Data Center Design and Implementation

IBM Internetworking Design Guide Series, Volume III

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number:

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: 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 users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The following third-party software may be included with your product and will be subject to the software license agreement:

CiscoWorks software and documentation are based in part on HP OpenView under license from the Hewlett-Packard Company. HP OpenView is a trademark of the Hewlett-Packard Company. Copyright © 1992, 1993 Hewlett-Packard Company.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Network Time Protocol (NTP). Copyright © 1992, David L. Mills. The University of Delaware makes no representations about the suitability of this software for any purpose.

Point-to-Point Protocol. Copyright © 1989, Carnegie-Mellon University. All rights reserved. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

The Cisco implementation of TN3270 is an adaptation of the TN3270, curses, and termcap programs developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981-1988, Regents of the University of California.

Cisco incorporates Fastmac and TrueView software and the RingRunner chip in some Token Ring products. Fastmac software is licensed to Cisco by Madge Networks Limited, and the RingRunner chip is licensed to Cisco by Madge NV. Fastmac, RingRunner, and TrueView are trademarks and in some jurisdictions registered trademarks of Madge Networks Limited. Copyright © 1995, Madge Networks Limited. All rights reserved.

XRemote is a trademark of Network Computing Devices, Inc. Copyright © 1989, Network Computing Devices, Inc., Mountain View, California. NCD makes no representations about the suitability of this software for any purpose.

The X Window System is a trademark of the X Consortium, Cambridge, Massachusetts. All rights reserved.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

978R

Introduction xiii

Intended Readers xiii

Cisco's Data Center Solutions xiii

Evolution of the Data Center xiii

PART 1 SNA Internetworking

Chapter 1 Introduction to SNA on the CIP 1-1

SNA Overview 1-1
- Subarea SNA Overview 1-1
- APPN Overview 1-3
- HPR Overview 1-5

Cisco SNA Support with a Channel-Attached Router 1-5
- SNA Channel Protocols Supported by the CIP 1-5
  - XCA Overview 1-6
  - MPC Overview 1-6
- SNA Appearance of the Channel-Attached Router 1-6
- SNA Device Connectivity 1-6
- Connectivity Options 1-7

Comparison of the CIP to Other Options 1-9
- Front-End Processors—IBM 3745 1-9
- The Cisco Channel-Attached Router as a FEP Alternative 1-10
- Benefits of a Cisco 7000 or 7500 Router with a CIP 1-12

Chapter 2 Network Design and Migration 2-1

Basic Design Considerations 2-1

Accessing Remote SNA Devices 2-2

Placement of SNA and WAN Functionality 2-2
- Data Center Scalability 2-2
- Data Center Availability 2-3
  - All in One (SNA, CIP, and WAN) 2-4
  - CIP and SNA Combined 2-4
  - CIP Solo 2-4

Determining How Many Channel-Attached Routers and CIPs Are Required 2-5
- CIP Capacity 2-5
- Channel-Attached Router Capacity 2-5
- Attaching the CIP to a Campus Backbone 2-5

Mainframe CPU Utilization 2-6

APPN in the Data Center 2-7
- Do You Need APPN for SNA Routing? 2-7
- APPN Functionality Placement 2-8

Dependent LU Support 2-8
Placement of DLUR Function 2-10
Sizing DLUR Routers 2-10
SSCP Takeover/Giveback 2-11

Migration to APPN from a Subarea Environment 2-11
VTAM APPN Node Types 2-12
Interchange Node 2-12
Migration Data Host 2-12
End Node or Network Node 2-12
Virtual Route Transmission Group 2-12
Migrating the Data Center to APPN 2-13
Migrating the Network to APPN/DLUR and the Channel-Attached Router 2-14

Role of APPN in the Parallel Sysplex Environment 2-16

Designing for High Availability 2-17
SNA Communication Using CSNA 2-17
Use of Duplicate Addresses for High Availability 2-18

Migration and Coexistence 2-21

Chapter 3 Migration Scenarios 3-1

SNA Communication over CSNA 3-1

VTAM Definitions 3-2
External Communication Adapter Major Node Definition 3-2
Switched Major Node Definition 3-2

Router Configuration 3-3
Configuration Relationships in the ESCON Environment 3-4
Configuration Relationships in the Bus and Tag Environment 3-5

Scenario 1: Single CIP to Single Host 3-5
Reasons for Change 3-6
Design Choices 3-6
Configuration 3-7
Implementation Overview 3-7

Scenario 2: Redundant CIP to Single Host 3-7
Reasons for Change 3-9
Design Choices 3-9
Router Configuration 3-10

Scenario 3: Single CIP to Multiple Host 3-10
Reasons for Change 3-11
Design Choices 3-11
Router Configuration 3-12

Scenario 4: Migrating to APPN 3-13
Reasons for Change 3-13
Design Choices 3-13
Router Configuration 3-14
4700 Router Configuration 3-14

APPN in a Parallel Sysplex Environment 3-14

Scenario 5: Migrating from SNI to APPN 3-15
Reasons for Change 3-16
Design Choices 3-17
Router Configuration 3-17

Chapter 4 Network Management 4-1

CiscoWorks Blue 4-1
CiscoWorks Blue Native Service Point 4-1
CiscoWorks Blue Maps and SNA View 4-3
Internetwork Performance Monitor 4-4

Management Comparison: Channel-Attached Router and CIP/3745 and NCP 4-5
Alerts 4-5
Statistics 4-6
Statistics Summary 4-7
Console Support 4-8
Trace/Debug 4-9
Connectivity Test 4-11
Memory Display/Dump 4-11
Recovery 4-12
Performance Monitoring 4-12
Configuration Management 4-13

Router Configuration for Host Management 4-14
XCA Major Node 4-14
Switched Major Node Definition 4-14
Router Configuration (Partial) 4-14

Figure I Simple SNA Network xiv
Figure II Evolution of IBM Networks xv
Figure III Data Center Design and Implementation Road Map xvi
Figure 1-1 SNA Network Components 1-3
Figure 1-2 Sample APPN Network and Associated Directory and Topology Databases 1-4
Figure 1-3 High-Performance Routing 1-5
Figure 1-4 SNA Device Connectivity 1-7
Figure 1-5 Connecting Local Resources to the CIP 1-8
Figure 1-6 Connecting Remote, Router-Attached Resources to the CIP 1-8
Figure 1-7 Connecting Remote SNA Devices over SDLC, X.25, or Frame Relay 1-9
Figure 2-1 APPN Intermediate Session Routing (ISR) Throughput 2-3
Figure 2-2 Alternatives for Functionality Placement 2-4
Figure 2-3 Impact on a 9121-982 Mainframe of Migrating from a FEP to a CIP 2-7
Figure 2-4 Session Establishment for Dependent LUs Using Subarea SNA 2-9
Figure 2-5 Session Establishment for Dependent LUs Using APPN DLUS/DLUR 2-10
Figure 2-6 SSCP Takeover Using APPN DLUS/DLUR 2-11
Figure 2-7 Migrating the Network: The Before Picture 2-15
Figure 2-8 Migrating the Network: The After Picture 2-16
Figure 2-9 Explorer Processing on a Source-Route Bridged LAN 2-18
Figure 2-10 Using Duplicate MAC Addresses with CIPs 2-19
Figure 2-11 Load Balancing Using Duplicate MAC Addresses and SRB 2-20
Figure 2-12 Load Balancing Using Duplicate MAC Addresses and DLSw+ 2-21
Figure 2-13 Migration from a FEP to a CIP 2-22
Figure 3-1 Communication between CSNA in the CIP and SNA Nodes 3-1
Figure 3-2 Using Virtual Rings to Provide Connectivity 3-3
Figure 3-3 Relationship among MVS, VTAM, and Router Configurations: ESCON 3-4
Figure 3-4 Relationship among MVS, VTAM, and Router Configurations: Bus and Tag 3-5
Figure 3-5 Single CIP to Single Host 3-6
Figure 3-6 Redundant CIPs to Single Host 3-8
Figure 3-7 Dual Routers with Duplicate MACs 3-9
Figure 3-8 Replacing a Single FEP with a Channel-Attached Router 3-11
Figure 3-9 Dual CIPs in a Single Router 3-12
Figure 3-10 APPN Scenario 3-13
Figure 3-11 Parallel Sysplex Environment 3-15

Figure 3-12 SNI Scenario 3-16
Figure 4-1 Native Service Point Main Screen 4-2
Figure 4-2 SNA View Dependency Screen 4-4
Figure 4-3 NetView Alert Screen 4-6
Figure 4-4 Statistics Record for an NCP-Managed Resource 4-7
Figure 4-5 Native Service Point Interface Statistics 4-8
Figure 4-6 Native Service Point Router CPU/Memory Utilization 4-13

LIST OF TABLES

Table 2-1 Campus Options 2-6

Table 4-1 Alerts 4-5

Table 4-2 Statistics Summary 4-7

Table 4-3 Console Support 4-8

Table 4-4 Trace/Debug 4-9

Table 4-5 Cisco IOS Software Debug Facilities 4-9

Introduction

This document describes how you can use the Cisco Systems Channel Interface Processor (CIP) in conjunction with the IBM services of the Cisco IOS™ software to:

- Address mainframe requirements
- Protect your investment in your mainframe and mainframe applications
- Allow you to run your business more efficiently

The document covers several CIP solutions, describes when to use them, how to configure them, offers network design and tuning suggestions, and provides performance results.

Intended Readers

This document is intended for anyone who wants to learn more about Cisco's data center solutions. It begins with an overview appropriate for all audiences. It also includes design guidelines and sample configurations appropriate for network designers, systems engineers, consulting engineers, and network support. The document assumes familiarity with networking and Cisco routers, but does not assume mastery of either.

Examples of key configuration commands are shown to aid in understanding a particular configuration. However, this document does not contain the exact and complete configurations. This information is available and regularly updated in Cisco Connection Online (CCO) and in the Cisco guides. CCO is Cisco's main real-time support system. Its World Wide Web address is http://www.cisco.com.

Cisco's Data Center Solutions

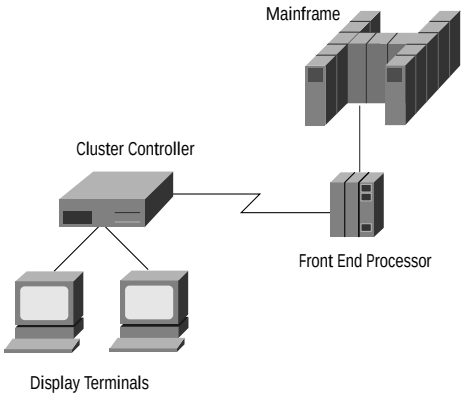
For the last 20 years, businesses have come to depend on mainframe applications. A trillion dollars have been spent on mainframe application code, and those applications will not simply disappear tomorrow. In addition, a great deal of work has gone into mainframe security, backup, and redundancy, making the mainframe an excellent server for the networks of tomorrow. For these reasons and others, mainframes will play a major role in networks for years to come. This reference guide describes how to use Cisco solutions to tightly integrate your mainframes with the rest of your network as your network evolves to support higher bandwidth and Internet and intranet access.

Evolution of the Data Center

In the early 1970s, computing cycles and memory were very expensive. Most enterprises centralized their computing cycles in large mainframe computers. These mainframe computers resided in a data center—often called a "glass house." End users accessed mainframe applications from teletype

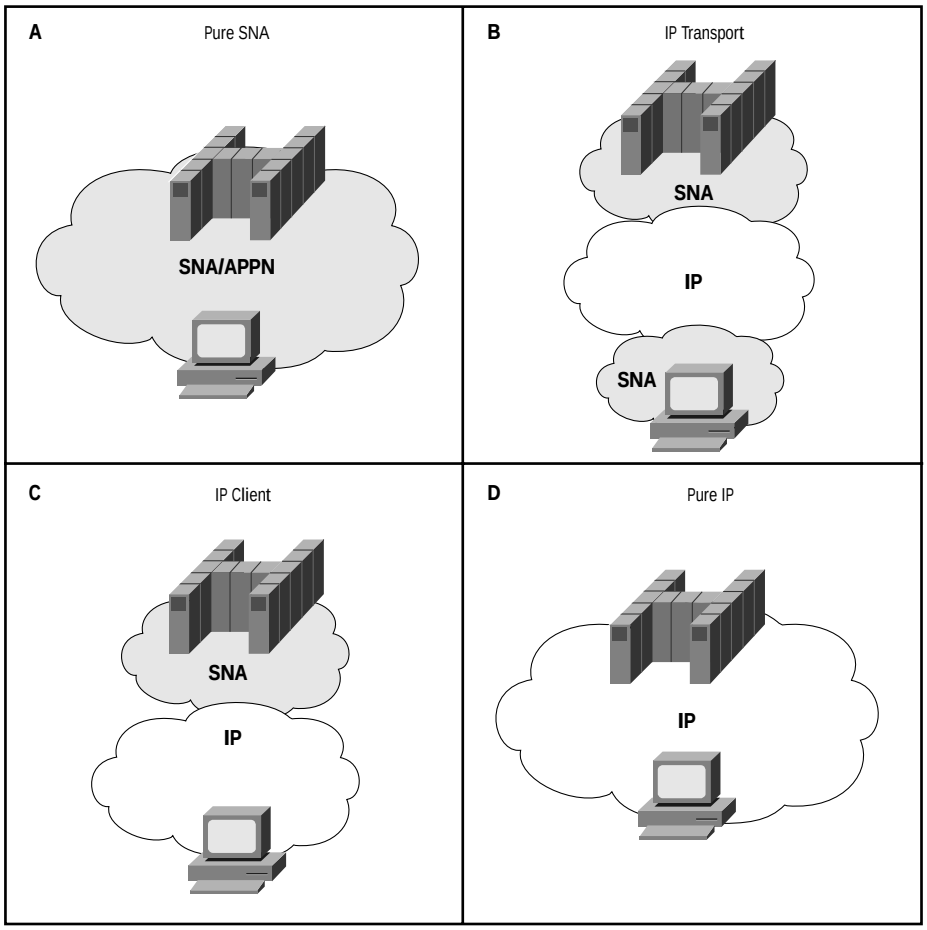
machines or display terminals (known as 3270 devices). IBM developed Systems Network Architecture (SNA) to define how display terminals could access applications and information in IBM mainframes. Figure I shows a simple SNA network and some of the key components.

Figure I Simple SNA Network



Today, computing cycles are so inexpensive, most desktop computers have more processing power than the mainframes of the 1970s. Processing power is spread around enterprises, not only on the desktop, but also in powerful workgroup computers. IBM mainframes are still used to support SNA applications, but access to those applications can either be from 3270 display terminals, PCs running 3270 emulation programs, PCs running more advanced SNA protocols, or Transmission Control Protocol/Internet Protocol (TCP/IP) end systems that transport key strokes using a protocol known as TN3270. IBM mainframes are also being used for more than just SNA applications. More than 40 percent of the mainframes worldwide also run TCP/IP, and that number is expected to grow to 85 percent by the year 2000. Figure II shows the four paradigms of IBM mainframe access.

Figure II Evolution of IBM Networks



Many IBM networks today still access SNA applications in the mainframe from SNA clients (shown in quadrant A). However, more than 40 percent have migrated their backbone to TCP/IP (shown in quadrant B). From a data center perspective, these two scenarios are the same. These scenarios are covered in Part 1, "SNA Internetworking."

With the proliferation of Internet connections and the fact that TCP/IP is included for free with Windows 95, more and more organizations are looking at TN3270 as a low-cost means to access some of their SNA applications. TN3270 eliminates the requirement for dual stacks on the desktop and minimizes the cost of specialized desktop software.

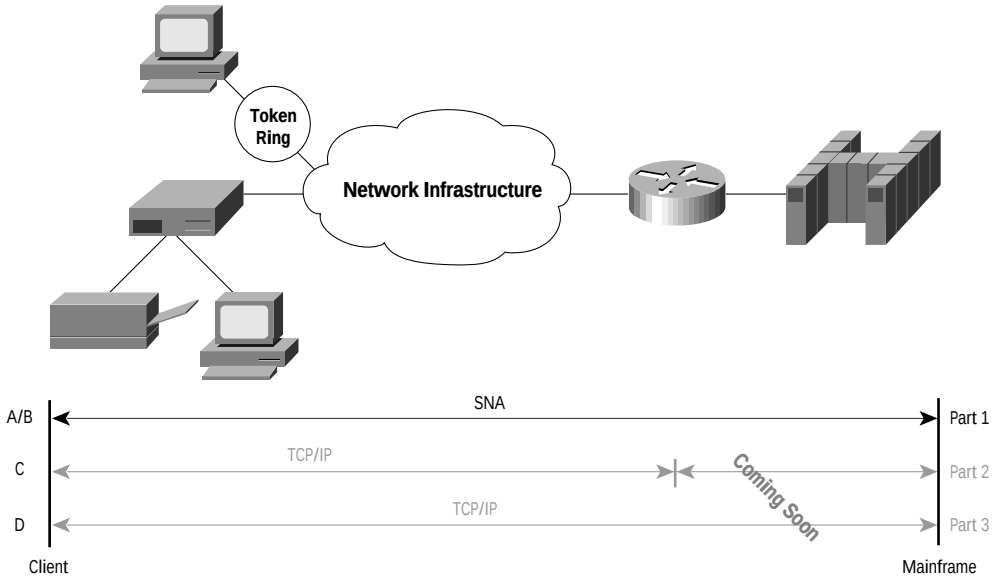
Another alternative, provided by the Cisco WebAccess for S/390 family, is to use a specialized Web server to download Java applets to clients. The Java applet provides access to a typical 3270-like interface or, optionally, a web-browser interface. No specialized software is required at the desktop, and the Web server automatically downloads the most current Java applet, eliminating the cost of purchasing and maintaining specialized desktop software. Web browsers offer an intuitive interface well understood by customers, suppliers, and employees. The Web server maintains a permanent and secure TN3270 connection to either a TN3270 server in a Cisco router or a TN3270 server running in an IBM mainframe.

Both of these options are similar. SNA is isolated to the data center, and the desktop has TCP/IP only. This scenario, shown in quadrant C, will be covered in Part 2, "Accessing SNA Applications from IP Clients."

Finally, some environments are either building new mainframe applications using TCP/IP, or rewriting existing applications to use TCP/IP. This scenario, shown in quadrant D, is covered in Part 3, " Mainframe TCP/IP."

Figure III is a road map that describes the content of each of the current and planned parts of this guide and their relationship to the four quadrants described in Figure II.

Figure III ***Data Center Design and Implementation*** **Road Map**



PART 1

SNA Internetworking

CHAPTER 1

Introduction to SNA on the CIP

More than 90 percent of Fortune 1000 companies still base their mission-critical applications on SNA. In addition, there are more than 750,000 SNA gateways and controllers currently installed and providing end users with access to SNA applications. Support for end-to-end SNA networks is a critical requirement of the CIP. This chapter will help you understand what features the CIP offers in this environment, when and where you can use the CIP and IBM services of Cisco IOS software, and how to best design your data center for optimal performance and availability.

This chapter includes:

- An overview of SNA for readers more familiar with Cisco routers and less familiar with SNA networking
- A description of how a channel-attached router connects to an SNA mainframe
- A comparison of the SNA support available in a channel-attached router with the support in other SNA channel gateways
- A description of when to consider the Cisco CIP as an SNA solution and what benefits it provides

This chapter is recommended for all readers.

SNA Overview

To understand the CIP SNA support, it is useful to have a basic understanding of SNA. SNA was invented in 1974 to architect a standard way for accessing applications on IBM mainframes. SNA has evolved over the years and looks quite different today from when it was first invented. However, many networks still run the original architecture, so it is important to understand all flavors of SNA: subarea SNA, Advanced Peer-to-Peer Networking (APPN), and high-performance routing (HPR).

Subarea SNA Overview

The original SNA architecture was hierarchical, with the applications and network control software residing on IBM mainframes. It was called subarea networking because the network was divided up into logical groupings named subareas to facilitate routing and directory functions.

The mainframe software that controls SNA subarea networks is known as virtual telecommunications access method (VTAM). VTAM contains a control point (known as a system services control point or SSCP) that establishes a control session with “dependent” SNA devices in its span of control (known as its domain). VTAM is responsible for several SNA control functions:

- Activating and deactivating SNA devices, similar to a “logical power-on” of the device
- Providing directory functions for SNA devices—finding the correct mainframe that houses an application

- Assisting in session establishment, similar to a telephone operator for SNA communication
- Routing SNA—routing traffic towards the destination SNA application
- Receiving alerts of events—receiving notification of what's happening in the network

In general, all devices within the domain of control of VTAM must be configured to that VTAM, although later VTAM releases allow resources to be dynamically associated with generic definitions. VTAM can dynamically find resources that are "owned" by another VTAM. These resources are known as cross-domain resources.

SNA uses the term physical unit (PU) to denote network processors that can participate in SNA networks. The term PU is followed by a number (1, 2, 2.1, 4, or 5). The number indicates the specific SNA functionality each PU type provides. VTAM implements physical unit type 5 (PU 5) functionality in SNA.

To off-load mainframe processing, IBM developed front-end processors (FEPs) that run the Network Control Program (NCP). These devices communicate to the mainframe over communication channels. The NCP handles SNA routing (routing SNA traffic to the correct mainframe that houses the destination application). Subarea routes must be statically configured in an NCP, but VTAM dynamically selects the first route matching the Class Of Service (COS) and destination subarea number. The NCP also prioritizes traffic on its outbound queues based on the transmission priority assigned to a particular SNA session. Finally, the NCP provides boundary function to allow devices on the "boundary" of the SNA network—for example, cluster controllers—to access mainframes. The NCP implements PU 4 functionality.

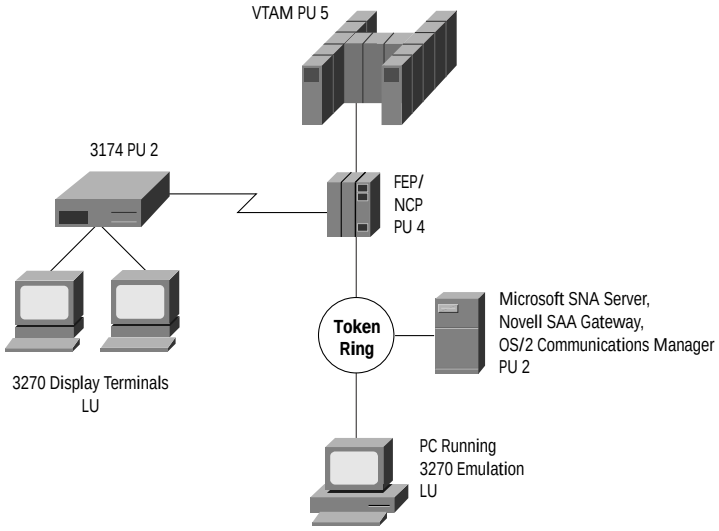
Cluster controllers (such as 3174s) provide access to SNA networks from display terminals or terminal emulators. Cluster controllers access the SNA network through an SNA boundary node (such as the NCP or VTAM), but they do not provide SNA routing or COS functions. They are sometimes called peripheral devices, since they sit on the periphery of an SNA network and do not fully participate in all the SNA functionality. Cluster controllers provide PU 2 functionality.

Display terminals (known as 3270 terminals) provide a means for end users to request application services. End users enter key strokes which are sent to the cluster controller. The cluster controller puts the key strokes in an SNA request unit (RU) with a boundary (peripheral) format-identifier 2 (FID2) header, and forwards the RU to an NCP. The NCP converts the header from a FID2 to a FID4 (converting local addresses to subarea addresses and adding the transmission priority field) and forwards it on to the next hop in the SNA network. Eventually the packet reaches an SNA mainframe application where the request is processed and the results are returned to the display terminal. (Because application processing is performed on the mainframe, every end user request and its associated response must traverse the network before the response is displayed to the end user. That is why availability and predictable response time are so key in the SNA world.) Applications, printers, and 3270 terminals or emulators are known as logical units (LUs). In particular, 3270 terminals or emulators generally appear as an LU 2 to VTAM.

There are several other LU types in subarea SNA. LU 0 applications use an unstructured data field to enable advanced functions. Advanced Program-to-Program Communications (APPC) applications communicate using LU 6.2, which is an architectured protocol for communication between two applications. Unlike display terminals, PCs can run applications and hence communicate program to program with a mainframe application, rather than simply asking a mainframe application to process a request. Printers generally appear as LU 1 or LU 3.

Personal computers also support 3270 emulation to allow them to communicate with existing 3270 mainframe applications. PC gateways such as Microsoft SNA Server, Novell SAA gateways, and OS/2 Communication Manager provide the PU 2 function previously provided by cluster controllers. Some client software implements both PU and LU functionality. Figure 1-1 shows the components of a subarea network.

Figure 1-1 SNA Network Components



One other concept worth mentioning is the concept of a Communication Management Configuration (CMC) environment, which is an environment where a single VTAM (the CMC host) owns all the SNA resources in a network and is involved in every session initiation and termination. All the other mainframes provide SNA application support only. This design keeps the network processing off of the application hosts and simplifies collection of management data.

APPN Overview

APPN was developed in 1985 to address some of the shortcomings of subarea APPN. APPN is much easier to understand and configure than subarea SNA, provides dynamic routing and dynamic directory capabilities, and extends SNA COS farther out in the network.

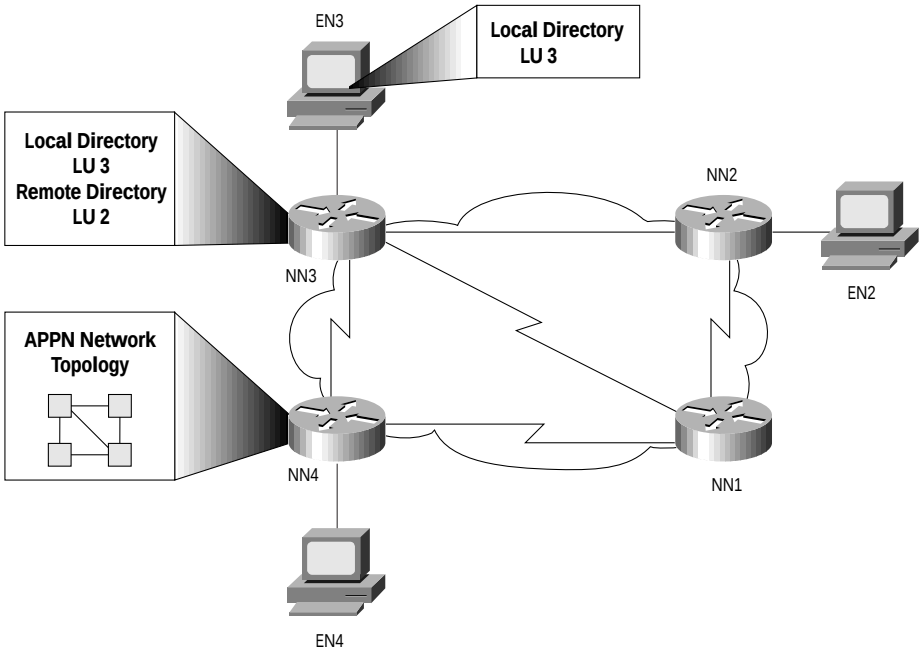
APPN is not a hierarchical network architecture but a peer architecture. There are three types of nodes in APPN: low entry networking (LEN) nodes, end nodes (ENs), and network nodes (NNs). These resources can communicate with each other without the assistance or involvement of mainframe VTAM. Instead of having a single control point in the mainframe, every EN and NN has its own control point and controls its local resources (applications and links). LEN nodes implement a rudimentary subset of function and require substantial configuration. They will not be discussed again. Figure 1-2 illustrates an APPN network.

APPN ENs provide local directory services and communicate with their NN server to access other resources in the network. APPN ENs can dynamically register their resources with their NN server.

NNs are SNA routers. NNs dynamically build routing tables using a link state protocol similar to Open Shortest Path First (OSPF) in TCP/IP. Only NNs appear in the network topology database, not ENs. In first-generation APPN, NNs forward SNA session traffic using intermediate session routing (ISR). ISR uses a connection-oriented data link control, which provides hop by hop error

correction and retransmission, so it is fairly processor intensive (this is equivalent to running a full TCP stack in every hop along the path). Also, APPN ISR does not support nondisruptive rerouting around link failures.

Figure 1-2 Sample APPN Network and Associated Directory and Topology Databases



NNs provide directory function for ENs. If an EN cannot find a resource locally, it sends a request to its NN server. The NN server searches its local directory, and if it doesn't find the resource, it does one of two things. If a Central Directory Server (CDS) is present, it sends the query to the CDS. If one is not present, it generates a LOCATE request and sends it (in a broadcast fashion) to all other NNs in the network. Currently, only VTAM implements a CDS.

APPN supports SNA COS all the way to the APPN end system, unlike subarea networks where COS applies only between FEPs and mainframes.

Because APPN is more dynamic and has so much more function, one might expect it to have quickly overtaken subarea networks. It hasn't for two key reasons. First, subarea SNA devices did not immediately support the new SNA. VTAM did not support APPN until Release 4.1. Until release 7.4, the NCP could participate in APPN only when combined with VTAM as a composite network node (CNN). Second, and even more important, when APPN was first invented, it only supported APPC applications. Most mainframe applications were dependent LU applications (3270 or LU 0 applications). This problem was addressed in VTAM 4.2 with a feature known as dependent logical unit server (DLUS), which will be discussed later.

APPN as a backbone protocol has not seen the acceptance one might expect, mainly as a result of IBM's delay in making APPN available and usable for subarea networks. However, many enterprises are considering APPN in the data center.

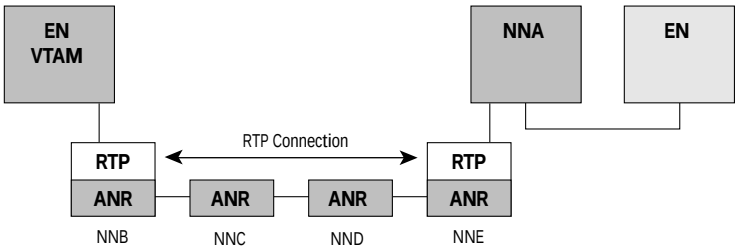
HPR Overview

HPR is the newest generation of SNA and an extension of APPN. It is designed to address two key limitations of APPN.

- First of all, HPR, unlike all previous versions of SNA, is able to reroute around path failures without disrupting end-user sessions.
- In addition, HPR incurs minimal processing overhead in intermediate routers when compared to APPN ISR.

HPR has two components. One component, known as Rapid Transport Protocol (RTP), provides reliable delivery similar to TCP (packet retransmission and error recovery). The other component, automatic network routing (ANR), provides fast packet forwarding similar to IP. Similar to how TCP/IP works, you only need two RTP nodes, and the RTP endpoints provide reliable transport of data between them. Intermediate nodes only need to implement ANR. This allows intermediate HPR nodes, that is, ANR nodes, to process much higher numbers of transactions. APPN ISR nodes (such as NNA in Figure 1-3) can coexist with APPN HPR nodes. Nondisruptive rerouting only occurs between the RTP endpoints (NNB and NNE in Figure 1-3). Reduced processing only occurs in ANR nodes (NNC and NND in Figure 1-3). RTP endpoints have the same amount or more processing than ISR nodes.

Figure 1-3 High-Performance Routing



High availability and high performance are critical in the data center, and hence, HPR is a key SNA protocol in the data center.

Cisco SNA Support with a Channel-Attached Router

The Cisco 7000 or 7500 router equipped with one or more CIPs provides mainframe channel connectivity. The Cisco SNA feature of the CIP provides channel connectivity directly to VTAM.

SNA Channel Protocols Supported by the CIP

The Cisco SNA software feature offers two ways to communicate over the channel: **csna** and **cmpc**. When using the **csna** command, the CIP appears to VTAM as an eXternal Communications Adapter (XCA). When using the **cmpc** command, Cisco communicates to VTAM using MultiPath Channel (MPC). Support for MPC will be available in Cisco IOS Release 11.3.

XCA Overview

XCA is used by the Cisco CIP and the IBM 3172. It allows one subchannel to support thousands of SNA PUs. This protocol is used primarily for VTAM to VTAM, VTAM to PU 2, and APPN ISR traffic. HPR is not supported by VTAM using XCA.

XCA uses a single half-duplex subchannel to communicate with VTAM.

MPC Overview

MPC is used for VTAM to VTAM, VTAM to APPN/ISR, and VTAM to HPR communication. It is supported by the 3172 and will be supported by the CIP in Cisco IOS Release 11.3. It is a stated direction for the 3746-950. It requires at least two subchannels for each adjacent SNA PU.

Cisco's MPC implementation supports one read channel and one write subchannel per adjacent SNA PU. It provides more efficient channel utilization and better mainframe utilization when compared to XCA or CDLC, which is used by the 3745. However, MPC may require more configuration than XCA. That is because MPC supports only one adjacent PU over a pair of subchannels whereas XCA supports thousands of PUs over a single subchannel. When implementing MPC, you may want to design your network to minimize the number of adjacent SNA PUs and hence the required definitions.

SNA Appearance of the Channel-Attached Router

Using the **csna** command, the CIP does not have an SNA PU appearance. It appears to VTAM as one or more XCA major nodes. (One XCA major node is required for each internal LAN adapter configured with the **csna** command.) A single CIP can support 6000 SNA PUs. Multiple CIP cards can run in a single router, providing mainframe access for tens of thousands of SNA PUs and LUs. In addition, using an ESCON director, the CIP can attach up to 64 channel-attached mainframes.

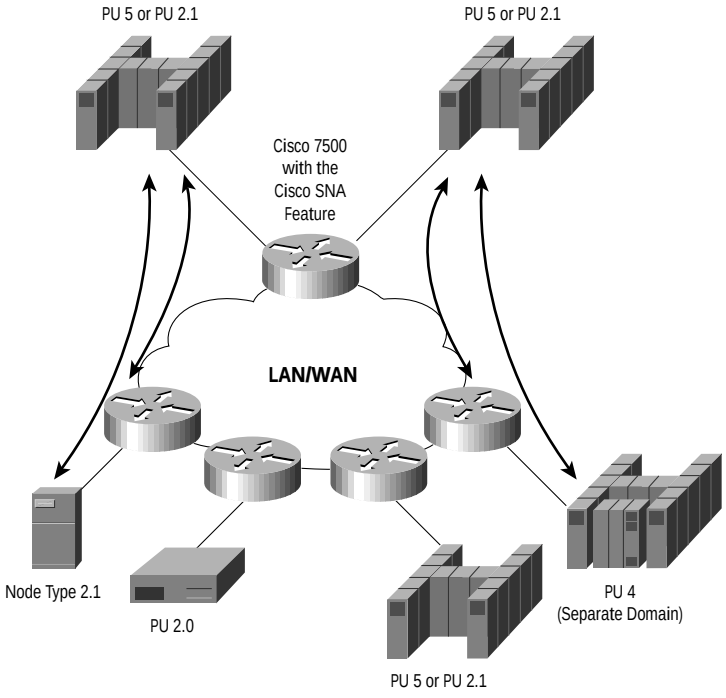
While the CIP may not have an SNA appearance, the router can. The router appears like an SNA PU 2.0 when configured with downstream PU (DSPU) concentration or the service point function, which allows the router to be managed from IBM's NetView or Sterling's SOLVE:Netmaster. The router provides APPN NN functionality when running the APPN feature.

In networks with multiple mainframes or VTAMs, SNA routing may be required. Just as a FEP offloads VTAM with subarea routing, the Cisco IOS software offloads VTAM with APPN routing. APPN can determine the correct mainframe or LPAR for SNA session traffic. APPN can be installed anywhere in the network—it does not have to be running in the channel-attached router. Alternatively, this routing can be done by VTAM.

SNA Device Connectivity

The Cisco channel-attached router provides connectivity between many diverse SNA devices, as shown in Figure 1-4. Using a Cisco 7000 or 7500 router with a CIP and the Cisco SNA feature installed, you can connect two mainframes together (either locally or remotely), connect a mainframe to a PU 2.0/1 device, or connect a mainframe to a FEP in another VTAM domain. (VTAM does not support FEP ownership through an XCA device, so the remote FEP must be activated through a local NCP.)

Figure 1-4 SNA Device Connectivity

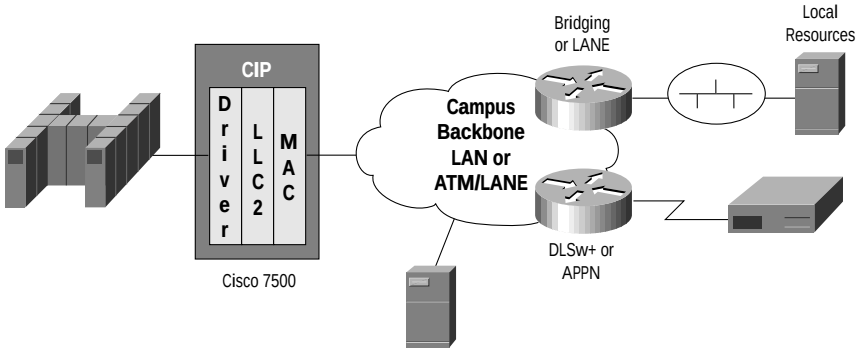


Connectivity Options

Many options are available for connecting SNA devices (PU 2.0s or PU 2.1s) to a CIP-attached router, as illustrated in Figure 1-5, Figure 1-6, and Figure 1-7. As shown in these figures, access to the CIP is always via Logical Link Control, type 2 (LLC2) and an internal virtual Token Ring, regardless of the media the end system is using. SNA functions such as Data Link Switching Plus (DLSw+) or APPN can reside in the channel-attached router or in a central campus router that is bridged to the channel-attached router.

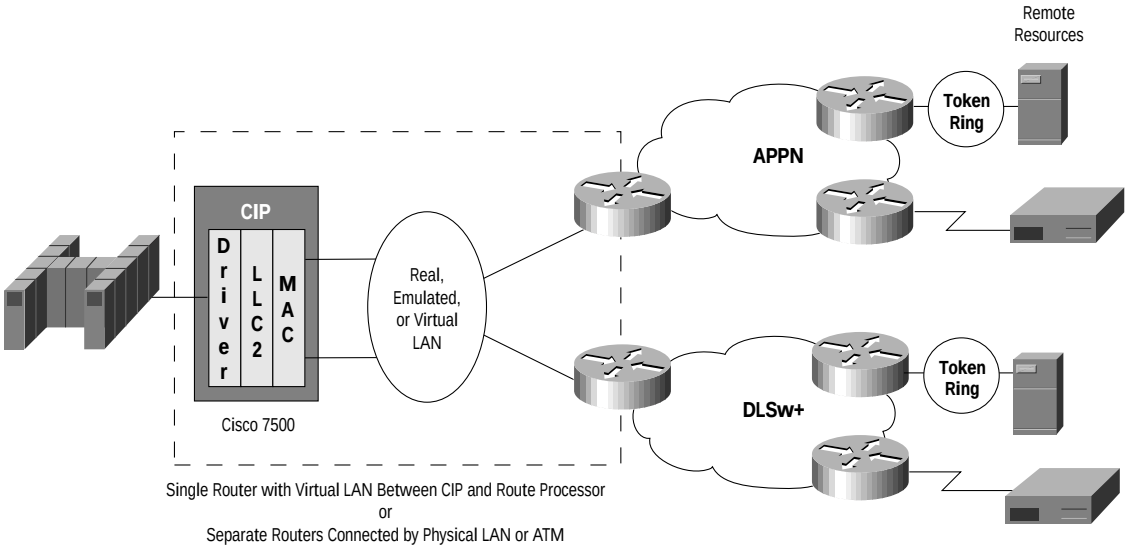
- Local LAN-attached resources or campus resources connected to an Asynchronous Transfer Mode (ATM) LAN Emulation (LANE) backbone can simply bridge into the CIP-attached router. Local SDLC devices can attach directly to a Cisco router and use either DLSw+ local switching or APPN to access the CIP via LLC2. (APPN or DLSw+ can be running in the CIP router or in another router that is bridged to the CIP router.) This is shown in Figure 1-5.

Figure 1-5 Connecting Local Resources to the CIP



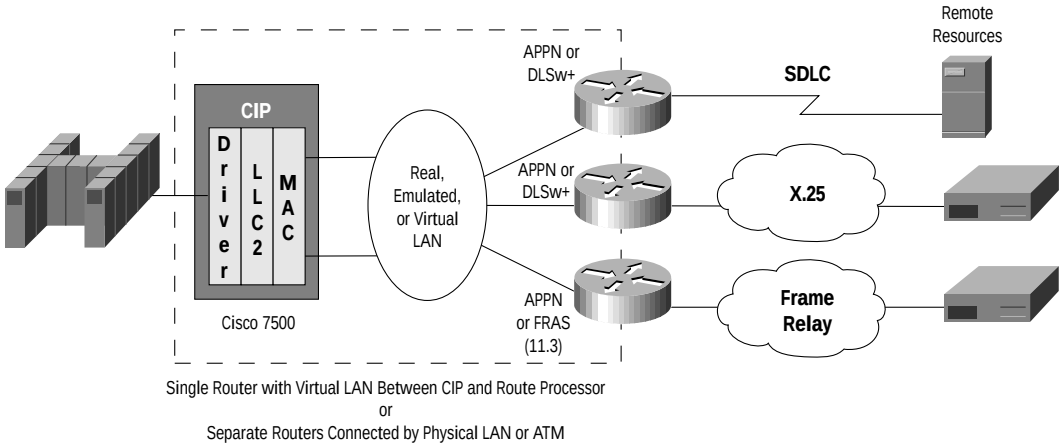
- Remote SNA devices can attach to remote Cisco routers and use any of Cisco's SNA transport technologies—DLSw+, APPN, Frame Relay Access Services (FRAS), or Remote Source Route Bridging (RSRB)—to access central site routers. These transport technologies can be running in the CIP router or in another router that is bridged to the CIP router, as shown in Figure 1-6.

Figure 1-6 Connecting Remote, Router-Attached Resources to the CIP



- SNA devices that use Qualified Logical Link Control (QLLC) to communicate over X.25 can connect to a Cisco router using QLLC. Again, either DLSw+ local switching or APPN can then be used to access the CIP via LLC2. (APPN or DLSw+ can be running in the CIP router or in another router that is bridged to the CIP router.) SNA devices can communicate directly to a central site Cisco router using RFC1490 encapsulation of LLC2. (Prior to Cisco IOS Release 11.3, this required the APPN feature set at the central site router. With Cisco IOS Release 11.3, this capability is provided with the FRAS Host feature.) This is shown in Figure 1-7.

Figure 1-7 Connecting Remote SNA Devices over SDLC, X.25, or Frame Relay



Comparison of the CIP to Other Options

The key options in use today to attach to an IBM mainframe are the 3745, 3174, 3172, Open Systems Adapter (OSA), and of course a Cisco router with a CIP. A Cisco router can be a direct replacement for a 3174, 3172, or OSA without any loss of function—simply better performance and availability. In many cases, a Cisco router can also be used as a higher-performance, lower-cost alternative to a FEP. However, for some functions, FEPs will still be required. This section describes the functions provided by an IBM FEP for SNA and describes which functions a channel-attached Cisco router can provide.

Front-End Processors—IBM 3745

IBM's primary solution for mainframe access has historically been the FEP. FEPs offer a great deal of functionality for subarea networks and legacy protocols. However, much of the functionality is only used in the largest SNA networks. Most small networks use only a subset of the functionality in a FEP. In addition, networks are changing rapidly, and the typical enterprise network now supports a multitude of protocols, LANs, WANs, and device types. Low-speed serial lines are being replaced with high-performance substitutes like LANs, high-speed serial lines, and Frame Relay. FEPs have not kept up with the requirements of today's enterprise networks. Other networking gear is needed to either augment or replace FEPs. If you are considering replacing some or all of your FEPs, first know what functions your FEP is providing today to ensure that you do not lose function as you move forward. The key FEP functions and their role in today's networks is described in the following:

- SNA Session Routing—Required in environments with multiple data centers or ACF/VTAM application hosts and a high volume of cross-domain SNA traffic. Routing may also be important in environments with distributed AS/400s.
- SNA COS—Allows prioritization of SNA traffic between FEPs and mainframes and is important in environments with SNA backbones. COS is of less significance in environments that have consolidated all their FEPs in the data center: in this case, there either is no FEP-to-FEP traffic, or the FEPs are connected at the data center over high-speed LANs that do not have bandwidth contention problems. However, some networks take advantage of Link Services Prioritization (LSPRI), which provides transmission priority based on COS for outbound traffic (for example, FEP to cluster controller).

- Serial Line Concentration—FEPs have long been used to concentrate large numbers of low-speed (9.6-kbps) lines. However, as backbone networks migrate to high-speed WAN backbones, the need for high-density, low-speed serial connectivity decreases.
- Switched Synchronous Data Link Control (SDLC)—Some enterprises rely on switched SDLC to support transient SNA connections to small branch offices or to provide switched network backup. As SDLC is being replaced by multiprotocol data links, switched SDLC requirements are diminishing. In place of SDLC, protocols such as Integrated Services Digital Network (ISDN), Point-to Point Protocol (PPP), and Serial Line Interface Protocol (SLIP) are being used to provide multiprotocol or IP-switched line support.
- SNA Boundary Function—FEPs provide a SNA boundary network node (BNN) function, which includes polling, conversion from local addresses to SNA addresses, and exchange identification (XID) conversion. In the absence of remote FEPs, this function is performed by local FEPs. In the absence of any FEPs, most of this function is performed by ACF/VTAM.
- SNA Network Interconnect—Many enterprises use FEPs for SNA Network Interconnection (SNI) to allow independent SNA networks to communicate. There are other alternatives— APPN border node function and electronic data exchange over the Internet—but any change on one side requires a change on the other side. Hence, this migration will be a slow one.
- SSCP Takeover—With this facility, if an owning VTAM goes down, another VTAM can assume ownership of those resources without disrupting any existing application sessions. The NCP plays a role in allowing this takeover.
- eXtended Routing Facility (XRF)—A program product that allows one VTAM application to take over for another. The XRF code in the NCP plays a key role in supporting this capability.
- X.25 Support—X.25 Interconnection (XID) allows the NCP to act as an X.25 packet switch. NCP Packet Switched Interface (NPSI) allows the NCP to connect to other resources over X.25 networks. It supports both SNA and non-SNA devices. For non-SNA (asynchronous and Binary Synchronous Communications Protocol) devices, it supports conversion to SNA.
- Specialized Program Products that Support Custom or Older Applications—Network Routing Facility (NRF) provides routing inside of the NCP without VTAM participation. Emulator Program (EP) allows the 3745 to connect to basic telecommunications access method (BTAM) in an IBM mainframe.
- Legacy Protocols—Program products, such as Non-SNA Interconnect (NSI) for Bisynch conversion, Airline Line Control Interconnection (ALCI) for airline line control protocol transport, and Network Terminal Option (NTO) for async conversion. These products can be installed in the FEP to handle non-SNA protocols. They are older protocols that are declining in usage.

The Cisco Channel-Attached Router as a FEP Alternative

The Cisco router/CIP combination focuses on the key features that most IBM customers use, such as mainframe channel attachment for both SNA and TCP, SNA routing, SNA COS, and access to SDLC- and LAN-attached resources.

Looking at the key FEP functions identified in the previous section, the Cisco IOS software and the CIP offer a means to address most of the key FEP functions while providing a higher performing, multipurpose channel gateway. For functions not addressed by the CIP, one or more FEPs may still be required.

- SNA Session Routing—The Cisco IOS software supports native APPN routing and, with Dependent LU Requestor (DLUR), can also support native SNA routing for legacy 3270 traffic in an APPN network. APPN is a logical progression from subarea SNA in many environments.

APPN is required to take full advantage of high-availability options in Parallel Sysplex environments and it is more dynamic (and hence less labor-intensive to maintain) than a subarea network.

- COS—This APPN feature also provides SNA COS for both APPC and legacy 3270 traffic in an APPN network. If Cisco's APPN feature is installed only in central site routers, it provides outbound prioritization based on COS, similar to LSPRI in the FEP. In a multiprotocol environment, Cisco's custom queuing feature reserves bandwidth for SNA traffic. DLSw+ supports LU and service access point (SAP) prioritization. Finally, in Cisco IOS Release 11.3, COS can be mapped to TCP type of service (ToS) to preserve SNA prioritization when transporting SNA over an IP backbone. (This mapping requires that both APPN and DLSw+ are running in the router.)
- Serial Line Concentration—The Cisco 4700 supports up to 54 serial lines, or 36 serial lines plus one LAN. The 7200 supports 48 serial and 1 LAN, which can be Fast Ethernet. Either of these are good solutions for low-speed SDLC serial line concentration. The MultiChannel Interface Processor (MIP) card is the best solution for high-speed serial concentration when the remote branches have routers and connect over 56- or 64-kbps lines or ISDN Basic Rate Interface (BRI). The Cisco 7500 MIP card supports 2 channelized T1/E1s or 2 primary rate ISDN lines, supporting up to 48 56-kbps or 64-kbps remote sites per card. Multiple MIP cards can be installed in a Cisco 7500. If your current network is pure SNA, your FEPs connect 200 or more low-speed (19.2 kbps or below) serial lines, the branches are too small to justify a router, and packet-switched services such as X.25 or Frame Relay are not an option, the FEP may still be the most cost-effective solution.
- Switched SDLC—The Cisco IOS software transports multiprotocol traffic, including SNA, over switched services. It does not, however, support dial-out to switched SDLC devices. (Dial-in requires that you code **sdlc role prim-xid-poll** on the appropriate serial interface).
- SNA Boundary Functions—The Cisco IOS software can reduce mainframe cycles by providing several boundary functions such as remote polling, group poll support, and DSPU concentration. Using APPN and DLUR, Cisco routers can provide many functions provided by a FEP.
- Autonomous Network Connection—SNI connections require a FEP in at least one of the connecting networks. The Cisco IOS software allows connection to an SNI gateway but does not provide SNI gateway functionality:
  - If the inter-enterprise connection uses back-to-back SNI gateways, then at least one FEP is required in each independent SNA network.
  - If the inter-enterprise connection can be an adjacent SNI configuration, one network can keep a FEP to provide the SNI gateway function, and the attaching network can replace FEPs with CIPs. The downside to this alternative is that certain topology changes in one network (for example, adding a new subarea node) may require changes in the other network.
  - Another alternative is to use an APPN border node connection between the networks. This alternative requires that APPN be implemented in both data centers, but it also allows either side to eliminate its FEP requirement.
  - If both sides cannot migrate to APPN, one network can implement an interchange node and connect in that manner to the NCP in the other network. This requires keeping at least one FEP for the SNI connection.
  - Casual connection could also be used, allowing one network to eliminate a FEP. This connection supports primary LU (application) initiated sessions only.
- SSCP Takeover—This facility is fully supported by the APPN DLUR feature of the Cisco IOS software.
- XRF—This product requires an NCP. There is no channel-attached router equivalent.

- X.25 Support—Cisco IOS software can be configured as an X.25 packet switch, and it supports transport of SNA over an X.25 backbone. There is no comparable function to provide asynch or Bisynch conversion to SNA, however. (The CIP does support the TN3270 server, which provides conversion from TN3270 to SNA.)
- Specialized Program Products that Support Custom or Older Applications—There is no function comparable to NRF in the Cisco IOS software. There is no feature comparable to EP in the Cisco IOS software.
- Legacy Protocols—While the Cisco IOS software can duplicate some special protocols supported by the FEP, such as asynchronous and Bisynch tunneling, comparable protocol support (that is, conversion to SNA) is not provided. (The CIP does support TN3270 Server, which provides conversion from TN3270 to SNA.)

Benefits of a Cisco 7000 or 7500 Router with a CIP

A Cisco channel-attached router offers additional features not available in a 3745. They are:

- Multipurpose—The CIP provides a state-of-the art, high-performance solution for mainframe connectivity for not only SNA application access but TCP application access as well. As networks begin to offer intranet and Internet services, tying the mainframe into TCP networks with features such as TN3270 Server and TCP Assist enables you to leverage your mainframe investment. The NCP's support of TCP is limited.
- Higher Speed—The CIP offers a tenfold improvement in performance over a 3745 model 200 for SNA, and much larger performance improvement for TCP/IP. Many networks have reached capacity for their existing 3745s. Rather than investing more money in older technology, organizations are choosing to migrate to more multifunction channel solutions.
- Connectivity—The FEP has limited connectivity. It does not support Fiber Distributed Data Interface (FDDI), ATM, LANE, Fast Ethernet, Switched Multimegabit Data Service (SMDS), T3, or even Ethernet (for SNA). The 3746 900 expansion frame supports Ethernet with an imbedded 8229 translational bridge.
- Lower Costs—The CIP in a Cisco 7500 router can save money. There is no recurring licensing fee, and the 3745 resale value often pays for the CIPs to replace them. In leasing environments, the payback period is 18 to 24 months.

In summary, the Cisco 7500 router in conjunction with a CIP offers a number of benefits to an IBM enterprise network in terms of speed, connectivity, and flexibility. By minimizing the number of FEPs required in a network, the CIP offers a means to reduce network costs while improving performance. However, some FEPs may still be required for the following:

- SNI connections to other enterprises or divisions
- Bisynch, asynchronous, or ALC conversion
- Specialized functions such as EP, XRF, or NRF

CHAPTER 2

Network Design and Migration

This section allows you to:

- Determine when to run SNA and WAN functionality of the channel-attached router and when to run it on a separate data center router
- Estimate the number of CIPS required
- Estimate changes to mainframe CPU
- Determine if APPN is required
- Determine placement of DLUR functionality
- Understand subarea to APPN migration options
- Design for high availability
- Understand FEP to channel-attached router migration options

Basic Design Considerations

The CIP is an interface card that goes in a Cisco 7000 or 7500 router. When designing an SNA network using the Cisco CIP, you need to decide:

- What SNA features to use to transport SNA traffic from remote sites to the data center
- Where to place SNA features such as DLSw+ or APPN—in the CIP-attached router or in other central site routers
- How many channel-attached routers and CIPs you need to support your traffic volumes and availability requirements
- If APPN is required for SNA routing in the data center
- How to design your network for maximum availability
- How to migrate safely and easily

To design a network with optimal performance, high availability, and minimal cost, you must answer these design questions.

Accessing Remote SNA Devices

One of the first design considerations is to determine how SNA traffic will get to the data center. There are several options. Traffic can be bridged; it can be transported over SDLC, X.25, or Frame Relay; you can use DLSw+ to transport SNA over an IP backbone; or you can use APPN to natively route SNA directly from the branch. You can also use these features in combination. Which of these solutions you choose depends on several factors: carrier services available, what applications you have or plan to have in your network, and so on. The key issue covered in this guide is not which option to chose in the backbone, but where to put the features for optimal network performance and scalability.

Placement of SNA and WAN Functionality

Your central site routers generally provide WAN connectivity, SNA functionality, and mainframe connectivity (via the CIP). It is possible to put all of these functions in a single router. Alternatively, you can have minimal functionality in the CIP router and put SNA and WAN functionality in other central site routers. Two reasons you may want to do the latter are scalability and availability.

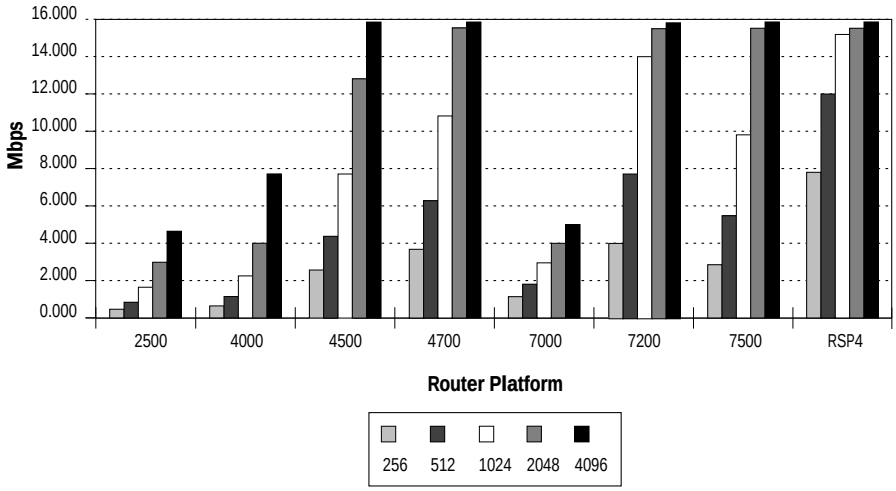
Data Center Scalability

Running SNA functionality such as DLSw+ or APPN in your channel-attached router may limit the scalability of your data center solution or increase the cost of the network.

If you run only source-route bridging (SRB) in your channel-attached router, and bridge SNA traffic onto one or more CIP cards in the router, the cumulative capabilities of the installed CIPs are the only limiting factors. SRB is fast switched and can switch more packets than a Cisco 7513 router full of CIPs can handle. The CIP can handle LLC2 processing for approximately 6000 SNA PUs and can process approximately 5000 packets per second. The capacity of a Cisco 7500 router with multiple CIPs is additive, because the processing required for the LLC2 processing is contained on the CIP card itself. This means a 7513 router with 10 CIPs can process 50,000 pps, which is well within the SRB capability of the router (assuming there are no access lists or filters running). If your backbone uses transparent bridging, the router uses source-route translational bridging (SR/TLB) to switch packets onto the CIP. SR/TLB is also fast switched (in Cisco IOS Release 11.2) and the 7500 router can handle more than 25,000 pps. This is a still a much higher traffic volume than seen in most SNA data centers, and it would require several mainframes to drive this traffic volume.

If you put DLSw+ or APPN/DLUR in the channel-attached router, the number of SNA devices that you can connect will be substantially less—up to a maximum of around 4000 SNA PUs if the transaction rate is low and no other processor-intensive features are running in the router. In addition, the transaction rate supported by a route processor is lower than the rate supported by the CIP. In both cases, the limiting factor is the route processor, not the CIP card(s). By separating SNA functionality (DLSw+ or APPN/DLUR) into lower-cost Cisco 4700s or 7200s and using the CIP router for SRB and IP only, you can scale your network up to thousands of SNA devices with a single channel-attached router (with one or more CIP cards) and reduce the total cost of the network. A single Cisco 7500 router with a CIP can keep up with three or four Cisco 4700s running DLUR. For more information about DLSw+ capacity, see the Cisco *DLSw+ Design and Implementation* guide. Figure 2-1 illustrates the APPN throughput of various platforms based on message size.

Figure 2-1 APPN Intermediate Session Routing (ISR) Throughput



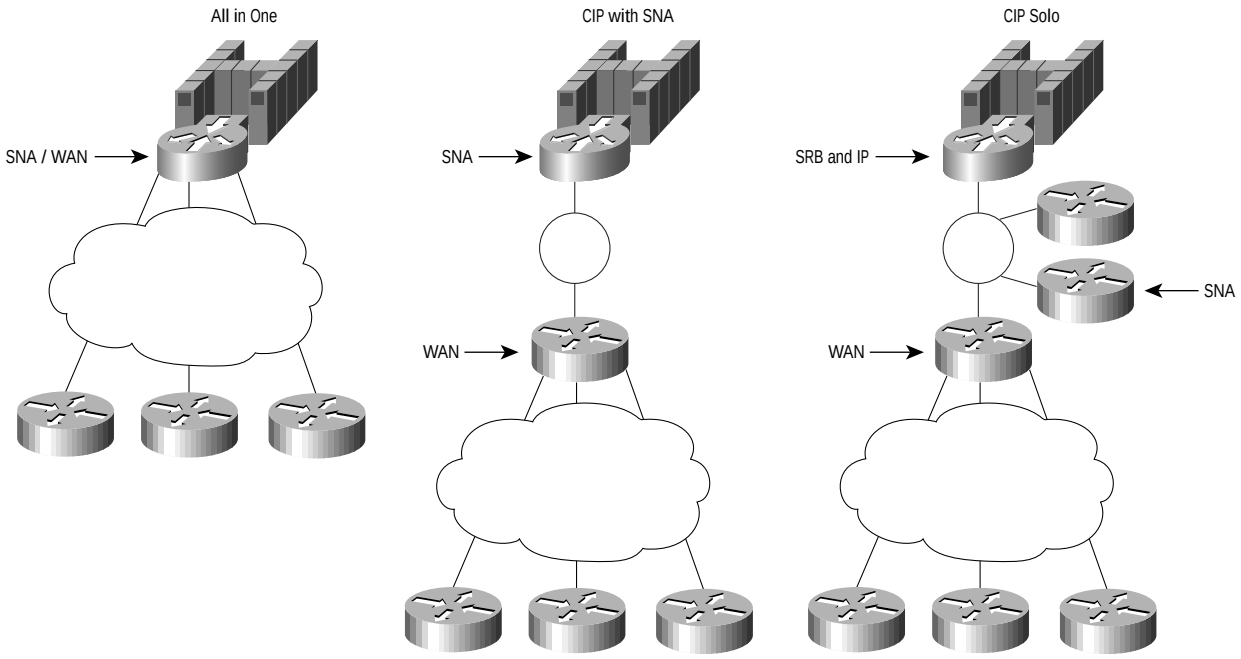
Data Center Availability

Running multiple functions and CIPs in a single router can impact availability. If you put all your functionality (the CIP, DLSw+, APPN, Frame Relay traffic shaping, and so on) in a single router, you increase the likelihood of a planned or unplanned outage in that router. For example, if you need to upgrade to a new Cisco IOS level to get HPR or the latest DLSw+ features, you need to reload the router. (With HPR, you can design your network to nondisruptively reroute around planned or unplanned outages of a CIP router.) If you separate SNA functionality from the CIP router, you minimize the potential for planned or unplanned outages in your CIP router. SRB functionality rarely needs updates for enhanced functionality. In addition, the less function you run in the CIP router, the smaller the chance of a failure. However, the tradeoff is that your SNA traffic must now go through an additional hop, creating an additional point of failure.

Some configuration changes (such as changing the maximum transmission unit [MTU] on a router) cause a restart of the interface cards, including the CIP. Good change management says that changes to channel-attached routers should only be made during nonproduction hours, but change windows are getting shorter and shorter. Limiting the function running in the channel-attached router minimizes the need for configuration changes and hence minimizes the occurrence of these short interruptions in mainframe availability.

Regardless of where you place SNA functionality, you may choose to load balance your workload across multiple central site devices to minimize the number of sessions disrupted by a single failure. Figure 2-2 compares three alternatives for functionality placement.

Figure 2-2 Alternatives for Functionality Placement



All in One (SNA, CIP, and WAN)

Having a CIP router that is also a WAN router and has SNA functionality (DLSw+, APPN, and so on) has the advantage that it requires the smallest number of central site routers. In small networks (30 to 50 branches) that are primarily SNA, this is a reasonable choice.

CIP and SNA Combined

Having a CIP router with SNA functionality but having a separate WAN router is a good solution for small to medium-sized networks (up to 200 remote branches) with a moderate amount of multiprotocol traffic. This design allows you to segregate multiprotocol broadcast replication from SNA processing.

CIP Solo

The third solution, bridging to a CIP router, is a good solution for medium to large networks (more than 200 remote branches) that require more than one or two central site routers for SNA. By segregating the SNA and WAN processing from the CIP-attached router, you can scale the network without buying additional CIP routers. By minimizing the functionality in the CIP router, you maximize its availability. The SNA functionality can either be in the WAN router or in separate peering routers at the data center. For large networks, using separate SNA routers and WAN routers further enhances scalability and maximizes availability. Also, in a Frame Relay environment, it allows a single Frame Relay data-link connection identifier (DLCI) to be used to access multiple DLSw+ peers.

Determining How Many Channel-Attached Routers and CIPs Are Required

As discussed in the previous section, function placement will play a role in determining how many channel-attached routers are required. Traffic volumes and the number of SNA PUs also play a role. This section provides some guidelines, but you may want to consult your local systems engineer for assistance. There are two limitations: CIP capacity and route processor capacity.

CIP Capacity

Determining how many CIPs are required is relatively straightforward. It depends on the transaction rate, the transaction size, and the number of LLC2 connections. It also depends on the number of hosts you need to attach to and what channel type you have—bus and tag or ESCON. If you are running multiple functions in a single CIP (such as IP datagram, TCP offload, or TN3270 server), consult your SE for assistance. The following numbers assume that only the Cisco SNA feature is running on the CIP card.

- A single CIP can handle about 6000 LLC2 connections and forward about 5000 pps.
- A single CIP with two daughter cards can attach to two bus and tag hosts.
- A single CIP with an ESCON adapter can attach up to 64 hosts by using the ESCON Multiple Image Facility (EMIF).

Other factors that may increase the number of CIPs required are availability and redundancy requirements and the number of other features running in the channel-attached router.

Channel-Attached Router Capacity

If you are running only SRB and IP in the channel-attached router, then you can easily put four to five CIPs in a single Cisco 7500 router. More than likely, performance won't be the determining factor in this case, but rather availability, redundancy, and risk.

If you run features such as APPN or DLSw+ in the channel-attached router, the route processor—not the CIP—will likely be the limiting factor. A Cisco 7500 router with a Route Switch Processor 2 (RSP2) running DLSw+ can support about 2000 to 4000 SNA PUs, depending on traffic volumes. The RSP4 is expected to support about 4000 to 6000 SNA PUs. APPN has similar limitations in the number of PUs. If APPN or DLSw+ are running in the channel-attached router, a single CIP can keep up with any SNA traffic the route processor can send it. In this case, the only reasons to put multiple CIPs in that router are for redundancy or to handle other functions such as TN3270 server or TCP offload. As described earlier, for medium to large networks, it makes more sense to separate process-switched SNA functionality from the CIP router.

Other limiting factors in the router processor can be OSPF, Frame Relay, or X.25. These features limit the capacity of the router, not the CIP, but if running in CIP-attached routers, they may limit the capacity of the combined solution. This document does not describe how to determine the route processor limitations of these features.

Attaching the CIP to a Campus Backbone

FEPs have traditionally attached to the campus network via Token Ring. With a channel-attached router, several other options are available. Table 2-1 lists these options, describes the Cisco IOS technology used to access these options, provides the prerequisite Cisco IOS release number, and lists any considerations.

Table 2-1 Campus Options

Campus Backbone	IOS Features in Channel-Attached Router	IOS Release	Consideration
Token Ring	SRB, DLSw+, or APPN	11.0	
FDDI	SRB, DLSw+, or APPN	11.0	If DLSw+ uses FDDI as a transport
	SRB	11.2	If end stations connect to DLSw+ over FDDI
	SR/TLB	11.2	Fast switched
Ethernet or Fast Ethernet	SR/TLB, DLSw+, or APPN	11.0	
ATM	DLSw+	11.0	If DLSw+ uses ATM as a transport
	APPN	11.1	RFC1483
	Ethernet LANE with SR/TLB, DLSw+ or APPN	11.2	If end stations connect to DLSw+ or APPN over Ethernet LANE
	Token Ring LANE with SRB, DLSw+, or APPN	11.3	If end stations connect to DLSw+ or APPN over Token Ring LANE

Mainframe CPU Utilization

A commonly asked question when considering a CIP as an alternative to the FEP is the impact on mainframe CPU cycles. Replacing a FEP with an XCA channel-attached device (such as a 3172 or a Cisco 7500 router with CIP2) will have minimal effect upon a given data center capacity plan, and then only if the current plan is nearing capacity. Our tests have shown that if a FEP is replaced with a CIP, you will see a slight increase in total mainframe CPU, but the increase is minimal—generally between 1 to 3 percent. The increased throughput of the CIP, however, will allow file transfers to occur in less time, therefore freeing up the mainframe CPU sooner.

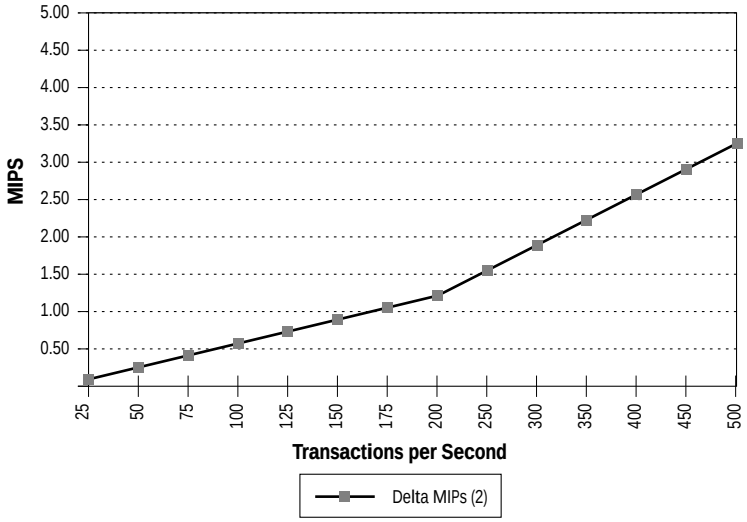
What has confused this issue in the past is the way Resource Monitoring Facility (RMF) measures host CPU usage. This tool doesn't accurately represent the allocation of CPU cycles to specific tasks. For example, when using the FEP/CDLC path through VTAM, a simple application write operation appears to spend more time in the application address space than in the VTAM address space. This makes the VTAM utilization appear very low. When using the XCA path through VTAM, the same application operation spends more time in the VTAM address space and less in the application address space. This makes the VTAM utilization appear much higher. The only thing that matters from a capacity planning perspective is the difference between the total CPU utilization of the two operations. This difference is what we measured.

In addition, the delta mips required to handle a given transaction load is smaller if the transaction rate is higher. This is in part due to the operation of coat-tailing at higher load and because the VTAM service request block can perform more work under each dispatch (that is, it is able to process more path information units [PIUs] before releasing the processor).

In one test, a 40-mips mainframe (9672-R22) had an average transaction rate of 4500 transactions per minute (75 TPS). In this case, replacing the FEP with a Cisco channel-attached router increased host usage by no more than 1.77 percent (0.78 of a mips). Running the same host at 70 percent of available cycles, and processing transactions at a rate well in excess of 11,000 transactions per minute (185 TPS) required at most an extra 3 percent (1.2 mips). Figure 2-3 illustrates the increase in host CPU (delta mips) based on transaction rate in a 9121-982 mainframe. The mainframe used for this graph was a higher-mips machine than the mainframe used in the testing cited above, so the results are slightly different.

Note that in addition to a slight mainframe mips increase, migrating from a FEP to an XCA device may increase mainframe memory requirements. You can get estimates from the formulas provided by IBM.

Figure 2-3 Impact on a 9121-982 Mainframe of Migrating from a FEP to a CIP



APPN in the Data Center

APPN is IBM's strategic direction for SNA. It plays a key role in the IBM Parallel Sysplex environment for providing high availability. It is the only SNA protocol that will run in IBM's strategic FEP replacements—the 950 and the 2216. It offers network dynamics and configuration simplicity far beyond what is available in subarea networking. Therefore, APPN is the SNA routing protocol that has been implemented in the Cisco IOS IBM services.

This section describes APPN, when its required, what it provides, and how you can take advantage of APPN dynamics and availability in a network with legacy SNA controllers and 3270 applications.

Do You Need APPN for SNA Routing?

Most SNA networks still use subarea routing and have not migrated to APPN. Since the Cisco IOS software provides SNA routing with APPN, one of the first things you need to determine is whether migrating to a Cisco CIP solution for SNA requires migrating to APPN in some portion of your network. (There are other reasons one may want to migrate to APPN. This section only determines if APPN is required to provide SNA routing in lieu of using FEPs for the same purpose.)

If you are currently using FEPs and running subarea SNA, and you are considering using the CIP to replace one or more of your FEPs, you may need APPN in your network. You do not need APPN for SNA routing if any of the following are true:

- You only have one active VTAM image at a time (you may have a second image for backup only).
- Your end users only access a single VTAM; they do not have cross-domain sessions (that is, each end user only accesses applications in a single LPAR).
- Your end users have sessions with applications in multiple hosts, but SNA sessions use VTAM and CTC for session routing, not your FEPs.
- You have a session monitor that every user logs on to, and all steady-state session traffic goes through that session monitor.

If you run multiple VTAM images concurrently, and your end users log on to one VTAM and then establish a cross-domain session with another VTAM, you are doing SNA routing in the data center. If that SNA routing is done by a FEP, you will want to consider APPN in your CIP design. Make sure you read the sections covering APPN in this chapter.

APPN Functionality Placement

If you require APPN in your network, the first thing you need to decide is where to place the APPN function. It can run in the channel-attached routers, in data center routers that are LAN-attached to the channel-attached router, or in distribution sites. You may want to run APPN in distribution sites if you have multiple data centers and you want to make SNA routing decisions outside of your data centers. The decision about running SNA function in a channel-attached router or in a LAN-attached data center router was covered earlier in this chapter under "Basic Design Considerations."

Dependent LU Support

Most SNA networks have dependent LUs that require a VTAM session in order to communicate with other SNA LUs. If you know you don't need dependent LU support, you can skip this section. Otherwise, read this section to understand what dependent LU support is, why it is needed, and where you should put the function.

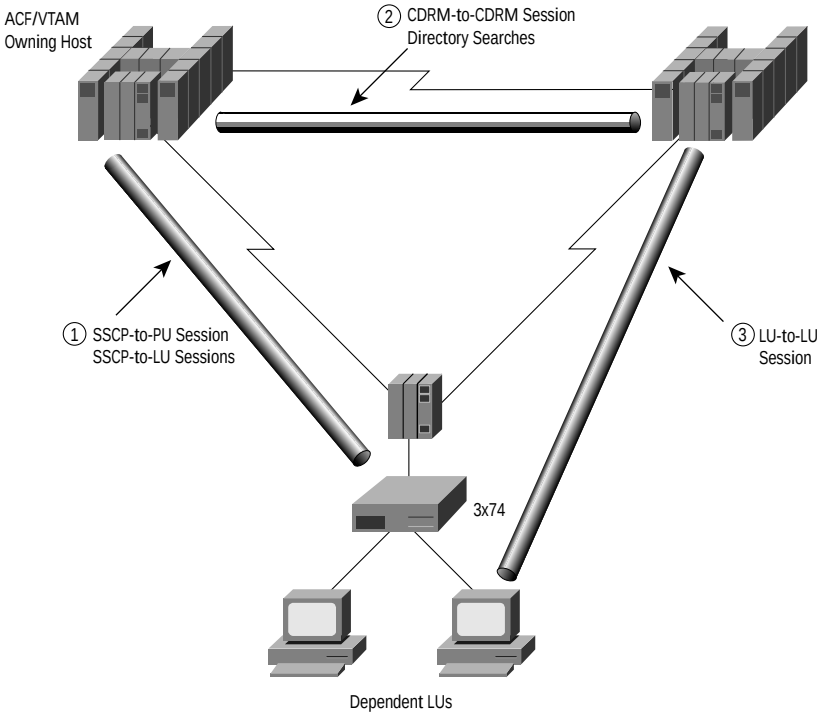
In subarea SNA, when SNA devices are "activated," VTAM establishes control sessions with these devices. The control sessions are SSCP-to-PU sessions or SSCP-to-LU sessions. These sessions are used to transport management data and to transport LU-to-LU session establishment requests from an LU to VTAM. VTAM provides directory services for LUs. It finds the destination application by searching its local directory, searching a remote directory, and querying other VTAMs. In subarea SNA, the span of control of VTAM is called a domain. A resource owned by a different VTAM is called a cross-domain resource. When the requesting LU is owned by one VTAM and the destination application resides in the domain of another VTAM, VTAM finds the application by looking at its list of cross-domain resources (CDRSCs) or by querying all the VTAMs it is in session with. VTAMs communicate with each other using cross-domain resource manager (CDRM) sessions.

Session establishment involves three key steps, as shown in Figure 2-4.

1. When a dependent LU wants to establish a session, it sends a session request to VTAM (using the SSCP-to-LU session).
2. VTAM finds the application (either locally or remotely).
3. Then the application host sends a session connection (BIND) request directly to the originating LU.

In Figure 2-4, the network has a remote FEP that provides SNA boundary function for the PU 2.0 device and makes routing decisions to forward steady-state session traffic directly from the remote LU to the application host.

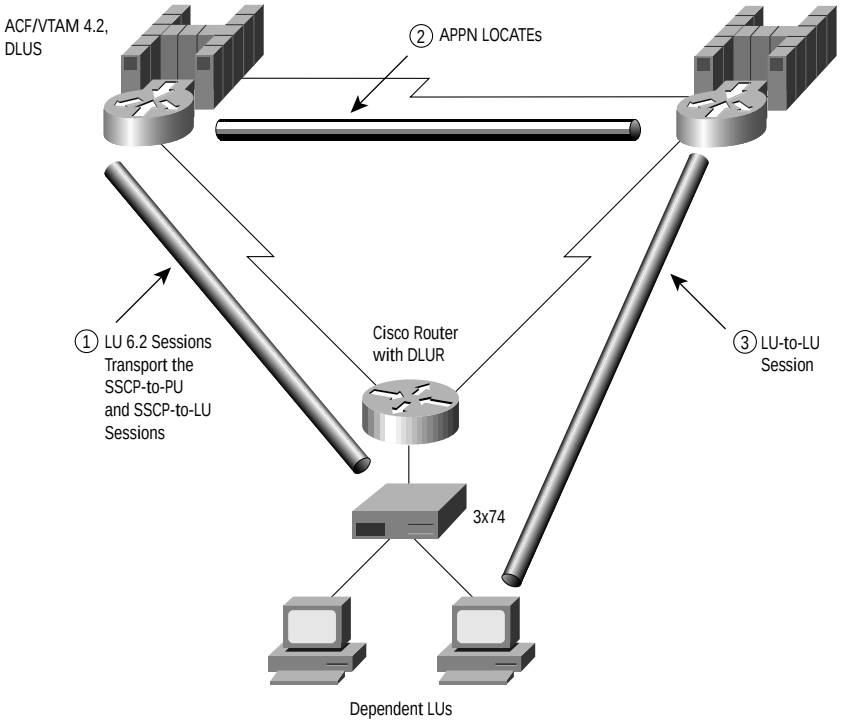
Figure 2-4 Session Establishment for Dependent LUs Using Subarea SNA



APPN does not operate the same way subarea operates. A key difference is that APPN supports only LU-to-LU sessions (APPN control points are special LUs). The sessions shown in Figure 2-4—the SSCP-to-PU, SSCP-to-LU, and CDRM-to-CDRM sessions—are not supported by APPN. For many years, this meant that legacy 3270 terminals or emulators could not access 3270 applications over an APPN network. With VTAM 4.2, this problem has been addressed. VTAM now supports a feature known as Dependent LU Server (DLUS), which when used in conjunction with a DLUR allows 3270 applications to take advantage of APPN networks. Figure 2-5 shows how DLUS/DLUR works.

As shown in Figure 2-5, when VTAM is configured to be a DLUS, it establishes a pair of LU 6.2 sessions with each DLUR. These sessions are used to carry the SSCP-to-PU and SSCP-to-LU sessions that the dependent devices require. When VTAM receives a session request from a dependent LU, it checks its directory, and if doesn't find the destination resource, it sends an APPN LOCATE to the network. (VTAM can provide central directory services for an APPN network, which minimizes the need for LOCATEs.) Once the destination application is found, the owning VTAM forwards the session request to that application, and the application sends a session start command (BIND) directly to the dependent LU. As shown in Figure 2-5, this session request actually goes to the DLUR, which forwards it to the dependent LU.

Figure 2-5 Session Establishment for Dependent LUs Using APPN DLUS/DLUR



What these two diagrams illustrate is that when FEPs are replaced with Cisco routers, the DLUR router can make the same routing decisions previously made by the FEP. In Figure 2-5, only the DLUR router and VTAM need APPN functionality. The channel-attached routers can be running either SRB (if the DLUR router is on the same campus) or DLSw+ (if the DLUR router is in a distribution site).

Placement of DLUR Function

In general, a good network design replaces a BNN FEP with a DLUR router. The channel-attached router can then replace one or more intermediate network node (INN) FEPs.

If your current network design has a single FEP providing both BNN and INN functions, you can still choose to put DLUR function in a data center router separate from the channel-attached router for improved scalability and availability, as described in "Placement of SNA and WAN Functionality" earlier in this chapter. DLUR function can also be placed in each branch instead of in a few data center routers, but this places an additional burden on VTAM because it must have a pair of CP-to-CP sessions with each DLUR. In addition, if the DLUR function is in NNs, there are scalability issues to be considered. See the Cisco *APPN Design and Implementation* guide for details.

Sizing DLUR Routers

Performance tests have shown that a single Cisco 4700 or 7200 router can provide DLUR function for 4000 SNA DSPUs. For these tests, however, each PU had only a single LU, and nothing else was running in the router. The number of LUs and sessions play into the equation because they increase the transaction rate and the memory requirements. Exact numbers depend on the transaction rate and size and on the other functions running in that router. Refer to the Cisco *APPN Design and Implementation* guide for memory estimates.

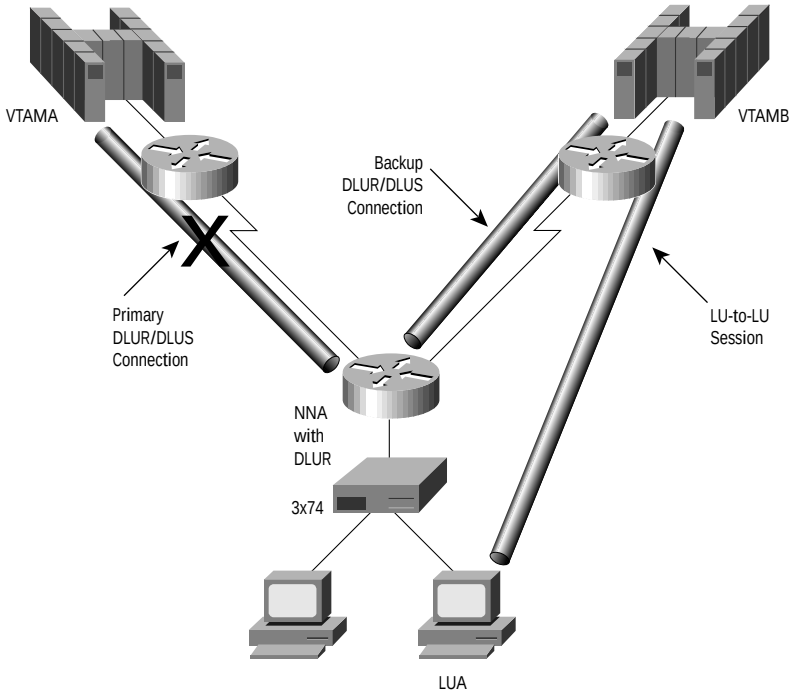
SSCP Takeover/Giveback

SSCP takeover is a function provided by VTAM and NCP. It maintains LU-to-LU sessions when an owning host fails and the application host is still active. Every resource in a subarea SNA network must be owned by an SSCP. When the owning SSCP fails, another SSCP can assume ownership of the failing host's resources by taking over the resources. This takeover does not disrupt LU-to-LU sessions. When the original owning SSCP recovers, it can resume ownership by performing the SSCP giveback function.

When using DLUR in a Cisco router, VTAM continues to provide full takeover and giveback capability. DLUR in the Cisco router provides boundary function for a dependent LU and also provides the SSCP takeover and giveback function. In Figure 2-6, LUA and the DLUR router (NNA) are owned by VTAMA. If VTAMA fails, VTAMB can take over ownership of the DLUR router and all its resources. The DLUR router immediately attempts to reestablish the DLUS-to-DLUR LU 6.2 pipe to the backup DLUS host. The device, LUA, has no knowledge that the owning SSCP has failed and that a new ownership has taken place. The existing LU-to-LU session between VTAMB and LUA is not disrupted as long as **ANS=CONT** is coded in VTAM.

When VTAMA recovers, VTAMB can give back ownership to VTAMA. This terminates the DLUS-to-DLUR pipe between VTAMB and NNA, and a new DLUS-to-DLUR pipe is established between VTAMA and NNA.

Figure 2-6 SSCP Takeover Using APPN DLUS/DLUR



Migration to APPN from a Subarea Environment

There are many reasons to migrate from subarea to APPN. Obviously, where SNA routing is required, migrating to APPN allows you to replace aging FEPs with newer, more flexible and less costly technologies. In addition, APPN is required to take full advantage of the Parallel Sysplex environments. HPR can improve network availability. Another key benefit of APPN is the

simplification of SNA network configuration. Maintaining an SNA network can be resource intensive. By taking advantage of the capabilities of APPN, you can free system programmers from having to do repetitive tasks. Skilled resources can then be redeployed to support next-generation network and application rollouts.

The good news is that it is relatively simple to enable APPN in the data center and in VTAM.

VTAM APPN Node Types

VTAM can be configured as one of several types of APPN node, each of which provides a different level of subarea and APPN function and interoperability. The implementation depends upon whether the node or nodes to be converted need to communicate with other subarea nodes, other APPN nodes, or both. A description of the APPN node types follows.

Interchange Node

The most common migration step for a multidomain network is to migrate the CMC VTAM subarea host to an ICN. An ICN combines the function of a subarea node and a network node. It implements APPN NN functionality, SSCP functionality, and CDRM functionality. The location of an ICN is on the border of an APPN network and a subarea network. Here it provides conversion between subarea and APPN protocols and enables the establishment of sessions between applications residing on an APPN VTAM host to LUs residing in the subarea network by converting session requests from one protocol to the other. It can also provide intermediate session routing.

An ICN can own and activate NCPs; it communicates network control data by using SSCP-to-SSCP sessions with other subarea nodes and CP-to-CP sessions with other APPN nodes. To enable it to participate in the subarea network, it is defined with a unique subarea number and requires subarea path definition statements. An ICN can be connected to other APPN nodes, LEN nodes, and subarea nodes.

Migration Data Host

A migration data host (MDH) is a VTAM data host that communicates to APPN resources as an APPN end node and communicates to directly attached VTAMs and NCPs using subarea flows. Unlike an ICN, it doesn't translate between the two (APPN and subarea), and it cannot own NCPs or provide ISR routing. An MDH is often implemented during migration because it allows the data host to be accessed either from an APPN node (for example, a Cisco router) or from a FEP at the same time, thereby providing the safest migration alternative.

End Node or Network Node

When VTAM is configured as an APPN EN or NN, it does not use SSCP-to-SSCP sessions. Instead, a it uses CP-to-CP sessions for network control data. Consequently, it does not require subarea network routing definitions. It requires static definitions only for those resources located within the APPN node and for local connections.

Virtual Route Transmission Group

One other useful term to understand is a Virtual Route (VR) Transmission Group (TG). Virtual routes are end-to-end paths through a subarea network used to carry SNA traffic. A VR TG is a collection of virtual routes connecting two VTAM nodes that are acting as either ICNs or MDHs. VR TGs allow CP-to-CP sessions between VTAMs to communicate using FID4 transmission

headers and to take advantage of the multilink transmission group feature of subarea SNA. They can be used if the path between the APPN ICNs or MDHs contains subarea FEPs, but they can also be used for channel-to-channel (CTC) connections between hosts.

Migrating the Data Center to APPN

The following three steps illustrate a possible migration from subarea to APPN. The order of these migration steps allows the safest migration because there is always a fallback to business-as-usual. Before you migrate a subarea network to APPN, you may wish to read the Cisco *APPN Design and Implementation* guide.

Step 1 Configure VTAM as an ICN.

Configuring VTAM as an ICN will not impact current subarea communications, but it will allow new APPN communications to occur side by side. Start by enabling APPN on at least one VTAM (running VTAM V4R2 or greater). A VTAM that owns your remote resources and FEPs is a good choice, because in the APPN world, this same VTAM will act as a DLUS and own your dependent LUs. If your network includes one or more CMC hosts, enable APPN on these hosts first. Enable APPN in this host by altering the VTAM start parameters as follows:

- NODETYPE=NN
- HOSTSA=nn (This statement is already specified in any subarea VTAM, but it is included here to point out that you should keep this definition because its inclusion combined with the previous statement is what makes this VTAM an ICN.)
- CPCP=YES
- SORDER=xxxx where xxxx is either SUBAREA, APPN, or APPNFRST. (If SUBAREA is specified, most sessions will be established using the subarea path, and you will not exploit APPN. If APPN is specified, APPN searches will always occur first, even if most resources reside in the subarea network. APPNFRST is only available in VTAM Version 4 Release 3 or later.)
- CDRDYN=YES
- CONNTYPE=APPN
- DYNADJCP=YES
- DYNLU=YES
- SSEARCH=YES

In addition, the following data sets need to be added to the VTAM startup: DSDB1, DSDB2, DSDBCTRL, and TRSDB. These data sets are used by VTAM to store the cache entries for APPN databases. These databases are optional and are only required if you do not want VTAM to rebuild the entire cache after VTAM is started. The inclusion of these data sets is most important when this VTAM is a CDS.

Finally, you should copy the APPN COS table named COSAPPN from the SAMPLIB to VTAMLST to provide COS default capabilities for APPN.

The selected VTAM is now an APPN network node with subarea capability. This VTAM can act as a DLUS for a Cisco router providing DLUR functionality for legacy SNA devices.

Step 2 Enable APPN VTAM in data hosts.

Application hosts or data hosts do not have to be APPN NNs. They can simply be ENs. In this case, they would be configured with another VTAM as their NN server (most likely the VTAM migrated in Step 1). Alternatively, application hosts can be configured as MDHs. This step is considered the safest, because it allows you to provide concurrent access to VTAM from either a subarea NCP or

the APPN network. Once you have migrated your application hosts to APPN, they can communicate to each other using CP-to-CP sessions instead of SSCP-to-SSCP and CDRM-to-CDRM sessions. In addition, once an application host is APPN-enabled, it can forward BINDs and steady-state traffic directly to a DLUR router without going through an owning VTAM. Enable APPN in your application hosts or data hosts by altering the VTAM start parameters as follows:

- NODETYPE=EN
- HOSTSA=nn (This statement is already specified in any subarea VTAM, but it is included here to point out that you should keep this definition if you want to migrate this host to an MDH. If you want to migrate this host to an EN, you should delete this statement.)
- CPCP=YES
- SORDER= xxxx (For an MDH, xxxx can be SUBAREA, APPN, or APPNFRST. For an EN, xxxx is APPN.)
- CDRDYN=YES
- CONNTYPE=APPN
- DYNADJCP=YES
- DYNLU=YES
- SSEARCH=YES

In addition, the following data sets need to be added to the VTAM startup: DSDB1, DSDB2, DSDBCTRL, and TRSDB. Copy the APPN COS table named COSAPPN from the SAMPLIB to VTAMLST to provide COS default capabilities for APPN. If you still have FEPs in your network, APPN MDH and ICN hosts can communicate to each other via VR TGs.

At the end of these two steps, existing subarea capability is basically unaffected, while APPN devices including 3174s, Cisco routers, and so forth, can connect to this host as an APPN node and support communication with LUs in the subarea network or in the APPN network. Step 3 is required to complete the VTAM migration.

Step 3 Enable a CDS.

To minimize APPN LOCATE traffic, you can configure a VTAM NN as a CDS. When VTAM is acting as a CDS, APPN ENs and NNs can automatically register their local resources with that VTAM. In addition, before a NN broadcasts a LOCATE across the network, it will send a directed search to its CDS.

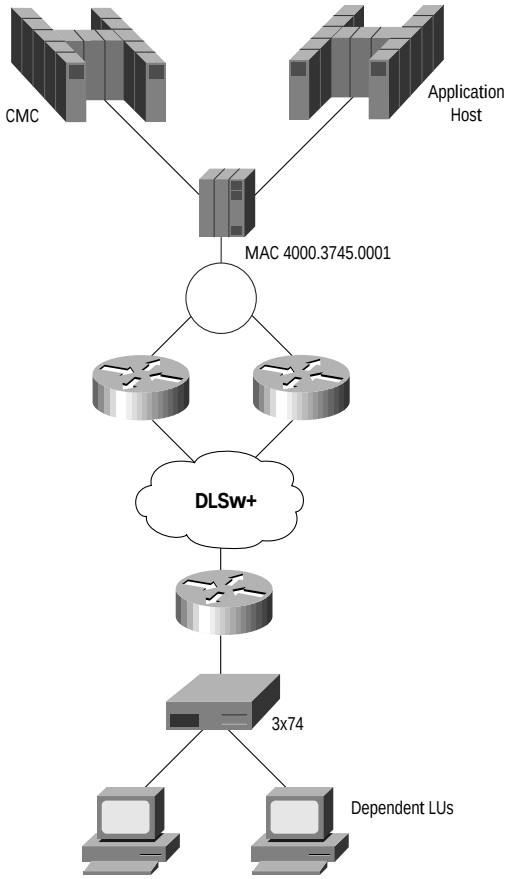
The following additions and changes in the VTAM start options will allow the VTAM host to act as a CDS. The location of the CDS should be chosen to maximize the efficiency of any searches.

- CDSERVR=YES
- VRTG=YES
- VRTGCPCP=YES
- SORDER=APPN

Migrating the Network to APPN/DLUR and the Channel-Attached Router

For simplicity, this document describes migrating a DLSw+ network because the concepts are similar, although DLSw+ simplifies controlling the rate of migration. In the “before” picture, as illustrated in Figure 2-7, remote sites connect to the data center routers using DLSw+. There are two data center routers, and each has a different cost. The lower-cost DLSw+ router is preferred, and the higher-cost router is used only when the lower-cost router is not available.

Figure 2-7 Migrating the Network: The Before Picture



Step 1 Add the CIP.

In this migration, because the CIP will not contain the DLUR function, the CIP will not have the same Media Access Control (MAC) address as the FEP. You can then issue VTAM commands to activate the channel and the XCA major node and associated switched major nodes.

Step 2 Add the DLUR router.

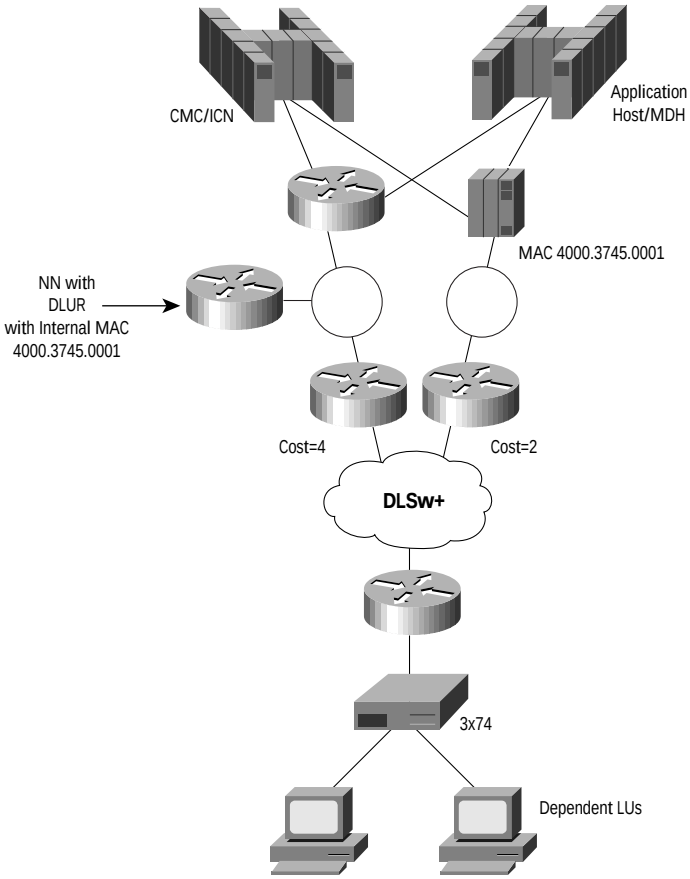
Add the DLUR router to the Token Ring attached to the higher-cost DLSw+ peer, as shown in Figure 2-8. Give the DLUR router the same internal MAC address as the FEP and point it to the adjacent ICN and MDH by configuring the link station addresses of the CIP. Once this step is completed, if the lower-cost peer is not available, devices will automatically connect to the higher-cost peer, which will forward session traffic to the DLUR router. If SORDER=APPN or APPNFRST, this router will use APPN protocols to find the correct application (in either the MDH or the ICN host). That host will initiate a session request (BIND), and the session traffic will go directly from the DLUR router to the correct host by way of the CIP.

Step 3 Change the peer costs.

You can then optionally change the peer costs so that the DLSw+ peer attached to the DLUR router has a lower cost. This will cause most traffic to use the channel-attached router and the DLUR router(s). If there is a failure in either of these, traffic will be automatically routed through the FEP. This method provides very high availability and a smooth migration.

While the “before” network will vary, the above migration steps should give you an idea of how to use Cisco IOS software with IBM services to complete the migration.

Figure 2-8 Migrating the Network: The After Picture



Role of APPN in the Parallel Sysplex Environment

A parallel system complex (Parallel Sysplex) is a cluster of independent S/390 machines cooperating to perform a series of tasks while providing a single system image to end users. The key benefits are higher availability and higher scalability through workload distribution. Many data processing centers have multiple MVS systems to support their business and these systems often share data and applications. A Parallel Sysplex environment is designed to provide a cost-effective solution to meet the user's expanding requirements by allowing MVS systems to be added and managed efficiently. The idea is to couple together hardware elements and software services.

A Parallel Sysplex consists of multiple 9672 CMOS processors. In an SNA environment, each CMOS processor presents a VTAM domain. The concept of multiprocessors introduces a problem. Today, users are accustomed to single images. For example, Information Management System (IMS) running on the mainframe can serve the entire organization on a single host image. With the multiprocessor concept, you would not want to tell User A to establish the session with IMS on System A and User B to establish the session with IMS on System B, because IMS may run on either system. To resolve this, a feature called Generic Resource was invented. The Generic Resource feature enables multiple application programs that provide the same function to be known and accessed by a single generic name. This means that User A may sometimes get IMS on System A, and sometimes IMS on System B. Because both systems have access to the same shared data in the sysplex, this switching of systems is transparent to the users. VTAM is responsible for resolving the

generic name and determining which application program is used to establish the session. This function enables VTAM to provide workload balancing by distributing incoming session initiations among a number of identical application programs that are running on different processors.

The Generic Resource feature only runs on VTAM with APPN support. In order to achieve session load balancing across the different processors, users have to migrate VTAM from subarea SNA to APPN.

A new feature known as Multi-Node Persistent Sessions (MNPS), available in VTAM Version 4 Release 4 and the latest Customer Information Control System (CICS), provides nondisruptive recovery from the loss of an application host. This feature requires HPR.

Designing for High Availability

When accessing SNA applications on a mainframe, high availability is key. This section describes how to achieve high availability by providing alternate data-link paths to access a mainframe and automatic—but disruptive—recovery around failures of a channel gateway. Nondisruptive rerouting around channel gateway failures can only be achieved with HPR (available in Cisco IOS Release 11.3) or TCP (when using the TN3270 server on the mainframe).

In the case of HPR, nondisruptive rerouting occurs only between the RTP endpoints. Loss of an RTP endpoint is disruptive to user sessions. More than likely, VTAM will be one of the endpoints. The other endpoint can be in the channel-attached router, another data center router, at each branch, or at each desktop.

- When possible, it is best not to place the other RTP endpoint in the channel-attached router because the router then becomes a single point of failure and the failure of that router is catastrophic (since so many resources use it).
- By placing the RTP endpoint in separate (and typically less-expensive) data center routers, you enable nondisruptive rerouting around a channel-attached router failure. In addition, you can balance SNA resources and traffic across a number of data center routers to minimize the impact of a single failure.
- The RTP endpoint can be in the branch. You should measure the impact this would have on VTAM, because maintaining large numbers of RTP endpoints puts an additional burden on VTAM. If your network strategy is to move to an IP backbone and isolate SNA to the data center, the previous alternative is a better choice.
- Extending HPR to the desktop is generally not recommended, because it increases the workload in VTAM and may adversely affect VTAM performance.

SNA Communication Using CSNA

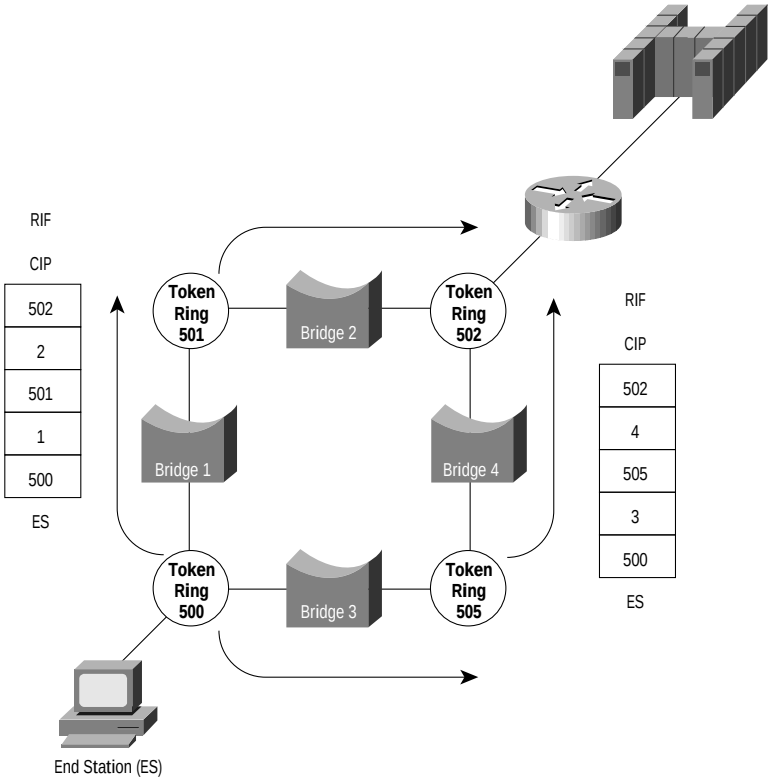
Because the CIP appears as a LAN port and the attaching SNA end systems appear as part of a switched major node, the CIP can take advantage of the redundancy features inherent in LANs and SRB. Cisco DLSw+ can provide SRB availability characteristics for devices on Ethernet or SDLC.

In the simplest network, SNA end systems attach to the channel-attached router over a source-route bridged LAN. As you will see, all other networks can be viewed as a variation of that, so this simple network design will be examined first. In order to understand this section, a basic understanding of how SNA works over a source-route bridged LAN is key. Therefore, this section starts with an overview of the technology.

In order for a LAN-attached end station to gain access to a host over a CIP, the end station must be configured with the MAC address of the CIP. In addition, the IDBLK and IDNUM specified in VTAM must match the corresponding value configured in the end station.

When an end station initiates an SNA connection, it sends an explorer (either a TEST or an XID) frame specifying the MAC address of the CIP. This explorer is copied by every source-route bridge on the path between the end system and the CIP. As each bridge copies the frame, it records its bridge number and the next ring number in the routing information field (RIF). If there are multiple paths between the end station and the CIP, the CIP will receive multiple copies of the explorer, as shown in Figure 2-9. The CIP responds to each of them and sends the response over the same path the explorer took to get there (as specified in the RIF). The end station then selects the route that will be used for the session, normally by using the route noted in the first explorer response received.

Figure 2-9 Explorer Processing on a Source-Route Bridged LAN

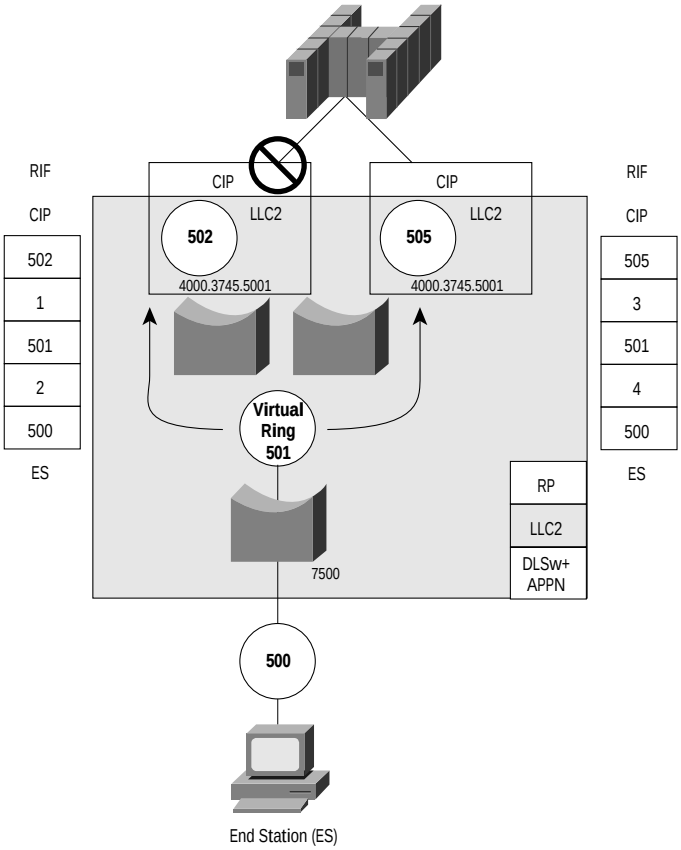


The end station then sends an XID to the CIP using this SRB path. The CIP forwards the XID to VTAM. The XID contains the IDBLK and IDNUM and must match an entry defined in VTAM for the session to be established.

Use of Duplicate Addresses for High Availability

Source-route bridged LANs support duplicate addresses (as long as they are on different ring segments), because to the end system they simply appear as two different paths to get to the same device. The CIP architecture takes advantage of that characteristic to offer redundancy and load balancing. If a CIP is out of service for any reason, and there is another CIP with the same MAC address located on a different ring segment, SNA end stations will automatically find the alternate CIP and use it to access the mainframe, as shown in Figure 2-10. In this example, recovery from the loss of a CIP or channel adapter is automatic, but disruptive. Because both CIPs are in the same router, failure of the channel-attached router is not addressed in this design.

Figure 2-10 Using Duplicate MAC Addresses with CIPs



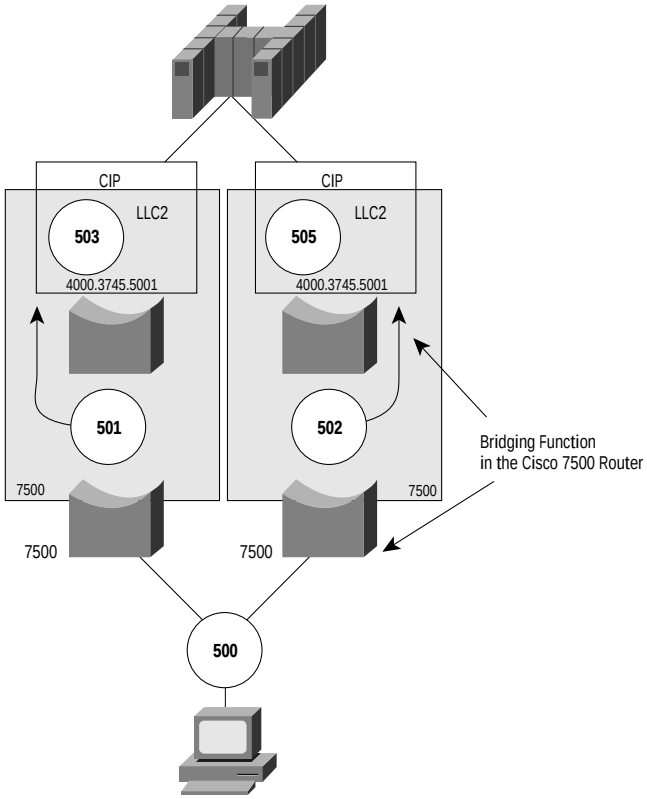
Duplicate addresses are not allowed on a single LAN segment. If there are duplicate addresses on different segments, these may be concurrently active. Note that in the case of the CIP, these segments (as indicated by rings 502 and 505 in Figure 2-10) can be logical ring segments. In the case of FEPs, these would have to be physical ring segments. Other network devices distinguish the duplicate addresses by the RIF used to reach them. The CIP always uses SRB internally to the channel-attached router, as illustrated by the logical "bridges" inside the Cisco 7500, and therefore multiple CIPs with the same MAC address can be active at the same time as long as they have unique virtual ring numbers. These duplicate CIPs can increase availability by automatically providing a backup capability for each other.

In a transparent bridging environment, duplicate addresses are not allowed. However through the use of DLSw+, Ethernet-attached devices can take advantage of the CIP redundancy described previously. In addition, DLSw+ allows SDLC devices to benefit. In the case of SDLC devices, the MAC address of the CIP is configured to DLSw+ instead of the SNA device.

Duplicate MAC addresses can also be used to load balance traffic across multiple routers equipped with CIPs and connected to the same VTAM. Figure 2-11 and Figure 2-12 show two possible scenarios. Both of these designs provide automatic backup from the loss of a channel-attached router, CIP, or channel adapter. Load balancing minimizes the number of resources affected by any single outage.

In Figure 2-11, load balancing occurs using standard SRB techniques of the end system. Most end systems select the first path to respond, but over time the end systems will tend to be spread over the two CIPs, because congestion on a given path through the LAN network or in a given gateway is likely to slow down the response and lead to the selection of a different path.

Figure 2-11 Load Balancing Using Duplicate MAC Addresses and SRB

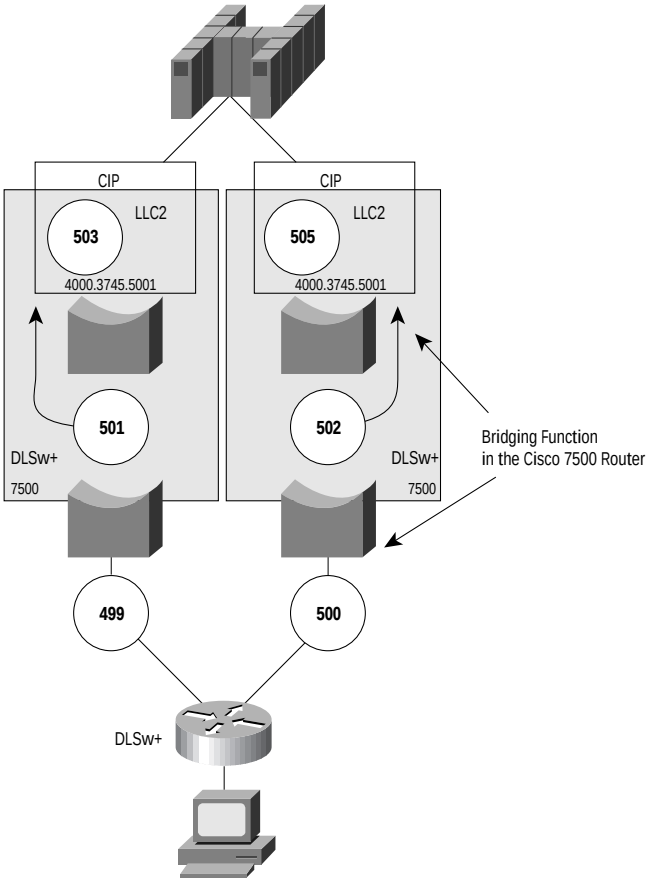


In Figure 2-12, DLSw+ has been configured to load balance, which means that each new circuit will alternate, in round-robin fashion, through the list of ports it can use to access the CIP.

Note DLSw+ caches only one RIF per MAC address on a given port. As a result, you can not load balance across duplicate MAC addresses that are accessed over a single port, even if they have different RIFs. You should use multiple ports, as shown in Figure 2-12.

If DLSw+ is running in the same router as the CIPs, DLSw+ views each CIP as a different port, so load balancing is possible.

Figure 2-12 Load Balancing Using Duplicate MAC Addresses and DLSw+



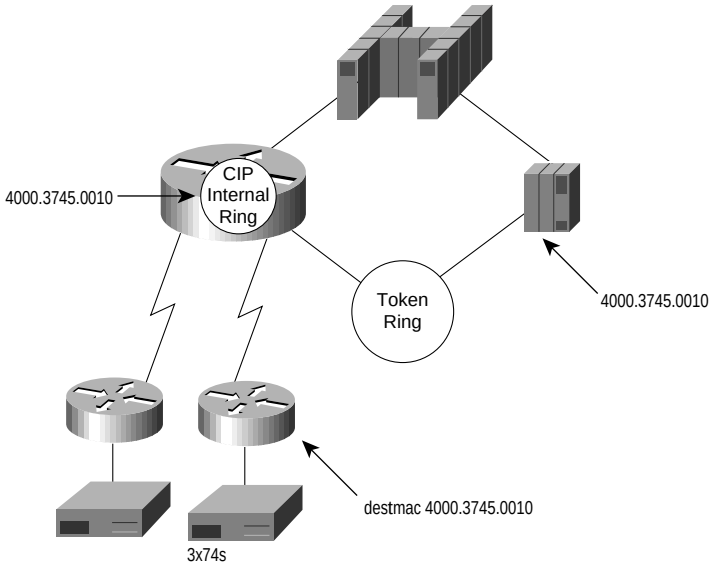
Migration and Coexistence

Most networks today use FEPs to access their mainframes. A Cisco router solution offers a cost-effective alternative to FEPs in many environments. Two key questions arise: How do you migrate from a FEP to a CIP, and can a FEP coexist with a CIP either permanently or during migration?

The easiest and safest way to migrate from a FEP to a CIP is to use SRB and configure duplicate MAC addresses on both the CIP and the FEP. This technique requires no changes to the end systems, and minimal or no changes to the FEP (assuming the FEP has a Token Ring adapter and is configured with a switched major node). The SRB protocol will provide rudimentary load balancing across the two mainframe channel gateways and automatic and dynamic backup of one for the other. Figure 2-13 shows a simple example of this technique.

If the existing FEP does not have a Token Ring card, SDLC devices can still be migrated, one line at a time, by connecting the SDLC line to a router instead of the FEP. Using local DLSw+ or APPN, the router can convert the SDLC to LLC2 for access to a CIP.

Figure 2-13 Migration from a FEP to a CIP



Migration Scenarios

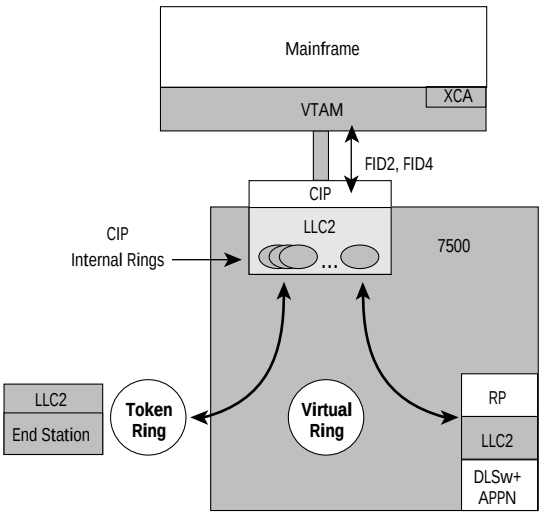
This chapter describes basic configuration and shows several sample networks. For each network, it describes the network design, explains when and why to use that network design, and in some cases briefly describes how to migrate from or coexist with a FEP. Examples include:

- Single CIP to a single host
- Dual CIP to a single host
- Multi-LPAR single CIP
- APPN network
- APPN in a sysplex environment
- SNI-to-APPN border node migration

SNA Communication over CSNA

SNA nodes communicate to the CIP using LLC2, a connection-oriented data link protocol for LANs. An LLC2 stack on the CIP card communicates with either the adjacent SNA device (over a physical Token Ring) or to DLSw+ or APPN running in the channel-attached router, as illustrated in Figure 3-1.

Figure 3-1 Communication between CSNA in the CIP and SNA Nodes



The CIP running CSNA will support multiple internal LAN interfaces, each of which looks like a LAN port to VTAM. (VTAM supports a maximum of 18 LAN ports.) However, only a single LAN port is required. CSNA also supports up to 256 open LLC2 SAPs per LAN port.

VTAM Definitions

The CIP running CSNA is not an SNA addressable node—it has no PU or LU appearance. CSNA is defined to the host control program (MVS or VM) as a channel-to-channel machine (a 3088). This provides VTAM a physical connection out to the LAN through a subchannel.

To enable VTAM communication over the CIP to SNA devices, you must configure an XCA major node and a switched major node to VTAM. The XCA major node allows VTAM to communicate with the CIP, and the switched major node definition allows SNA devices to communicate with VTAM over the CIP.

External Communication Adapter Major Node Definition

Define an XCA major node for each connection (port) between VTAM and a CSNA connection. A single XCA major node can support up to 4096 LLC2 connections, although experience has shown that better results are achieved with 3000 or fewer LLC2 connections per XCA major node. If more LLC2 connections are needed, define additional XCA major nodes. Multiple XCA major nodes can also be configured for availability, with each one pointing to a different CIP.

The CSNA feature is defined to the host control program (MVS or VM) as being a channel-to-channel adapter or machine (CTCA), for example, a 3088. VTAM identifies the CSNA gateway through a combination of the following:

- ADAPNO—Adapter number
- CUADD—Subchannel address
- SAPADDR—SAP address

```
XCANAME VBUILD TYPE=XCA              ** EXTERNAL COMMUNICATION ADAPT**
PORTNAME PORT ADAPNO=?,              ** RELATIVE ADAPTER NUMBER     ** X
                CUADDR=???,           ** CHANNEL UNIT ADDRESS        ** X
                MEDIUM=RING,          ** LAN TYPE                    ** X
                SAPADDR=4             ** SERVICE ACCESS POINT ADDRESS**
GRPNAME GROUP ANSWER=ON,              ** PU DIAL INTO VTAM CAPABILITY** X
                AUTOGEN=(5,L,P),      ** AUTO GENERATE LINES AND PUS ** X
                CALL=INOUT,           ** IN/OUT CALLING CAPABILITY   ** X
                DIAL=YES,             ** SWITCHED CONNECTION         ** X
                ISTATUS=ACTIVE        ** INITIAL ACTIVATION STATUS   **
```

Switched Major Node Definition

Configure one or more switched major nodes. Within a switched major node definition, configure every SNA PU that will access VTAM through the CIP. For each PU, configure its associated LUs. Many networks today already have the SNA devices defined in a switched major node. For example, if the devices attach to a FEP over Token Ring, they are already defined as part of a switched major node. In this case, the only change is to add the XCA major node.

```
SWMSNAME VBUILD TYPE=SWNET,           **                             X
                MAXGRP=14,            **                             X
                MAXNO=64              **
PUNAME   PU     ADDR=01,              **                             X
                PUTYPE=2,             **                             X
                IDBLK=???,            **                             X
                IDNUM=?????,          **                             X
```

```
                  ISTATUS=ACTIVE       **
LUNAME1  LU     LOCADDR=02
LUNAME2  LU     LOCADDR=03
LUNAME3  LU     LOCADDR=04
LUNAME4  LU     LOCADDR=05
LUNAME5  LU     LOCADDR=06
```

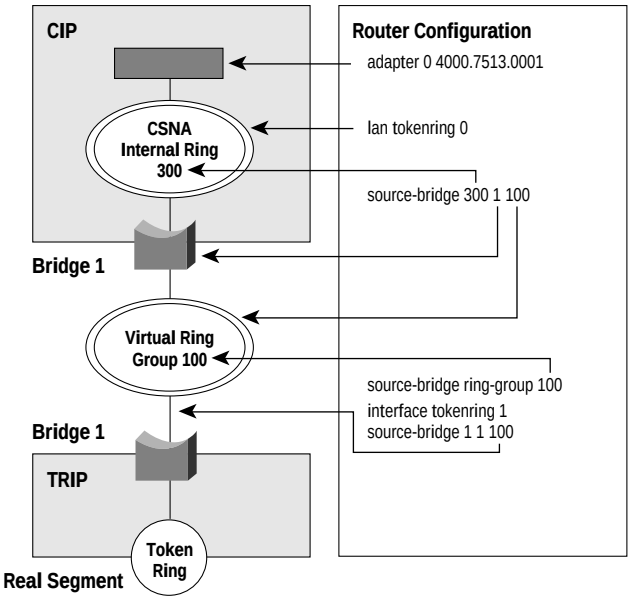
Router Configuration

The router must be configured to:

- Bridge traffic from a physical LAN or a router component (DLSw+, SRB, SR/TLB, and so forth) onto the router virtual ring
- Bridge data from the router virtual ring to one of the CIP internal rings, or connect a data link user (APPN, DSPU) to one of the CIP internal rings
- Connect the CIP to VTAM

Figure 3-2 shows the major configuration parameters of the CIP and of the Token Ring interfaces and how they are logically combined using the source-bridge definition. The CIP ring is referred to as an internal ring. The RSP ring is referred to as a virtual ring.

Figure 3-2 Using Virtual Rings to Provide Connectivity

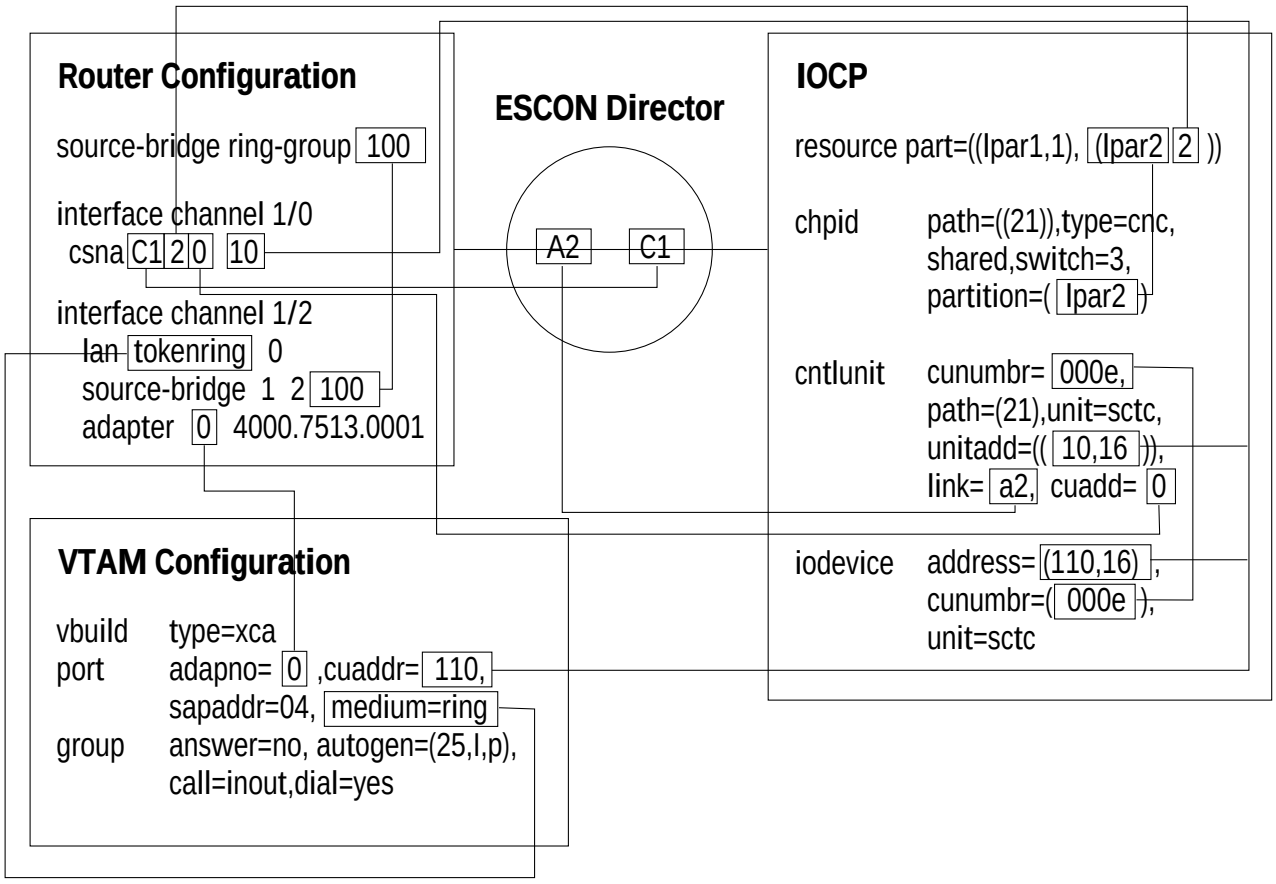


Configure an adapter on the CIP to be associated with the XCA major node definition. For each adapter configured, CSNA creates an internal Token Ring. A virtual bridge connects the CSNA internal ring to a virtual ring group in the router. The Token Ring interface processor (TRIP) is also configured to connect to the same virtual ring group as the CIP.

Configuration Relationships in the ESCON Environment

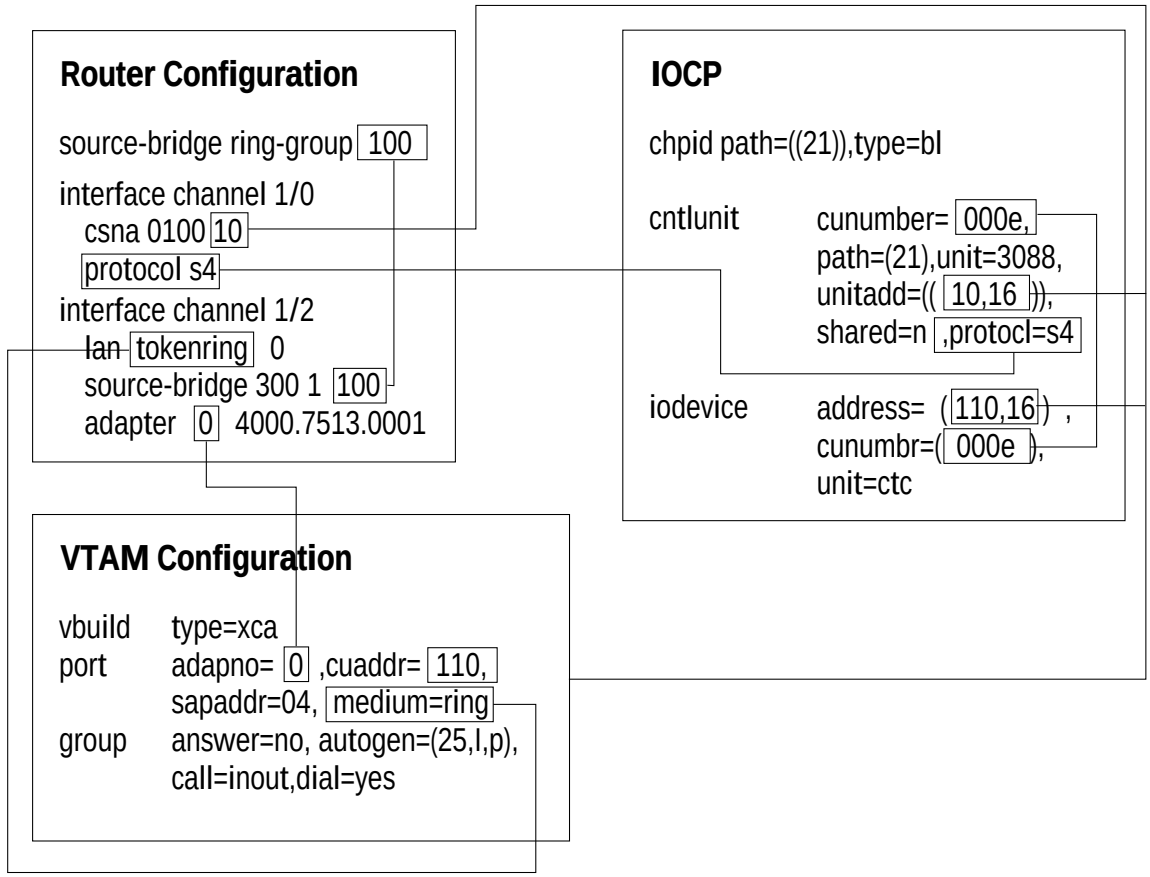
Figure 3-3 shows the relationship among router configuration, VTAM parameters, and MVS IOCP generation commands when the CIP connects via an Escon director. Figure 3-4 shows the relationship among router configuration, VTAM parameters, and MVS IOCP generation commands when the CIP connects via bus and tag.

Figure 3-3 Relationship among MVS, VTAM, and Router Configurations: ESCON



Configuration Relationships in the Bus and Tag Environment

Figure 3-4 Relationship among MVS, VTAM, and Router Configurations: Bus and Tag



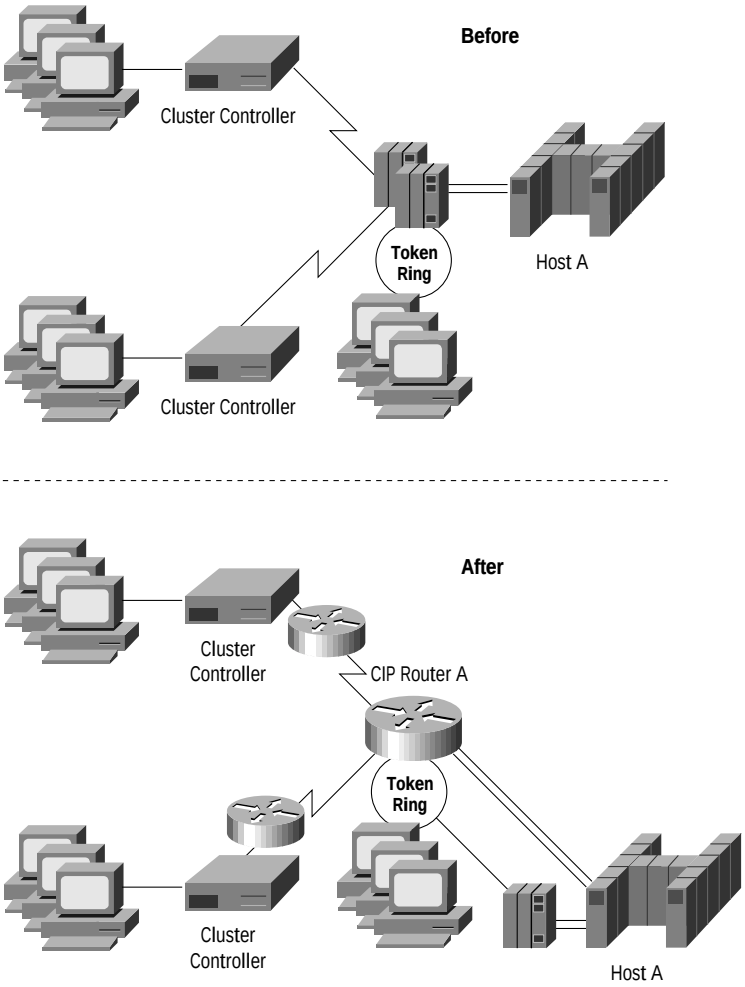
Scenario 1: Single CIP to Single Host

The first scenario is a network that replaces a FEP with a CIP. As shown in Figure 3-5, there is a single mainframe in this network. Historically, IBM SNA networks were built using the IBM FEP, and remote terminals were connected via SDLC links. In the Before scenario, a second FEP was in place for backup only.

In the After scenario, one FEP has been replaced with a channel-attached router with a CIP. Both the CIP and the remaining FEP have the same MAC address. Eventually the second FEP will also be replaced, but for now it provides SNI connectivity to a supplier and can also function as a backup to the CIP. DLSw+ is used to transport SNA traffic from remote sites to the central site.

Once data reaches the headquarters site, DLSw+ sends most traffic to the CIP, which will typically be the first to respond to explorers, but in the event that the CIP is not available, the FEP is automatically used.

Figure 3-5 Single CIP to Single Host



Reasons for Change

The FEP was at capacity and the customer preferred to use their information services dollars on technology that would carry them into the future as well as address today's requirement. In addition, the Cisco channel-attached router replacing the leased FEP would pay for itself in 18 months—with savings coming from lease costs and monthly NCP licensing costs. Migrating from an SDLC/FEP network to a LAN/channel-attached router network simplified SNA system configuration significantly and reduced the downtime for planned outages. Finally, the customer planned to use TCP mainframe applications in the near future and wanted to build an infrastructure that enabled them to do that.

Design Choices

This customer opted to combine SNA functionality (DLSw+) and WAN connections in the CIP router, because the network was very small (25 sites). The design provides a very safe fallback to the FEP, but at the same time enables SRB dynamics and configuration simplicity.

Configuration

XCA Major Node Configuration

```
XCANODE  VBUILD TYPE=XCA
PRTNODE  PORT   ADAPNO=0,CUADDR=770,SAPADDR=04,MEDIUM=RING,TIMER=30
*
GRPNODE  GROUP ANSWER=ON,                                          X
               AUTOGEN=(100,L,P),                                  X
               CALL=INOUT,                                         X
               DIAL=YES,                                           X
               ISTATUS=ACTIVE
```

Router Configuration

```
!
source-bridge ring-group 100
!
interface tokenring 1/0
 no ip address
 no ip route-cache
 ring-speed 16
 source-bridge 200 1 100
!
interface Channel1/0
 no ip address
 csna 0100 70
!
interface Channel1/2
 no ip address
 no keepalive
 lan TokenRing 0
  source-bridge 300 1 100
  adapter 0 4000.7000.0001
!
end
```

Implementation Overview

The first step is to implement DLSw+ from the remote site to the central site and to change the FEP access from SDLC to Token Ring. As part of this step, configure the VTAM switched major nodes. Once that is done, the following steps enable the CIP in this configuration:

Step 1 Perform IOCP generations to configure the channel definitions, as shown in either Figure 3-3 or Figure 3-4.

Step 2 Configure VTAM XCA major node.

Step 3 Configure the attached router with the CIP definitions and bridge traffic from the internal ring group to the CIP virtual ring.

Step 4 Vary the channel online (**Vary E00,ONLINE**).

Step 5 Confirm the CIP is online (**Display U,,,E00,1**).

Step 6 Activate the VTAM XCA (**Vary NET,ACT,ID=name_of_member**).

Scenario 2: Redundant CIP to Single Host

Initially this site had a 3745-410 running in twin-standby mode to provide better network resiliency. In this case there is one active NCP while the second one is in standby mode. The second NCP takes over only if the first NCP has problems. This allows quick recovery from storage-related failures and

from a CCU hardware check. Note that the idle CCU is totally inactive unless a failure is detected. With the inclusion of duplicate Token Ring, addressing this design can also provide another level of network redundancy.

Optionally, the 3745-410 could be configured in twin-backup mode, where each CCU controls approximately half the network. It is the equivalent of having two 210s running at half capacity. If there is a failure in one CCU, the other CCU can take over, just as in the first example. However, only half the resources are impacted and hence recovery is faster.

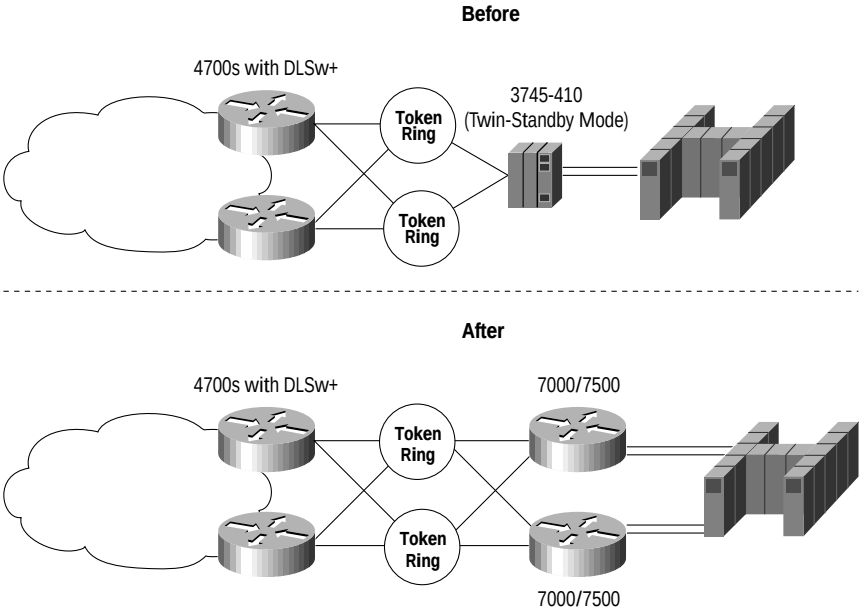
Irrespective of the configuration in use, the use of CSNA on two Cisco 7500 series routers with one or more CIP cards can provide better load sharing and redundancy features, as described in the previous chapter in the section titled “Designing for High Availability.”

The After scenario is designed so there is no single point of failure in the network. The redundant CIP to a single host scenario is often used when the end systems cannot afford the downtime of a failure. For many companies that require online access to provide 24 by 7 customer support, the loss of host access for even a short period of time can incur a significant loss in both income and credibility. It is important for these networks to implement a solution that will avoid or minimize the amount of downtime due to network problems.

Also for these companies the redundancy option provides the necessary network configuration to perform maintenance or configuration changes to the network with minimal impact to the end-system users.

Providing redundancy to the single CIP to single host solution is quite straightforward. In Figure 3-6, two Cisco 7500 routers, each with a CIP, are deployed in place of the 3745-410. In this example both CIPs have the same virtual MAC address. When one router is not available, the SNA end system will automatically find the backup router using standard SRB protocols. Note that in both the Before and the After networks, loss of a channel-attached gateway is disruptive.

Figure 3-6 Redundant CIPs to Single Host



Reasons for Change

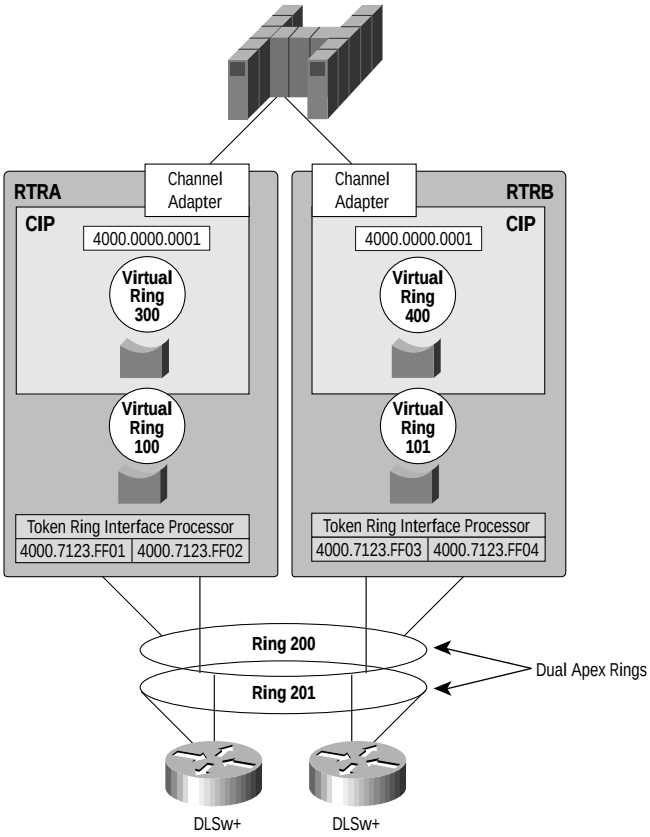
The 3745-410 did not have the capacity to support the entire network if one of the processors was down. During outages, the entire network slowed down. To address this problem with more FEPs was not cost-effective. In addition, this enterprise was considering migrating their campus to FDDI, which the 3745 does not support. With the Cisco channel-attached routers, they could migrate their campus to either FDDI or ATM in the future.

Design Choices

In this network they opted to separate DLSw+ from the channel-attached router. This minimizes both scheduled and unscheduled outages in their network. Also, they already had DLSw+ installed in these routers before they installed the CIPs. Hence, this simplified migration. Finally, as their DLSw+ routers (Cisco 4700s) reach capacity, it is less costly to add a Cisco 4700 router than a Cisco 7500 with a CIP. Either of the channel-attached routers can handle their entire capacity today, and if the network grows, they have sufficient slots in their 7500s to add CIPs to their channel-attached routers.

The network uses load balancing across central site DLSw+ routers and duplicate Token Rings to ensure there is no single point of failure, as shown in Figure 3-7.

Figure 3-7 Dual Routers with Duplicate MACs



Router Configuration

This configuration uses the same MAC address on internal Token Ring LANs of two different routers.

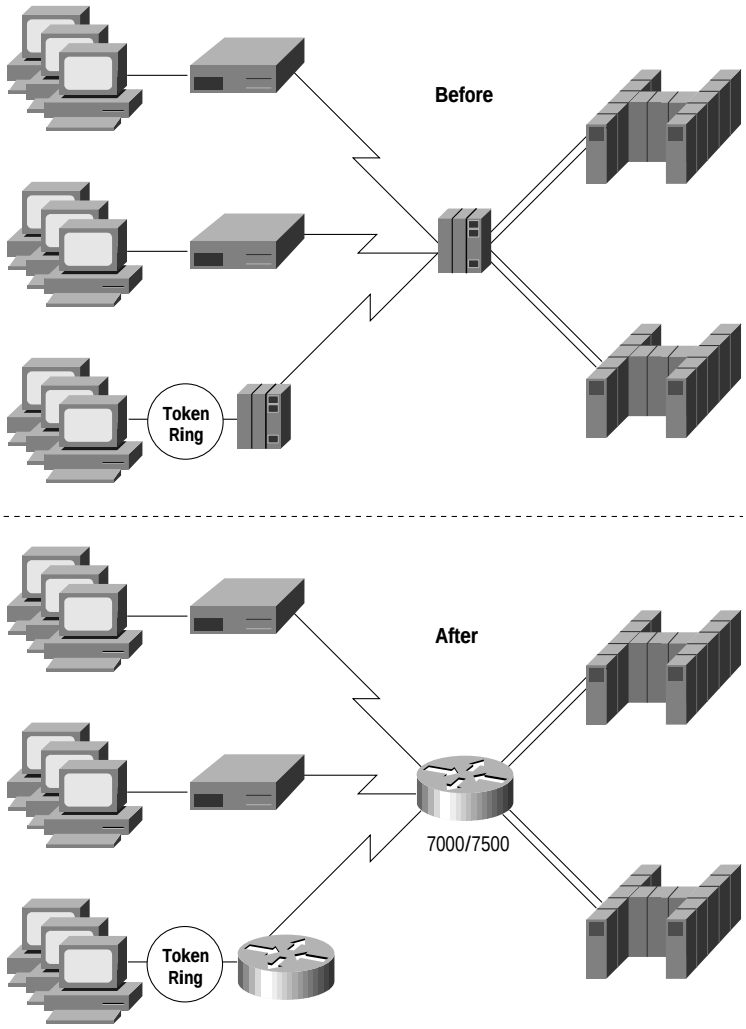
```
 RTRA
!
source-bridge ring-group 100
int tok 0/0
source-bridge 200 1 100
int tok 0/1
source-bridge 201 2 100
!
interface Channel1/0
 no ip address
 csna 0100 70
!
lan TokenRing 0
  source-bridge 300 1 100
  adapter 0 4000.0000.0001
!

 RTRB
!
source-bridge ring-group 101
int tok 0/0
source-bridge 200 1 101
int tok 0/1
source-bridge 201 2 101
!
interface Channel1/0
 no ip address
 csna 0100 80
!
lan TokenRing 0
  source-bridge 400 1 101
  adapter 0 4000.0000.0001
!
```

Scenario 3: Single CIP to Multiple Host

This scenario shows a legacy SNA network with several remote sites connected via SDLC links to cluster controllers. Also, a high-speed line was connected to a remote 3745 at a site that demanded high-speed connection back to the mainframe and had more remote users than a cluster controller could support. This enterprise also had a separate multiprotocol network running in parallel.

At the data center, there are two VTAMs. One is used primarily for production and the other used primarily for testing. There is little, if any, cross-domain routing. Figure 3-8 shows the Before and After networks.

Figure 3-8 Replacing a Single FEP with a Channel-Attached Router



Reasons for Change

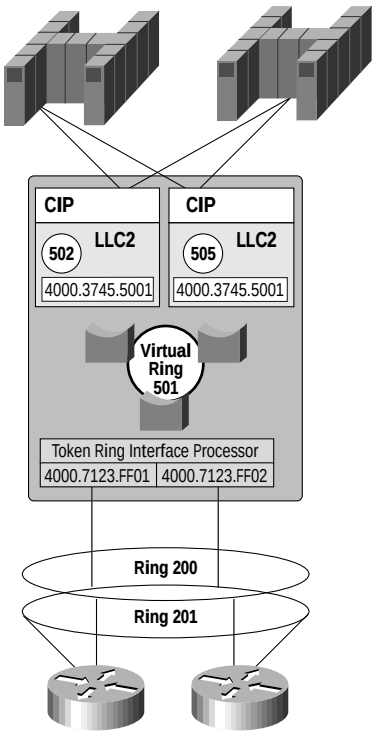
The primary reasons for change were to minimize costs and increase throughput and flexibility. The remote 3745 was replaced with a lower-cost Cisco 4500 router to eliminate recurring NCP and maintenance charges, consolidate multiprotocol and SNA WAN traffic, and simplify network configuration. The central site FEP was replaced with a channel-attached router to increase channel throughput and to enable TCP/IP on the mainframe in the future.

Design Choices

This enterprise chose not to implement APPN even though they had multiple mainframes. The reason is that all SNA sessions were in the same domain. The VTAM in the second mainframe was simply used for testing and backup. They chose not to implement two channel-attached routers for redundancy, but they did select to use two CIPs in a single channel-attached router. This created higher availability than they had previously, and provided an option in the future to separate CIP

functionality across multiple CIPs. In the future they plan to add TN3270 server capability to the CIP to allow access to VTAM applications from Web-based clients, and they also anticipate a need for TCP/IP on the mainframe. Figure 3-9 shows the logical configuration.

Figure 3-9 Dual CIPs in a Single Router



Router Configuration

```
!
source-bridge ring-group 501
int tok 0/0
 source-bridge 200 1 501
int tok 0/1
source-bridge 201 2 501
!
interface Channel1/0
 no ip address
 csna 0100 70
!
interface Channel1/1
 no ip address
 csna 0101 80
!
interface Channel1/2
 no ip address
 no keepalive
 lan TokenRing 0
  source-bridge 502 1 501
  adapter 0 4000.3745.5001
lan TokenRing 1
  source-bridge 505 1 501
  adapter 1 4000.3745.5001
!
```

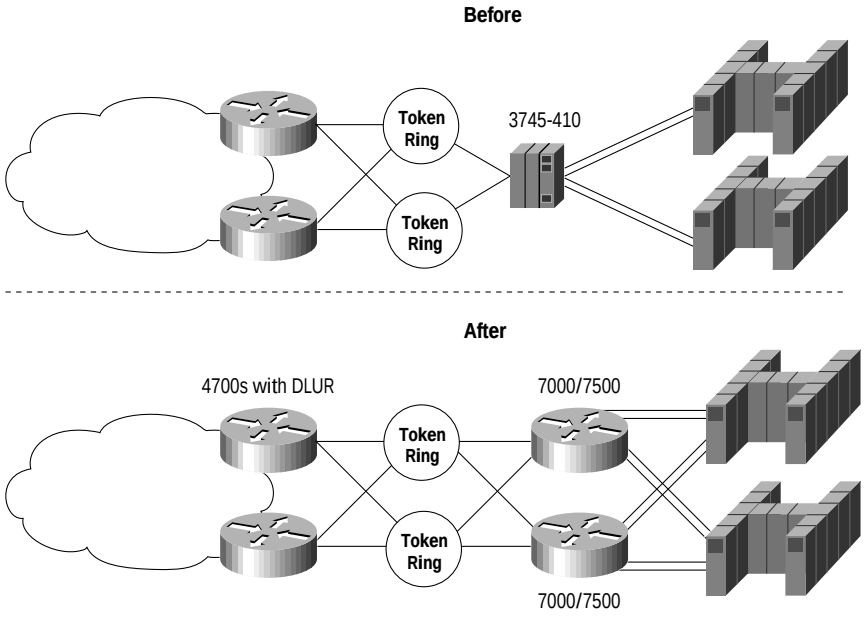
Scenario 4: Migrating to APPN

In the Before environment, the FEP provided SNA routing. The FEP can be replaced without loss of function by implementing APPN in a channel-attached router. APPN was being considered for this data center even if the FEP were not being replaced. Recent enhancements to VTAM's APPN implementation simplify network definition and enhance availability.

This scenario shows the replacement of the FEP with a Cisco router running APPN/DLUR. One host is configured as an NN and the other as an EN. The NN provides NN server function for the EN and provides DLUS functionality. Figure 3-10 illustrates this scenario.

Note For more detail on APPN, refer to the Cisco *APPN Design and Implementation* guide.

Figure 3-10 APPN Scenario



Reasons for Change

This enterprise was interested in simplifying their SNA network and reducing their FEP dependency to reduce costs. They also wanted to improve throughput at the data center. Although they were starting with APPN/ISR routing, they intend to migrate to HPR in the future. With HPR, loss of a channel gateway, LAN adapter, or channel adapter can be dynamically recovered without disrupting end-user sessions.

Design Choices

This enterprise chose to put DLUR functionality in their existing data center routers to maximize the scalability of their channel-attached routers and minimize the cost of their total network. In addition, when they migrate to HPR, this design will allow them to nondisruptively reroute around the failure of a channel-attached router by configuring the channel-attached router as an ANR node.

Router Configuration

This partial router configuration shows that there are three required parameters and one optional parameter for defining an APPN connection. Refer to the VTAM configuration manuals for more details on the changes required to VTAM.

The **APPN CONTROL-POINT** command is used to identify the router.

The **LINK-STATION** defines the connection to the router. (This statement is required in at least one of two APPN nodes connected over a link.)

The **PORT** defines a point of connection into the APPN network.

The **APPN ROUTING** command is optional and will automatically start APPN routing when the router is started.

4700 Router Configuration

```
version 11.0
!
hostname RTRA
!
enable password cisco
!
appn control-point NETA.RTRA
dlus NETA.VTAMA
 dlur
 complete
!

!
appn link-station linkA
complete
!
appn port porta dlsw
complete
!
appn routing
!
end
```

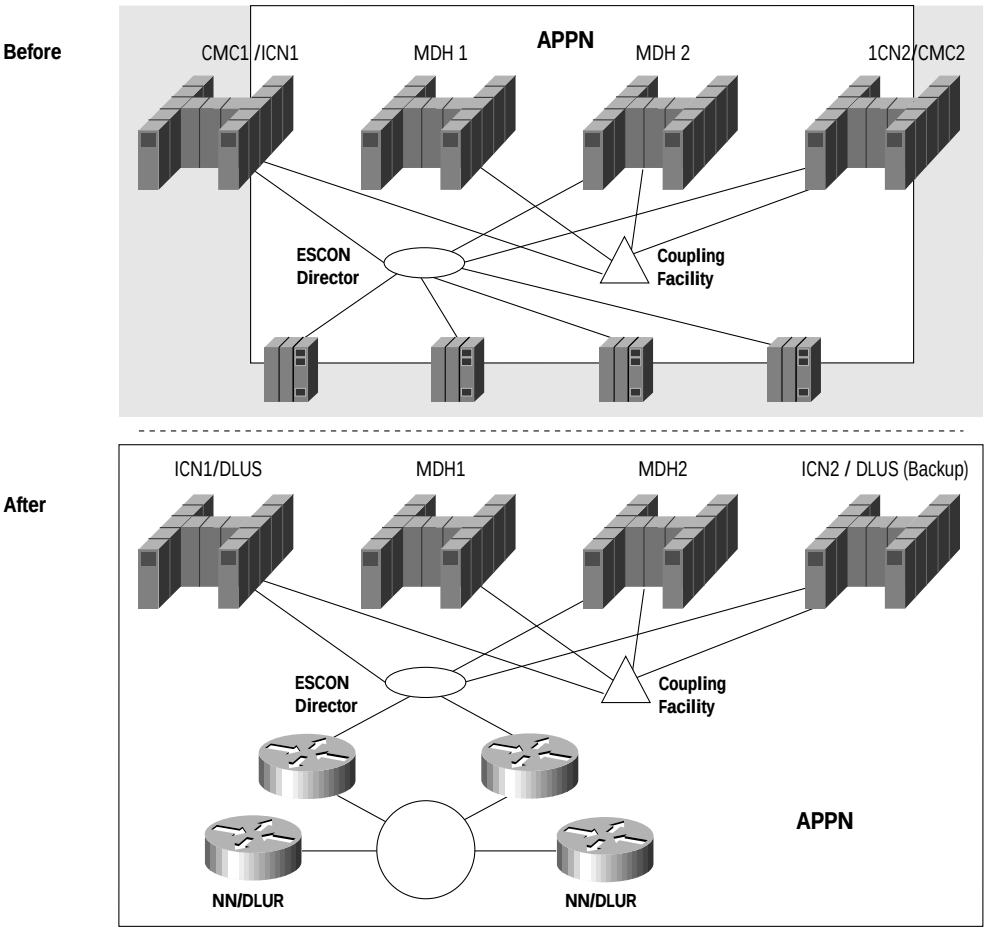
APPN in a Parallel Sysplex Environment

APPN is required in VTAM, at a minimum, in order to take advantage of a Parallel Sysplex environment. In the Before picture illustrated in Figure 3-11, APPN is implemented in each VTAM host, while the FEPs and the rest of the network continue to use subarea protocols. This environment allows SNA sessions to take advantage of generic resources. The Generic Resource feature of VTAM enables end-user sessions to be dynamically spread across alternate, identical images of an application. The end user logs on to a generic resource (for example, CICS), and the CMC host (which is also an ICN) establishes the session with a specific application (perhaps CICS01) running in one of the migration data hosts. The CMC/ICN balances CICS sessions across all the sysplex processors, and recovery from the failure of any single processor is disruptive but dynamic. In VTAM V4R4 and the latest CICS, this recovery will be nondisruptive, using a facility know as Multi-Node Persistent Sessions (MNPS).

In the After picture shown in Figure 3-11, data center routers provide DLUR function for legacy traffic. The Cisco channel-attached router can handle the capacity of multiple FEPs, so there are only two channel-attached routers in the After picture. The DLUR function was installed in existing data

center routers to maximize scalability and availability. The DLUR router routes traffic directly to the correct migration data host using APPN routing. (In the After picture, if there were really no FEPs, you could convert the ICNs to NNs and the MDHs to ENs.)

Figure 3-11 Parallel Sysplex Environment



Scenario 5: Migrating from SNI to APPN

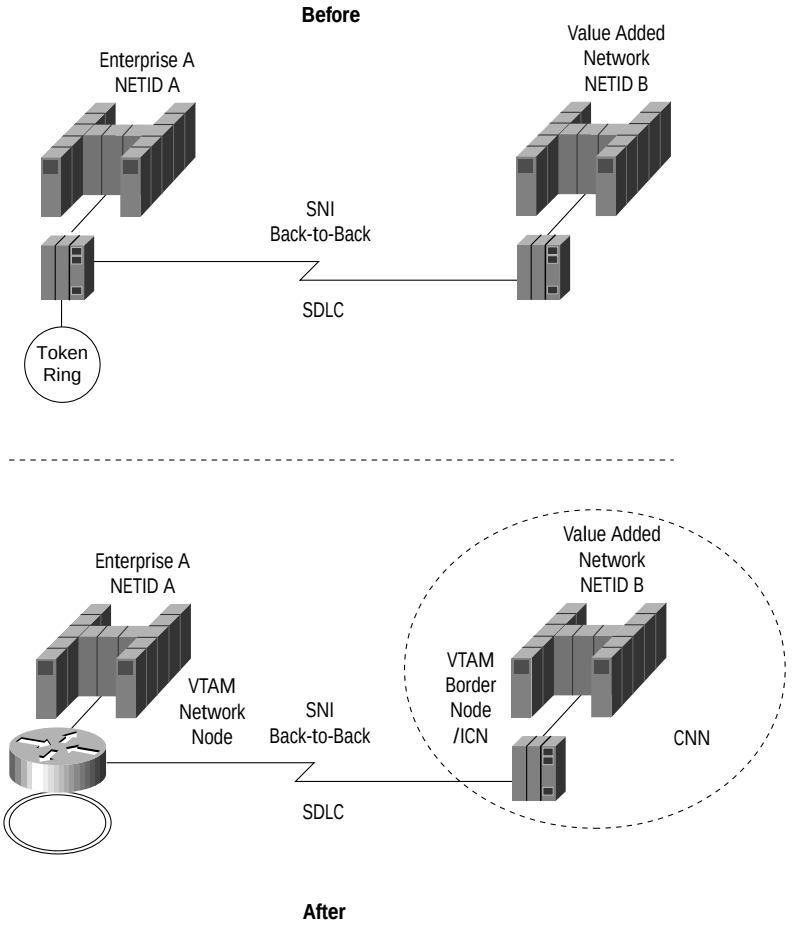
In the Before environment, Enterprise A connected to a value-added network over a back-to-back SNI connection. Enterprise A had a small network with a single FEP. They wanted to eliminate the FEP, but they were using it for SNI.

In the After environment, the FEP in Enterprise A has been replaced with a Cisco channel-attached router. In the first phase, the router was configured for local DLSw+ conversion from LAN to SDLC. In the second phase, for which the configuration in Figure 3-12 applies, APPN/DLUR functionality was added to allow the channel-attached router to directly route all steady-state session traffic going to the value-added network, without requiring VTAM. In the value-added network, VTAM migrated to become an ICN. It continues to use subarea protocols for attaching to other networks,

but uses APPN for attaching to this network. In the future, as more enterprises select this connectivity option, the value-added network provider hopes to replace some FEPs with Cisco channel-attached routers.

Note For more detail on APPN, refer to the Cisco *APPN Design and Implementation* guide.

Figure 3-12 SNI Scenario



Reasons for Change

Enterprise A was interested in reducing their FEP costs. The value-added service provider had a large number of FEPs supporting SNI, and by migrating one customer, they only put a small dent in their FEP SNI traffic. However, they also recognized that as soon as one migration was successful, they could offer this alternative to other clients. They were willing to do this for Enterprise A in the hopes that it would allow them to migrate other customers in the future.

Design Choices

Enterprise A and the value-added service provider chose to use the border node (BN) function of APPN. They selected this alternative because Enterprise A was already migrating to APPN/DLUR, and this option gave them the most application flexibility (either session end could initiate the connection) while at the same time providing topology independence. Additional design alternatives for SNI are discussed in the section, "The Cisco Channel-Attached Router as a FEP Alternative" in the chapter, "Introduction to SNA on the CIP."

Router Configuration

The following shows the router configuration in the final phase.

```
interface Channel 1/0
 no ip address
 no keepalive
 csna 0100 00

interface Channel 1/2
 no ip address
 no keepalive
 lan TokenRing 0
 source-bridge 7 1 1000
 adapter 0 4000.7507.0000

interface Serial4/0
 no ip address
 encapsulation sdlc
 no ip route-cache optimum
 bandwidth 64
 no keepalive
 nrzi-encoding
 sdlc vmac 4000.3745.0000
 sdlc address 01
 sdlc partner 4000.7507.0000 01
 sdlc dlsw 1

appn control-point NETA.CP7507
 dlus NETA.VTAMA
 dlur
 complete
!
appn port CIP rsrb
 desired-max-send-btu-size 1500
 max-rcv-btu-size 1500
 retry-limit infinite
 rsrb-virtual-station 4000.7507.0001 6 1 1000
 complete
!
appn port SDLC0 Serial4/0
 sdlc-sec-addr 02
 complete
!
appn link-station VANFEP
 port SLDC0
 retry-limit infinite
 sdlc-dest-address 0
 complete
!
appn link-station VTAMA
 port CIP
lan-dest-address 4000.7507.0000
retry-limit infinite
```

```
complete
!
appn routing
!
end
```

Network Management

This section describes tools that are available to manage Cisco channel-attached routers, CIPs, and Cisco router networks. It also compares these tools to tools that are commonly used to manage an NCP.

CiscoWorks Blue

CiscoWorks Blue is a suite of network management products that support management of integrated SNA and router networks. The key products in this suite include:

- CiscoWorks Blue Native Service Point and optionally CiscoWorks SNA View for management of the network from the host platform. SNA View is only required if you want to view the SRB RIF from the host.
- CiscoWorks Maps in conjunction with SNA View for management from a distributed management platform
- Internetwork Performance Monitor for end-to-end performance management

These tools will speed problem identification, simplify problem isolation, and enable trend analysis. They also simplify event correlation by consolidating the SNA view and the router view on a single console of your choice. In addition to these tools, simple **show** commands can be used to query CIP traffic statistics, memory utilization, and cycle utilization. A brief summary of each product follows.

CiscoWorks Blue Native Service Point

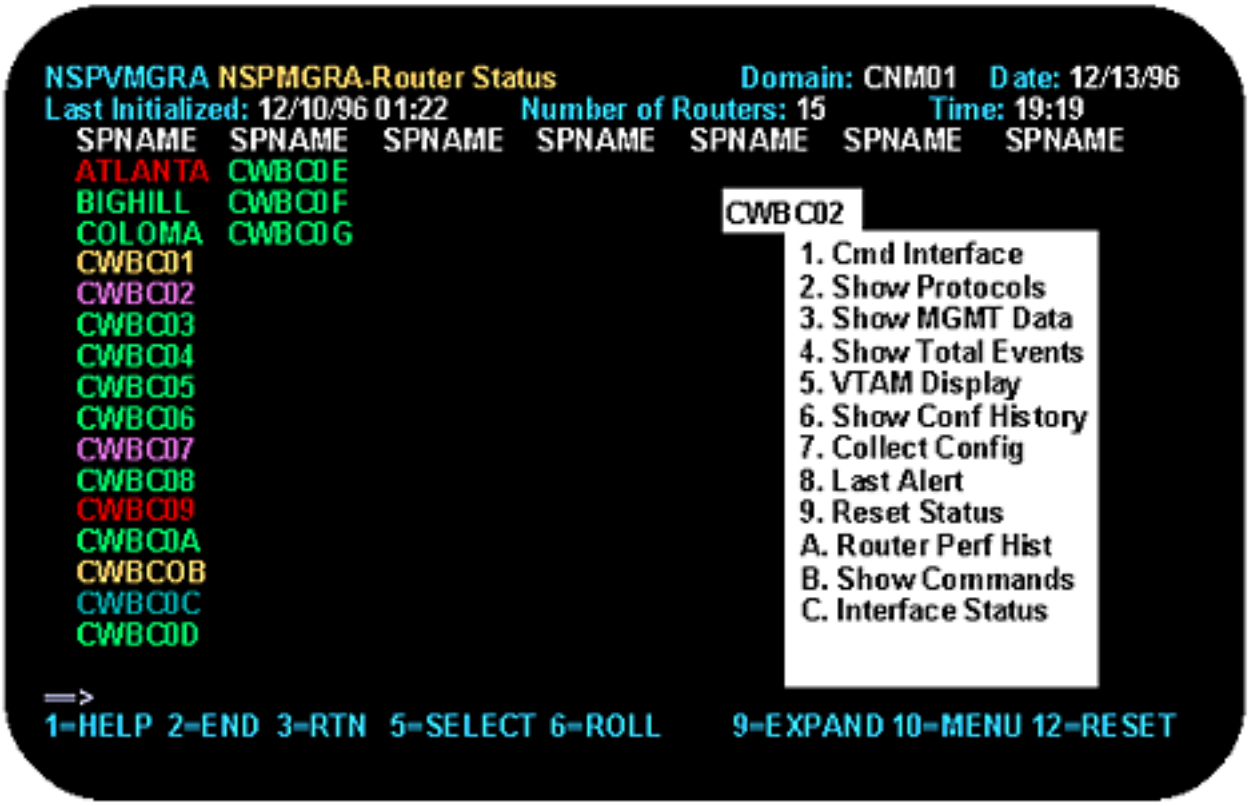
Native Service Point Release 2.0 enables Sterling SOLVE:Netmaster or IBM NetView/390 operators to have full visibility of a Cisco router network from a single mainframe console, regardless of whether that router network is routing SNA traffic. To use Native Service Point to manage a channel-attached router, you must install the service point feature on the router. This feature gives the router the appearance of a PU 2.0 device. The service point feature on the router enables the router to send SNA alerts to your host SNA management product and to accept run commands **(RUNCMDs)** from it.

Native Service Point is an application that runs on top of Sterling's SOLVE:Netmaster or IBM's NetView. Using this product, commands traditionally entered at the router console can be issued from the mainframe console. Native Service Point then converts these commands to **RUNCMDs**. The router responds to a **RUNCMD** with a network management vector table (NMVT) request unit and the router responses are displayed to the mainframe operator as a full-screen panel response.

In addition to responses to **RUNCMD**, the router transports NMVT unsolicited alerts to the mainframe where they are displayed by the NetView or SOLVE:Netmaster event display features.

To manage routers from NetView for MVS or SOLVE:Netmaster, a VTAM connection must be established for each router, and the appropriate service point must be defined in the configuration file of each router using Cisco IOS software SNA interface commands. Figure 4-1 shows an Native Service Point screen.

Figure 4-1 Native Service Point Main Screen



Native Service Point provides the following from a mainframe console:

- Cisco router management and performance monitoring of all the routers being monitored by Native Service Point via the service point function. The color of the service point name of a router indicates the status of that router. Status includes up, down, connect, performance degraded, interface down, and alert received. This status panel also includes a command pop-up menu, which makes some of the most commonly used router diagnostic commands easily accessible to a mainframe operator.
- Security Options Through Easy-to-Use Setup Panels—Operators can be authorized to change router configurations; in cases where multiple operators manage a large network, some operators can be restricted to view-only access.
- Router Grouping—To facilitate scope of control, the routers displayed on operator status panels can be grouped based on profile definitions; operator displays can be modified to show groups of user-defined routers, allowing segmentation of responsibility

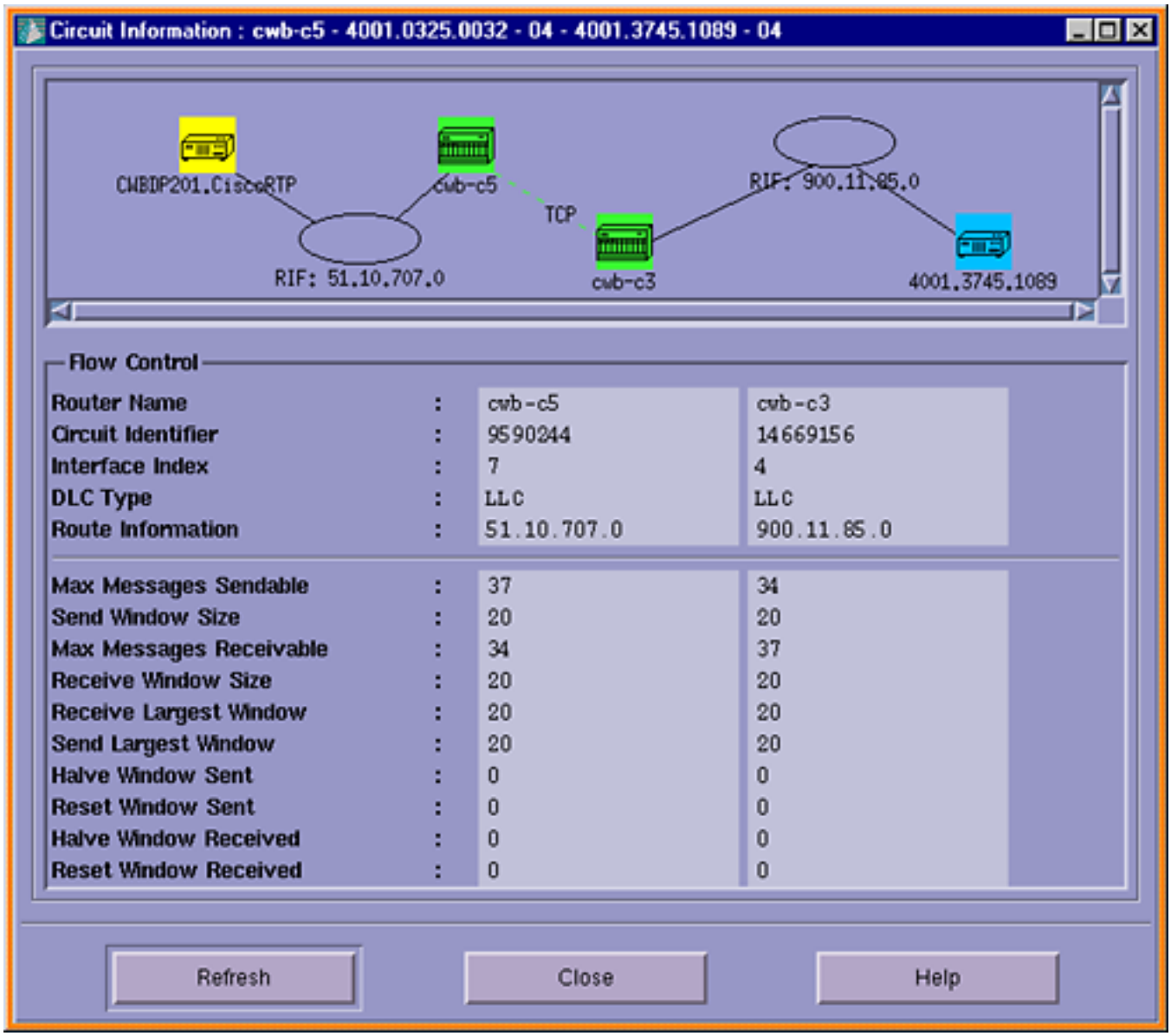
- Correlation of Events—Router events forwarded to the mainframe by Cisco IOS software are correlated with the managed routers, allowing operators easy selection of those alerts that apply to a particular router
- DSPU and CIP Management Assistance—Cisco IOS software commands that are typically used to diagnose CIP and DSPU problems are available via a full-screen interface to make management of these devices simpler.
- A command-line interface enables mainframe operators to connect to and issue any commands to a router that they would normally issue via a Telnet session to the router. This command-line interface does not require TCP/IP at the mainframe.
- Filters that allow exception viewing.
- Interface Performance Monitoring—Performance data is periodically collected from routers and interfaces at user-defined intervals and is viewable from a variety of Native Service Point panels.
- Router and Interface Statistics Archiving—Performance statistics for both routers and the interfaces enabled in those routers are logged in virtual storage access method (VSAM) data sets that can be used later for performance analysis.
- Configuration Archiving—Router configurations can be logged in a VSAM database for later use in problem diagnosis and disaster recovery.
- RIF Archiving—If CiscoWorks Blue SNA View Release 1.1 is installed, operators can display route information for sessions that pass through the routers being managed by Native Service Point.

CiscoWorks Blue Maps and SNA View

For those customers that want to manage SNA resources from a distributed management platform, Cisco offers CiscoWorks Blue Maps and SNA View. Maps provides a graphical representation of the routers providing SNA transport via either APPN, DLSw+, or RSRB. SNA View allows you to monitor and control all the SNA PUs and LUs in your network from an Simple Network Management Protocol (SNMP) console.

SNA View includes a program operator application that allows communication between your SNMP manager and VTAM, allowing you to display status and activate or inactivate SNA resources. In addition, you can display the dependency view of how those SNA resources are connected over a Cisco router network, providing a simple, graphical means to correlate events. Figure 4-2 shows an example of the view dependency screen.

Figure 4-2 SNA View Dependency Screen



Internetwork Performance Monitor

With the introduction of CiscoWorks Blue Internetwork Performance Monitor, network managers now have the tools they need to isolate performance problems, locate bottlenecks, diagnose latency, and perform trend analysis in the network. With Cisco IOS Release 11.2, Internetwork Performance Monitor can find the possible paths used between two devices and display the performance for each of the hops in each path.

Internetwork Performance Monitor measures both IP connections and SNA sessions. By providing network managers with the capability to collect "on-demand" response time data, as well as long-term trending information, Internetwork Performance Monitor can remove some of the guesswork from response time management and diagnosis, enabling network managers to provide a consistent level of network response time to network users.

Management Comparison: Channel-Attached Router and CIP/3745 and NCP

This section compares the service aids provided by IBM for NCP with the service aids that are available for a similar CIP/router configuration. The functions that are examined are:

- Alerts
- Statistics
- Console support
- Trace/debug
- Connectivity test
- Memory display/dump
- Recovery
- Performance monitoring
- Configuration management
- Router configuration for host management

Alerts

Alerts are either generated by or passed through the NCP to VTAM. In VTAM, the alerts are forwarded to either NetView or SOLVE:Netmaster. Both the NCP and the CIP (via service point) provide alerts when a resource fails. NCP generates alerts for all the resources that it manages. NCP will also forward alerts received from an external resource. The NCP does not create traps or support SNMP. The CIP/router will provide alerts for SNA resources, and some traps are converted to alerts. It also creates traps for all the alerts. Table 4-1 compares NCP and CIP alerts.

Table 4-1 Alerts

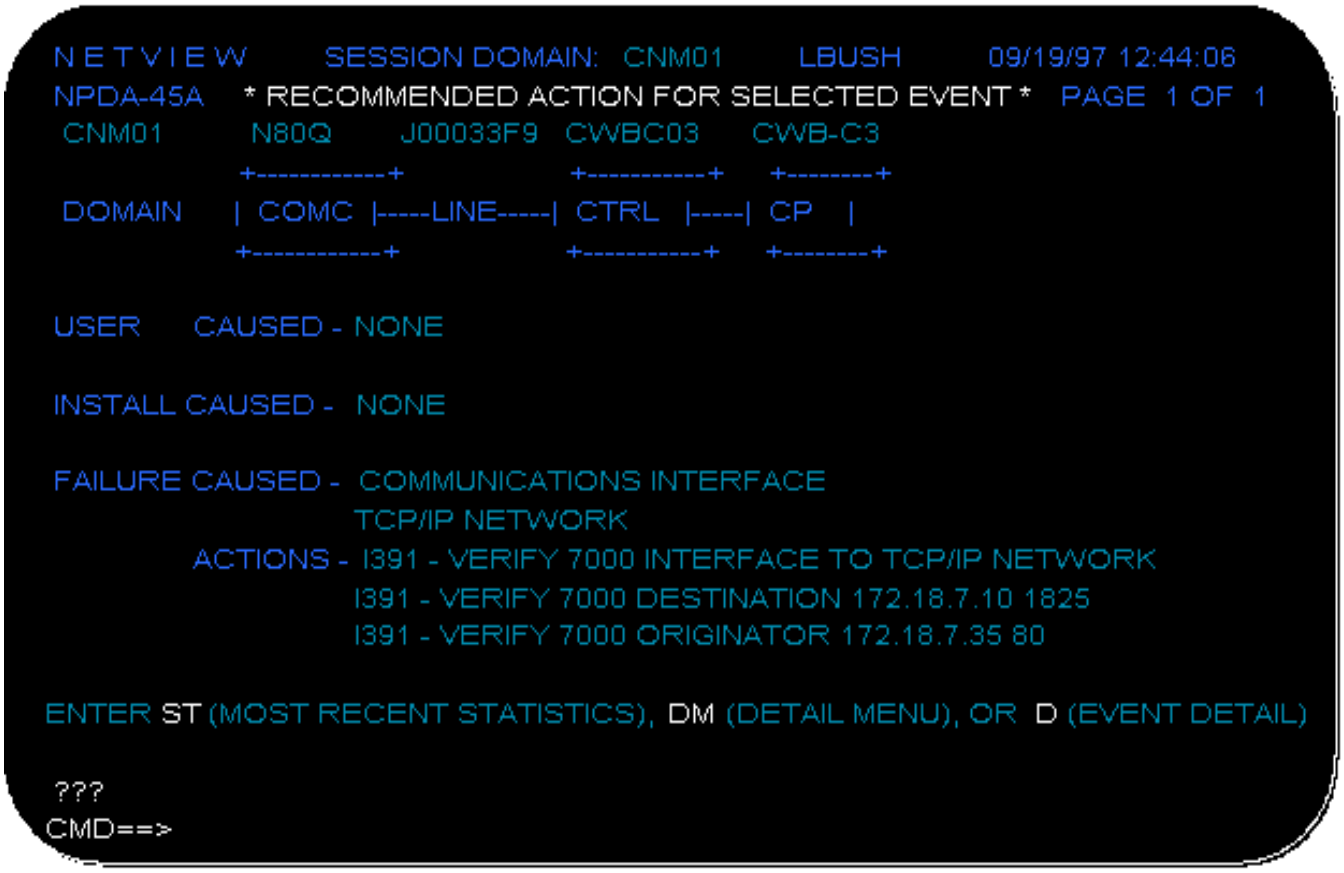
Alert Support Comparison	NCP	CIP
Local Interface Failure	Yes	Yes
Downstream Alerts	Yes	Limited
Resolved Alerts	No	Possible (NSP* with Syslog)
Threshold	Slowdown	Possible (NSP)

*NSP stands for the Cisco product Native Service Point.

NCP has the ability to generate alerts for soft errors when intensive-mode recording (IMR) is initiated from VTAM.

Figure 4-3 shows an example of an alert received from a router.

Figure 4-3 NetView Alert Screen



Statistics

NCP provides statistics for all links, lines, and PUs. NetView provides the ability to also log the statistics to SMF.

NCP provides statistics for the following conditions:

- Whenever the NCP is shut down normally
- Whenever a resource fails or is made inactive
- Whenever a counter is filled that relates to the interface, such as traffic or soft errors

Statistics Summary

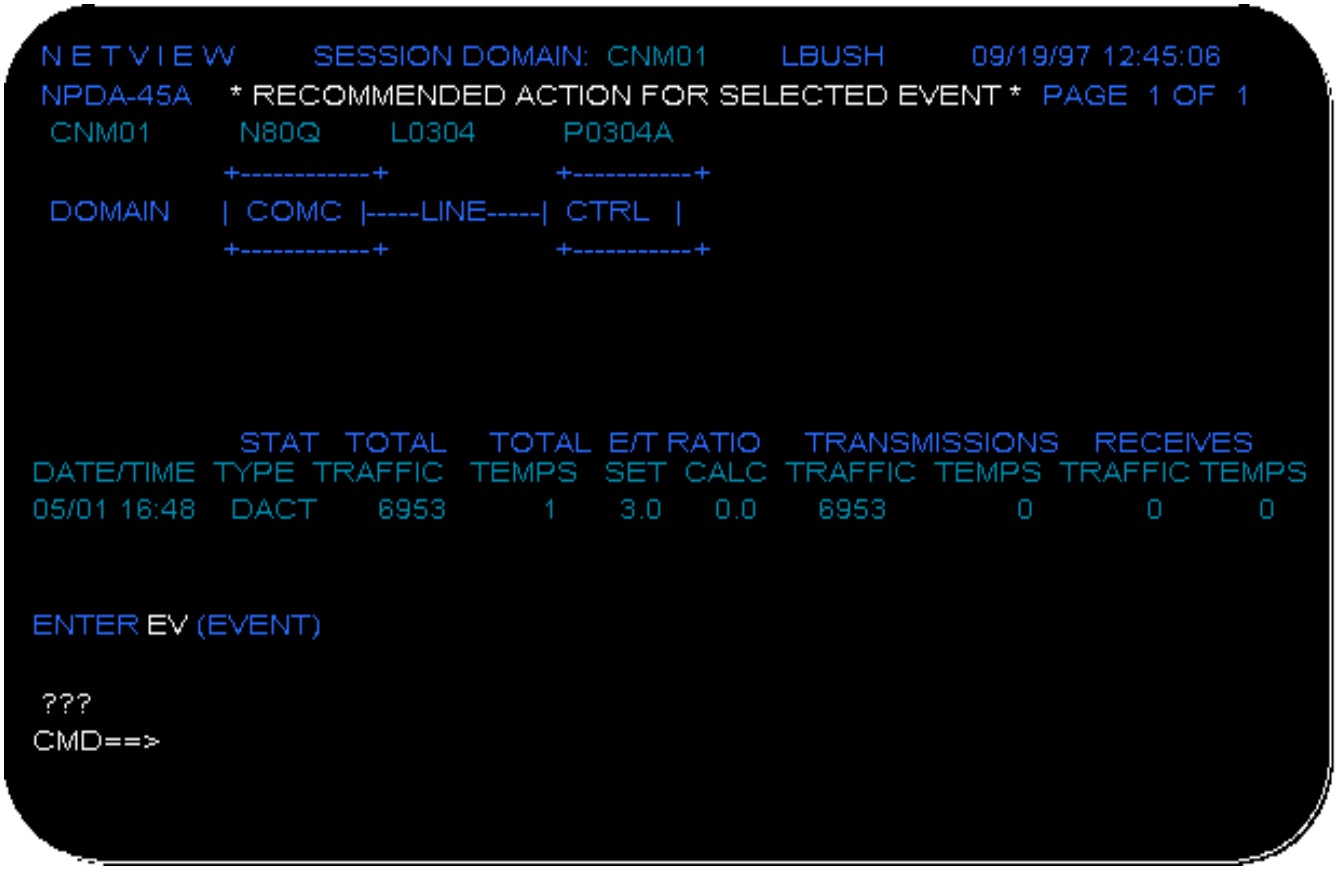
Table 4-2 Statistics Summary

Statistics Summary	NCP	CIP
End of Day (EOD)	Yes	No
Threshold	Yes	No
Solicited	No	Yes (NSP*)
Archived	Yes (NPDA)	Yes (NSP)

*NSP stands for the Cisco product Native Service Point.

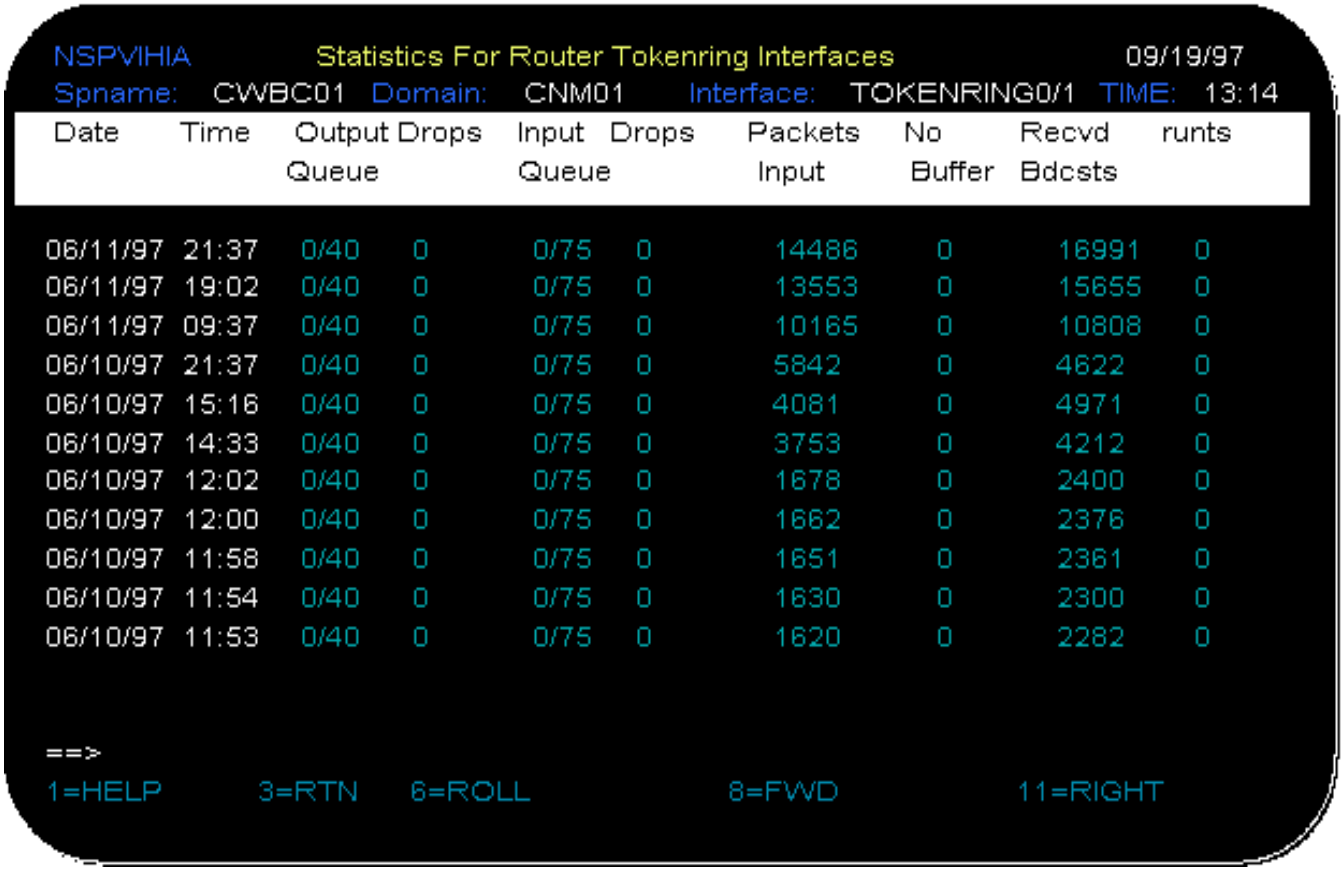
Figure 4-4 is an example of a statistics record for an NCP managed resource.

Figure 4-4 Statistics Record for an NCP-Managed Resource



Native Service Point provides the ability to collect statistics based on user-defined intervals. Router CPU and memory utilization data is collected and archived. Interface statistics also can be collected and archived. Figure 4-5 shows an example of records collected for an Native Service Point-managed interface.

Figure 4-5 Native Service Point Interface Statistics



Console Support

The FEP allows attachment of a console that can be used for service support of the FEP. The console (MOSS) has limited functional use with the FEP. It is not supported by NCP. It also requires high technical skill because it is primarily used to display and alter storage on the FEP.

The CIP/router has various options. A terminal can be attached to the router console interface. A terminal can be attached via a Telnet session. NetView or SOLVE:Netmaster can be attached as a console when the service-point function is implemented in the router. The console support for the router allows all router functions to be performed.

The MOSS console is usually located next to the FEP, and access to the console is usually restricted. The console support for the router can be local or remote and has security features to control accesses and command level.

Table 4-3 Console Support

Console Support	NCP	CIP/Router
Console	Yes (MOSS)	Yes
Telnet Access	No	Yes
NetView Access	Yes	Yes (RUNCMD)

Trace/Debug

VTAM provides trace facilities that can be used to trace either the NCP or a CIP. NCP has a line trace that is initiated from VTAM. The output is sent back to VTAM and recorded using the Generalized Trace Facility (GTF). Table 4-4 contrasts the trace/debug support of the NCP and CIP/Router.

Table 4-4 Trace/Debug

Trace/Debug	NCP	CIP/Router
Data Trace	Yes (VTAM)	Yes (VTAM)
Line Trace	Yes (VTAM)	No (See debug)
Packet Trace	No	Yes (DEBUG)

The router provides various debug facilities that allow detailed problem determination. In most cases the debug facility requires an authorized operator. It is recommended that trace type of debug operations be done through a Telnet session rather than across the service point interface.

The Cisco IOS software provides extensive debug facilities. Table 4-5 provides a list of some of the debug facilities provided by the router that might be encountered in an IBM environment.

Table 4-5 Cisco IOS Software Debug Facilities

Facility	Description
aaa	AAA authentication, authorization, and accounting
access-expression	Boolean access expression
all	Enable all debugging
appn	APPN debug commands
arp	IP ARP and HP probe transactions
async	Async interface information
atm	ATM interface packets
broadcast	MAC broadcast packets
bsc	BSC information
bstun	BSTUN information
cBus	ciscoBus events
callback	Callback activity
cdp	CDP information
channel	Channel interface information
compress	COMPRESS traffic
custom-queue	Custom output queueing
dhcp	DHCP client activity
dialer	Dial on demand
dlsw	DLSw events
dnsix	Dnsix information
domain	Domain Name System

Table 4-5 Cisco IOS Software Debug Facilities (Continued)

Facility	Description
dspu	DSPU information
dxi	atm-dxi information
eigrp	EIGRP protocol information
entry	Incoming queue entries
ethernet-interface	Ethernet network interface events
fastethernet	Fast Ethernet interface information
fddi	FDDI information
filesys	File system information
frame-relay	Frame Relay
fras	FRAS debug
ip	IP informatio
ipc	Interprocess communications debugging
ipx	Novell/IPX information
kerberos	KERBEROS authentication and authorization
lane	LAN Emulation
lapb	LAPB protocol transactions
list	Set interface or/and access list for the next debug command
llc2	LLC2 information
lnm	LAN Network Manager information
lnx	Generic QLLC/LLC2 conversion activity
local-ack	Local acknowledgement information
modem	Modem control/process activation
nbf	NetBIOS information
ncia	Native Client Interface Architecture (NCIA) events
netbios-name-cache	NetBIOS name cache tracing
nhrp	NHRP protocol
ntp	NTP information
packet	Log unknown packets
pad	X25 PAD protocol
ppp	Point-to-Point Protocol (PPP) information
priority	Priority output queueing
qllc	QLLC debug information
radius	RADIUS protocol
rif	RIF cache transactions
rtr	RTR monitor information
sdlc	SDLC information
sdllc	SDLLC media translation
serial	Serial interface information

Table 4-5 Cisco IOS Software Debug Facilities (Continued)

Facility	Description
smf	Software MAC filter
sna	SNA information
snapshot	Snapshot activity
snmp	SNMP information
source	Source bridging information
spanning	Spanning-tree information
tbridge	Transparent bridging
telnet	Incoming Telnet connection
tftp	TFTP packets
token	Token Ring information
vlan	VLAN information
x25	X.25 information

Connectivity Test

Connectivity test allows the user to verify a remote connection. In the SNA world, NPDA provides some functions that allow this. The LPDA function was added to support modems that have the LPDA feature.

The router provides the ability to ping a remote resource if it has an IP address. In addition, Internetwork Performance Monitor can do connectivity tests and report exceptions.

Memory Display/Dump

VTAM provides two types of facilities to obtain memory information from the NCP.

1 Display storage:

DISPLAY NET,NCPSTOR,ID=&NCP,ADDR=&ADR,LENGTH=&LEN

NetView provides a CLIST (NCPSTOR) to simplify the use of this command:

```
Command>
NCPSTOR NCP572P,260

Response>
 IST097I NCPSTOR ACCEPTED
 IST244I NCP STORAGE FOR ID = NCP572P
 IST245I 000260 81C2282F 104828AE 415CF00F 991528B3
 IST245I 000270 0108E1F0 80804154 A821D410 25B9F2A0
```

2 Dump an active NCP:

MODIFY NET,DUMP,&OPTIONS

NetView provides a CLIST (NCPDUMP) to simplify the use of the command.

```
Command>
NCPDUMP NCP1,DYNA,PDS=NCPDUMP
```

The router provides the ability to dump router memory. The options that are available for the **show mem** command are:

allocating-process	Show allocating process name
dead	Memory owned by dead processes
fast	Fast memory stats
free	Free memory stat
io	IO memory stats
multibus	Multibus memory stats
pci	PCI memory stats
processor	Processor memory stats
summary	Summary of memory usage per alloc PC

Recovery

When an NCP fails or an interface on an NCP fails, automation routines must be added to do the recovery. Without automation, the interfaces will stay inactive and NCP does not try to recovery the interface.

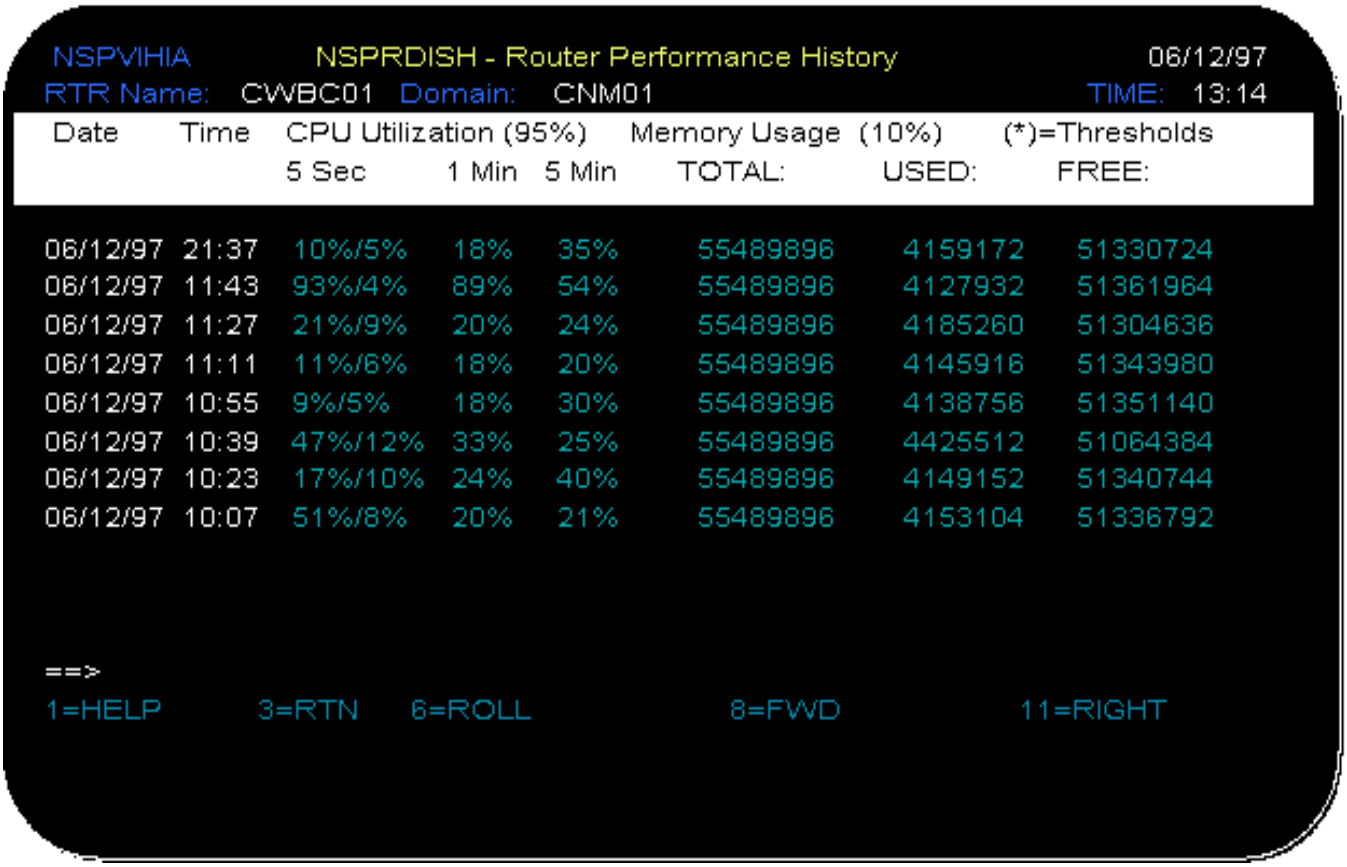
On the Cisco router, interfaces will attempt to recover unless they are administratively down. However, automation routines need to be added in NetView or SOLVE:Netmaster to recover the channel when the CIP is reloaded.

Performance Monitoring

Performance monitoring covers many areas. Monitoring is done to determine if the performance of the FEP and interfaces is acceptable. Monitoring is also done for planning purposes. In most environments, products like NETSPY or NPM are used to monitor performance.

With the router, **show** commands allow you to monitor buffers utilization, memory utilization, or CPU. Figure 4-6 shows an example of router performance data that has been archived by Native Service Point.

Figure 4-6 Native Service Point Router CPU/Memory Utilization



Configuration Management

Except for dynamically adding lines, PUs and LUs, NCP configurations must be assembled and loaded to add new features. This function is performed at the mainframe. A copy of the source is passed to VTAM so that it knows what has been generated in the NCP.

For the CIP/router environment, VTAM does not need to know what is configured in the router. However, it is necessary to define a TYPE=XCA major node that identifies the channel that the CIP will be using, and all resources that will connect to VTAM via the CIP need to be defined in a TYPE=SWNET. NCPs are loaded via the host channel. Routers are loaded from an FTP server.

Cisco's Native Service Point allows the customer to archive the router configuration in the mainframe. It also provides the ability to discover and monitor all interfaces configured in the router.

Router Configuration for Host Management

XCA Major Node

```
*********************************************************************
*                                                                   *
* DDDLU LUGROUP FOR TN3270                                          *
*                                                                   *
* DATE CHANGED   WHO        WHAT                                    *
* ------------  ---------   ---------------------------------------- *
*                                                                   *
*********************************************************************
XCAPUGEN VBUILD  TYPE=XCA
X31PR04  PORT  MEDIUM=RING,ADAPNO=4,SAPADDR=4,CUADDR=8C0,TIMER=90
*X31PR04  PORT  MEDIUM=RING,ADAPNO=4,SAPADDR=4,CUADDR=8C0,TIMER=90,    X
*            TGP=TRING16M,VNNAME=NETA.CNNNET1,VNGROUP=CNNGRP1
*
CNNGRP1  GROUP   DIAL=YES,ISTATUS=ACTIVE,ANSWER=ON,CALL=INOUT,         X
AUTOGEN=(100,L,P)
GRP390T5 GROUP DIAL=NO
LN390T5  LINE  USER=SNA,ISTATUS=ACTIVE
P390T5   PU    MACADDR=400170000390,TGN=1,SAPADDR=04,SUBAREA=39,       X
               PUTYPE=5,ISTATUS=ACTIVE
```

Switched Major Node Definition

```
SWDRTRS VBUILD TYPE=SWNET
*********************************************************************
*     SW MAJ NODE FOR LAB AND RUNCMD TESTING OF ROUTERS             *
*
*
*
* LAB  TEST ROUTER  CWBC01
*
CWBC01   PU    ADDR=01,                                               X
               PUTYPE=2,                                              X
               IDBLK=05D,                                             X
               IDNUM=CC001,                                           X
               DISCNT=(NO),                                           X
               ISTATUS=ACTIVE,                                        X
               MAXDATA=521,                                           X
               IRETRY=YES,                                            X
               MAXOUT=7,                                              X
               PASSLIM=5,                                             X
               MAXPATH=4
*
```

Router Configuration (Partial)

```
s
 Building configuration...
Current configuration:
!
version 11.2
service udp-small-servers
service tcp-small-servers
```

```
!
hostname cwb-c1
!
boot system flash slot0:c7000-js-mz
boot system mzallocc/c7000-j-mz 171.69.160.22
 enable password -- suppressed --
!
microcode CIP flash slot0:cip208-0_kernel_hw4
microcode reload
ip subnet-zero
ip domain-name cisco.com
ip name-server 171.69.160.21
ip name-server 171.68.10.70
ip accounting-list 0.0.0.1 255.255.255.0
source-bridge ring-group 900
source-bridge remote-peer 900 tcp 172.18.9.17
source-bridge remote-peer 900 tcp 172.18.9.145
dlsw local-peer peer-id 172.18.9.161 promiscuous
!
> DSPU is required for focalpoint connection via the CIP.
dspu rsrb 325 1 900 4000.7000.0001
dspu rsrb enable-host lsap 4
!
dspu host CWBC01 xid-snd 05dcc001 rmac 4000.3333.4444 rsap 4 lsap 4 focalpoint
!
dspu rsrb start CWBC01
!
interface Tunnel0
no ip address
!
interface Ethernet1/0
no ip address
shutdown
no mop enabled
!
interface Ethernet1/1
description ethernet to hub 2
no ip address
shutdown
no mop ena
bled
!
interface Ethernet1/2
no ip address
shutdown
no mop enabled
!
interface Ethernet1/3
no ip address
ip accounting output-packets
ip accounting access-violations
shutdown
> Listing terminated
```