/RTP Node with SNI Network

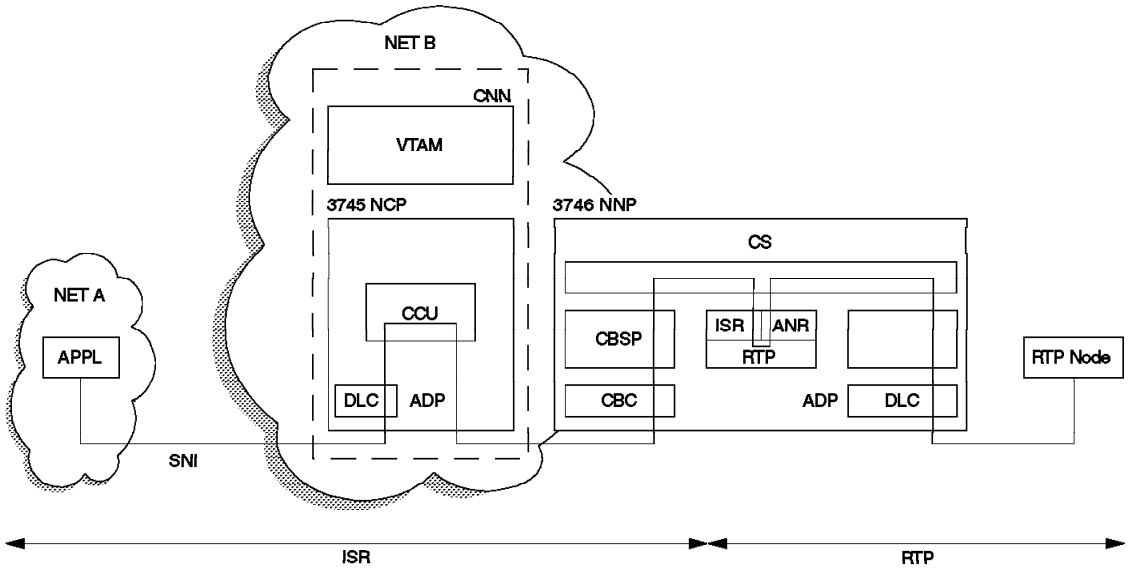


Figure 29. 3746 as an APPN/RTP Node with SNI Network

External APPN Connection between a 3745-Composite Network Node and a 3746-900

A simple way to interconnect a 3745-CNN and the attached 3746-900 Network Node is to use an external connection (token-ring or serial link). Compared to the internal APPN connection (see 51), this connection does not support as much traffic between the 3745-CNN and the 3746-NN, for example traffic between nodes such as ENA and ENB.

For example, in Figure 30, the advantages of a connection network, duplicate MAC addresses, and optimal route computation are achieved by using an “external” token-ring interconnecting the 3745-CNN and the attached 3746-900 NN.

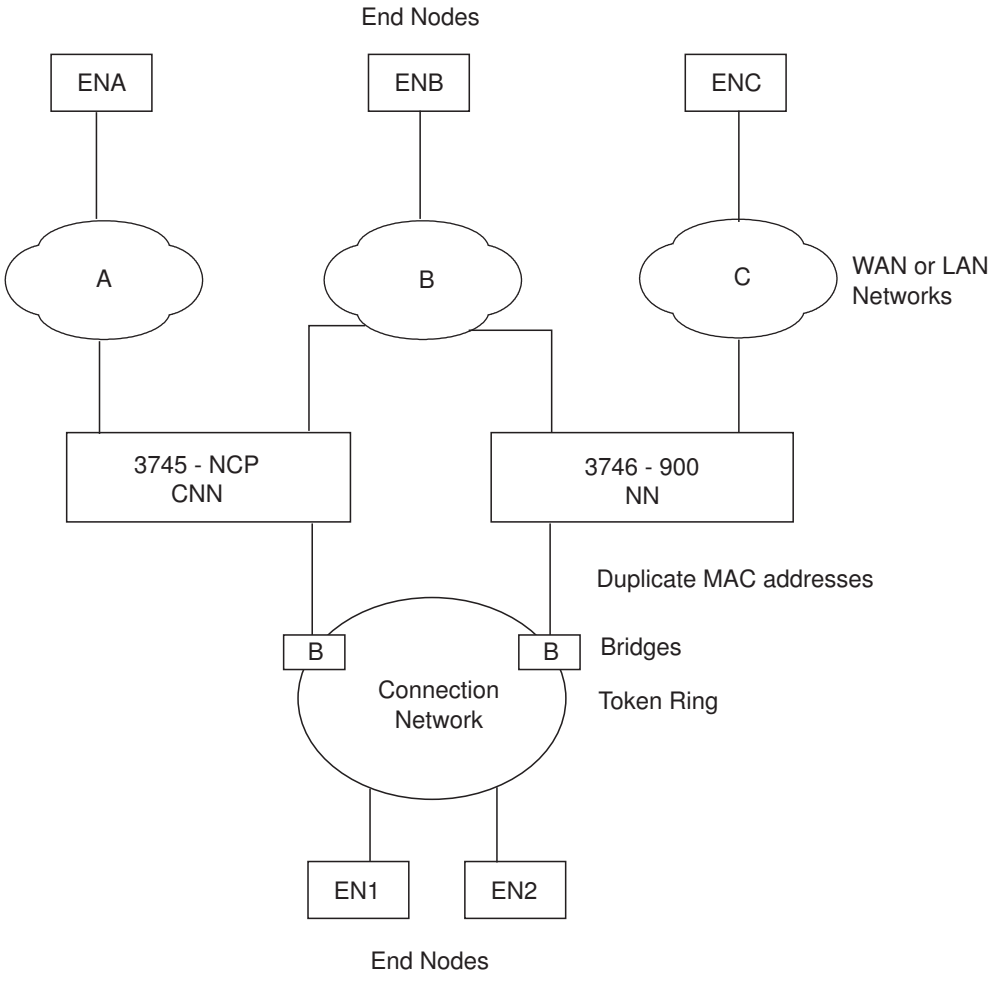


Figure 30. External Connection of 3745-CNN and 3746-NN

If ENA wants to establish a session with ENC, the route will be
ENA → CNN → Token-Ring LAN (Connection Network) → 3746 NN → ENC.

End nodes cannot have multiple network node servers at the same time, they can have ***only*** one.

By using duplicate MAC addresses between the 3745 TIC and the 3746 TIC, end nodes connected to the connection network LAN will use “at random” either the 3745 or the 3746 as a network node server.

Referring to Figure 30, suppose EN1 has CNN as a network node server:

Case 1: EN1 establishes an LU session with EN2

The CNN will send back the TG vector of the connection network and EN1 will establish the session with EN2 through the connection network. The 3746 NN is not involved, and the 3745 CNN is no longer involved once the session has been set up.

Case 2: EN1 establishes an LU session with ENA

As ENA is not reachable by the 3746 NN, the 3745 CNN will send back the RSCV containing the route:
EN1 → CNN → ENA.
Here, only CNN is used and the 3746 NN is not involved.

Case 3: EN1 establishes a LU session with ENB

In its route computation, the CNN (as a network node of EN1) will find two possible routes:
EN1 → CNN → ENB
OR
EN1 → 3746 NN → ENB.
This is because CNN uses the topology database with all nodes and TGs. CNN will choose the best route that maps the COS of the required session.

If the best route is:
EN1 → 3746 NN → ENB,
EN1 will send the BIND and all data directly to 3746 NN. The CNN is not involved.

Case 4: EN1 establishes a LU session with ENC

This is more or less identical to case 3. CNN finds one route that is:
EN1 → 3746 NN → ENC,
and thus EN1 will send the BIND and all data directly to 3746 NN. The CNN is then no longer involved.

HPR MLTGs in the 3746

HPR MLTGs on the 3746 can consist of any mix of CLP and TRP links (ESCON is not supported) running any mix of SDLC, frame-relay, X25 and 802.2 LLC protocols.

HPR MLTGs are defined in CCM from the APPN parameters panel for APPN stations. You can specify the name and TG number (1-20) of the MLTG here. Figure 31 shows the MLTG definition panel.

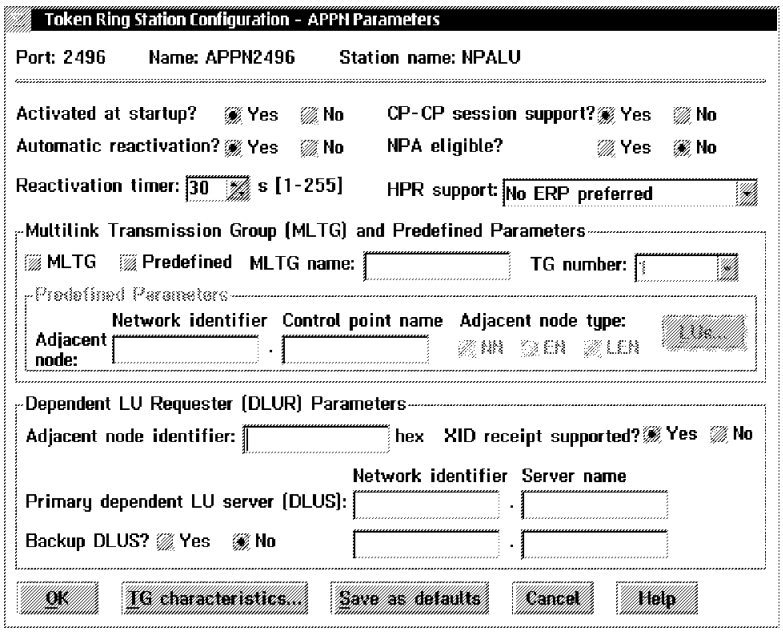


Figure 31. Defining MLTGs in CCM

Other links that belong to the same TG must be defined with the same name and TG number. If during XID exchange, the 3746 APPN CP discovers that a new TG does not go to the same adjacent node as the already active TGs in that MLTG, then the TG activation will fail.

In addition, the CCM performs checking that an MLTG name is only associated with a single MLTG number across all MLTG definitions.

The previous example shows how to define MLTGs at each link station, there is also a central way of defining and checking all MLTG definitions in CCM. From the main CCM panel select **Configuration -> APPN -> MLTG**. This displays a panel where all defined MLTGs, and all defined links stations can be seen. From this panel it is possible to change existing MLTGs and define new MLTGs.

User Defined Parameters

The 3746-9x0 implements three "User Defined Parameters" (UDP1, UDP2 and UDP3). Their purpose is to allow the network operator to alter the TG weight between the 3746-9x0 and its adjacent Network Nodes and so favor some TGs for route selection over other TGs. APPN route selection will select the route with the lowest TG weight that satisfies all other parameters for the session. The TGs with a heavier TG weight being used in case of congestion or unavailability of the lower weight TG.

There are three ways to make UDP definitions:

1. **Class Of Services and LOGMODE definitions**

   User Defined Parameters are enabled only for user defined Class Of Services (COS) and logmodes, changing standard logmodes such as #CONNECT or #INTER, would reduce UDP effectiveness. In order to define your own COS and LOGMODE, go to the Configuration menu from the CCM main panel, select **APPN** then select **MODE/COS** to get following panel:

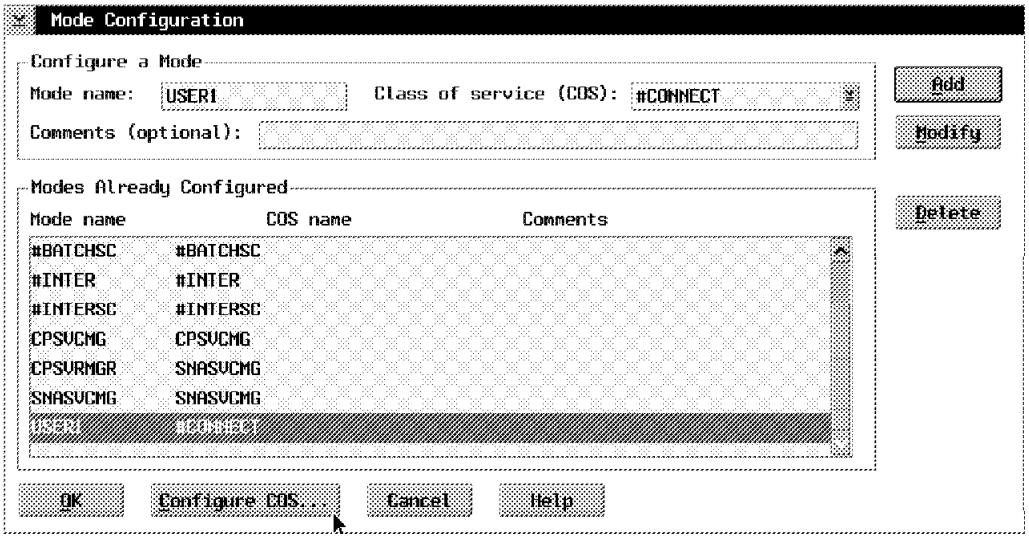


Figure 32. Mode Configuration Panel

   Click **Configure COS...** to create your own Class Of Services Enter COS Name and click **Add**. Select TG Row to specify the different TG weights and associated UDPs ranges. This gives the following panel:

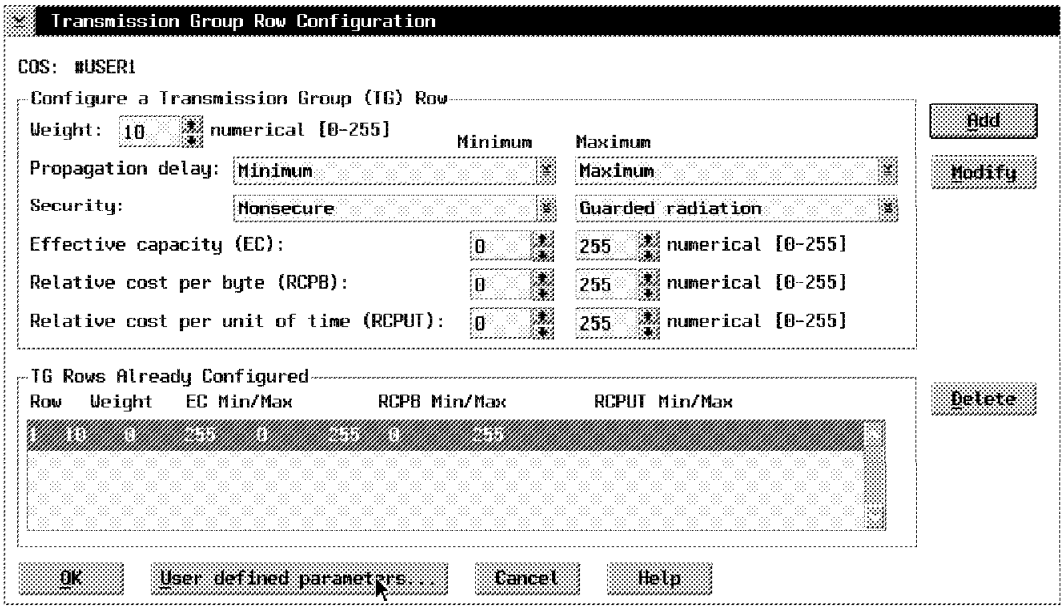


Figure 33. TG Row Configuration

Enter the TG weight you want to define, then click **User defined parameters...**. This gives the following panel:

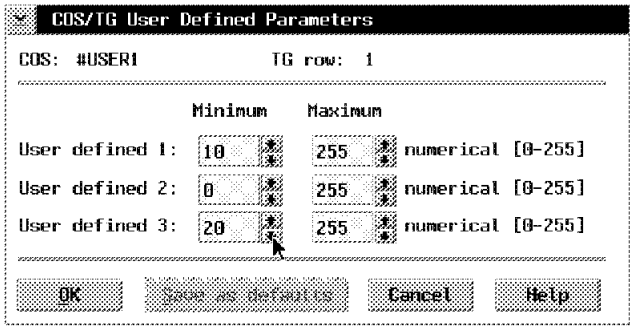


Figure 34. COS/TG User Defined Parameter Panel

You can now specify the ranges for UDP1, UDP2 and UDP3 which will be associated to the TG weight previously defined. Click **OK** to go back to TG Row configuration panel Repeat this operation for each different TG weight you want to define then click successively **OK** to return to the CCM main panel.

2. **UDPs definitions at PORT level**

   You can specify specific UDPs values for each APPN Port you define from CCM. These values will be compared to the ranges defined in COS and LOGMODE tables and the corresponding TG weight will be associated to the PORT. According to UDPs values, different weights will be associated PORTs, thus allowing APPN to compute the best route.

3. **TGs characteristics modification at STATION level**

   By default, the PORT UDPs values are used for any STATION on that port. These UDPs can be specified for specific stations in order to force a different route weight.

   From Station Definition panel, under CCM, click **APPN parameters...** then **TG characteristics...** to get the following panel:

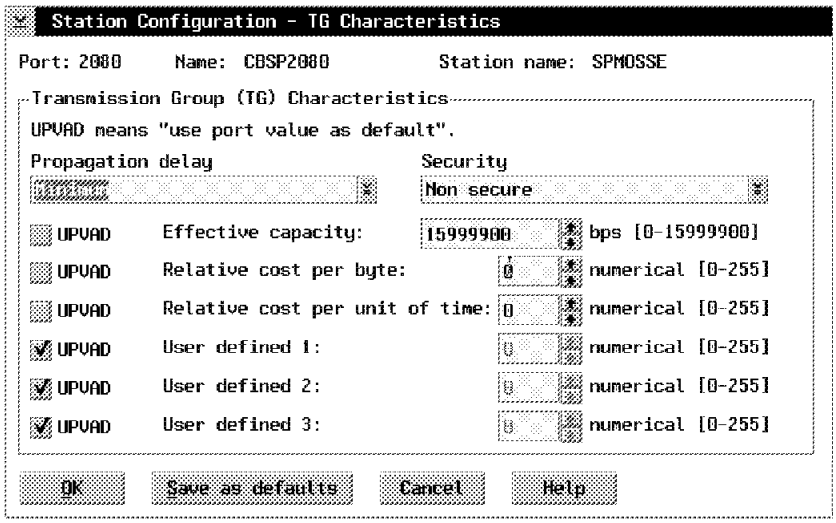


Figure 35. Station UDPs

De-select the pushbutton for the parameters you want to alter, then enter the new parameter value. Click **OK** after you have defined the new values. If ***UPVAD*** (use port value as default) is selected, then the port parameters are used as default for this link.

3746 Network Nodes in SNA/APPN/HPR Networks: Operation

When operating in an APPN/HPR or mixed SNA and APPN/HPR environment, the 3746-900 and 3746-950 provide the following networking capabilities:

- APPN/HPR network node services
- Dependent logical unit requester (DLUR)
- Automatic Network Routing (ANR) and Rapid Transport Protocol (RTP) for HPR traffic.

APPN/HPR Network Node

The 3746-9x0 supports APPN/HPR network node functions. They include the network node services for the APPN end nodes connected to the 3746 (adjacent end nodes). As a network node, the 3746 automatically and dynamically learns the full, up-to-date connection topology of the network. It dynamically locates any resource and computes routes within the network. The 3746-9x0 can also register the resources of adjacent end nodes to the APPN central directory server node such as VTAM.

The 3746 network node supports the following types of end-node connections (see Figure 36 on page 64):

- APPN (PU type 2.1, such as PS/2s and IBM 3174s)
- Non-APPN (including PU types 1.0 and 2.0, such as 3270-type devices)
- Low-entry networking (PU type 2.1, such as IBM System 36™ or nodes without APPN installed, for example, an IBM AS/400®, IBM 3174, IBM PS/2®, or other PCs).

The 3746-9x0 APPN/HPR control point functions are performed by a dedicated processor (the network node processor). The routing of data is done by the adapters (either port-to-port within an adapter or adapter-to-adapter) without any control point intervention. This allows the 3746-9x0 to support high speed data transfer.

Dependent Logical Unit Requester (DLUR)

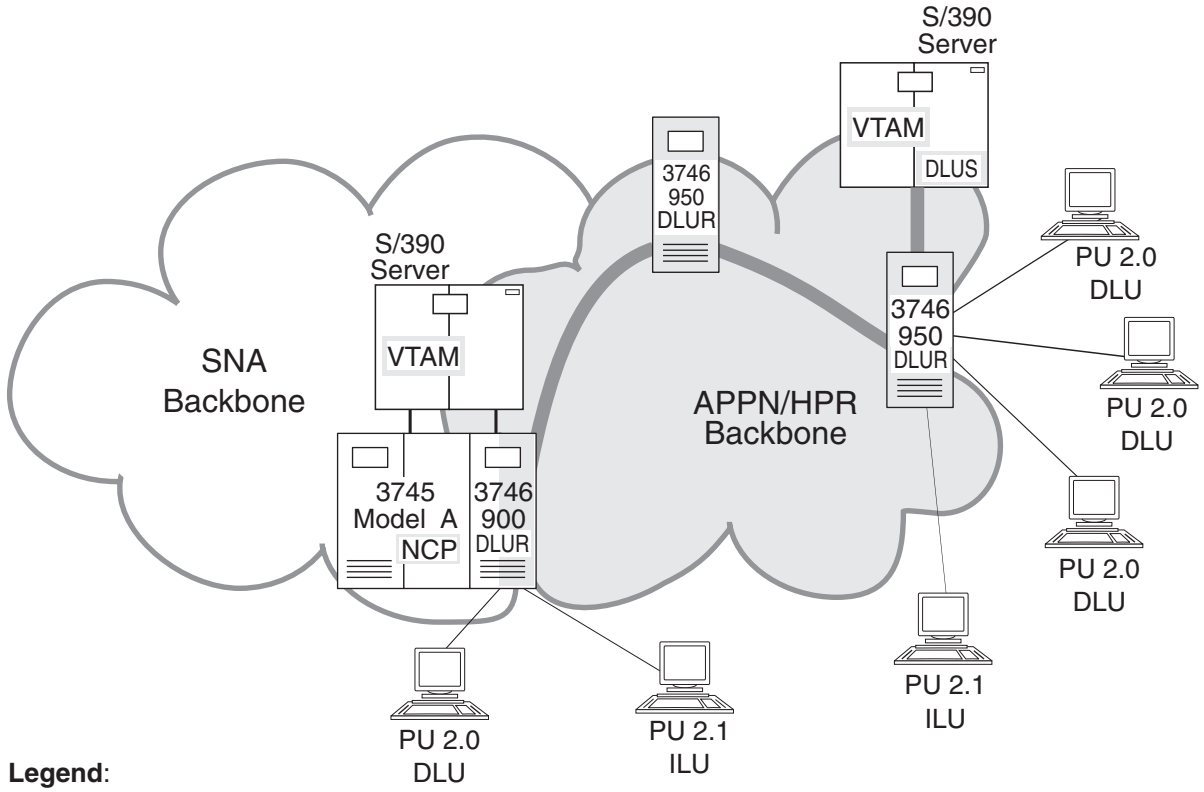


Figure 36. Dependent LU Support

The 3746 network node allows existing host-dependent SNA devices to access S/390 applications across an APPN/HPR backbone network. For example (see Figure 36), a physical unit type 1.0 or type 2.0 attached to the rightmost controller can access applications in any of the two S/390 servers.

Host-dependent logical units (LUs) need a control session with their VTAM system services control point (SSCP). This SSCP-LU session allows the dependent LUs to request VTAM to set up LU-LU sessions for them. Once an LU-LU session has been established, the dependent LU (secondary LU) can exchange data with the application LU (primary LU).

In an APPN environment, the dependent LUs (DLU) must reside on, or be owned by an APPN node providing the DLUR function. The DLUR node requests the dependent logical unit server (DLUS) of a VTAM network node to provide the SSCP services for its dependent LUs. To support session establishment for the dependent LUs, the traditional SSCP-PU or SSCP-LU data flows through two LU 6.2 sessions between the DLUR node and DLUS node.

The 3746-9x0 provides the DLUR function, in conjunction with the DLUS support provided by VTAM Version 4 Release 2 or higher level. In a network with multiple VTAMs, only one VTAM with DLUS support is required.

The DLUS can be in any APPN/HPR network, provided that an APPN path exists between the DLUS and each DLUR.

High-Performance Routing

The IBM 3746 Model 900 and 950 support the High-Performance Routing (HPR). HPR is an extension to the APPN architecture that takes advantage of fast links with low error rates. HPR enhances the routing mechanisms and provides the following benefits:

- Dynamic rerouting around failed nodes and links without session loss
- Better routing performance
- Enhanced congestion control which improves link efficiency
- Reduction of amount of storage required in intermediate nodes
- Very high data throughputs between the S/390® servers and the network
- Synergy with the Parallel Sysplex® processor implementation providing end-to-end non-disruptive path switching up to the applications. This includes the S/390® support of multi-node persistent session (product direction).

The HPR architecture is made of two layers:

- Automatic network routing (ANR), the HPR base, mainly in the intermediate nodes
- Rapid transport protocol (RTP), the HPR transport tower, in the edge nodes.

ANR is responsible for data packets routing across an HPR network. ANR uses a new form of addressing to identify routes through an HPR network. This addressing is based on the links and nodes that make up the route. It consists of labels which are contained in the data packet header – each label describing the outbound link to be taken to exit an intermediate node, processing performed in each intermediate node is reduced. ANR provides several functions, for example:

- Source-independent routing
- Connectionless, stateless, fast routing without hop-by-hop error recovery procedure (non-ERP mode)
- Discarding of incoming packets in the event of congestion.

RTP establishes end-to-end connections between edge nodes of the APPN/HPR network. Each RTP connection can carry traffic for multiple end-to-end user and control sessions. RTP relies on ANR to perform the packet forwarding across the HPR network and offers the following functions:

- Transport of APPN and SNA boundary traffic (DLUR)
- Selective transmission, based on class of service
- Flow control and network congestion avoidance: Automatic Rate Based (ARB)
- End-to-end error recovery and selective retransmission
- Non-disruptive rerouting around network failures.

HPR Multilink Transmission Group

Multilink Transmission Group (MLTG) enables the 3746 Models 900 and 950 to use a variable bandwidth on a single logical Transmission Group (TG) composed of multiple physical links or LANs, most helpful in situations where single or multiple sessions require more bandwidth than a single physical link or LAN can provide.

The MLTG is defined with a single TG number. It is reported and seen as a single TG by Topology Management, and viewed as a single TG in the route calculation process. Based on link error rates, error recovery may be run on an individual link basis. Links may be dynamically removed from the MLTG when no longer needed, thus resulting in cost savings. HPR MLTG is supported over SDLC, frame-relay and X.25 links, token-ring and Ethernet LANs.

3746 Model 900 as a Mixed SNA and APPN/HPR Node

In a mixed SNA and APPN/HPR network, as shown in Figure 36 on page 64, the 3746-900 NN can operate as an SNA node (PU type 4) for the network resources owned by the NCP running in the 3745, and as an APPN/HPR network node (PU type 2.1) for the resources owned by the 3746 APPN/HPR control point.

In Figure 36 on page 64, the 3745/3746-900 NN is channel-attached to a VTAM which operates as an interchange node (ICN). This ICN allows SNA devices connected to the SNA backbone to access applications over the APPN/HPR backbone, and SNA/APPN devices connected to the APPN/HPR backbone to access S/390 applications in the SNA backbone, therefore providing any-to-any networking.

X.25 Network Connectivity

The X.25 Support feature natively controls X.25 connections without using the support of NCP or NCP Packet Switching Interface (NPSI). It allows the 3746 to attach to private or public X.25 networks as DTE nodes for routing of APPN, SNA/DLUR, HPR, and IP traffic over those X.25 connections. Supported functions include:

- Support of Qualified Logical Link Control (QLLC) connections for APPN, SNA/DLUR, and HPR traffic
- Routing of mixed APPN, SNA/DLUR, HPR, IP, and SNA/NCP traffic on the same X.25 link
- PVC and SVC connections
- Up to 2.048-Mbps speed
- Direct DTE-to-DTE attachment
- Support of SDLC, frame-relay, ISDN, X.25, X.25 NCP, and X.25 NPSI links attached to a single Communication Line Processor (CLP).

Frame-Relay Networking

The IBM 3746 Models 900 and 950 provide frame-relay networking functions. They are similar to those provided by NCP for 3746-900, with the exception of frame-relay switching functions, refer to *3745/3746 Planning Series: Serial Line Adapters*, GA27-4235.

Physical Media

The 3746-900 network node and 3746-950 provide the same connectivity. They both support:

- Token-ring and Ethernet LANs
- Leased frame-relay links
- Switched and leased SDLC links
- ESCON channels
- Frame-relay network connections
- X.25 network connections

The 3746 network node supports RFC 1490, including:

- Frame-relay BAN
- Frame-relay BNN

More information about the adapters that support network node connectivity can be found in the *IBM 3745 Communication Controller Models A, IBM 3746 Nways Multiprotocol Controller, Models 900 and 950: Overview*.

3746-9x0 MAE APPN/HPR Implementation

The MAE, together with the Multi-Protocol Access Services V1R1 (MAS) software, has the The MAE has the capability of being an APPN network node (NN) with intermediate routing functions and provides network services to both APPN and LEN end nodes.

MAE Implementation Specifics

APPN over DLSw

The MAE supports APPN over DLSw for connectivity to nodes through a remote DLSw partner. An example is shown in Figure 37 on page 68. The MAE only supports remote DLSw.

Note: It is recommended that you use APPN over direct DLCs when available instead of APPN over DLSw.

When APPN is configured on the MAE to use a Data Link Switching (DLSw) port, DLSw is used to provide a connection-oriented interface (802.2 LLC Type 2) between the APPN component in the MAE and APPN nodes and LEN end nodes attached to a remote DLSw partner.

When configuring a DLSw port for APPN on the MAE, the network node itself is assigned a unique MAC and SAP address pair that enables it to communicate with DLSw. The MAC address for the network node is locally administered and must not correspond to any physical MAC address in the DLSw network.

Figure 37 on page 68 shows how TCP/IP and DLSw are used to transport APPN traffic over an IP network.

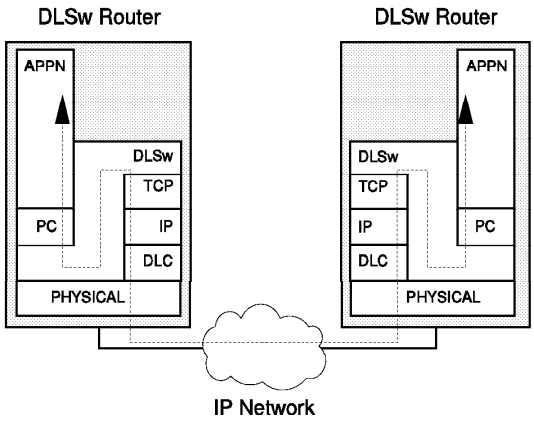


Figure 37. APPN over DLSw

Supported Traffic Types

APPN ISR uses the QLLC protocol for X.25 direct data link control, the IEEE 802.2 LLC Type 2 protocol for token-ring, Ethernet, PPP, and frame-relay and SDLC protocol for the SDLC data link control. APPN HPR, which is supported on token-ring, Ethernet, PPP and frame relay, does not use LLC Type 2 protocol, but does use some functions of an APPN link station for XID and inactivity timeout. A single APPN link station is therefore used for ISR or HPR. Different mechanisms are used to distinguish between ISR and HPR traffic depending upon the DLC type:

For token-ring and Ethernet LAN ports

Each protocol that uses a port must have a unique SAP address, with the exception of DLSw (which may use the same SAP address as other protocols because DLSw frames will not be destined for the local MAC address, but rather a DLSw MAC address). A unique SAP address identifies the APPN link station for HPR traffic (local HPR SAP address parameter). If ISR traffic is destined for a link station, then a different SAP address (local APPN SAP address parameter) must be used. The ISR traffic uses LLC Type 2 LAN frames. The HPR traffic is handled in a similar fashion to LLC Type 1 LAN frames and must have a different SAP address. The default SAP address for HPR traffic is X'C8'. If X'C8' has already been used by another protocol on a port, the default must be overridden. Note that there is only one APPN link station even though APPN ISR and HPR traffic use different SAP addresses.

For frame-relay ports

APPN ISR traffic and APPN HPR traffic transferred over a frame-relay data link connection support both the RFC 1490 bridged frame format and the RFC 1490 routed frame format. RFC 1490 routed frame format APPN ISR traffic will be transferred over a frame-relay data link connection using the connection-oriented multiprotocol encapsulation method defined in RFC 1490 using:

- NLPID = X'08' (Q.933 encoding)
- L2PID = X'4C80' (Layer 2 protocol identifier indicating 802.2 LLC)
- L3PID = X'7083' (Layer 3 protocol identifier indicating APPN)

APPN HPR traffic transferred over a frame-relay data link connection does not use IEEE 802.2 LLC. It uses a different multiprotocol encapsulation as defined in RFC 1490 using:

- NLPID = X'08' (Q.933 encoding)
- L2PID = X'5081' (Layer 2 protocol identifier for no Layer 2 protocol)
- L3PID = X'7085' (Layer 3 protocol identifier indicating APPN HPR)

APPN HPR does not use a SAP for traffic transferred using the RFC 1490 routed frame format because there is no Layer 2 protocol. APPN HPR uses a SAP for traffic transferred using the RFC 1490 bridged frame format.

The IBM 2210 and 2216 support both the routed and bridged frame formats, the 6611 supports only the routed frame format.

For PPP ports

APPN ISR traffic uses 802.2 LLC over the PPP connection. Since there is no Layer 2 protocol used in HPR's RFC 1490 encapsulation (non-ERP), no SAP is used for HPR traffic.

Topology Safestore

Topology and Routing Services (TRS) can store the APPN topology database on the 3746 NNP and 3746 Multiaccess Enclosure hard disks. In order to reduce the number of topology database updates (TDUs) transmitted over the network, the backup copy of the topology database is restored when the APPN topology database maintained in the NNP and MAE memory is lost due to either a power loss or reboot. After the topology database is retrieved from the hard disk during start up, TRS advertises the last TDU sequence number received by the NNP and MAE. Only APPN network changes made after that sequence number will be broadcast. Without this feature, a complete set of TDU broadcasts are sent that significantly increases network traffic.

The NNP and MAE only save the topology to their hard disks once a day during garbage collection.

Route Test

Currently, HPR's route test can only be invoked through SNMP. Two variations of route test exist. The first tests the wrap-around time of an established HPR connection. This route test is invoked specifying the NCL and RTP connection identifiers of an HPR connection. The NCL and RTP connection identifiers are unique identifiers used to identify HPR connections. These identifiers can be retrieved from the HPR RTP connection table MIB information.

The second tests the wrap-around time of an APPN selected route to a specified destination node. This route test is invoked specifying the APPN network and LU name of the destination node and the mode used for the session. APPN's route selection algorithm is used to calculate the best route to the destination. If the selected route is an HPR connection originating at the 3746 Multiaccess Enclosure, the route is then tested.

When a route test is initiated, a separate time-stamped message is sent to each node within the HPR connection. At the destination node, the message is returned to the originating node. The route test message is only processed by the NCL forwarders in the intermediate and destination nodes. Upon receipt of the returned route test message, the wrap-around time is recorded along with the corresponding node. The individual link rates can be calculated by comparing the round-trip time for each route test message.

User API

The MAE implementation of APPN does not provide an application program interface to support user-written LU 6.2 programs.

Limited Resource Link Stations

On the MAE, limited resource link stations are supported on the following links:

- Connection network links
- X.25 SVC links (Previewed for APPN)
- PPP links running over ISDN or V.25 bis
- Frame-relay links running over ISDN.

Session-Level Security

A session-level security feature can be enabled for connections between the MAE network node and an adjacent node. Both partners require a matching hexadecimal key that enables each node to verify its partner before a connection is established.

Parallel TGs

Parallel TGs are not supported between two router network nodes using the same port on each router. However, parallel TGs are supported between two router network nodes using different ports on one or both routers. Also, parallel TGs are supported between a router network node and another non-router remote node over the same port using different remote SAP addresses, provided that the remote node has a mechanism to define or accept different local SAP addresses for APPN on the same port.

DLUR Restrictions

The DLUR option, as implemented on the router network node, has the following functional restrictions:

- Only secondary LUs (SLUs) can be supported by the DLUR function. An LU supported by DLUR cannot function as a primary LU (PLU). Therefore, the downstream physical unit (DSPU) should be configured as secondary.
- Because only SLUs are supported, Network Routing Facility (NRF) and Network Terminal Option (NTO) are not supported. Extended recovery facility (XRF) and XRF/CRYPTO are not supported.
- You must be able to establish an APPN-only or APPN/HPR-only session between DLUS and DLUR. The CPSVRMGR session cannot pass through a subarea network.

Connection Network Restrictions

The router APPN support has the following connection network restrictions:

- Connection networks defined on the router network node are only supported on token-ring and Ethernet LAN ports.
- The same connection network (VRN) can be defined on only one LAN. However, the same VRN can be defined on multiple ports having the same characteristics to the same LAN.

- The same connection network can be defined on a maximum of five ports to the same LAN on the router network node.
- There is only one connection network TG from a given port to a given connection network's VRN.
- The same connection network TG characteristics apply for each port on which a given connection network is defined on this router network node. The TG characteristics could be different on a different node.
- Because the VRN is not a real node, CP-CP sessions cannot be established with or through a VRN.
- When a connection network is defined on the router network node, a fully qualified name is specified for the connection network name parameter. Only connection networks with the same network ID as the router network node may be defined. The network ID of the VRN is then the same as the network ID of the router network node.

APPN over DLSw Restrictions

The following restrictions apply to APPN over DLSw:

- Connectivity through remote DLSw partners only
- Only 1 DLSw port per router
- Use of a locally administered MAC address
- HPR is not supported on DLSw ports
- DLSw ports cannot be members of connection networks
- Parallel TGs are not supported over more than one DLSw port.

  A parallel TG may contain a single DLSw port, and any combination of other supported DLCs, but a parallel TG may never contain more than one DLSw port.

Summary of Implemented APPN Functions

Note: See the notes at the end of the tables (page 74) for abbreviations and explanation of terms used.

Table 12 (Page 1 of 3). Summary of Implemented Base Functions (APPN Version 2). "CS OS/390" refers to the IBM eNetwork Communications Server for OS/390® product, which contains VTAM.

Function		CS OS/390 (VTAM)	3746	3746
Option Set	**Description**	**V2 R8**	**NNP**	**MAE FC 3001**
Configuration Services				
001	LEN-level XID3	EN/NN	NN	NN
002	All XID3 States	EN/NN	NN	NN
003	Link Station Role Negotiation	EN/NN	NN	NN
006	CP Name on XID3	EN/NN	NN	NN
007	TG Number Negotiation	EN/NN	NN	NN
008	Multiple TGs	EN/NN	NN	NN
010	Single-Link TG	EN/NN	NN	NN
1001	Secondary-Initiated Non-Activation XID	EN/NN	NN	NN
1004	Adjacent Node Name Change	EN/NN	NN	NN
Intermediate Session Routing				
011	LFSID Addressing	EN/NN	NN	NN
013	Priority Queuing for Transmission	2	NN	NN
Address Space Manager				
020	Extended BIND and UNBIND	EN/NN	NN	NN
021	Adaptive Pacing for Independent LU BINDs	3	NN	NN
023	Bind Segmenting and Reassembly	-	NN	NN
024	Adaptive Pacing for Dependent LU BINDs	-	NN	NN
Session Services				
030	CP-CP Sessions	EN/NN	NN	NN
031	CP-CP Capabilities Exchange	EN/NN	NN	NN
033	FQPCID Generation	EN/NN	NN	NN
034	CD-Initiate	EN/NN	NN	NN
035	Reconstruct CD-Initiate Reply	EN/NN	NN	NN
036	COS/TPF	EN/NN	NN	NN
037	BIND (ILU=PLU)	EN/NN	NN	NN
038	Limited Resource	EN/NN	NN	NN
039	BIND without RSCV from Any LEN or APPN Node	EN/NN	NN	NN
040	Propagate Unrecognized CVs	NN	NN	NN
041	Session RU Segmenting and Reassembly	EN/NN	NN	NN
042	Interleaved Segments	EN/NN	NN	NN
1015	CP-CP Session Activation Enhancements	EN/NN	NN	NN
Directory Services				
050	Register EN Resources	EN/NN	NN	NN
051	Locate/Find/Found	EN/NN	NN	NN
052	Reconstruct GDS Variables for Locate Reply and CD-Initiate Reply	EN/NN	NN	NN
053	Participate in Network Searches	EN/NN	NN	NN
054	Send Wildcard Reply	7	NN	NN
055	Broadcast and Directed Searches	EN/NN	NN	NN
056	ENCP Search Control	EN/NN	NN	NN
057	Partial Directory Entries	-	NN	NN
059	Accept Unqualified LU Name	EN/NN	NN	NN
060	Locate Chains - Locate(keep)	EN/NN	NN	NN
061	Sending Locate to a Gateway	NN	NN	NN
062	Cache Resource Locations	NN	NN	NN
063	Favor Explicit Replies	NN	NN	NN
064	Network-Qualified LU Names	EN/NN	NN	NN
065	Central Directory Client	NN	NN	NN
066	Abbreviated Resource Hierarchy	NN	NN	NN

Table 12 (Page 2 of 3). Summary of Implemented Base Functions (APPN Version 2). "CS OS/390" refers to the IBM eNetwork Communications Server for OS/390® product, which contains VTAM.

Function		CS OS/390 (VTAM)	3746	3746
Option Set	**Description**	**V2 R8**	**NNP**	**MAE FC 3001**
068	Authentic Net ID Indicator	EN/NN	NN	NN
069	DS Support for Domain LEN Resources	EN/NN	NN	NN
1103	Retry Referred Search	NN	NN	NN
1104	Topology-Based Directory Nonverify	5	NN	NN
1105	PCID Modifier	EN/NN	NN	NN
1109	Surrogate Owner	NN	NN	NN
1117	Bypass of Directed Locate Not Allowed	5	-	-
1119	Report Branch Topology to Manager	NN	NN	NN
1120	Branch Awareness	NN	NN	NN
1121	Branch Extender Function	NN	NN	NN
Topology and Routing Services				
070	Process Local Resource Change	EN/NN	NN	NN
073	Initial Topology Exchange	EN/NN	NN	NN
074	Flow Reduction Sequence Numbers	EN/NN	NN	NN
075	Resource Sequence Numbers	EN/NN	NN	NN
076	Topology Broadcast	NN	NN	NN
077	Garbage Collection	NN	NN	NN
078	Topology Isolation at Net ID Boundaries	NN	NN	NN
079	Build RSCV	NN	NN	NN
080	Calculate Route Using Connection Networks	NN	NN	NN
081	Class-of-Service Manager	EN/NN	NN	NN
082	Route Randomization	NN	NN	NN
083	Member of Connection Network	EN/NN	NN	NN
084	Select One-Hop Routes	NN	NN	NN
085	Select Network Routes	NN	NN	NN
086	Topology Awareness of CP-CP Sessions	NN	NN	NN
087	Garbage Collection Enhancements	NN	NN	NN
088	TDU Flow Improvements	NN	-	-
1202	Safe-Store of Topology DB	NN	NN	NN
Node Operator Command Set				
090	Common Node Operator Command Set	EN/NN	NN	-
091	Network Node Operator Command Set	NN	NN	-
Intermediate Session Routing				
100	Extended/Unextended BIND and UNBIND	EN/NN	NN	NN
101	Fixed Session-Level Pacing	EN/NN	NN	NN
102	Adaptive Session-Level Pacing	EN/NN	NN	NN
103	Intermediate Session Segmenting/Reassembly	-	NN	NN
104	Routing BIND and UNBIND	EN/NN	NN	NN
105	Intermediate Session Routing for Dependent LU Sessions	EN/NN	NN	NN
106	Intermediate Session Routing for Type 6.2 LU-LU Sessions	EN/NN	NN	NN
Management Services - Multiple-Domain Support				
150	MDS Common Base	4	NN	NN
151	MDS End Node Support	4	NN	-
152	MDS Network Node Support	4	NN	NN
153	MDS High Performance Option	4	-	-
154	MDS Transport Confirmation Option	-	-	-
Management Services - MS Capabilities				
160	MS_CAPS Base End Node Support	4	NN	-
161	MS_CAPS Have a Backup or Implicit FP	4	NN	1
162	MS_CAPS Be a Sphere of Control End Node	4	-	-
163	MS_CAPS Base Network Node Support	4	NN	NN
164	MS_CAPS Have a Subarea FP	6	-	-
Management Services - Entry Point Alerts				

Table 12 (Page 3 of 3). Summary of Implemented Base Functions (APPN Version 2). "CS OS/390" refers to the IBM eNetwork Communications Server for OS/390® product, which contains VTAM.

Function		CS OS/390 (VTAM)	3746	3746
Option Set	**Description**	**V2 R8**	**NNP**	**MAE FC 3001**
170	EP Alert Base Subset	4	NN	NN
171	Problem Diagnosis Data in Alert	-	NN	NN
174	Operator-Initiated Alert	4	-	-
175	Qualified Message Data in Alert	-	-	-
176	Self-Defining Message Text Subvector in Alert	-	-	-
177	LAN Alert	-	-	-
178	SDLC/LAN LLC Alert	-	-	-
179	X.21 Alert	-	-	-
180	Hybrid Alert	-	-	-
181	X.25 Alert	-	-	-
182	Held Alert for CPMS	-	-	NN
183	Resolution Notification Support	-	-	-
184	Operations Management Support in Alert	-	-	-
Miscellaneous				
1013	Inter-operability with Peripheral Border Node	NN	NN	NN

Notes:

EN/NN = End Node and Network Node

NN = Network Node

- = Not Supported

1 Backup Focal Point only.

2 Supported by NCP's BF only.

3 VTAM will respond to a BIND pacing request received, but will never set the pacing request indicator on a BIND.

4 Function supported through NetView.

5 VTAM does perform topology database lookup (to see if an unknown resource is a NNCP), but does not skip sending the APPN locate. This locate is then sent as a directed search to the NN. Because of this processing, VTAM has implemented option set 1117.

6 VTAM/NetView can be the alert focal point for EP_ALERTs (function sets 170 to 184, except for 174), but does not generate EP_ALERTs itself.

7 In some cases, CS OS/390 sends wildcard replies, but does not allow wildcard definitions.

Table 13 (Page 1 of 2). Summary of Implemented Optional Functions (APPN Version 2). "CS OS/390" refers to the IBM eNetwork Communications Server for OS/390 product, which contains VTAM.

Function		CS OS/390 (VTAM)	3746	3746
Option Set	**Description**	**V2 R8**	**NNP**	**MAE FC 3001**
Configuration Services				
1002	Adjacent Link Station Name	EN/NN	NN	NN
1003	Short-Hold Mode	EN/NN	-	-
1006	Dynamic Name Change	EN/NN	-	-
1007	Parallel TGs	EN/NN	NN	NN
CP Capabilities				
1011	Multiple Local LUs	EN/NN	NN	-
1012	LU Name = CP Name	-	NN	NN
1014	Peripheral Border Node	-	-	-
1016	Extended Border Node	NN	-	NN
1017	Gateway	-	-	-
1018	Delete EN Resources Before Registering	EN/NN	-	-
Dependent LU Support				
1060	Prerequisite for Session Services Extensions CP Support	EN/NN	NN	NN
1061	Prereqs. for SSE NNS Support	NN	NN	NN
1062	Session Services Ext. CP Support	EN/NN	NN	NN
1063	Session Services Ext. NNS Support	NN	NN	NN
1064	Session Services Ext. PLU Node Support	EN/NN	-	-
1065	Session Services Ext. CP(SLU) (SSCP) Support	EN/NN	-	-
1066	Dependent LU Server	NN	-	-
1067	Dependent LU Requester	-	NN	NN
1071	Generalized ODAI Usage	-	NN	NN
Cryptography Support				
1070	Session Cryptography	EN/NN	-	-
Directory Services				
1100	Safe-Store of Directory Cache	NN	-	-
1101	Preloaded Directory Cache	NN	NN	NN
1102	EN Authorization	-	-	-
1106	Central Directory Server	NN	-	-
1107	Central Resource Registration (of LUs)	EN/NN	NN	NN
1108	Nonverify	2	-	-
1116	DLUS-Served LU Registration NNS Support	NN	NN	NN
1118	EN TG Vector Registration	EN/NN	-	-
Topology and Routing Services				
1200	Tree Caching and TG Caching	NN	NN	NN
1201	Permanent Storage Medium	EN/NN	NN	NN
1203	Detection and Elimination of TDU Wars	3	NN	NN
Intermediate Session Routing				
1300	Tuning Values for ISR	EN/NN	NN	-
1301	Nonpaced Intermediate Session Traffic	EN/NN	-	-
High Performance Routing				
1400	HPR Base (ANR)	NN	NN	NN
1401	Rapid Transport Protocol	EN/NN	NN	NN
1402	Control Flows over RTP	EN/NN	NN	NN
1403	Dedicated RTP Connections	-	-	-
1404	Multilink TG (MLTG)	-	NN	-
1405	HPR Border Node	NN	-	NN

Table 13 (Page 2 of 2). Summary of Implemented Optional Functions (APPN Version 2). "CS OS/390" refers to the IBM eNetwork Communications Server for OS/390 product, which contains VTAM.

Function		CS OS/390 (VTAM)	3746	3746
Option Set	**Description**	**V2 R8**	**NNP**	**MAE FC 3001**
Management Services - File Services				
1500	File Services Support Base	-	-.	-
1501	Network Operator Support for File Services	-	-	-
Management Services - Change Management				
1510	CM Base	-	-	-
1511	CM Production Only Activate	-	-	-
1512	CM Execution Window Timing	-	-	-
1513	CM Activate Report	-	-	-
1514	CM Alter Active Install	-	-	-
1515	CM Object Disposition Install	-	-	-
1516	CM Initiate Command	-	-	-
1517	CM Cancel Command	-	-	-
1518	CM Activate Last	-	-	-
Management Services - Operations Management				
1520	Common Operations Services	-	-	-
1521	Operations Management	1	-	-

Notes:

EN/NN = End Node and Network Node

NN = Network Node

- = Not Supported

1 Function provided by NetView.

2 Only at the NN(OLU).

3 CS OS/390 support is prestandard; most of the option set is implemented.

Summary of Supported DLCs and APPN Functions

The following table gives an overview of the DLC types supported by APPN capable hardware. The APPN function supported over these DLCs are listed.

Table 14. Summary of Supported DLCs and APPN Functions

DLC TYPE	MAE	3746
Token-Ring	IHD	IHD
Ethernet	IHD	IHD
Twinax	n/a	n/a
Frame-Relay BNN	IHD	IHD
Frame-Relay BAN	IHD	IHD
Point-to-Point Protocol	IH	n/a
APPN over DLSw	ID	ID (see note)
HPR over IP	H	H (see note)
SDLC Leased Line	ID	IHD
X.25 PVC and SVC (Previewed)	ID	IHD
APPN over PPP over ISDN	IH	n/a
APPN over Frame Relay over ISDN	IHD	n/a
APPN over ATM Forum Compliant LAN Emulation	IHD	n/a
Native HPR over ATM	H	n/a
APPN over PPP over V.25 bis	IH	n/a
SNA over Asynch	n/a	n/a
ESCON	IH	IH
PARALLEL CHANNEL	IH	n/a

Note: Needs the MAE installed.

Legend:

I = Intermediate Session Routing

H = High-Performance Routing

D = Dependent LU Requester, this refers to the port providing the connection to the downstream PU (DSPU).

Chapter 2. Internet Protocol (IP) Overview

This chapter gives an overview of the Internetwork Protocol (IP). It is not just one protocol, but a group of protocols that make up an architecture designed for communication between and across diverse network platforms and network architectures. (The word *internet* used here refers to internetwork operations in general rather than the cooperative public domain network known as *the Internet*.)

This chapter describes:

- The need for a means of communicating across multiple network architectures
- How IP meets those needs
- The main features of IP

The Need for Transparency in Communication

The computer networks of large organizations have evolved through the merger, interconnection, and expansion of previously autonomous networks. Such interconnected networks support diverse protocols, multiple speed requirements, and incompatible topologies. For example, suppose there is a community of users, A, B, C, and D, see Figure 38, who need to reach each other across four networks.

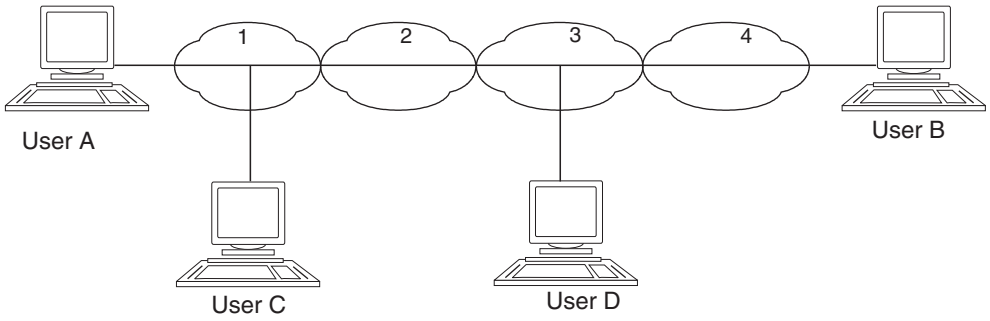


Figure 38. Communicating across Multiple Networks

They would each need to know about intervening networks:

- Users A and C only need to know about Network 1.
- Users B and D need to know about each other's networks (3 and 4).
- Users A and C, and User B, need to know about ***all*** networks between them before they can communicate (1, 2, 3, 4), including two (2 and 3) to which they are not themselves connected.

This is obviously an impractical and unsatisfactory situation.

A solution is one that overlays existing network architectures and provides a single unified view of all networks between any two users or applications.

The Internet Protocol (IP) is just such an architecture[2] . IP provides a unified appearance to users and applications independent of the actual networks

[2] Internet also refers to an *interconnected network*, a network consisting of two or more otherwise autonomous networks.

connecting them by the simple expedient of a common addressing scheme. This relationship of IP to networks is shown in Figure 39 on page 80.

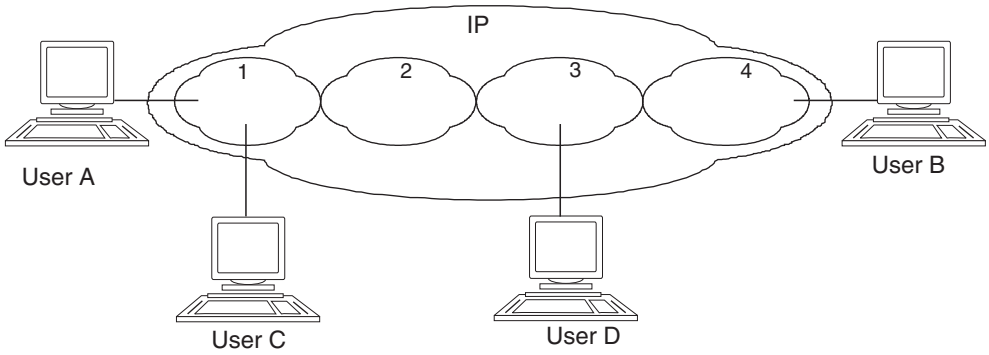


Figure 39. The Internet Protocol (IP) Overlays Networks

To communicate with each other now, users need only know the IP address of their target destination. Communication is handled transparently across all intervening networks. A 3746 Network Node with the IP Feature (FC 5033) can be used to connect incompatible or independent networks. Its role is to route data from one network to the other, and when used in this context, is called an *IP router*, or *IP gateway*.

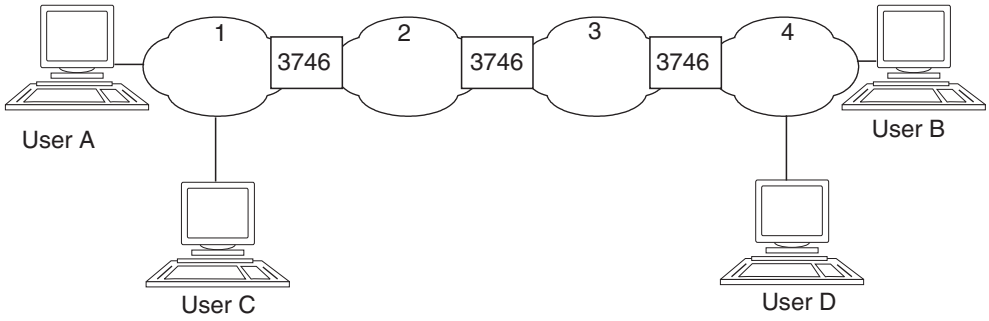


Figure 40. 3746 Network Nodes with the IP Feature (FC 5033). They link the networks and route data between the them.

Physically, users are connected into their local respective networks. The IP addressing scheme is known to the 3746 Network Node IP routers that connect the networks, so they can forward data if the destination address is in a network different to the source address.

IP Addressing

The addressing scheme provides a network-transparent means of communicating. To send data, you only need to know the destination address, regardless of what types of network serve source and destination, and regardless of any intervening type of network.

The IP Address

IP addresses can be symbolic or numeric. The symbolic form is easier to read; for example:

```
myname@ibm.com.
```

The numeric form is a 32-bit unsigned binary value that is normally expressed in *dotted decimal format*. For example:

```
128.2.7.9
```

is a valid Internet address. Its binary form is:
B'10000000 00000010 00000111 00001001'
The numeric form is used by the IP software, which also provides the mapping from symbolic to numeric forms.

IP Address Classes

The address shown above is an example of one class of IP address but is not suitable for all network configurations. The proportion of networks to hosts can be vastly different from one enterprise to another. IP addresses are thus arranged in ***classes*** to suit different network characteristics. See Figure 41

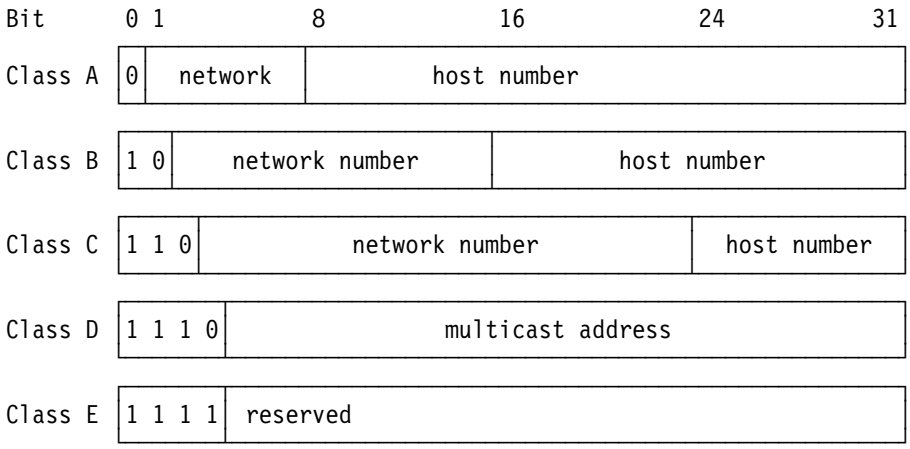


Figure 41. Classes of IP Addresses

Each class, having a different proportion of network number to host number, can be assigned to different sizes of network. See Table 15.

Table 15. Use of IP Address Classes

Class	Maximum Number of Networks	Maximum Number of Hosts per Network
A	126	16 777 214
B	16382	65534
C	2 097 150	254
D	Not applicable	Not applicable
E	Not applicable	Not applicable

Host and Network Numbers

The IP address consists of a pair of numbers:

```
IP address = <network number><host number>
```

The network number is administered centrally by the Internet Network Information Center (the InterNIC) and is unique for each network. The host number (also known as host address or host ID), is assigned to each host within a network and belongs to the authority that owns the network. Table 16 shows the components of the example address given in "The IP Address" on page 81.

Table 16. IP Address Structure

IP address=	<Network number>	<Host number>
128.2.7.9	128.2	7.9

IP Addresses for Routers

A router appears on both networks it connects. It must have a network number and a host number to make a complete IP address. For example, suppose a router routes data between networks 128.2 and 131.5.

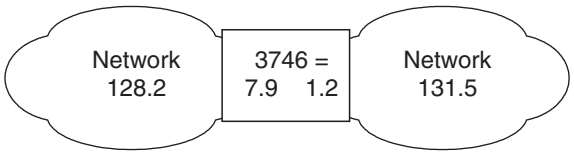


Figure 42. Routers Need Two Addresses

It must only have one address when seen from each network, but each network has its own network number. Thus, the router must have two addresses, one for each network it connects. Its resulting addresses are shown in Table 17.

Table 17. IP Addresses for a Router

IP address	Network number	Host number
128.2.7.9	128.2	7.9
131.5.1.2	131.5	1.2

Note: A ***router*** is not the same as a ***bridge***, despite the apparent similarity of their positions between networks.

Subnets

With the massive growth of networks, the use of assigned IP addresses becomes too inflexible to allow easy changes to local network configurations. These changes can occur when:

- A new physical network is installed.
- Growth of the number of hosts requires splitting the local network into two or more separate networks.
- Reorganization of an enterprise requires new address structures.

To avoid having to request additional IP network addresses in these cases, the concept of *subnets* was introduced. The host number part of the IP address is subdivided again into a network number and a host number. This second network is termed a *sub-network* or *subnet*.

Subdividing the Network

The main network now consists of a number of subnets and the IP address is interpreted as:

```
IP address=<network number> <<subnet number><host number>>
```

The combination of the subnet number and the host number is often termed the *local address* or the *local part*.

Subnetting is transparent to remote networks. A host within a network which has subnets is aware of the subnetting but a host in a different network is not. It still regards the local part of the IP address as a host number.

Administrators can assign subnet addresses to represent, for example:

- Groups of similar types of host
- Departmental clusters of hosts
- Hierarchical or security level of the host users.

Subnets provide a customizable address system within the IP address scheme.

Note: They do not have to represent the physical network connections, as it is a purely *logical* addressing system.

The Subnet Mask

The division of the local part of the IP address into subnet number and host number parts can be chosen freely by the local administrator. Any bits in the local part can be used to form the subnet. The division is done using a *subnet mask*, which is a 32-bit number:

- Ones (1) indicate bit positions assigned to the subnet number.
- Zero (0) bits in the subnet mask indicate bit positions assigned to the host number.

The bit positions in the subnet mask belonging to the network number are set to ones but are not used. Subnet masks are usually written in dotted decimal form, like IP addresses. The special treatment of ***all bits zero*** and ***all bits one*** applies to each of the three parts of a subnetted IP address just as it does to both parts of an IP address that has not been subnetted.

Example Subnet Mask

For example, a subnetted Class B network, which has a 16-bit local part, could use one of the following schemes:

- The first byte is the subnet number, the second the host number. This gives us 254 (256 minus 2 with the values 0 and 255 being reserved) possible subnets, each having up to 254 hosts. The subnet mask is `255.255.255.0`.
- The first 12 bits are used for the subnet number and the last four for the host number. This gives us 4094 possible subnets (4096 minus 2) but only 14 hosts per subnet (16 minus 2). The subnet mask is `255.255.255.240`.

There are many other possibilities.

Building Good Masks

While the administrator is completely free to assign the subnet part of the local address in any legal fashion, the objective is to assign a number of bits to the subnet number and the remainder to the local address. Therefore, it is normal to use a contiguous block of bits at the beginning of the local address part for the subnet number because this makes the addresses more readable (this is particularly true when the subnet occupies 8 or 16 bits). With this approach, either of the subnet masks above are good masks, but masks such as `255.255.252.252` and `255.255.255.15` are not.

Multiple Destinations

The point of the IP addressing scheme is to get messages, whatever their content, from one user to another. There are three ways this might be done:

- Unicasting. The majority of IP addresses refer to a single recipient. These are called *unicast addresses*.
- Broadcasting. Messages are sent out to every user on the network.
- Multicasting. Messages are broadcast to a select group of users.

There are two special types of IP address that are used for addressing multiple recipients:

- Broadcast addresses
- Multicast addresses.

These addresses are used for sending messages to multiple recipients. Each requires different handling from the point of view of IP addressing.

Broadcasting

There are a number of addresses that are used for IP broadcasting. All use the convention that all-bits-1 indicates all-addresses. Broadcast addresses are never valid as source addresses, only as destination addresses. The different types of broadcast address are listed here:

Limited broadcast address

The address 255.255.255.255 (1s in all bits of the IP address) or 0.0.0.0 (0s in all bits of the IP address) is used on networks that support broadcasting, such as token-rings, and it refers to all hosts on the subnet. It does not require the host to know any IP configuration information at all. All hosts on the local network will recognize the address, but routers will never forward it.

Network-directed broadcast address

If the following conditions are true:

- The network number is a valid network number
- The network is not subnetted
- The host number is all ones or all zeros.

then the address, for example, `128.2.255.255`, refers to all hosts on the specified network `128.2`. Routers should forward these broadcast messages unless configured otherwise.

Subnet-directed broadcast address

If the following conditions are true:

- The network number is a valid network number
- The subnet number is a valid subnet number
- The host number is all ones or all zeros.

then the address refers to all hosts on the specified subnet. Since the sender's subnet and the target subnet may have different subnet mask, the sender must somehow find out the subnet mask in use at the target. The actual broadcast is performed by the router which receives the datagram into the subnet.

Multicasting

Broadcasting has a major disadvantage - its lack of selectivity. If an IP datagram is broadcast to a subnet, every host on the subnet will receive it, and have to process it to determine whether the target protocol is active. If it is not, the IP datagram is discarded. Multicasting avoids this overhead by using groups of IP addresses. Each group is represented by a 28-bit number, which is included in a Class D address. See Figure 41 on page 81.

Multicast group addresses are IP addresses in the range 224.0.0.0 to 239.255.255.255. For each multicast address there is a set of zero or more hosts which are listening to it. This set is called the *host group*. There is no requirement for any host to be a member of a group to send to that group.

There are two kinds of host groups:

Permanent

The IP address is permanently assigned. The membership of a host group is not permanent; a host may leave or join the group at will. Some IP addresses are assigned permanently to host groups. Important ones are:

- 224.0.0.0 - Reserved base address
- 224.0.0.1 - All systems on this subnet
- 224.0.0.2 - All routers on this subnet.

A permanent group exists even if it has no members.

Transient

Any group which is not permanent is transient and is available for dynamic assignment as needed. Transient groups cease to exist when their membership drops to zero.

Domains

The system of symbolic names (see "The IP Address" on page 81,) is more convenient to use than the IP numeric address structure. However, this requires:

- The mapping of all host names to their numeric addresses
- The maintenance of a database in all hosts of such a mapping
- Considerable work in sending changes in the database to all possible hosts.

In all but the smallest networks this is an almost impossible task. An alternative method is required.

A new concept was developed to handle this problem. The whole Internet community was divided into *domains*, and the mapping of symbolic names to IP addresses called the *Domain Name System*.

The Domain Name System allows a program running on a host to perform the mapping of a high-level symbolic name to an IP address for any other host. It does, however, require a formalized use of symbolic names if mapping is to be successful.

The Hierarchical Name Space

Consider the internal structure of a large organization. As the chief executive cannot do everything, the organization will probably be partitioned into divisions, each of them having autonomy within certain limits. Specifically, the executive in charge of a division has authority to make direct decisions, without permission from the chief executive. Domain names are formed in a similar way, and will often reflect the hierarchical delegation of authority used to assign them.

For example, consider the name `lcs.mit.edu`. The lowest-level domain name, `lcs`, is a subdomain of `mit`, which again is a subdomain of `edu` (education) which is called a top-level domain. We can also represent this naming concept by a hierarchical tree. See Figure 43.

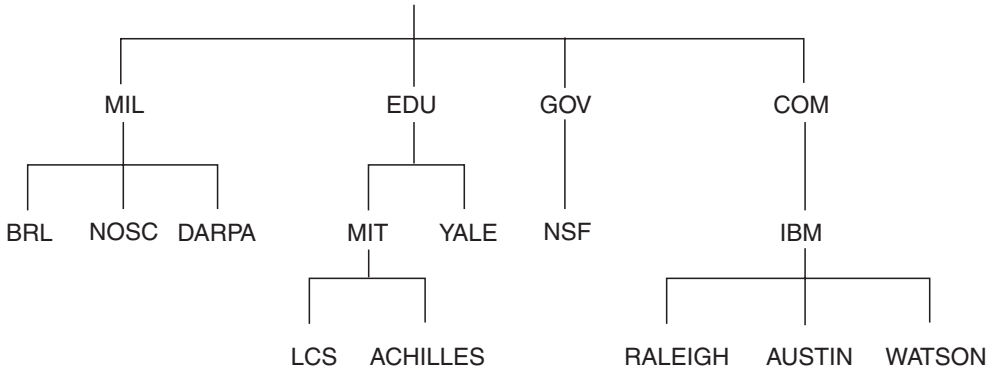


Figure 43. Hierarchical Structure of Domains

Figure 43 shows the chain of authority assigning domain names. This tree is only a tiny fraction of real namespace. Table 18 on page 87 shows some of the top-level domains. The single domain above the top-level domains has no name and is referred to as the root domain.

Fully Qualified Domain Names (FQDNs)

When using the Domain Name System, it is common to work with only a part of the domain hierarchy, for example the `ral.ibm.com` domain. The Domain Name System provides a simple method of minimizing the typing necessary in this circumstance. If a domain name ends in a dot, for example, `wtscpok.itsc.pok.ibm.com.` it is assumed to be complete. This is termed a Fully Qualified Domain Name (FQDN) or an absolute domain name. If, however, it does not end in a dot, for example `wtscpok.itsc` it is incomplete and will be completed by appending a suffix such as `.pok.ibm.com` to the domain name. The rules for doing this are implementation dependent and locally configurable.

Generic Domains

The three-character top-level names are called the *generic domains* or the *organizational* domains.

Table 18. The Generic Top-Level Domains

Domain Name	Meaning
edu	Educational institutions
gov	Government institutions
com	Commercial organizations
mil	Military groups
net	Networks
int	International organizations
org	Other organizations

The organization of the hierarchical namespace initially had only US organizations at the top of the hierarchy, and it is still largely true that the generic part of the namespace contains US organizations. However, only the **.**gov and **.**mil domains are restricted to the US.

Country Domains

There are also top-level domains named for each of the ISO 3166 international two-character country codes, for example **.**uk for the United Kingdom and **.**nl for the Netherlands. These are called the *country domains* or the *geographical domains*.

Many countries have their own second-level domains which parallel the generic top-level domains. For example, in the United Kingdom, the domains equivalent to the generic domains **.**com and **.**edu are .co.uk and .ac.uk (ac is an abbreviation for academic).

3746-9x0 Router Node Implementation

The 3746 Nways Controller Models 900 and 950 provide the following set of IP functions:

- IP routing providing connectivity over:
  - ESCON channels:
    To IBM and other equipment manufacturers (OEM) processors that adhere to the ESCON architecture, possibly via one or two cascaded ESCON directors (IBM 9032 or 9033).
  - Token-ring LANs
  - Ethernet LANs:
    Ethernet access requires the 3746-9x0 Ethernet feature. Refer to “Ethernet Adapters” chapter in the *3745/3746 Planning Series: Token Ring and Ethernet* and “Physical Planning Details” chapter in the *3745/3746 Planning Series: Physical Planning* for detailed information on this feature.
  - Leased lines:
    Leased lines using either the PPP or frame-relay protocol.

  - Frame-relay and X.25 networks
- Dynamic routing protocol support, using:
  - RIP Version 1
  - OSPF Version 2
  - BGP Version 4
- ARP and proxy ARP
- BOOTP relay.

If you use only one type of adapter, the maximum connectivity is up to:

- 16 ESCON channel couplers
- 32 token-ring couplers
- 32 line interface couplers, with 120 lines (of any permissible speed).

Overview of 3746 IP Routing

First, it is necessary to understand the model on which IP is based. Each station has to be attached to a least one network. Most often this is a local area network attachment, but stations might be attached via a serial line (PPP, or frame relay), or, for that matter, be ESCON-attached.

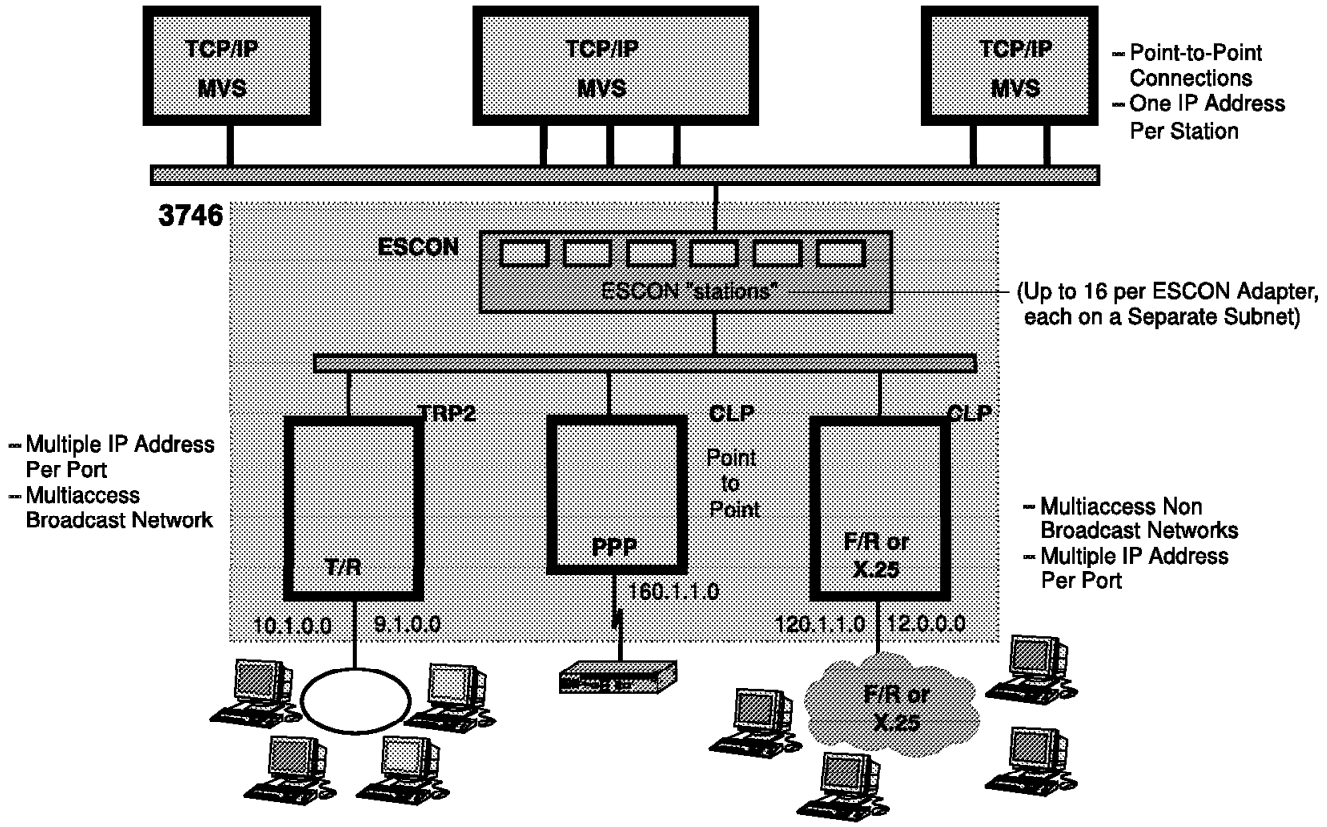


Figure 44. IP Address Support Example

Stations can send datagrams to any other system on its own network.

Networks can be:

- Multiaccess broadcast networks

  Multiaccess broadcast networks allow the attachment of multiple stations. To send data to a destination node attached to the same network, the physical address of the node must be learned, and direct communication can take place. Broadcasting allows a node to send a datagram to multiple stations at the same time.

  Examples of multiaccess broadcast networks are token-ring, Ethernet, and FFDI[3].

- Multiaccess nonbroadcast networks

  Multiaccess nonbroadcast networks also allow the attachment of multiple stations. To send data to a destination node attached to the same network, the physical address of the node must be learned, and direct communication can take place. In general, unless special provisions are taken, broadcasting is not possible. Examples of multiaccess nonbroadcast networks are frame relay, and X.25.

- Point-to-point (PtP) networks

  Point-to-point networks allow direct communication between two adjacent nodes. No broadcast is required on PtP connections From an IP routing perspective, PtP connection comprise a separate network, although only two stations connect. Instead of the term PtP network, the term PtP connection is more commonly used. Examples of point-to-point networks are PPP, SLIP[3], SNAlink, and ESCON connections

IP General Functions

Broadcasting

The 3746 IP Router is capable of using one the following types of broadcast:

- Limited or local-wire broadcast.

  Uses either all zeros (0.0.0.0), or all ones (255.255.255.255) as the broadcast address.

- Subnet-directed broadcast.

  Uses a broadcast address comprised of the subnetted network identifier and a host identifier of either all zeros or all ones. (For example, 9.132.56.0 or 9.132.56.255).

During customization either local-wire or subnet-directed broadcasting is selected, using either all ones or all zeros

[3] Not supported by the 3746.

The 3746 IP Router will accept the following types of broadcasts:

- Limited or local-wire broadcast.

  Destination IP address 255.255.255.255, and source IP address 0.0.0.0 are accepted.

- Subnet-directed broadcast.

  Destination IP address containing the subnetted network identifier and a host identifier of either all zeros or all ones, will be accepted, if the source IP address belongs to the network interface on which it has been received.

- Network-directed broadcast.

  Destination IP address containing the (non-subnetted) network number and a host number of either all zeros or all ones, will be accepted, if the source IP address belongs to the network interface on which it has been received (for example, 9.255.255.255 or 9.0.0.0).

The 3746 IP Router never forwards limited broadcast. Directed broadcasts will be forwarded, if not received from the network to which it is directed, and only if the packet was not received as a link-level (for example token-ring LAN) broadcast. Directed broadcasts are forwarded as a link-level broadcast. The 3746 contains an option to disable the forwarding of directed broadcasts.

Supernetting (Route Aggregation)

There is a major problem with the use of a range of Class C address instead of a single Class B addresses: each network must be routed separately. Standard IP routing understands only the class A, B and C network classes. Within each of these types of network, subnetting can be used to provide better granularity of the address space within each network, but there is no way to specify that multiple class C networks are actually related. The result of this is termed *the routing table explosion problem:* a Class B network of 3000 hosts requires one routing table entry at each backbone router, but if the same network is addressed as a range of Class C networks, it requires 16 entries.

The solution to this problem is a scheme called *Classless Inter-Domain Routing (CIDR).* CIDR is a proposed standard protocol with a status of elective. CIDR does not route according to the class of the network number (hence the term classless) but solely according to the high order bits of the IP address, which are termed the *IP prefix.* Each CIDR routing entry contains a 32 bit IP address and a 32-bit network mask, which together give the length and value of the IP prefix. This can be represented as <IP_address network_mask>. For example <194.0.0.0 254.0.0.0> represents the 7 bit IP prefix B '1100001'. CIDR handles the routing for a group of networks with a common prefix with a single routing entry. This is the reason why multiple Class C network numbers assigned to a single organization have a common prefix. This process of combining multiple networks into a single entry is termed *address aggregation* or *address summarization*. It is also called *supernetting* because routing is based upon network masks that are shorter than the natural network mask of the IP address, in contrast to subnetting where the network masks are longer than the natural mask.

Unlike subnet masks, which are normally contiguous but may have a non-contiguous local part, supernet masks are always contiguous. The 3746 IP Router uses CIDR in its BGP-4 implementation.

Multiple IP Addresses for a Network Interface

The 3746 IP Router supports class A, B, C, and D addresses. Class A, B, and C addresses are unicast addresses. Class D addresses are for multicast services, for example by the OSPF routing protocol.

One or up to 16 IP addresses can be assigned to a network interface for token-ring and frame relay. A subnet mask must be assigned together with each IP address. The IP addresses must be unicast addresses. Two reasons to use multiple addresses per interface are:

1. Consolidation of two routers into one with no change to the host definitions.

   Figure 45 shows a situation that requires three routers to handle communication between three IP networks.

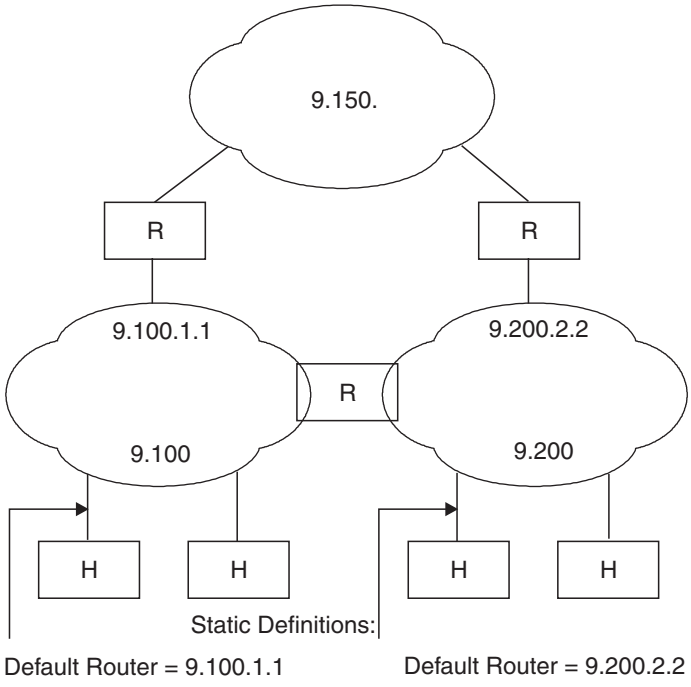


Figure 45. Three Networks and Three Routers Before Consolidation of the Routers

Figure 46 shows the situation after consolidation into one 3746 IP Router. Users see the network addresses as before and require no definition changes.

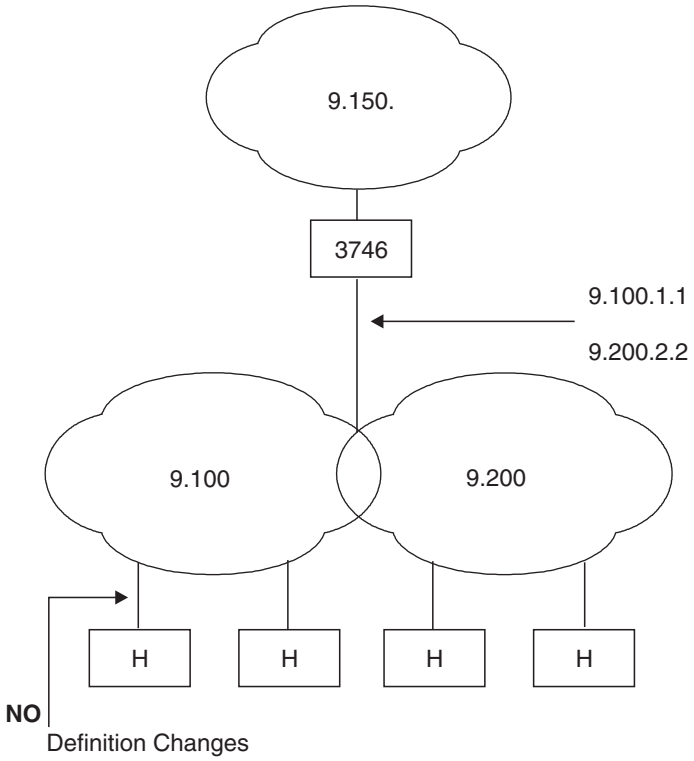


Figure 46. Three Networks and One 3746 IP Router After Consolidation

2. Route aggregation of multiple Class C addresses.

   Suppose an enterprise requests 1000 new IP host addresses for its internal network. They are given ***four*** contiguous ranges of class C addresses, but the four networks are connected to a single port on the 3746 IP Router. Figure 47 shows that the single port can be assigned four IP addresses, one for each IP network. To each network, the 3746 IP Router appears as a single IP address.

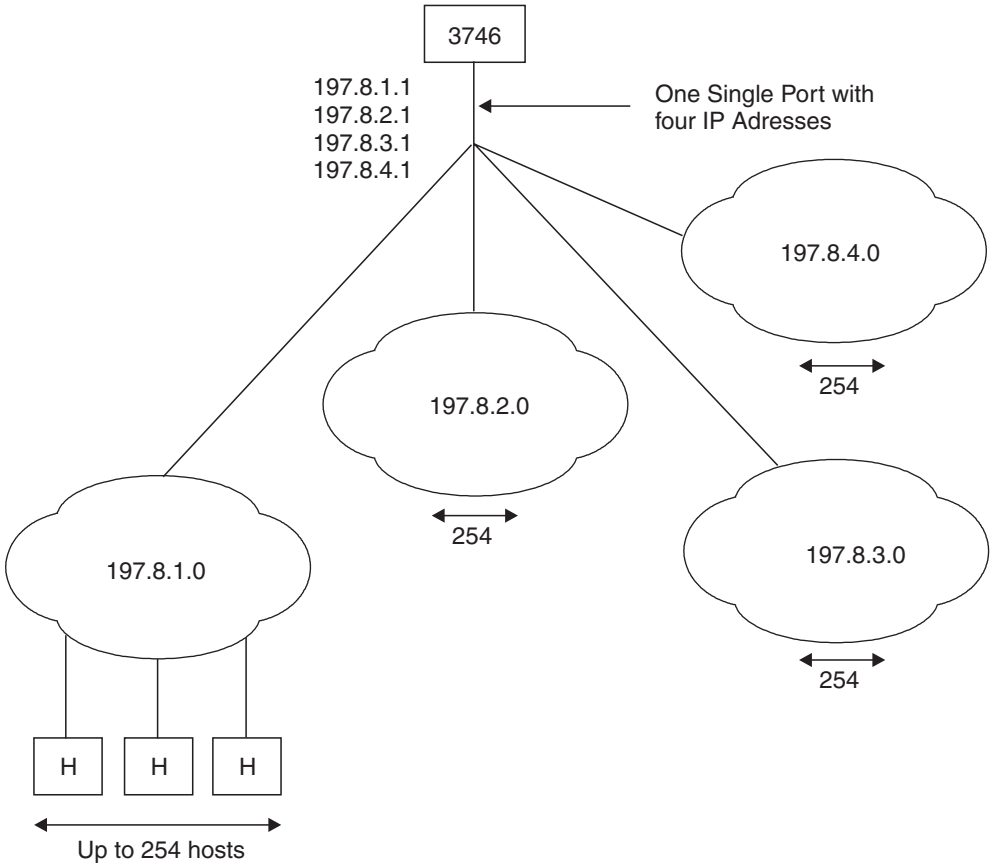


Figure 47. A Single 3746 IP Router Serving Four IP Networks via a Single Port

It is not necessary to assign an IP address to the 3746 PPP interface, but frame-relay and X.25 interfaces do need at least one IP address. However, unnumbered interfaces (that is, without IP address) cannot be addressed (for example, Ping and Traceroute cannot be directed to the interface) and require OSPF as a interior routing protocol.

In addition to the interface addresses a *router_ID* must be assigned. Rather than specifying a specific interface, this IP address specifies the router as a whole. The router_ID is used for Ping, Traceroute, and OSPF messages originating from the 3746 IP Router. To avoid routing problems, it is recommended to set the router_ID to one of the 3746 interface IP addresses.

User Datagram Protocol (UDP)

The 3746 IP Router uses UDP for RIP and/or SNMP data transport. If a UDP packet with an unknown (unregistered) destination port is received, this event is logged. For destination ports other than 9 (RFC863, *Discard protocol*) an ICMP destination unreachable message (port unreachable) is returned, unless the packet was a link-level broadcast or the source IP address was a broadcast or multicast IP address.

Transmission Control Protocol (TCP)

The 3746 IP Router uses TCP for its Telnet, SNMP, and BGP functions. Note that OSPF uses IP directly, it does not pass through TCP (nor UDP).

Internet Control Message Protocol (ICMP)

The 3746 IP Router recognizes the following ICMP types:

0 Echo Reply

When an Echo request is received, an Echo reply is returned containing the data from the Echo request.

3 Destination Unreachable

The 3746 may generate the following ICMP destination unreachable messages:

- Network unreachable

  When there is no active route to the destination address, the destination network is zero, or the destination address is not a valid class A, B, C, or D address.

- Fragmentation needed [the Do Not Fragment (DF) bit is set]

  An outgoing packet needs fragmentation but the DF bit in its IP header is set, or fragmentation results in an invalid fragment offset.

- Protocol unreachable

  An IP datagram destined for the 3746 IP Router contains an unsupported protocol number.

- Port unreachable

  An UDP datagram destined for the 3746 IP Router contains an unsupported UDP port number.

- Source route failed

  The next hop IP address in a datagram strict source routing is not on a directly connected network.

4 Source quench

Source quench messages are logged but no action is taken. The 3746 never generates a source quench message.

5 Redirect

Redirect messages are logged but no action is taken. The 3746 generates a redirect message (redirect datagram for the host) when a packet is forwarded on the same interface as received, the network is not point-to-point, and the subnet or network number of the source IP address matches that of the next hop IP address.

8 Echo Request

Echo request messages are responded with the echo reply message. ICMP Echo request are generated by the Ping application (see “Ping” on page 103) at the user's request.

11 Time exceeded

Time exceeded messages are logged. The 3746 generates a time exceeded message (time to live exceeded in transit) if the time to live (TTL) field in a datagram that the 3746 IP Router is forwarding is 0 or 1.

12 Parameter problem

Parameter problem messages are logged. The 3746 generates a parameter problem message (pointer indicates the error), if:

- Options field in IP header indicates that the options extend beyond the end of the IP header.
- Pointer is less than 4 in loose source route, strict source route, or record route option. Pointer is less than 5 in a timestamp option.
- Pointer is less than the length in a record route or timestamp option, but insufficient room for the IP router to insert its IP address and/or timestamp.
- In a record route option, the option is full (no data can be added).

13 Timestamp

Timestamp messages are logged. The 3746 never generates or responds to timestamp messages.

14 Timestamp reply

Timestamp reply messages are logged. The 3746 never generates or responds to timestamp reply messages.

15 Information request

Information request messages are logged. The 3746 never generates or responds to information request messages.

16 Information reply

Information reply messages are logged. The 3746 never generates information reply messages.

17 Address mask request

Address mask request messages are dropped if:

- The destination IP address matches the 3746's internal IP address.
- The source IP address is 0.0.0.0 and the receiving interface has more than one IP address assigned to it.
- The source IP address is 0.0.0.0 and the receiving network is not broadcast or point-to-point. The 3746 never generates address mask request messages.

18 Address mask reply

Address mask reply messages are returned in response to valid address mask request messages. An address mask reply message is returned with the destination IP address set to 255.255.255.255 if the (request) source IP address is 0.0.0.0; otherwise, the (reply) destination IP address is set to the (request) source IP address.

When the 3746 IP Router receives an ICMP message with a Type value it does not recognize, it logs the event. If the Type is greater than 18, it increments the count

of erroneous received ICMP messages. The 3746 keeps transmit and receive counts per-Type, for values less than 19.

The TTL value in the IP header of the ICMP messages generated by the 3746 IP Router is equal to the value it generally sets for all IP datagram, ***60***. The precedence and Type of Service (TOS) fields are set to zero. No options are included. No mechanism exists to limit the rate at which ICMP messages are sent.

Address Resolution Protocol (ARP)

The 3746 IP Router supports ARP requests and responses. An ARP request is sent when the requested address is not found in the ARP cache table. Requests are broadcast on the local physical network. An ARP request is also sent when attempting to refresh an existing entry. In this case, the ARP request is directed to the current entry's hardware address.

A received ARP request contains the requester's protocol and hardware address, and the destination IP address. ARP responds by providing the 3746 IP Router's IP address of the interface on which the ARP request is received. The requester's address translation is also gleaned from the received ARP request and an entry made in the ARP table cache.

An ARP response is sent when a valid ARP request is received. An unsolicited ARP response is broadcast when a new IP address pair (resulting from new local hardware) is registered, or a previously registered pair is changed. When an ARP response is received, the address translation information is cached in the ARP cache.

ARP Caching

To improve performance ARP entries are cached in the ARP table. Each 3746 CLP maintains independent ARP tables. The table contains dynamic and permanent entries. Dynamic entries are learned, while permanent entries are operator defined.

Each ARP entry contains a 6-byte token-ring LAN address and protocol-specific data referred to a *side-car.* Side-car information maintained for IP over token-ring is the routing information field (RIF). On the 3746 IP Router, the support for source-route bridging (SRB) is always active.

ARP table entries that have not been recently used or updated (refreshed) are discarded. Permanent entries are never discarded. The default time for an entry to be retained before being discarded is five minutes. User commands exist to delete all (dynamic), or specific ARP (dynamic and permanent) entries. Dynamic ARP table entries are also removed when a network interface is considered down.

The 3746 IP Router can be configured to attempt to refresh an unused entry before it ages out. This is referred to as the *auto-refresh* function. If configured, ARP will send out a request to the hardware address in the table to verify the address. The request is sent out approximately 30 seconds before an entry ages out. The default is to disable this function. The ARP table sizes are limited by available memory. ARP will continue to request memory for available entries until 3746 processor memory is depleted, at which time the IP routing function is restarted. Care should be taken in setting the aging timers, as this could impact the ARP table size. Special care should also be taken in disabling this timer.

Proxy-ARP

The 3746 IP Router supports proxy-ARP. By user configuration, either RFC 925 or RFC 1027 can be selected. RFC 925 proxy-ARP is referred to as *ARP net routing*. RFC 1027 proxy-ARP is referred to as *ARP subnet routing*. The proxy-ARP support is optional; it can be enabled or disabled for the whole 3746 IP, but it cannot be enabled or disabled on an interface basis. It is disabled by default. Proxy-ARP is an appendage to ARP. When enabled and an ARP request is received in which the destination address does not match any of the router's IP addresses, proxy-ARP is called. Proxy-ARP looks up the destination protocol address in the routing table, and, in general, if it finds an active route to the destination, it tells ARP to send an ARP reply. No ARP reply is returned, if:

- There is no route to the destination IP address in the ARP request.
- The source IP address in the ARP request is not in a network directly attached to the 3746 IP Router.
- Source and destination IP address do not have the same network identifier.

  Note: An option exists to disable this option.
- The physical transmit interface of the route to the destination IP address is the same interface from which the ARP request is received.
- The route found for the destination protocol address is a filter.

Routing Protocols

The IBM 3746-9x0 supports the following IP routing protocols:

- Routing Information Protocol, Versions 1 and 2 (RIP)
- Open Shortest Path First Protocol, Version 2 (OSPF)
- Border Gateway Protocol Version 4 (BGP)

Each is explained in more detail below.

Routing Information Protocol (RIP) Version 1

RIP Version 1 is implemented in both the 3746 and the MAE. It includes support for ***split horizon***.

To speed network convergence, triggered updates are sent.

Note: ***Poison reverse*** is not available.

Route Acceptance Policy: Per interface the user can configure, whether or not:

- RIP will listen.
- Network, subnet, and/or host routes are learned.
- Default and/or static routes can be overridden with a learned route.

Note: Default routes are indicated by a destination and mask of 0.0.0.0.

Route Advertisement Policy: Per interface the user can configure, whether or not:

- RIP will be advertised.
- Network, subnet, and/or host routes are advertised.
- Default and/or static route are advertised.

Subnets will be advertised if they are part of the same natural network (that is, class A, B, or C) as the interface's IP address, and the route subnet mask must be

the same as the interface's subnet mask. Host routes (mask 255.255.255.255) are exempt from these rules.

Routing Information Protocol (RIP) Version 2

RIP Version 2 is implemented in both the 3746 and the MAE. This support of RIP2 enables, for example, the ESCON adapter to reduce loads on the host by using an IP multicast address to broadcast periodic RIP2 messages.

RIP2 has the following features:

Support for variable subnet masks: This is the major enhancement brought by RIP V2. RIP V2 supports subnet masks of variable sizes within the same router, while in RIP V1 all the subnet masks had to be the same for a given router.

Password authentication: Defines an authentication key that is added to each RIP V2 advertisement packet originating from the interface that is being defined as supporting RIP V2.

Multicasting (instead of broadcasting): RIP V1 broadcasts advertisement packets over all local interfaces.

RIP V2 sends RIP2 advertisement packets, from the interfaces where RIP V2 is defined, to the multicast group having the class D address 224.0.0.9.

RIP Metrics

Where you have multiple interface, the RIP metrics allow you set the weight of one interface higher than another. For example, for traffic that can flow out over either of two interfaces, it will always go out over the interface with the lower weight (lower metric value).

In-Metric: This metric is added to the RIP routes learned on an interface prior to adding the routes to the routing table.

When an interface receives RIP messages, the metric is used when storing routes in the routing table. Later, when looking up a route in the table, the stored metric is taken into account in the route.

The in-metric range is 1 to 15.

Out-metric: This metric is added to RIP routes advertised on an interface. The metric is set on RIP messages that are sent to other routers on the interface.

The out-metric range is 0 to 15.

Open Shortest Path First Protocol (OSPF)

The 3746 IP Router supports the following features of OSPF, Version 2, which have implementation-specific behavior:

- Area border (AB) router support
- Support for stub areas
- Autonomous system border (ASB) support
- OSPF interface support
- Equal-cost multipath routing
- Simple authentication
- OSPF routing policies

- Multicast OSPF (MOSPF) support

There is no support for Type of Service (TOS) based routing; that is, TOS 0 is the only supported TOS.

Area Border (AB) Router Support: 3746 IP supports attachment to multiple areas and summarization of routing information between areas. Area border routers must attach to the backbone (0.0.0.0) and at least one other area. Summarization information from one area will manifest itself as type 3 and 4 link state advertisements (LSAs) in other areas.

Support For Stub Areas: 3746 IP supports attachment to stub areas. OSPF autonomous system external (ASE) LSAs will not be advertised into stub areas. Rather a type 3 network summary LSA for the default route (destination/mask 0.0.0.0) is generated.

Autonomous System Border (ASB) Support: 3746 IP can be configured as an autonomous system border (ASB) router. Non-OSPF routes can be imported into OSPF as OSPF autonomous system externals (ASEs). This implies that the 3746 IP will generate type 5 LSAs.

OSPF Interface Support: 3746 IP supports the following types of OSPF interface:

- Numbered point-to-point (PtP)

  Numbered PtP connections are links to which an IP address has been assigned. Examples are ESCON and PPP connections.

- Unnumbered point-to-point (PtP)

  Unnumbered PtP connections are links to which no IP address has been assigned. OSPF packets will be sent using the 3746 IP Router-ID as source address.

- Broadcast

  A broadcast is, for example, a token-ring interface. Link-level multicast is used to broadcast OSPF frames to all attached OSPF routers.

- Nonbroadcast multiaccess (NBMA).

  Viewing a network, for example a frame-relay network, as an NBMA network can be used when the network is fully meshed (meaning virtual circuits exist between any pair of routers). In routers that are eligible to become designated routers, neighbors must be configured whether or not the neighbor is eligible to become designated router. The configurable poll interval defines the interval at which the designated router will attempt to contact the neighboring routers to establish an adjacency. NBMA connections are supported for frame-relay networks. If the network is partially meshed, it is more useful to view the network as a point-to-multipoint network.

- Point-to-multipoint (PtM)

  This interface type is used to allow BMBA topologies to be non-fully meshed. Rather than electing a designated router for the network and having that router generate network LSAs for the network, each router includes its neighbors in its router LSAs. When the route table is calculated, the network topology will appear as multiple point-to-point links rather than a single cloud. On one side of the frame-relay virtual circuit, the neighboring router must be configured to

allow the two routers to form an OSPF adjacency. Point-to-multipoint connections are supported for frame-relay networks.

- Virtual link

  Virtual links are supported to extend the backbone area's connectivity through a transit area. The two endpoints of the virtual link are area border routers.

Equal-Cost MultiPath Routing: 3746 IP supports up to four equal-cost next hops for a route. When multiple next hops exist, the traffic to the destination is spread over the next hops round-robin.

Simple Password Authentication: 3746 IP supports both simple password and no authentication. When simple password authentication is used, an 8-byte password is included in each OSPF packet. Upon reception, this password is validated with packets failing validation being dropped. The authentication type (simple or none) is configured on the area level, while the authentication key is configured for each interfaces in areas with simple password authentication enabled.

OSPF Routing Policies: The 3746 IP OSPF policy can be explained in terms of rules for:

- Advertisements of OSPF routes
- Import of external routes into OSPF as OSPF AS external (ASE) routes
- Generation of the default route and import as an OSPF ASE LSA
- OSPF route policy when multiple routes to a destination exist

OSPF Advertisement of Routes: OSPF allows filtering of LSAs on area boundaries only. All routers within an area have the same view of the area topology. To limit the number of LSAs advertised outside the area, one can configure the network ranges associated with an area at the area boundary. This, in effect, will aggregate a number of networks into a single advertisement. The cost associated with the network range will be the lowest for any of the component networks. Additionally, one can define a network range that will not be visible. Normally, OSPF ASE LSAs are flooded throughout the entire routing domain. One can prevent this for a given area, by defining the area as a stub area. Within the stub area, the area border router will advertise single default route (destination/mask 0.0.0.0).

Importing Routes into OSPF: The 3746 IP Router configuration determines whether or not non-OSPF routes can be imported as OSPF AS external routes, and advertised as OSPF ASE LSAs throughout the OSPF routing domain. Imported routes can be imported as ASE type 1 (router) or ASE type 2 (network) routes. ASE type 1 route always override type 2 routes. It has a single metric that is the sum of the path cost to the AS border router, and the AS border router metric. Conversely, the metric for a type 2 ASE has internal and external components, namely the path cost to the AS border router and the route's external metric. When comparing ASE type 2 routes to the same destination, the one with the lower external metric will be always be preferred, independent of the internal metric. The metric used for both the OSPF ASE type 1 route and the external component of the type 2 route is the metric from the protocol from which it is imported.

Default Route: 3746 IP allows generation of a default routes and advertisement of the routes through an AS external (ASE) LSA. For details see "Inter-operability of Routing Protocols" on page 101.

Border Gateway Protocol Version 4 (BGP)

The IBM 3746-9x0 supports a full implementation of BGP Version 4 with null authentication. Only BPG Version 4 support is provided; earlier BPG versions are not supported. Configuration options exist to:

- Enable BGP, and specify the local autonomous system number.
- Define BGP neighbors.
- Define (exclude) ASs from which no routing information will be accepted.
- Define send, receive, and originate policies.
- Define aggregate routes. The 3746 IP Router requires that aggregated routes are preconfigured. When defining aggregated routes, make sure that the individual routes that make up the aggregated route are not exported (that is, define a send policy).

Inter-operability of Routing Protocols

When combinations of routing protocols are used on the IBM 3746-9x0 it is necessary to specify how to pass routes learned by one protocol to another. Examples of situations where this is required include:

- Advertising static/default route
- Passing route information between RIP and OSPF gateway protocols
- Passing route information between the interior gateway protocols (RIP/OSPF) and BGP

The principle behind route export is simple but there are a number of implementation details that must be understood for the IBM 3746-9x0.

RIP Specifics: The following rules apply when there is both a RIP route and a route from another protocol to the same destination:

- The RIP route will override a BGP route.
- The RIP route will be overridden by an OSPF internal route.
- The RIP route will override a static route if the RIP route's metric is less.
- The RIP route will override a default route if the RIP route's metric is less.
- The RIP route will override an existing OSPF autonomous system external (ASE) type 1 route if the OSPF external comparison switch is set to type 1, and the RIP metric is lower than the OSPF metric.
- The RIP route will override an existing OSPF autonomous system external (ASE) type 2 route if the OSPF external comparison switch is set to type 1, or the OSPF external comparison switch is set to type 2 and the RIP metric is lower than the OSPF metric.

The 3746-9x0 RIP implementation does not allow the import of OSPF or BGP learned routes. The 3746 IP Router may advertise itself as the default router within the RIP routing domain depending on the values configured within the Originate Default Route field. You have the option:

- To always originate the default route.
- To originate the default route when a BGP route for a specific destination has been received. The default route will be generated if the route corresponds with a specific AS. AS 0 indicates that the AS number should not be checked.
- To originate the default route when OSPF routes are present in the routing table.

OSPF Specifics

The 3746-9x0 has a configuration option to enable route imports. The type of routes that are imported can be specified. Options exist to import static routes, direct routes, subnet routes, RIP routes, and BGP routes.

All routes are imported as OSPF AS external routes and advertised into the OSPF network using AS external link state advertisements.

When OSPF imports routes, it is necessary to specify additional parameters to define how the external route will be advertised into the OSPF network. These parameters are the metric type (1 or 2) and the external route tag.

Metric type 2
: defines the metric to the destination to be larger than any internal path.

Metric type 1
: means that the metric is comparable to internal paths.

It is recommended that type 2 be selected to ensure that external routes have a larger metric than internal ones. Type 1 should be selected only if the operational effect of using it is fully understood.

The external route tag provides additional information in the AS external link state advertisement, although it is currently only defined for use with BGP. The tag can normally therefore be set to any value.

The 3746 IP Router may advertise itself as the default router within the OSPF routing domain depending on the values configured within the Originate Default Route field. You have the option:

- To always originate the default route.
- To originate the default route when a BGP route for a specific destination has been received. The default route will be generated if the route corresponds with a specific AS. AS 0 indicates that the AS number should not be checked.

The forwarding address indicates to which router default packets are routed. It must be a router interface address that is adjacent, that is, part of the same (sub)net, to the 3746-9x0. 3746 IP routing policies when multiple routes to the same destination are available, are used in the following order:

- Interior gateway protocol (RIP, OSPF) routes are preferred over BGP routes.
- OSPF routes are always preferred over other type of routes (other than routes to directly attached networks).
  - OSPF intra-area routes are preferred to inter-area routes.
- RIP routes and static routes can override OSPF ASE routes. It can be configured if external routes will be compared to OSPF ASEs as type 1 or type 2 routes. Given the preceding definitions of the configurable OSPF ASE route, static and RIP routes may override OSPF ASE routes in the following situations:
  - The OSPF comparison is configured as type 1, and the OSPF ASE route is an OSPF ASE type 2 route.
  - The OSPF comparison is configured as type 1, and the OSPF ASE route is an OSPF ASE type 1 route but has a higher cost than the RIP or static route.

– The OSPF comparison is configured as type 2, and the OSPF ASE route is an OSPF ASE type 2 route but has a higher cost than the RIP or static route.

BGP Specifics: The routing information that is sent by BGP to its BGP neighbor depends on the routing information within the IP routing table (that is, locally defined static routes and routes learned from RIP and/or OSPF), and routes received from BGP neighbors. This process is controlled by defining originate and send policies, and by defining aggregated routes.

Static/Default Routes: The default referred to in this subsection is the default route that is generated by BGP if the generate default route option is enabled. Export default cannot be used to export an intra-AS default route without BGP being configured. If this is a requirement it must be met by the use of the static route (0.0.0.0) exported to the interior gateway protocol within the AS. Default should be exported to the interior gateway protocol being used within the AS. It will become advertised when and only when BGP communications are established with a neighbor that is configured to generate a default route.

Internal Applications

Two important applications implemented on the 3746 IP Router that rely on ICMP messages are:

- Ping
- traceroute

Both applications are used in diagnosing connectivity problems. Each application can be invoked by using either the CCM or a TELNET command line mode.

Ping

Ping is the simplest of all TCP/IP applications. It sends one or more messages to a specified destination host requesting a reply and measures the round trip time. The word *ping,* which is used as a noun and a verb, is taken from the sonar operation to locate an underwater object. It is also an abbreviation for *Packet InterNet Groper*.

Traditionally, if you could ping a host then other applications such as Telnet or FTP could reach that host. With the advent of security measures on the Internet which control access to networks by application protocol and/or port number, this is no longer strictly true. Nonetheless, the first test to reach a host is still to attempt to ping it.

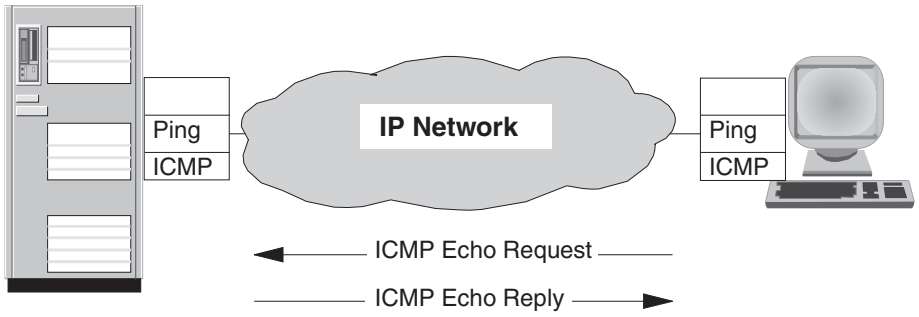


Figure 48. Packet InterNet Groper (PING)

The syntax that is used in different implementations of ping varies from platform to platform. The following syntax is for the 3746 IP implementation:

```
ping host
```

Where host is the target IP address. On the 3746 IP Router the target IP address specified must be in dotted decimal notation. Host names are not supported.

Ping uses the ICMP Echo and Echo Reply messages. Since ICMP is required in every TCP/IP implementation, hosts do not require a separate server to respond to pings. Ping is useful for verifying a TCP/IP installation. Consider the following forms of the command; each requires the operation of an additional part of the TCP/IP installation.

ping loopback	Verifies the operation of the base TCP/IP software.
ping my-IP-address	Verifies whether the physical network device can be addressed.
ping a-remote-IP-address	Verifies whether the network can be accessed.

Be aware that IP is a connectionless protocol and that a Ping request and its reply may traverse different routes through the network. Being able to ping a node does not necessarily mean that the reply can be returned as well. Ping requests contain a destination address that is set to the target host indicated in the Ping command. The 3746 IP Routers sets the source IP address to its router_ID. Therefore, to enable the target host to return the Ping reply, an active route between this host and the 3746 Router ID is required.

Note: For Pings to be successful, make sure that the Ping ICMP messages are not filtered along the route between the 3746 IP Router and the destination host.

In normal operation Ping builds and sends an ICMP echo request. Ping waits up to 1 second to receive an ICMP echo reply to calculate the round-trip time, and display the size of the echo request/reply packet (not including IP header), its source IP address, and the round-trip in milliseconds. 3746 IP echo request/reply messages are always 64 bytes long (excluding IP header).

Ping keeps count of the echo requests it sends and the echo replies it receives. It keeps a sum of the round-trip times, and calculates maximum and minimum round-trip times. In addition, it keeps count of the ICMP destination unreachable (network or host unreachable). 3746 IP Ping stops when the user presses any key. Ping statistics are then displayed which include:

- The number of Echo request sent.
- The number of Echo replies received.
- The percentage of packets lost (no replies received).
- The number of destination unreachable messages received.
- The number of Echo request not sent due to lack of buffers.

Traceroute

The Ping command described in the previous section can be used to verify connectivity between two hosts. In addition, for example when the Ping command fails, the Traceroute command can be used to determine the route that IP datagrams follow from host to host.

Traceroute relies on ICMP time exceeded and destination unreachable messages. It sends a UDP datagram with a TTL of 1 to the destination host. The first router to see the datagram will decrement the TTL to 0 and return an ICMP Time Exceeded

message as well as discarding the datagram. In this way, the first router in the path is identified. This process can be repeated with successively larger TTL values in order to identify the series of routers in the path to the destination host. Traceroute sends UDP datagrams to the destination host that reference a port number outside the normally used range. This enables Traceroute to determine when the destination host has been reached, that is, when an ICMP destination (Port) unreachable message is received.

For each TTL value, the UDP datagram is sent three times, waiting up to three seconds between transmissions to receive a response. Traceroute continues this process until either a TTL value of 33 has been reached or an ICMP destination unreachable message received.

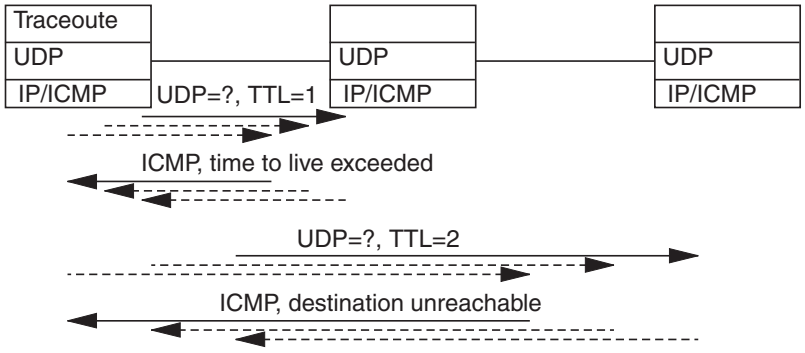


Figure 49. Traceroute

When a route exist between the 3746 IP Router and a destination node, each intermediate router will return an ICMP time exceeded message. However, a situation might exist where somewhere along the route the Traceroute frame cannot be forwarded.

Note: For Traceroute to be successful, make sure that the Traceroute ICMP messages are not filtered along the route between the 3746 IP Router and the destination host. For each TTL value, Traceroute displays a line with the following information:

- 'BF' each time the 3746 IP is unable to send the UDP frame due to lack of buffers.
- '*' each time no response is received.
- The source IP address of the response, if different from the previous response received.
- The round-trip time in milliseconds.
- '!P' if the response is a destination unreachable (protocol unreachable).
- '!H' if the response is a destination unreachable (host unreachable).

Bootstrap Protocol (BOOTP)

One restriction with the scheme described in the previous section is related to the use of the limited broadcast address for BOOTP requests; it requires that the server is on the same subnet as the recipient.

The 3746 IP Router, however, has a mechanism to forward BOOTP requests to one or multiple preconfigured BOOTP servers. If the BOOTP request's router

address is zero, the 3746 BOOTP relay agent sets it to the IP address of its receiving interface.

The 3746 IP BOOTP relay agent discards the BOOTP request message when:

- BOOTP request's "hops" value is greater than the value configured by the user.
- BOOTP request's "hops" value is greater than or equal to 16.
- BOOTP request's "seconds (retry)" value is greater than the value configured by the user.

  This allows BOOTP servers on the local network a chance to respond before the BOOTP relay agent has forwarded to remote BOOTP servers.

The BOOTP relay agent forwards a BOOTP reply message to the interface whose IP address matches the BOOTP reply's router IP address. Because the BOOTP client may not know its IP address and therefore may not be able to respond to an ARP request, the 3746 IP BOOTP relay agent installs an entry in the outgoing interface ARP cache table using the client IP and hardware address specified in the BOOTP reply message.

Once a BOOTP server has responded and the BOOTP client has processed the reply, it may proceed with the transfer of the boot file and execute the full boot process. The transfer of the boot file is usually done, using the trivial file transfer protocol (TFTP). The full boot process will replace the minimum IP protocol stack used by BOOTP and TFTP by a normal IP protocol stack transferred as part of the boot file and containing the correct customization for the client.

Security

The 3746 IP Router offer two methods to control its IP forwarding functions, namely by defining:

- Filters
- Access controls.

Both are described in more detail below.

3746 IP Filters

The 3746 IP filters are essentially user-defined static routes. Any packet received or originated by the 3746 IP Router in which the destination IP address matches a filter is discarded. No error message will be generated. Each filter, like a static route, consists of an IP address and a mask. When an IP datagram is forwarded, the destination address is ANDed with the filter mask. If the result equals the filter address, then the datagram is discarded.

```
destination_address & filter_mask = filter_address = discard!
```

The 3746 IP Router installs filters in its routing table; therefore the numbers of filters is limited by the size of the routing table. Routes that match a filter are not advertised when using a dynamic routing protocol.

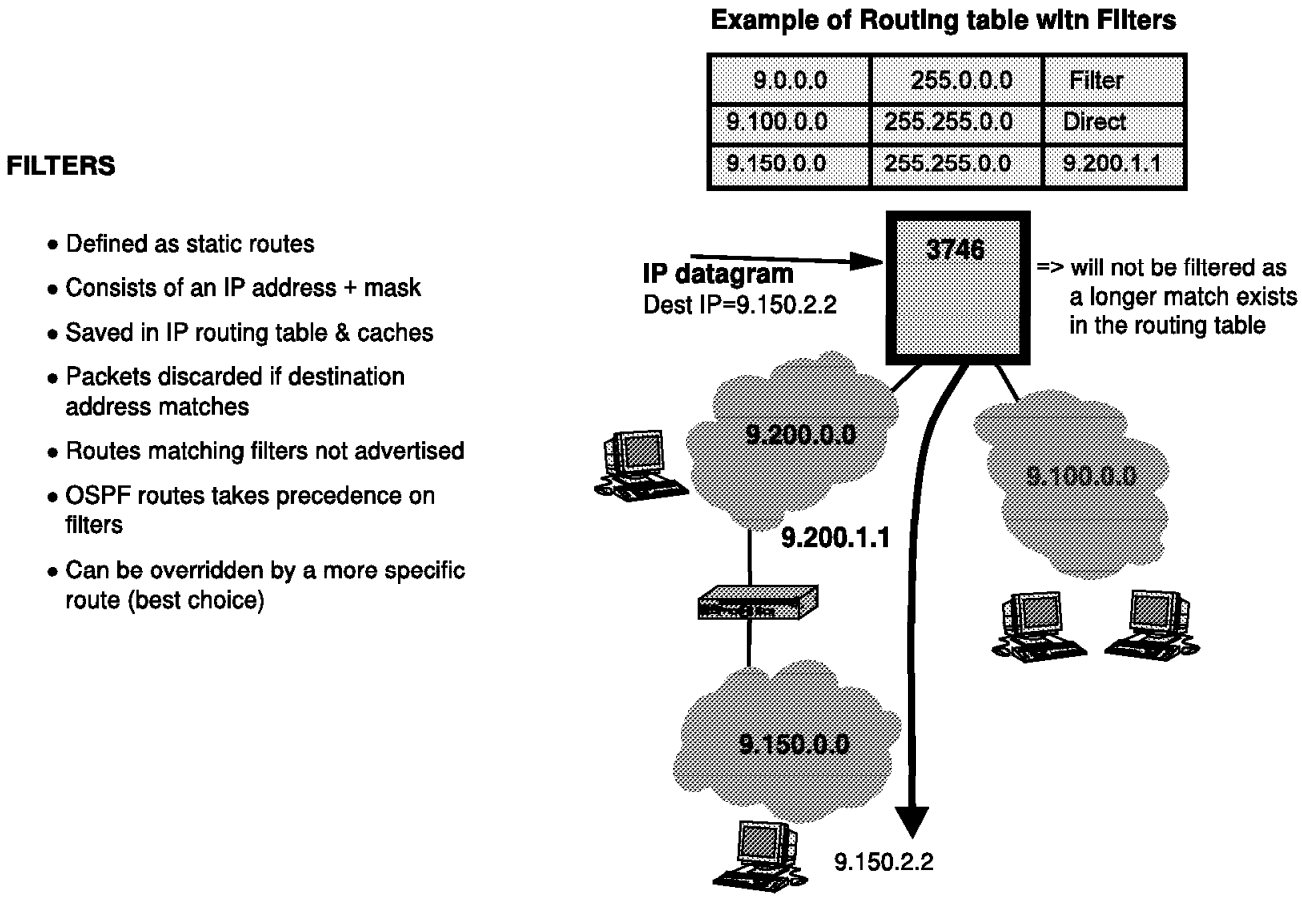


Figure 50. IP Filters

3746 Access Control

Access control provides a way for the user to control which IP packets are forwarded by the 3746 IP Router based on the packet's source IP address, destination IP address, IP protocol number, and TCP or UDP port number. It is applied to all IP packets that are received or originated by the 3746 IP Router. Access control is an optional function that by default is disabled.

Note: The 3746 implements access control for the whole of the 3746, ***not at the port (interface) level***. You cannot select individual ports for access control.

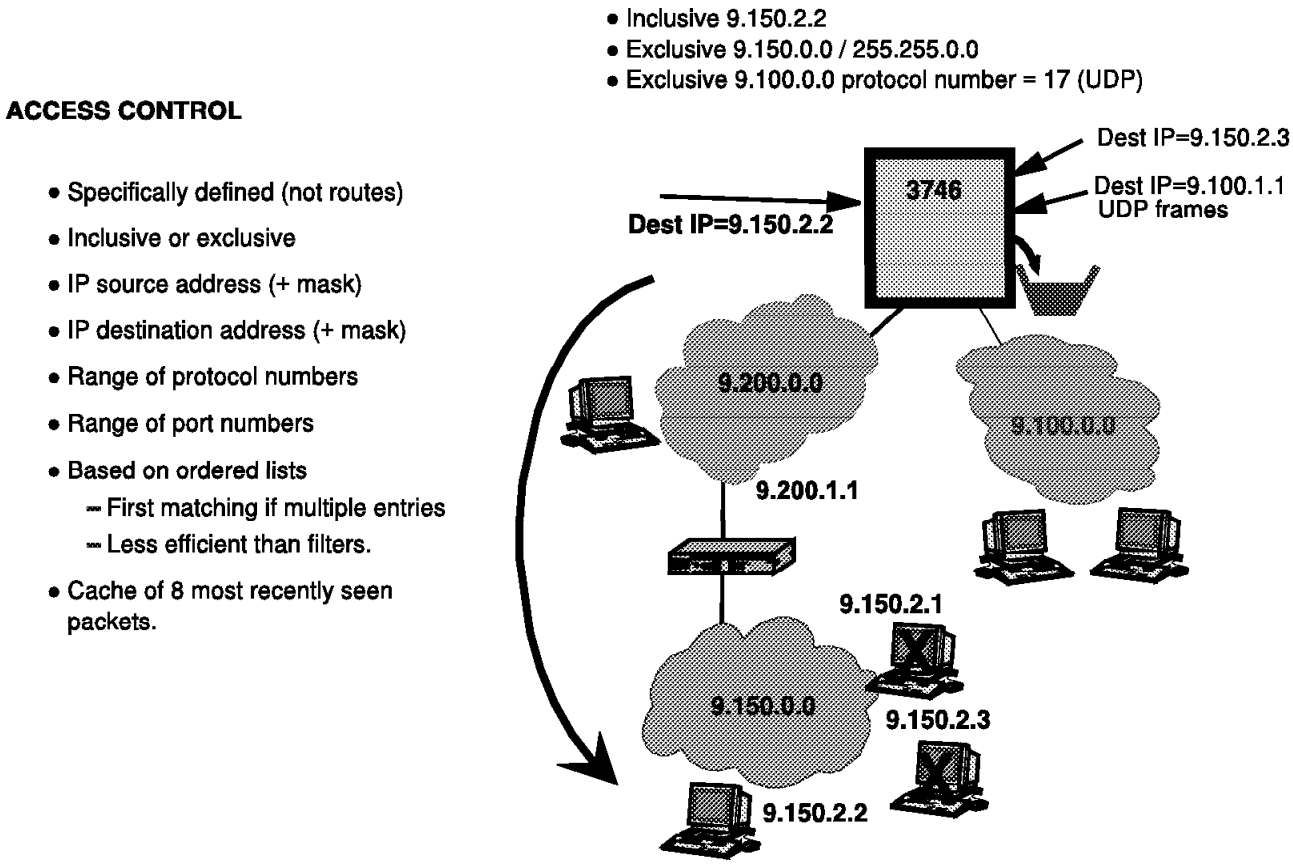


Figure 51. IP Access Control

Multiple access entries can be specified, each having the parameters shown in Table 19.

Table 19 (Page 1 of 2). IP Multiple Access Parameters

Parameter	Description
Access control type	The access control type can be inclusive or exclusive indicating that if this entry is matched the datagram will be forwarded, or discarded, respectively.
Source IP address	Value compared to the datagrams source IP address.
Source IP address mask	Value ANDed with the datagrams source IP address before comparing it with the access control entry's source IP address value.
Destination IP address	Value compared to the datagrams destination IP address.

Table 19 (Page 2 of 2). IP Multiple Access Parameters	
Parameter	**Description**
Destination IP address mask	Value ANDed with the datagrams destination IP address before comparing it with the access control entry's source IP address value.
First protocol number	The lower bound of a range of IP protocol numbers; a datagram matches the access control entry only if its IP protocol number is greater than or equal to this value.
Last protocol number	The upper bound of a range of IP protocol numbers; a datagram matches the access control entry only if its IP protocol number is less than or equal to this value.
First port number	The lower bound of a range of TCP/UDP port number; a packet in which the IP protocol number indicates TCP or UDP matches the access control entry only if its TCP or UDP port number is greater or equal to this value.
Last port number	The upper bound of a range of TCP/UDP port numbers; a packet in which the IP protocol number indicates TCP or UDP matches the access control entry only if its TCP or UDP port number is less or equal.

The access control entries are organized into a single list which is used for all interfaces. The access list is ordered, meaning that if a packet matches multiple entries in the list, the first matching entry in the list is the one that takes effect. If no matching access control entry is found, the 3746 discards the datagram.

Note: CCM always adds an all-inclusive entry at the end of the list, meaning that datagrams are forwarded unless discarded because of other entries in the list. Use the TELNET operator interface to insure that this entry is on that list.

Attention

PTR Z237641 needs to be examined to ensure correct IP addressing on the Service LAN. The ***exclusive*** and ***inclusive*** statements should be coded with care according to the particular installation.

Filters Versus Access Controls

Filters

A filter on a destination IP address is added to the IP routing table with indication ***filter***. The position of a route in the routing table depends on its IP address. Filters are saved into the main routing table maintained on the CBSP2 and the routing table cache on each of the 3746 processors.

A filter is a route like a static route. The primary difference is that filters are not advertised by RIP, or BGP, and if a filter is replaced by another type of route (for example, OSPF) that later goes away, the filter is not automatically restored. OSPF internal routes (intra-area and inter-area) take preference over filter routes. This is to prevent unexpected reachability problems in OSPF networks. Because it is a link state protocol, OSPF does not take filters into account in its advertisements, so filters in an OSPF network can cause reachability problems. To be sure to filter the traffic, access control must be used instead.

Filters have another shortcoming; they can be partially overridden by a more specific route. Assume a filter for 9.0.0.0 with mask 255.0.0.0, and a route for 9.100.0.0 with mask 255.255.0.0 has been installed. Because the routing table search looks for the most specific match, datagrams to 9.100.x.x will follow the route instead of the filter.

Access Control: Access control entries are searched sequentially for each datagram until a matching entry is found. This may lead to considerable overhead when many access control entries have been specified. There is no special search of a routing table for a filter. The routing table is searched once for the best matching route, and if that match turns out to be a filter, the datagram is dropped.

Recommendation: In general, the use of filters is advised rather than using access control. However, you should be aware of the shortcomings of filters mentioned above.

IP over 3746 Networks

Figure 52 depicts how TCP/IP functions have been implemented on the 3746-9x0 components identified.

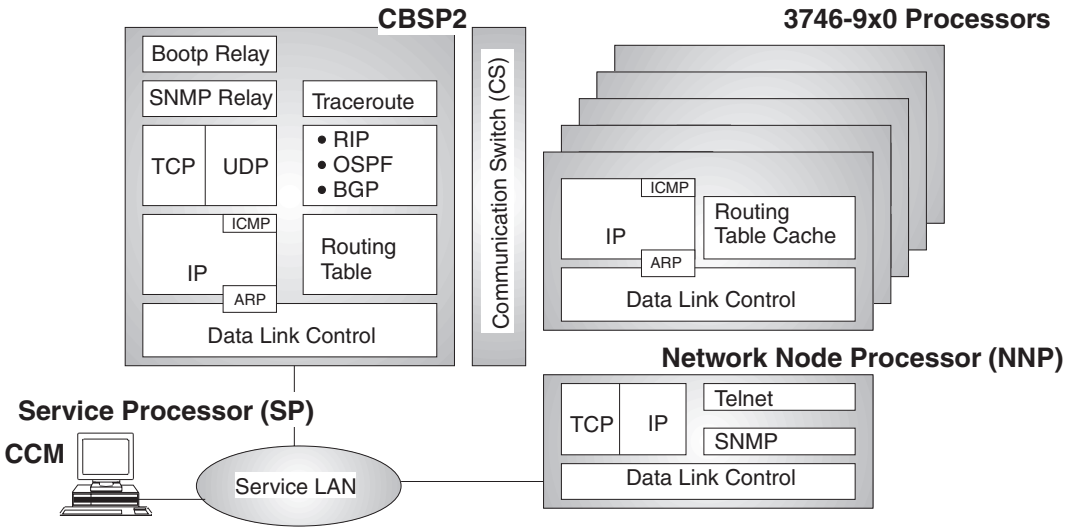


Figure 52. 3746-9X0 IP Base

Each 3746-9x0 processor, including the CBSP2, provides IP routing and data link control (DLC) functions. The DLC functions enable data transport to adjacent nodes. The DLC functions are shared between protocol stacks (IP and APPN/HPR). The IP functions allow IP transport between each of the 3746-9x0 adapters, and to and from externally attached IP equipment. To perform the IP routing, each adapter maintains a routing table cache. The code that performs the IP routing functions is present on all processors. However, it will only be activated on processors on which an IP interface has been configured. The routing cache is built during the transport of IP data, using routing information learned from the CBSP2.

In addition to the IP forwarding and DLC functions, more functions are required. All dynamic IP routing protocols (RIP, OSPF, and BGP) run on the CBSP. The CSBP2 is responsible for processing routing (RIP/OSPF/BGP) packets received

from, and generating routing packets destined for, external equipment. The adapters are instrumental in forwarding these packets between the external equipment and the CBSP2, and conversely.

The CSBP2 builds and maintains a routing table using static routes and IP interfaces defined on the 3746-9x0, and routing information learned from the dynamic routing protocols. To minimize the routing information maintained on each of the adapters, each processor maintains a routing table cache that contains a subset of the information stored in the CSBP2 routing table. When, during IP forwarding, a processor is not capable of making a routing decision based on the information maintained in its routing table cache, the appropriate routing information is retrieved by querying the CBSP2. Routes learned from the CSBP2 are stored within the routing table cache, and used to route successive IP datagrams. The Routing Table Caches contain one entry per *destination host* and ***not*** per *destination network*. This is to prevent less specific routes from masking more specific routes.

For example, if the most specific route that matches a particular destination IP address is the default route, if the default route is saved in the cache, then everything matches it. Thus everything is forwarded on the *default route* and more specific routes are ignored. Caching everything as host routes avoids the complications of dealing with more specific routes.

All cached entries are subject to an aging mechanism, and will be periodically removed.

Attached to the service LAN is the network processor (NNP). The main functions of the NNP are the 3746 IP operator and SNMP functions. In addition, the NNP contains the 3746 IP configuration file. When the 3746 IP code is restarted, each adapter retrieves a copy of the 3746 IP configuration file and configures itself. For details of SNMP functions, refer to “3746 Management Overview” chapter in the *3745/3746 Planning Series: Management Planning*.

Also attached to the service LAN is the service processor (SP). The SP provides a repository of the microcode running on the 3746-9x0 adapters. Each 3746-9x0 adapters loads its microcode from the SP during an initial microcode load (IML). The 3746-9x0 controller configuration and management (CCM) tool can be accessed from the SP.

IP Interfaces

The 3746 IP Router supports attachment of IP equipment using ESCON, token-ring, Ethernet, or serial lines. For serial line-attached equipment frame-relay, X.25, and Point-to-Point Protocol (PPP) connections can be used (see Figure 53 on page 112). Both switched, for example, using a public switched telephone network (PSTN), and leased-line PPP and frame-relay connections are supported.

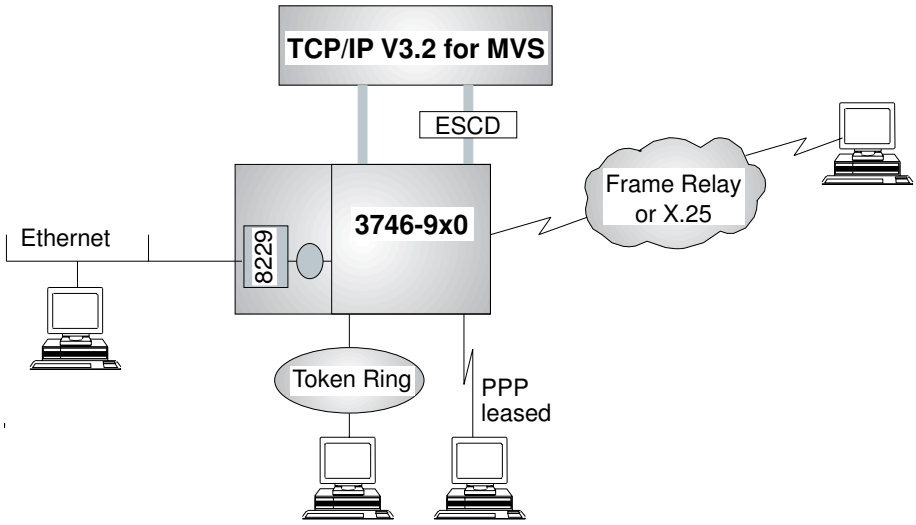


Figure 53. IP Interfaces

Each of these interfaces will be discussed in more detail in the following section.

ESCON

ESCON attachments can be used to provide native IP transport, using the channel data link control (CDLC), between the 3746 IP and host systems running TCP/IP for MVS™ (at least Version 3, Release 1). See Figure 54. The host systems can be directly attached to the 3746-9x0, or connected via an ESCON Director (ESCD).

The ESCON implementation on the 3746-9x0 is based on the concept of host links and link stations. A host link is a logical connection between a host system and the 3746-9x0. A link station represents a point-to-point link between the 3746-9x0 and host programs such as TCP/IP for MVS, VTAM, and/or TPF. Host link and link station definitions need to be entered before IP (or, for that matter, APPN/HPR or SNA subarea) communication is possible.

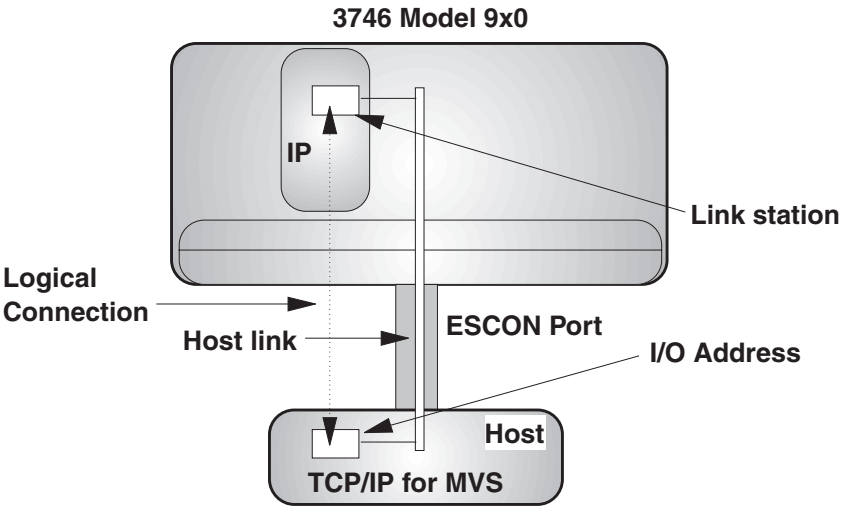


Figure 54. ESCON Port, Host Link, and Link Station

On each 3746-9x0 you can install up to 16 ESCON adapters (15 on a 3746-900 attached to a dual CCU Model 3745). Each ESCON adapter controls a single

ESCON coupler. An ESCON coupler provides a single physical connection to a single host system, unless you are using an ESCON Director (ESCD). An ESCD provides a physical connection to multiple host systems (See Figure 55 on page 113).

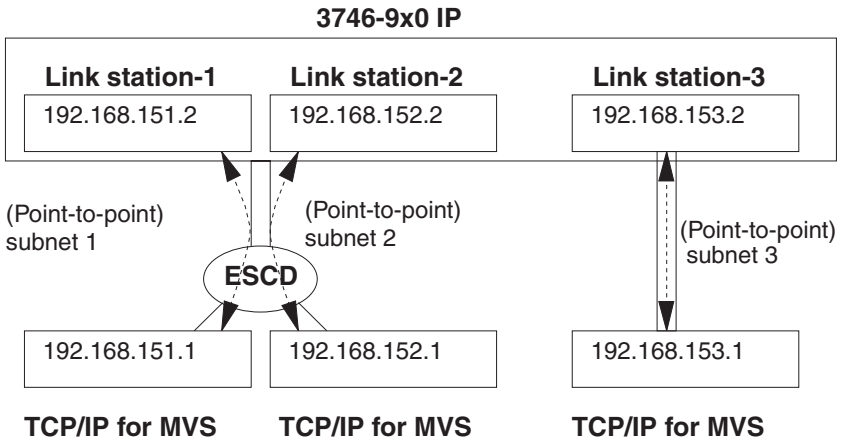


Figure 55. Multiple 3746 IP ESCON Links

Single IP addressing is possible on multiple ESCON stations to provide easier coding for multiple host access over the ESCON adapter.

On each ESCON adapter you can define up to 32 host links. For each host system you can define only one host link, unless the host system uses the ESCON Multiple Image Facility (EMIF), in which case you can define a separate host link (up to 32) to each of the logical partitions (LPs). On each host link you can define one or multiple link stations; however, the maximum number of link stations that can be defined per ESCON adapter is sixteen.

Note: Using the above figures, a single 3746-9x0 can provide ESCON attachment for up to 512 (16x32) host systems, and communicate with up to 512 host programs.

The ESCON configuration process consists of two phases:

1. A general definition part in which host links and link stations are defined, and the link stations are assigned to the appropriate protocol stack (3746 IP for IP routing).
2. The actual IP port configuration.

ESCON: General Configuration

To define an ESCON link, an ESCON port, a host link, and a link station definition are required. A host link, comprising a connection between a S/390® operating system and the 3746-9x0, is the logical equivalent of a port. On a single port, multiple host links can be defined, with multiple link stations on each host link. Figure 56 on page 114 depicts in configurations 1 and 2 an ESCON port on which a single host link and a single link station has been defined.

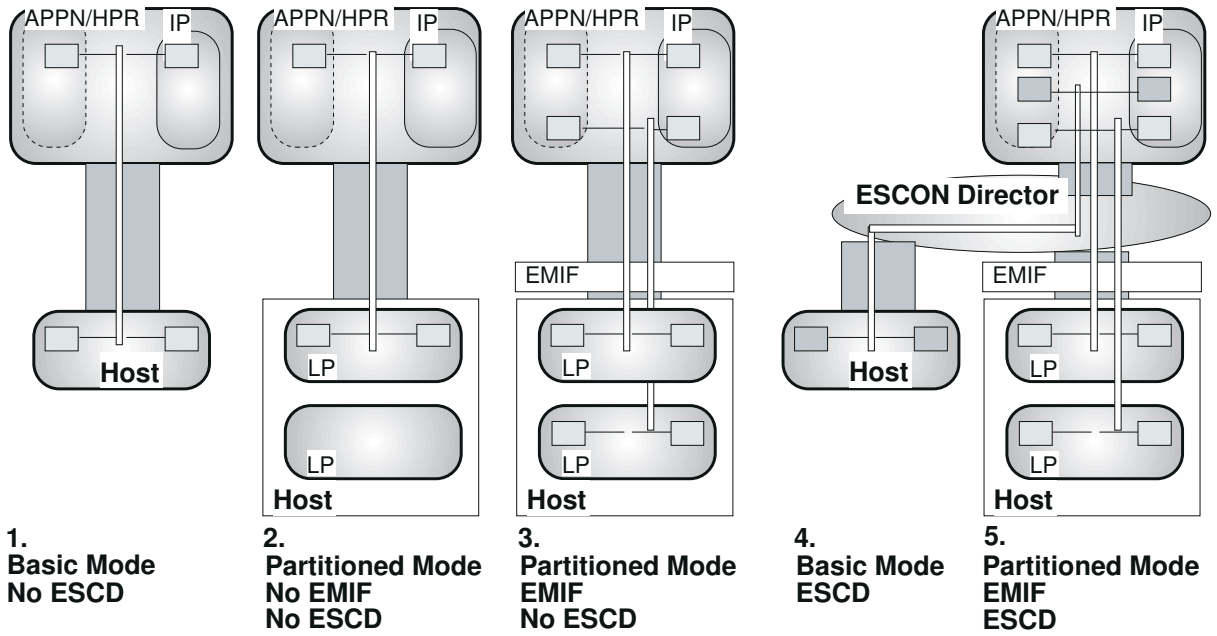


Figure 56. ESCON Host Links and Link Stations

The maximum number of host links that can be defined per ESCON adapter is 32. The actual number depends on the type of physical attachment between your host and the 3746-9x0:

Configurations 1 and 2
If your host is directly attached and running in basic (non-partitioned) mode only, or in the partitioned mode without the IBM ESCON Multiple Image Facility (EMIF), then a single host link can be defined.

Configuration 3
If your host is directly attached, is running in partitioned mode, and uses the ESCON multiple image facility (EMIF), then a single host link can be defined to each LP.

Configuration 4
If your host is connected via an ESCON Director (ESCD), then a single host link is possible to each host running in basic (non-partitioned) mode.

Configuration 5
If your host is connected via an ESCON Director (ESCD), then a single host link is also possible to each LP on the host running in partitioned mode and using the ESCON multiple image facility (EMIF).

Link stations map one-to-one with I/O addresses on your host. By using a specific I/O address to, for example, TCP/IP for MVS and assigning the corresponding link station to the 3746-9x0 IP functions, native IP communication between the two is possible.

ESCON: Port Sharing

As discussed in the previous section, up to 32 link stations can be defined per ESCON adapter. Each link station provides a point-to-point connection. See Figure 57 on page 115.

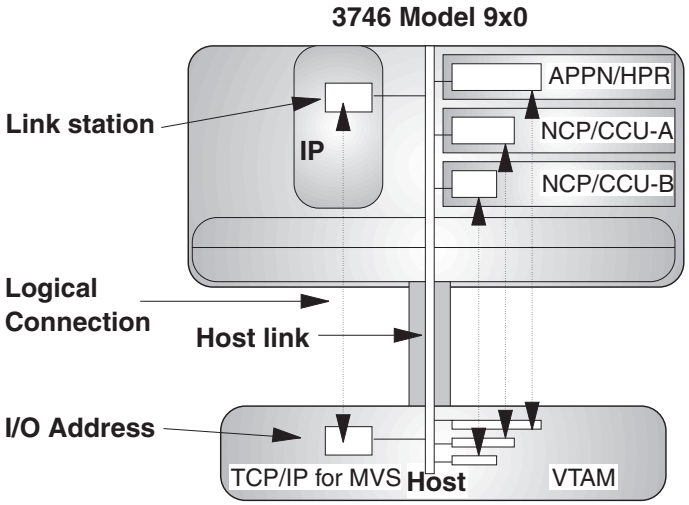


Figure 57. ESCON Port Sharing

ESCON ports can be defined and simultaneously activated from all protocol stacks available (IP, APPN/HPR, and for 3746-900 only; NCPs running on CCU-A and CCU-B on the attached 3745). On a 3746-900, each link station must be assigned to either 3746 IP, NCP/CCU-A, NCP/CCU-B, or the 3746 NN function; on a 3746-950, a link station must be assigned to either the 3746 IP, NCP or the 3746 NN function.

Link stations map one-to-one on I/O addresses defined on attached host systems. The I/O addresses are used by host programs to communicate with the corresponding protocol stack. The 3746-9x0 IP protocol stack can only communicate with TCP/IP for MVS (Version 3, Release 1 or 2), while the 3746 APPN/HPR and/or NCP protocol stacks can communicate with VTAM and/or TPF.

Link stations are independently assigned, and, therefore, an ESCON port and each host link can be shared between up to four (two on the 3746-950) 3746 protocol stacks. The total number of link stations per physical port cannot exceed 32.

ESCON: IP Addresses and Subnet Addresses Rules

The following section explains the rules for IP address definitions for ESCON channels.

The following general rules apply:

- One (physical) host can run multiple IP address spaces. Each IP address space is a full TCP/IP MVS stack (partition).
- Each IP address space is independent of the others.
- Each IP address space can run one or multiple CDLC instances.
- Each CDLC instance of a given IP address space must run on a separate ESCON fiber.

The following rules are defined by TCP/IP for MVS:

- CDLC instances of a ***single*** IP address space cannot have the same next-hop IP address.
- CDLC instances of ***different*** IP address spaces can have the same next-hop IP address, as they are in independent IP stacks.

The following rules are defined by the 3746:

- For hosts with only 1 IP address space and 1 CDLC in the IP address space.

  Users can define a single subnet between the hosts and the 3746 stations.

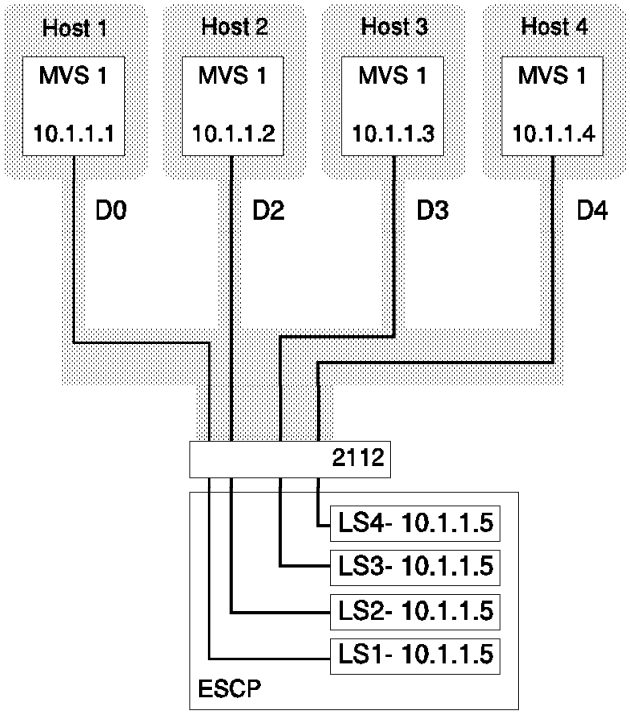


Figure 58. Four ESCP Stations with the Same IP Addresses

- For hosts with many IP address spaces and 1 CDLC per IP address space. Users can define a single subnet between the hosts and the 3746 stations.

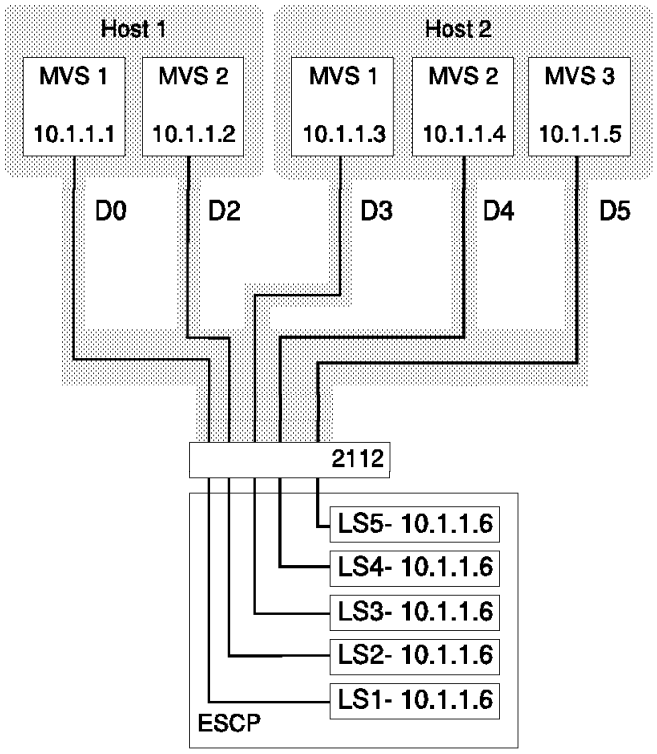
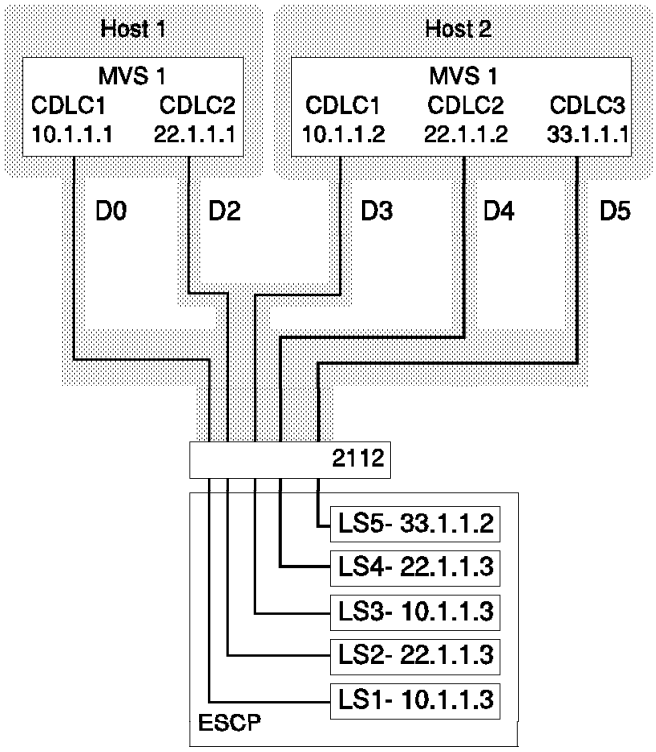


Figure 59. Five ESCP Stations with the Same IP Addresses

- For hosts with many IP address spaces and many CDLC per IP address space.

  Users ***must*** define multiple ***subnets***, the basic rule being that two CDLCs of the same MVS IP address space cannot be in the same subnet.




```
Subnets:
- 10.0.0.0 used for HOST1/CDLC1, HOST2/CDLC1 and ESCP LS1 and LS3
- 22.0.0.0 used for HOST1/CDLC2, HOST2/CDLC2 and ESCP LS2 and LS4
- 33.0.0.0 used for HOST2/CDLC3 and ESCP LS5.
```

Figure 60. ESCP Stations on Separate Subnets

ESCON: IP Configuration

The IP configuration for ESCON link stations consists of:

- Assigning an IP address and subnet mask to the link station. Each link station represents a separate point-to-point CDLC link, therefore, for each link station an IP address must be assigned that is part of a different subnet.
- Enabling dynamic routing protocol on this interface (or define static routes). Assigning an IP address (see “IP Addressing” on page 80) and subnet mask (see “The Subnet Mask” on page 83) is mandatory. In addition, the channel adapter slowdown time (CASDL), the attention timer (TIMEOUT), and the delay time (DELAY) timer have to be defined.

Enabling dynamic routing protocols is optional. It is only required when the TCP/IP for MVS system has multiple IP connections, and static routing does not suffice. The only dynamic routing protocol currently supported by TCP/IP for MVS (Version 3, Release 1 and 2) is RIP.

Token-Ring

token-ring attachments can be used to provide IP transport between the 3746 IP and IP stations or routers running TCP/IP.

For the IP communication over token-ring, the 3746-9x0 uses (connectionless) IEEE 802.2 logical link control (LLC). IEEE 802.2 LLC requires the use of a local and a remote service access point (SAP). For IP communication both local and remote SAP should be equal to X'AA', indicating sub-network access protocol (SNAP) encapsulation. See Figure 61. The (optional) ***routing information field (RIF)*** in the MAC header indicates the support for source route bridging, which is by default available.

SD - Starting Delimiter
AC - Access Control Field
FC - Frame Control Field
DMAC - Destination MAC address
SMAC - Source MAC address
RIF - Routing Information Field
DSAP - Destination SAP (AA for IP)
SSAP - Source SAP (AA for IP)

OUI PID - Organization/Protocol Identifier
OUI - 00 00 00
PID - 0800,0806 (IP, ARP)
FCS - Frame Check Sequence
ED - End Delimiter
FS - Frame Status Field

Figure 61. Token-Ring Encapsulation

On each 3746-9x0, you can install up to 16 token-ring adapters. Each token-ring adapter can control up to two token-ring interface couplers (TIC3). Each token-ring coupler provides a single physical connection to a token-ring LAN.

Note: The 3746-9x0 supports the attachment of up to 32 token-ring LANs (31 on a 3746-900 attached to a dual CCU Model 3745).

The token-ring configuration process consists of two phases:

1. A general definition part in which token-ring port specifics are defined
2. The actual IP port configuration.

Token-Ring: General Configuration

To define a token-ring port you have to specify its IP and APPN/HPR (if relevant) names, the speed of the token-ring LAN, and the local MAC address. The APPN and HPR SAPs are only relevant if the port is also used for APPN traffic. Make sure the IP maximum transmission unit (MTU) is high enough to prevent fragmentation of IP datagrams on the 3746 IP Router. However, in a bridged environment, make sure that the MTU is smaller than the lowest value configured on any on the LAN bridges. Select IP parameters to enter the IP over token-ring configuration. For IP transport no station needs to be defined.

Token-Ring: Port Sharing

token-ring ports can be defined on all protocol stacks. However, simultaneous activation of the port is limited to the IP protocol stack, APPN/HPR protocol, and (3746-900 only) either the NCP running on CCU-A or the NCP running on CCU-B of the attached 3745. Therefore, on the 3746-900, a token-ring port can be shared between the 3746 IP, a single NCP and the 3746 NN function; on a 3746-950, the token-ring port can be shared between the 3746 IP and the 3746 NN function. The 3746-9x0 data link control layer differentiates traffic from/to any of these protocol stacks using the service access points (SAPs) within the token-ring MAC header.

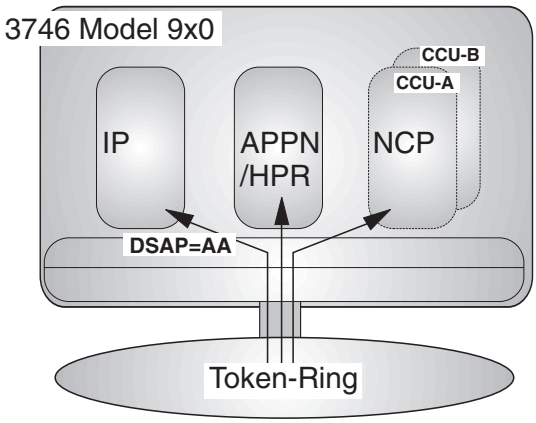


Figure 62. Token-Ring Port Sharing

When receiving data the 3746-9x0 will accept the following source SAPs:

- X'AA' - data to/from 3746 IP stack.
- X'04' - SNA data to/from NCP protocol stack (3746-900 only).
- X'C8' - HPR non-ERP data to/from NCP protocol stack (3746-900 only).
- X'xx' - APPN data to/from 3746 NN protocol stack *xx* is configured in the APPN local SAP field during token-ring port configuration.
- X'yy' - HPR non-ERP data to/from 3746 NN protocol stack *yy* is configured in the APPN/HPR local SAP field during token-ring port configuration.

Token-Ring: IP Configuration

The IP configuration for token-ring ports consists of:

- Assigning an IP address and subnet mask to the token-ring port.

  Note that the 3746 IP Router allows you to specify multiple IP addresses and subnet masks to the same physical interface. When defining multiple IP addresses, the 3746 IP Router connects to multiple subnets. The 3746-9x0 is capable of routing between subnets on the same physical interface, although in general this is not recommended.

- Enabling dynamic routing protocol for each IP address (or define static routes).

  The 3746 IP dynamic routing protocols operate independently for each IP address defined on a token-ring interface; therefore, each IP address is defined in the configuration.

Assigning an IP address and subnet mask is mandatory. At least one but optionally multiple (up to 16) IP addresses can be defined. If multiple IP addresses are defined, make sure that the addresses are part of different subnets.

The RIF timer indicates how many seconds will elapse between the last reference to an ARP entry and when it will be deleted. Increasing the timer may result in more storage being required to cache ARP entries. A zero value will disable the ARP caching function.

Enabling dynamic routing protocols is optional. It is only required when any of the token-ring attached devices have multiple IP interfaces, and static routing does not suffice. Dynamic routing protocols supported by the 3746-9x0 are RIP, OSPF, and BGP.

External IP Connection Between 3745 and 3746-900

With the introduction of NCP V7R6 it is now possible to link the NCP IP router and the 3746 IP router together via the CBC between the 3745 and 3746. Previously, an external link between the 3745 and 3746 was need to connect the two routers. To support this function from the 3746 side, the optional FC 5800 is needed. This is supported by microcode level D46130I (ECA 170) and later versions.

The internal connection or connections between the two routers are seen as token-ring point-to-point (PtP) IP connections, these connections must be defined in the NCP and 3746 CCM. Each connection uses a separate TIC3 on the 3746, this TIC3 may also be used to drive a token-ring, but beaconing on that token-ring or other problems may interfere with the IP routing function. For that reason it is recommended, but not mandatory, that each TIC3 used for an internal IP connection is used only for that function.

Figure 63 on page 122 shows a representation of the internal point-to-point IP connection.

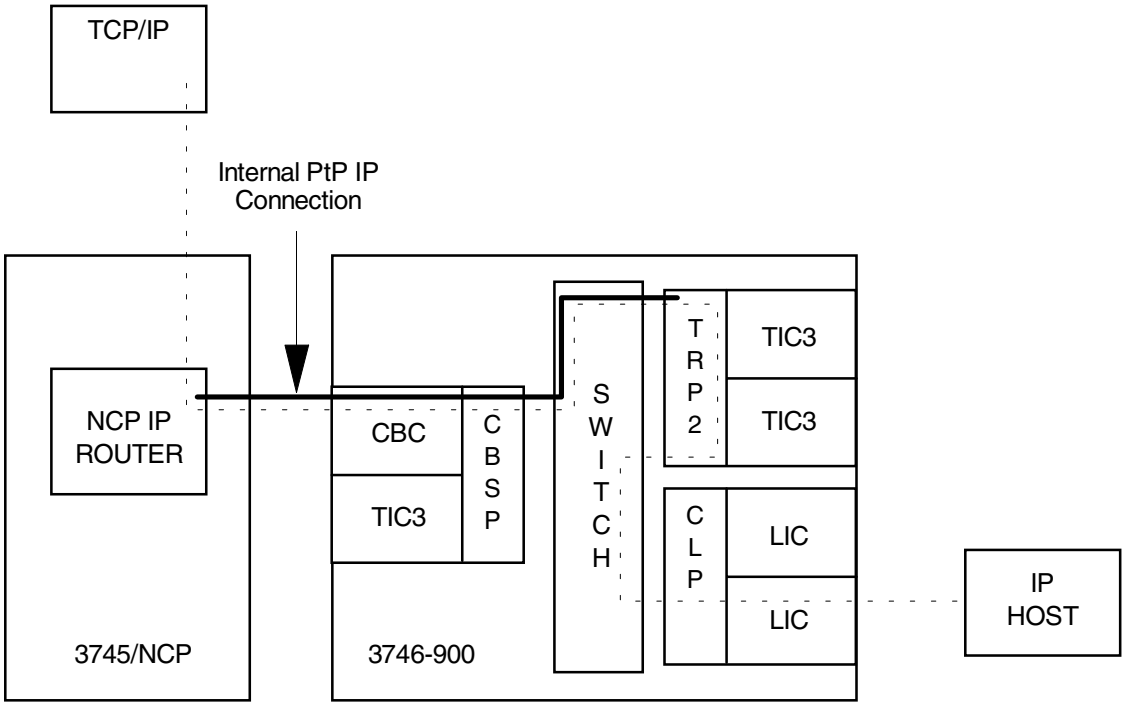


Figure 63. Internal IP PtP Connection

Internal IP Connection Definitions

The following sections explain how to define an internal point-to-point IP connection. Figure 64 shows the configuration which is being defined. The definitions shown here include all the information needed for this part of the NCP generation process, the actual PtP link is defined in the LN2880 LINE (1), and IP2880 PU (2) statements, and the IPLOCAL statement for LADDR=10.04.00.99 (5). The NETWORK must be IP (3), and PUTYPE must be 1 (4).

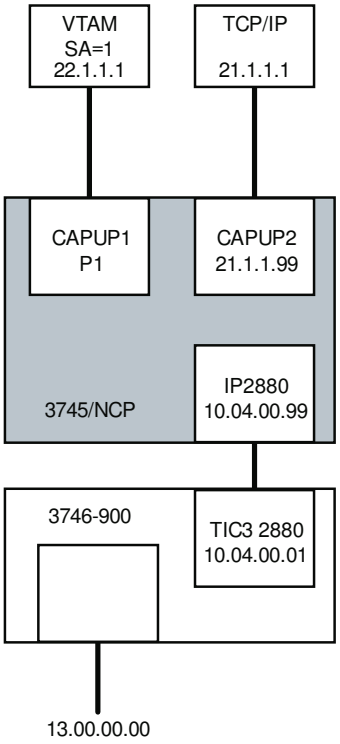


Figure 64. Example Configuration

NCP Definitions: The following examples show the NCP definitions needed to configure the internal IP PtP link from the 3745 side.

```
*************************************************************************
* VTAM HOST DEFINITIONS
*************************************************************************
*
HOSTA01  HOST  BFRPAD=0,DELAY=0.0,INBFRS=6,MAXBFRU=32,
               SUBAREA=1,
               STATMOD=YES,UNITSZ=1024
*
*************************************************************************
*  TOKEN-RING LINE 2880
*************************************************************************
*
ODLCGRP1 GROUP ECLTYPE=(PHY,ANY),ADAPTER=TIC3,
               DIAL=NO,LNCTL=SDLC,TYPE=NCP
LN2880   LINE  ADDRESS=(2880,FULL)  1 ,
               LOCADD=400000002880,
               MAXPU=2,
               MAXTSL=16732,
               NPACOLL=YES,
               PORTADD=2,
               SPEED=9600,
               TRSPEED=16
IP2880   PU    ADDR=02,
               INTFACE=(TR2880,2048)  2 ,
               NPACOLL=YES,
               NETWORK=IP  3 ,
               PUTYPE=1  4 ,
               ARPTAB=(1)

*************************************************************************
*              CHANNEL ADAPTERS
*************************************************************************
*
CAGRP1   GROUP LNCTL=CA,CA=TYPE7,NCPCA=ACTIVE,MONLINK=CONT,
               TIMEOUT=240.0,ISTATUS=ACTIVE,CASDL=420.0,DELAY=0.0
*
*************************************************************************
*  VTAM HOST CHANNEL ATTACHMENT
*************************************************************************
*
CALNP1   LINE  ADDRESS=P1
CAPUP1   PU    PUTYPE=5,TGN=1
*
*************************************************************************
*  CHANNELS FOR IP CHANNEL ATTACHED ROUTERS
*************************************************************************
*
CALNP2   LINE  ADDRESS=P2,CASDL=420,DELAY=0.0,MONLINK=NO
CAPUP2   PU    PUTYPE=1,INTFACE=CPU2,ARPTAB=(10,,NOTCANON)
```

```
*************************************************************************
*        IP ROUTING DEFINITIONS
*************************************************************************
*
         IPOWNER HOSTADDR=21.1.1.1,NUMROUTE=(25,25,25),UDPPORT=580,
                 INTFACE=(CPU2),MAXHELLO=6,NUMDRIF=10

         IPLOCAL LADDR=21.1.1.99,INTFACE=CPU2,METRIC=1,
                 P2PDEST=21.1.1.1,PROTOCOL=RIP
*
         IPLOCAL LADDR=10.04.00.99 [5] , INTFACE=TR2880, METRIC=1,
                 P2PDEST=10.04.00.01 [6] , PROTOCOL=RIP, SNETMASK=255.255.0.0
*
         IPROUTE DESTADDR=13.0.0.0 [7] ,
                 NEXTADDR=10.4.00.01 [8] ,
                 INTFACE=TR2880,
                 METRIC=1,DISP=PERM,HOSTRT=NO
*
GENEND   GENEND
         END
```

For reference, the following is a short description of some of the parameters used:

IPOWNER Identifies the TCP/IP MVS/VM host that manages the routing tables (NCPROUTE)

IPLOCAL Defines an interface to the NCP IP router.

IPROUTE Defines an entry in the NCP IP routing table.

HOSTADDR Defines the IP address of the owning IP host.

INTFACE Defines the name of the IP interface to NCPROUTE.

LADDR Defines the IP address of the interface.

P2PDEST Defines IP address of the destination IP host.

SNETMASK Defines subnet mask for the interface.

3746 CCM Definitions:

1. The token-ring port 2880 must be configured first, and IP must be activated on that port.

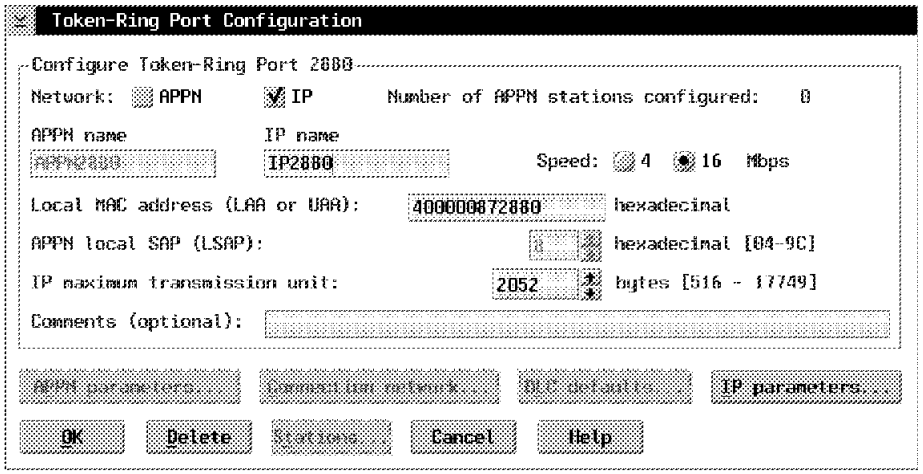


Figure 65. Port Configuration

2. On port 2880, an IP address must be defined, this is the IP address of the 3746 end of the PtP IP connection, 10.4.0.1. This must match the IP address specified on the P2PDEST operand on the IPLOCAL statement in NCP.

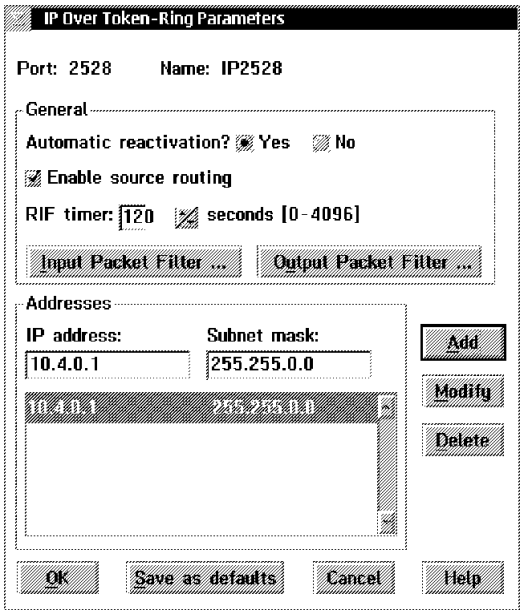


Figure 66. IP over Token-Ring Parameters

3. RIP should be activated as shown on port 2880.

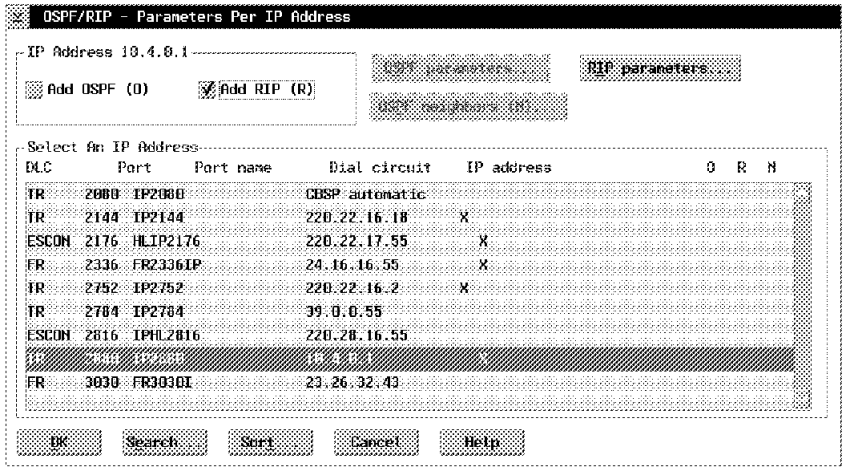


Figure 67. OSPF/RIP Parameters per IP Address

4. The following RIP parameters should be activated for IP address 10.4.0.1.

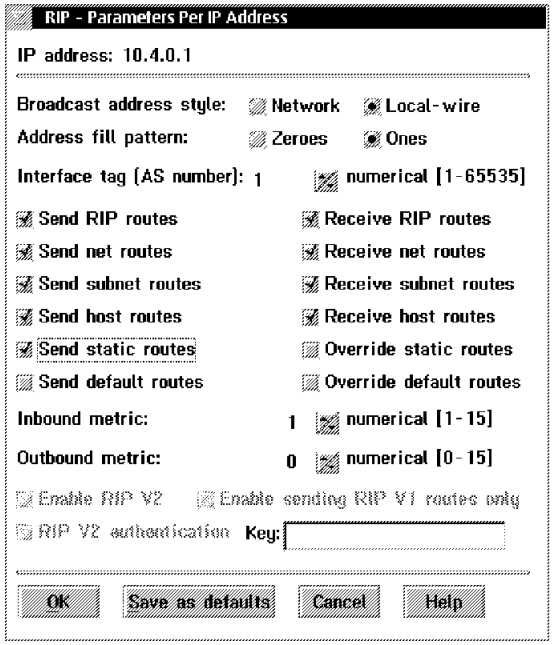


Figure 68. RIP Parameters per IP Address

To use the internal PtP link for IP routing, to reach the destination network 13.0.0.0 (DESTADDR=13.0.0.0 **7**) from NCP, the next hop (NEXTADDR **8**) points to the IP address of the 3746 end of the PtP connection 10.4.0.1.

Internal IP Connection Between 3745 and 3746-900

In the previous sections it has been explained that on a 3746-900, NCP and 3746 IP functions can coexist. As NCP is also providing IP routing functions, it is important that a distinction is made between the 3746 IP (stand-alone) and the NCP-controlled IP (NCP-IP) routing functions.

3746 IP provides IP routing for ESCON channel, token-ring (TIC3), Ethernet, and serial line (frame relay, X.25, and PPP) attached equipment. Connectivity is provided through 3746-900 attachments only. NCP-IP provides IP routing for ESCON channel, parallel channel, token-ring (TIC1/TIC2), Ethernet, and serial line (frame relay) attached equipment. However, with the exception of ESCON, NCP-IP connectivity is provided through base attachments only, that is, for equipment not attached to the 3746-900.

3746 IP and NCP-IP perform their IP routing functions in a fully independent fashion. IP connectivity between both IP routers requires an external connection. Internal (via the CBC) IP connections is not supported. Figure 69 on page 128 depicts how direct IP connectivity between NCP-IP and 3746 IP can be realized via token-ring, Ethernet, and frame relay. In all cases, a port (token-ring, Ethernet, or frame relay, respectively) is required on both the 3746-900 and the 3745 base frame (or a 3746 Model L1x).

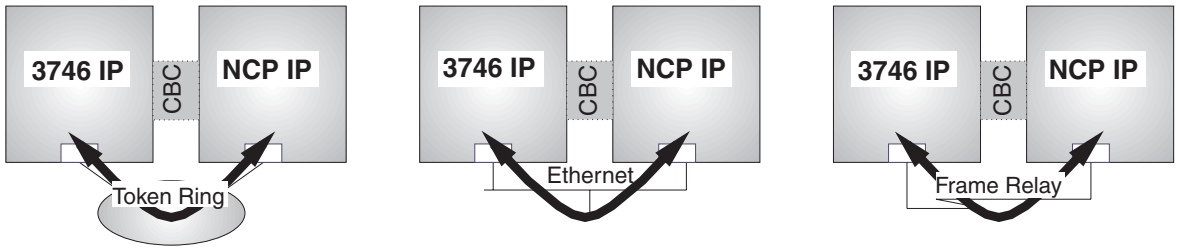


Figure 69. Direct NCP-IP 3746 Routing

Figure 70 shows an alternative for the direct 3746 IP to NCP-IP attachment. A single ESCON channel can be used to connect TCP/IP for MVS (Version 3, Release 1 or 2) to both 3746 IP and NCP-IP. The result, however, of IP connectivity between 3746 IP and NCP-IP is that all IP datagrams that are sent between 3746 IP and NCP-IP will be routed via TCP/IP for MVS.

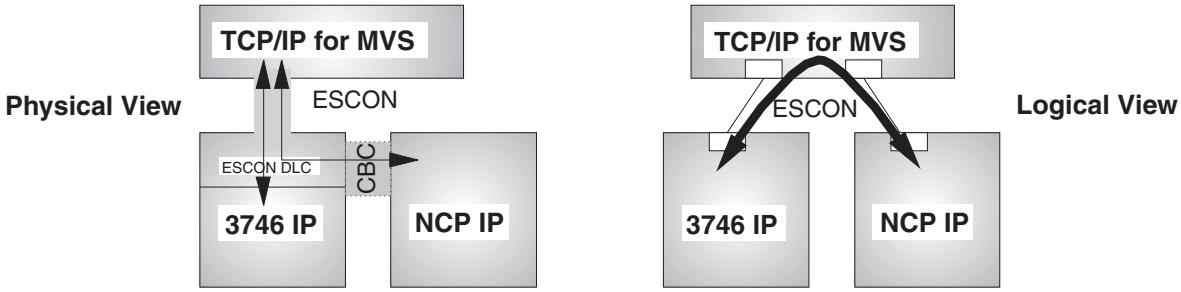
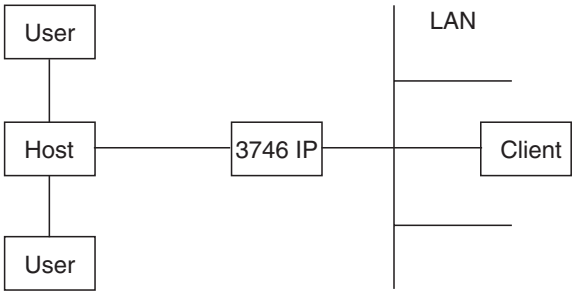


Figure 70. NCP-IP 3746 Routing Over ESCON

Telnet Operations via the 3746 Network Node

The Telnet protocol provides a standardized interface through which a program on one host (the Telnet client) may access the resources of another host (the Telnet server) via a 3746 Network Node as though the client were a local terminal connected to the server (see Figure 71 on page 129). For example, a user on a workstation on a LAN may connect to a host as though the workstation were a terminal attached directly to the host.

The 3746 Network Node provides the through connection.



How Telnet appears to the host and client.

Figure 71. Telnet Connection via a 3746 Network Node

Telnet allows the LAN-attached user to log in the same way as the local terminal user.

Note: The 3746 Network Node provides the connection but does not provide the actual host/client function. Refer to the documentation of the respective host and client systems for the functions available on those hosts/clients. This chapter gives an overview of Telnet possibilities.

Basic Operation

The Telnet protocol is based on three ideas:

- Network Virtual Terminal (NVT) concept

  An NVT is an imaginary device having a basic structure common to a wide range of real terminals. Each host maps its own terminal characteristics to those of an NVT, and assumes that every other host will do the same.

- A symmetric view of terminals and processes
- Negotiation of terminal options

  The principle of negotiated options is used by the Telnet protocol, because many hosts wish to provide additional services, beyond those available with the NVT. Various options may be negotiated. After this minimum understanding is achieved, they can negotiate additional options to extend the capabilities of the NVT to reflect more accurately the capabilities of the real hardware in use. Because of the symmetric model used by Telnet, both the host and the client may propose additional options to be used.

Telnet operations, enabling and disabling, can be protected by passwords.

Network Virtual Terminal

The NVT has a printer (or display) and a keyboard. The keyboard produces outgoing data, which is sent over the Telnet connection. The printer receives the incoming data. The basic characteristics of an NVT, unless they are modified by mutually agreed options are:

- The data representation is 7-bit ASCII transmitted in 8-bit bytes.
- The NVT is a half-duplex device operating in a line-buffered mode.
- The NVT provides a local echo function.

All of these may be negotiated by the two hosts.

NVT Printer

An NVT Printer has an unspecified carriage width and page length. It can handle printable ASCII characters (ASCII code 32 to 126) and understands some ASCII control characters.

Full-Screen Capability

Full-screen Telnet is possible provided the client and server have compatible full-panel capabilities. For example, VM and MVS provide a TN3270-capable server. To use this facility, a Telnet client must support TN3270.

Command Structure

The communication between client and server is handled with internal commands, which are not accessible by users. All internal Telnet commands consist of 2 or 3-byte sequences, depending on the command type. An Interpret As Command (IAC) character is followed by a command code. This command deals with option negotiation, and has a third byte to show the code for the referenced option.

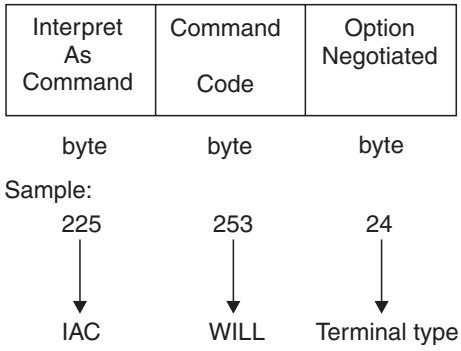


Figure 72. Telnet Command Structure

Host/Client Implementations

You can only use Telnet if it is implemented on ***both*** client ***and*** host machines, refer to your documentation for both. The respective documentation should also tell you the full range of Telnet functions available for those systems.

Mandatory Access Control Entry

The following entry in the access control list is mandatory and may ***not*** be removed:

```
PERMIT   0.0.0.0   0.0.0.0   0.0.0.0   0.0.0.0
```

If this entry is removed, NetView/6000 cannot gain access to the SNMP agent that resides on the NNP and no SNMP management of the 3746 will be possible.

List of Abbreviations

AB	area border
ACF	advanced communications function
ACF/VTAM	advanced communications function for the virtual telecommunications access method
ANR	automatic network routing
APPN	advanced peer-to-peer networking
ARB	adaptive rate-based flow/congestion control
ARC	active remote connector
ARP	address resolution protocol
AS	autonomous system
ASB	autonomous system border
ASE	autonomous system external
ASCII	american national standard code for information interchange
AUTO	automatic
BAN	boundary access node
BECN	backward explicit congestion notification
BER	box event record
BGP	border gateway protocol
BOOTP	bootstrap protocol
bps	bits per second
BRS	bandwidth reservation system
BSC	binary synchronous communication
C&SM	communications and system management
CBSP	control bus and service processor
CCITT	Comité Consultative International Télégraphique et Téléphonique The international telegraph and telephone consultative committee
CCU	central control unit
CD	carrier detector
CDF-E	configuration data file - extended
CE	customer engineer
CF3745	3745 and 3746 configurator and performance model
CHPID	channel path id
CIDR	classless inter-domain routing
CIR	committed information rate
CLIST	command list
CLA	communication line adapter
CLP	communication line processor
CM	communications manager
CNN	composite network node
CNM	communication network management
COS	cost of service
CP	control point
CR	communications rate
CSU	customer service unit
DCAF	distributed console access facility
DCE	data circuit-terminating equipment
DDS	digital data service
DE	discard eligibility
DLC	data link control
DLCI	data link connection identifier
DLSw	data link switching
DLUR	dependent LU requester
DLUS	dependent LU server
DMUX	double multiplex circuit
DSU	data service unit
DTE	data terminal equipment
DX	duplex
EBCDIC	extended binary-coded decimal interchange code
EBN	extended border node
EC	engineering change
EMIF	ESCON multiple image facility
EN	end node
EP	emulation program
EPO	emergency power OFF
ESCA	ESCON channel adapter
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
FRFH frame-relay frame handler
FRSE frame-relay switching equipment
FRTE frame-relay terminating equipment
HCD hardware configuration definition
HDX half duplex
HI high
HLA host link address
HONE hands-on network environment
HPR high performance routing
HSS high-speed scanner
ICMP internet control message protocol
IML initial microcode load
INN intermediate network node or IBM information network
IOCP Input/Output Configuration Program
IP internet, or internetwork, protocol
IPL initial program load
IPR installation planning representative
ITU-T international telecommunications union - telecommunications (ex-CCITT)
KB kilobyte (processor storage) 1KB = 2^{10} bytes (1 024 bytes)
kbps kilobits per second (speed or communication volume per second) 1 kbps = 1 000 (one thousand) bits per second
LAA locally administered address
LAN local area network
LCB line connection box
LCBB line connection box base
LCBE line connection box expansion
LCP link control protocol
LDM limited distance modem
LED light emitting diode
LIB n line interface board type n
LIC n line interface coupler type n
LSA link state advertisement
LIU n line interface coupler unit type n
LIV link integrity verification
LMI local management interface
LP logical partition
LPDA® link problem determination aid
LQ line quality
LU logical unit
LSS low-speed scanner
MAC medium access control
MAU medium attachment unit
MB megabyte (processor storage) 1MB = 2^{20} bytes (1 048 576 bytes)
Mbps megabits per second (speed or communication volume per second) 1 Mbps = 1 000 000 (one million) bits per second
MCL microcode change level
MES miscellaneous equipment specification
MIB management information base
MIH missing interrupt handler
MLC machine level control
MLTG multi-link transmission group
MOSS-E maintenance and operator subsystem - extended
MTP multipoint
MUX multiplex circuit
MVS multiple virtual storage
NAU network addressable unit
NMBA nonbroadcast multiaccess
NCP Network Control Program
NDRS non-disruptive route switching
NGMF netView graphic monitor facility
NN network node
NNP network node processor
NPM netView performance monitor
NRZI non-return-to-zero inverted
NVT network virtual terminal
ODLC outboard data link control
OSPF open shortest path first
PBN peripheral border node
PCI Peripheral component interconnect
PEP partitioned emulation program
PING packet internet groper
PN peripheral node
PPP point-to-point protocol
PPPNCP point-to-point network control protocol
PTP point-to-point

PTT	post, telegraph, and telephone
PU	physical unit
PVC	permanent virtual circuit
QUAL	quality
RCV	receive clock
RETAIN®	remote technical assistance information network
RFS	ready for sending
RIP	routing information protocol
RNR	receive not ready
ROS	read-only storage
RR	receive ready
RSF	remote support facility
RTP	rapid transport protocol
RTS	request to send
SDLC	synchronous data link control
SMUX	single multiplex circuit
SNBU	switched network backup
SNI	SNA network interconnection
SNMP	simple network management protocol
SPAU	service processor access unit
SRC	service reference code
S/S	start-stop
SVC	switched virtual circuit
TC	test control
TCM	trellis code modulation
TCP	transmission control protocol
TG	transmission group
THRES	threshold
TICn	Token-ring interface coupler type n
TIM	time services
TOS	type of service
TPF	transaction processing facility
TRA	Token-ring adapter
TRP	Token-ring processor
TSS	transmission subsystem
UDP	user datagram protocol
UTP	unshielded twisted pair
VTAM	virtual telecommunications access method
XID	exchange station identification
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 is 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 and 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 chhnection (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*.

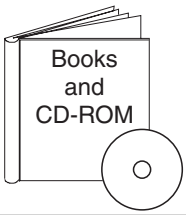
V.24, V.35, and X.21. ITU-T (ex-CCITT) recommendations on transmission interfaces.

Bibliography

Customer Documentation for the 3745 (All Models), and 3746 (Model 900)

Table 20 (Page 1 of 6). Customer Documentation for the 3745 Models X10 and X1A, and 3746 Model 900

This customer documentation has the following formats:

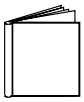


Finding Information

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



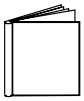
GA33-0092

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.

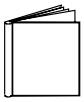


GA33-0180

IBM 3745 Communication Controller Models A and 170[2]
IBM 3746 Nways Multiprotocol Controller
Models 900 and 950

Overview

Gives an overview of connectivity capabilities within SNA, APPN, and IP networking.



GA27-4234

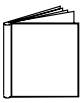
IBM 3745 Communication Controller Models A[2]
IBM 3746 Nways Multiprotocol Controller
Models 900 and 950

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 20 (Page 2 of 6). Customer Documentation for the 3745 Models X10 and X1A, and 3746 Model 900



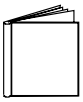
GA27-4235

IBM 3745 Communication Controller Models A[2]
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.



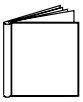
GA27-4236

IBM 3745 Communication Controller Models A[2]
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 desription and configuration.



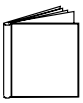
GA27-4237

IBM 3745 Communication Controller Models A[2]
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

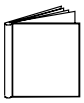
IBM 3745 Communication Controller Models A[2]
IBM 3746 Nways Multiprotocol Controller
Models 900 and 950

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 20 (Page 3 of 6). Customer Documentation for the 3745 Models X10 and X1A, and 3746 Model 900



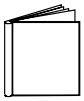
GA27-4239

IBM 3745 Communication Controller Models A²
IBM 3746 Nways Multiprotocol Controller
Models 900 and 950

Planning Series:
Management Planning

Provides information for:

- Overview for 3746
- 3746 APPN/HPR, IP router, and X.25
- NetView Performance Monitor (NPM), remote consoles, and RSF
- MAE APPN/HPR management.



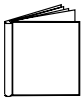
GA27-4240

IBM 3745 Communication Controller Models A²
IBM 3746 Nways Multiprotocol Controller
Models 900 and 950

Planning Series:
Multiaccess Enclosure Planning

Provides information for:

- 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:

- Overview and details about APPN/HPR and IP.

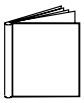
On-line information

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



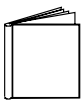
GC22-7064

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 *Planning Guide*, GA33-0457.



GA33-0127

IBM 3745 Communication Controller
Models 210, 310, 410, and 610

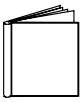
Preparing for Connection

Helps for preparing the 3745 Models 210 to 610 cable installation.

For 3745 Models A refer to the *Connection and Integration Guide*, SA33-0129.

Table 20 (Page 4 of 6). Customer Documentation for the 3745 Models X10 and X1A, and 3746 Model 900

Preparing for Operation

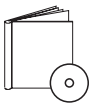


GA33-0400

IBM 3745 Communication Controller All Models[3]
IBM 3746 Nways Multiprotocol Controller
Models 900 and 950

Safety Information[1]

Provides general safety guidelines.

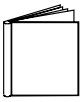


SA33-0129

IBM 3745 Communication Controller All Models[3]
IBM 3746 Nways Multiprotocol Controller Model 900

Connection and Integration Guide[1]

Contains information for connecting hardware and integrating network of the 3745 and 3746-900 after installation.

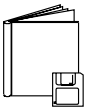


SA33-0416

Line Interface Coupler Type 5 and Type 6
Portable Keypad Display

Migration and Integration Guide

Contains information for moving and testing LIC types 5 and 6.



SA33-0158

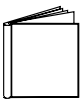
IBM 3745 Communication Controller All Models[3]
IBM 3746 Nways Multiprotocol Controller Model 900

Console Setup Guide[1]

Provides information for:

- 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:
  - DCAF program
  - Telnet Client program
  - Java Console support.

Customizing Your Control Program



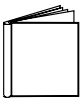
SA33-0178

Guide to Timed IPL and Rename Load Module

Provides VTAM procedures for:

- Scheduling an automatic reload of the 3745
- Getting 3745 load module changes transparent to the operations staff.

Operating and Testing

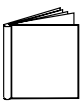


SA33-0098

IBM 3745 Communication Controller
All Models[4]

Basic Operations Guide[1]

Provides instructions for daily routine operations on the 3745 Models 130 to 610.



SA33-0177

IBM 3745 Communication Controller Models A[2]
IBM 3746 Nways Multiprotocol Controller Model 900

Basic Operations Guide[1]

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.

Table 20 (Page 5 of 6). Customer Documentation for the 3745 Models X10 and X1A, and 3746 Model 900

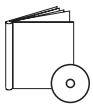
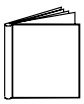
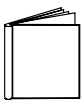
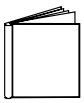
	SA33-0097	***IBM 3745 Communication Controller All Models***[3] ***Advanced Operations Guide***[1] Provides instructions for advanced operations and testing, using the 3745 MOSS console.
	On-line Information	***Controller Configuration and Management Application*** Provides a graphical user interface 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.
	SH11-3081	***IBM 3746 Nways Multiprotocol Controller Models 900 and 950*** ***Controller Configuration and Management: User's Guide***[5] Explains how to use CCM and gives examples of the configuration process.
	GA33-0479	***IBM 3745 Communication Controller Models A*** ***IBM 3746 Nways Multiprotocol Controller Models 900 and 950*** ***NetView Console APPN Command Reference Guide*** Explains how to use the RUN COMMAND from the NetView S/390 Program and gives examples.
Managing Problems		
	SA33-0096	***IBM 3745 Communication Controller All Models***[3] ***Problem Determination Guide***[1] A guide to perform problem determination on the 3745 Models 130 to 61A.
	On-line Information	***Problem Analysis Guide*** An online guide to analyze alarms, events, and control panel codes on: • IBM 3745 Communication Controller Models A[2] • IBM 3746 Nways Multiprotocol Controller Models 900 and 950.
	SA33-0175	***IBM 3745 Communication Controller Models A***[2] ***IBM 3746 Expansion Unit Model 900*** ***IBM 3746 Nways Multiprotocol Controller Model 950*** ***Alert Reference Guide*** Provides information about events or errors reported by alerts for: • IBM 3745 Communication Controller Models A[2] • IBM 3746 Nways Multiprotocol Controller Models 900 and 950.

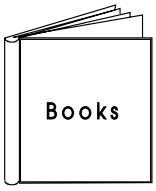
Table 20 (Page 6 of 6). Customer Documentation for the 3745 Models X10 and X1A, and 3746 Model 900

[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

Table 21. Additional Customer Documentation for the 3745 Models 130 to 17A

This customer documentation has the following format:

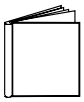


Finding Information

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



GA33-0138

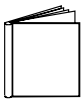
IBM 3745 Communication Controller
Models 130, 150, 160, and 170

Introduction

Gives an introduction about the IBM Models 130 to 170 capabilities, including Model 160.

For Model 17A refer to the *Overview*, GA33-0180.

Preparing Your Site



GA33-0140

IBM 3745 Communication Controller
Models 130, 150, 160, and 170

Preparing for Connection

Helps for preparing the 3745 Models 130 to 170 cable installation.

For 3745 Model 17A refer to the *Connection and Integration Guide*, SA33-0129.

[1] Documentation shipped with the 3745.

Customer Documentation for the 3746 Model 950

Table 22 (Page 1 of 4). Customer Documentation for the 3746 Model 950

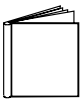
This customer documentation has the following formats:

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



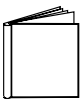
GA33-0400

IBM 3745 Communication Controller All Models[1]
IBM 3746 Expansion Unit Model 900
IBM 3746 Nways Multiprotocol Controller Model 950

Safety Information[2]

Provides general safety guidelines.

Evaluating and Configuring

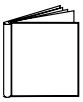


GA33-0180

IBM 3745 Communication Controller Models A and 170[3]
IBM 3746 Nways Multiprotocol Controller
Models 900 and 950

Overview

Gives an overview of connectivity capabilities within SNA, APPN, and IP networking.



GA27-4234

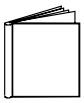
IBM 3745 Communication Controller Models A[2]
IBM 3746 Nways Multiprotocol Controller
Models 900 and 950

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 22 (Page 2 of 4). Customer Documentation for the 3746 Model 950



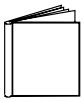
GA27-4235

IBM 3745 Communication Controller Models A2
IBM 3746 Nways Multiprotocol Controller
Models 900 and 950

Planning Series:
Serial Line Adapters

Provides information for:

- 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.



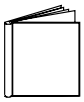
GA27-4236

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.



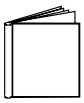
GA27-4237

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 22 (Page 3 of 4). Customer Documentation for the 3746 Model 950

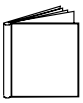
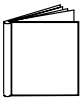
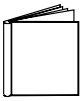
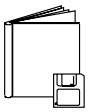
	GA27-4239	***IBM 3745 Communication Controller Models A***[2] ***IBM 3746 Nways Multiprotocol Controller*** ***Models 900 and 950*** ***Planning Series:*** ***Management Planning*** Provides information for: • Overview for 3746 • 3746 APPN/HPR, IP router, and X.25 • NetView Performance Monitor (NPM), remote consoles, and RSF • MAE APPN/HPR management.
	GA27-4240	***IBM 3745 Communication Controller Models A***[2] ***IBM 3746 Nways Multiprotocol Controller*** ***Models 900 and 950*** ***Planning Series:*** ***Multiaccess Enclosure Planning*** Provides information for: • MAE adapters details • MAE ESCON planning and configuration • ATM and ISDN support.
	GA27-4241	***IBM 3745 Communication Controller Models A***[2] ***IBM 3746 Nways Multiprotocol Controller*** ***Models 900 and 950*** ***Planning Series:*** ***Protocols Description*** Provides information for: • Overview and details about APPN/HPR and IP.
	On-line information	***IBM 3745 Communication Controller Models A***[2] ***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.

Table 22 (Page 4 of 4). Customer Documentation for the 3746 Model 950

Operating and Testing



SA33-0356

IBM 3746 Nways Multiprotocol Controller
Model 950

User's Guide[2]

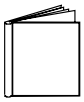
Explains how to:

- 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:
  - DCAF program
  - Telnet client program
  - Java Console support.

On-line information

Controller Configuration and Management Application

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.

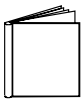


SH11-3081

IBM 3746 Nways Multiprotocol Controller
Models 900 and 950

Controller Configuration and Management: User's Guide[2]

Explains how to use CCM and gives examples of the configuration process.



GA33-0479

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

NetView Console
APPN Command Reference Guide

Explains how to use the RUN COMMAND from the NetView S/390 Program and gives examples.

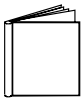
Managing Problems

On-line information

Problem Analysis Guide

An on-line guide to analyze alarms, events, and control panel codes on:

- IBM 3745 Communication Controller Models A[3]
- IBM 3746 Nways Multiprotocol Controller Models 900 and 950.



SA33-0175

IBM 3745 Communication Controller Models A[3]
IBM 3746 Expansion Unit Model 900
IBM 3746 Nways Multiprotocol Controller Model 950

Alert Reference Guide

Provides information about events or errors reported by alerts for:

- IBM 3745 Communication Controller Models A[3]
- IBM 3746 Nways Multiprotocol Controller Models 900 and 950.

[1] Models 130 to 61A.
[2] Documentation shipped with the 3746-950
[3] 3745 Models 17A to 61A.

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

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

X

Y

Tell Us What You Think!

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

Protocols Description

Publication No. GA27-4241-01

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
	☐	☐

How satisfied are you that the information in this book is:	Satisfied	Dissatisfied
Accurate	☐	☐
Complete	☐	☐
Easy to find	☐	☐
Easy to understand	☐	☐
Well organized	☐	☐
Applicable to your task	☐	☐

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

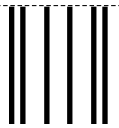
Company or Organization

Phone No.

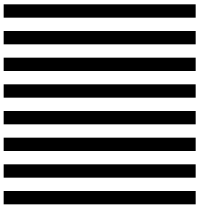
Tell Us What You Think!
GA27-4241-01

Cut or Fold
Along Line

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

Cut or Fold
Along Line

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

GA27-4241-01