Troubleshooting Internetworking Systems

DECbrouter 90 System Software
Version 10.3

Digital Equipment Corporation

The products and specifications, configurations, and other technical information regarding the products contained in this manual are subject to change without notice. All statements, technical information, and recommendations contained in this manual are believed to be accurate and reliable but are presented without warranty of any kind, express or implied, and users must take full responsibility for their application of any products specified in this manual.

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

Possession, use, or copying of the software described in this publication is authorized only pursuant to a valid written license from Digital or an authorized sublicensor.

Digital Equipment Corporation makes no representations that the use of its products in the manner described in this publication will not infringe on existing or future patent rights, nor do the descriptions contained in this publication imply the granting of licenses to make, use, or sell equipment or software in accordance with the description.

The following are trademarks of Digital Equipment Corporation: DDCMP, DEC, DECnet, DECNIS, DECserver, DECsystem, DECwindows, Digital, DNA, OpenVMS, ULTRIX, VAX, VAXstation, VMS, VMScluster, and the DIGITAL logo.

Portions of this document is used with permission of Cisco Systems, Incorporated. Copyright © 1990 - 1995, Cisco Systems, Inc.

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.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

About This Manual

This section discusses the audience, scope, organization, use, and conventions of the *Troubleshooting Internetworking Systems* publication.

Audience and Scope

This publication addresses the network administrator or system administrator who will maintain a router or bridge running Software Release 9.21 and later software. Administrators should know how to configure a router and should be familiar with the protocols and media that their routers have been configured to support. Awareness of the basic network topology is also essential.

Document Organization and Use

Troubleshooting Internetworking Systems provides information about troubleshooting router-based internetworks. This publication consists of the following major parts:

- Part 1, "Introduction, Startup Problems, and Serial Problems," is divided in to three chapters: a general introduction to troubleshooting in routed internetworks, troubleshooting suggestions for hardware and system initialization problems, and troubleshooting suggestions for serial lines. Material in the first chapter introduces a generic model of problem solving and provides basic information regarding troubleshooting router-based internetworks. Read this chapter before proceeding to other chapters of the manual. The second chapter outlines router hardware troubleshooting suggestions and presents troubleshooting information associated with startup problems. The third chapter describes standard procedures for evaluating serial line problems and improving throughput over serial lines. In addition, there are a series of symptom modules that cover modem-to-access server connectivity.
- Part 2, "Troubleshooting Connectivity," consists of ten chapters. Protocols and technologies covered in Chapters 4 through 13 include AppleTalk, Banyan VINES, bridging, DECnet, IBM (including SRB, SDLC, and SDLLC), ISO CLNS, Novell IPX, TCP/IP, WAN interconnections (point-to-point serial and packet-switching), and XNS. In general, each chapter consists of a series of problem-solving scenarios that focus on common internetworking problems associated with each technology and a series of symptom modules that include step-by-step procedures for analyzing each symptom.
- Part 3, "Troubleshooting Performance," is composed of only two chapters, but is divided into the same two primary components as Part 2: a series of problem-solving scenarios and a series of symptom modules. Chapter 14, "Performance Problem Scenarios," presents problem-solving scenarios that focus on identifying, isolating, and solving internetworking performance problems. Each scenario describes the symptoms identified, an associated internetworking environment, problem cause alternatives, the process of problem isolation, and a summary of the process.

Chapter 15, “Troubleshooting Internetwork Performance,” focuses on common symptoms associated with poor performance in internetworks, possible causes of those symptoms, and general suggestions for identifying, isolating, and resolving causes.

- Appendixes in this publication provide supplemental troubleshooting information, including a list of information that your technical support representative needs to facilitate problem resolution; troubleshooting worksheets; a description of core dumps; a memory map for routers; and a list of references and recommended reading.

Document Conventions

Our software and hardware documentation uses the following convention:

- The symbol ^ represents the key labeled *Control*.

  For example, ^*D* means hold down the *Control* key while you press the *D* key.

- A string is defined as a nonquoted set of characters. For example, when setting up a community string for SNMP to “public,” do not use quotes around the string, or the string will include the quotation marks.

Command descriptions use these conventions:

- Examples that contain system prompts denote interactive sessions, indicating that the user enters commands at the prompt. The system prompt indicates the current command mode. For example, the prompt `router(config)#` indicates global configuration mode.
- Commands and keywords are in **boldface** font.
- Arguments for which you supply values are in *italic* font.
- Elements in square brackets ([ ]) are optional.
- Alternative but required keywords are grouped in braces ({ }) and separated by vertical bars (|).

Examples use these conventions:

- Terminal sessions and information the system displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords, are in angle brackets (< >).
- Default responses to system prompts are in square brackets ([ ]).
- Exclamation points (!) at the beginning of a line indicate a comment line.

Note is a special paragraph that means *reader take note*. It usually refers to helpful suggestions, the writer’s assumptions, or reference to materials not contained in this manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning Means *danger.* You are in a situation the could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and standard practices for preventing accidents.

PART 1

Introduction, Startup Problems, and Serial Problems

CHAPTER 1

Troubleshooting Overview

Internetworks come in a variety of topologies and levels of complexity—from single-protocol, point-to-point links connecting cross-town campuses to highly meshed, large-scale wide-area networks (WANs) traversing multiple time zones and international boundaries. The overall trend is toward increasingly complex environments, involving multiple media, multiple protocols, and sometimes interconnection to "unknown" networks. As a result, the potential for connectivity and performance problems in internetworks is often high, even when all elements of an environment appear to be fully operational. The objective of this publication is to help you identify potential problem sources in your internetwork and then to resolve problems that arise.

Focus on Symptoms, Causes, and Actions

Failures in internetworks are characterized by certain *symptoms* (such as clients being unable to access specific servers). Each symptom can be diagnosed based on *problems* or *causes* by using specific troubleshooting tools. Once identified, each cause can be remedied by implementing a series of *actions*.

Use this manual as a starting point to develop a problem-solving process for your internetwork. This publication aims to integrate the process of symptom definition, problem identification, and action implementation into an overall troubleshooting model. It illustrates how problems can be detected and diagnosed within the context of case environments.

What This Guide Is Not

With these broad objectives stated, it is equally important to outline topics that are beyond the scope of this publication.

- This publication is not to intended to be the last word in troubleshooting. It does not guide you through every possible error condition, obscure anomaly, or subtle protocol problem. Instead, *Troubleshooting Internetworking Systems* is a roadmap that illustrates the *common* pitfalls and problems most frequently encountered by internetwork administrators.
- *Troubleshooting Internetworking Systems* is not a maintenance and repair guide; nor is it a reference guide. Refer to your hardware installation and maintenance publication for additional details regarding maintenance of router hardware. Refer to the *Router Products Configuration Guide* and *Router Products Command Reference* publications for configuration command details.

  This publication recommends actions for resolving a spectrum of common internetworking problems. In general, it assumes that routers are operational. However, several brief tables provided later in this chapter summarize typical router hardware problems.

- Finally, *Troubleshooting Internetworking Systems* is not a *network* troubleshooting publication. Although suggestions about troubleshooting certain media (including Ethernet, FDDI, serial, and Token Ring) are provided, the focus of the publication is not on troubleshooting media, per se. Several commercially available publications provide this information, such as *LAN Troubleshooting Handbook* by Mark Miller. Appendix E, "References and Recommended Reading," suggests some others.

What, then, does that leave? The discussions that follow outline how you can use this publication to resolve common *internetworking* problems.

The remainder of this overview addresses the following topics:

- Using this publication
- Using router diagnostic tools
- Using CiscoWorks to troubleshoot your internetwork
- Using third-party troubleshooting tools

Using This Publication

Troubleshooting Internetworking Systems focuses on identifying failure symptoms and their associated causes, detecting and isolating those causes, and then resolving problems through specific actions. The symptom discussions and scenarios provided concentrate on issues pertaining to *router* configuration and the interoperation of nodes within a multivendor internetwork.

Within this context, use *Troubleshooting Internetworking Systems* as a guide to do the following:

- Identify possible problem causes when your internetwork is down or slow
- Get direction about resolving problems
- See what kinds of problems have been encountered and resolved in the past
- Avoid falling into the same traps
- Develop your own processes for troubleshooting

To support these activities, this guide uses three key organizational elements (defined in the discussions that follow):

- General problem-solving model
- Symptom modules
- Troubleshooting scenarios

In addition, this overview provides guidelines for the following tasks:

- Using this publication to troubleshoot problems
- Using this publication as a tutorial

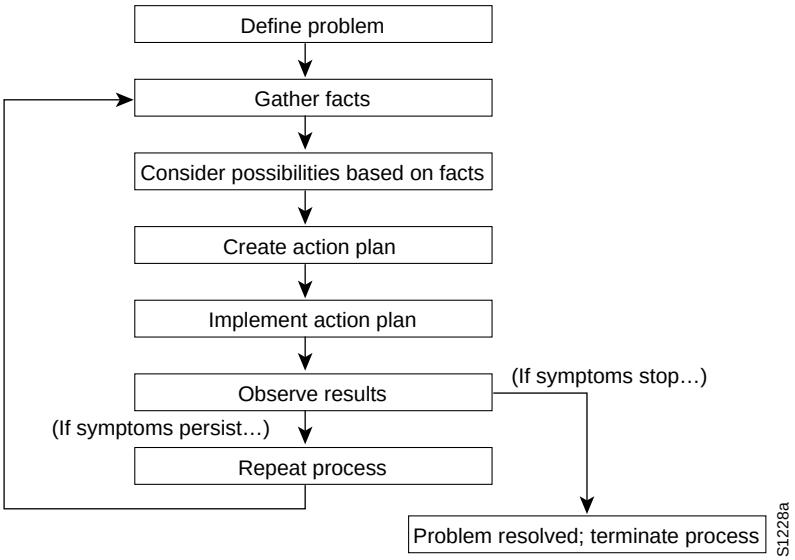
General Problem-Solving Model

Before embarking on your troubleshooting effort, be sure to have a *plan* in place to identify prospective problems, isolate the likely causes of those problems, and then systematically eliminate each potential cause.

The problem-solving model that follows is not a rigid "cookbook" for solving internetworking problems. It is a foundation from which you can build problem-solving plans to suit your particular environment.

Figure 1-1 illustrates process flow for the general problem-solving model described in the steps that follow.

Figure 1-1 General Problem-Solving Flow Diagram



The following steps detail the problem-solving process outlined in Figure 1-1:

Step 1 Define problems in terms of a set of *symptoms* and associated *causes*.

Make a clear problem statement. You must recognize and define the problem/failure mode by identifying any associated general symptoms and then identifying the possible kinds of problems that result in the listed symptoms.

For example, certain hosts might not be responding to service requests from certain clients (a symptom). Possible causes include a misconfigured host, bad interface cards, or missing router commands.

Step 2 Gather facts.

After you list your symptoms and identify possible causes, collect facts. Fact gathering might involve obtaining network analyzer traces, serial line traces, stack dumps, core dumps, and output from a variety of **show** and **debug** privileged EXEC commands. The definition of the problem will point to a more specific set of data to gather.

Step 3 Consider possibilities based on facts.

Armed with a working knowledge of the product, you should be able to eliminate entire classes of problems associated with system software and hardware. This way, you can narrow the scope of interest to only those portions of the product, media, or host problems that are relevant to the specific problem or failure mode.

Step 4 Create an action plan.

The action plan should be based on the set of possibilities you just derived. Your action plan must limit manipulation to *one* variable at a time. This approach allows you to reproduce a given solution to a specific problem. If you alter more than one variable simultaneously, you might solve the problem, but identifying the specific change that eliminated the symptom becomes more difficult.

Step 5 Implement the action plan.

This phase consists of executing the action plan you just created. It is important to be very specific in creating the action plan (that is, identify a specific set of steps and then carefully implement each step).

Step 6 Observe the results of each action.

After having manipulated a variable in an attempt to find a solution to a problem, be sure to gather results based on this action plan (obtain relevant traces, capture **debug** privileged EXEC command data, examine output of **show** EXEC commands, and so forth). This data can be used to fine-tune the action plan until the proper solution is achieved. It is during this phase that you must determine whether the problem has been resolved. This is the exit point of the loop shown in Figure 1-1.

Step 7 Narrow possibilities based on results.

In order to reach a point where you can exit this problem/solution loop, you must strive to make continuous progress toward a smaller set of possibilities, until you are left with only one.

Step 8 Repeat the problem-solving process.

After narrowing your possibility list, repeat the process, starting with a new action plan based on a new (possibly shorter or longer) list of possibilities. Continue the process until a solution is found. Problem resolution can consist of several modifications to hosts, routers, or media.

Note If you exhaust all the common causes and actions (either those suggested here or ones that you have identified for your environment), your last recourse is to contact your router technical support representative. Appendix A, “Technical Support Information List,” outlines information needed by technical support representatives to troubleshoot internetworking problems. One objective of this publication is to help you develop your own processes for gathering data, resolving problems, and preventing problems from recurring (with a minimum of downtime and external intervention).

Symptom Modules

The *symptom modules* in this publication are *not* comprehensive case studies, but instead are brief snapshots of likely problems associated with a specific symptom. Use them as tools for compiling lists of candidate problems (by symptom). The connectivity and performance chapters are organized around the symptom modules. These chapters are not meant to be read from beginning to end; rather, specific information in these symptom-oriented chapters is intended to be used as needed.

Each symptom module includes a brief summary statement and a table listing possible causes. A series of suggested actions is provided for each listed cause to help you determine whether the specific cause is actually the source of the symptom and then to resolve the problem.

Troubleshooting Scenarios

The *troubleshooting scenarios* combine the problems and actions presented in symptom modules with the methods outlined in the section "General Problem-Solving Model" within a context of integrated *case studies*.

Each scenario outlines a set of "observed" symptoms, an internetworking environment, and a list of likely problems for each symptom. Scenarios focus on the process of problem diagnosis (discovery), isolation, and resolution. Not all symptoms discussed in this publication are explored in the scenarios. Instead, selected multiple symptoms are addressed per scenario. An effort has been made to choose common, realistic problems.

Using This Publication to Troubleshoot Specific Symptoms

When using this publication to troubleshoot your internetwork, follow these general steps:

Step 1 Identify symptoms encountered on your internetwork.

Step 2 Eliminate hardware as a possible problem by either fixing any hardware problems or ruling out hardware as a possible cause. (For hardware troubleshooting details, refer to the "Troubleshooting Router Startup Problems" chapter.)

Step 3 Each of the "Troubleshooting Connectivity" chapters offers a "Connectivity Symptoms" section which contains individual *symptom modules* that describe a symptom, possible causes for the symptom, and suggested actions to take to resolve each cause. To identify symptoms similar to those you are experiencing, refer to the chapters that address the technologies or protocols used in your internetwork.

Step 4 Within the appropriate symptom modules, evaluate the problems listed and compare them to your internetworking environment. Note those problems that could apply to your situation.

Step 5 Systematically apply actions for each suspected problem until all symptoms are eliminated, or the possible cause list is exhausted.

Step 6 If problems persist after all of the suggested actions are performed, contact your technical support representative.

Using This Publication as a Tutorial

When using this guide as a tutorial, associated activities are a little less structured than when using it to troubleshoot a specific problem. Nonetheless, you can think of the learning process as a series of steps, as follows:

Step 1 Review the section "General Problem-Solving Model" earlier in this chapter to see recommendations for approaching the troubleshooting process.

Step 2 Read through the troubleshooting scenarios presented in the "Troubleshooting Connectivity" chapters and those in the "Performance Problem Scenarios" chapter.

Step 3 Characterize similarities or differences between these scenarios and your own internetworking environment.

Step 4 Review the symptom modules associated with protocols or technologies implemented in your internetwork.

Step 5 Develop a list of possible symptoms and problems that you encounter in your internetwork. Be as specific as possible. Keep this list on hand in a troubleshooting binder.

Step 6 When similar symptoms occur, use this list to start the troubleshooting process. Remember to modify your problem-solving procedures as you find subtleties associated with your implementation. The key to developing an effective response to problems in your environment is being able to identify the causes of those problems and then implement an action plan. Whatever you can do to preempt time spent in diagnosis will pay off in terms of reducing downtime.

Step 7 Periodically revisit this process to accommodate changes to your internetwork.

Using Router Diagnostic Tools

The following tools are universally applicable when gathering information to troubleshoot problems in router-based internetworks:

- **show** EXEC commands (Although many of these commands are user-accessible, other relevant **show** commands for troubleshooting are privileged EXEC commands.)
- **debug** privileged EXEC commands
- **ping** (Echo Request/Echo Reply) EXEC command
- **trace** EXEC command
- **exception dump** global configuration command and **write core** privileged EXEC command

The discussions that follow summarize using these tools. Appendix C of this publication, "Creating Core Dumps," describes the **exception dump** and **write core** commands. The *Debug Command Reference* publication defines the **debug** commands for protocols and technologies discussed in this publication. The *Router Products Command Reference* publication details the **show**, **ping**, and **trace** commands.

Using show Commands

The **show** commands are among your most important tools for understanding the status of a router, detecting neighboring routers, monitoring the network in general, and isolating problems in your internetwork.

These commands are essential in almost any troubleshooting and monitoring situation. Use **show** commands for the following activities:

- Monitoring router behavior during initial installation
- Monitoring normal network operation
- Isolating problem interfaces, nodes, media, or applications
- Determining when a network is congested
- Determining the status of servers, clients, or other neighbors

For some protocols, such as Novell IPX and AppleTalk, the methodical use of **show** commands is one of the most reliable ways to create a topology map of your internetwork. To create a topology map, use the **show** commands as follows:

Step 1 Use the appropriate **show** *protocol* **route** EXEC command (such as **show novell route**) to determine which neighbors are directly connected.

Step 2 Record the names and network addresses of all directly connected neighbors.

Step 3 Open a connection to each of these directly connected neighbors and obtain the output of the **show** *protocol* **route** command for those neighbors.

Step 4 Continue this process for all routers in your internetwork.

The resulting map reflects all paths to the routers in your internetwork.

Using debug Commands

The **debug** privileged EXEC commands can provide a wealth of information about the traffic being seen (or *not* seen) on an interface, error messages generated by nodes on the network, protocol-specific diagnostic packets, and other useful troubleshooting data. But be aware that these commands often generate data that is of little use for a specific problem.

Use **debug** commands to isolate problems, not to monitor normal network operation. Because the high overhead of **debug** commands can disrupt router operation, you should use **debug** commands only when you are looking for specific types of traffic or problems and have narrowed your problems to a likely subset of causes.

Note You can use the **terminal monitor** privileged EXEC command to copy **debug** command output and system error messages to your current terminal display—as well as to the console terminal. This permits you to establish a Telnet connection to the router and view **debug** command output remotely, without being connected through the console port.

This publication refers to specific **debug** commands that are useful when troubleshooting specific problems. Complete details regarding information provided in **debug** command output are provided in the *Debug Command Reference* publication. However, the *Debug Command Reference* does not document *every* **debug** command that exists in the router code, but only those identified as particularly useful for troubleshooting specific media and protocols.

Caution The use of **debug** commands is suggested for obtaining information about network traffic and router status. Use these commands with great care. In general, it is recommended that these commands only be used under the direction of your router technical support representative when troubleshooting specific problems. Enabling debugging can disrupt operation of the router when internetworks are experiencing high load conditions. When you finish using a **debug** command, remember to disable it with its specific **no debug** command or with the **no debug all** command (the **undebug** command is also accepted).

If you intend to keep the output of the **debug** command, spool the output to a file. The procedure for setting up such a **debug** output file is described in the *Debug Command Reference* publication.

Using ping and trace Commands

Two of the most useful internetworking diagnostic tools are the **ping** and **trace** EXEC commands. The *ping* capability provides a simple mechanism to determine whether packets are reaching a particular destination. Routers from other manufacturers may not forward pings, and some hosts may not reply normally, but even an error packet (ERPDU) response can be useful because it confirms the reachability of the host.

The *trace* capability allows you to determine the specific path taken to a destination and where packets are stopping. Together, these functions may be two of the most important troubleshooting tools available.

Both the **ping** and **trace** commands are available as both user-accessible EXEC commands and as privileged EXEC commands. Depending on the situation, the user-accessible EXEC command may be adequate for testing connectivity. However, if you intend to perform any custom tests, use the privileged EXEC command versions.

Note The **ping** and **trace** commands are protocol specific. The **ping** command can be used with AppleTalk, Banyan VINES, IP, ISO CLNS, Novell IPX, and XNS internetworks, and only routers running one of those protocols will respond. AppleTalk, Banyan VINES, IP, and ISO CLNS support the **trace** function. To use the **trace** command, one of these protocols must be enabled for routing, and only nodes running the specific protocol will respond.

Using Core Dumps

The **exception dump** global configuration command and **write core** privileged EXEC command are among the more obscure (although useful) diagnostic commands available in your router toolkit. When the system software fails, analyzing a *core dump* (produced by the **exception dump** command) is sometimes the only way to determine what happened. The **write core** command is useful if the router is malfunctioning, but has not crashed.

Caution Use these commands only in coordination with a qualified technical support representative. The resulting binary file must be directed to a specific UNIX syslog server and subsequently interpreted by qualified technical personnel. Appendix C, “Creating Core Dumps,” briefly describes the process.

Developing a Strategy for Isolating Problems

One important consideration to remember when troubleshooting broken interconnections is that *normally* everything does not break at the same time. As a result, when trying to isolate a problem, you can typically work out from an operational node to the point of failure. The following basic steps should help when you are trying to isolate the source of connection disruption:

Step 1 First, determine whether the local host that is experiencing connectivity problems is properly configured.

Step 2 For AppleTalk, Banyan VINES, IP, ISO CLNS, and Novell IPX internetworks, use the **ping** or **trace** EXEC commands (as applicable) to determine whether the routers and bridges through which the local host must communicate can respond. Start with the most local router or bridge and progressively "ping out" through the internetwork.

Step 3 If you cannot get through a particular router, examine the configuration of the router and use the various **show** commands to determine the state of that router.

Step 4 If you access all the routers in the path, check the configuration of the remote host (or get the help of someone to do so).

Step 5 Use the appropriate **show** *protocol* **route** command to see if the hosts in question appear in the routing tables. Use other protocol-specific **show** commands to check for anomalies.

Using CiscoWorks to Troubleshoot Your Internetwork

The CiscoWorks product is a set of router management applications that allows you to manage your internetwork from a central location. You can use CiscoWorks software to monitor and troubleshoot complex internetworks. Because CiscoWorks uses the Simple Network Management Protocol (SNMP), it can monitor and control any SNMP device on an internetwork. The CiscoWorks software comprises five different applications: configuration management, fault management, accounting management, performance management, and security management.

In addition to the basic SNMP management functions, the CiscoWorks software provides a fully integrated relational database and uses built-in SunNet Manager (SNM) capabilities to produce a dynamic, user-configurable visual network map. The automatic map-generation features associated with the CiscoWorks Path Tool capabilities can help you visually trace the routes to problem nodes. Tools that can help you isolate connectivity and performance problems are outlined briefly in the following discussions. Refer to the *CiscoWorks User Guide* for complete details about using CiscoWorks to monitor and control your internetwork.

Using CiscoWorks to Troubleshoot Connectivity Problems

Use the following CiscoWorks fault management applications when troubleshooting connectivity problems in your internetwork:

- Device Monitor—Monitors specific devices for environmental and interface information. Sends event information to SNM that causes a glyph to change state.
- Path Tool—Graphically displays a route of the path from a source device to a destination device.
- Environmental Monitor—Graphically displays the temperature and voltage data from an AGS+ router.
- Real-Time Graphs—Monitors the behavior of device interfaces or other network elements suspected of operating in a degraded mode and displays them in a graph.
- Show Commands—Enable you to view data similar to output from router **show** EXEC commands.

- Health Monitor—Provides information about the health of a device with access to several CiscoWorks applications on one window (including Show Commands and Real-Time Graphs) to monitor router activity.
- Contacts—Provides quick access to find your emergency contact person for a particular device.
- Log Manager—Enables you to store, query, and delete messages gathered from CiscoWorks applications and Cisco Systems devices on the internetwork.

Using CiscoWorks to Troubleshoot Performance Problems

Use the following CiscoWorks performance management applications when troubleshooting performance problems in your internetwork:

- Device Polling—Probes and extracts data about the condition of your network devices.
- Polling Summary—Displays polling data, and stops and starts polling.
- Real-Time Graphs—Monitors the behavior of device interfaces or other network elements suspected of operating in a degraded mode and displays them in a graph.
- Path Tool—Graphically displays a route of the path from a source device to a destination device.
- Show Commands—Provide data similar to router **show** EXEC commands output.
- Sybase DWB—Allows you to access the Sybase Data Workbench application to write reports.

Using Third-Party Troubleshooting Tools

This publication emphasizes diagnostic tools provided with the router. However, other troubleshooting tools also are discussed in the symptom modules and scenarios.

In some cases, third-party diagnostic tools can be more useful than integrated tools. For example, enabling a **debug** privileged EXEC command can be disastrous in any environment experiencing excessively high traffic levels. Attaching a network to the suspect network is less intrusive and more likely to yield applicable information without exacerbating load problems for a router.

The following list summarizes some typical third-party troubleshooting tools:

- *Time Domain Reflectometer (TDR)*—A TDR transmits a short pulse of known amplitude and duration down a cable and measures the corresponding amplitude and time delay associated with resultant signal reflections. TDRs are available for all LAN types. Optical TDRs provide a similar test capability for fiber cable.
- *Optical Power Source and Meter*—This device employs an optical power source connected to one end of a fiber cable and a meter placed at the other end to measure optical power. Also called a “light meter,” this device is a cost-effective alternative to an optical TDR.

- *Oscilloscope*—Oscilloscopes graphically display signal voltage per unit of time; commonly used to measure voltages on EIA/TIA-232 and EIA/TIA-422 interfaces.

Note Prior to the acceptance of the EIA/TIA standard by the ANSI committee, these interface standards were referred to as recommended standards RS-232 and RS-422.

- *Breakout Box* —A breakout box displays and monitors status of EIA/TIA-232-D interface leads between data terminal equipment (DTE) and data circuit-terminating equipment (DCE). Breakout boxes are useful for reconfiguring interfaces.
- *Network Analyzer*—Network analyzers (also known as "protocol analyzers" and "LAN analyzers") capture, record, and analyze frames transmitted on a network. Analyzers attach to a network just as any node does. All analyzers support a range of physical interface specifications (including Ethernet, Token Ring, and FDDI), as well as a spectrum of network protocols (including TCP/IP, Novell IPX, IBM SNA, AppleTalk, DECnet, and ISO CLNS).
- *WAN/Serial Line Analyzer*—WAN analyzers generally focus on WAN/serial line analysis, but can include LAN analysis capabilities. WAN analyzers support a range of physical interfaces (such as EIA/TIA-232, EIA/TIA-422, EIA/TIA-449, T1/E1, ITU-T V.35, and ITU-T X.21) and protocols (including HDLC, SDLC, Frame Relay, and ISDN).

Note The ITU-T carries out the functions of the former Consultative Committee for International Telegraph and Telephone (CCITT).

CHAPTER 2

Troubleshooting Router Startup Problems

A common problem for any newly installed system is its inability to initialize itself correctly. This chapter addresses the following common router startup problems:

- Diagnosing Router Hardware Problems
- Troubleshooting Media Problems
- Troubleshooting Router Booting Problems
- Router Booting Process Symptoms
- Recovering a Lost Password

Diagnosing Router Hardware Problems

Although this publication focuses on troubleshooting *overall* internetworking problems, the tables that follow provide some suggestions for diagnosing router hardware problems. Your hardware installation and maintenance publications provide information about specific light-emitting diode (LED) indicators.

This discussion does not provide a step-by-step procedure. It is included as a checklist and should be used as a starting point for troubleshooting. The following discussion suggests a three-stage process:

- Physically inspecting your system
- Applying power and evaluating the system
- Testing and verifying operation

Each of these stages is discussed separately.

Inspecting Your Router

When you are initially evaluating a router that is having a problem, keep the following three rules in mind:

- Contrast what *should be* happening with what *is* happening.
- Do not overlook the obvious.
- Do not alter *anything* before powering-up your router.

At this stage, concentrate on problems that are obvious. Follow these inspection steps.

Note Platform-specific comments are noted in parenthetical additions to specific steps. Unless otherwise specified, all references to platform numbers (such as Cisco 7000) refer to the product *series* to which the platform belongs.

Step 1 Skip this step if you are troubleshooting an access router (Cisco 2000 series, Cisco 2500 series, Cisco 3000 series, Cisco 4000 series or IGS). For modular systems (except the Cisco 4000 and Cisco 7000), switch the power off and inspect the system for loose cards, cables, and port adapters. Reseat any that are loose. When cards are new, a thin film of carbon or oxidation buildup can prevent good contact. After reseating each card once or twice, you should achieve good contact.

For the Cisco 4000 series systems, look for a loose network interface module (NIM). For the Cisco 7000 series systems, look for a loose Route Processor (RP), Switch Processor (SP), Silicon Switch Processor (SSP), or interface processor. Reseat any that are unseated. Be sure to use the ejector levers properly and to tighten all captive installation screws on the RPs, SPs, SSPs, interface processors, and power supplies. After reseating each card and tightening the captive installation screws, you should achieve good contact. For more information, refer to your hardware installation manual.

Step 2 Remove the chassis access panel and inspect the interior. Are the wires to the power supply connected correctly? Are wires burned or otherwise damaged?

Step 3 For systems *other than* Cisco 7000 series systems, look for damaged cards, backplanes, and ribbon cables. Are there any visibly crimped or shorted wires or cables?

Step 4 Check for missing or loose parts, incorrectly connected cables, and anything that appears out of place. Does the unit need to be cleaned? Is there damage to the interior or exterior?

Note *Do not change anything before powering up the system for evaluation* so that you can determine the source of suspected hardware problems during subsequent evaluation. Making changes can mask problems.

Applying Power and Evaluating the System

After you inspect the system, apply power to the unit and observe its behavior. If you suspect a hardware problem, follow these steps to evaluate operational conditions upon power-up:

Step 1 Power up the system (with system disconnected from a network).

(When you power up a Cisco 7000 series system, the enabled LED on an SP, SSP, or interface processor will eventually go on if the card is seated correctly. If any enabled LEDs do not go on, power down the system and be sure that the cards are properly seated as discussed in the previous section, “Inspecting Your Router.”)

Step 2 Compare system behavior against symptoms outlined in Table 2-1.

Step 3 If a failure does not fit the examples in Table 2-1, verify that the software in the processor and the microcode in the various cards are compatible with the individual card revisions within the chassis. Refer to the release document provided with your system.

Step 4 If the system boots, use the **show controllers** {**token** | **mci** | **fddi** | **cbus**} EXEC command to ensure that the interface hardware addresses are nonzero. Hardware addresses of all zeros *will* cause problems in a network.

(For Cisco 7000 series systems, use the **show controllers cxbus** EXEC command and check the output of the **show configuration** privileged EXEC command. With downloadable microcode and software images stored in Flash memory, the system might be configured to load incompatible software or microcode.)

Note If the system boot-up sequence requires a password, the memory card and circuitry are working correctly. If the configuration in memory does not match the hardware configuration, problems can occur. Possible problems include hung ports, uninitialized ports, ping failures, bus timeout errors, and reboots.

Step 5 As a last resort, for systems *other than* Cisco 7000 series systems, you can use a voltmeter to ensure that all the power supply direct current (DC) voltages are within specifications. Refer to the configuration note (if one has been provided) for your power supply model.

Warning Normally, you should turn off power to the chassis and unplug the power cord before accessing the chassis interior. However, if you are measuring power supply voltages, you must have power applied to the system. Use extreme caution when power is applied, and the internal chassis is exposed. Potentially harmful voltages are present. Only qualified router service technicians should perform power supply tests.

For Cisco 7000 series systems, LEDs on the power supplies indicate whether power is within specification: the green alternating current (AC) power LED should be on and the red DC fail LED should be off. You can also use the **show environment** EXEC command to obtain a reading of the power supply voltages.

Note Configuration notes are only shipped with spares and replacement parts.

Table 2-1 Router Power-Up Problems

Symptoms at Power-Up	Possible Causes
System appears to be dead	Power supply not seated properly (Cisco 7000); check LEDs on power supply
	Fuse blown (Cisco 2000, Cisco 3000, Cisco 4000, and I, M, and C chassis)
	Bad or tripped circuit breaker (A-type chassis)
	Bad power supply
	Bad switch
	Bad backplane
	Bad power cable or connector (to source or power supply port)
	Bad or no input power (AC or DC)
No fan or blower movement (MGS, CGS, Cisco 7000 series)	Bad fan
	Bad blower
	Bad 12V power supply (MGS, CGS)
	Bad +24V power (Cisco 7000 series)
	Shorted or broken wires on harness or backplane
No blower movement (A-type, AGS+)	Bad blower
	Bad circuit breaker
	Tripped circuit breaker
	Shorted or broken wires
	Bad 110 or 220 VAC capacitor
No power supply LEDs on or power supply Failed LED is on (Cisco 7000 only)	Power supply not seated properly
	Bad input (source) power
	Shorted or broken wires on harness or backplane
	Environmental shutdown
No LEDs on at boot for any card (except Cisco 7000)	Bad 5V power supply (no LEDs for problem card are on); box might boot
	Shorted or broken wires
	Bad backplane
	Incompatible microcode on card with LEDs that do not go on
No processor LEDs go on at boot; power supply LEDs are OK (Cisco 7000 only)	Partially inserted card has hung bus
	Bad processor card or processor is poorly seated
	Bad software or incompatible microcode
	Shorted or broken wires on harness or backplane
	Bad boot instructions in configuration file or corrupted image file in Flash memory

Symptoms at Power-Up	Possible Causes
Router will not boot	Bad power supply
	Miswired power supply (except Cisco 7000 series)
	Bad/disconnected console cable (system still boots; no monitor output)
	Bad processor card or card is poorly seated
	Bad software
	Corrupted or incorrectly seated read-only memory (ROM)
	Bent ROM pins
	ROMs installed out of sequence
	Bad nonvolatile random-access memory (NVRAM) card (except Cisco 7000 series)
	Shorted wires (except Cisco 7000 series)
System will not boot; boot error or CPU halt LED is on (Cisco 7000 series only)	Partially inserted card has hung bus
	Bad processor card or processor is poorly seated
	Bad software
	Corrupted or incorrectly seated ROMs
	Entire system image did not copy into Flash memory; Flash memory is full
No cards show up in power-on message display	Bad backplane
	Bad controller or interface card
	Cards not seated in backplane
	Conflicting or incompatible microcode version on card (or in Flash memory for Cisco 7000 series)
	Bad power supply (except Cisco 7000 series)
Cards missing from power-on message display	Bad controller or interface card
	Cards not seated in backplane
	Conflicting DIP switch setting on card with other devices (except Cisco 7000 series)
	Card not supported with software version
	Bad power supply (except Cisco 7000 series)
	Bad arbiter (Cisco 7000 series)
Circuit breaker trips or fuse blows (except Cisco 7000 series)	Bad power supply
	Bad backplane
	Shorted wires
	Load too large on power supply
	No load on power supply
	Bad breaker
	Bad blower
	Bad card

Symptoms at Power-Up	Possible Causes
Constant or partial reboot	Bad processor, controller, or interface card
	Poorly seated processor (Cisco 7000 series)
	Bad backplane
	Bad power supply (except Cisco 7000 series)
	Bad software
	Bad microcode
	Poorly seated SIMMs (IGS, Cisco 2000, Cisco 2500, Cisco 3000, Cisco 4000, and Cisco 7000 series)
	Poorly seated ROMs (CSC/3, CSC/4, RP, IGS)

Testing and Verifying Replacements

If you are replacing a part or card to remedy a suspected problem, remember the following rules:

- Make only one change at a time.
- Eliminate suspected problems one at a time.
- Think in terms of card replacement only.
- Keep track of *any* unrecorded failure symptoms or unexpected behaviors for future revisions of this guide.
- To test a system, start with a simple hardware configuration and add one card at a time until a failed interface appears or is isolated. Use a simple software configuration and test connectivity using a ping test.

Use Table 2-2 as the next step in evaluating hardware. The problems listed are *not* all of the possible failures for each product, but do represent commonly encountered symptoms. Where applicable, possible error messages associated with failure symptoms are also listed.

If you determine that a part or card replacement is required, contact your sales or technical support representative. Specific instructions concerning part or card installation are included with the configuration note provided with the replacement.

Warning Before accessing the chassis interior and removing any cards, turn off power to the chassis. Use extreme caution around the chassis. Potentially harmful voltages are present. To prevent damage to components that are sensitive to electrostatic discharge (ESD), attach ESD protection before opening a chassis. Make certain that the power cord is connected, but that power is off. ESD damage prevention guidelines are provided in the hardware installation and maintenance publication for your router.

If a part replacement appears to solve a problem, make certain to reinstall the suspect part to verify the failure. *Always* double-check a repair.

Note Any interface processor, the RP, the SP, or the SSP can prevent a Cisco 7000 series router from booting if the processor is not completely connected to the bus. Be sure to check the seating of processors if the system is not booting properly. Use the ejector levers to reseat all processor modules, then reboot.

Table 2-2 Specific Cards and Products: Failure Symptoms and Associated Problems

Card or Product	Symptom
RP (Cisco 7000 series only)	System is down after running a short time; blower on.
	System will not power up; blower on.
	Boot Error or CPU halt LEDs might be on.
	Configuration cannot be written to memory.
	System will not boot (any combination of processor LEDs on, other than green LED alone).
	The SP or SSP card is not recognized.
	Partial boot only or system will not boot.
	Random reboot occurs after initial boot.
	System reboots when configuration memory is written.
	No response from keyboard or apparent problem with console terminal.
	Configuration memory is wrong size.
	Error Indicators—Bad checksum for configuration memory, configuration memory not set up, nonvolatile memory not present.
CSC-ENVM	System is down after running a short time; DC voltages off; blower on.
	System will not power up; DC voltages off; blower on.
	Configuration cannot be written to memory; system loses memory over time.
	CSC-ENVM fails to shut system down even with excessive heat or DC voltage.
	Error Indicators—Bad checksum for configuration memory, configuration memory not set up, nonvolatile memory not present.
CSC/2, CSC/3, and CSC/4 cards	System will not boot (any combination of processor LEDs on, other than green LED alone).
	Multibus cards are not recognized.
	The ciscoBus controller is not recognized (CSC/3 and CSC/4 cards only).
	Partial boot only.
	Random reboot occurs after initial boot.
	System will autoboot but cannot boot manually.
	System will reboot when configuration memory is written.
	No response from keyboard.
	Error Indicators—Parity error, software versus hardware error, local timeout, bus error, wrong interface, emulation line error, software-forced crashes, checksum mismatch error.
SP or SSP (Cisco 7000 series only)	Some or all CxBus cards are not recognized.
	Enabled LED does not go on (processor card not initialized).
	Error Indicators—MEMD failure, MEMA failure, arbiter/processor card failure.

Card or Product	Symptom
CSC-CCTL and CSC-CCTL2	Some or all ciscoBus cards are not recognized. No LEDs are on. All LEDs are on. Some or all Multibus cards are not recognized. *Error Indicators*—MEMD failure, MEMA failure, ciscoBus daughter controller failure.
FIP (Cisco 7000 series only)	Not recognized by arbiter, SP, or SSP. Fiber Distributed Data Interface (FDDI) ring will not come up. FDDI ring comes up, but ping does not work on the FDDI ring or only works intermittently; only certain packet sizes ping. No keyboard response after FDDI ring comes up; keyboard locks up. Cannot see FDDI upstream/downstream neighbors. LEDs are on in the wrong sequence. FDDI ring comes up in "wrap-mode" only—wrap A or wrap B. No ping through FDDI ring or to address of unit under test (UUT); intermittent ping. FDDI ring will intermittently or constantly transition. Ring status LEDs do not go on. *Error Indicators*—Unknown data error, card in slot *n* does not respond.
CSC-FCI, CSC-C2FCI, and CSC-C2FCIT cards	Not recognized by ciscoBus controller. FDDI ring will not come up. FDDI ring comes up, but ping does not work on the FDDI ring or only works intermittently; only certain packet sizes ping. No keyboard response after FDDI ring comes up; keyboard locks up. Cannot see FDDI upstream/downstream neighbors. *Error Indicators*—Unknown data error, MEMD failure, MEMA failure, ciscoBus daughter controller failure.
FDDI appliques (APP-LMM, APP-LMS, APP-LSM, and APP-LSS)	FDDI ring will not come up. LEDs are on in wrong sequence. FDDI ring comes up in "wrap-mode" only—wrap A or wrap B. No ping through FDDI ring or to address of UUT; intermittent ping. FDDI ring intermittently or constantly transitions. Cannot see FDDI upstream/downstream neighbors. Ring status LEDs are not on.
EIP (Cisco 7000 series only)	Card is not recognized by the arbiter, SP, or SSP. Unable to ping on any or some ports; intermittent ping; only certain packet sizes will ping. All LEDs are on. No LEDs are on. Wrong number of LEDs are on. *Error Indicators*—Timeout, arbiter, SP, or SSP failure, halted output.

Card or Product	Symptom
CSC-MEC and CSC-C2MEC cards	Card is not recognized by ciscoBus controller.
	Unable to ping on any or some ports; intermittent ping; only certain packet sizes will ping.
	All LEDs are on.
	No LEDs are on.
	Wrong number of LEDs are on.
	Error Indicators—Multibus timeout, ciscoBus daughter controller failure, halted output.
FSIP card (Cisco 7000 series only)	Card is not recognized by arbiter or SP or SSP.
	No LEDs are on.
	All LEDs are on.
	No ping on any or some ports; DTE will ping and DCE will not ping (or vice versa); intermittent ping; only certain packet sizes will ping.
	Ports will not initialize—some or all.
	Will not netboot or ping to network; no ping to address of unit under test (UUT).
	Error Indicators—Local timeout, MEMD failure, MEMA failure, halted output, bus or ALU failure, configuration memory not set up, excessive input serial errors, CxBus timeouts, or SxBus timeouts (SxBus timeouts apply to older Cisco 7000 routers only).
FSIP port adapters	Interface up, but ping does not work, or intermittent ping functionality.
	DTE will ping but DCE will not ping (or vice versa).
	System reboots.
CSC-MCI and CSC-SCI	Card is not recognized by the processor card.
	No LEDs are on.
	All LEDs are on.
	No ping on any or some ports; DTE will ping but DCE will not ping (or vice versa); intermittent ping; only certain packet sizes will ping.
	Ports will not initialize—some or all.
	Will not netboot or ping to network; no ping to address of UUT.
	CSC-MCI-3 card cannot see random-access memory (RAM) and NVRAM.
	Wrong number of LEDs on—too many or too few.
	Error Indicators—Local timeout, MEMD failure, MEMA failure, halted output, bus/ALU failure, configuration memory not set up, excessive input serial error, or Multibus timeouts.
Arbiter, SP, or SSP (Cisco 7000 series only)	Cannot write configuration memory on RP; no memory access; memory access causes reboot.
	CxBus cards are not recognized.
	System will not boot or will reboot.
	No DC voltages—some or all.
	Bad power supply (caused by shorted backplane).
	Blower is not working.
	Systems consistently crash when attempting to boot.

Card or Product	Symptom
ciscoBus backplane and Multibus backplane	Cannot write configuration to memory; cannot access memory; memory access causes reboot.
	Multibus or ciscoBus cards are not recognized.
	System will not boot or will reboot.
	No DC voltages—some or all.
	Bad power supply (caused by shorted backplane).
TRIP card (Cisco 7000 series only)	Card is not recognized by the processor.
	No ping to outside address or address of UUT; intermittent ping.
	No hardware address recognized.
	Error Indicators—Halted output, beaconing, local timeout, Open failed: lobe test.
CSC-R, CSC-R16M, CSC-1R, CSC-2R, and CSC-C2CTR cards	Card is not recognized by the processor.
	No ping to outside address or address of UUT; intermittent ping.
	No hardware address recognized.
	Error Indicators—Halted output, beaconing, local timeout, Open failed: lobe test, Multibus timeout.
CSC-M, CSC-MT, CSC-MC, and CSC-MC+ cards	NVRAM not recognized by MCI-3, CSC-1R, or CSC-2R card (CSC-MC and CSC-MC+ cards only).
	Configuration cannot be written to memory.
	Memory lost over time.
	Configuration and/or Multibus memory wrong size (CSC-MT card only).
	Error Indicators—Bad checksum for configuration memory, configuration memory not set up, nonvolatile memory not present.
Serial appliques	Interface up but ping does not work, or intermittent ping functionality.
	DTE will ping, DCE will not ping (or vice versa).
	System reboots (with dual-mode V.35, suggests bad ground contact).
	5V or 12V power supply LEDs indicate no power detected.
Cisco 4000	System will not boot.
	Fuse blows.
	Constant or partial reboot.
IGS, Cisco 2000, Cisco 2500, and Cisco 3000	System will not boot.
	Fuse blows (except Cisco 2500 series).
	Fan does not run.
	Constant or partial reboot.
500-CS	System will not boot.
	Fuse blows.
	Fan does not run.
	LEDs fail to go on.

Troubleshooting Media Problems

Table 2-3 through Table 2-6 summarize general problem-solving guidelines for common media (Ethernet, Token Ring, serial lines, and FDDI).

Table 2-3 Media Problems: Ethernet

Media Problem	Suggested Actions
Excessive errors or noise on Ethernet	**Step 1** Use the **show interfaces ethernet** EXEC command to determine the status of the interface. **Step 2** Use a time domain reflectometer (TDR) to find any unterminated Ethernet cables. **Step 3** Check host cables to determine whether any are incorrectly terminated, overly long, or damaged. **Step 4** Look for a jabbering transceiver attached to a host (might require host-by-host inspection). **Step 5** Look for badly spaced taps causing reflections.

Table 2-4 Media Problems: Token Ring

Media Problem	Suggested Actions
Nonfunctional Token Ring	**Step 1** Use the **show interfaces token** command to determine the status of the interface. **Step 2** If the status line indicates that the interface and line protocol are not up, check the cable from router to Multistation Access Unit (MAU). Make sure that the cable is good; replace if necessary. If you are performing a new installation, make sure that the MAU has been properly initialized. Consult the manufacturer's documentation for information on initializing your MAU. **Step 3** If the **show interfaces token** output indicates that the interface and line protocol are up, use the **ping** command between routers to test connectivity. **Step 4** If the remote router does not respond, check the ring specification on all nodes attached to the Token Ring backbone. Ring speed for all must be the same. The options are 4 Mbps (default) and 16 Mbps. Use the **write terminal** privileged EXEC command to determine which speed is active. **Step 5** If necessary, modify ring speed specifications for clients, servers, and routers. **Step 6** Use the **ring-speed** interface configuration command to modify the ring speed configuration for Token Ring cards that support software speed configuration; change jumpers as needed for modular router platforms that do not support software speed configuration. For more information about ring speed specifications, refer to the hardware installation and maintenance manual for your system.

Table 2-5 Media Problems: Serial Lines

Media Problem	Suggested Actions
Nonfunctional serial line	**Step 1** Use the **show interfaces serial** EXEC command to determine the status of the interface. **Step 2** If the **show interfaces serial** command indicates that the interface and line protocol are up, use the **ping** EXEC command between routers to test connectivity. Isolate possible circuit problems by looping the local DTE back to the RTS interface pin. **Step 3** If routers do not respond to the ping test, follow the troubleshooting techniques as discussed in the "Troubleshooting Serial Line Problems" chapter. **Step 4** If clock and data signals are out of phase, invert the clock signal.

Table 2-6 Media Problems: FDDI

Media Problem	Suggested Actions
Nonfunctional FDDI ring	**Step 1** Use the **show interfaces fddi** EXEC command to determine status of interface. **Step 2** If the **show interfaces fddi** command indicates that the interface and line protocol are up, use the **ping** command between routers to test connectivity. **Step 3** If the interface and line protocol are up, make sure the media access control (MAC) addresses of upstream and downstream neighbors are as expected. If all zeros appear in either of the address fields for these neighbors, a physical connection problem is likely. **Step 4** In this case (or if status line does *not* indicate that the interface and line protocol are up), check patch-panel connections or use an optical TDR or light meter to check connectivity between neighbors. Ensure that signal strength is within specification.
Upstream neighbor has failed and bypass switch is installed. Bypass switches can cause signal degradation because they do not repeat signals like a normal transceiver.	**Step 1** Check upstream neighbor to determine if it is operational. **Step 2** If the node is down, and a bypass switch is in place, resolve any problems found in upstream neighbor.

Troubleshooting Router Booting Problems

Routers allow for system initialization (booting) using several methods. Systems can be booted in any of four ways:

- From a file over the network
- From Flash memory
- From ROM
- From a PCMCIA Flash memory card

The material that follows addresses problems that might arise during the booting process.

Booting Troubleshooting Information

If you are unable to resolve your booting problem, collect the following information for the technical support representative:

- ROM images (using the **show version** EXEC command)
- Programmable ROM labels
- NVRAM configurations for client and adjacent routers (via the **write terminal** privileged EXEC command)
- Debugging output from the adjacent router using the following privileged EXEC commands:
  - **debug ip packe**t
  - **debug arp**
  - **debug ip udp**
  - **debug tftp**

  For more information about these **debug** commands, refer to the *Debug Command Reference* publication.

Notes on Netbooting

Routers support netbooting via both the Trivial File Transfer Protocol (TFTP) and the DEC Maintenance Operation Protocol (MOP) across all supported media types such as Ethernet, FDDI, serial lines, Token Ring, and High-Speed Serial Interface (HSSI). During netbooting sessions, routers behave like hosts: they route via proxy Address Resolution Protocol (ARP), Serial Line Address Resolution Protocol (SLARP) information, Internet Control Message Protocol (ICMP) redirects, or a default gateway. When netbooting, routers ignore dynamic routing information, static IP routes, and bridging information. As a result, intermediate routers are responsible for handling ARP and User Datagram Protocol (UDP) requests correctly. For serial and HSSI media, ARP is not used.

If you need to netboot from a server, you should first **ping** the server from the ROM software. If you are unable to **ping** the server, first look for a solution in Table 2-7. If none of the problems described in Table 2-7 explains the ping failure, there is probably a problem with the server configuration or hardware. Contact your router or TFTP server technical support representative for assistance.

Using a Fault-Tolerant Boot Strategy

Network failures can make netbooting impossible. After Flash memory is installed and configured, configure the router to boot in the following order to reduce the effects of a server or network failure:

1. Boot an image from Flash memory
2. Boot an image from a system filename (netboot)
3. Boot from a ROM image

Example

The order of the commands needed to implement this strategy is illustrated in the following sample output:

```
klamath# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
klamath(config)# boot system flash gsxx
klamath(config)# boot system gsxx 131.108.1.101
klamath(config)# boot system rom
klamath(config)# ^Z
klamath#
%SYS-5-CONFIG_I: Configured from console by console
klamath# write memory
[ok]
klamath#
```

Using this strategy, a router has three sources from which to boot: Flash memory, netboot, or ROM. Providing alternative sources can help to mitigate any potential failure of the TFTP server or the network.

Note The configuration register must be set to allow ROM image booting following failed netbooting attempts. Refer to the hardware configuration manual for your router product.

Timeouts and Out-of-Order Packets

When netbooting, it is not unusual for a client to retransmit requests before receiving a response to an initial ARP request. The retransmissions can result in timeouts, out-of-order packets, and multiple responses. Timeouts (shown as periods in a netbooting display) and out-of-order packets (shown as uppercase Os) do not necessarily prevent a successful boot. It is acceptable to have either or both of these in the first few packets. Exclamation points represent good packets. The following examples show successful netbooting sessions even though timeouts and out-of-order packets have occurred:

```
Booting gs3-bfx from 131.108.1.123: !.!!!!!!!!!!!!!!!!!!!!
```

```
Booting gs3-bfx from 131.108.1.123: !O.O!!!!!!!!!!!!!!!!!!!!
```

If your session has many out-of-order packets and timeouts, the problem will require some attention. Problems that might result in timeouts and out-of-order packets and recommended solutions are discussed in the troubleshooting tables that follow.

Router Booting Process Symptoms

Booting problem symptoms are discussed in the following sections:

- Router Cannot Netboot from TFTP Server
- Timeouts and Out-of-Order Packets Occur during Netbooting
- Netbooting Problems Resulting from Invalid Routing Paths
- Client ARP Requests Time Out when Netbooting
- Vector Errors Occur when IGS Attempts Netbooting
- Buffer Overflow Errors Occur when Netbooting
- Undefined Load Module Error when Netbooting
- Router Cannot Boot from Another Router (TFTP Server)
- Local Timeouts Occur when Booting from ROM
- Router Hangs after ROM Monitor Initializes
- Router Is Stuck in ROM Monitor Mode
- Scrambled Output when Booting from ROM
- Vector Error Occurs when Booting from Flash Memory
- Router Partially Boots from Flash and Display Shows Boot Prompt
- Router Fails to Boot from Flash Memory
- Terminal Connected to Unconfigured Access Server Is Unresponsive

Router Cannot Netboot from TFTP Server

Symptom: In the most general case, a router tries to obtain its system image over the network, but fails. Netbooting failures can result from several problems. Following is an example display generated by the system when it cannot boot:

```
Booting gs3-bfx.........[failed]
```

Table 2-7 outlines possible causes and suggests actions for when a router cannot boot from a TFTP server. Other specific symptoms and problems are outlined in subsequent discussions.

Note Refer to the host (boot server) manual for details about setting up a TFTP server.

Table 2-7 Router Startup: Router Cannot Netboot from a TFTP Server

Possible Causes	Suggested Actions
Network is disconnected or isolated	**Step 1** Boot the router from ROM or Flash memory if possible. **Step 2** Use the **ping** EXEC command to send a message to the broadcast address (255.255.255.255). **Step 3** Look for an ICMP Echo Reply response for a TFTP server. **Step 4** If no response occurs, use the **show arp** EXEC command to look for an entry associated with the server. **Step 5** Use the **show ip route** EXEC command to look for an entry listing the network or subnet for the server. If a path to a boot server exists, a disconnected network is not the problem. If no path exists, make sure that a path is available before continuing to attempt router netbooting.
TFTP server is down	**Step 1** Check the intended server system to determine whether the TFTP server is running. You can do this by attempting to make a TFTP connection from the boot server to itself. The connection will be successful if the TFTP server is running. **Step 2** If the TFTP server is not running, initialize it. The actual initialization process varies depending on the type of boot server. (For a BSD UNIX server, check the */etc/inetd.conf* file. If the TFTP server is not included in this file, add the appropriate line and cause inetd to reload its configuration.)
Misconfigured server (router image in wrong directory)	**Step 1** Look at the server configuration file to see if it points to the directory in which the router image resides. **Step 2** Move the router image to the correct directory if necessary. **Step 3** Make sure the */tftpboot* directory is reachable over the network.
Misconfigured server (router system image file permission is incorrect)	**Step 1** Check the permission of the file. **Step 2** If necessary, change the permission. For example, for a UNIX boot server, set the permission for the file to owner read/write, group read, and global read (the UNIX command for setting this permission is **chmod 0644**).
Misconfigured server (bad protocol address)	**Step 1** Check the server configuration file for the IP address of the host. **Step 2** Change if incorrect.

Possible Causes	Suggested Actions
Server requires default gateway configuration	**Step 1** Check the router configuration file for the **ip default-gateway** global configuration command, which defines a default gateway. **Step 2** Refer to the section "IP Default Gateway Configuration Notes" later in this chapter for more information about configuring default gateway support.
Misconfigured router (bad server address specification in **boot system** global configuration command)	**Step 1** Check the router configuration file for the boot server address (IP address of a TFTP server or MAC address of a MOP server). **Step 2** Change if necessary.
Misconfigured router (bad router address specification)	**Step 1** Check the router configuration file for the router address (IP address only). **Step 2** Change if not correct.
Misconfigured router (wrong filename)	**Step 1** Check the router configuration file for boot filename. **Step 2** Change as necessary. (Check the host's documentation for details about setting the name of the system image on the TFTP server.) Note that some versions of the ROM are case sensitive. Contact your router technical support representative for specific details.
Misconfigured router (wrong configuration register setting)	**Step 1** Check the configuration register setting for your system. (If you want to boot from a server over the network, you must set the configuration register appropriately. The specific configuration for netbooting depends on the platform that is being booted.) **Step 2** Determine whether you want to manually or automatically netboot from a TFTP server. To manually netboot, the configuration register must set to 0x0; otherwise, you will be netbooting automatically using the default system image name or one specified with the **boot system** global configuration command. Refer to your configuration, command reference, and hardware installation and maintenance publications for more details about setting the configuration register.
Incorrect filename	**Step 1** Compare the router image filename on the boot server with the name specified in the router configuration. **Step 2** Make sure they match.

Timeouts and Out-of-Order Packets Occur during Netbooting

Symptom: Timeouts (shown as periods on a netbooting display) and out-of-order packets (shown as uppercase Os) might prevent systems from netbooting. Depending on the cause, the number of timeouts and out-of-order packets indicated on the router's console display can vary—suggesting different underlying problems.

The following example shows a netbooting session that contains excessive timeouts and out-of-order packets:

```
Booting gs3-bfx from 131.108.1.123: !O.O!.O..O!!!OOO.O!!.O.O.....
```

It is possible that the client router will boot under this situation. However, when excessive timeouts and out-of-order packets are occurring, there is probably some kind of problem on the network, and netbooting (as well as network service availability) may be inconsistent.

Table 2-8 outlines possible causes and suggests actions to take when timeouts or out-of-order packets prevent a netboot.

Table 2-8 Router Startup: Timeouts and Out-of-Order Packets Prevent Booting

Possible Cause	Suggested Actions
Link is saturated	**Step 1** Boot the router from ROM and ping the server. Determine whether timeouts and out-of-order packets appear. **Step 2** Check local network concentrators for excessive collisions on the same network. (If excessive collisions are encountered, try reorganizing your network topology to reduce collisions.) **Step 3** Use an appropriate **show interfaces** EXEC command on routers in the path or place a network analyzer between the router and server. **Step 4** Look for dropped packets and output errors. **Step 5** If approximately 15 percent or more of the traffic is being dropped or any output errors occur, congestion might be the problem. **Step 6** Wait until the traffic subsides before attempting to netboot the router. If the problem is chronic, increase bandwidth or move the server closer to the router being booted.
Link is broken, possible routing loops	**Step 1** Check the continuity of the path from the booting router to the boot server using **ping** or **trace** EXEC commands. **Step 2** If a break is found, restore link between router and boot server.

Netbooting Problems Resulting from Invalid Routing Paths

Symptoms: As a TFTP client, the router can determine the path to a TFTP server using ARP. Using this technique, the router sends TFTP packets over the same path from which it received an ARP response. If this path becomes invalid, packets sent from the router to the server might fail even though the router has successfully received an ARP response to its ARP request. If the router is sending packets over an invalid path, a message similar to one of the following is displayed on the console:

```
Booting gs3-bfx!OOOO.........[timed out]

Booting gs3-bfx!.O.O.O.O.........[timed out]

Booting gs3-bfx!!!!!!!!!!OOOOOOOOOO.........[timed out]
```

In some cases, you also might notice that there is an initial response from a server, but that the netboot sequence still fails. The boot message would be similar to the following:

```
Booting gs3-bfx!.........[failed]
```

Note A limitation of proxy ARP is that a device can answer at any time, even after the router has received a response and identified a path to the server. The ARP implementation of the router uses the path designated by the most recent ARP response when routing traffic using ARP information.

Table 2-9 outlines possible causes and suggests actions when invalid routing paths prevent netbooting.

Table 2-9 Router Startup: Invalid Routing Paths Prevent Netbooting

Possible Cause	Suggested Actions
Bad routing paths on neighbor routers	**Step 1** Verify that neighbor routers can ping the server.
	Step 2 Use the **trace** EXEC command to determine their paths to the server.
	Step 3 Use the **show arp** or **show ip route** EXEC command to examine the ARP tables or IP routing tables of the neighbor routers to verify that the server is listed and that the routing table entries are appropriate.
	Step 4 Use the **clear arp-cache** and **clear ip-route** privileged EXEC commands as necessary.
	Step 5 Attempt to netboot the router again.

Possible Cause	Suggested Actions
Problems caused by multiple paths	**Step 1** Shut down all extra interfaces except the one over which you intend to netboot the router. **Step 2** Use the **no ip proxy-arp** interface configuration command on all neighboring routers to shut down their ability to provide proxy ARP responses. Make this change with care because it can cause problems for other network traffic. As an alternative, boot the router from ROM and configure the **ip default-gateway** global configuration command if you do not want to disable proxy ARP. Use of this command is discussed briefly in the following section "IP Default Gateway Configuration Notes." **Step 3** Try to netboot the router.

IP Default Gateway Configuration Notes

To send IP packets to other stations on the same network, an end station must have an IP address and a network mask. A router discovery protocol, such as the ICMP Router Discovery Protocol (IRDP) or the Gateway Discovery Protocol (GDP), can be used to learn new addresses. Another way to facilitate communication is to use proxy ARP, which, when supplied by a router, allows an end station to believe that other stations are on the same network, even though the other stations are actually behind the router that is supplying proxy ARP.

Some system images do not support IRDP, GDP, and proxy ARP. The system images that do not support IRDP, GDP, and proxy ARP are the igs-rxboot image, which is the system image stored in the Cisco 3000 EPROM, and the xx-rxboot image, which is the system image stored in the Cisco 4000 EPROM. These system images do not contain the IP routing software found in the EPROMs of other router models. Instead, they are smaller images that are capable of booting from Flash memory and of netbooting. When Flash memory does not contain a valid image, use the **copy tftp flash** privileged EXEC command to copy a fully functional system image from a TFTP server to Flash memory.

If you have booted a local router using the igs-rxboot image or the xx-rxboot image, and you need to obtain a system image from a TFTP server that is on a different network and the intervening router does not support IRDP, GDP, or proxy ARP for the port adjacent to the local router, the local router must have the **ip default-gateway** global configuration command in its configuration to identify the IP address of the intervening router.

Note During netbooting, IP routing information (including static routing information) is ignored, so the **ip default-gateway** global configuration command is also useful when netbooting a router that does include IP routing software in its EPROM.

Consider a case in which the Flash memory of a Cisco 2500, a Cisco 3000, or a Cisco 4000 has no usable image due to an error, such as copying an incorrect image to it. If a reboot occurs, the only image available to run is the xx-rxboot image. Use the **copy tftp flash** privileged EXEC command to copy a new system image to the Cisco 4000. Before you can use the **copy tftp flash** command, you must include the **ip default-gateway** global configuration command in the Cisco 4000's configuration to reach a remote TFTP server. A sample session illustrating the use these commands follows:

```
router(boot)# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ip default-gateway 130.108.1.7
^Z
%SYS-5-CONFIG_I: Configured from console by console
router(boot)# copy tftp flash
IP address or name of remote host [255.255.255.255]? server1
Name of tftp filename to copy into flash []? IJ09140Z
copy IJ09140Z from 131.131.101.101 into flash memory? [confirm] <Return>
xxxxxxxx bytes available for writing without erasure.
erase flash before writing? [confirm] <Return>
Clearing and initializing flash memory (please wait)####...
Loading from 131.131.101.101: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!... [OK - 324572/524212 bytes]
Verifying checksum...
VVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV...
Flash verification successful. Length = 1204637, checksum = 0x95D9
```

Client ARP Requests Time Out when Netbooting

Symptoms: When netbooting via a path that requires the client to use proxy ARP, the router being netbooted sends an ARP request to the server over every available network interface configured for IP. The router expects the server or an intermediate system to return an ARP response. If the router does not receive an ARP response, a message similar to the following is displayed at the console:

```
Booting gs3-bfx.........[timed out]
```

Table 2-10 outlines possible causes and suggests actions when client ARP requests time out during a netboot.

Table 2-10 Router Startup: Client ARP Requests Time Out during Netboot

Possible Cause	Suggested Actions
Wrong filename or other configuration problem	**Step 1** Check the filename definition and path specified on the server. **Step 2** Check the problems discussed earlier in this section under the symptom "Router Cannot Netboot from TFTP Server."
Intermediate routers have ARP filtering enabled	**Step 1** Boot the router from ROM. **Step 2** Make sure you can ping the server from the router. **Step 3** Try the **write network** privileged EXEC command to test TFTP connectivity with the server. **Step 4** If these steps are successful, at the intermediate router check the configuration using the **show arp** EXEC command. **Step 5** Enable the **debug arp** privileged EXEC command to determine whether neighbor proxy ARP responses are being generated. **Step 6** If the neighbor is not sending proxy ARP responses and its configuration contains the **no ip proxy-arp** interface configuration command, disable ARP filtering by removing the entry. Note that proxy ARP is enabled by default. **Step 7** If you need to have a **no ip proxy-arp** entry in the neighbor router configurations, use the **ip default-gateway** global configuration command in the router. Use of this command is discussed briefly in the section "IP Default Gateway Configuration Notes," earlier in this chapter.
Configuration of the serial interface on the router being netbooted includes a broadcast destination, but an intermediate router does not have the required IP helper address defined to point to the TFTP server	**Step 1** Check the configurations of all routers in the path. **Step 2** Include helper addresses as required using the **ip helper-address** interface configuration command. If you are unicasting to your server, you do not need to use the IP helper address, but if you are broadcasting to 255.255.255.255 (by omitting the IP address of the server), add the **ip helper-address** command on the *neighboring* router interface used in the netbooting broadcast.

Vector Errors Occur when IGS Attempts Netbooting

Symptom: For an IGS attempting netbooting, console display indicates "vector errors." Figure 2-1 illustrates an example of the kind of message that will appear.

Figure 2-1 Example Vector Error Output

```
vector=2, sr=0xFE0F2700, pc=0x10352D2
vector=2, sr=0xFE0F2700, pc=0x10352D2
vector=2, sr=0xFE0F2700, pc=0x10352D2
vector=2, sr=0xFE0F2700, pc=0x10352D2
vector=2, sr=0xFE0F2700, pc=0x10352D2
vector=2, sr=0xFE0F2700, pc=0x10352D2
vector=2, sr=0xFE0F2700, pc=0x10352D2
vector=2, sr=0xFE0F2700, pc=0x10352D2
vector=2, sr=0xFE0F2700, pc=0x10352D2
vector=2, sr=0xFE0F2700, pc=0x10352D2
vector=2, sr=0xFE0F2700, pc=0x10352D2
vector=2, sr=0xFE0F2700, pc=0x10352D2
vector=2, sr=0xFE0F2700, pc=0x10352D2
vector=2, sr=0xFE0F2700, pc=0x10352D2
vector=2, sr=0xFE0F2700, pc=0x10352D2
vector=2, sr=0xFE0F2700, pc=0x10352D2
vector=2, sr=0xFE0F2700, pc=0x10352D2
```

Table 2-11 outlines a possible cause and suggests actions when vector errors occur during a netboot.

Table 2-11 Router Startup: Vector Errors Occur during Netbooting

Possible Cause	Suggested Actions
The IGS is attempting to boot a compressed system image (for Software Release 9.0 and earlier versions)	**Step 1** On the boot server, check the software image file type. (For example, use the UNIX command **file** *image-name* at a UNIX-based server. If the file is compressed, the server will return a "compressed file" message.) **Step 2** Uncompress the file using the **uncompress** *image-name* command (in UNIX) or equivalent. **Step 3** Try to netboot the router.

Buffer Overflow Errors Occur when Netbooting

Symptom: When netbooting a router, the console display indicates that "buffer overflow" has occurred, and the router is unable to boot. Table 2-12 outlines possible causes and suggests actions when buffer overflows occur during the netboot process.

Table 2-12 Router Startup: Buffer Overflow Errors Occur during Netboot

Possible Cause	Suggested Actions
Not enough memory to boot image (Cisco 2500 and Cisco 4000)	**Step 1** Use the **show version** EXEC command to determine the amount of installed memory. **Step 2** Upgrade to 16 megabytes (MB) of memory.
Not enough memory to boot image (IGS)	**Step 1** Use the **show version** EXEC command to determine the amount of installed memory. **Step 2** Upgrade to 4 MB if necessary.
Not enough memory in router to boot image (CSC/3 card running Software Release 9.1)	**Step 1** For systems that have a CSC/3 card and 9.1 ROMs, you *must* netboot a compressed image. Compressed image files usually have names that end with a .Z extension (although this is not a requirement). Compressed images netboot exactly like uncompressed images; the router uncompresses the image after it is loaded. **Step 2** If the CSC/3 card is running Software Release 9.0 or 9.1, increase the memory efficiency of the decompression algorithm by upgrading to the maintenance release recommended by your technical support representative.

Undefined Load Module Error when Netbooting

Symptom: When netbooting a router, the console display indicates "undefined load module" error, and the router is unable to boot. Table 2-13 outlines a possible cause and suggests actions when an undefined load module error occurs during a netboot.

Table 2-13 Router Startup: Undefined Load Module Errors Occur during Netboot

Possible Cause	Suggested Actions
Attempting to netboot router configuration (text) file	**Step 1** If you are booting manually, refer to the *Getting Started Guide* for your router to see the proper command line format.
	Step 2 Check the router configuration file.
	Step 3 Compare the filename specified in the global configuration command **boot system** *filename* [*address*] entry with the actual router image filename. Make sure they match.
	Step 4 If they differ, change the name in the configuration file.

Note Remember to use the router image filename in the **boot system** global configuration command specification and the configuration filename with the **boot host** and **boot network** global configuration commands.

Router Cannot Boot from Another Router (TFTP Server)

Symptom: When booting a router from another router acting as a TFTP server, the router is unable to initialize properly. This symptom can be caused by *any* of the problems outlined in the preceding netbooting symptom discussions.

This section focuses on the problems of routers that are acting as TFTP servers. Table 2-14 outlines possible causes and suggests actions when a router cannot boot from other routers.

Table 2-14 Router Startup: Router Is Unable to Boot from Another Router

Possible Cause	Suggested Actions
Misconfigured TFTP server/router (missing or incorrect **tftp-server** global configuration command)	**Step 1** Use the **write terminal** privileged EXEC command to determine whether the **tftp-server system** global configuration command is missing or incorrectly specified. **Step 2** Add or modify the **tftp-server system** global configuration command as necessary on the router intended to be the TFTP server. Specify the name of a file in Flash memory.
Wrong/incomplete image in Flash memory	**Step 1** Use the **show flash** EXEC command to determine whether the image is incomplete. This display might show that the image is deleted and indicate the reason. Figure 2-2 shows an example of **show flash** output. Figure 2-3 illustrates the "wrong system software" message that is displayed when a router attempts to boot an incorrect image. In this case, the router is being booted from the ROM monitor. **Step 2** Obtain the correct image. (If necessary, contact your router technical support representative to determine which image is correct.) **Step 3** When you identify the correct image, use the privileged EXEC command **copy tftp flash** at the router to retrieve the image.

Figure 2-2 show flash Command Output Indicating Image Is Deleted

```
xx2# show flash
2048K bytes of flash memory sized on embedded flash.
File  name/status
 0  xx-k.914-0.16
 1  xx3-confg
 2  xx-k.91-4.2 [deleted] [invalid cksum]
 [0/2097152 bytes free/total]
```

S2609

Figure 2-3 ROM Monitor Output when Attempting to Boot an Incorrect Image

```
> b gs3-klingon 131.108.9.40

Booting gs3-klingon from 131.108.9.40: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK - 2056792/3394950 bytes]
F3: 2011628+45132+192972 at 0x1000

Wrong system software for this hardware
```

S2610

Local Timeouts Occur when Booting from ROM

Symptom: When a router is booting from ROM, the processor might be unable to access a portion of the system memory. If this is the case, the router will be unable to complete its boot process and will not start the ROM monitor. Table 2-15 outlines a possible cause and suggests actions when local timeouts occur when booting from ROM.

Table 2-15 Router Startup: Local Timeouts Occur when Booting from ROM

Possible Cause	Suggested Actions
Bad EPROM, bent pin, EPROM in wrong socket, or EPROM poorly seated (Generally, this only occurs if you have just replaced your system EPROMs.)	**Step 1** Power off system. **Step 2** Physically inspect each EPROM. **Step 3** Make sure each EPROM is correctly positioned in the socket (with notches properly aligned) in the correct socket. **Step 4** If a pin is bent, straighten it carefully. Reinstall the EPROM and power on the system. If a pin breaks off, the EPROM must be replaced. **Step 5** If an EPROM has been installed backward, and power has been applied to it, the EPROM has been damaged and must be replaced. **Step 6** If local timeouts persist, contact you router technical support representative.

Router Hangs after ROM Monitor Initializes

Symptom: When booting a Cisco 7000 series, AGS+, AGS, ASM-CS, MGS, IGS, or CGS router from ROM, the systems might hang after the ROM monitor initializes.

Table 2-16 outlines possible causes and suggests actions when a router hangs after the ROM monitor initializes.

Table 2-16 Router Startup: Router Hangs after ROM Monitor Initializes

Possible Cause	Suggested Actions
Incorrect EPROM size setting	**Step 1** Power off system. **Step 2** Inspect EPROM size jumper(s). Refer to the hardware installation and maintenance publication for your router to determine the proper setting. **Step 3** Modify as required.
Configuration register is not set correctly	**Step 1** Power off system. **Step 2** Check your configuration settings (boot ROM jumpers and software configuration). If no jumper is set at bit 0, and no other boot field is defined, you must reconfigure your system so that it can boot properly. **Step 3** To enable your router to boot properly, do one of the following: • Configure the software configuration register of the router using the **config-register** *value* global configuration command. (This applies to the IGS, Cisco 2500, Cisco 3000, and Cisco 7000 platforms running Cisco Internetwork Operating System (Cisco IOS) Release 10.0 or later in the EPROM.) • Set the boot ROM jumper to permit booting. • Include the correct **boot system** global configuration commands to boot the system. • Set bit 0 to a value of 1 to force booting from ROM. • Refer to your configuration, reference, and hardware installation and maintenance publications for more information about configuring your router for the various booting options.

Router Is Stuck in ROM Monitor Mode

Symptom: When booting a router from ROM, the system boots into ROM monitor mode, but does not boot the complete system image. Table 2-17 outlines possible causes and suggests actions when a router is stuck in ROM monitor mode.

Table 2-17 Router Startup: Router Is Stuck in ROM Monitor Mode

Possible Cause	Suggested Actions
Incorrect configuration register setting	**Step 1** At ROM monitor prompt (>), enter **b** to boot the system. **Step 2** If a configuration exists in NVRAM, the system will display the vacant message. Press the Return key to continue. If a configuration does not exist in NVRAM, the setup menu appears. For the purposes of this activity, skip the setup process. **Step 3** Use the **show version** EXEC command to determine the configuration register setting. **Step 4** Look for an invalid configuration register setting. The default is 0x101, which disables the Break key and forces the router to boot from ROM. A typical "bad" setting has a zero in the least significant bit (for example 0x100). (For more details about setting the configuration register, refer to your hardware installation and maintenance publication.)
Break key pressed during boot process (Software Release 9.1 and later)	**Step 1** At the ROM monitor prompt, enter **c** to allow router to continue booting.
Console cable inserted or removed during boot process, or console power-cycled during boot process (Software Release 9.1 or later)	**Step 1** Press the Return key. **Step 2** Look for the ROM monitor prompt (>). **Step 3** If this prompt appears, enter **c** at the prompt to continue the booting process.

Scrambled Output when Booting from ROM

Symptom: When booting from ROM, the router displays indecipherable textual output on the monitor. Table 2-18 outlines possible causes and suggests actions when output is scrambled while booting from ROM.

Table 2-18 Router Startup: Scrambled Output when Booting from ROM

Possible Cause	Suggested Actions
Wrong terminal speed setting or wrong configuration register setting	**Step 1** Use the monitor setup menu to check the terminal line speed setting for the monitor. **Step 2** Check the terminal speed configured on the router as specified in the configuration register setting (default is 9600 baud, 8 databits, 2 stop bits, and no parity). **Step 3** If the terminal speed of the monitor and the router do not match, modify as necessary. (Refer to your hardware installation and maintenance documentation for details about setting up the monitor.)
Bad router hardware An example is a bad dual universal asynchronous receiver transmitter (DUART). The DUART controls the system console and auxiliary ports. A failed DUART causes the far left LED on a CSC/3 or CSC/4 card to blink repeatedly.	**Step 1** Troubleshoot router hardware as discussed in the section "Diagnosing Router Hardware Problems," earlier in this chapter.

Vector Error Occurs when Booting from Flash Memory

Symptom: When booting a router from Flash memory, the system display indicates that a vector error occurred. Table 2-19 outlines possible causes and suggests actions when vector errors occur when booting from Flash memory.

Table 2-19 Router Startup: Vector Errors Occur when Booting from Flash Memory

Possible Cause	Suggested Actions
Compressed system image (Cisco 2000, Cisco 2500, Cisco 3000, and Cisco 4000)	**Step 1** Power cycle the router. **Step 2** Within the first minute of booting, press the Break key to access the ROM monitor. **Step 3** At the ROM monitor prompt (>), enter **o/r** (without arguments) to set the configuration register to boot from ROM. **Step 4** Enter **b** to boot (router enters setup mode). **Step 5** Press **Ctrl-C** to bypass setup. **Step 6** Enter the **configure memory** privileged EXEC command. **Step 7** Obtain an uncompressed system image. You can do this as follows: From the router prompt, use the privileged EXEC command **copy flash tftp** to send the compressed image back to the TFTP server. Uncompress the image at the TFTP server. (This cannot be done at a router.) **Step 8** Use the **copy tftp flash** privileged EXEC command at the router to retrieve the uncompressed image. **Step 9** Check the configuration register using the **show version** EXEC command. Set the router to boot from Flash memory (for example, 0x102). **Step 10** Use the **write terminal** privileged EXEC command to determine whether the router configuration includes the **boot system flash** global configuration command in the correct order with respect to the other **boot system** commands. Include the **boot system flash** command if it is missing. Confirm that the order of **boot system** commands is correct. Use the **write memory** command to save this change. **Step 11** Enter the **reload** privileged EXEC command to restart the box.
Bad router hardware	**Step 1** Troubleshoot router hardware as discussed earlier in this chapter.

Note The **boot system** global configuration commands are saved in the same order in which they were entered. The most recent entry goes to the bottom of the list.

Router Partially Boots from Flash and Display Shows Boot Prompt

Symptom: When booting a router from Flash memory, the boot process halts and the router displays the boot [router(boot)>] prompt. In addition, the router will not route, although the EXEC commands may appear to be operational. This symptom only applies to Cisco 2000, Cisco 2500, Cisco 3000, and Cisco 4000 routers.

Table 2-20 outlines possible causes and suggests actions when a router boots partially and displays the router(boot)> prompt on the console.

Table 2-20 Router Startup: Router Boots Partially and Displays router(boot)> Prompt

Possible Cause	Suggested Actions
No system image in Flash memory	**Step 1** Use the **show flash** EXEC command to determine whether an image exists in Flash memory. **Step 2** If no image exists, use the **copy tftp flash** privileged EXEC command to copy the system image from your TFTP server to the router's Flash memory. See the section "IP Default Gateway Configuration Notes," earlier in this chapter, for extra steps that you might have to perform. **Step 3** Enter the privileged EXEC command **reload** to boot the router.
Misconfigured router (missing **boot system flash** global configuration command)	**Step 1** Enter enabled mode. **Step 2** Use the **write terminal** privileged EXEC command to determine whether the active configuration includes an entry for the **boot system flash** global configuration command. Use the **show configuration** privileged EXEC command to determine if the **boot system flash** command is included in the configuration stored in NVRAM. **Step 3** Check the order of the **boot system** commands. For the recommended ordering, refer to the section "Using a Fault-Tolerant Boot Strategy" earlier in this chapter. **Step 4** Add the **boot system flash** command or reorder the **boot system** commands if necessary. **Step 5** Save the configuration change to NVRAM using the **write memory** privileged EXEC command.
Misconfigured configuration register	**Step 1** Check the configuration register setting; make sure it is set to boot from Flash memory (for example, 0x102). **Step 2** Refer to your hardware installation and maintenance publication for details regarding configuration register settings.

Router Fails to Boot from Flash Memory

Symptom: When booting a router from Flash memory, the boot process appears to complete, but the router does not route traffic or communicate with neighbors. The EXEC might or might not function. Table 2-21 outlines possible causes and suggests actions when a router fails to boot from Flash memory.

Table 2-21 Router Startup: Router Fails to Boot from Flash Memory

Possible Cause	Suggested Actions
Incorrect or corrupted image; EXEC does not function	**Step 1** Check the configuration register using the **show version** EXEC command. Set the register to boot from Flash memory (for example, 0x2102). **Step 2** Power-cycle the router. **Step 3** Within the first minute of booting, press the Break key to access the ROM monitor. **Step 4** At the ROM monitor prompt (>), enter **o/r 0x1** to set the configuration register to boot from ROM. **Step 5** Enter **i** to reinitialize router, which causes the router to enter setup mode. **Step 6** Obtain the correct system image. (If necessary, contact your router technical support representative to determine which image is correct.) **Step 7** Once the correct image is identified, use the privileged EXEC command **copy tftp flash** at the router to retrieve the image. **Step 8** Check the configuration register using the **show version** EXEC command. Set the register to boot from Flash memory (for example, 0x102). For information about configuration register settings, refer to your hardware installation and maintenance documentation. **Step 9** Use the **write terminal** privileged EXEC command to determine whether the router configuration contains the **boot system flash** global configuration command. NOTE: Issuing the **write memory** command at this point on a Cisco 2500 series, Cisco 3000 series, Cisco 4000 series, or Cisco 7000 series will overwrite the configuration. Make sure you have a backup of your configuration file. **Step 10** Include the **boot system flash** command if it is not in the configuration. Be sure to use the **write memory** command after this change. **Step 11** Enter the privileged EXEC command **reload** to restart the router.

Possible Cause	Suggested Actions
Incorrect or corrupted image; EXEC functions	**Step 1** Find a correct system image. (If necessary, contact your router technical support representative to determine which image is appropriate.) **Step 2** Once the correct image is identified, use the privileged EXEC command **copy tftp flash** at the router to retrieve the image. **Step 3** Check the configuration register using the **show version** EXEC command. Set the register to boot from Flash memory (for example, 0x102). For information about configuration register settings, refer to your hardware installation and maintenance documentation. **Step 4** Use the **write terminal** privileged EXEC command to determine whether the active configuration contains **boot system flash** global configuration command. Use the **show configuration** privileged EXEC command to determine if the **boot system flash** command is included in the configuration stored in NVRAM. **Step 5** Include the **boot system flash** command if it is not in the configuration. Be sure to use the **write memory** privileged EXEC command to save your modification after this change. **Step 6** Enter the **reload** privileged EXEC command to restart the router.

Terminal Connected to Unconfigured Access Server Is Unresponsive

Symptom: A terminal connected to the console port of an unconfigured Cisco access server (currently, the Cisco 2500 series access servers are the only Cisco devices that have an RJ-45-based console port) displays bootup banners and begins the Setup routine, but the user cannot input commands from the terminal keyboard. Table 2-22 describes possible causes and suggests actions for an unresponsive terminal connection to an unconfigured access server.

Table 2-22 Router Startup: Unresponsive Terminal Connection to Unconfigured Access Server

Possible Causes	Suggested Actions
Flow control configured on the terminal conflicts with the EIA/TIA-232 control signals supported by the access server console port (RJ-45 to DB-25)	**Step 1** Check if flow control is configured on your terminal. **Step 2** Disable all flow control on the terminal. With flow control enabled, the terminal will wait indefinitely for a CTS (Clear to Send) signal because the RJ-45 console port on the access server does not assert CTS. For information on how to check for and disable flow control on your specific terminal, consult the documentation provided by your terminal manufacturer. **Step 3** Alternately, you can "strap CTS high" by providing the proper voltage on the CTS signal lead to make the signal active. Find an unused signal that is known to be active and "strap," or short, CTS to it. The terminal sees CTS being asserted (indicating that the access server is ready to receive data) and allows input to be entered. **Step 4** On an already configured access server, another alternate solution is to connect your terminal to the auxiliary port of the access server. The auxiliary port, unlike the console port, does assert CTS and the terminal will therefore allow input. However, on a brand new access server with no configuration, this is *not* an alternative, because the bootup banners and Setup routine are seen only on the console port.
Hardware problem	**Step 1** Check all hardware for damage, including cabling (broken wire), adapters (loose pin), access server ports, and the terminal itself. **Step 2** Replace any hardware that is damaged or excessively worn.

Recovering a Lost Password

The following procedures describe the steps required to recover a lost login or enable password. The procedure differs depending on the platform and the software used, but in all cases, password recovery requires that the router be taken out of operation and powered down. Should you need to perform one of the following procedures, make certain that there are secondary systems that can temporarily serve the functions of the router undergoing the procedure. If this is not possible, advise all potential users and, if possible, perform the procedure during low use hours. Finally, be aware of the possible consequences of removing and reinserting a router on a functioning network.

Note Making a note of your password and storing it in a secure place is recommended.

All of the procedures for recovering lost passwords depend upon changing the configuration register of the router. Depending on the platform and software you are using, this will be done by reconfiguring the router software or by physically moving a jumper or dual inline package (DIP) switch on the router. Table 2-23 shows which platforms have configuration registers in software and which require that you change the jumper or DIP switch position to change the configuration register.

Table 2-23 Configuration Registers for Specific Cisco Platforms and Software

Platform (and Software, if Applicable)	Software Configuration Register	Hardware Configuration Register (Jumper)	Hardware Configuration Register (DIP Switch)
Cisco 2000 series	Yes	–	–
Cisco 2500 series	Yes	–	–
Cisco 3000 series	Yes	–	–
Cisco 4000 series	Yes	–	–
Cisco 7000 series running Software Release 9.17(4) or later (Flash/netboot) or Cisco IOS Release 10.0 or later (ROM)	Yes	–	–
Cisco 7000 running Software Release 9.21 or earlier from ROM	–	Yes	–
Cisco IGS running Software Release 9.1 or later	Yes	–	–
Cisco IGS running software prior to Software Release 9.1	–	–	Yes
Cisco CGS	–	Yes	–
Cisco MGS	–	Yes	–
Cisco AGS	–	Yes	–
Cisco AGS+	–	Yes	–

Password Recovery Procedure: Platforms Running Current Cisco IOS Releases

The more recent platforms produced by Cisco run from Flash memory or are netbooted and have the capability to ignore the contents of NVRAM upon booting. (Cisco 7000 series routers that boot from Flash memory or netboot have this capability as well; a Cisco 7000 that boots from ROM has this capability if it is running Cisco IOS Release 10.0 or later.) Ignoring the contents of NVRAM permits you to bypass the configuration file (which contains the passwords) and gain complete access to the router. You can then recover the lost password(s) or configure new ones.

Note If your password is encrypted, you cannot recover it. You must configure a new password.

Figure 2-4 shows a flow chart describing the password recovery procedure for the following platforms:

- Cisco 2000, Cisco 2500, Cisco 3000, and Cisco 4000 series access servers and routers
- Cisco 7000 series routers running Software Release 9.17(4) and later from Flash/netboot *or* Cisco IOS Release 10.0 or later from ROM
- Cisco IGS routers running Software Release 9.1 or later
- Cisco CGS, MGS, AGS, and AGS+ routers running Software Release 9.1(7) or later
- Cisco 7000 series routers running Software Release 9.17(4) through 9.21 from ROM

Figure 2-4 illustrates the password recovery procedure for all of these platforms. Some of these platforms are configurable in software and do not require a hardware change. Others require that you physically change the position of the configuration register jumper on the processor card. Figure 2-4 shows diverging paths, when necessary, to take you through the steps required for the platform and software with which you are working. Refer to Table 2-23 to determine if the platform with which you are working is configurable in the software, or if it requires you to physically move the jumper.

The following procedure describes the password recovery process for the following platforms *only*:

- Cisco 2000, Cisco 2500, Cisco 3000, and Cisco 4000 series routers
- Cisco 7000 series routers running Software Release 9.17(4) or later (Flash memory or netboot) or Cisco IOS Release 10.0 or later from ROM
- Cisco IGS Running Software Release 9.1 or later

For the platforms listed, be certain to follow the path shown in the flowchart (see Figure 2-4) labeled "Cisco 2000, 2500, 3000, 4000 series; Cisco 7000 series running Software Release 9.17(4) or later (Flash/netboot) or Cisco IOS Release 10.0 or later (ROM); IGS running Software Release 9.1 or later."

For the step-by-step password recovery sequence for other platforms, see one of the following sections: "Password Recovery Procedure: Platforms Running Recent Software Releases," "Password Recovery Procedure: Platforms Running Earlier Software Releases," "Password Recovery Procedure: IGS Running Software Prior to Software Release 9.1," or "Password Recovery Procedure: Cisco 500-CS Communication Server."

Note To complete this procedure, you must have a terminal or a personal computer (running terminal emulation software) connected to the console port of the router. In addition, you should know the key sequence necessary to issue the **break** command from your terminal.

Following is the password-recovery procedure for Cisco platforms running current Cisco IOS software:

Step 1 Power cycle the router. (This consists of turning off the power to the router and turning it back on again.)

Step 2 Issue the **break** key sequence for your terminal or terminal emulation software within 60 seconds of turning on the power.

The ROM monitor (>) prompt will appear.

Step 3 Enter the command, **e/s 2000002**. (For Cisco 7000 series routers, enter **e/s XXXXXXXX**.) This command examines the short (16 bit) memory location for the software configuration register.

Record the output resulting from this command. This is the software configuration register value.

Note In this procedure, 2102 is used as an example software configuration register value.

Step 4 Enter the **q** (quit) command to return to the ROM monitor (>) prompt.

Step 5 Enter the **o/r 0x42** command. (For a Cisco 2500, use the command **0x041**.) The value 42 (or 41 on a Cisco 2500) sets the software configuration register bit to position 6, which allows the router to ignore the contents of NVRAM when booting. (Be sure to enter **0x** followed by the configuration register value.)

Step 6 Enter the **i** (initialize) command at the ROM monitor (>) prompt. The router will reboot.

Step 7 Answer **no** to all of the Setup questions.

Step 8 Enter the **enable** EXEC command at the Router> prompt.

Step 9 If your password is clear text (is not encrypted), proceed to Step 13.

or

If your password is encrypted, continue with Step 10.

Step 10 If your password is encrypted, enter the **configure memory** privileged EXEC command. This writes the stored configuration into running memory.

Step 11 Enter the **configure terminal** privileged EXEC command to enter router configuration mode.

Step 12 If you lost the enable password, use the **enable-password** global configuration command to configure a new password and press **^Z** to exit configuration mode.

or

If you lost the login password, configure the console line using the **login** and **password** line configuration commands. Enter **^Z** to exit configuration mode and proceed to Step 15.

Step 13 If your password is clear text (is not encrypted), enter the **show configuration** privileged EXEC command to view the current configuration.

Step 14 If you lost the enable password, locate the **enable-password** global configuration command entry in the configuration and record the password.

or

If you lost the login password, find the configuration entries for the console line and record the password indicated by the **password** line configuration command.

Step 15 Issue the **write memory** privileged EXEC command to write the configuration into running memory.

Caution Issuing the **write memory** command at this point on a Cisco 2500, Cisco 3000, or Cisco 4000 will overwrite the configuration. Make certain you have a backup of your configuration file.

Step 16 The router is now fully functional, and you can use your recovered or reconfigured password(s) as usual.

Note Restore the software configuration register to its original value as soon as possible. If it is not returned to the value you noted in Step 3, the router will always ignore the contents of NVRAM and enter the Setup routine upon booting. Continue with Step 17 to return the software configuration register to its original value.

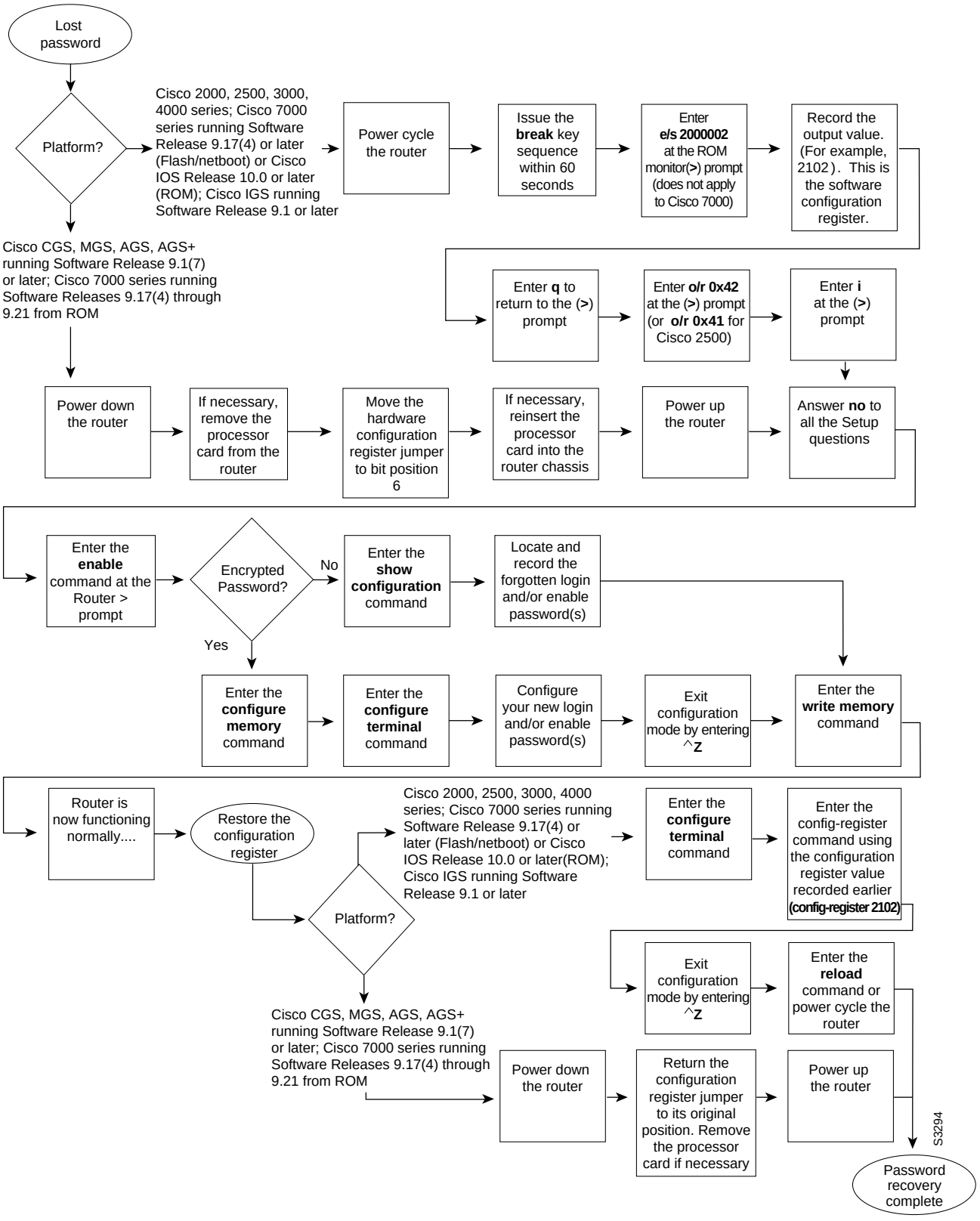
Step 17 In privileged EXEC mode, enter router configuration mode using the **configure terminal** privileged EXEC command.

Step 18 Change the software configuration register to its original value using the **config-register** global configuration command. You must enter **0x** and then the software configuration register value that you recorded in Step 3. Using the example value of 2102, the command would be **config-register 0x2102**.

Step 19 Exit from router configuration mode by entering **^Z**.

The next time the router is power cycled or restarted with the **reload** privileged EXEC command, the bootup process will proceed as normal. Use your new or recovered password to gain access to the router after it reboots.

Figure 2-4 Password Recovery: Platforms Running Current Cisco IOS Releases and Recent Software Releases



Password Recovery Procedure: Platforms Running Recent Software Releases

The Cisco CGS, MGS, AGS, and AGS+ platforms, and Cisco 7000 series routers running software prior to Cisco IOS Release 10.0 from ROM, all have their configuration registers in hardware, so you must physically change the position of the configuration register jumper during the password recovery process. It may be necessary to remove the processor card from the router chassis in order to access the hardware configuration register jumper. Consult your hardware documentation for detailed instructions on removing and inserting the processor card from the router chassis if necessary.

Moving the hardware configuration register jumper to bit position 6 allows the router to ignore the contents of NVRAM while booting. This permits you to bypass the configuration file (and therefore the passwords) and gain complete access to the router. You can then recover the lost password(s) or configure new ones.

Note If your password is encrypted, you cannot recover it. You must configure a new password.

Figure 2-4 shows a flow chart describing the password recovery procedure for the following platforms:

- Cisco 2000, Cisco 2500, Cisco 3000, and Cisco 4000 series access servers and routers
- Cisco 7000 series routers running Software Release 9.17(4) and later from Flash memory/netboot

  or

  Cisco 7000 series routers running Cisco IOS Release 10.0 or later from ROM
- Cisco IGS routers running Software Release 9.1 or later
- Cisco CGS, MGS, AGS, and AGS+ routers running Software Release 9.1(7) or later
- Cisco 7000 series routers running Software Release 9.17(4) through 9.21 from ROM

Figure 2-4 illustrates the password recovery procedure for all of these platforms. Some of these platforms are configurable in software and do not require a hardware change. Others require that you physically change the position of the configuration register jumper on the processor card. Figure 2-4 takes you through the steps required for the platform and software with which you are working, and shows diverging paths when necessary to account for platform-specific requirements. Refer to Table 2-23 to determine if the platform on which you are working is configurable in the software, or if it requires you to physically move the jumper.

The following textual procedure describes the password recovery process for the following platforms *only*:

- Cisco CGS, MGS, AGS, and AGS+ routers running Software Release 9.1(7) and later
- Cisco 7000 series routers running Software Release 9.17(4) through 9.21 from ROM

For these platforms, follow the path shown in the flowchart (see Figure 2-4) labeled “Cisco CGS, MGS, AGS, AGS+ running Software Release 9.1(7) or later; Cisco 7000 series running Software Release 9.17(4) through 9.21 from ROM.”

For the step-by-step password recovery sequence for other platforms, see one of the following sections: “Password Recovery Procedure: Platforms Running Current Cisco IOS Releases,” “Password Recovery Procedure: Platforms Running Earlier Software Releases,” “Password Recovery Procedure: IGS Running Software Prior to Software Release 9.1,” or “Password Recovery Procedure: Cisco 500-CS Communication Server.”

Note To complete this procedure, you must have a terminal or a personal computer (running terminal emulation software) connected to the console port of the router.

Following is the password-recovery procedure for Cisco platforms running recent software releases:

Step 1 Power down the router.

Step 2 Change the hardware configuration register by moving the jumper from bit position 0 (zero) or 1 to bit position 6.

This will force the router to ignore the contents of NVRAM, and therefore the configuration file, after it loads the operating system. Note the original position of the jumper.

Note To move the hardware configuration register jumper, you might need to remove the processor card from the router chassis. This is the case with the Route Processor (RP) card in Cisco 7000 series routers. Consult your hardware documentation for complete instructions on removing and inserting the processor card. If you had to remove the processor card, reinsert it before continuing.

Step 3 Power up the router.

The router will boot but will ignore the contents of NVRAM and enter the Setup routine.

Step 4 Answer **no** to all of the Setup questions.

The Router> prompt appears.

Step 5 Enter the **enable** EXEC command.

Step 6 If the password is clear text (is not encrypted), go to Step 10. If the password is encrypted, continue with Step 7.

Step 7 If the password is encrypted, enter the **configure memory** privileged EXEC command. This writes the stored configuration into running memory.

Step 8 Enter the **configure terminal** privileged EXEC command to enter router configuration mode.

Step 9 If you have lost the enable password, use the **enable-password** global configuration command to configure a new password. If you have lost the login password, configure the console line with a new login password using the **login** and **password** line configuration commands. Press **^Z** to exit configuration mode. Proceed to Step 12.

Step 10 If your password is clear text (is not encrypted), enter the **show configuration** privileged EXEC command.

Step 11 If you have lost the enable password, locate the **enable-password** global configuration command entry and record the password. If you have lost the login password, find the configuration entries for the console line and record the password indicated by the **password** line configuration command.

Step 12 Issue the **write memory** privileged EXEC command to write the configuration into running memory.

Step 13 The router is now fully functional and you can use your recovered or reconfigured password(s) as usual.

Note Return the hardware configuration register jumper to its original position as soon as possible. If the jumper is not returned to the bit position you noted in Step 2, the router will always ignore the contents of NVRAM and enter the Setup routine upon booting. Continue with Step 14 to return the jumper to its original position.

Step 14 Power down the router.

Step 15 Move the hardware configuration register jumper from bit position 6 to its original position (the position you noted in Step 2).

It might be necessary to remove the processor card to gain access to the jumper. Consult your hardware documentation for complete instructions on removing and inserting the processor card if necessary. If you had to remove the processor card, reinsert it before continuing.

Step 16 Power up the router. Use your new or recovered password to gain access to the router.

Password Recovery Procedure: Platforms Running Earlier Software Releases

Cisco CGS, MGS, AGS, and AGS+ platforms, and Cisco 7000 series routers running software prior to Cisco IOS Release 10.0 from ROM, all have their configuration registers in the hardware, so you must physically change the position of the configuration register jumper during the password recovery process. It might be necessary to remove the processor card from the router chassis in order to access the hardware configuration register jumper. Consult your hardware documentation for detailed instructions on removing and inserting the processor card from the router chassis if necessary.

Note It is important to remember that if your password is encrypted, you cannot recover it. You must configure a new password.

Figure 2-5 shows a flowchart that describes the password recovery procedure for the following platforms:

- CGS, MGS, AGS, and AGS+ routers running Software Release 9.1(6) and earlier
- Cisco 7000 series routers running Software Release 9.17(3) and earlier from ROM

The step-by-step procedure that follows and the password recovery flow chart shown in Figure 2-5 apply only to the indicated platforms running the indicated software. There is another procedure for recovering a password on these platforms if they are running more recent software. See the previous section, “Password Recovery Procedure: Platforms Running Recent Software Releases.”

Note To complete this procedure, you must have a terminal or a personal computer (running terminal emulation software) connected to the console port of the router.

Following is the password-recovery procedure for Cisco platforms running earlier software releases:

Step 1 Power down the router.

Step 2 Change the hardware configuration register by moving the jumper from bit position 0 (zero) or 1 to bit position 15.

Note the original position of the jumper.

Note To move the hardware configuration register jumper, you might need to remove the processor card from the router chassis. This is the case with the Route Processor (RP) card in Cisco 7000 series routers. Consult your hardware documentation for complete instructions on removing and inserting the processor card. If you had to remove the processor card, reinsert it before continuing.

Step 3 Power up the router. The ROM monitor (>) prompt appears.

Step 4 Enter the **b** (bootstrap) command at the (>) prompt.

Step 5 Press the Return key until the Test-System> prompt appears.

Step 6 Enter privileged mode by issuing the **enable** EXEC command.

Step 7 If the password is clear text (is not encrypted), go to Step 12.

or

If the password is encrypted, continue with Step 8.

Step 8 If the password is encrypted, enter the **configure memory** privileged EXEC command.

This writes the stored configuration into running memory.

Step 9 Enter the **configure terminal** privileged EXEC command to enter router configuration mode.

Step 10 If you have lost the enable password, use the **enable-password** global configuration command to configure a new password and press **^Z** to exit configuration mode.

or

If you have lost the login password, configure the console line with a new password using the **login** and **password** line configuration commands. Press **^Z** to exit configuration mode.

Step 11 Issue the **write memory** privileged EXEC command to write the configuration into running memory. Proceed to Step 14.

Step 12 If your password is clear text (is not encrypted), enter the **show configuration** privileged EXEC command.

Step 13 If you have lost the enable password, locate the **enable-password** global configuration command entry in the configuration and record the password.

or

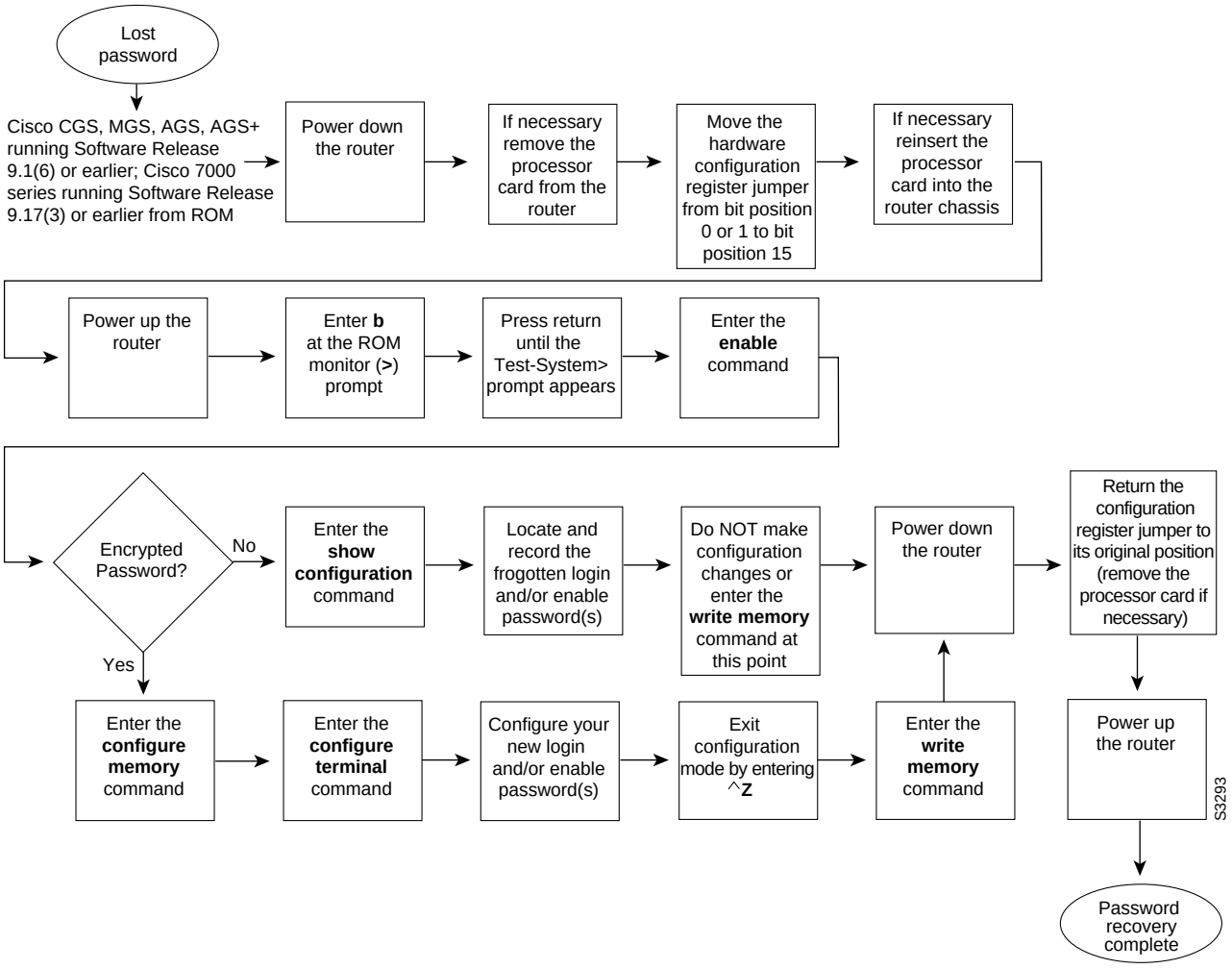
If you have lost the login password, find the configuration entries for the console line and record the password indicated by the **password** line configuration command. Do *not* make configuration changes or use the **write memory** command at this time.

Step 14 Power down the router.

Step 15 Remove the processor card and move the hardware configuration register jumper from bit position 15 to its original position (the position you noted in Step 2).

Step 16 Power up the router. Use your new or recovered password to gain access to the router.

Figure 2-5 Password Recovery: Platforms Running Earlier Software Releases



Password Recovery Procedure: IGS Running Software Prior to Software Release 9.1

Cisco IGS routers have a bank of DIP switches located on the rear panel. These DIP switches are used to set the hardware configuration register and must used in the password recovery process if the router is running system software prior to Software Release 9.1.

Figure 2-6 shows the password recovery procedure for the Cisco IGS running software prior to Software Release 9.1. There is another procedure for the IGS platform if it is running Software Release 9.1 or later. See the section, “Password Recovery Procedure: Platforms Running Current Cisco IOS Releases.”

Note It is important to note that if your password is encrypted, you cannot recover it. You must configure a new password.

Note To complete this procedure, you must have a terminal or a personal computer (running terminal emulation software) connected to the console port of the router.

Following is the password-recovery procedure for IGS routers running software prior to Software Release 9.1:

Step 1 Power down the router.

Step 2 Record the settings of the DIP switches located on the rear panel of the router. You will need to return these switches to their original positions after you have recovered your password.

Step 3 Set switch number 7 to the ON position (down).

Step 4 Set switches 0–3 to the OFF position (up).

Step 5 Power up the router.

The router will boot up, and the terminal will display the ROM monitor (>) prompt.

Step 6 Enter the **b** (bootstrap) command at the (>) prompt.

Step 7 Press the Return key until the Test-System> prompt appears.

Step 8 Enter the **enable** privileged EXEC command at the Test-System> prompt.

Step 9 If the password is clear text (is not encrypted), go to Step 14.

or

If the password is encrypted, continue with Step 10.

Step 10 If the password is encrypted, enter the **configure memory** privileged EXEC command. This writes the stored configuration into running memory.

Step 11 Enter the **configure terminal** privileged EXEC command to enter router configuration mode.

Step 12 If you have lost the enable password, use the **enable-password** global configuration command to configure a new password and press **^Z** to exit configuration mode.

or

If you have lost the login password, configure a new password on the console line using the **login** and **password** line configuration commands. Press **^Z** to exit configuration mode.

Step 13 Enter the **write memory** privileged EXEC command to write the configuration changes into stored memory. Proceed to Step 16.

Step 14 If your password is clear text (is not encrypted), enter the **show configuration** privileged EXEC command.

Step 15 If you have lost the enable password, locate the **enable-password** global configuration command entry in the configuration and record the password.

or

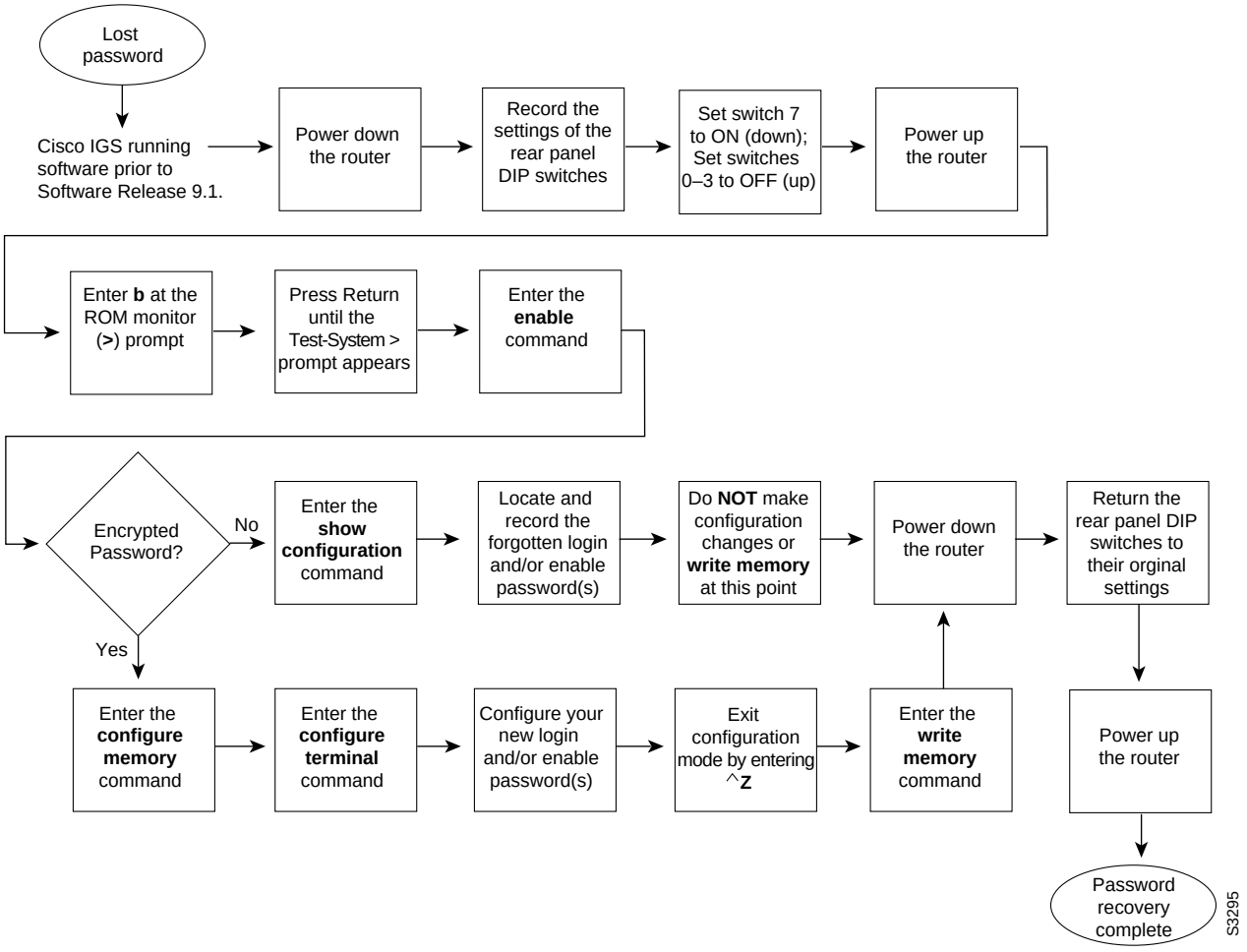
If you have lost the login password, find the configuration entries for the console line and record the password indicated by the **password** line configuration command. Do *not* make configuration changes or issue the **write memory** command at this time.

Step 16 Power down the router.

Step 17 Return the hardware configuration register DIP switches located on the back panel of the router to their original settings (the settings you noted in Step 2).

Step 18 Power up the router. Use your new or recovered password to gain access to the router.

Figure 2-6 Password Recovery: IGS Running Software Release Prior to 9.1



Password Recovery Procedure: Cisco 500-CS Communication Server

Lost passwords cannot be recovered from Cisco 500-CS communication servers. The only way to recover from a lost password is to return the communication server to its factory default configuration using the reset button located on the top of the case.

The following procedure describes how to restore the Cisco 500-CS to its default configuration:

Step 1 Power down the communication server.

Step 2 Press and hold down the reset button on the top of the case while turning on the power to the communication server.

Step 3 The 500-CS is returned to its factory default configuration.

You must reconfigure the communication server. For information on configuring a Cisco 500-CS communication server, consult the *Access and Communication Servers Configuration Guide* and the *Access and Configuration Servers Command Reference* publications.

CHAPTER 3

Troubleshooting Serial Line Problems

There are a variety of tools and techniques to troubleshoot serial line problems. This chapter includes the following sections that discuss a range of universally applicable tools for troubleshooting serial links:

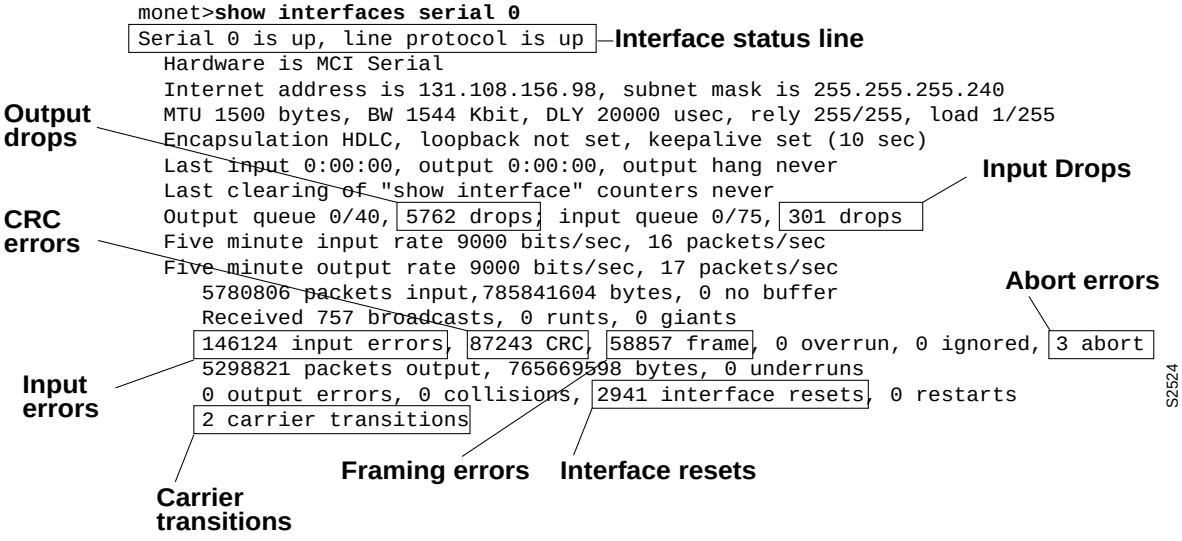
- Using the show interfaces Command to Troubleshoot Serial Lines—This section discusses the **show interfaces serial** *number* EXEC command and explains the various fields that appear in the output. For complete details about variables and options for **show** commands, refer to the *Router Products Configuration Guide* and *Router Products Command Reference* publications.
- Using the show controllers Command to Troubleshoot Serial Lines—This section discusses the various **show controllers** EXEC commands and provides an explanation of some of the important fields that appear in the output. For complete details about variables and options for **show** commands, refer to the *Router Products Configuration Guide* and *Router Products Command Reference* publications.
- Using debug Commands to Troubleshoot Serial Lines—This section describes important **debug** commands. Details about **debug** commands are provided in the *Debug Command Reference* publication.
- Troubleshooting Clocking Problems—This section discusses serial line clock issues and troubleshooting techniques.
- Using Extended ping Tests to Troubleshoot Serial Lines—This section discusses the use of extended **ping** tests.
- Adjusting Buffers to Ease Overutilized Serial Links—This section provides information on adjusting the size of buffers and queues.
- Special Serial Line Tests—This section discusses local and remote channel service unit (CSU) and data service unit (DSU) loopback tests.
- Troubleshooting Access Server to Modem Connectivity—This section discusses common modem connection problems and includes a number of symptom modules that address specific symptoms and suggest specific solutions.

Using the show interfaces Command to Troubleshoot Serial Lines

The **show interfaces** EXEC command is an important and useful show command. The specific information displayed depends on the interface type being examined (serial, Ethernet, Token Ring, or FDDI) and the type of encapsulation being used on the network (such as X.25 or Switched Multimegabit Data Service [SMDS]). This discussion focuses on information in the serial version of the display and outlines the specific fields used to diagnose serial line connectivity problems in a wide-area network (WAN) environment.

Figure 3-1 illustrates the **show interfaces serial** *number* EXEC command output for a High-Level Data Link Control (HDLC) serial interface. The interface is not running packet-switched software. The fields presented in this display are detailed in the *Router Products Configuration Guide* and *Router Products Command Reference* publications. This section describes the fields that are particularly important for diagnosing serial line problems.

Figure 3-1 Output from the HDLC Version of the show interfaces serial Command



Interface and Line Protocol Status

Five possible problem states can be identified in the interface status line (see Figure 3-1) of the **show interfaces serial** *number* display:

- Serial *x* is down, line protocol is down
- Serial *x* is up, line protocol is down
- Serial *x* is up, line protocol is up (looped)
- Serial *x* is up, line protocol is down (disabled)
- Serial *x* is administratively down, line protocol is down

Table 3-1 summarizes the causes associated with each of these conditions and suggests appropriate actions.

Table 3-1 Interface Status Conditions Displayed by the show interfaces serial Command

Status Line State	Possible Causes and Suggested Actions
Serial *x* is down, line protocol is down (data terminal equipment [DTE] mode)	This status indicates that the router is not sensing a carrier detect (CD) signal (that is, CD is not active). **Possible Causes:** **1** Telephone company problem—Line down; line not connected to CSU/DSU **2** Faulty or incorrect cabling **3** Faulty or incorrect applique (AGS/CGS/MGS only) **4** Hardware failure (CSU/DSU) **Suggested Actions:** **Step 1** Check the LEDs on the CSU/DSU to see if CD is active, or insert a breakout box on the line to check for the CD signal. **Step 2** Verify that you are using the proper cable and interface (see your hardware installation documentation) **Step 3** Check the applique. If it is incorrect, install the correct applique (AGS/CGS/MGS only). **Step 4** Insert a breakout box; check all control leads. **Step 5** Contact your leased-line or other carrier service. **Step 6** Swap faulty parts. **Step 7** If you suspect faulty router hardware, change the serial line to another port or applique. If the connection comes up, the previously connected interface or applique has a problem.

Status Line State	Possible Causes and Suggested Actions
Serial *x* is up, line protocol is down (DTE mode)	**Possible Causes:** **1** Local or remote router misconfigured **2** Keepalives not being sent by remote router **3** Leased-line or other carrier service problem—noisy line; misconfigured or failed switch **4** Timing problem on cable (serial clock transmit external [SCTE] not set on CSU/DSU) **5** Failed local or remote CSU/DSU **6** Router hardware failure (local or remote) **Suggested Actions:** **Step 1** Put the modem, CSU, or DSU in local loopback mode and use the **show interfaces serial** *number* command to determine whether the line protocol comes up. If the line protocol does come up, it is likely that there is a telephone company problem or that the remote router is down. **Step 2** If the problem appears to be on the remote end, repeat Step 1 on the remote modem, CSU, or DSU. **Step 3** Verify all cabling. Make certain that the cable is attached to the correct interface, the correct CSU/DSU and the correct telephone company network termination point. Use the **show controllers** EXEC command to determine which cable is attached to which interface. **Step 4** Enable the **debug serial interface** EXEC command. **Step 5** If the line protocol does not come up in local loopback mode and if the output of the **debug serial interface** EXEC command shows that the keepalive counter is not incrementing, a router hardware problem is likely; swap router interface hardware. **Step 6** If the line protocol comes up, and the keepalive counter increments, the problem is *not* in the local router. Troubleshoot the serial line as described in the sections "Troubleshooting Clocking Problems" and "CSU and DSU Loopback Tests," later in this chapter. **Step 7** If you suspect faulty router hardware, change the serial line to an unused port or applique. If the connection comes up, the previously connected interface or applique has a problem.

Status Line State	Possible Causes and Suggested Actions
Serial *x* is up, line protocol is down (data communications equipment [DCE] mode)	**Possible Causes:** **1** Missing **clockrate** interface configuration command **2** The DTE device does not support (or is not set up for) SCTE mode (terminal timing) **3** Failed remote CSU or DSU **4** Failed or incorrect cable **5** Router hardware failure **Suggested Actions:** **Step 1** Add the **clockrate** interface configuration command on the serial interface. **Step 2** Set the DTE device to SCTE mode if possible. If your CSU/DSU does not support SCTE, you might have to disable SCTE on the Cisco router interface. See the section "Inverting the Transmit Clock" later in this chapter. **Step 3** Verify that the correct cable is being used. **Step 4** If protocol is still down, there is a possible hardware failure or cabling problem. Insert a breakout box and observe leads. **Step 5** Replace faulty parts as necessary.
Serial *x* is up, line protocol is up (looped)	**Possible Causes:** **1** Loop exists in circuit. The sequence number in the keepalive packet changes to a random number when a loop is initially detected. If the same random number is returned over the link, a loop exists. **Suggested Actions:** **Step 1** Use the **write terminal** privileged EXEC command to look for any instances of the **loopback** interface configuration command. **Step 2** If you find an occurrence of the **loopback** interface configuration command, use the **no loopback** interface configuration command to remove the loop. **Step 3** If you do not find the **loopback** interface configuration command, examine the CSU/DSU to determine whether they are configured in manual loopback mode. If they are, disable manual loopback. **Step 4** Reset the CSU or DSU and inspect the line status. If the protocol comes up, no other action is needed. **Step 5** If the CSU or DSU is not configured in manual loopback mode, contact the leased-line or other carrier service for line troubleshooting assistance.

Status Line State	Possible Causes and Suggested Actions
Serial *x* is up, line protocol is down (disabled)	**Possible Causes:** **1** High error rate due to telephone company service problem **2** CSU or DSU hardware problem **3** Bad router hardware (interface, applique) **Suggested Actions:** **Step 1** Troubleshoot with serial analyzer and breakout box; look for toggling Clear To Send (CTS) and Data Set Ready (DSR) signals. **Step 2** Loop CSU/DSU (DTE loop). If the problem continues, it is likely that there is a hardware problem. If the problem does not continue, it is likely that there is a telephone company problem. **Step 3** Swap out bad hardware as required (CSU, DSU, switch, local or remote router).
Serial *x* is administratively down, line protocol is down	**Possible Causes:** **1** Router configuration includes the **shutdown** interface configuration command **2** Duplicate IP address **Suggested Actions:** **Step 1** Check router configuration for the **shutdown** command. **Step 2** Use the **no shutdown** interface configuration command to remove the **shutdown** command. **Step 3** Verify that there are no identical IP addresses using the **write terminal** privileged EXEC command or the **show interfaces** EXEC command. **Step 4** If there are duplicate addresses, resolve the conflict by changing one of the IP addresses.

Evaluating Input Errors

When input errors appear in the **show interfaces serial** *number* output, you must consider several possibilities in order to determine the source of those errors. The most likely problems are summarized in the list of possible causes that follows.

Note Any input error value for cyclic redundancy check (CRC) errors, framing errors, or aborts above one percent of the total interface traffic suggests some kind of link problem that should be isolated.

Symptom Increasing number of input errors in excess of one percent of total interface traffic.

Possible Cause The following causes can result in this symptom:

- Faulty telephone company equipment
- Noisy serial line
- Incorrect clocking configuration (SCTE not set)
- Incorrect cable; cable too long
- Bad cable or connection
- Bad CSU or DSU
- Bad router hardware
- Data converter or other device being used between router and DSU

Note Cisco strongly recommends against the use of data converters when you are connecting a router to a WAN or serial network.

Recommended Action The following steps are suggested for this symptom:

Step 1 Use a serial analyzer to isolate the source of the errors. If you detect errors, it is likely that there is a hardware problem or a clock mismatch in a device that is external to the router.

Step 2 Use the loopback and ping tests described later in this chapter to isolate the specific problem source.

Step 3 Look for patterns. For example, if errors occur at a consistent interval, they could be related to a periodic function such as the sending of routing updates.

Table 3-2 details the meaning of CRC errors, framing errors, and aborts. These fields appear in the display shown in Figure 3-1.

Table 3-2 Meaning of Key Input Errors for Serial Line Troubleshooting

Input Error Type (Field Name)	Possible Causes and Suggested Actions
CRC errors (CRC)	**Meaning:** CRC calculation does not pass; some data is corrupted. **Possible Causes:** **1** Noisy serial line **2** Serial cable is too long; cable from the CSU/DSU to the router is not shielded **3** SCTE mode is not enabled on DSU **4** CSU line clock is incorrectly configured **5** Ones density problem on T1 link (incorrect framing or coding specification) **Suggested Actions:** **Step 1** Ensure that the line is clean enough for transmission requirements; shield cable if necessary. **Step 2** Make sure the cable is within the recommended length (no more than 50 feet [15.24 meters] or 25 feet [7.62 meters] for T1 link). **Step 3** Ensure that all devices are properly configured for common line clock. Set SCTE on the local and remote DSU. If your CSU/DSU does not support SCTE, see the section "Inverting the Transmit Clock" later in this chapter. **Step 4** Make certain that the local and remote CSU/DSU is configured for the same framing and coding scheme (for example, Extended Superframe Format [ESF]/Binary 8-Zero Substitution [B8ZS]) used by the leased-line or other carrier service. **Step 5** Contact your leased-line or other carrier service and have them perform integrity tests on the line.

Input Error Type (Field Name)	Possible Causes and Suggested Actions
Framing errors (frame)	**Meaning:** Detected packet does not end on an 8-bit byte boundary. **Possible Causes:** **1** Noisy serial line **2** Improperly designed cable; serial cable is too long; the cable from the CSU or DSU to the router is not shielded **3** SCTE mode is not enabled on the DSU; the CSU line clock is incorrectly configured; one of the clocks is configured for local clocking **4** Ones density problem on T1 span (incorrect framing or coding specification) **Suggested Actions:** **Step 1** Ensure that the line is clean enough for transmission requirements. Make certain you are using the correct cable. Shield the cable if necessary. **Step 2** Make sure the cable is within the recommended length (no more than 50 feet [15.24 meters] or 25 feet [7.62 meters] for T1 link) **Step 3** Ensure that all devices are properly configured to use common line clock. Set SCTE on the local and remote DSU. If your CSU/DSU does not support SCTE, see the section “Inverting the Transmit Clock” later in this chapter. **Step 4** Make certain that the local and remote CSU/DSU is configured for the same framing and coding scheme (for example, ESF/B8ZS) used by the leased-line or other carrier service. **Step 5** Contact your leased-line or other carrier service and have them perform integrity tests on the line.

Input Error Type (Field Name)	Possible Causes and Suggested Actions
Aborted transmission (abort)	**Meaning:** Illegal sequence of one bits (more than 7 in a row) **Possible Causes:** **1** SCTE mode is not enabled on DSU **2** CSU line clock is incorrectly configured **3** Serial cable is too long; cable from the CSU or DSU to the router is not shielded **4** Ones density problem on T1 link (incorrect framing or coding specification) **5** Packet terminated in middle of transmission; typical cause is an interface reset or a framing error **6** Hardware problem—bad circuit, bad CSU/DSU, bad sending interface on remote router **Suggested Actions:** **Step 1** Ensure that all devices are properly configured to use common line clock. Set SCTE on the local and remote DSU. If your CSU/DSU does not support SCTE, see the section "Inverting the Transmit Clock" later in this chapter. **Step 2** Shield the cable if necessary. Make certain the cable is within the recommended length (no more than 50 feet [15.24 meters] or 25 feet [7.62 meters] for T1 link); ensure that all connections are good. **Step 3** Check the hardware at both ends of the link. Swap faulty equipment as necessary. **Step 4** Lower data rates and determine if aborts decrease. **Step 5** Use local and remote loopback tests to determine where aborts are occurring (see the section "Special Serial Line Tests," later in this chapter.) **Step 6** Contact your leased-line or other carrier service and have them perform integrity tests on the line.

Inverting the Transmit Clock

If you are attempting serial connections of greater than 64 kbps with a CSU/DSU that does not support serial clock transmit external (SCTE), you might have to invert the transmit clock on the router. Inverting the transmit clock compensates for phase-shifts between the data and clock signals.

On a Cisco 7000 series router, enter the **invert-transmit-clock** interface configuration command. For Cisco 4000 series routers, use the **dte-invert-txc** interface configuration command. To ensure that you are using the correct command syntax for your router, check the *Router Products Configuration Guide* and the *Router Products Command Reference* publications.

Note On older platforms, inverting the transmit clock might require that you move a physical jumper.

Evaluating Output Drops

Output drops appear in the output of the **show interfaces serial** *number* command when the system is attempting to hand off a packet to a transmit buffer but no buffers are available. The output drops count is illustrated in Figure 3-1.

Symptom Increasing output drops

Possible Cause Input rate to serial interface exceeds bandwidth available on serial link

Recommended Action The following steps are suggested for this symptom:

Step 1 Minimize periodic broadcast traffic such as routing and SAP updates by using access lists or other means. For example, to increase the delay between SAP updates, use the **ipx sap-interval** interface configuration command.

Step 2 Increase the output hold queue size in small increments, using the **hold-queue out** interface configuration command.

Step 3 On affected interfaces, turn off fast switching for heavily-used protocols. For example, to turn of IP fast switching, enter the **no ip route-cache** interface configuration command. For the command syntax for other protocols, consult the *Router Products Configuration Guide* and the *Router Products Command Reference* publications.

Step 4 Implement priority queuing on slower serial links by configuring priority lists. For information on configuring priority lists, see the *Router Products Configuration Guide* and the *Router Products Command Reference* publications.

Note Output drops are acceptable under certain conditions. For instance, if a link is known to be overused (with no opportunity or way to remedy the situation), it is often considered preferable to drop packets than to hold them. This is true for protocols that support flow control and can retransmit data (such as TCP/IP and Novell IPX). However, some protocols, such as DECnet and Local Area Transport (LAT) are sensitive to dropped packets and accommodate retransmission poorly, if at all.

Evaluating Input Drops

Input drops appear in the **show interfaces serial** *number* EXEC command when too many packets from that interface are still being processed in the system. The input drops count is illustrated in Figure 3-1.

Symptom Increasing number of input drops

Possible Cause Input rate exceeds the capacity of the router or input queues exceed the size of output queues.

Note Input drop problems are typically seen when traffic is being routed between faster interfaces (such as Ethernet, FDDI, and Token Ring) and serial interfaces. When traffic is light, there is no problem. As traffic rates increase, backups start occurring. By design, routers drop packets during these congested periods.

Recommended Action The following steps are recommended when this symptom is encountered:

Step 1 Increase the output queue size on common destination interfaces for the interface that is dropping packets. Use the **hold-queue out** interface configuration command.

Step 2 Reduce the input queue size (using the **hold-queue in** interface configuration command) to force input drops to become output drops. Output drops have less impact on the performance of the router than do input drops.

Evaluating Interface Resets

Interface resets that appear in the **show interfaces serial** *number* EXEC command are the result of missed keepalive packets. The interface resets count is illustrated in Figure 3-1.

Symptom Increasing interface resets

Possible Cause The following causes can result in this symptom:

- Congestion on link (typically associated with output drops)
- Bad line causing CD transitions
- Possible hardware problem at the CSU, DSU, or switch

Recommended Action When analyzing interface resets, you must examine other fields of the **show interfaces serial** *number* command output to determine the source of the problem. Assuming an increase in interface resets is being recorded, examine the following fields (illustrated in Figure 3-1):

Step 1 If there are a high number of output drops in the **show interfaces serial** *number* output, see the section "Evaluating Output Drops" earlier in this chapter.

Step 2 Check the carrier transitions field in the **show interfaces serial** *number* display. If carrier transitions are high while interface resets are being registered, the problem is likely to be a bad link or bad CSU or DSU. Contact your leased line/carrier service and swap faulty equipment as necessary.

Step 3 Examine the input errors field in the **show interfaces serial** *number* display. If input errors are high while interface resets are increasing, the problem is probably a bad link or bad CSU/DSU. Contact your leased line or other carrier service and swap faulty equipment as necessary.

Evaluating Carrier Transitions

Carrier transitions appear in the output of the **show interfaces serial** *number* EXEC command whenever there is an interruption in the carrier signal; for example, when there is an interface reset at the remote end of a link. The carrier transitions count is illustrated in Figure 3-1.

Symptom Increasing carrier transitions count

Possible Cause The following causes can result in this symptom:

- Line interruptions due to an external source (examples: physical separation of cabling; Red or Yellow T1 alarms; lightning strikes somewhere along the network)
- Faulty switch, DSU, or router hardware

Recommended Action The following steps are suggested when this symptom is encountered:

Step 1 Check hardware at both ends of the link (attach breakout box or serial analyzer and test to determine source of problems).

Step 2 If analyzer or breakout box are unable to identify any external problems, check router hardware.

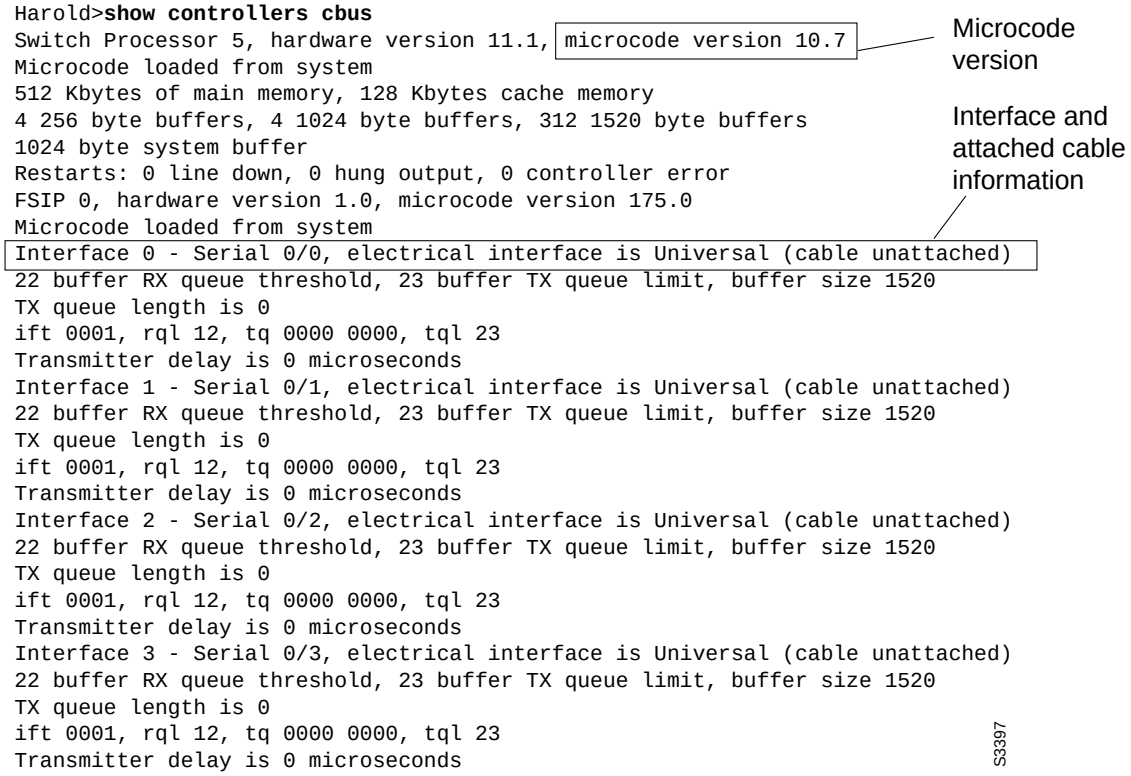
Step 3 Swap faulty equipment as necessary.

Using the show controllers Command to Troubleshoot Serial Lines

The **show controllers** EXEC command is another important diagnostic tool. For serial interfaces on Cisco 7000 series routers, use the **show controllers cbus** EXEC command. For Cisco access products, use the **show controllers** EXEC command. For the AGS, CGS, and MGS, use the **show controllers mci** EXEC command.

Figure 3-2 shows the output from the **show controllers cbus** EXEC command. This command is used on Cisco 7000 series routers with the fast serial interface processor (FSIP) card. Make certain that the cable to the CSU/DSU is attached to the proper interface. Check the microcode version to see if it is current.

Figure 3-2 show controllers cbus Command Output



The **show controllers** EXEC command is used on access products such as the Cisco 2000, Cisco 2500, Cisco 3000, and Cisco 4000 series. Figure 3-3 shows the **show controllers** command output from the basic-rate interface (BRI) and serial interfaces on a Cisco 2503. (Note that, in the interest of space, some output is not shown.) The **show controllers** output indicates the state of the interface channels and describes the whether a cable is attached to the interface. In Figure 3-3, serial interface 0 has an RS-232 DTE cable attached; serial interface 1 has no cable attached.

Figure 3-3 show controllers Command Output

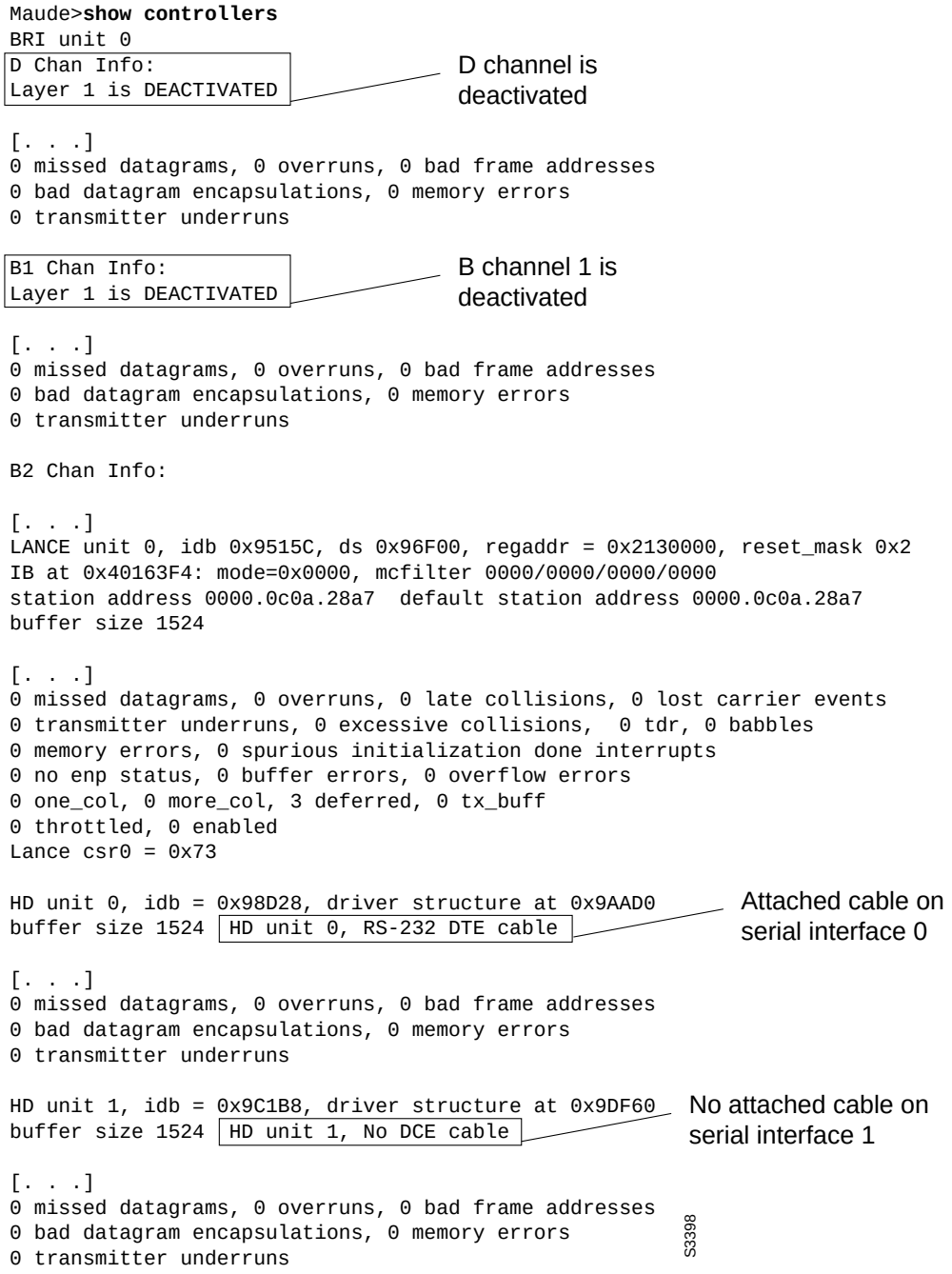
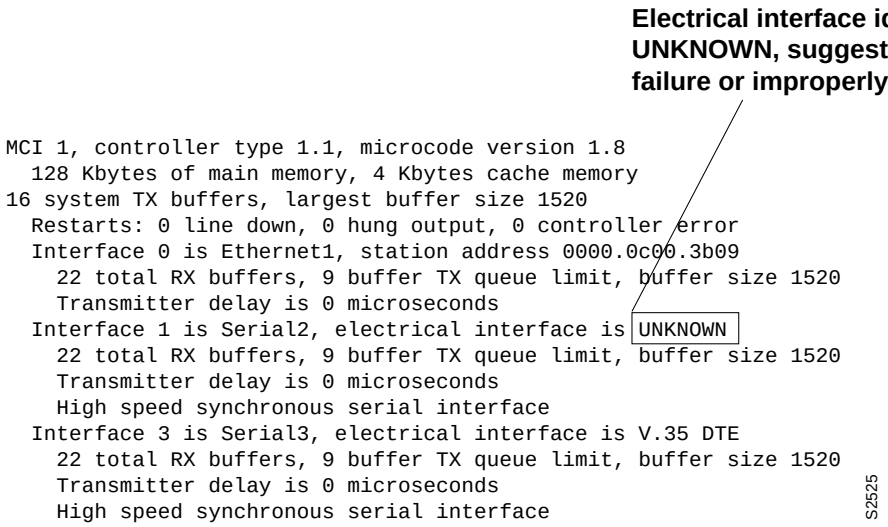


Figure 3-4 illustrates the output for the **show controllers mci** command. This command is used on AGS, CGS, and MGS routers only. If the electrical interface is displayed as "UNKNOWN" (instead of V.35, EIA/TIA-449, or some other electrical interface type), a bad applique or a problem with the internal wiring of the card is likely. This might also indicate an improperly connected cable. In addition, the corresponding display for the **show interfaces serial** *number* EXEC command will show that the interface and line protocol are down. (See Figure 3-1.)

Figure 3-4 Output from the show controllers mci Command



Using debug Commands to Troubleshoot Serial Lines

The output from **debug** privileged EXEC commands provides diagnostic information concerning a variety of internetworking events relating to protocol status and network activity in general.

Caution Throughout this and other chapters, the use of **debug** commands is suggested for obtaining information about network traffic and router status. Use these commands with great care. In general, it is recommended that these commands only be used under the direction of your router technical support representative when troubleshooting specific problems. Enabling debugging can disrupt operation of the router when internetworks are experiencing high load conditions. When you finish using a **debug** command, remember to disable it with its specific **no debug** command or with the **no debug all** command (the **undebug** command is also accepted).

To minimize the impact of using **debug** commands, follow this procedure:

Step 1 Issue the **no logging console** global configuration command on your router. This command disables all logging to the console terminal.

Step 2 Telnet to a router port and enter the **enable** EXEC command.

Step 3 Issue the **terminal monitor** command and issue the necessary **debug** commands.

Following this procedure minimizes the load created by using **debug** commands because the console port no longer has to generate character-by-character processor interrupts.

Following are some **debug** commands that are useful when troubleshooting serial and WAN problems.

- **debug serial interface**—Verifies whether HDLC keepalive packets are incrementing; if not, a possible timing problem exists on the interface card or in the network.
- **debug x25 events**—Detects X.25 events, such as the opening and closing of switched virtual circuits (SVCs). The resulting "Cause and Diagnostic" information is included with the event report. Refer to the *Debug Command Reference* publication for more information concerning this command.
- **debug lapb**—Obtains LAPB or Level 2 X.25 information.
- **debug arp**—Indicates whether the router is sending information about or learning about routers (with ARP packets) on the other side of the WAN cloud. Use this command when some nodes on a TCP/IP network are responding, but others are not.
- **debug frame-relay lmi**—Obtains local management interface (LMI) information for determining whether a Frame Relay switch and router are sending and receiving LMI packets.
- **debug frame-relay events**—Determines whether exchanges are occurring between a router and a Frame Relay switch.
- **debug ppp negotiation**—Shows Point-to-Point Protocol (PPP) packets transmitted during PPP startup, where PPP options are negotiated.
- **debug ppp packet**—Shows PPP packets being sent and received. This command displays the low-level packet dumps.
- **debug ppp errors**—Shows PPP errors (such as illegal or malformed frames) associated with PPP connection negotiation and operation.
- **debug ppp chap**—Shows PPP Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) packet exchanges.
- **debug serial packet**—Shows SMDS packets being sent and received. This display also prints out necessary error messages to indicate why a packet was not sent or was received erroneously. For SMDS, dumps the entire SMDS header and some payload data when an SMDS packet is transmitted or received.

More information about the output of each debug command is provided in the *Debug Command Reference* publication.

Troubleshooting Clocking Problems

Clocking conflicts in serial connections can lead to either chronic loss of connection service or generally degraded performance. The following discussion addresses five issues regarding clocking problems:

- Clocking Overview
- Clocking Problem Causes
- Detecting Clocking Problems
- Isolating Clocking Problems
- Suggested Clocking Problem Remedies

Clocking Overview

The CSU/DSU derives the data clock from the data that passes through it. In order to recover the clock, the CSU/DSU hardware *must* receive at least one 1 bit value for every 8 bits of data that pass through it (this is known as *ones density*.) Maintaining ones density allows the hardware to recover the data clock reliably.

Newer T1 implementations commonly use Extended Superframe Format (ESF) framing with Binary 8-Zero Substitution (B8ZS). B8ZS provides a scheme by which a special code is substituted whenever 8 consecutive zeros are sent through the serial link. This code is then interpreted at the remote end of the connection. This technique guarantees ones density independent of the data stream.

Older T1 implementations use D4 (also known as Superframe Format) framing and Alternate Mark Inversion (AMI) coding. AMI requires that the sending device maintain ones density, because it does not utilize a coding scheme like B8ZS. This restricts the type of data that can be transmitted because ones density is not maintained independent of the data stream.

Another important element in serial communications is serial clock transmit external (SCTE) terminal timing. The SCTE is the clock echoed back from the data terminal equipment (DTE) device (for example, a router) to the data communications equipment (DCE) device (for example, the CSU/DSU). When the DCE device uses the SCTE instead of its internal clock to sample data from the DTE, it is better able to sample the data without error even if there is a phase-shift in the cable between the CSU/DSU and the router. Using SCTE is highly recommended for serial transmissions faster than 64 kbps. If your CSU/DSU does not support SCTE, see the section “Inverting the Transmit Clock” earlier in this chapter.

Clocking Problem Causes

In general, clocking problems in serial WAN interconnections can be attributed to one of the following basic causes:

- Incorrect DSU configuration
- Incorrect CSU configuration
- Cables out of specification (longer than 50 feet [15.24 meters] or unshielded)
- Noisy or poor patch panel connections
- Several cables connected together in a row

Detecting Clocking Problems

To detect clocking conflicts on your serial interface, look for input errors as follows:

Step 1 Use the **show interfaces serial** *number* EXEC command on the routers at both ends of the link.

Step 2 Examine the display output for CRC, framing errors, and aborts.

Step 3 If either of these steps indicates errors exceeding an approximate range of 0.5 to 2.0 percent of traffic on the interface, clocking problems are likely to exist somewhere in the WAN.

Step 4 Isolate the source of the clocking conflicts as outlined in the next procedure, "Isolating Clocking Problems."

Step 5 Bypass or repair faulty patch panel.

Isolating Clocking Problems

After you determine that clocking conflicts are the most likely cause of input errors, the following general steps will help you isolate the source of those errors:

Step 1 Perform a series of loopback and **ping** tests, both local and remote, as described in the section "CSU and DSU Loopback Tests" later in this chapter.

Step 2 Determine which end of the connection is the source of the problem, or if the problem is in the line. In local loopback mode, run different patterns and sizes in the **ping** tests (for example, use 1500 byte datagrams). Using a single pattern and packet size may not force errors to materialize, particularly when a serial cable to the router or CSU/DSU is the problem.

Step 3 Issue the **show interfaces serial** *number* EXEC command and determine whether input errors counts are increasing and where they are accumulating.

If input errors are accumulating on both ends of the connection, clocking of the CSU is the likely problem.

If only one end is experiencing input errors, there is likely to be a DSU clocking or cabling problem.

If you see aborts on one end, it suggests that the *other* end is sending bad information or that there is a line problem.

Note Always refer back to the **show interfaces serial** *number* display output and log any changes in error counts or note if the error count does not change.

Suggested Clocking Problem Remedies

Table 3-3 outlines suggested remedies for clocking problems, based on the source of the problem.

Table 3-3 Serial Lines: Clocking Problems and Suggested Remedies

Clocking Problem Cause	Suggested Actions
Incorrect CSU configuration	**Step 1** Determine whether the CSUs at both ends are in agreement regarding the clock source (local or line). **Step 2** Configure both to agree if not already correctly configured (usually the line is the source). **Step 3** Check Line Build Out (LBO) setting on CSU/DSU to ensure that the impedance matches that of the physical line. For information on configuring your CSU, consult your CSU hardware documentation.
Incorrect DSU configuration	**Step 1** Determine whether the DSUs at both ends have SCTE mode enabled. **Step 2** Enable SCTE on both ends of the connection if not already correctly configured. (For any interface that is connected to a line of 128 kbps or faster, SCTE *must* be enabled. If your CSU/DSU does not support SCTE, see the section "Inverting the Transmit Clock" earlier in this chapter.) **Step 3** Make sure that ones density is maintained. This requires that the DSU use the same framing and coding schemes (for example, ESF and B8ZS) used by the leased-line or other carrier service. **Step 4** If your carrier service uses AMI coding, either invert the transmit clock on both sides of the link or run the DSU in bit-stuff mode. For information on configuring your DSU, consult your DSU hardware documentation.
Cable to router out of specification	**Step 1** Use shorter cable if longer than 50 feet (15.24 meters). **Step 2** Replace with shielded cable.

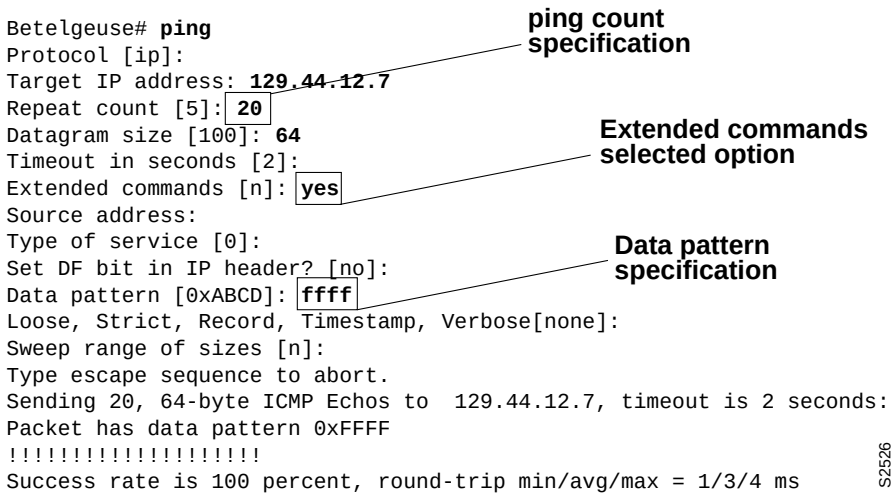
Using Extended ping Tests to Troubleshoot Serial Lines

The *ping* function is one of the useful tests available on Cisco internetworking systems (as well as on many host systems). In TCP/IP terminology, this diagnostic tool also is known as the "Internet Control Message Protocol (ICMP) Echo Request."

Note The ping function is particularly useful when high levels of input errors are being registered in the **show interfaces serial** *number* display (see Figure 3-1).

Cisco internetworking systems provide a mechanism to automate the sending of many ping packets in sequence. Figure 3-5 illustrates the menu used to specify extended ping options. This example specifies only 20 successive pings; however, when testing the components on your serial line, you should specify a much larger number, such as 1000 pings.

Figure 3-5 Extended ping Specification Menu



In general, perform serial line ping tests as follows:

Step 1 Put CSU or DSU into local loopback mode.

Step 2 Configure the extended **ping** command to send different data patterns and packet sizes. Figure 3-6 and Figure 3-7 illustrate two useful **ping** tests, an all-zeros 1500 byte **ping** and an all-ones 1500 byte **ping**, respectively.

Figure 3-6 All-Zeros 1500 Byte ping Test

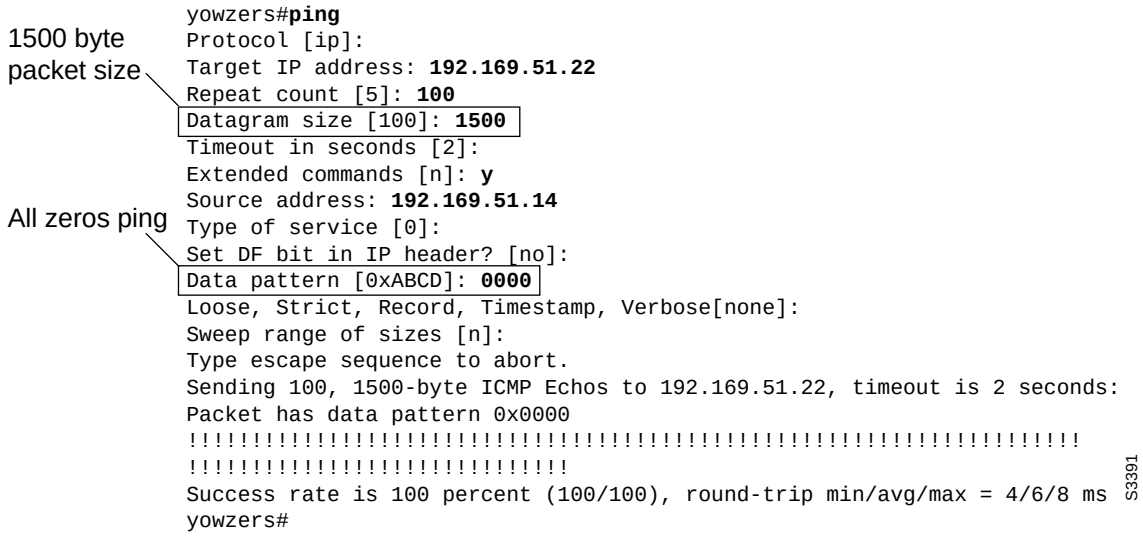
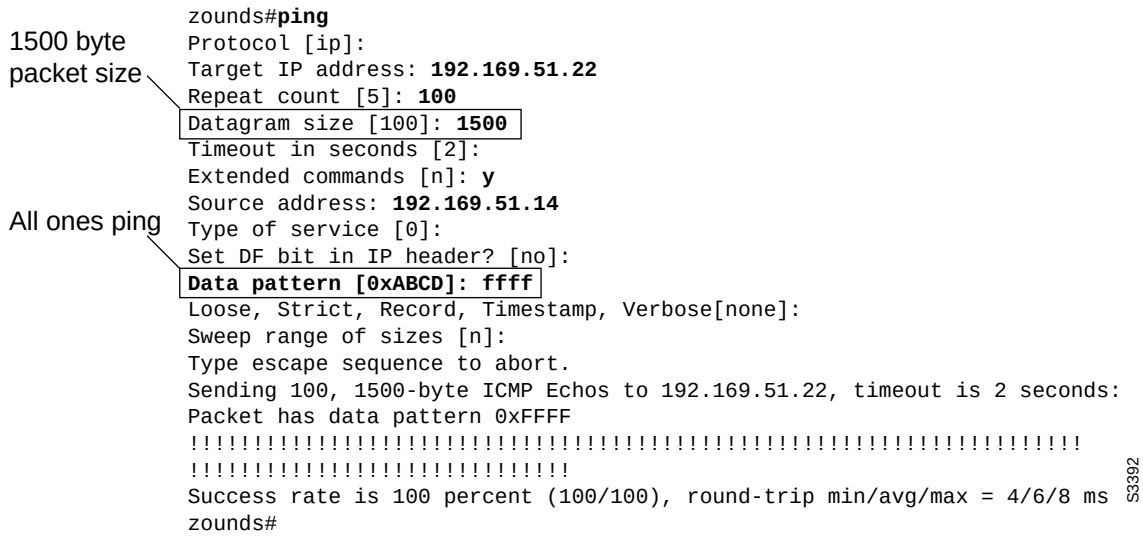


Figure 3-7 All-Ones 1500 Byte ping Test



Step 3 Examine the **show interfaces serial** *number* statistics and determine whether input errors have increased. If input errors have not increased, the local hardware (DSU, cable, router interface card, and applique) is likely to be good.

Assuming that this test sequence was prompted by the appearance of a large number of CRC and framing errors, a clocking problem is likely. Check the CSU or DSU for a timing problem. Refer to the section "Troubleshooting Clocking Problems," later in this chapter.

Step 4 If you determine that the clocking configuration is correct and operating properly, put the CSU or DSU into remote loopback mode.

Step 5 Repeat the ping test and look for changes in the input error statistics.

Step 6 If input errors increase, there is either a problem in the serial line or on the CSU/DSU. Contact the WAN service provider and swap the CSU or DSU. If problems persist, consult your router technical support representative.

Adjusting Buffers to Ease Overutilized Serial Links

Excessively high bandwidth utilization results in reduced overall performance and can cause intermittent failures. For example, DECnet file transmissions may be failing due to packets being dropped somewhere in the network. If the situation is bad enough, you *must* add bandwidth; however, adding bandwidth may not be necessary or immediately practical. One way to resolve marginal serial line overutilization problems is to control how the router uses data buffers.

Caution In general, you should *not* adjust system buffers unless you are working closely with your router technical support representative. You can severely affect the performance of your hardware and your network if you incorrectly adjust the system buffers on your router.

You have three options to control how buffers are used:

- Adjust parameters associated with system buffers
- Specify the number of packets held in input or output queues (called “hold queues”)
- Prioritize how traffic is queued for transmission (also called “priority output queuing”)

The configuration commands associated with these options are fully described in the *Router Products Configuration Guide* and *Router Products Command Reference* publications.

The following discussion focuses on identifying situations in which these options are likely to apply and defining how you can use these options to help resolve connectivity and performance problems in serial/WAN interconnections. Commands are discussed as appropriate.

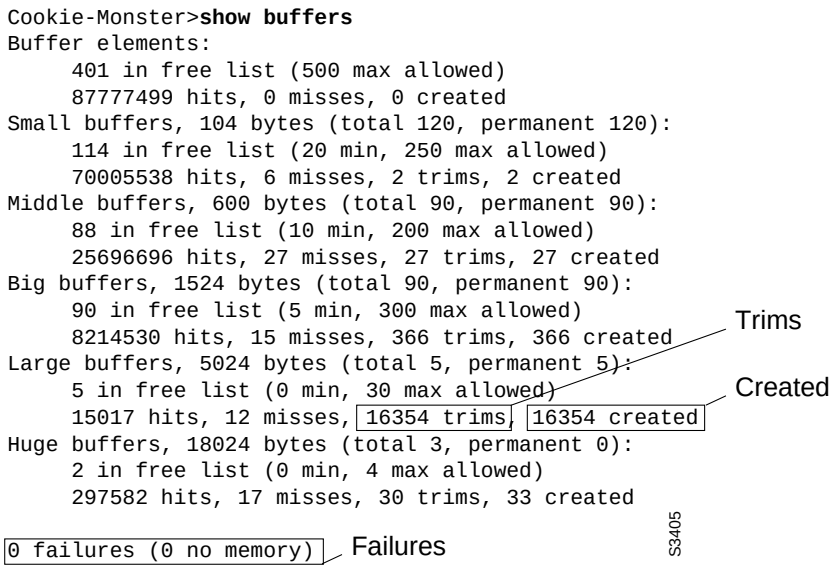
Tuning System Buffers

There are two general buffer types on Cisco routers. These are referred to as “hardware” buffers and “system” buffers. Only the system buffers are directly configurable by system administrators.

The hardware buffers are specifically used as the receive and transmit buffers associated with each interface and (in the absence of any special configuration) are dynamically managed by the system software itself.

The system buffers are associated with the main system memory and are allocated to different size memory blocks. A useful command for determining the status of your system buffers is the **show buffers** EXEC command. Figure 3-8 shows an example of the output from the **show buffers** command.

Figure 3-8 show buffers Command Output



The **show buffers** command output in Figure 3-8 indicates high numbers in the trims and created fields for Large Buffers. If this is the case, you can increase your serial link performance by increasing the max-free value configured for your system buffers. Use the **buffers max-free** *number* global configuration command to increase the number of free system buffers. The value you configure should be approximately 150 percent of the figure indicated in the Total field of the **show buffers** command output. Repeat this process until the **show buffers** output no longer indicates trims and created buffers.

If the **show buffers** command output shows a large number of failures in the "(no memory)" field (see the last line of output in Figure 3-8), you must reduce the usage of the system buffers or increase the amount of shared or main memory (physical RAM) on the router. Call your router technical support representative for assistance.

Implementing Hold Queue Limits

Hold queues are buffers used by each router interface to store outgoing or incoming packets. Use the **hold-queue** interface configuration command to increase the number of data packets queued before the router will drop packets.

Note The **hold-queue** command is used for process switched packets and periodic updates generated by the router.

Use this command to prevent packets from being dropped and to improve serial-link performance under the following conditions:

- You have an application that cannot tolerate drops and the protocol is able to stand longer delays. DECnet is an example of a protocol that meets both criteria. LAT does not because it does not tolerate delays.
- The interface is very slow. (Low bandwidth and/or anticipated utilization is likely to sporadically exceed available bandwidth.)

Note When you increase the number specified for an output hold queue, you might need to increase the number of system buffers. The value used depends on the size of the packets associated with the traffic anticipated for the network.

Using Priority Queuing to Reduce Bottlenecks

Priority queuing is a list-based control mechanism that allows network administrators to prioritize traffic transmitted into networks on an interface-by-interface basis. In a manner that is analogous to Cisco's access list traffic control mechanisms, priority queuing involves two steps:

Step 1 Create a priority list by protocol type and level of priority.

Step 2 Assign the priority list to a specific interface.

Both of these steps use versions of the **priority-list** global configuration command (with the keywords **protocol** and **interface**, as appropriate). In addition, further traffic control can be applied by referencing **access-list** global configuration commands from **priority-list** specifications. For examples of defining priority lists and details about command syntax associated with priority queuing, refer to the *Router Products Configuration Guide* and *Router Products Command Reference* publications.

Note Priority queuing automatically creates four hold queues of varying size. This overrides any hold queue specification included in your configuration.

Use priority queuing to prevent packets from being dropped and to improve serial link performance under the following conditions:

- When the interface is slow, there are a variety of traffic types being transmitted, and you want to improve terminal traffic performance.
- If you have a serial link that is intermittently experiencing very heavy loads (such as file transfers occurring at specific times), you can use priority lists to select which types of traffic should be discarded at high traffic periods.

In general, start with the default number of queues (altered with the **queue-limit** keyword option of the **priority-list** global configuration command) when implementing priority queues. After enabling priority queuing, monitor output drops with the **show interfaces serial** *number* EXEC command. If you notice that output drops are occurring in the traffic queue you have specified to be high priority, increase the number of packets that can be queued.

Note When bridging DEC LAT traffic, your router must drop very few packets, or LAT will not function correctly (that is, sessions will terminate unexpectedly). A high priority queue depth of about 100 (specified with the **queue-limit** keyword) is a typical working value when your router is dropping output packets, and the serial lines are subjected to about 50 percent bandwidth utilization. If the router is dropping packets and is at 100 percent utilization, you need another line. Another tool to relieve congestion when bridging DEC LAT is LAT compression. You can implement LAT compression with the interface configuration command **bridge-group** *group* **lat-compression**.

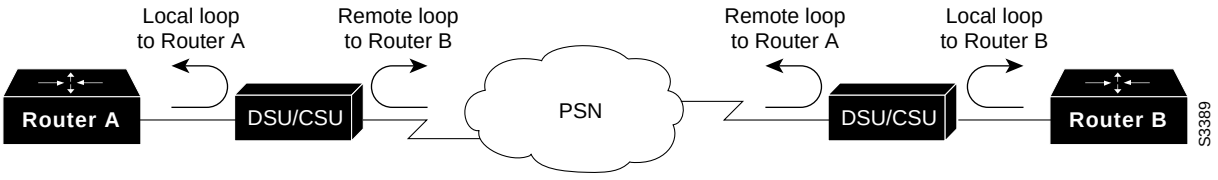
Special Serial Line Tests

In addition to the basic diagnostic capabilities provided with routers, there are a variety of supplemental tools and techniques that can be used to determine the conditions of cables, switching gear, modems, hosts, and remote internetworking hardware. Although complete discussions of these tools are beyond the scope of this publication, some hints about using these alternative tools are provided here. For more information, consult the documentation for your CSU, DSU, serial analyzer, or other equipment.

CSU and DSU Loopback Tests

If the output of the **show interfaces serial** *number* EXEC command indicates that the serial line is up, but the line protocol is down, use the CSU/DSU loopback tests to determine the source of the problem. Perform the local loop test first, then the remote test. Figure 3-9 illustrates the topology of the CSU/DSU local and remote loopback tests.

Figure 3-9 CSU/DSU Local and Remote Loopback Tests



Note These tests are generic in nature and assume attachment of the internetworking system to a CSU or DSU. However, the test is essentially the same for attachment to a multiplexer with built-in CSU/DSU functionality. Because there is no concept of a loopback in X.25 or Frame Relay packet-switched network (PSN) environments, loopback tests do not apply to X.25 and Frame Relay networks.

CSU and DSU Local Loopback Tests for HDLC or PPP Links

The following is a general procedure for performing loopback tests in conjunction with built-in Cisco system diagnostic capabilities.

Step 1 Place the CSU/DSU in local loop mode. In local loop mode, the use of the line clock (from the T1 service) is terminated, and the DSU is forced to use the local clock.

Step 2 Use the **show interfaces serial** *number* EXEC command to determine whether the line status changes from "line protocol is down" to "line protocol is up (looped)," or if it remains down.

Step 3 If the line protocol comes up when the CSU or DSU is in local loopback mode, it suggests that the problem is occurring on the remote end of the serial connection. If the status line does not change state, there is a possible problem in the router, connecting cable, or CSU/DSU.

Step 4 If the problem appears to be local, issue the **debug serial interface** privileged EXEC command.

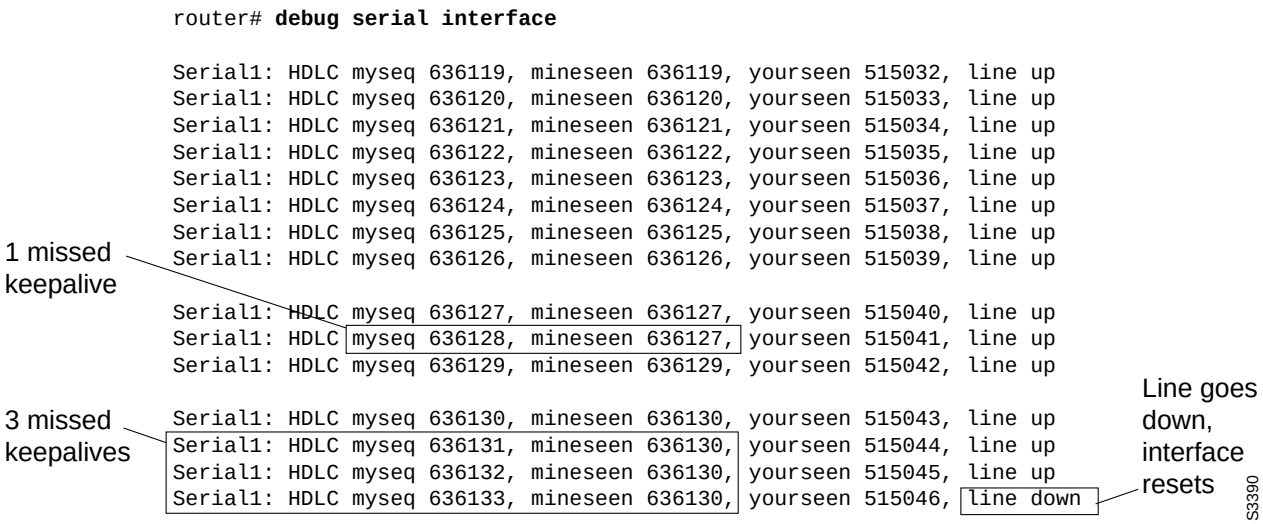
Step 5 Take the CSU/DSU out of local loop mode. With the line protocol *down* and the **debug serial interface** command enabled, the **debug serial interface** output will indicate that keepalive counters are not incrementing.

Step 6 Again place the CSU/DSU in local loop mode. This should cause the keepalive packets to begin to increment. Specifically, the values for *mineseen* and *yourseen* keepalives will increment every 10 seconds. This information will appear in the **debug serial interface** output. If the keepalives do not increment, there may be a timing problem on the interface card or on the network. (For information on correcting timing problems, refer to the section "Troubleshooting Clocking Problems," earlier in this chapter.)

Step 7 Check the local router and CSU/DSU hardware, and any attached cables. Make certain the cables are within the recommended lengths (no more than 50 feet [15.24 meters], or 25 feet [7.62 meters] for T1 link). Make certain the cables are attached to the proper ports. Swap faulty equipment as necessary.

Figure 3-10 shows the output from the **debug serial interface** command for an HDLC serial connection, with missed keepalives eventually causing the line to go down and the interface to reset.

Figure 3-10 debug serial interface Command Output



CSU and DSU Remote Loopback Tests for HDLC or PPP Links

If you are able to determine that the local hardware is functioning properly, but you still encounter problems when attempting to establish connections over the serial link, try using the remote loopback test that follows to isolate the problem cause.

Note This remote loopback test assumes that HDLC encapsulation is being used and that the preceding local loop test was performed immediately before this test.

Step 1 Put the remote CSU or DSU into remote loopback.

Step 2 Using the **show interfaces serial** *number* EXEC command, determine whether the line protocol remains up, with the status line indicating "Serial *x* is up, line protocol is up (looped)" or if it goes down, with the status line indicating "Line protocol is down."

Step 3 If the line protocol remains up (looped), the problem is probably at the remote end of the serial connection (between the remote CSU/DSU and the remote router). Perform both local and remote tests at the remote end to isolate the problem source.

Step 4 If the line status changes to "Line protocol is down" when remote loopback mode is activated, make certain that ones density is being properly maintained. The CSU/DSU must be configured to use the same framing and coding schemes (for example, ESF and B8ZS) used by the leased-line or other carrier service.

Step 5 If problems persist, contact your WAN network manager or the WAN service organization.

Troubleshooting Access Server to Modem Connectivity

This section offers recommended procedures for properly setting up an access server-to-modem connection, and presents a number of symptom modules that describe access server-to-modem connectivity problems and suggested actions for resolving them. This section does not cover hardware problems. For information on troubleshooting your hardware, see the "Troubleshooting Router Startup Problems" chapter. See the "Troubleshooting AppleTalk Connectivity" chapter for modem troubleshooting information that is directly related to AppleTalk Remote Access (ARA) dial-in sessions.

The first part of this section, "Initiating a Reverse Telnet Session to a Modem," describes the procedure for establishing a reverse Telnet session with your modem in order to set the proper speed and configure it at that speed. The rest of the section includes the following troubleshooting symptom modules:

- No Connectivity Between Access Server and Modem
- Remote Dial-In Sees "Garbage"
- High Rate of Data Loss Over Modem Connection
- Modem Does Not Disconnect Properly
- Remote Dial-In Client Receives No EXEC Prompt
- Remote Dial-In Interrupts Existing Sessions

Initiating a Reverse Telnet Session to a Modem

Establishing a reverse Telnet session with your modem allows you to configure the modem at the speed at which you want it to communicate with the Cisco device. As long as you lock the DTE-side speed of the modem (see Table 3-6 for information on locking the modem speed), the modem will always speak to the access server or router at the desired speed. Be certain that the speed of the Cisco device is configured prior to issuing commands to the modem via a reverse Telnet session. (See Table 3-6 for information on configuring the speed of the access server or router.)

To initiate a reverse Telnet session to your modem, perform the following steps:

Step 1 From your terminal, issue the command

telnet *x.x.x.x* **20***yy*

where *x.x.x.x* is the IP address of any active, connected interface on the Cisco device that is currently up, and *yy* is the line number to which the modem is connected. For example, the following command

```
telnet 192.169.53.52 2001
```

would connect you to the auxiliary port on a Cisco router with IP address 192.169.53.52. A Telnet command of this kind can generally be issued from anywhere on the network that can **ping** IP address *x.x.x.x.*

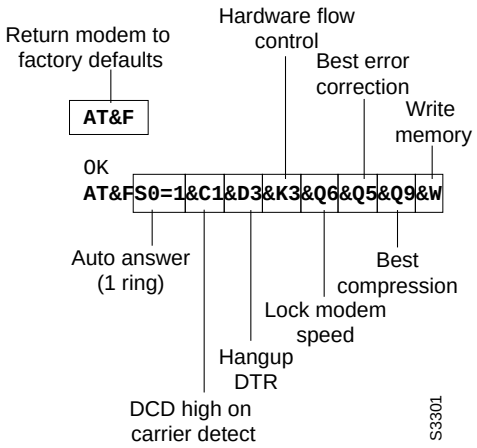
Note On a Cisco router, port 01 is the auxiliary port. On a Cisco access server, the auxiliary port is *last_tty+1*, so on a 16-port access server, the auxiliary port is port 17. Use the **show line** EXEC command to make certain you are working with the correct line.

Step 2 If the connection is refused, there may already be a user connected to that port. Issue the **show users** EXEC command to determine if the line is being used. If desired, the line can be cleared from the console using the **clear line** privileged EXEC command. When you are certain the line is not in use, attempt the Telnet connection again.

Step 3 If the connection is again refused, confirm that you have set modem control to **modem inout** for that line. See Table 3-4 for information on configuring a line on a Cisco device for modem control.

Step 4 After successfully making the Telnet connection, you are ready to configure the modem. Make sure that when you enter **AT**, the modem replies with OK. Figure 3-11 shows a typical Hayes-compatible modem command string. Again, be certain to check the documentation for your specific modem to verify the exact syntax of these commands.

Figure 3-11 Typical Hayes-Compatible Modem Command String



No Connectivity Between Access Server and Modem

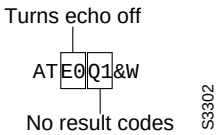
Symptom: Connectivity between a modem and a Cisco access server or router is nonexistent. Attempts to initiate a reverse Telnet session to the modem have no result, or the user receives a "Connection Refused by Foreign Host" message. Table 3-4 describes possible causes and suggests actions when modem to access server connections are unresponsive.

Table 3-4 Modem: No Connectivity Between Access Server and Modem

Possible Causes	Suggested Actions
Modem control is not enabled on the access server (modem control on auxiliary ports is only available in Software Release 9.21 and later).	**Step 1** Issue the **show line** EXEC command on the access server or router. The output for the auxiliary port should show inout or RIisCD in the Modem column. This indicates that modem control is enabled on the line of the access server or router. For an explanation of the **show line** output, see the "Interpreting show line Output" section later in this chapter. **Step 2** If you are running software prior to Software Release 9.21, and therefore do not have modem control, perform these steps and do not proceed to Step 3: • Disable echo on the modem. This is typically done with the **E0** modem command. Check your modem documentation for the exact syntax of modem commands. • Disable result codes on the modem. This is typically done using the **Q1** modem command. Check your modem documentation for the exact syntax. See Figure 3-12 for a modem command string that disables echo and result codes on a Hayes-compatible modem. • On the access server or router, configure the line to which the modem is connected with the **exec timeout** line configuration command. This command tells the access server to end the EXEC session after a specified period of time of no activity. **Step 3** If you are running Software Release 9.21 or later, configure the line for modem control using the **modem inout** line configuration command. Modem control is now enabled on the access server. The **debug modem** output should indicate the change. NOTE: Be certain to use the **modem inout** command in favor of the **modem ri-is-cd** command while the connectivity of the modem is in question. The latter command allows the line to accept incoming calls only. Outgoing calls will be refused, making it impossible to establish a Telnet session with the modem to configure it. If you want to enable the **modem ri-is-cd** command, do so only after you are certain the modem is functioning correctly.

Possible Causes	Suggested Actions
Incorrect cabling configuration	**Step 1** Check the cabling between the modem and the access server or router. Confirm that the modem is connected to the auxiliary port on the access server or router with a rolled RJ-45 cable and an MMOD DB-25 adapter. This cabling configuration is recommended and supported by Cisco for RJ-45 ports. **Step 2** If you are using a rolled RJ-45 cable with an MDCE DB-25 adapter, or a straight RJ-45 cable with an MDTE DB-25 adapter, you must dismantle the connector on the EIA/TIA-232 side and move pin 6 to pin 8. This turns the MDCE or MDTE adapter into an MMOD adapter by wiring the DCD output of the modem to the DSR input of the access server or router. **Step 3** Use the **show line** *line-number* EXEC command to verify that the cabling is correct. See the explanation of the **show line** command output in the section "Interpreting show line Output," following.
Hardware problem	**Step 1** Verify that you are using the correct cabling and that all connections are good. **Step 2** Check all hardware for damage, including cabling (broken wire), adapters (loose pin), access server ports, and modem. **Step 3** See the "Troubleshooting Router Startup Problems" chapter for more information on hardware troubleshooting.

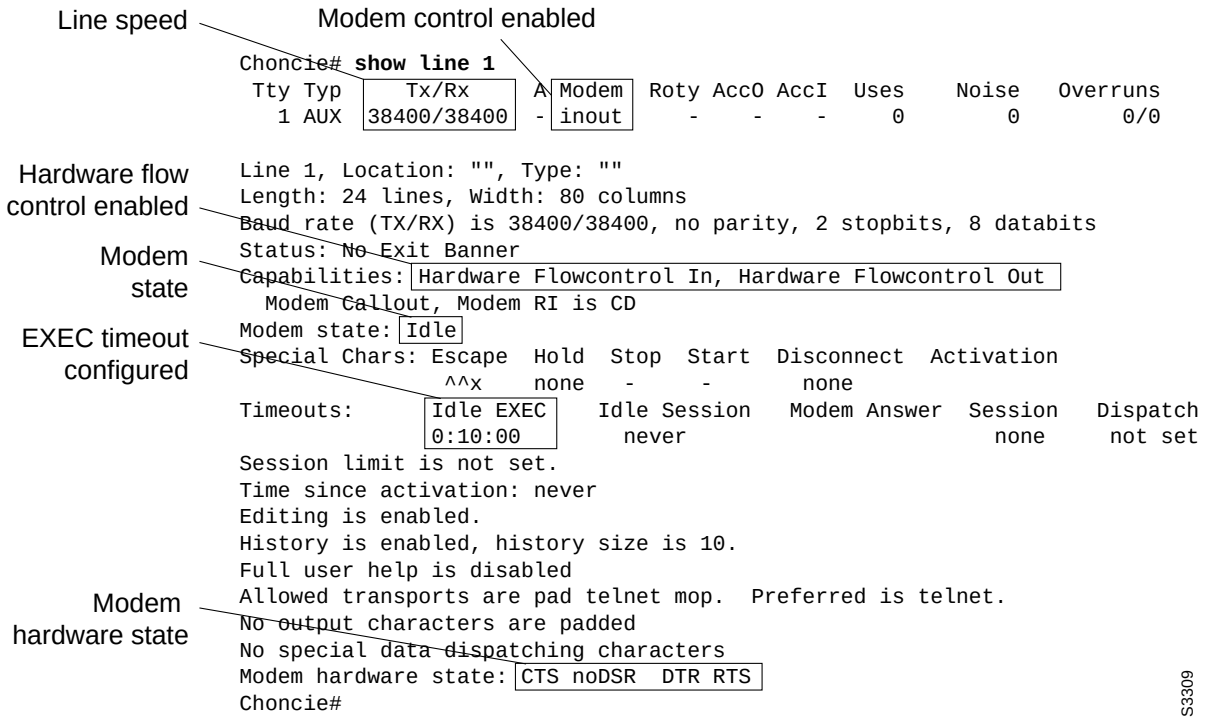
Figure 3-12 Hayes-Compatible Modem Command String for Pre-Modem Control Software



Interpreting show line Output

The output from the **show line** *line-number* EXEC command is useful when troubleshooting a modem-to-access server or router connection. Figure 3-13 shows the output from the **show line** *line-number* command. Important fields and their meanings are noted following.

Figure 3-13 show line Command Output



When connectivity problems occur, important output appears in the Modem State and the Modem Hardware State fields.

Note The Modem Hardware State field does not appear in the **show line** *line-number* output for every platform. In certain cases, the indications for signal states will be shown in the Modem State field instead.

Table 3-5 shows typical Modem State and Modem Hardware State strings from the output of the **show line** *line-number* command and explains the meaning of each state.

Table 3-5 Modem and Modem Hardware States in show line Output

Modem State	Modem Hardware State	Meaning
Idle	CTS noDSR DTR RTS	These are the proper modem states for connections between an access server or router and a modem. Output of any other kind generally indicates a problem.
Ready	–	If the Modem State is Ready instead of Idle, there are three possibilities: **1** Modem control is not configured on the access server or router. Configure the access server or router with the **modem inout** line configuration command. **2** A session exists on the line. Issue the **show users** EXEC command and use the **clear line** privileged EXEC command to kill the session if desired. **3** DSR is high. There are two possible reasons for this: — Cabling problems—The DSR signal from the modem is connected to DSR from the access server. The proper signalling is DCD (modem) to DSR (access server). Check the cabling configuration as described in Table 3-4. — Modem configured for DCD always high—The modem should be reconfigured to have DCD high only on carrier detect (CD). This is usually done with the **&C1** modem command (see Figure 3-11), but check your modem documentation for the exact syntax for your modem. You might have to configure the access server line to which the modem is connected with the **no exec** line configuration command. Clear the line with the **clear line** privileged EXEC command, initiate a reverse Telnet session with the modem, and reconfigure the modem so that DCD is high only on CD. End the Telnet session by entering **disconnect** and reconfigure the access server line with the **exec** line configuration command.

Modem State	Modem Hardware State	Meaning
Ready	noCTS noDSR DTR RTS	There are four possibilities for the noCTS string appearing in the Modem Hardware State field: **1** Modem is turned off. **2** Modem is not connected to the access server properly. Check the cabling connections from the modem to the access server. **3** Incorrect cabling configuration (either rolled MDCE or straight MDTE, but without the pins moved). See Table 3-4 for information on the recommended cabling configuration. **4** Modem is not configured for hardware flow control. Disable hardware flow control on the access server with the **no flowcontrol hardware** line configuration command. Enable hardware flow control on the modem via a Reverse Telnet session. (Consult your modem documentation and see the section "Initiating a Reverse Telnet Session to a Modem," earlier in this chapter.) Reenable hardware flow control on the access server with the **flowcontrol hardware** line configuration command.
Ready	CTS DSR DTR RTS	There are two possibilities for the presence of the DSR string instead of the noDSR string in the Modem Hardware State field: **1** Incorrect cabling configuration (either rolled MDCE or straight MDTE, but without the pins moved). See Table 3-4 for information on the recommended cabling configuration. **2** The modem is configured for DCD always high. Reconfigure the modem so that DCD is only high on CD. This is usually done with the **&C1** modem command (see Figure 3-11), but check your modem documentation for the exact syntax for your modem. Configure the access server line to which the modem is connected with the **no exec** line configuration command. Clear the line with the **clear line** privileged EXEC command, initiate a reverse Telnet session with the modem, and reconfigure the modem so that DCD is high only on CD. End the Telnet session by entering **disconnect**. Reconfigure the access server line with the **exec** line configuration command.
Ready	CTS* DSR* DTR RTS	If this string appears in the Modem Hardware State field, it is likely that modem control is not enabled on the access server. Use the **modem inout** line configuration command to enable modem control on the line. See Table 3-4 for more information on configuring modem control on an access server or router line.

Remote Dial-In Sees “Garbage”

Symptom: Attempts to establish remote dial-in sessions over a modem to a Cisco access server or router return “garbage” and ultimately result in no connection to the remote site. User might see a “Connection Closed by Foreign Host” message. Table 3-6 describes possible causes and suggests actions for remote dial-in sessions seeing “garbage.”

Table 3-6 Modem: Remote Dial-In Sessions Seeing “Garbage”

Possible Causes	Suggested Actions
Modem speed setting is not locked.	**Step 1** Issue the **show line** EXEC command on the access server or router. The output for the auxiliary port should indicate the currently configured transmit (Tx) and receive (Rx) speeds. For an explanation of the output from the **show line** command, see the “Interpreting show line Output” section earlier in this chapter. **Step 2** If the line speed is not configured to the speed you desire, you must reconfigure the line. Use the **speed** line configuration command to set the line speed on the access server or router line. Set the value to the highest speed in common between the modem and the access server or router port. NOTE: If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data. **Step 3** Issue the **show line** EXEC command again and confirm that the line speed is set to the desired value. **Step 4** When you are certain that the access server or router line is configured for the desired speed, initiate a reverse Telnet session to the modem via that line. For more information, see the section “Initiating a Reverse Telnet Session to a Modem.” **Step 5** Issue a modem command string that includes the lock DTE speed command for your modem. See your modem documentation for exact configuration command syntax. NOTE: The lock DTE speed command, which might also be referred to as *port rate adjust* or *buffered mode*, is often related to the way in which the modem handles error correction. This command varies widely between modems. Locking the modem speed ensures that the modem always communicates with the Cisco access server or router at the speed configured on the Cisco auxiliary port. If this command is not used, the modem will revert to the speed of the data link (the telephone line) instead of communicating at the speed configured on the access server.

High Rate of Data Loss Over Modem Connection

Symptom: Remote sessions over a modem connection experience a high rate of data loss. Table 3-7 shows possible causes and suggests actions when there is a high rate of data loss over a modem connection.

Table 3-7 Modem: High Rate of Data Loss Over Modem Connection

Possible Causes	Suggested Actions
Error correction is not configured on the modem.	**Step 1** Make certain the modem is configured for error correction. For the exact syntax of the command, see your modem documentation.
Flow control is not enabled, is enabled only on one device (either DTE or DCE), or is misconfigured.	**Step 1** Display detailed information about the auxiliary line using the **show line** *aux-line-number* EXEC command. In the Capabilities field (see Figure 3-13), look for the following: `Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out...` If there is no mention of hardware flow control in this field, hardware flow control is not enabled on the line. Cisco recommends hardware flow control for access server-to-modem connections. For an explanation of the output from the **show line** command, see the "Interpreting show line Output" section earlier in this chapter. **Step 2** Configure hardware flow control on the line using the **flowcontrol hardware** line configuration command. NOTE: If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data. **Step 3** After enabling hardware flow control on the access server or router line, initiate a reverse Telnet session to the modem via that line. For more information, see the section "Initiating a Reverse Telnet Session to a Modem." **Step 4** Issue a modem command string that includes the RTS/CTS Flow command for your modem. This command ensures that the modem is using the same method of flow control (that is, hardware flow control) as the Cisco access server or router. See your modem documentation for exact configuration command syntax. Figure 3-11 shows the hardware flow control command string for a Hayes-compatible modem.

Modem Does Not Disconnect Properly

Symptom: Modem does not disconnect properly. Connection to modem does not terminate when **quit** command is entered. Table 3-8 describes possible causes and suggests actions for a modem that does not disconnect properly.

Table 3-8 Modem: Modem Not Disconnecting Properly

Possible Causes	Suggested Actions
Modem is not sensing DTR.	**Step 1** Enter the Hangup DTR modem command string. This command tells the modem to drop carrier when the DTR signal is no longer being received. On a Hayes-compatible modem the **&D3** string is commonly used, as shown in Figure 3-11. For the exact syntax of this command, see the documentation for your modem.
Modem control is not configured on the router or access server (modem control on auxiliary ports is only available in Software Release 9.21 and later).	**Step 1** See Table 3-4 for instructions on configuring modem control on a router or access server port.

Remote Dial-In Client Receives No EXEC Prompt

Symptom: Remote dial-in client opens a session and appears to be connected, but the user does not receive an EXEC prompt (for example, a Username or Router> prompt). Table 3-9 describes possible causes and suggests actions for a remote dial-in client that is not receiving an EXEC prompt.

Table 3-9 Modem: Remote Dial-In Client Is Not Receiving an EXEC Prompt

Possible Causes	Suggested Actions
Autoselect is enabled on the line.	**Step 1** Attempt to access EXEC mode by issuing a carriage return.
Line is configured with the **no exec** command.	**Step 1** Use the **show line** *line-number* EXEC command to view the status of the appropriate line. Check the Capabilities field to see if it says "EXEC suppressed." If this is the case, the **no exec** line configuration command is enabled. **Step 2** Configure the **exec** line configuration command on the line to allow EXEC sessions to be initiated.
Flow control is not enabled, is enabled only on one device (either DTE or DCE), or is misconfigured.	**Step 1** For information on configuring flow control, see Table 3-7.
Modem speed setting is not locked.	**Step 1** For information on setting the speed of your access server or modem, see Table 3-6.

Remote Dial-In Interrupts Existing Sessions

Symptom: Remote dial-in session interrupts an already existing session initiated by another user. Table 3-10 describes possible causes and suggests actions for remote dial-in sessions interrupting existing sessions.

Table 3-10 Modem: Remote Dial-In Interrupts Existing Sessions

Possible Causes	Suggested Actions
Modem configured for DCD always high.	**Step 1** The modem should be reconfigured to have DCD high only on carrier detect (CD). This is usually done with the **&C1** modem command string (see Figure 3-11), but check your modem documentation for the exact syntax for your modem. **Step 2** You might have to configure the access server line to which the modem is connected with the **no exec** line configuration command. Clear the line with the **clear line** privileged EXEC command, initiate a reverse Telnet session with the modem, and reconfigure the modem so that DCD is high only on CD. **Step 3** End the Telnet session by entering **disconnect** and reconfigure the access server line with the **exec** line configuration command.
Modem control is not configured on the router or access server (modem control on auxiliary ports is only available in Software Release 9.21 and later).	**Step 1** See Table 3-4 for instructions on configuring modem control on a router or access server port.
Incorrect cabling configuration	**Step 1** See Table 3-4 for information on the recommended cabling configuration.

PART 2

Troubleshooting Connectivity

CHAPTER 4

Troubleshooting AppleTalk Connectivity

This chapter presents protocol-related troubleshooting information for AppleTalk connectivity problems. The emphasis is on symptoms and problems associated with AppleTalk network connectivity.

This chapter consists of the following sections:

- AppleTalk Internetworking Terminology
- AppleTalk Internetworking Guidelines
- Preventing AppleTalk Configuration Problems
- AppleTalk Diagnostic Techniques
- AppleTalk Service Availability Scenario
- Example AppleTalk Enhanced IGRP Diagnostic Session
- AppleTalk Connectivity Symptoms

The symptom modules presented in this chapter consist of the following sections:

- Symptom statement—A specific symptom associated with AppleTalk connectivity
- Possible causes and suggested actions—A table of possible symptom causes and suggested actions for resolving each cause

AppleTalk Internetworking Terminology

The following discussion establishes a framework for analyzing AppleTalk internetworking problems.

Networks and Internetworks

Distinguishing problems that occur on a single cable segment from problems that occur on an entire network is difficult to do without making an explicit distinction between *networks* and *internetworks*. For this discussion, the term *network* refers to individual networks as defined by their associated, unique AppleTalk network numbers or cable ranges. The term *internetwork* refers to the entire collection of networks connected via internetwork routers.

Phase 1 and Phase 2 Routers

In AppleTalk, the terms *Phase 1* and *Phase 2* are often confusing. Cisco refers to *routers* as being Phase 1 or Phase 2 with respect to their ability to support the AppleTalk Phase 2 enhancements. Cisco routers dynamically determine whether their neighbors are Phase 2 compliant, and operate in Phase 1 compatibility mode if necessary. Most currently offered routers are Phase 2 routers. Older routers that have not been upgraded may be Phase 1 routers.

Note Some routers can be configured for Phase 1, Phase 2, or *transition mode*. Cisco recommends that routers be configured for Phase 2 at the earliest opportunity, subject to limitations in software (such as routers that do not allow nonextended Ethernet configurations for Phase 2). Cisco recommends against the use of transition mode, which is an interim solution at best. Transition mode implementations can be avoided by using enhancements available in Cisco routers.

Nonextended and Extended Networks

To describe a network or interface, Cisco uses the terms *nonextended* and *extended*. A nonextended network contains a single network number (such as network 2) and does not allow two nodes on a single network segment to belong to different zones.

An extended network can contain multiple consecutive network numbers (Cisco refers to this as a cable range), though it does not require it (for example, 3-3 is a valid extended cable range). An extended network also allows multiple zones to be configured on a single network segment. Nonextended networks use Advanced Research Projects Agency (ARPA) Ethernet Type II encapsulation on Ethernet. Extended networks use Subnetwork Access Protocol (SNAP) encapsulation, which is also used by Fiber Distributed Data Interface (FDDI), Token Ring, and most other newer media.

Note There are no inherent problems in transporting traffic from extended networks across nonextended networks. However, there are certain implementation rules that apply to internetworks that use both Phase 1 and Phase 2 routers. These rules are discussed in "Identifying a Phase 1 and Phase 2 Rule Violation," later in this chapter.

AURP Tunnel

The AppleTalk Update-based Routing Protocol (AURP) allows two noncontiguous AppleTalk networks to communicate by way of a tunnel through a backbone network. AppleTalk traffic and AURP routing information are encapsulated in the backbone protocol header (for example, IP), sent through the backbone network, and stripped of the foreign header upon arriving at the far end of the tunnel.

Exterior Router

An exterior router is a router that borders an AppleTalk network and a backbone network using another protocol, such as IP. Exterior routers are connected to an AURP tunnel and are responsible for encapsulating and de-encapsulating AppleTalk traffic as it is passed in and out of the backbone network. An exterior router places the AppleTalk data in the protocol header used by the backbone, which affords the AppleTalk traffic the same advantages as any other traffic on the backbone. In addition, exterior routers use AURP routing updates to maintain routing tables for AppleTalk destinations located on the far side of the AURP tunnel.

AppleTalk Remote Access

AppleTalk Remote Access (ARA) is an Apple protocol that allows a remote user on a Macintosh personal computer to access the resources of a remote site via a point-to-point connection to an ARA server (such as a Cisco access server).

AppleTalk Internetworking Guidelines

Internetworks based on the AppleTalk networking protocol suite can be complex. The fact that AppleTalk was designed to be easy to use does not necessarily make AppleTalk internetworks easy to administer. Before exploring specific symptoms, the following discussions outline some hints and suggestions for AppleTalk internetwork troubleshooters.

When you are setting up an AppleTalk internetwork, remember these two guidelines:

- Every router that is connected to a specific network must agree on the configuration of that network (here, network refers to a single cable segment).
- Every network number in an internetwork must be unique.

Common AppleTalk Internetworking Problems

The following discussion covers some of the most common problems associated with AppleTalk internetworks. The problems include the following:

- Configuration Mismatch
- Duplicate Network Numbers
- Phase 1 and Phase 2 Rule Violations
- ZIP Problems
- Access List Errors
- Unstable Routes
- Unexpected Back Door

The problem descriptions outline the general nature of each problem and provide some diagnostic notes. Specific actions associated with each problem are detailed in the symptom modules, later in this chapter, that include these problems as likely causes. These problems do not represent all known AppleTalk internetworking problems. Indeed, only a small subset of potential pitfalls are covered. However, these problems are commonly encountered when creating, upgrading, or modifying AppleTalk internetworks.

Configuration Mismatch

A configuration mismatch occurs when the following AppleTalk rule is violated:

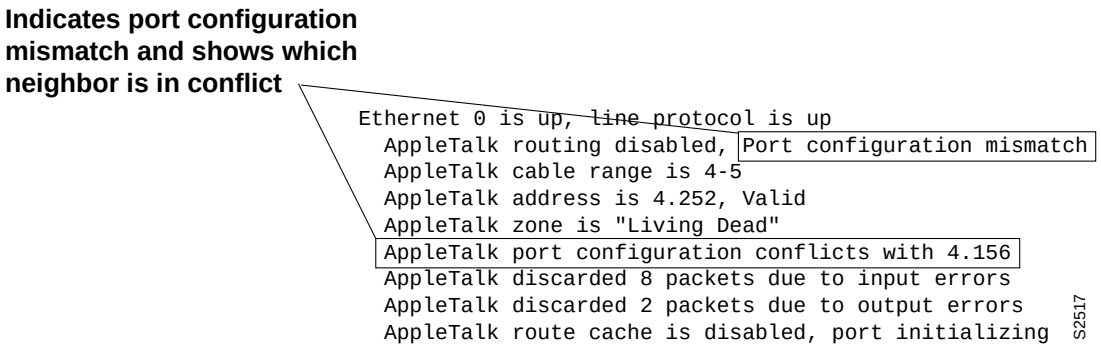
> *All AppleTalk routers on a given cable must agree on the configuration of that cable (meaning that all routers must have matching network numbers, default zone, and zone list).*

To protect against configuration errors that violate this rule, AppleTalk routers block activation of any port on which a violation of this rule exists. At interface initialization, if other routers on the network do not agree with the way a Cisco router is configured, the Cisco router will not allow AppleTalk to become operational on that interface. Cisco routers attempt to restart such an interface every 2 minutes to avoid outages that result from transient conditions.

However, if the router is already operational, and another router whose configuration does not match becomes active, the router will continue to operate on that interface until the interface is reset. At that point, the interface will fail to become active, and the router will declare a port configuration mismatch in the **show appletalk interface** EXEC command.

Figure 4-1 is an example of **show appletalk interface** command output when a configuration mismatch exists.

Figure 4-1 Output of the show appletalk interface Command that Illustrates Port Mismatch



You can display the Name Binding Protocol (NBP) registered name of the conflicting router, which can simplify resolution of a port mismatch problem. To see registered NBP names, enable the **appletalk name-lookup-interval** global configuration command. When that command is enabled, the **show appletalk interface** EXEC command displays nodes by NBP registration name.

Duplicate Network Numbers

Network numbers are analogous to postal codes—both are used to route information to the proper destination. A duplicate network number or postal code causes confusion about the location of the proper destination that can prevent delivery. In AppleTalk, network numbers must be unique within an internetwork. If duplicate network numbers exist, some packets are not routed to their intended destinations and are lost or misdirected. Duplicate network numbers can cause other connectivity and performance problems as well.

Phase 1 and Phase 2 Rule Violations

When Phase 1 and Phase 2 routers are in the same internetwork, the internetwork specifications must conform to the following rules:

- There can be no “wide” cable range specifications in the Phase 2 extended portion of the internetwork. In other words, all cable ranges must span no more than *one* network number. Examples of acceptable cable ranges are 9–9, 20–20, and 2–2.
- Multiple zones cannot be assigned to narrow cable ranges (such as 3–3).

If these rules are not followed, connectivity between the nonextended and extended portions of an internetwork becomes degraded or is even lost. In particular, services located on nonextended networks serviced by Phase 1 routers will not be visible on the other side of the Phase 1 router.

Phase 1 AppleTalk has three types of NBP packets, and Phase 2 AppleTalk has four types of NBP packets. This difference can lead to communication problems between Phase 1 and Phase 2 routers. Table 4-1 lists the NBP packet types for AppleTalk Phase 1 and Phase 2.

Table 4-1 Comparison of Phase 1 and Phase 2 NBP Packet Types

Phase 1 NBP Packet	Phase 2 NBP Packet
BrRq (Broadcast Request)	BrRq (Broadcast Request)
LkUp (Lookup)	FwdReq (Forward Request)
	LkUp (Lookup)
LkUp-Reply (Lookup Reply)	LkUp-Reply (Lookup Reply)

As shown in Table 4-1, Forward Request packets do not exist in Phase 1. Only Phase 2 routers know what to do with them. Phase 1 routers that receive Forward Request packets simply drop them.

Note Just because a router is configured for nonextended networks *does not mean* it is a Phase 1 router. A Cisco router running Software Release 8.2 or a later release is a Phase 2-compliant router *regardless* of how the interfaces are configured.

ZIP Problems

Routers use the Zone Information Protocol (ZIP) to exchange zone information, and end systems use ZIP to acquire zone lists. No AppleTalk mechanism forces routers to update zone lists. After a zone has been acquired, routers do not make another ZIP request unless the network has aged out of the routing table for some reason. For that reason, you must use care when adding or removing zone names from an active network.

A *ZIP storm* occurs when a router propagates a route for which it currently has no corresponding zone name; the route is then propagated by downstream routers.

Cisco routers provide a *firewall* against ZIP storms in the internetwork. If a Cisco router receives a routing update from a neighbor, it does not propagate that new route until it receives the accompanying zone name.

You can use the **show appletalk traffic** EXEC command to check if a ZIP storm is in progress. Look for AppleTalk traffic counters for ZIP requests that increment very rapidly. Use the **debug apple zip** privileged EXEC command to identify the network for which the zone is being requested by neighboring routers. You can also use the **show apple private** EXEC command to check on the number of pending ZIP requests.

If you determine that a ZIP storm is occurring, search for the router that injected the network number into the internetwork (and that is causing the excessive ZIP traffic). The **show appletalk traffic** and **show appletalk route** EXEC commands provide information that can help you find the suspect router. When you find the offending node, stop it from propagating invalid routes. This might require you to upgrade the software on the router.

Access List Errors

Access lists provide a powerful way to control traffic and limit access to resources on an AppleTalk network. However, improperly implemented access lists can lead to a number of failures on your internetwork. Typical problem symptoms associated with incorrectly specified access lists include services for a particular network that are not visible to other networks, zones that are missing from the Chooser, and services that are visible in the Chooser, but are not accessible.

Unstable Routes

Excessive load on internetworks that have many routers can prevent some routers from sending Routing Table Maintenance Protocol (RTMP) updates every 10 seconds as they should. Because routes begin to be aged out after the loss of two successive RTMP updates, the failure of RTMP updates to arrive results in unnecessary route changes. Zones may fade in and out of the Chooser or exhibit other unpredictable behavior. Route instability associated with load problems is known as *route flapping*.

Unexpected Back Door

A *back door* is any unexpected path or route through an internetwork. The existence of a back door can result from a number of different events: IP gateways establishing a DDP/IP link unexpectedly; bridges being installed without notice; or even users connecting networks with dial-up connections. Back doors typically cause a change in performance over the internetwork and connectivity problems. Performance problems usually occur because all traffic between two sites is going through a lower-bandwidth circuit, or because all traffic is being sent through a single gateway. Connectivity problems can result when routing loops form or when duplicate network numbers are introduced.

Preventing AppleTalk Configuration Problems

This section offers a number of preventative measures and tips for avoiding and addressing configuration problems in AppleTalk internetworks. It consists of the following topics:

- AppleTalk Problem-Prevention Suggestions—This table describes preventative actions that can help avoid or reduce configuration problems on your AppleTalk internetwork.
- AppleTalk Protocol Startup Tips—Tips on bringing up new interfaces on existing AppleTalk networks.
- Internetwork Reconfiguration Problem Prevention—Tips on preventing problems when performing internetwork configuration changes.
- Changing Zone Names—Describes the recommended procedure for changing AppleTalk zone names.
- Forcing an Interface Up—Describes how to force an AppleTalk interface to come up in spite of configuration conflicts.

AppleTalk Problem-Prevention Suggestions

Table 4-2 provides a list of suggestions intended to reduce problems when you are configuring a router for AppleTalk.

Table 4-2 AppleTalk Problem-Prevention Suggestions

Preventive Action	Comments
Upgrade to Phase 2 wherever possible.	To minimize interoperability problems, upgrade all routers to Phase 2. Phase 1/Phase 2 networks can be problematic, as can AppleTalk networks using nonextended Ethernet.
When you are configuring or making changes to a router or interface for AppleTalk, enable the **debug apple events** privileged EXEC command.	The **debug apple events** privileged EXEC command tracks the progress and status of changes in the internetwork and alerts you to any errors. You also should run this command periodically when you suspect network problems. However, in a stable network, this command does not return any information. Remember to disable this command with the **no debug apple events** command when you have completed diagnostic activities. You may want to add the configuration command **appletalk event-logging** and establish a *syslog server* at your site, which will keep a running log, with timestamps, of significant events on your network.
Minimize the number of different zones in the internetwork.	Give all of the backbone/wide-area network (WAN) connections the same zone name (such as ZZSerial) or have WAN connections share the zone name of the smaller of the two sites that it connects. In most internetworks, it is not desirable to have the zone names for all backbone or WAN connections appear in the Chooser list. If you make the zone name of all the WAN links the same (ZZSerial), only that entry appears in the Chooser menu.
Design your network with special attention to the direction in which traffic will flow.	Careful zone-mapping design can minimize unnecessary NBP traffic. Note that in System 6, if a user opens the Chooser, the Macintosh continually sends NBP BrReq packets. In System 7, a logarithmic backoff minimizes the amount of traffic generated. Taking this action can be particularly important in WANs where traffic traversing WAN links (such as X.25) can be quite expensive.
Zones should be named for the convenience of end users and not for diagnostic purposes.	Zones should not be used as cable labels (in other words, do not identify one zone per cable with names like “Bld2 S/W Serial T1”). In general, a mixture of location and departmental naming conventions works best (for example, “Bldg 13 Engineering”).
Control the number of zones used.	Many routers have specific limits on the number of routes and zones they can handle. These limits usually result from memory constraints, but are sometimes fixed limits or are related to available bandwidth. If you exceed such a limit on a cable connected to one of these devices, zones may come and go unpredictably. Cisco routers do not impose fixed limits. However, it recommended that you not configure all zones on all cables.

Preventive Action	Comments
Use the **appletalk timers** global configuration command in busy networks with large numbers of internetwork routers on a single network.	On very busy networks with many LocalTalk-to-EtherTalk routers, the LocalTalk Link Access Protocol (LLAP) routers may not send RTMP updates every 10 seconds as they should, which results in unnecessary route flapping. To prevent this problem, adjust the AppleTalk timers by using the **appletalk timers 10 30 90** command. The first number should always be 10, and the third number should always be three times the value of the second number. However, setting the second and third numbers to excessively high values can result in slow routing convergence when network topology changes. Timers should be consistently set to the *same value* throughout the internetwork, or at a minimum, throughout the backbone of the internetwork. Check with a qualified technical support representative before changing AppleTalk timer values.

AppleTalk Protocol Startup Tips

When bringing an interface up on an existing cable where a long zone list is defined, the following actions will help you avoid mistakes and save effort.

1. Bring up the interface in *discovery mode* (using the **appletalk discovery** interface configuration command). The **debug apple events** privileged EXEC command will let you know when the process is complete by displaying an "operational" message.
2. After discovery is complete, and while in interface configuration mode, enter the **no appletalk discovery** interface configuration command for the specific AppleTalk interface being initialized. This action allows the acquired information to be saved and requires that the configuration be validated at port startup. The router exits out of discovery mode for normal operation (it is recommended that discovery mode only be used when initially configuring networks). Thereafter, all routers should be configured for *seed*, or nondiscovery, mode.
3. Issue the **write memory** privileged EXEC command to save the acquired information to nonvolatile RAM.
4. Verify the configuration with the **show configuration** EXEC command.

Internetwork Reconfiguration Problem Prevention

It is common to create configuration conflicts when changing zone names or cable range numbers. In particular, problems arise when routers exist on the internetwork about which you are not (administratively) aware.

Remember that many devices can act as routers (for example, Pathworks servers or UNIX workstations running CAP to do print and file sharing). In general, if you are changing zone names or cable range numbers in your internetwork, all routers should be shut down, or a Cisco router will see a conflict and prevent AppleTalk from initializing on the interface.

Use the **show appletalk neighbors** EXEC command to determine on which routers to disable AppleTalk routing. Routers that are on the same network segment and that have sent RTMP updates in the last 10 seconds should have Appletalk disabled. Disable AppleTalk routing on all of the appropriate interfaces, wait approximately 10 minutes, and then bring up the master seed router.

Changing Zone Names

When changing a zone name on an existing network, perform the following actions:

Step 1 Disable AppleTalk on all interfaces on the cable for about 10 minutes. This allows all routers in the internetwork to age out the network number from their routing tables.

Step 2 Configure the new zone list.

Step 3 Re-enable AppleTalk on all interfaces.

These actions are required because AppleTalk makes no provisions for informing neighbors in the internetwork about a changed zone list. Routers only make ZIP queries when a new or previously aged-out network appears on the internetwork.

Adding a new zone to an extended cable configuration will result in the router refusing to bring up its interface for AppleTalk after the interface has been reset. This is because its configuration no longer matches that of its neighbors (configuration mismatch error).

Forcing an Interface Up

In certain situations, you might need to force an interface to come up despite the fact that its zone list conflicts with that of another router on the network. This can be done using the **appletalk ignore-verify-errors** global configuration command. Usually this other router would be one over which you have no administrative control, but which you are certain has an incorrect zone list.

The **appletalk ignore-verify-errors** command allows you to bypass the default behavior of an AppleTalk interface, which is to not come up if its zone list conflicts with that of its neighbors. However, you should use this command with *extreme* caution; bringing up an interface with a zone list that conflicts with that of other routers can cause serious network problems. In addition, the other router *must* be reconfigured at some point so that all the routers on the network agree on the zone list.

Once all the AppleTalk routers on the network have conforming zone lists, the **appletalk ignore-verify-errors** command should be disabled using the **no** form of the command. For complete information on the **appletalk ignore-verify-errors** global configuration command, see the *Router Products Configuration Guide* and the *Router Products Command Reference* publications.

AppleTalk Diagnostic Techniques

Use the following suggestions from router technical support representatives to help speed problem diagnosis and ensure efficient data gathering in the event of failures:

- The **debug apple events** privileged EXEC command is completely silent in a stable network. If the command produces any output, unnecessary changes are occurring on the internetwork. To monitor the internetwork for configuration and status changes, you can continuously log the output from this command to a *syslog daemon* on a UNIX host.
- To identify problem nodes, you can run ping tests. For example, **ping appletalk 2.24** pings AppleTalk node 2.24. Use this command to verify that the node is reachable from the router. The **ping** privileged EXEC command also supports a number of AppleTalk parameters, which provide additional troubleshooting capabilities. In particular, use the NBP option when AppleTalk zones are listed in the Chooser, but services are not available. If a configuration contains the **appletalk name-lookup-interval** global configuration command, the NBP option of the AppleTalk ping function displays nodes by their NBP registration name.

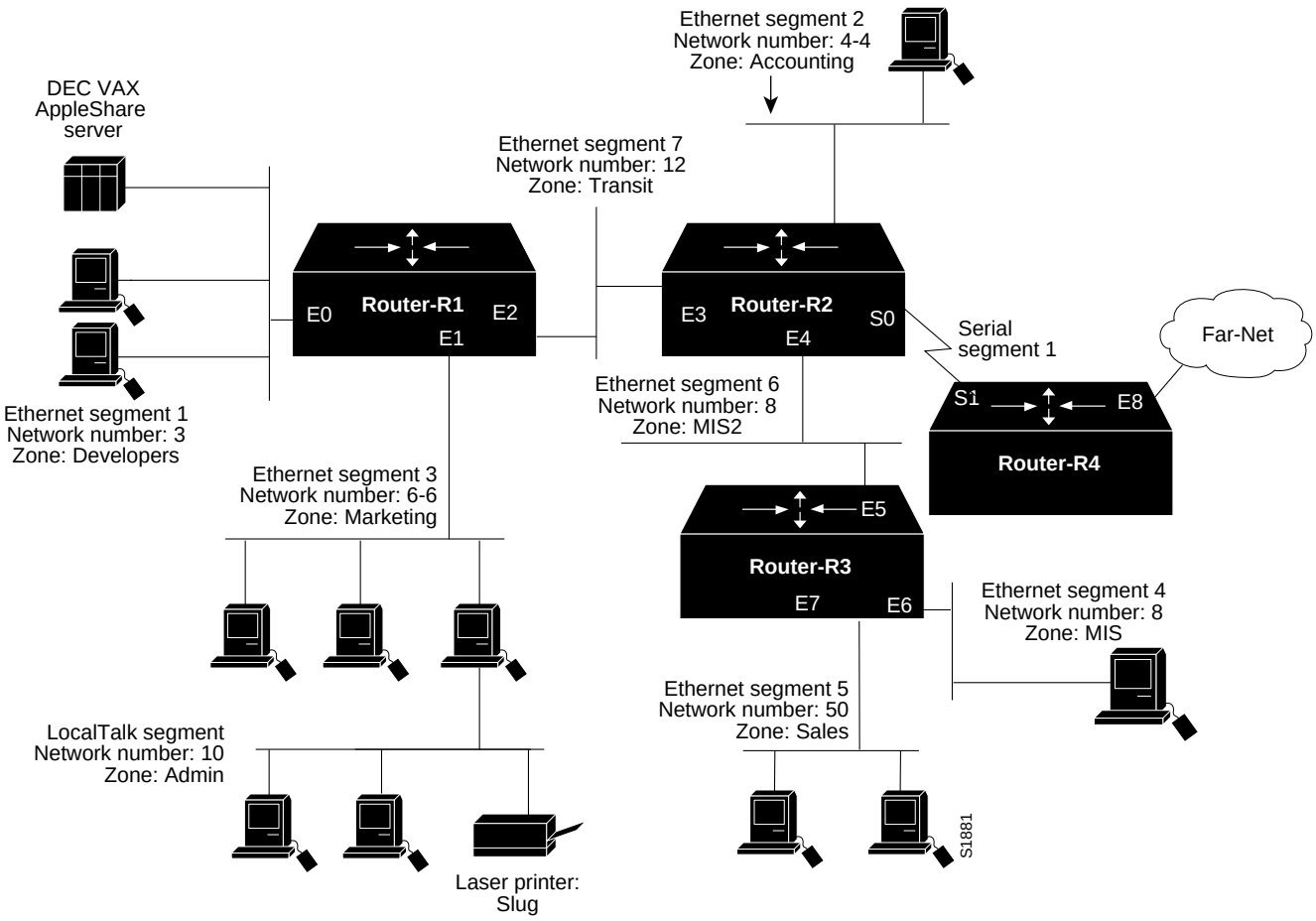
AppleTalk Service Availability Scenario

In recent years, AppleTalk-based internetworks have grown in size and scope of implementation. Once viewed as a simple protocol for small networks, AppleTalk has been stretched to allow handling of more nodes and sharing of services in larger internetworks. Along with these larger-scale and more complex implementations have come some of the implementation headaches common to any multivendor enterprise internetwork. This scenario focuses on several common problems that can block access to servers and services on an AppleTalk internetwork.

Symptoms

As shown in Figure 4-2, a number of local networks are segmented with routers, and a remote network is linked over a serial line.

Figure 4-2 Initial AppleTalk Connectivity Scenario Map



Assume that the following three symptoms were reported for this AppleTalk internetwork:

1. Macintosh user Melvin on Ethernet segment 2 reports that the laser printer Slug (attached to the LocalTalk network connected to IR-1) is not visible on his Chooser.
2. DEC VAX-based AppleShare server on Ethernet segment 1 is not visible to any users except Macintosh users Debbie and Biff on Ethernet segment 5.
3. AppleShare server Spunky on Ethernet segment 4 is sometimes visible in the Choosers of Macintosh users in this internetwork, but no one can access services on that server. Although users on the same network as Spunky can see local services, they find it difficult to access offnet services.

There are several problems that might lead to these symptoms. The first step is to characterize the configuration of this internetwork and then develop a list of likely suspect problems.

Environment Description

Some relevant facts regarding the internetworking environment shown in Figure 4-2 can be summarized as follows:

- Three Cisco routers (Router-R1, Router-R2, and Router-R3) and a non-Cisco internetwork router (IR-1) provide interconnection between local Ethernet segments and a LocalTalk network attached to IR-1.
- Remote service is provided via Router-R2 and the remotely located Cisco Router-R4 to an AppleTalk network (Far-Net) that is not controlled by local network administration.
- Macintosh users in the same zone as the DEC VAX can see all zones and can access offnet services.
- Users on all the local networks can access AppleTalk services on directly connected network cables.
- The routers in this internetwork are in the process of being converted from Phase 1 support to Phase 2 support.
- The only other protocol used in this internetwork is TCP/IP.
- With the exception of one LocalTalk segment, local networks are IEEE 802.3 thin Ethernets; the serial link is a dedicated T1 link (1.544 Mbps).
- The network applications intended to run over the T1 line include typical AppleTalk network services.

Diagnosing and Isolating Problem Causes

Given the situation, a number of problems could explain reported symptoms.

The following problems are likely candidates for symptom number 1 (laser printer Slug on Ethernet segment 3 is reported as not visible on Chooser by Macintosh user Melvin on Ethernet segment 2):

- Misconfigured router (Router-R1 or IR-1)
- Ethernet port on Router-R1 is shut down

The following problems are likely candidates for symptom number 2 (DEC VAX-based AppleShare server on Ethernet segment 1 is not visible to any users except users on Ethernet segment 5—a nonextended network):

- Duplicate network number
- Phase 1 and Phase 2 internetworking rule violation
- Network or port configuration mismatch

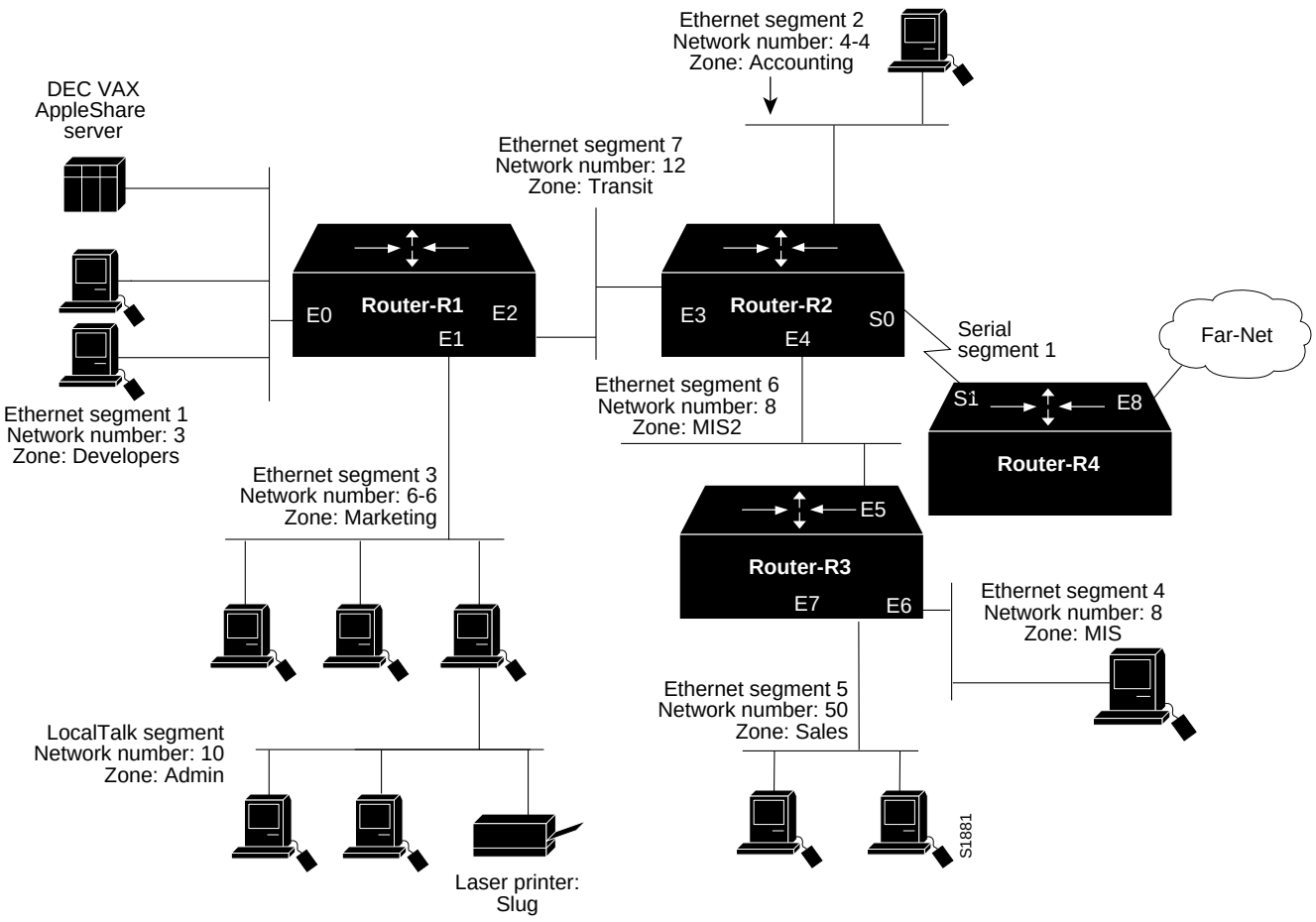
The following problems are likely candidates for symptom number 3. (AppleShare server Spunky on Ethernet segment 4 is sometimes visible in the Chooser of Macintosh systems in this internetwork. However, no one can access services on that server.)

- Duplicate network number
- Zone Information Protocol (ZIP) storm

After you identify a possible problem list, you must systematically analyze each potential cause. The following discussion considers the possible problems listed and illustrates resolution of discovered problems.

Before continuing with this process, it will be useful to map out the assignment of network numbers, cable ranges, and zones (or zone lists) associated with the internetwork. Figure 4-3 illustrates the known network numbers, cable ranges, and zones.

Figure 4-3 AppleTalk Zone and Network Number/Cable Range Assignments



Problem Resolution Process

This analysis starts by considering the problem list associated with the intermittent availability of Spunky (symptom number 3). Because the DEC VAX problem shares a possible cause with the Spunky availability problem, the analysis also evaluates the possibility of a common problem causing both symptoms. After that, the analysis steps through the list of possible causes until all possible causes are exhausted.

Looking for a ZIP Storm

It is not unusual to start with a possible problem because it is *easy* to diagnose. With this in mind, first consider the possibility of a ZIP storm.

Step 1 To detect a ZIP storm, first examine network activity with the **show appletalk traffic** command.

Look for ZIP requests in the output. Repeat this command after about 30 seconds or so. If the number is greater than 10 and increasing, there is likely to be a ZIP storm.

Step 2 If you observe an apparent ZIP storm, use the **show appletalk route** command and look for a network that shows up in the table but has "no zone set" for its zone listing. If such a listing appears, determine why the node is not responding to ZIP requests.

For this case, assume that no unusual number of ZIP requests appear, and you have eliminated a ZIP storm as a cause for symptom number 3. All symptoms are still being experienced.

Isolating Duplicate Network Numbers

The next possible cause for both symptom number 2 *and* symptom number 3 is the existence of duplicate network numbers in the internetwork. Unfortunately, these are not usually easy to find.

Step 1 First, use the **show appletalk interface ethernet 6** command on Router-R3 to obtain the AppleTalk network number for the local network. In this case, the (nonextended) network number is 8. Figure 4-4 illustrates a typical output for this command.

Figure 4-4 show appletalk interface ethernet 6 Command Output

```
Ethernet 6 is up, line protocol is up
  AppleTalk address is 8.12
  AppleTalk zone is "MIS"
```

S2391

Step 2 Next, disable AppleTalk using the **no appletalk routing** global configuration command as illustrated in Figure 4-5.

Figure 4-5 Disabling AppleTalk at the Router

```
Router-R3# configure terminal
no appletalk routing
<Ctrl-Z>
```

S2392

If there are no duplicate network numbers (another network number 8), the command **no appletalk routing** results in network number 8 being aged out of all routing tables in the internetwork.

Step 3 To determine whether this happens, perform successive **show appletalk route 8** commands on Router-R3 until the hop count stabilizes (indicating that a duplicate does exist), or until the route ages out (indicating that a duplicate does not exist).

If there is a duplicate, network 8 will not age out, but instead appears as a learned route from some other interface. Figure 4-6 illustrates how this change is registered in the **show appletalk route 2** display.

Figure 4-6 show appletalk route 2 Command Output

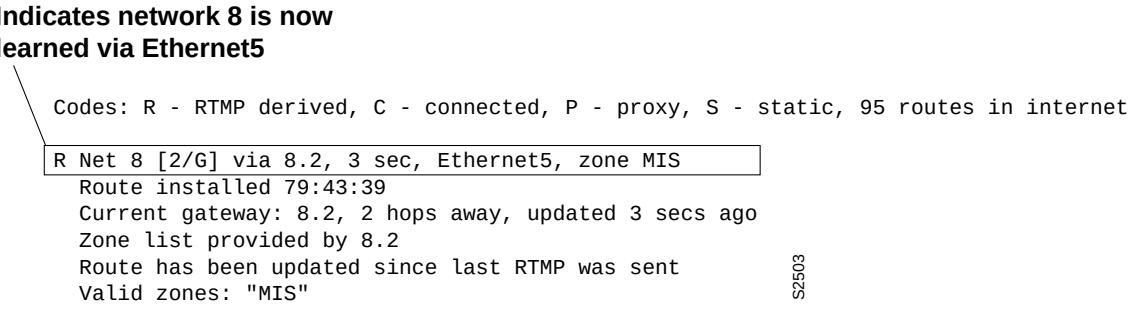


Figure 4-6 indicates the neighbor from which the location of the duplicate was learned. Because IP is also enabled in this internetwork, you can pinpoint the duplicate network number by connecting to the indicated neighbor. Use Telnet to connect to the indicated neighbor (here at *network.node* address 8.2), using the IP address or host name of the router. (In this case, assume Router-R2.)

Step 4 When a connection is made to the neighbor, repeat the **show appletalk route 8** command and examine the resulting output for the location of network number 8. Repeat this process until the display indicates that the network is *directly* connected.

Step 5 When the network is shown as directly connected, you have found the duplicate network number location. Now, you must change one of the routers (Router-R3 or the found router), as well as any other routers connected to the suspect network.

Assume that restoring service to Ethernet interface 6 on Router-R3 solves symptom 3 and that offnet Macintosh users in the internetwork can now access AppleShare server Spunky. However, users still cannot access the DEC VAX AppleShare server, and the laser printer Slug remains inaccessible.

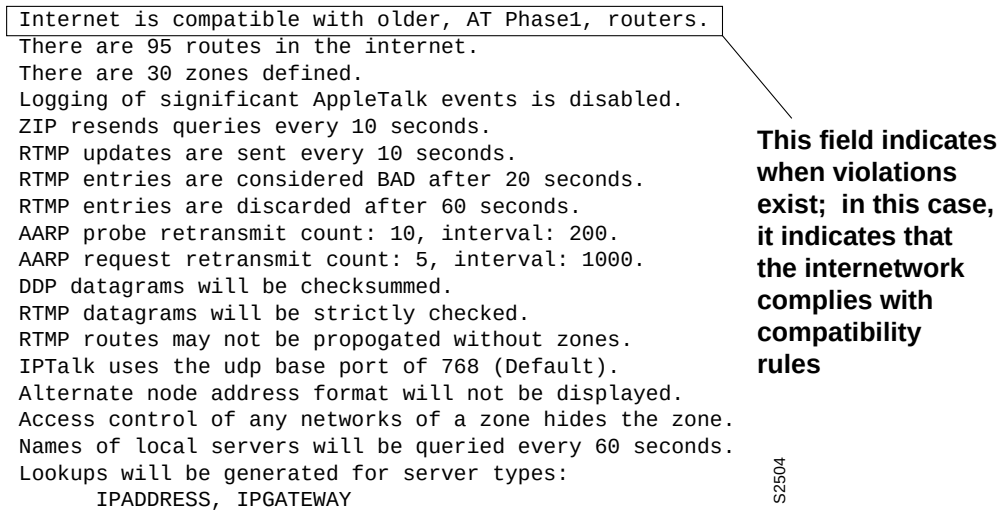
Identifying a Phase 1 and Phase 2 Rule Violation

It is possible that another duplicate network number in the internetwork is making the DEC VAX unavailable as an AppleShare server. However, remember that DEC VAX AppleShare service is accessible to Macintosh users Biff and Debbie on Ethernet segment 5 (network number 50), which eliminates a duplicate network number as the cause of the problem. DEC VAX AppleShare service to Macintosh users Biff and Debbie also rules out port configuration mismatch as a problem, because Router-R1 and Router-R3 agree about network configuration (network number/cable range and zone/zone list). This leaves a Phase 1 and Phase 2 rule violation as the remaining identified possible cause.

Step 1 To determine whether this is the problem, use the **show appletalk globals** command. Figure 4-7 illustrates the output of this command when the network is in compatibility mode. However, this display shows that the internetwork is *not* in compatibility mode, which indicates a Phase 1 and Phase 2 rule violation. A rule violation exists when any node has a configuration that does not conform to the following rules:

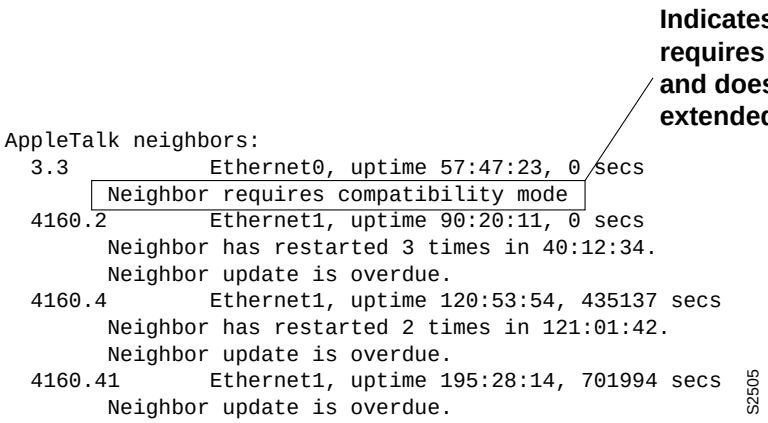
- There can be no wide cable range specifications in the Phase 2 extended portion of the internetwork. (Cable ranges must be specified to include only a single network number, such as 2-2 or 10-10.)
- Multiple zones cannot be assigned to networks or cable ranges.

Figure 4-7 show appletalk globals Command Output



Step 2 Next, use the **show appletalk neighbors** command at Router-R1 to identify the specific neighboring router that requires compatibility mode. Figure 4-8 illustrates such a listing.

Figure 4-8 show appletalk neighbors Command Output



Step 3 In this case, the neighbor in need of compatibility mode is the DEC VAX itself. You can upgrade the DEC VAX AppleShare server or use the **appletalk proxy-nbp** global configuration command to create what is in effect a virtual network off Router-R1. The command would be as follows:

appletalk proxy-nbp 200 Developers

Note that no router can have the same network number defined as a proxy network and that the specified network number cannot be associated with a physical network.

Adding **appletalk proxy-nbp** forces Router-R1 to send the proper NBP lookup packet for the zone named "Developers" to all networks. Using this command resolves the problem of access to the DEC VAX AppleShare server from extended networks.

However, laser printer Slug is still not accessible from Macintosh user Melvin on Ethernet segment 2.

Establishing Printer Service over the Internetwork

Two possible causes were cited for blocking availability to Slug: either the Router-R1 port is down, or Router-R1 or IR-1 has a configuration problem. Assume that Bobbi and Ernst (on extended network 6-6, zone Marketing) can now access offnet zones and service over Router-R1, but cannot see services on the other side of IR-1. This suggests that Router-R1 is probably operational and that the problem probably is with IR-1.

Step 1 Use the **show appletalk neighbors** command to determine whether Router-R1 can see IR-1. Look for any neighbors. If IR-1 has a configuration problem, it probably will not appear in the neighbor listing.

Step 2 Before proceeding with any further configuration analysis, verify that the cabling at IR-1 is intact. Try the **show appletalk neighbors** command from Router-R1 again. If router IR-1 still does not appear in the neighbor listing at this point, it is safe to suspect that IR-1 is a Phase 1 router and will require upgrading to support AppleTalk Phase 2 to operate in this internetwork.

Step 3 For further evidence, use the **show appletalk traffic** command and look for encapsulation failures. More than 100 encapsulation failures suggest Phase 1 and Phase 2 problems and support the hypothesis that IR-1 is the problem in this case. Figure 4-9 illustrates the output of the **show appletalk traffic** command.

Figure 4-9 show appletalk traffic Command Output

```
AppleTalk statistics:
  Rcvd:  1807514 total, 0 checksum errors, 7541 bad hop count
         1596186 local destination, 0 access denied
         0 for MacIP, 0 bad MacIP, 0 no client
         0 port disabled, 0 no listener
         0 ignored, 0 martians
  Bcast: 808385 received, 560408 sent
  Sent:  1530871 generated, 7422 forwarded, 222001 fast forwarded 24408 loopback
         0 forwarded from MacIP, 0 MacIP failures
         1087 encapsulation failed, 16 no route, 0 no source
  DDP:   1602380 long, 0 short, 0 macip, 0 bad size
  NBP:   1174003 received, 0 invalid, 0 proxies
         224166 replies sent, 912844 forwards, 387300 lookups, 1223 failures
  RTMP:  497388 received, 9 requests, 0 invalid, 0 ignored
         482638 sent, 0 replies
  ATP:   0 received
  ZIP:   1241 received, 4383 sent, 105 netinfo
  Echo:  28 received, 0 discarded, 0 illegal
         0 generated, 28 replies sent
  Responder:  0 received, 0 illegal, 0 unknown
         0 replies sent, 0 failures
  AARP:  384 requests, 595 replies, 1341 probes
         30 martians, 0 bad encapsulation, 0 unknown
         772 sent, 0 failures, 276 delays, 1087 drops
  Lost: 0 no buffers
  Unknown: 0 packets
  Discarded: 826 wrong encapsulation, 0 bad SNAP discriminator
```

Field reporting encapsulation failures

S2506

Step 4 To verify that IR-1 is a Phase 1 router, first bring up Router-R1 in discovery mode. This is done by using the **appletalk address** interface command to temporarily set the AppleTalk address for Ethernet interface 1 to 0.0. When this configuration is done, Router-R1 attempts to acquire configuration information for that cable from an operational Phase 1 router.

Making this change has the following effects:

- Ethernet interface 1 on Router-R1 comes up as a nonextended network.
- All nodes on the attached network cable range 6-6 are isolated.

However, this confirms that IR-1 is a Phase 1 router. (You can also confirm that IR-1 is a Phase 1 router by using the IR-1 configuration utility.)

Step 5 To resolve this access problem, IR-1 must be upgraded to be a Phase 2 AppleTalk router, and the Ethernet interface 1 on Router-R1 must be reconfigured to its original state (an extended network cable range of 6–6).

Problem Solution Summary

This scenario focused on diagnosing blocked service access in AppleTalk internetworks. Modifications discussed in this scenario included the following:

- Upgrading a Phase 1-only router to support Phase 2 removed blocked print service.
- Using the **appletalk proxy-nbp** command allowed access to a DEC VAX-based AppleShare server requiring Phase 1 compatibility.
- Eliminating duplicate network numbers ensured access to AppleShare server Spunky.

Figure 4-10 illustrates an example final configuration listing for Router-R1 obtained using the **write terminal** EXEC command, where **appletalk proxy-nbp** has been added.

Figure 4-10 Complete AppleTalk Router-R1 Final Configuration

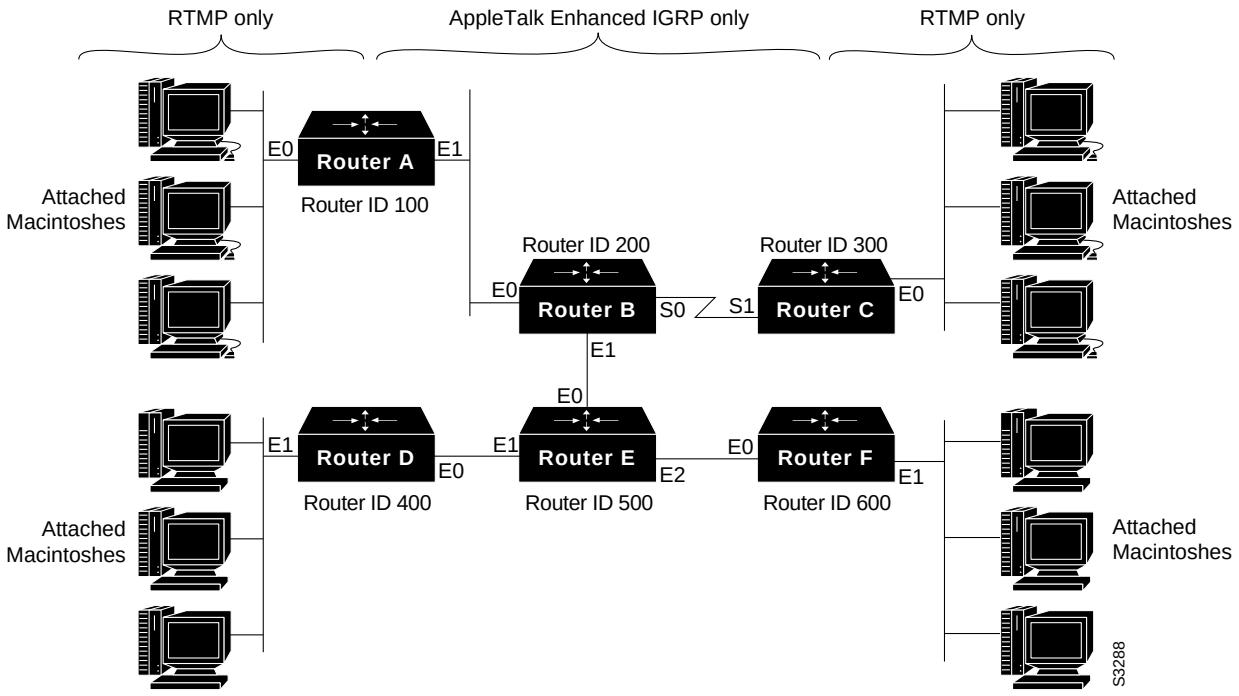
```
version 9.1
!
hostname Router-R1
!
enable-password toYNetgnm
!
appletalk routing
!
interface Ethernet 0
ip address 131.108.29.18 255.255.255.0
ip helper-address 131.108.13.111
ip helper-address 131.108.1.255
ip helper-address 131.108.13.255
keepalive 5
appletalk address 3.24
appletalk zone Developers
!
interface Ethernet 1
ip address 131.108.160.18 255.255.255.0
ip helper-address 131.108.1.255
keepalive 5
appletalk cable-range 6-6 6.19
appletalk zone Marketing
!
interface Ethernet 2
ip address 131.108.161.18 255.255.255.0
ip helper-address 131.108.1.255
keepalive 5
appletalk address 12.90
appletalk zone Transit
!
ip route 131.108.171.0 255.255.255.0 131.108.165.73
ip route 131.108.170.0 255.255.255.0 131.108.165.73
!
!
appletalk name-lookup-interval 60
appletalk lookup-type IPADDRESS
appletalk lookup-type IPGATEWAY
appletalk proxy-nbp 200 Developers
!
line aux 0
login
line vty 0 4
login
line con 0
exec-timeout 0 0
password klEwdGD
line aux 0
no exec
exec-timeout 0 0
password klEwdGD
line vty 0
exec-timeout 0 0
password klEwdGD
!
end
```

S2397

Example AppleTalk Enhanced IGRP Diagnostic Session

This section presents a sample diagnostic and troubleshooting session in an AppleTalk Enhanced IGRP environment. In this example network, AppleTalk Enhanced IGRP is running on the backbone, while RTMP is running on the edges, on the LANs with connected Macintosh PCs. This network topology is illustrated in Figure 4-11.

Figure 4-11 AppleTalk Network Running AppleTalk Enhanced IGRP and RTMP



Six Cisco routers are in the network shown in Figure 4-11. Four of the routers border LAN segments with connected Macintosh PCs. Router A runs RTMP on Ethernet interface 0 and AppleTalk Enhanced IGRP on Ethernet interface 1; Router C runs RTMP on Ethernet interface 0 and AppleTalk Enhanced IGRP on serial interface 1; and Router D and Router F run RTMP on Ethernet interface 1 and AppleTalk Enhanced IGRP on Ethernet interface 0.

Unlike the border routers, which run two routing protocols, Router B and Router E both run AppleTalk Enhanced IGRP exclusively on all of their interfaces. This is the Enhanced IGRP backbone of the network.

It is important to note that Macintosh PCs do not understand AppleTalk Enhanced IGRP, so only RTMP should be running on LAN segments with connected Macintosh PCs. Furthermore, while it may be desirable or necessary in certain network topologies, Cisco generally recommends that you not enable AppleTalk Enhanced IGRP and RTMP on the same interface, because doing so produces unnecessary bandwidth and processor overhead that might affect network performance. Only one or the other should be enabled on each interface. Allow route redistribution to exchange routing information between the two routing processes.

The following diagnostic tables (Table 4-3 and Table 4-4) illustrate step-by-step procedures for troubleshooting poor or lost connectivity in an internetworking environment like that shown in Figure 4-11. Potential trouble areas are identified and are ordered based on the likelihood of their

being the actual problem. A series of actions is then suggested for each problem. Table 4-3 encompasses the diagnostic and troubleshooting procedures for the multiprotocol portions of the Apple network shown in Figure 4-11, that is, the sections of the network running both RTMP and AppleTalk Enhanced IGRP. Table 4-4 addresses the single-protocol backbone of the Apple network in Figure 4-11, that is, the routers running only AppleTalk Enhanced IGRP.

Note Table 4-3 and Table 4-4 do not address hardware problems that might contribute to network connectivity problems. For information on troubleshooting hardware problems, see the "Troubleshooting Router Startup Problems" chapter.

Table 4-3 Multiprotocol AppleTalk Internetwork Diagnostics (RTMP and AppleTalk Enhanced IGRP)

Possible Problem	Suggested Actions
AppleTalk Enhanced IGRP is not globally configured on the appropriate routers.	**Step 1** Check the configuration of Router A using the **write terminal** privileged EXEC command. Look for an **appletalk routing eigrp** global configuration command entry. This command turns on AppleTalk Enhanced IGRP routing on the router.
	Step 2 If AppleTalk Enhanced IGRP routing is not enabled on Router A, use the **appletalk routing eigrp 100** global configuration command to enable it. The number indicated by the command is the AppleTalk Enhanced IGRP router ID. This number must be unique on the network (although a router can have more than one router ID configured).
	Step 3 Perform the same actions on Router C, Router D, and Router F. The **appletalk routing eigrp** global configuration command must be enabled on all routers that are running AppleTalk Enhanced IGRP. The router ID must be different for each router.
AppleTalk Enhanced IGRP is not enabled on the appropriate interfaces.	**Step 4** Issue the **write terminal** privileged EXEC command on Router A and examine the interface configurations. In order for an interface to generate AppleTalk Enhanced IGRP routing updates, the **appletalk protocol eigrp** interface configuration command must be present.
	Step 5 In the network shown in Figure 4-11, Router A should have AppleTalk Enhanced IGRP enabled only on Ethernet interface 1. Use the **appletalk protocol eigrp** interface configuration command to tell the interface to begin sending routing updates.
	Step 6 Perform the same actions on Router C, Router D, and Router F. On Router C, only serial interface 0 should have AppleTalk Enhanced IGRP enabled; on Router D, only Ethernet interface 0; and on Router F, only Ethernet interface 0.

Possible Problem	Suggested Actions
Routes are not being redistributed between RTMP and AppleTalk Enhanced IGRP.	**Step 7** Use the **write terminal** privileged EXEC command on Router A to determine whether route redistribution is disabled. Route redistribution is enabled by default on a router when the **appletalk routing** global configuration command is issued. However, it can be explicitly disabled using the **no appletalk route-redistribution** global configuration command.
	Step 8 If route redistribution is disabled, enable it using the **appletalk route-redistribution** global configuration command. If routes are not properly redistributed between RTMP and AppleTalk Enhanced IGRP, routing tables will not be accurate and packets will be lost.
	Step 9 Ensure that routes are being redistributed on all routers that border both the RTMP and the AppleTalk Enhanced IGRP environments. In Figure 4-11, this includes Router A, Router C, Router D, and Router F.
AppleTalk Enhanced IGRP is running on a LAN with connected Macintosh PCs.	**Step 10** Use the **write terminal** privileged EXEC command on Router A to make sure that only RTMP is enabled on Ethernet interface 0, which is connected to the LAN running the Macintosh PCs. Macintoshs do not understand AppleTalk Enhanced IGRP.
	Step 11 If RTMP is disabled, issue the **appletalk protocol rtmp** interface configuration command.
	Step 12 If necessary, disable AppleTalk Enhanced IGRP on Ethernet interface 0 using the **no appletalk protocol eigrp** interface configuration command.
	Step 13 Perform the same actions on Router C, Router D, and Router F. These routers all border network segments with connected Macintosh PCs.
AppleTalk Enhanced IGRP and RTMP are running simultaneously on the same interface.	**Step 14** Use the **write terminal** privileged EXEC command on Router A, Router C, Router D, and Router F to determine whether AppleTalk Enhanced IGRP and RTMP are both enabled on the same interface.
	Step 15 Running both AppleTalk Enhanced IGRP and RTMP on the same interface is generally not advised because doing so needlessly increases bandwidth and processor overhead. Determine which routing protocol should be running on each interface and disable the other if necessary.

Table 4-4 Single-Protocol AppleTalk Internetwork (AppleTalk Enhanced IGRP Only)

Possible Problem	Suggested Actions
AppleTalk Enhanced IGRP is not globally configured on the appropriate routers.	**Step 1** Check the configuration of Router B using the **write terminal** privileged EXEC command. Look for an **appletalk routing eigrp** global configuration command entry. This command turns on AppleTalk Enhanced IGRP routing on the router.
	Step 2 If AppleTalk Enhanced IGRP routing is not enabled on Router B, use the **appletalk routing eigrp 200** global configuration command to enable it. The number indicated by the command is the AppleTalk Enhanced IGRP router ID. This number must be unique on the network (although a router can have more than one router ID configured).
	Step 3 Perform the same actions on Router D. The **appletalk routing eigrp** global configuration command must be enabled on all routers that are running AppleTalk Enhanced IGRP. The Router ID must be different for each router.
AppleTalk Enhanced IGRP is not enabled on the appropriate interfaces.	**Step 4** Issue the **write terminal** privileged EXEC command on Router B and examine the interface configurations. In order for an interface to generate AppleTalk Enhanced IGRP routing updates, the **appletalk protocol eigrp** interface configuration command must be present.
	Step 5 In the network shown in Figure 4-11, Router B should have AppleTalk Enhanced IGRP enabled on all of its interfaces. Use the **appletalk protocol eigrp** interface configuration command to tell the interface to begin sending routing updates.
	Step 6 Perform the same actions on Router E. Router E should also have AppleTalk Enhanced IGRP enabled on all of its interfaces.
Route redistribution is not occurring between AppleTalk Enhanced IGRP routers.	**Step 7** Use the **write terminal** privileged EXEC command on Router B to determine if route redistribution is occurring between Router B and Router E. Route redistribution between AppleTalk Enhanced IGRP routers can be disabled using the **no appletalk route-redistribution** global configuration command.
	Step 8 If the **no redistribute eigrp** command is present, re-enable redistribution between Router B and Router E using the **appletalk route-redistribution** global configuration command. If routes are not properly redistributed between the routers, routes known to one router will not appear in the routing tables of others and connectivity between nodes will be lost.
	Step 9 Be certain that the **appletalk route-redistribution** global configuration command is enabled on Router E as well. Otherwise, routes known to Router B will not be advertised to Router E.

Possible Problem	Suggested Actions
Timer value is mismatched.	**Step 10** Issue the **show appletalk eigrp neighbors** EXEC command on Router B. Make sure that all directly connected AppleTalk Enhanced IGRP routers appear in the output.
	Step 11 Examine the Uptime field in the **show appletalk eigrp neighbors** output. A continuously resetting uptime counter indicates that Hello packets from the neighboring router are arriving sporadically. This may be caused by a timer value mismatch or by hardware problems.
	Step 12 Issue the **show interface** EXEC command to determine if the interface and line protocol are up. Look for high numbers in the queue fields and excessive drop counts. If there are many drops, if the queue count is high, or if the interface or line protocol are down, there is probably something wrong with the interface or other hardware. For more information on troubleshooting hardware, see the "Troubleshooting Router Startup Problems" and the "Troubleshooting Serial Line Problems" chapters.
	Step 13 Use the **write terminal** privileged EXEC command on all AppleTalk Enhanced IGRP routers in the network. (In the network shown in Figure 4-11, this includes all of the routers.) Look for **appletalk eigrp-timers** interface configuration command entries. The values configured by this command must be the same for all AppleTalk Enhanced IGRP routers on the network.
	Step 14 If there are routers with conflicting timer values, reconfigure them to bring them into conformance with the rest of the routers on the network. These values can be returned to their defaults with the **no appletalk eigrp-timers** interface configuration command.
RTMP is enabled on AppleTalk Enhanced IGRP-only interfaces.	**Step 15** Use the **write terminal** privileged EXEC command on Router B and Router E to determine whether AppleTalk Enhanced IGRP and RTMP are both enabled on the same interface.
	Step 16 Running both AppleTalk Enhanced IGRP and RTMP on the same interface is generally not advised because doing so needlessly increases bandwidth and processor overhead. Disable RTMP on the router interfaces using the **no appletalk protocol rtmp** interface configuration command.

AppleTalk Connectivity Symptoms

The symptom modules that follow pertain to AppleTalk internetwork problems. Each module is presented as a set of general problems. Symptoms are discussed in the following sections:

- Users Cannot See Zones or Services on Remote Networks
- Services on a Network Not Visible to Other Networks
- Interface Fails to Start AppleTalk
- Some Zones Missing from Chooser
- Services Not Always Available
- Services Visible, but Users Cannot Connect
- Zone List Changes Each Time Chooser Is Opened
- Connections to Services Drop
- Port Seems Stuck in Restarting or Acquiring Mode
- Old Zone Names Still Appear in Chooser
- Routes Not Propagated through AURP Tunnel
- Slow Performance from ARA Dial-In Connection
- ARA Client Unable to Connect to ARA Server
- ARA Connection Hangs after “Communicating At...” Message
- Enhanced IGRP Router Stuck in Active Mode

Users Cannot See Zones or Services on Remote Networks

Symptom: Although users are able to access services on their own network, offnet zones and services expected to be available from the Chooser are not accessible. Table 4-5 outlines a possible cause and suggests actions when access is blocked to offnet zones and network resources.

Table 4-5 AppleTalk: Users Cannot See Zones or Services on Remote Networks

Possible Cause	Suggested Actions
Configuration mismatch	**Step 1** Examine the output of the **show appletalk interface** EXEC command for a "port configuration mismatch" message, which indicates that the configuration disagrees with its listed neighbor.
	Step 2 If the output of the **show appletalk interface** EXEC command does not include the "port configuration mismatch" message, use the **clear interface** privileged EXEC command on the interface in question. If the interface becomes operational after clearing, a configuration mismatch does not exist.
	Step 3 Enter the **show appletalk interface** EXEC command again. If its output still contains a "port configuration mismatch" message, verify that the configuration for each router agrees with respect to network number or cable range and with respect to zone or zone list. In some cases, the configuration shown is not the configuration being used, so if problems persist, set the problem router to get its configuration information from the network. (That is, put the router in discovery mode by specifying the interface configuration command **appletalk address 0.0** on a nonextended network or **appletalk cable-range 0-0** on an extended network.)
	Step 4 If router configurations do not agree, modify them as necessary.
	Step 5 If the problem persists, try to determine which router is at fault. The **show appletalk interface** command displays the network and node address of the conflicting router. If the **appletalk name-lookup-interval** global configuration command is enabled, the **show appletalk interface** command displays the NBP registration name. If you are unable to identify the misconfigured router using the node address, determine the hardware address of the conflicting router with the **show appletalk arp** EXEC command. This command also allows you to determine the vendor code. (An explanation of vendor codes is available in RFC 1340.)
	Step 6 As an alternative, configure all routers but one for discovery mode and restart the routers that are in discovery mode.

Services on a Network Not Visible to Other Networks

Symptom: Users find that the AppleTalk services for a particular network do not appear in their Choosers. Table 4-6 outlines possible causes and suggests actions when services on a network are not visible to other networks.

Table 4-6 AppleTalk: Services Not Visible to Other AppleTalk Networks

Possible Causes	Suggested Actions	
Configuration mismatch	**Step 1**	See Table 4-5 for suggested actions.
Duplicate network numbers	**Step 1**	The network on which AppleTalk services do not appear in the Chooser is likely to be the network that has been assigned the duplicate network number. Change the network number of the affected network or remove AppleTalk from the interface for the affected network. In either case, if the network number persists, you probably have found the duplicate network number. If the network number disappears from the internetwork within a few minutes, you have not found the duplicate.
	Step 2	If you changed the network number on the interface, no further action is required. If not, change it to a unique network number now. Remember to reenter the zone name and any other interface configurations for AppleTalk on that interface.
Phase 1 and Phase 2 rule violations	**Step 1**	Use the **show appletalk globals** EXEC command to determine whether the internetwork is in compatibility mode.
	Step 2	Enable the **appletalk name-lookup-interval** global configuration command and use the **show appletalk neighbors** EXEC command to determine which specific neighbor (by NBP name) is in compatibility mode.
	Step 3	Select one of three solutions: Ensure that all routers are in compliance with the two Phase 1 and Phase 2 rules. Upgrade AppleTalk Phase 1 routers to AppleTalk Phase 2 compliance and reconfigure the internetwork. Use the **appletalk proxy-nbp** global configuration command. To use **appletalk proxy-nbp**, create at least one *virtual* network on the router that has the same zone name as the network where the unreachable services exist. This forces the router to use Phase 1-type NBP lookups (in addition to Phase 2-style Forward Requests) when sending NBP requests through the network. Because the lookup is defined for Phase 1 routers, the Phase 1 router will properly route the request on to the service, and a reply should be received.
Misconfigured access lists	**Step 1**	Disable access lists on suspect routers and see whether connectivity returns.
	Step 2	If connectivity returns, an access list error is the likely suspect. Check access lists and associated configuration commands for errors.
	Step 3	Modify any access lists as necessary.
	Step 4	If connection problems persist, consult with your router technical support representative for more assistance.

Interface Fails to Start AppleTalk

Symptom: Router interface connected to a network will not initialize AppleTalk operation. Table 4-7 outlines possible causes and suggests actions when an AppleTalk interface fails to initialize.

Table 4-7 AppleTalk: Interface Fails to Start AppleTalk

Possible Causes	Suggested Actions
Configuration mismatch	**Step 1** See Table 4-5 for suggested actions.
Phase 1 and Phase 2 rule violations	**Step 1** See Table 4-6 for suggested actions.

Some Zones Missing from Chooser

Symptom: Users on different networks report that zones associated with a particular network do not appear in their Choosers. Table 4-8 outlines possible causes and suggests actions for zones not appearing in the Chooser on networks that are connected by a router.

Table 4-8 AppleTalk: Zones Not Appearing in Chooser

Possible Causes	Suggested Actions
Configuration mismatch	**Step 1** See Table 4-5 for suggested actions.
ZIP storm	**Step 1** Use the **show appletalk traffic** command to look for the number of ZIP requests. Note the number and repeat the **show appletalk traffic** command after about 30 seconds. **Step 2** Compare the two numbers. If the number of ZIP requests is greater than 10 and is increasing, a ZIP storm is probably occurring. **Step 3** Use the **show appletalk route** EXEC command to see whether a network shows up in the table, even though the display indicates that no zone is set. If you find a network for which no zone is set, a node on that network is probably not responding to ZIP requests, resulting in the ZIP storm. **Step 4** Determine why the node is not responding to ZIP requests. **Step 5** ZIP storms may result from a defect in the software running on the node. Contact the vendor to determine whether there is a known problem.
Misconfigured access lists	**Step 1** See Table 4-6 for suggested actions.
Unstable routes	**Step 1** Use the **show interfaces** EXEC command to check traffic load. You may need to segment the network further to limit traffic on interfaces with a load that is greater than 50 percent. **Step 2** Use the **debug apple events** privileged EXEC command to determine whether routes are being aged incorrectly. **Step 3** Use the **appletalk timers** global configuration command to correct the problem. Suggested parameter values for the command are 10, 30, and 90 to start, but do not exceed 10, 40, and 120. The first number must always be 10, and the third value should be three times the second. NOTE: You can return the timers to their defaults (10, 20, 60) by using the **no appletalk timers** global configuration command. Timers should be consistently set to the *same value* throughout the internetwork, or at a minimum, throughout the backbone of the internetwork. This type of problem often can be alleviated by simply segmenting the network to limit the number of routers on a segment.
Too many zones in internetwork	**Step 1** If the Macintosh is running a version of System 6, upgrade it to the most recent version of System 7. The Chooser in System 6 could only display a limited number of zones, which presents problems in large internetworks that have many zones.

Services Not Always Available

Symptom: Users report that services are intermittently unavailable. Services come and go without warning. Table 4-9 outlines possible causes and suggests actions for intermittent loss of AppleTalk services.

Table 4-9 AppleTalk: Services Not Always Available

Possible Causes	Suggested Actions
Duplicate network numbers	**Step 1** See Table 4-6 for suggested actions.
ZIP storm	**Step 1** See Table 4-8 for suggested actions.
Unstable routes	**Step 1** See Table 4-8 for suggested actions.
Overloaded network, where routes are being aged out	**Step 1** Use the **show interfaces** EXEC command to check traffic load. **Step 2** For interfaces with more than a 50 percent load, you may need to segment the network further to limit traffic. **Step 3** Use the **debug apple events** privileged EXEC command to determine whether routes are being aged incorrectly. Then use the **appletalk timers** global configuration command to correct the problem. Timers should be consistently set to the *same value* throughout the internetwork, or at a minimum, throughout the backbone of the internetwork.

Services Visible, but Users Cannot Connect

Symptom: Users report that AppleTalk services appear in their Choosers, but they are unable to access the services. Table 4-10 outlines possible causes and suggests actions when services appear in the Chooser but are not accessible.

Table 4-10 AppleTalk: Services Visible but Users Cannot Connect

Possible Causes	Suggested Actions
Duplicate network numbers	**Step 1** See Table 4-6 for suggested actions.
ZIP storm	**Step 1** See Table 4-8 for suggested actions.
Misconfigured access lists	**Step 1** See Table 4-6 for suggested actions.

Zone List Changes Each Time Chooser Is Opened

Symptom: Users report that whenever they open the Chooser, the zone list appears to change. Table 4-11 outlines possible causes and suggests actions when zones change whenever the Chooser is opened.

Table 4-11 AppleTalk: Zone List Constantly Changing

Possible Causes	Suggested Actions
Unstable routes	**Step 1** See Table 4-8 for suggested actions.
Routers on the network have different zone lists.	**Step 1** Verify that all router configurations agree on zone lists. **Step 2** If the router configurations do not agree, reconfigure the routers so that their zone lists match for relevant networks.

Connections to Services Drop

Symptom: Users complain that their sessions with AppleTalk services suddenly drop for no apparent reason. Table 4-12 outlines a possible cause and a suggests an action when AppleTalk network services are unexpectedly lost.

Table 4-12 AppleTalk: Services Drop Unexpectedly

Possible Cause	Suggested Actions
Unstable routes	**Step 1** See Table 4-8 for suggested actions.

Port Seems Stuck in Restarting or Acquiring Mode

Symptom: A router is unable to discover routes or to poll neighbors on an attached cable. Table 4-13 outlines possible causes and suggests actions for a router port stuck in restarting or acquiring mode.

Table 4-13 AppleTalk: Port Stuck in Restarting or Acquiring Mode

Possible Causes	Suggested Actions	
Crossed serial circuits with multiple lines between two routers.	**Step 1**	Check physical attachment of serial lines to ensure that they are correctly wired.
	Step 2	If needed, rewire and use the output of the **show interfaces** and **show appletalk interface** commands to confirm that the interface and line protocol are up.
	Step 3	If the router is still unable to find routes, consult your router technical support representative for more assistance.
Router is in discovery mode, and no seed router exists on the network.	**Step 1**	Put the router in nondiscovery mode.
	Step 2	Use the **appletalk address** or **appletalk cable-range** interface configuration command to assign a network number or cable range.
	Step 3	If the router is still unable to find routes, consult your router technical support representative for more assistance.
Conflicting zone lists	**Step 1**	Issue the **show appletalk route** EXEC command. Look for neighboring nodes that have the same cable-range but a different zone list.
	Step 2	Bring the zone lists into agreement.
Software problem	**Step 1**	If the router issues a message that says “restart port pending,” upgrade to the latest system software maintenance release or contact your router technical support representative.

Old Zone Names Still Appear in Chooser

Symptom: Users report that they are seeing zones that were deleted from the network.
Table 4-14 outlines possible causes and suggests actions when old AppleTalk zones continue to appear in the Chooser.

Table 4-14 AppleTalk: Old Zone Names Appear in Chooser

Possible Causes	Suggested Actions
Configuration mismatch	**Step 1** See Table 4-5 for suggested actions.
Invalid zone names in the routing tables	**Step 1** Check the network numbers for each AppleTalk interface in the router configuration. **Step 2** Remove any network number that is associated with an old zone name. **Step 3** Use the **show appletalk zones** command to verify that the ghost zone no longer appears in the list.

Note AppleTalk does not provide a way to update ZIP tables when changing the mapping of zone names to networks/cable ranges. For example, if the zone name for network number 200 is *Twilight Zone*, but you decide to change the zone to *No Parking Zone*, the zone name on the interface can be changed, and the new zone name takes effect locally. However, unless you keep network 200 off the internetwork long enough for it to be completely aged out of the routing tables, some routers will continue to use the old zone name (called *ghost zones*). Alternatively, if you cannot keep the network off the internetwork that long, change the underlying network number when you change the zone name of a cable.

Routes Not Propagated through AURP Tunnel

Symptom: AppleTalk routes are not propagated through an AURP tunnel. Routes that are known to exist on one side of the tunnel do not appear in the routing tables of the exterior router on the other side of the tunnel. Table 4-15 shows a possible cause and suggests actions for routes not being propagated through an AURP tunnel.

Table 4-15 AppleTalk: Routes Not Propagated through AURP Tunnel

Possible Cause	Suggested Actions
Routes are not redistributed between AURP and RTMP.	**Step 1** Use the **show appletalk interface** EXEC command to verify that the interfaces on the AURP exterior routers are in the up state. **Step 2** If the tunnel interfaces on the exterior routers are properly connected to the network and are operational, but AppleTalk routes remain invisible on one side of the AURP tunnel, issue the **debug apple redistribution** privileged EXEC command to help determine whether routes are being redistributed among routing protocols. **Step 3** Issue the **appletalk route-redistribution** global configuration command on any AURP tunnel interfaces. This command specifies that routing information be redistributed among Apple routing protocols. The output from the **debug apple redistribution** command will indicate that routes are now being redistributed among routing protocols.

Slow Performance from ARA Dial-In Connection

Symptom: Remote dial-in ARA sessions exhibit slow performance. Table 4-16 describes a possible cause and suggests actions when performance is slow over an ARA connection.

Table 4-16 AppleTalk: Slow Performance from ARA Dial-In Connection

Possible Cause	Suggested Actions
Flow control is not enabled, is enabled only on one device (either DTE or DCE), or is misconfigured.	**Step 1** Configure hardware flow control on the line using the **flowcontrol hardware** line configuration command. Cisco recommends configuring hardware flow control for access server-to-modem connections. NOTE: If for some reason you are unable to use flow control, it is recommended that you limit the line speed to 9600 bps. Faster speeds will likely result in lost data. **Step 2** After enabling hardware flow control on the access server or router line, initiate a reverse Telnet session to the modem via that line. For more information, see the section "Initiating a Reverse Telnet Session to a Modem," in the "Troubleshooting Serial Line Problems" chapter. **Step 3** Issue a modem command string that includes the RTS/CTS Flow command for your modem. This command ensures that the modem is using the same method of flow control (that is, hardware flow control) as the Cisco access server or router. See your modem documentation for exact configuration command syntax. For more information see the section "Troubleshooting Access Server to Modem Connectivity" in the "Troubleshooting Serial Line Problems" chapter.

ARA Client Unable to Connect to ARA Server

Symptom: ARA client (such as a Macintosh) attempts to connect to an ARA server (such as a Cisco access server) and is unable to initiate a remote session. User may be able to connect briefly but the connection is immediately terminated. Table 4-17 describes possible causes and suggests actions when an ARA client is unable to connect to an ARA server.

Table 4-17 AppleTalk: ARA Client Unable to Connect to ARA Server

Possible Causes	Suggested Actions
Missing **arap network** command entry	**Step 1** If you are running Cisco Internetwork Operating System (Cisco IOS) Release 10.2 or later on a Cisco access server, configure the **arap network** global configuration command to run ARA. **Step 2** Issue the **write terminal** privileged EXEC command to be certain that the command is configured.
AppleTalk routing is not enabled on the appropriate access server or router interface	**Step 1** Issue the **show apple interfaces** EXEC command to determine if the interfaces are operational and whether AppleTalk routing is enabled on the correct interfaces. **Step 2** If AppleTalk routing is not enabled on the proper interfaces, refer to the *Router Products Configuration Guide* for detailed information on configuring an interface for AppleTalk routing.
Modem, serial line, or hardware problems	**Step 1** For modem and serial line troubleshooting information, see the “Troubleshooting Serial Line Problems” chapter. For hardware troubleshooting information, see the “Troubleshooting Router Startup Problems” chapter.

ARA Connection Hangs after “Communicating At...” Message

Symptom: ARA client (for example, a Macintosh) tries to connect to an ARA server (such as a Cisco access server) over client and server modems. The client receives a connect message such as “Communicating at 14.4 Kbps,” but then hangs for 10–30 seconds, and finally shows a “connection failed” message. Table 4-18 shows a possible cause and suggests actions for a modem connection hanging after issuing a “communicating at...” message.

Table 4-18 AppleTalk: ARA Connection Hangs after Issuing “Communicating At...” Message

Possible Cause	Suggested Actions
MNP4 Link Request packets sent by ARA stack in client are being responded to by the serving modem instead of the ARA server	**Step 1** Check the version numbers of the ARA software on the client and the Cisco IOS software on the access server. If you are using ARA version 1.0 and Cisco IOS Release 10.2 or earlier, it is advisable to upgrade to ARA 2.0 and Cisco IOS Release 10.2 or later. ARA 2.0 modifies the framing of MNP4 Link Request packets, allowing them to be passed to the access server rather than responded to by the serving modem. **Step 2** If it is not possible to upgrade your software, try modifying the behavior of the modem to use a LAPM-to-No Error Correction fallback instead of a LAPM-to-MNP4-to-No Error Correction fallback. The modem will no longer listen for and respond to MNP4 messages, allowing MNP4 packets to reach the access server. NOTE: Many modems cannot be configured in this manner. **Step 3** If your modem does not use LAPM error correction, it might be possible to modify *all* ARA client scripts to extend the 500 ms (millisecond) pause before exiting. Configure an additional delay that takes into account the behavior of the *serving* modem.

Enhanced IGRP Router Stuck in Active Mode

Symptom: An AppleTalk Enhanced IGRP router is stuck in Active mode. An Enhanced IGRP router can be in either Passive or Active mode. A router is said to be Passive for Network A when it has an established path to Network A in its routing table.

If the Enhanced IGRP router loses the connection to Network A, it becomes Active for that network. The router sends out queries to all of its neighbors in order to find a new route to Network A. The router remains in Active mode until it has either received replies from *all* of its neighbors or until the active timer, which determines the maximum period of time a router will stay Active, has expired.

If the router receives a reply from each of its neighbors, it computes the new next hop to Network A and becomes Passive for that network. However, if the active timer expires, the router removes from its neighbor table any neighbors that did not reply, again enters Active mode, and issues a "Stuck-in-Active" message to the console:

```
%DUAL-3-SIA: Route 2.24 Stuck-in-Active
```

Note It is essential to note that the occasional appearance of these messages is *not* cause for concern. This is simply the manner in which an Enhanced IGRP router recovers if it does not receive replies to its queries from all of its neighbors. However, if these error messages occur frequently, the problem should be investigated.

Table 4-19 describes possible causes and suggests actions when an AppleTalk Enhanced IGRP router is stuck in Active mode.

Table 4-19 AppleTalk: Enhanced IGRP Router Stuck in Active Mode

Possible Causes	Suggested Actions
Active timer value is misconfigured	**Step 1** The active timer determines the maximum period of time that an Enhanced IGRP router will wait for replies to its queries. If the active timer value is set too low, there might not be enough time for all of the neighboring routers to send their replies to the Active router.
	Step 2 Check the configuration of each Enhanced IGRP router using the **write terminal** privileged EXEC command. Look for the **timers active-time** router configuration command associated with the **appletalk routing eigrp** global configuration command.
	Step 3 The value set by the **timers active-time** command should be consistent among routers. Cisco strongly recommends configuring a value of 3 (3 minutes, which is the default value) to allow all Enhanced IGRP neighbors to reply to queries.

Possible Causes	Suggested Actions
Interface or other hardware problem	**Step 1** If queries and replies are not sent and received properly, the active timer will time out and cause the router to issue an error message. Issue the **show appletalk eigrp neighbors** EXEC command and examine the Uptime and Q Cnt (queue count) fields in the output. If the uptime counter is continually resetting or if the queue count is consistently high, there might be a problem with hardware. **Step 2** Determine where the problem is occurring by looking at the output of the stuck in Active error message, which will indicate the AppleTalk address of the problematic node. **Step 3** Make sure the suspect router is still functional. Check the interfaces on the suspect router. Make sure the interface and line protocol are up and determine whether the interface is dropping packets. For more information on troubleshooting hardware, see the "Troubleshooting Router Startup Problems" and the "Troubleshooting Serial Line Problems" chapters. **Step 4** Make sure the suspect router has not had its configuration changed in a manner that could effect the convergence of the Enhanced IGRP routing protocol. Static routes, for example, can cause problems. **Step 5** Try jumpstarting the Enhanced IGRP router using the **clear appletalk eigrp neighbors** privileged EXEC command. This causes the router to clear its neighbor table, enter Active mode, and attempt to reacquire its neighbor information.
Flapping route	**Step 1** If there is a flapping serial route (caused by heavy traffic load), queries and replies might not be forwarded reliably. Route flapping caused by heavy traffic on a serial link can cause queries and replies to be lost, resulting in the active timer timing out. **Step 2** Take steps to increase the bandwidth of the link.

CHAPTER 5

Troubleshooting Banyan VINES Connectivity

This chapter presents protocol-related troubleshooting information for connectivity problems related to Banyan's Virtual Integrated Network Service (VINES). This chapter consists of Banyan VINES symptom modules. Each symptom module consists of the following sections:

- Symptom statement—A specific symptom associated with Banyan VINES connectivity.
- Possible causes and suggested actions—A table for each symptom containing possible causes for the symptom and suggested actions for resolving each cause.

Banyan VINES Connectivity Symptoms

The symptom modules that follow pertain to Banyan VINES internetwork problems. The symptoms are discussed in the following sections:

- Clients Cannot Communicate with Banyan VINES Servers over Routers
- Clients Cannot Connect to Server over Packet-Switched Network
- Serverless Client Cannot Connect to Server over Packet-Switched Network

Clients Cannot Communicate with Banyan VINES Servers over Routers

Symptom: Clients might not be able to connect to servers on their directly connected networks. In either case, connections cannot be made to servers on the other side of the router. Table 5-1 outlines possible causes and suggested actions when clients cannot communicate with VINES servers over a router.

Table 5-1 VINES: Clients Cannot Communicate with VINES Servers over Router

Possible Cause	Suggested Actions
Clients or servers not attached to the network	**Step 1** Connect both clients and servers to the same network and verify that they can communicate. **Step 2** If they cannot communicate, check the configuration of the client and server. Refer to host software documentation for troubleshooting information. **Step 3** Attach a network analyzer to the network to which clients and servers are temporarily connected. Look for the source addresses of both. **Step 4** If you find the source addresses, the clients and servers are operating properly. If you do not find their addresses, check the configuration of the clients and servers. (Consult your client and server documentation for more information.)
Router interface not functioning	**Step 1** Use the **show interfaces** EXEC command to check the operation of the router. **Step 2** If the status line indicates that the interface is "administratively down," specify the **no shutdown** interface configuration command on the interface. **Step 3** If the status line indicates that the interface or protocol is "down," check cable connections from the router. If necessary, replace the cable. **Step 4** If, after replacing the cable, the **show interfaces** EXEC command still does not indicate that the interface and line protocol are "up," contact your router technical support representative.
VINES metric value not specified	**Step 1** Use the **show vines interface** EXEC command to check the operation of the router. Look for an interface that has the **vines metric** interface configuration command, which enables VINES processing on the interface. **Step 2** If the **vines metric** interface configuration command is not specified for the interface, specify that command for the interface.
Missing **vines serverless** or **vines arp-enable** commands	**Step 1** Use the **show vines interface** EXEC command or the **write terminal** command to check the operation of the router. A network that does not have a server must be configured with the **vines serverless** and **vines arp-enable** router configuration commands. **Step 2** If the **vines serverless** and **vines arp-enable** commands are not specified for this interface, specify those commands for this interface.

Possible Cause	Suggested Actions
Misconfigured access list	**Step 1** Remove the specification of any **vines access-group** commands on all relevant interfaces. **Step 2** Test the connection from the client to the target server to see whether traffic can get through. If the connection works, the access list needs modification. **Step 3** To isolate the bad access list specification, apply one access list statement at a time until you can no longer create connections. **Step 4** Make sure that access lists are applied to the correct interface. Normally, traffic filters are applied to *outgoing* interfaces.
Nonfunctional FDDI ring	**Step 1** Use the **show interfaces fddi** EXEC command to determine the status of the interface. **Step 2** If the output of the **show interfaces fddi** EXEC command indicates that the interface and line protocol are up, use the **ping vines** privileged EXEC command to test connectivity between routers. **Step 3** If the interface and line protocol are up, verify that the Media Access Control (MAC) addresses of upstream and downstream neighbors are as expected. If all zeros appear in either of the address fields for these neighbors, a physical connection problem is likely. **Step 4** In this case (or if status line does *not* indicate that the interface and line protocol are up), check patch-panel connections and check connectivity between routers using an optical time domain reflectometer (TDR) or light meter. Ensure that signal strength is within specification.
Nonfunctional serial link	**Step 1** Use the **show interfaces serial** command to determine the status of interface. **Step 2** If the **show interfaces serial** command indicates that the interface and line protocol are up, use the **ping vines** command to test connectivity between routers. **Step 3** If routers do not respond to the ping test, follow the troubleshooting techniques discussed in Chapter 3, “Troubleshooting Serial Line Problems.”
Nonfunctional Ethernet backbone	**Step 1** Use the **show interfaces ethernet** command to determine the status of the interface. **Step 2** If the status line does not indicate that the interface and line protocol are up, check the physical attachment of the router to the Ethernet backbone. **Step 3** If the **show interfaces ethernet** command indicates that the interface and line protocol are up, use the **ping vines** command to test connectivity between routers. **Step 4** Obtain analyzer traces and look for packets from target servers, clients, and routers. **Step 5** Any nodes that do not appear as expected are potential problem nodes. Determine whether the node and its cables are functional. If not, replace or reconfigure as needed.

Possible Cause	Suggested Actions
Nonfunctional Token Ring backbone	**Step 1** Use the **show interfaces token** command to determine the status of the interface. **Step 2** If the status line indicates that the interface and line protocol are not up, check the cable from the router to the multistation access unit (MAU). Make sure that the cable is good; replace the cable if necessary. **Step 3** If the **show interfaces token** command indicates that the interface and line protocol are up, use the **ping vines** command to test connectivity between routers. **Step 4** If the remote router does not respond, check the ring specification on all nodes attached to the Token Ring backbone. All of the nodes must have the same ring speed. If necessary, modify ring speed specifications for clients, servers, and routers. **Step 5** Use the **ring-speed** interface configuration command to modify the ring speed for Token Ring cards that support software speed configuration. Change jumpers as needed for modular router platforms. For more information about ring speed specification, refer to the hardware installation and maintenance manual for your system.
Mismatched MAC-level encapsulation methods in broadcast	**Step 1** Check the encapsulation type of each VINES interface. **Step 2** Compare the encapsulation type with the encapsulation type assigned on the router. Modify the router configuration as necessary. The **vines encapsulation** command only affects broadcasts from the router. The router keeps track of which encapsulation is used by each of its neighbors and uses that encapsulation type when it talks directly to a neighbor.

Clients Cannot Connect to Server over Packet-Switched Network

Symptom: Local servers are responding, but servers on the other side of a packet-switched network that interconnects routers do not respond. A router *appears* to block VINES over the packet-switched network. Table 5-2 outlines possible causes and suggested actions when clients cannot connect to VINES servers over a packet-switched network.

Table 5-2 VINES: Clients Cannot Connect to VINES Server over PSN

Possible Cause	Suggested Actions
X.25 address mapping error	**Step 1** Use the **write terminal** EXEC command to examine the configuration of the router. **Step 2** Make sure that the MAC addresses and X.121 addresses specified in any **x25 map vines** interface configuration commands match the addresses associated with the respective destination routers.
Permanent virtual circuit not set up	**Step 1** Use the **write terminal** EXEC command to examine the configuration of the router. **Step 2** Make sure that an **x25 pvc** *n* **vines** *address* interface configuration command sets up a permanent virtual circuit (PVC) between the two routers.

Serverless Client Cannot Connect to Server over Packet-Switched Network

Symptom: Servers on the other side of a packet-switched network that interconnects routers do not respond. A router *appears* to block VINES over the packet-switched network. Table 5-3 outlines possible causes and suggested actions when a serverless client cannot connect to a server over a packet-switched network.

Table 5-3 VINES: Serverless Client Cannot Connect to VINES Server over PSN

Possible Cause	Suggested Actions
X.25 address mapping error	**Step 1** See Table 5-2 for suggested actions.
PVC not set up	**Step 1** See Table 5-2 for suggested actions.
VINES broadcasts not sent over packet-switched network	**Step 1** Use the **write terminal** command to examine the configuration of the router. **Step 2** Make sure that the **vines propagate** interface configuration command is configured on the serial interface of the router that is providing the serverless packet switched node service.

CHAPTER 6

Troubleshooting Bridging Connectivity

This chapter presents troubleshooting information for connectivity problems in bridged internetworks. The emphasis here is on symptoms and problems encountered in internetworks featuring transparent bridging, internetworks transitioning from bridging to routing, and internetworks composed of bridging and routing nodes.

Note Problems associated with source-route bridging (SRB), translational bridging, and source-route transparent (SRT) bridging are addressed in the "Troubleshooting IBM Connectivity" chapter.

This chapter consists of the following sections:

- Transparent Bridging Connectivity Scenario
- Creating Network Maps
- Bridge-Based Connectivity Symptoms

The section on bridge-based connectivity symptoms consists of the following:

- Symptom statement—A specific symptom associated with the bridge connectivity
- Possible causes and suggested actions—A table for each symptom containing possible causes for the symptom and suggested actions for resolving each cause

Transparent Bridging Connectivity Scenario

Bridge-based internetworks often encounter problems associated with packet looping and conflicts between transparent bridges. The following scenario explores some common problems that can lead to these kinds of connectivity problems in environments that feature transparent bridging over parallel paths.

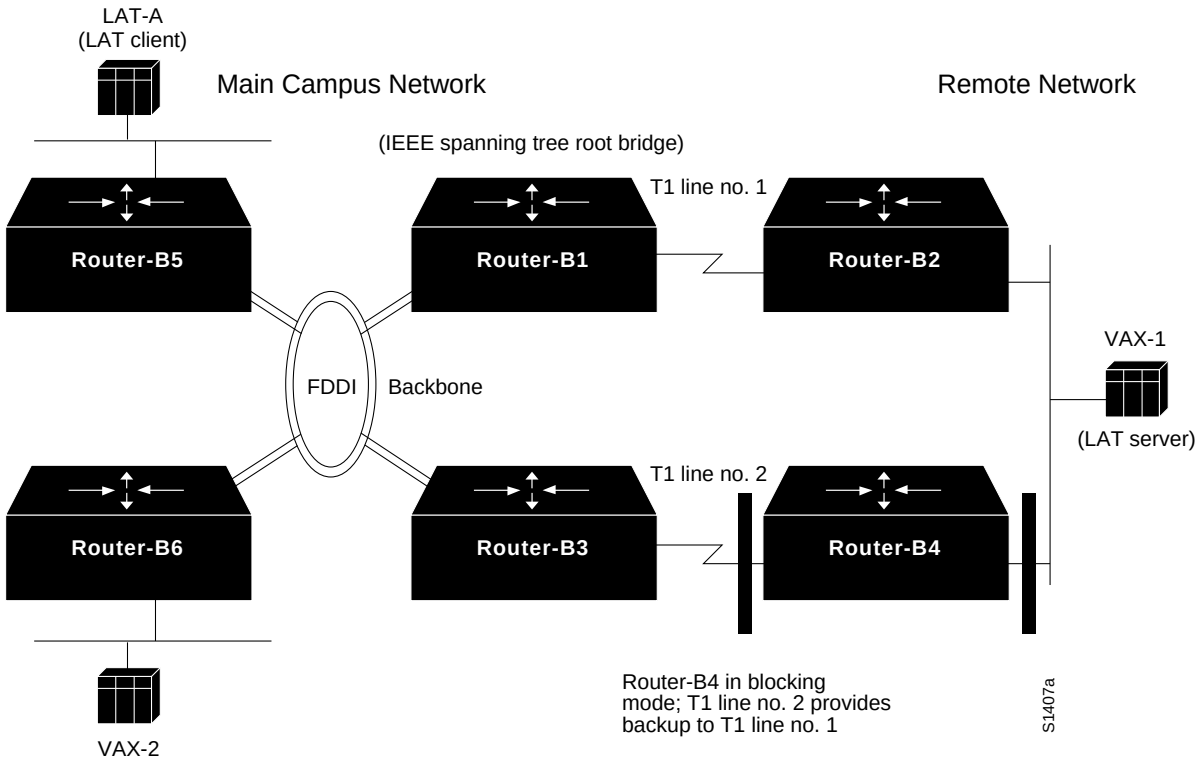
In this scenario, problems and symptoms that afflict a stable internetwork over a period of time are discussed sequentially. The scenario is split into two parts:

- Scenario Part 1: Problems associated with "spanning tree wars" resulting in no connectivity on the entire internetwork
- Scenario Part 2: Problems associated with packet looping and broadcast storms, resulting in excessively high traffic on the internetwork, extremely poor network performance, and, ultimately, blocked communications

These two parts are discussed separately. The “Problem Solution Summary” section provided at the end of the scenario addresses both parts.

Figure 6-1 illustrates the basic stable network map for this environment. Assume in this network that all the bridges are configured to use the IEEE spanning tree algorithm and that under normal conditions, T1 Line number 2 is a backup link with Router-B4 in blocking mode. Bridged traffic between the main campus network and the remote network passes over T1 line number 1.

Figure 6-1 Stable Transparent Bridging Scenario Network Map



Scenario Part 1: Symptoms

After a prolonged period of normal operation, assume that all connectivity on this internetwork suddenly stops. Users are unable to access any network resources, even on the same segment.

Scenario Part 1: Environment Description

The relevant elements of the internetworking environment shown in Figure 6-1 can be summarized as follows:

- LANs are Ethernet-based; the Main Campus Network is interconnected over an FDDI backbone, and the serial link to Remote Network is a dedicated T1 link (1.544 Mbps). A second T1 link provides a backup path.
- DECnet is being routed between various VAX hosts; traffic consists of file transfers.
- Local area transport (LAT) connection service is provided to a communication server (LAT-A) from a LAT server (VAX-1). LAT is bridged.

- All internetworking nodes in this environment are Cisco devices.
- All connected bridges are required to run the IEEE spanning tree algorithm.
- Bridging node Router-B1 is the spanning tree root bridge by administrative specification.

Diagnosing and Isolating Part 1 Problem Causes

In this situation, three problems might explain these connectivity symptoms:

- Unstable media (connected to root bridge)
- Unstable internetworking hardware (connected to root bridge)
- Excessive traffic

In general, it is useful to eliminate the most likely problems first, and then tackle more complex problems as necessary. The problem-solving process that follows illustrates this strategy.

After you identify a possible problem list, you must analyze each potential cause until connectivity is restored. The following discussion considers the list of problems and illustrates resolution of discovered problems.

Eliminating Excessive Traffic as the Problem

In this case, up until the network failure, traffic was normal. That is, users were able to make connections and despite occasionally slow service, complaints were minimal. A sign that excessive traffic might be a problem would be consistently degraded service, chronically slow host response, and dropped connections.

To determine whether excessive traffic has been occurring, use the **show interfaces** command; look for output drops and collisions on Ethernets, or high 5-minute input and output rates and full input and output queues on serial interfaces.

If these underlying symptoms do not appear, you can eliminate excess traffic as the problem.

Diagnosing Unstable Media and Hardware

After eliminating congestion as the problem, the most likely cause is some kind of hardware problem associated with the root bridge or other hardware attached to the root. These problems can result in a spanning tree war as bridges attempt to assert themselves as the root bridge every time a suspect device or bad link causes the root bridge to reset an interface. Diagnose this kind of problem using the steps that follow.

Step 1 Use the **show interfaces** EXEC command and examine the output for transition and reset counters at the root bridge or at an internetworking device connected to the root bridge. Figure 6-2 illustrates an example display indicating that these counters are incrementing.

Figure 6-2 Output of the show interfaces Command Illustrating Resets and Transitions

Example illustrating interface resets and transitions

```
Serial 0 is up, line protocol is up
  Hardware is MCI Serial
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 0:00:00, output 0:00:00, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 1676000 bits/sec, 1258 packets/sec
  Five minute output rate 1547000 bits/sec, 1150 packets/sec
     22294913 packets input, 1512306928 bytes, 0 no buffer
     Received 72958 broadcasts, 0 runs, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     18437782 packets output, 1232397733 bytes, 0 underruns
     0 output errors, 0 collisions, 22 interface resets, 0 restarts
     22 carrier transitions
```

S2507

Problems that can cause transition and reset counters to increment include bad modems, bad modem cables, noisy lines, unreliable LAN media, or bad appliques at the bridges.

For information about troubleshooting LAN media in general, refer to Chapter 1, "Troubleshooting Overview." For more information about troubleshooting hardware, refer to Chapter 2, "Troubleshooting Router Startup Problems." For more information about troubleshooting serial lines, refer to Chapter 3, "Troubleshooting Serial Line Problems."

Step 2 After you isolate a hardware problem, replace suspected devices or cables with known working devices or cables.

Step 3 Use the **clear counters** command at bridges attached to the problem hardware; then use the **show interfaces** command again to determine whether the carrier transition and reset counters have stopped incrementing. Determine whether connectivity has been restored.

In this case, assume that connectivity is restored. Now, consider the problems discussed in Part 2 of this scenario.

Scenario Part 2: Symptoms

As discussed previously, Figure 6-1 illustrates a stable bridging network. After resolving Part 1, connectivity is reestablished and normal internetwork operations are restored. However, after a period of uninterrupted service, network managers notice that internetwork performance has again declined following increased instances of broadcast storms.

Scenario Part 2: Environment Description

The relevant elements of the internetworking environment are the same as in Part 1. One note regarding this environment is that the network managers had been making modifications to the internetwork and reconfiguring the internetworking devices when symptoms started to occur.

Diagnosing and Isolating Part 2 Problem Causes

Given the situation, there are two likely problems that can explain these connectivity symptoms:

- Mixed spanning tree environment
- Multiple bridging domains

Diagnosis for these identified possible problems follows.

Diagnosing Mixed Spanning Tree Algorithm Problems

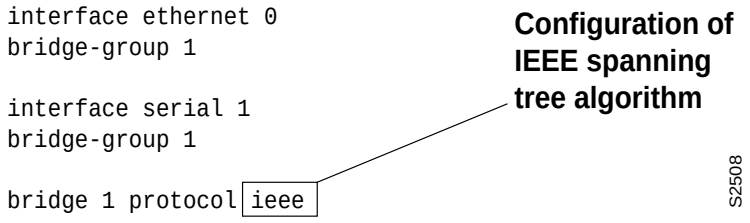
Problems can arise for internetworks in which both IEEE and DEC spanning tree algorithms are used by bridging nodes. These problems are caused by differences in the way the bridging nodes handle spanning tree bridge protocol data unit (BPDU) packets (or hello packets) and in the way they handle data. The following procedure shows you how to determine whether both spanning tree algorithms are running:

Step 1 Use the **show interfaces** EXEC command to obtain input and output packet count statistics. If these counters increment at an abnormally high rate (with respect to your normal traffic loads), a loop is likely.

Step 2 Use the **show span** EXEC command on Cisco bridges to determine whether multiple root bridges exist and to determine which spanning tree protocols are being used.

Step 3 If both DEC and IEEE appear, reconfigure bridges so that all use the same spanning tree protocol version. Use the **bridge** *group* **protocol ieee** global configuration command to make this change. Figure 6-3 illustrates the use of this command, as well as other required commands.

Figure 6-3 Configuration of IEEE Spanning Tree Algorithm

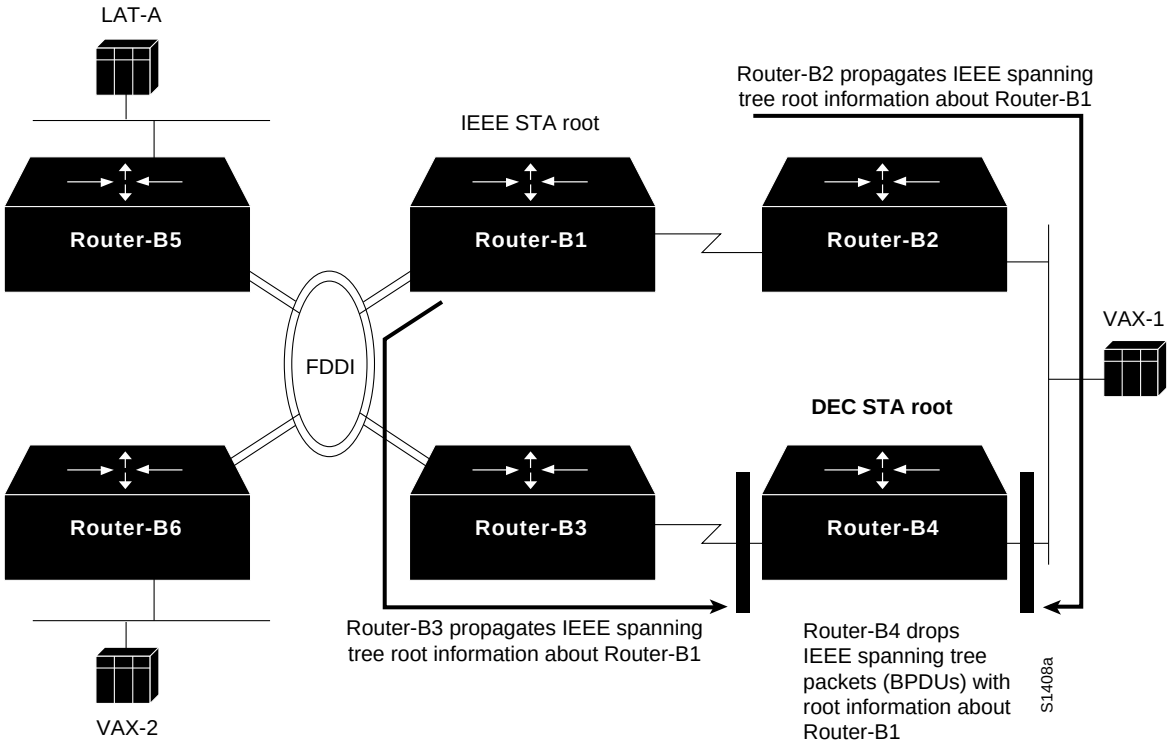


In this scenario, Router-B1, Router-B2, and Router-B3 are found to be running the IEEE spanning tree algorithm, while Router-B4 is inadvertently misconfigured to use the DEC spanning tree version. To resolve this problem, Router-B4 is reconfigured for IEEE. Figure 6-3 illustrates how to configure the IEEE spanning tree algorithm.

The effect of implementing the mixed spanning tree environment in this configuration is outlined in the following discussion and illustrated in Figure 6-4 through Figure 6-6.

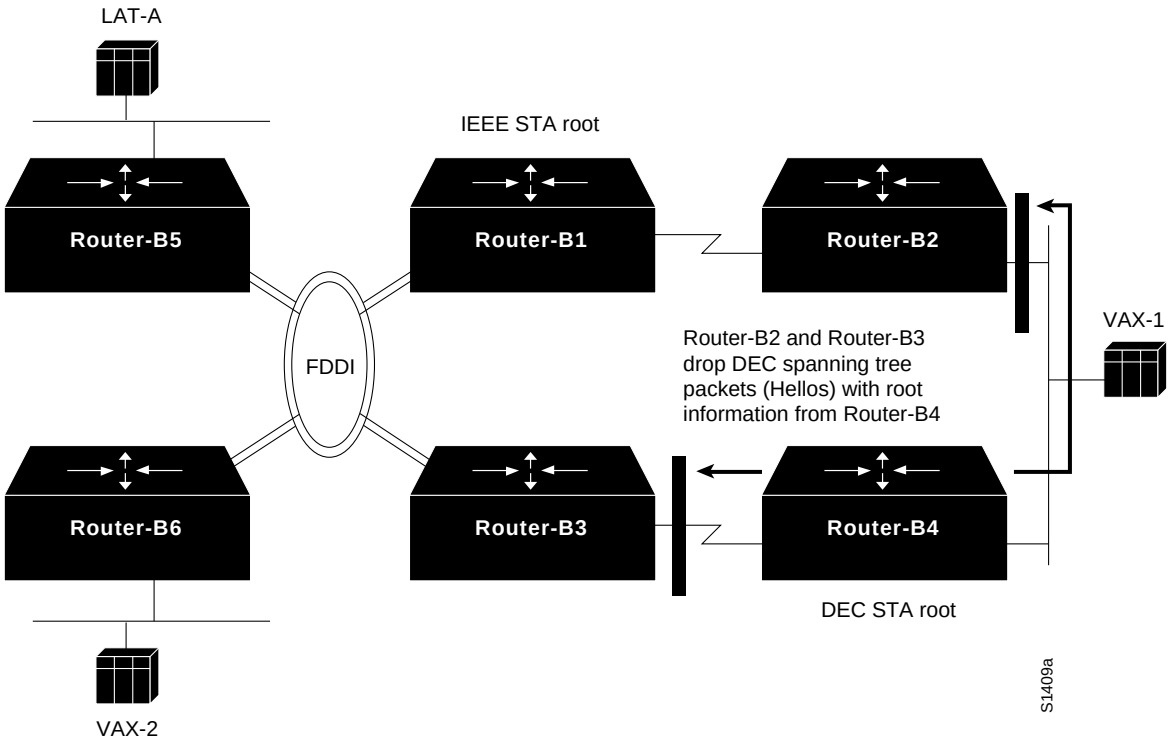
- Router-B1 claims to be the IEEE root, while Router-B4 claims to be the DEC root.
- Router-B2 and Router-B3 propagate root information on all interfaces for IEEE spanning tree, indicating that Router-B1 is the root. However, Router-B4 drops IEEE spanning tree information regarding IEEE root Router-B1, as shown by Figure 6-4.

Figure 6-4 Router-B4 Drops IEEE Root Information Propagated by Router-B2 and Router-B3



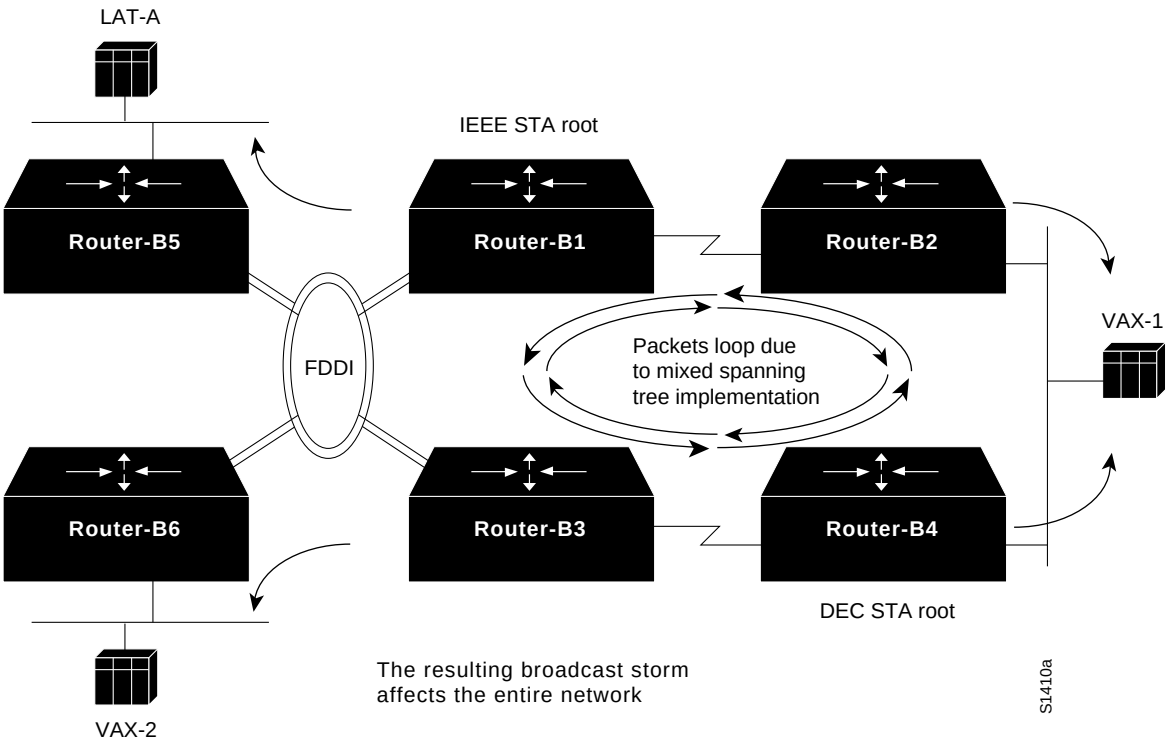
- Meanwhile, Router-B2 and Router-B3 similarly drop DEC root information relayed from Router-B4. (See Figure 6-5.)

Figure 6-5 Router-B2 and Router-B3 Drop DEC Root Information from Router-B4



- The result is that none of the bridges in this internetwork believe that there is a loop. When a broadcast packet is sent on the network, a “broadcast storm” results over the entire internetwork (including the FDDI backbone and other networks attached via Router-B5 and Router-B6), as shown by Figure 6-6.

Figure 6-6 Mixed Spanning Tree Implementation Results in Packet Looping



Although a configuration change is necessary here, it might not be sufficient to reestablish connectivity. Assume that in this case, connectivity is not restored, even when all bridging nodes are reconfigured to use the same spanning tree algorithm.

Diagnosing Multiple Domain Problems

Another configuration problem that results in packet looping is the inappropriate use of the spanning tree "domain" capability of Cisco bridges. The following procedure outlines how to determine whether multiple domains are specified and how to resolve the problem:

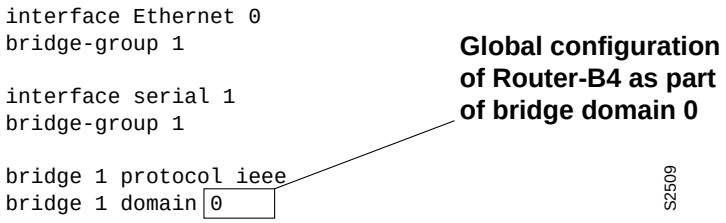
Step 1 Use the **show span** EXEC command on Cisco bridges to determine whether multiple root bridges exist and to ensure that all domain group numbers match for given bridging domains. The key here is that only one path can exist between different bridging domains because bridges in different domains do not exchange spanning tree information.

In this case, assume that Router-B4 was incorrectly specified as belonging to bridge domain number 2, while all other routers are specified to be in the default domain (bridge domain number 0).

Step 2 Change the configurations so that the domain specifications match using the **bridge** *group* **domain** *domain-number* global configuration command. In this case, Router-B4 is changed to bridge domain number 0.

Figure 6-7 illustrates the use of this command, as well as other required commands.

Figure 6-7 Modification to Router-B4 Placing It in Bridge Domain 0



Problem Solution Summary

This scenario focused on diagnosing blocked connectivity in internetworks that implement transparent bridging. The following problems were discussed:

- Unstable media or hardware (resulting in spanning tree wars)—Part 1 of this scenario used several router diagnostic tools to illustrate how to identify media and hardware problems that block network connectivity. In this case, the hardware must be tested and replaced if it is out of tolerance.
- Router configuration problems with multiple spanning tree implementations and bridge domain specifications, resulting in packet looping—Part 2 of this scenario discussed these two common configuration problems. These problems can result in packet looping and in blocked network connectivity. Simple configuration changes stopped broadcast storms and restored network service.

  Figure 6-8 provides a complete configuration listing for Router-B4 (obtained using the **write terminal** command) after changes were made to the type of spanning tree algorithm and to the bridge domain specification.

Note Bridge 1 domain 0 is not shown because it is the default.

Figure 6-8 Complete Router-B4 Final Configuration

```
Current configuration:
version 9.1
!
hostname Router-B4
!
enable-password lUVbuKit
!
decnet routing 22.65
decnet node area
decnet max-address 1023
!
interface ethernet 0
ip address 131.8.123.7 255.255.255.0
decnet cost 5
bridge-group 1
!
interface serial 1
ip address 131.8.12.18 255.255.255.0
decnet cost 20
bridge-group 1
!
bridge 1 protocol ieee
!
line aux 0
login
line vty 0 4
login
line con 0
exec-timeout 0 0
password baRFaUxbtZ
line aux 0
no exec
exec-timeout 0 0
password baRFaUxbtZ
line vty 0
exec-timeout 0 0
password baRFaUxbtZ
!
end
```

S2611

Creating Network Maps

An accurate and up-to-date map of your internetwork topology is an essential first step when you are troubleshooting connectivity problems. The **show span** EXEC command is a simple tool that you can use to create topology maps in transparent bridging networks. This command is particularly useful when all bridges consist of Cisco internetworking nodes. The information provided in the following discussion is presented in three parts:

- Explanation of the key information displayed by the **show span** EXEC command
- Method for creating network maps from the **show span** display output
- Example of the map creation process

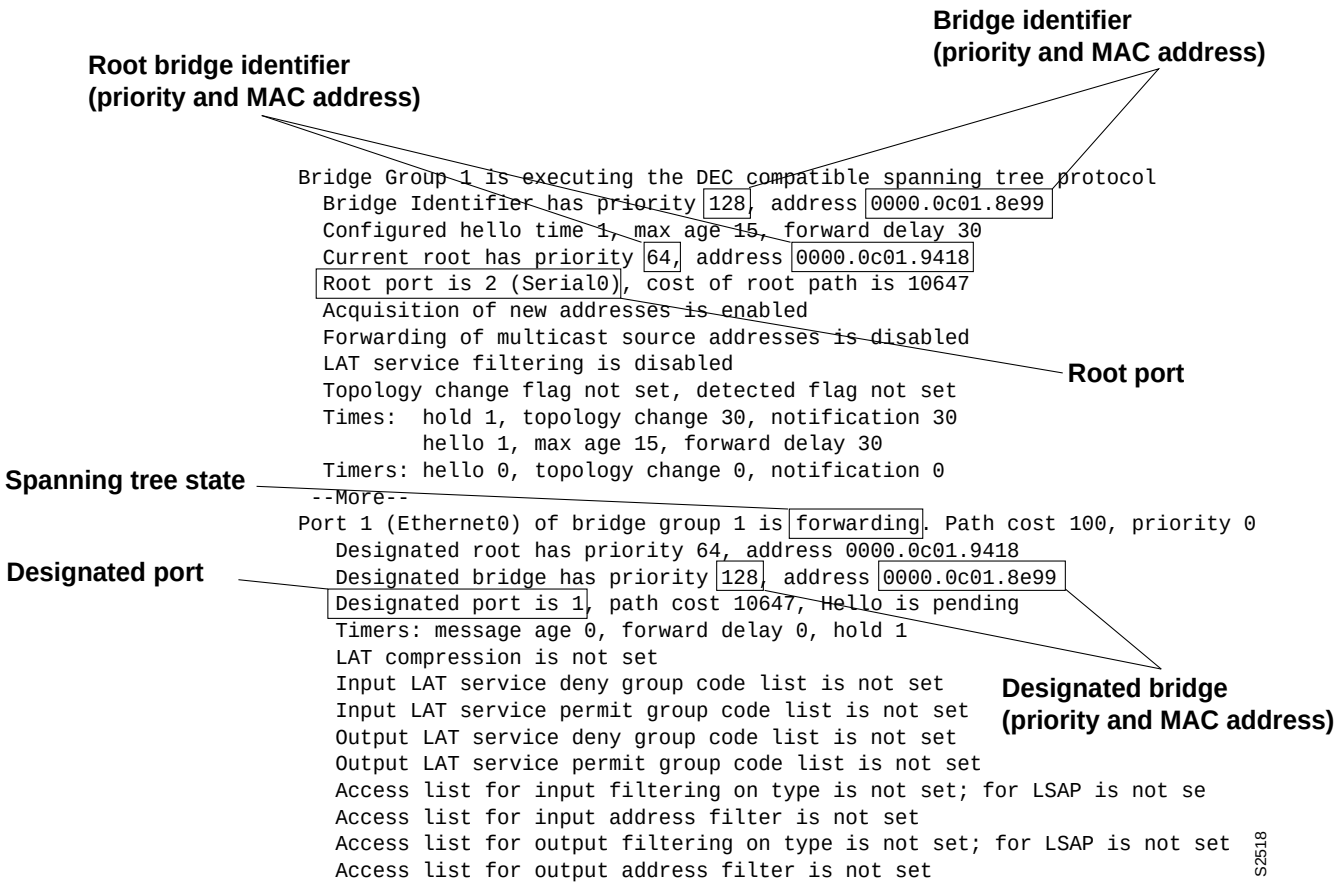
Note This discussion assumes that the internetwork does not have any connectivity or design problems. If you try to create a map of a nonoperational internetwork, multiple root bridges may appear or bridging nodes may not be accessible.

Key show span Command Information

Figure 6-9 highlights the key fields for building a network map that are displayed by the **show span** EXEC command. The fields include the following:

- Bridge identifier—Spanning tree priority and Media Access Control (MAC) address of the bridging node for which the **show span** EXEC command was executed.
- Root bridge identifier—Spanning tree priority and MAC address of the known root bridge; this information appears in two places: with global information and with port-specific information.
- Root port—Spanning tree port on the bridge being examined through which the root bridge for the internetwork is found.
- Spanning tree state—When a port is in forwarding mode, it is actively able to pass traffic over the link; when a port is in blocking mode, the link is an online backup that is not forwarding bridge traffic. Other possible modes are down, listening, and learning. Traffic is only forwarded over the link when the port is in forwarding mode.
- Designated bridge—Spanning tree designated bridge MAC address for the port or interface. If the designated bridge does not match the bridge identifier, and the port is in the forwarding state, the port is a root port. If the designated bridge matches the bridge identifier, the port is in the forwarding state or is down.
- Designated port—Spanning tree port associated with the designated bridge.

Figure 6-9 show span Command Output Illustrating Location of Key Fields



General Method

Creating a network map is a relatively simple, iterative process that consists of the following steps:

Step 1 Obtain the **show span** EXEC command output for each Cisco bridging node and make note of the values of the key fields.

Step 2 For each nonroot bridge, determine the direction, in terms of the relevant interface and port, to the root bridge.

Step 3 Draw your map as you identify the links.

The following rules apply when using spanning tree information to create a network map:

- When the MAC address of the designated bridge is the same as the MAC address of the root bridge, the port or interface of the bridge being examined and the root bridge are attached to the same network.
- When the MAC address of the designated bridge is different from the MAC address of the bridge being examined, the designated bridge is in the path to the root bridge.

- When the MAC address of the designated bridge is the same as the bridge identifier of the bridge being examined, the port or interface points away from the root bridge.
- The designated port value specified for a particular port belongs to the bridge associated with the designated bridge shown in the port listing.

Creating a Sample Network Map

This section guides you through the steps of using the output of the **show span** EXEC command to create a map for an internetwork that consists of four bridges (Wanaka, Pauanui, Turangi, and Auckland). For each bridge, the discussion includes the output of the **show span** EXEC command, an interpretation of the output, and a network map.

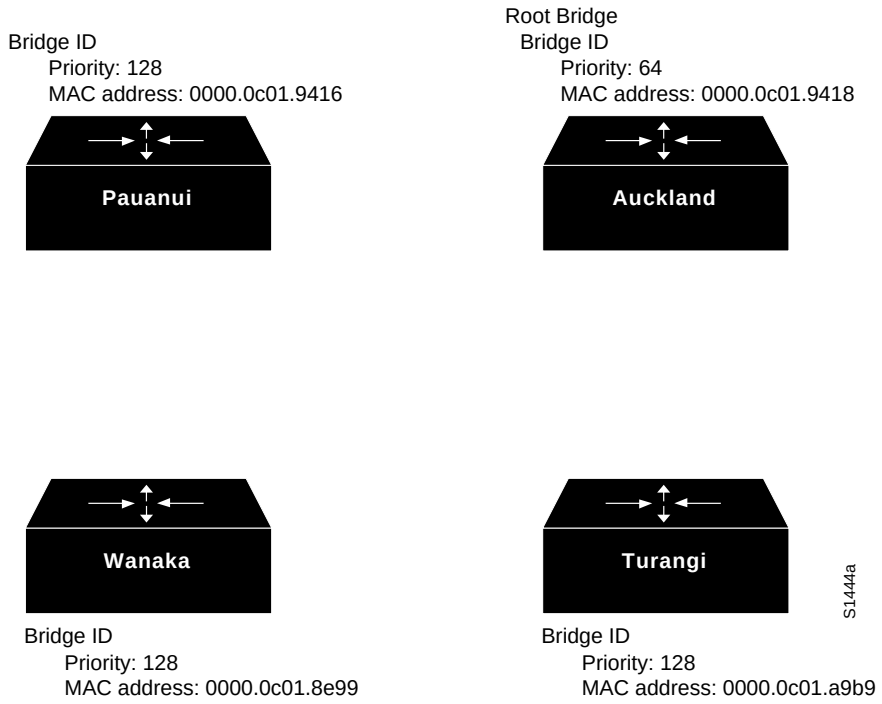
Step 1 Gather the key **show span** information. Table 6-1 summarizes the key information for the four bridges.

Table 6-1 Summary of Show Span Display Information for Each Bridge

Spanning Tree Parameter	Wanaka	Pauanui	Turangi	Auckland
Bridge priority	128	128	128	64
Bridge MAC address	0000.0c01.8e99	0000.0c01.9416	0000.0c01.a9b9	0000.0c01.9418
Root status	Nonroot	Nonroot	Nonroot	Root bridge
Root port	Port 2 (Serial0)	Port 2 (Serial0)	Port 2 (Serial2)	–
Port 1 interface	Ethernet0	Ethernet0	Ethernet0	Ethernet0
Port 1 designated bridge	000.0c01.8e99	0000.0c01.9416	0000.0c01.a9b9	0000.0c01.9418
Port 1 designated port for designated bridge	Port 1	Port 1	Port 1	Port 1
Port 1 status	Forwarding	Forwarding	Forwarding	Forwarding
Port 2 interface	Serial0	Serial0	Serial2	Serial0
Port 2 designated bridge	0000.0c01.9416	0000.0c01.9418	0000.0c01.9418	0000.0c01.9418
Port 2 designated port for designated bridge	Port 3	Port 2	Port 3	Port 2
Port 2 status	Forwarding	Forwarding	Forwarding	Forwarding
Port 3 interface	Serial1	Serial1	Serial3	Serial1
Port 3 designated bridge	0000.0c01.a9b9	0000.0c01.9416	0000.0c01.a9b9	0000.0c01.9418
Port 3 designated port for designated bridge	Port 3	Port 3	Port 3	Port 3
Port 3 status	Blocking	Forwarding	Forwarding	Forwarding

Step 2 Use the output of the **show span** EXEC command to label the bridges and specify bridge indentifiers (MAC addresses). Figure 6-10 is a basic map of the four internetworking nodes without any linkages.

Figure 6-10 Example Bridge Internetwork Map Illustrating Names and Addresses

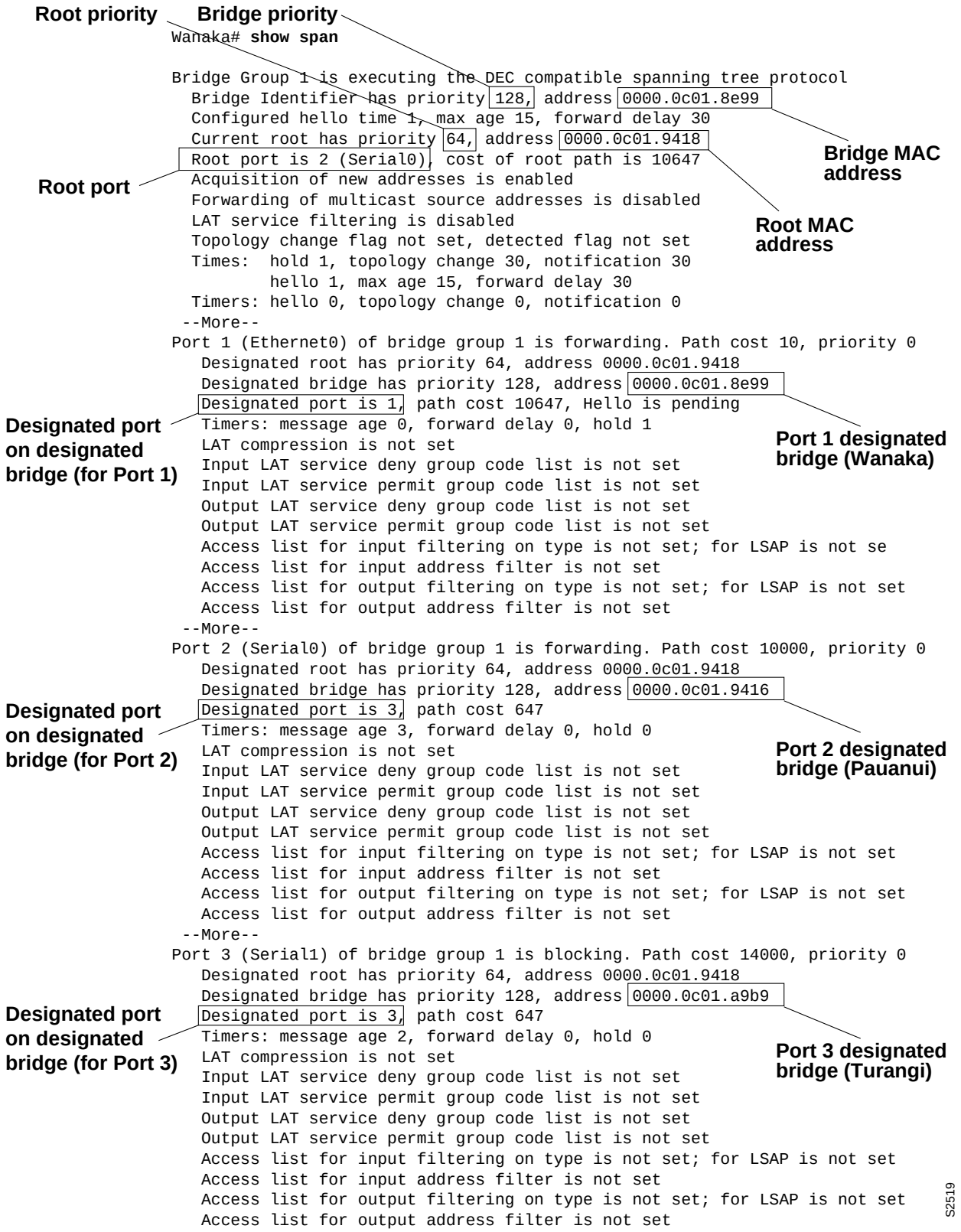


Step 3 If possible, use the **show span** EXEC command output to find the root bridge. Determine the port numbers and match these to the interface names. This information will be used later in the analysis to complete the network map.

Step 4 Now you can start drawing lines between the bridges based on information from the **show span** output. Start with one of the bridges and move from bridge to bridge until you have defined all the linkages. For this example, start with the bridge named Wanaka. Figure 6-11 illustrates the **show span** EXEC command output for Wanaka.

Note If you have an idea of the node that is farthest from the root bridge (the path that has the most intervening nodes), you might try working toward the root bridge from that node.

Figure 6-11 Output of the show span EXEC Command for Wanaka



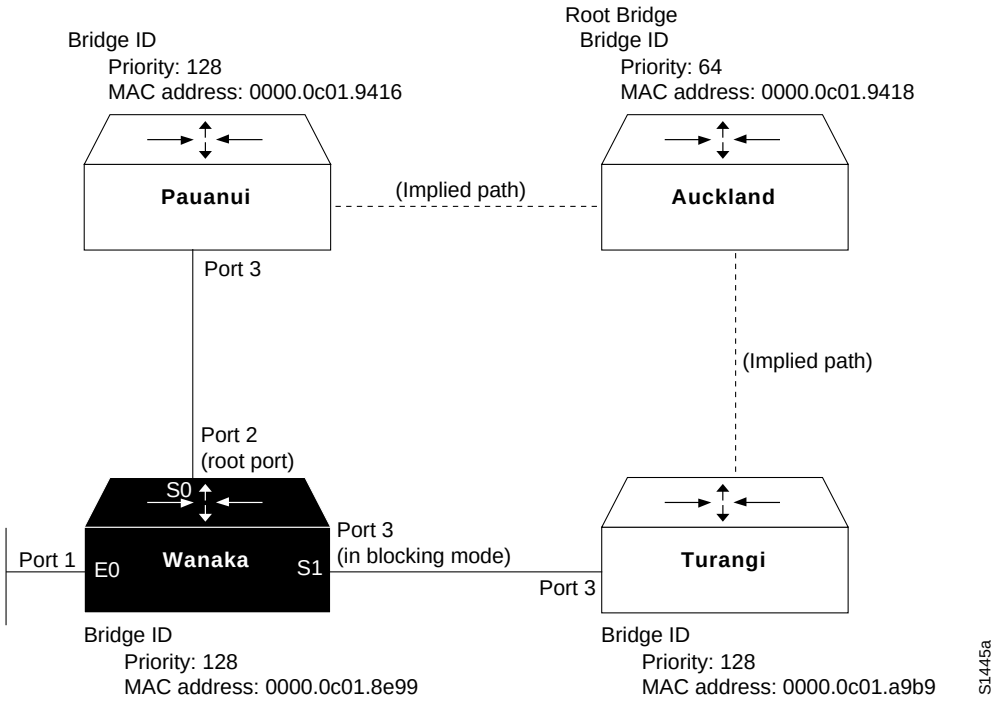

```
Wanaka# show span

Bridge Group 1 is executing the DEC compatible spanning tree protocol
  Bridge Identifier has priority 128, address 0000.0c01.8e99
  Configured hello time 1, max age 15, forward delay 30
  Current root has priority 64, address 0000.0c01.9418
  Root port is 2 (Serial0), cost of root path is 10647
  Acquisition of new addresses is enabled
  Forwarding of multicast source addresses is disabled
  LAT service filtering is disabled
  Topology change flag not set, detected flag not set
  Times:  hold 1, topology change 30, notification 30
          hello 1, max age 15, forward delay 30
  Timers: hello 0, topology change 0, notification 0
 --More--
Port 1 (Ethernet0) of bridge group 1 is forwarding. Path cost 10, priority 0
   Designated root has priority 64, address 0000.0c01.9418
   Designated bridge has priority 128, address 0000.0c01.8e99
   Designated port is 1, path cost 10647, Hello is pending
   Timers: message age 0, forward delay 0, hold 1
   LAT compression is not set
   Input LAT service deny group code list is not set
   Input LAT service permit group code list is not set
   Output LAT service deny group code list is not set
   Output LAT service permit group code list is not set
   Access list for input filtering on type is not set; for LSAP is not se
   Access list for input address filter is not set
   Access list for output filtering on type is not set; for LSAP is not set
   Access list for output address filter is not set
 --More--
Port 2 (Serial0) of bridge group 1 is forwarding. Path cost 10000, priority 0
   Designated root has priority 64, address 0000.0c01.9418
   Designated bridge has priority 128, address 0000.0c01.9416
   Designated port is 3, path cost 647
   Timers: message age 3, forward delay 0, hold 0
   LAT compression is not set
   Input LAT service deny group code list is not set
   Input LAT service permit group code list is not set
   Output LAT service deny group code list is not set
   Output LAT service permit group code list is not set
   Access list for input filtering on type is not set; for LSAP is not set
   Access list for input address filter is not set
   Access list for output filtering on type is not set; for LSAP is not set
   Access list for output address filter is not set
 --More--
Port 3 (Serial1) of bridge group 1 is blocking. Path cost 14000, priority 0
   Designated root has priority 64, address 0000.0c01.9418
   Designated bridge has priority 128, address 0000.0c01.a9b9
   Designated port is 3, path cost 647
   Timers: message age 2, forward delay 0, hold 0
   LAT compression is not set
   Input LAT service deny group code list is not set
   Input LAT service permit group code list is not set
   Output LAT service deny group code list is not set
   Output LAT service permit group code list is not set
   Access list for input filtering on type is not set; for LSAP is not set
   Access list for input address filter is not set
   Access list for output filtering on type is not set; for LSAP is not set
   Access list for output address filter is not set
```

You can use the rules outlined in the "General Method" section earlier in this chapter and the **show span** EXEC command output for Wanaka to make the following conclusions:

- Wanaka Port 1 (Ethernet0) points away from the root bridge, because the designated bridge for this port is the bridge identifier for Wanaka.
- Wanaka Port 2 (Serial0) points at another bridge (in this case Pauanui) that is in the path to the root bridge, because the designated bridge has a different MAC address.
- Wanaka Port 3 (Serial1) points to another bridge (in this case Turangi) that is in the path to the root bridge, because the designated bridge has a different MAC address.
- The root bridge in this internetwork (assuming that all the bridges are in a common, closed internetwork) is Auckland (bridge priority 64 and MAC address 0000.0c01.9418). In this case, the root bridge has been administratively assigned, based on priority.
- The designated port on Pauanui that points toward Wanaka is Port 3; the specific interface cannot be determined from the available information.
- The designated port on Turangi that points toward Wanaka is Port 3; the specific interface cannot be determined from the available information.
- Wanaka Port 1 is in forwarding mode; Wanaka Port 2 is in forwarding mode; and Wanaka Port 3 is in blocking mode.

Figure 6-12 illustrates the partial network map that can be drawn based on the information obtained from the **show span** EXEC command output for Wanaka. The map includes two implied links that are based on information from Wanaka; you should use the **show span** EXEC command output from each bridge to verify these implied links.

Figure 6-12 Example Bridge Internetwork Map Illustrating show span Information from Wanaka



Step 5 Examine the next bridge, Pauanui. Figure 6-13 illustrates the **show span** EXEC command output for Pauanui.

You can use the rules outlined in the "General Method" section earlier in this chapter and the **show span** EXEC command output for Pauanui to make the following conclusions:

- Pauanui Port 1 (Ethernet0) points away from the root bridge, because the designated bridge for this port is the bridge identifier for Pauanui.
- Pauanui Port 2 (Serial0) is directly connected to the root bridge, because its designated bridge MAC address matches the MAC address of the root bridge.
- Pauanui Port 3 (Serial1) points away from the root bridge, because the designated bridge for this port is the bridge identifier for Pauanui.
- The designated port on Auckland that points toward Pauanui is Port 2; the specific interface cannot be determined from the available.
- All three ports on Pauanui are in forwarding mode.

Figure 6-14 illustrates the partial network map that can be drawn based on the information obtained from the **show span** EXEC command output for Pauanui (combined with Wanaka). This map still includes an implied link between Auckland and Turangi.

Figure 6-13 Output of the show span EXEC Command for Pauanui

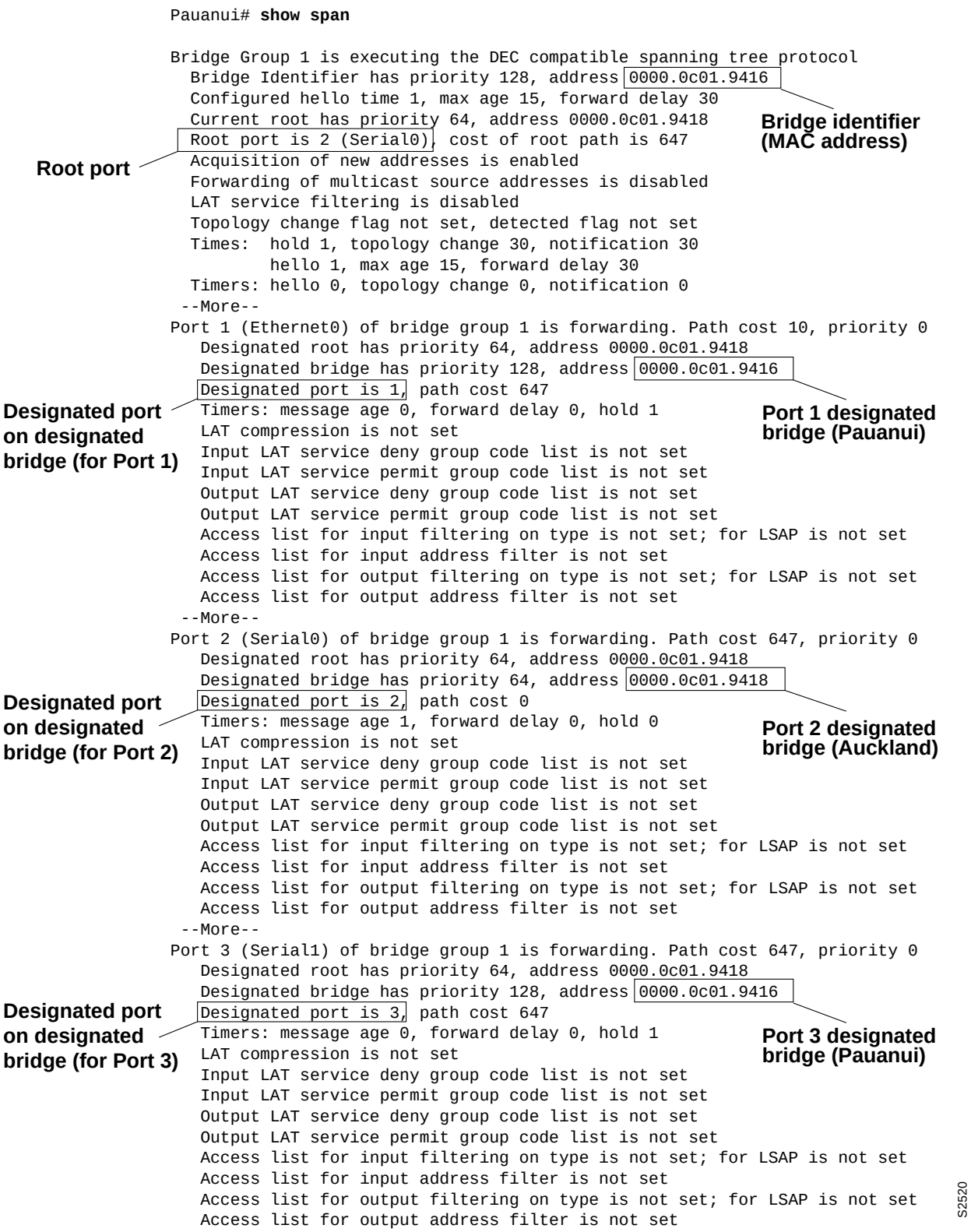
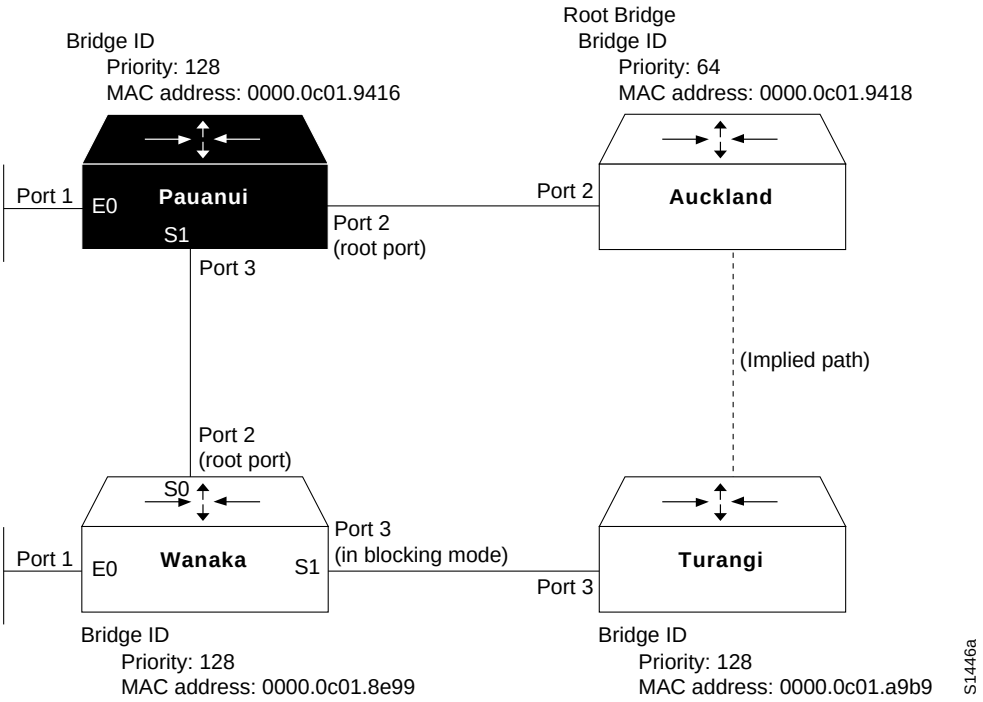


Figure 6-14 Example Bridge Internetwork Map Illustrating Additional show span Information from Pauanui



Step 6 Examine the next bridge, Turangi. Figure 6-15 illustrates the **show span** EXEC command output for Turangi.

You can use the rules outlined in the "General Method" section earlier in this chapter and the **show span** EXEC command output for Turangi to make the following conclusions:

- Turangi Port 1 (Ethernet0) points away from the root bridge, because the designated bridge for this port is the bridge identifier for Turangi.
- Turangi Port 2 (Serial2) is directly connected to the root bridge, because its designated bridge MAC address matches the MAC address of the root bridge.
- Turangi Port 3 (Serial3) points away from the root bridge, because the designated bridge for this port is the bridge identifier for Turangi.
- The designated port on Auckland that points toward Turangi is Port 3; the specific interface cannot be determined from the available information.
- All three ports on Turangi are in forwarding mode.

Figure 6-15 Output of the show span EXEC Command for Turangi

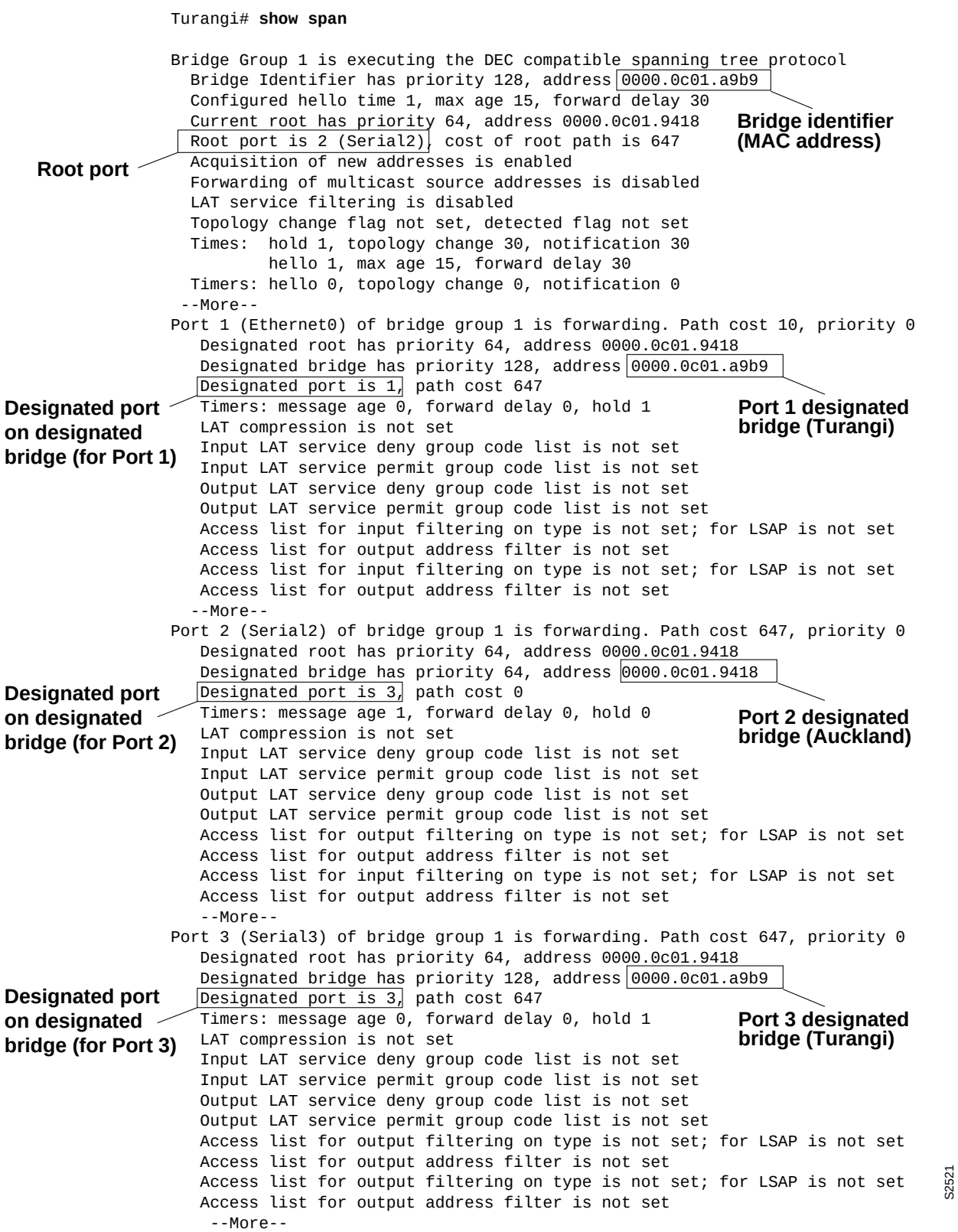
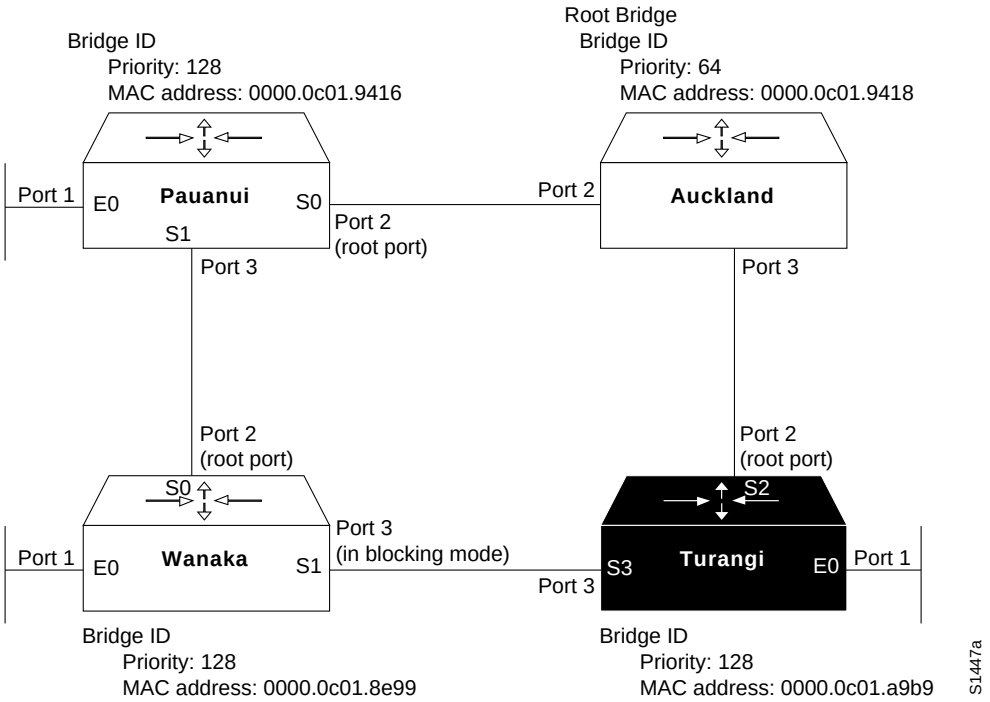


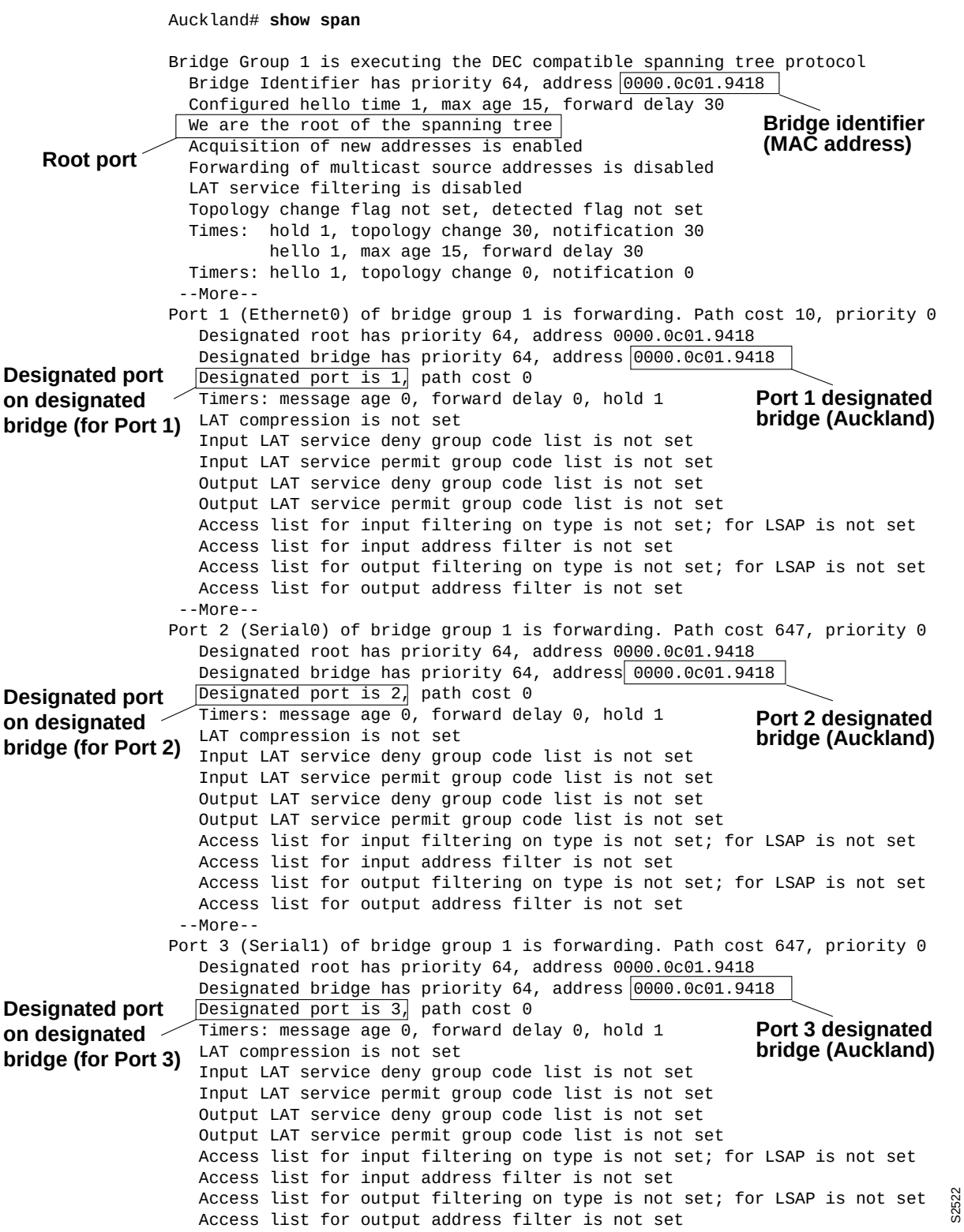
Figure 6-16 illustrates the partial network map that can be drawn based on the information obtained from the **show span** EXEC command output for Turangi (combined with Wanaka and Pauanui).

Figure 6-16 Example Bridge Internetwork Map Illustrating Additional show span Information from Turangi



Step 7 The last step is to complete this map for the root bridge, Auckland. Figure 6-17 illustrates the **show span** EXEC command output for Auckland.

Figure 6-17 Output of the show span EXEC Command for Turangi

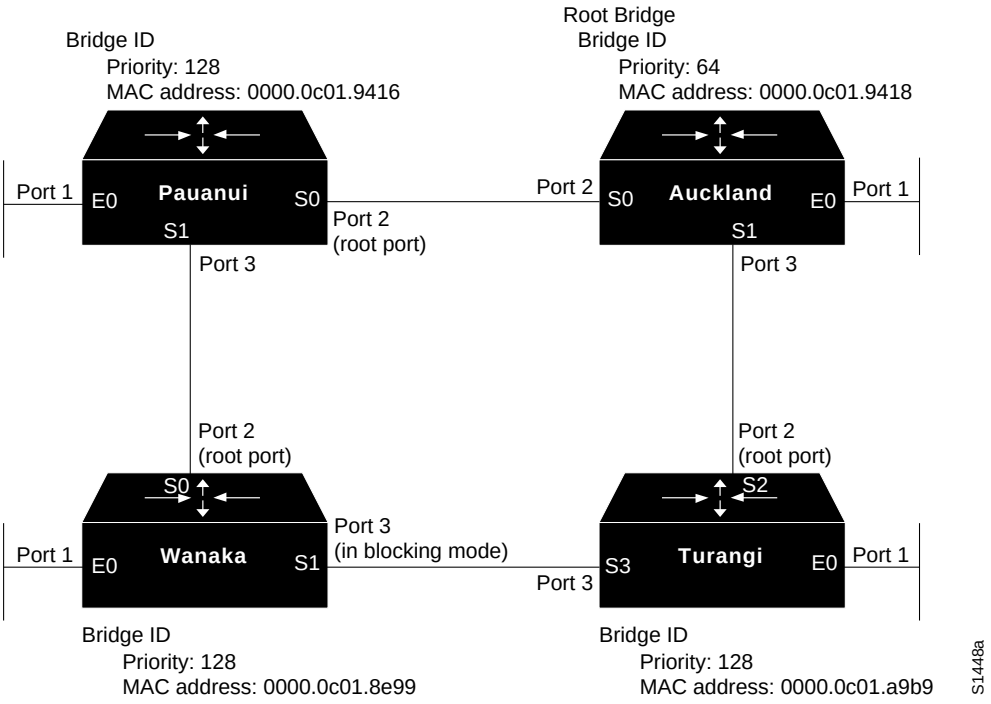


You can use the rules outlined in the "General Method" section earlier in this chapter and the **show span** EXEC command output for Auckland to make the following conclusions:

- Auckland Port 1 (Ethernet0), Port 2 (Serial0), and, Port 3 (Serial1) all point away from the root bridge, because the designated bridge for each port is the bridge identifier for Auckland (the root bridge).
- Auckland Port 1, Port 2, and Port 3 are in forwarding mode.

Figure 6-18 illustrates the completed network map based on the information obtained from the **show span** EXEC command output for Auckland.

Figure 6-18 Complete Bridging Internetwork Map



Bridge-Based Connectivity Symptoms

The symptom modules in this section pertain to bridge-based internetwork problems and cover the following topics:

- Packet Looping and Broadcast Storms Occur in Transparent Bridging Internetwork
- Excessive Packet Drops by Internetwork Nodes
- Host Connection Sessions Time Out
- Users Cannot Connect over Concurrent Bridging and Routing Internetwork
- Routing Loop Occurs in Bridging and Routing Internetwork

Packet Looping and Broadcast Storms Occur in Transparent Bridging Internetwork

Symptom: The internetwork is experiencing media saturation; end stations are forced into excessive retransmission; sessions are timing out and dropping.

Note Packet loops are typically caused by network design problems.

Table 6-2 outlines possible causes and suggested actions when packet looping and broadcast storms occur in transparent bridging environments.

Table 6-2 Bridging: Packet Looping and Broadcast Storms in Transparent Bridging Internetwork

Possible Causes	Suggested Actions
No spanning tree to prevent packets from looping	**Step 1** Create and examine a topology map of your internetwork. **Step 2** Look for possible loops and eliminate any that exist or make sure that appropriate links are in backup mode. **Step 3** If broadcast storms and packet loops persist, use the **show interfaces** EXEC command to obtain input and output packet count statistics. If these counters increment at an abnormally high rate (with respect to your normal traffic loads), a loop is still likely. **Step 4** Conduct a binary search by segmenting networks in order to isolate any loops. **Step 5** Redesign your network to eliminate any loops. **Step 6** Implement a spanning tree algorithm to prevent loops.
Both IEEE and DEC spanning tree algorithms running on a looped topology	**Step 1** Use the **show interfaces** EXEC command to obtain input and output packet count statistics. If these counters increment at an abnormally high rate (with respect to your normal traffic loads), a loop is likely. **Step 2** Use the **show span** EXEC command on bridges to determine whether multiple root bridges exist and to determine which spanning tree algorithms are being used. **Step 3** If both DEC and IEEE appear, reconfigure bridges so that all use the same spanning tree algorithm.
Multiple bridging domains incorrectly configured	**Step 1** Use the **show span** EXEC command on bridges to determine whether multiple root bridges exist and to ensure that all domain group numbers match for given bridging domains. **Step 2** If multiple domain groups are configured for the bridge, ensure that all domain specifications match intended bridging domains. Use the **bridge** *group* **domain** *domain-number* global configuration command to make any necessary changes. **Step 3** Make sure that no loops exist between bridging domains.

Excessive Packet Drops by Internetwork Nodes

Symptom: Dropped packets are typically accompanied by the inability to make connections over a bridge. Table 6-3 outlines possible causes and suggested actions when bridged internetworks experience dropped packets.

Table 6-3 Bridging: Excessive Packet Drops by Bridged Internetwork Nodes

Possible Causes	Suggested Actions
Misconfigured bridging filters	**Step 1** Use the **write terminal** privileged EXEC command to determine whether any bridge filters exist. **Step 2** Remove bridge filters on suspect interfaces. **Step 3** Determine whether connectivity returns. If connectivity does not return, the filter is not the problem. If connectivity resumes after removing filters, one or more bad filters are causing the connectivity problem. **Step 4** If multiple access lists and lists with multiple statements exist, apply each filter and access list individually to identify the problem filter.
Physical connection problem at the bridge	**Step 1** Use the **show interfaces** EXEC command to determine whether the line protocol is up. **Step 2** If the line protocol is down, check the physical connection between that interface and the network. Make sure that the connection is secure. **Step 3** If the line protocol is up, but input and output packet counters are not incrementing, check the media and the connectivity of other hosts.
Input and output queues full due to excessive routed and broadcast traffic	**Step 1** Use the **show interfaces** command to look for input and output drops. Drops suggest excessive traffic over the media. **Step 2** Reduce the traffic on attached networks by implementing bridging filters, or segment the network using more internetworking devices. **Step 3** If the connection is a serial link, increase bandwidth, apply priority queuing, increase the hold queue size, or modify the system buffer size. Refer to Chapter 3, “Troubleshooting Serial Line Problems,” for more details.
Target host is down, resulting in flooding	**Step 1** Use the **show bridge** EXEC command on all bridges to make sure that all forwarding databases include the required end nodes. **Step 2** If any end nodes are missing, identify them and check their status to verify that they are available. **Step 3** Reinitialize or reconfigure end nodes as necessary and reexamine the forwarding databases.

Host Connection Sessions Time Out

Symptom: Users can make connections, but sessions terminate abruptly. Table 6-4 outlines possible causes and suggested actions for host sessions that drop in a bridged environment.

Table 6-4 Bridging: Host Connection Sessions Time Out in Bridged Environment

Possible Causes	Suggested Actions
End station sessions timer is too low	**Step 1** Use a network analyzer to look for host retransmissions. **Step 2** If you see retransmissions, increase the transmission timers on the host. **Step 3** Use a network analyzer to determine whether the number of retransmissions subsides.
Excessive delay over slow serial link	**Step 1** Increase bandwidth, apply priority queuing, increase the hold queue size, or modify the system buffer size. For more details, refer to the "Troubleshooting Serial Line Problems" chapter.

Users Cannot Connect over Concurrent Bridging and Routing Internetwork

Symptom: In a routing and bridging environment, users are unable to make connections over the router. Table 6-5 outlines possible causes and suggested actions when connectivity is blocked in an internetwork that features routing and bridging.

Table 6-5 Bridging: Users Cannot Connect over a Bridging and Routing Internetwork

Possible Causes	Suggested Actions
Poor network design; misconfigured network address	**Step 1** Check the router configuration for assignment of incorrect network addresses. Modify any that are incorrect. **Step 2** Check each end station for an incorrectly assigned network address. Modify any network addresses that are incorrect. **Step 3** Refer to the appropriate protocol-specific chapter in this publication for more information about network address problems and conventions.
Misconfigured router	**Step 1** Use the **write terminal** privileged EXEC command to examine the configurations of all bridges and routers in the internetwork. **Step 2** Make sure traffic that needs to be bridged is being bridged and traffic that needs to be routed is being routed.

Routing Loop Occurs in Bridging and Routing Internetwork

Symptom: Blocked connectivity to certain portions of an internetwork and the appearance of duplicate addresses suggest the presence of a routing loop. Table 6-6 outlines possible causes and suggested actions for routing loops in a bridging and routing internetwork.

Table 6-6 Bridging: Routing Loop Occurs in a Bridging and Routing Internetwork

Possible Causes	Suggested Actions
Misconfigured network address	**Step 1** Use the **write terminal** privileged EXEC command to check the network address assignment for suspect interfaces. **Step 2** Make sure that all bridges are in the same bridge group or bridge domain. **Step 3** Retry host connections.
Disconnected cable	**Step 1** Check the physical attachment of all affected networks to ensure proper cable attachment. **Step 2** Retry host connections.
Backdoor bridge	**Step 1** Use the **show interfaces** EXEC command to look for excessive accumulation of input and output packets. **Step 2** Check the network topology for possible backdoor bridges that connect two or more separate networks. **Step 3** If you cannot find the backdoor bridge by inspection, use a network analyzer to examine the source MAC address of each remote node. When a router is used to segment local and remote networks, the MAC address of the router replaces the source MAC address of the remote node. If you find a packet from a remote note whose source MAC address is not the MAC address of the router, the packet arrived through a backdoor bridge.

CHAPTER 7

Troubleshooting DECnet Connectivity

This chapter presents protocol-related troubleshooting information for DECnet Phase IV connectivity problems. This chapter consists of the following sections:

- DECnet Connectivity Scenario
- Configuring a DECnet Node to Log DECnet Events
- DECnet Connectivity Symptoms

The symptom modules consist of the following sections:

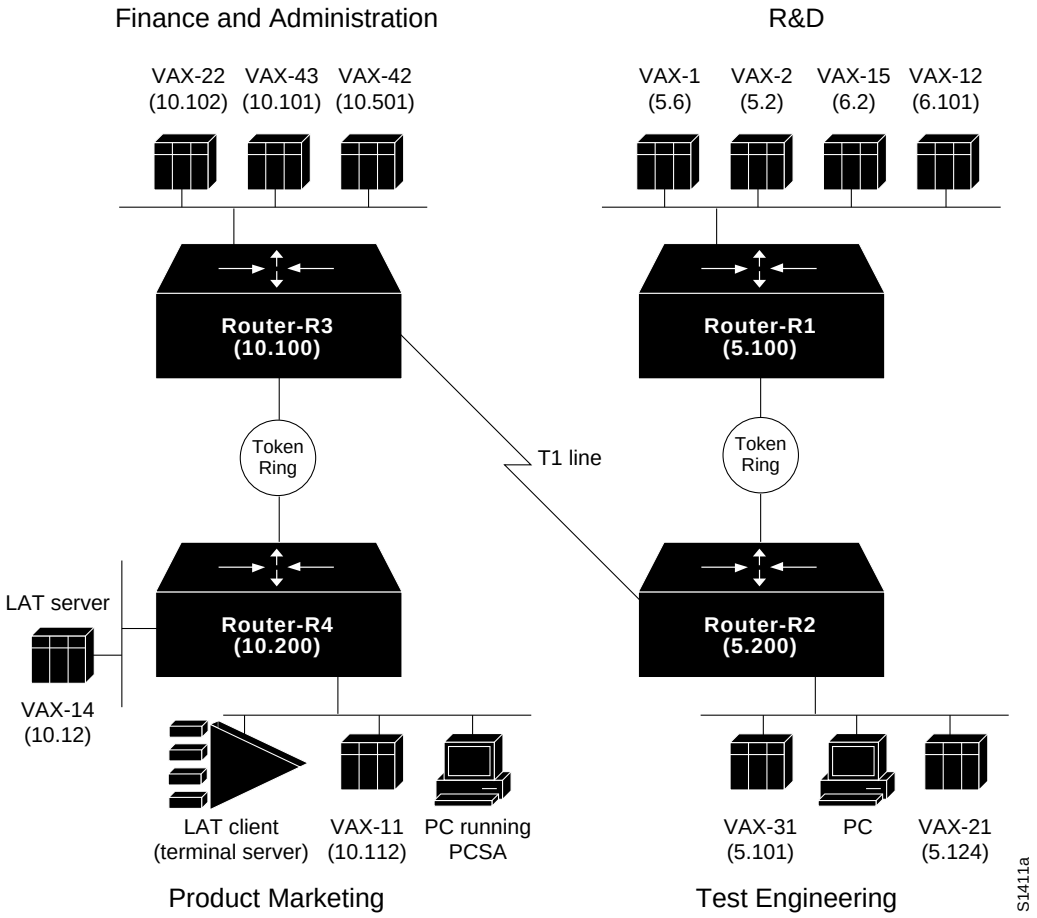
- Symptom statement—A specific symptom associated with the state of DECnet connectivity
- Possible causes and suggested actions—A table for each symptom containing possible causes for the symptom and suggested actions for resolving each cause

DECnet Connectivity Scenario

Many DECnet internetworks continue to employ DEC's proprietary Phase IV network architecture. This scenario explores some internetworking problems unique to DECnet Phase IV. Figure 7-1 is a network map for this scenario and shows the network addresses of relevant end systems and routing nodes.

Note DECnet Phase V is equivalent to ISO Connectionless Network Service (CLNS). For information about ISO CLNS/DECnet Phase V internetworking issues, see the "Troubleshooting ISO CLNS Connectivity" chapter.

Figure 7-1 Network Map for DECnet Phase IV Connectivity Scenario



Symptoms

Assume that the following symptoms have been reported for this DECnet Phase IV network:

- VAX-21 and VAX-31 in Test Engineering cannot communicate with VAX-42 in Finance and Administration. Note that VAX-31 can access VAX-43.
- VAX-12 and VAX-15 in R&D cannot communicate with VAX hosts in Finance and Administration, Product Marketing, and Test Engineering, although they can communicate with each other. VAX-12 and VAX-15 are also unable to communicate with VAX-1 and VAX-2 (which are also in R&D).
- VAX-21 and VAX-31 in Test Engineering cannot communicate with VAX-11 and VAX-14 in Product Marketing. Similarly, VAX-22, VAX-43, VAX-1, and VAX-2 are also unable to communicate with VAX-11 and VAX-14.

Note For the purposes of this scenario, assume that the hosts in Test Engineering (VAX-31 and VAX-21) are fully operational.

Environment Description

The relevant elements of the internetworking environment shown in Figure 7-1 can be summarized as follows:

- Intercampus service is provided via a T1 serial link; Router-R2 and Router-R3 interconnect the networks.
- The various DEC hosts are connected to Ethernets, with intervening Token Ring segments interconnecting certain segments.
- The network applications that run over the network include DECnet file transfer and Local Area Transport (LAT) connection service (bridged). The network is a Phase IV network divided into several DECnet areas.

Diagnosing and Isolating Problem Causes

The following problems are likely candidates for the first symptom (VAX-21 and VAX-31 cannot communicate with VAX-42):

- Certain interfaces connected to affected segments do not have DECnet routing enabled.
- A misconfigured or incorrectly applied access list is blocking specific traffic.
- Certain end systems are in a partitioned area.
- DECnet protocol parameter values associated with the path between nodes exceed the maximum values specified on the router. The associated DECnet routing parameters may be incorrectly assigned.
- The node number associated with an end node is higher than allowed by the **decnet max-address** global configuration command on one of the routers.

The following problems are likely candidates for the second symptom (no connectivity to or from VAX-12 and VAX-15 in DECnet area 6):

- A misconfigured or incorrectly applied access list.
- The area is partitioned.
- The router that is attached to the physical network segment of this area is not in the same area as the isolated nodes (no Level 2 routers).

The following problems are likely candidates for the third symptom (R&D, Test Engineering, and Finance nodes cannot communicate to any nodes in Product Marketing):

- DECnet is not enabled on certain routers or Ethernet segments.
- Routers are in different areas (no Level 2 routers).
- Area is partitioned.
- DECnet routing parameters (such as maximum area or maximum cost) are incorrectly assigned.
- DEC Token Ring implementations and differing router software versions combine to block connectivity.

After you identify a list of possible problems, you can analyze each potential cause. Use your judgment and experience to determine where to start the diagnosis process. Notice that for these symptoms, some of the possible problems overlap. The following discussion considers the problems listed and illustrates resolution of discovered problems. Where possible, overlapping problems are addressed for all symptoms.

Determining Which Connections Are Working

The first diagnostic activity to perform before attacking specific problems is to identify what connectivity *is* available on the network, as well as what is not.

Assume that the following connectivity is verified using **set host** connection commands from various (known operational) VAX hosts on the network:

- VAX-21 and VAX-31 (Test Engineering) can communicate with VAX-22 and VAX-43 (in Finance and Administration) and VAX-1 and VAX-2 (in R&D).
- VAX-22 and VAX-43 can also communicate with VAX-1 and VAX-2.
- All nodes in an area can communicate with other nodes in the same area. For instance, VAX-12 and VAX-15 in area 6 can communicate with each other. Similarly, VAX-14 and VAX-11 in area 10 also can communicate with each other. However, no node can communicate with any host outside of its area.

Determining Whether DECnet Is Enabled

After you identify working and broken connections, determine whether routers in the path of connection problems are enabled to support the routed or bridged protocols. Inspect the configuration listings for each of the routers as follows:

Step 1 Use the **write terminal** or **show decnet interface** EXEC commands to determine whether the configuration includes the **decnet routing** *decnet-address* global configuration command, as well as any **decnet cost** *cost-value* interface configuration commands for interfaces intended to route DECnet traffic.

Step 2 Because LAT is being bridged in this internetwork, review the configurations for appropriate bridging configuration commands, including the **bridge** *group* **protocol** global configuration command and the **bridge-group** *group* interface configuration command.

In this case, assume that these routers have been properly configured to support DECnet routing and to bridge LAT as needed.

Checking Configurations for Misconfigured Access Lists

Next, determine whether any access lists have been incorrectly applied or configured.

Step 1 Remove any access list specifications on all relevant interfaces.

Step 2 See whether traffic can get through by testing the connection from any clients to the target server.

Step 3 If connections now work, a misconfigured access list needs modification. If connectivity is not restored, access lists are not necessarily the problem. However, it is possible that access lists are improperly implemented, but masked by another problem. You may have to return to this step if, after connectivity is restored, connections are again lost when you reinstall access lists.

Step 4 If access lists are known to be the problem, isolate the location of the bad access list specification by applying one access list statement at a time until you can no longer create connections. Make sure that access lists are applied to the correct interface.

For the purposes of this scenario, assume that no access lists are used.

Determining Whether Nodes Are in a Partitioned Area

If a DECnet area is not contiguous (parts of one area are separated by another area), it is "partitioned," and nodes in the separate areas cannot communicate with each other. Use the following steps to determine whether areas are contiguous.

Step 1 Review the topology for any discontiguous areas.

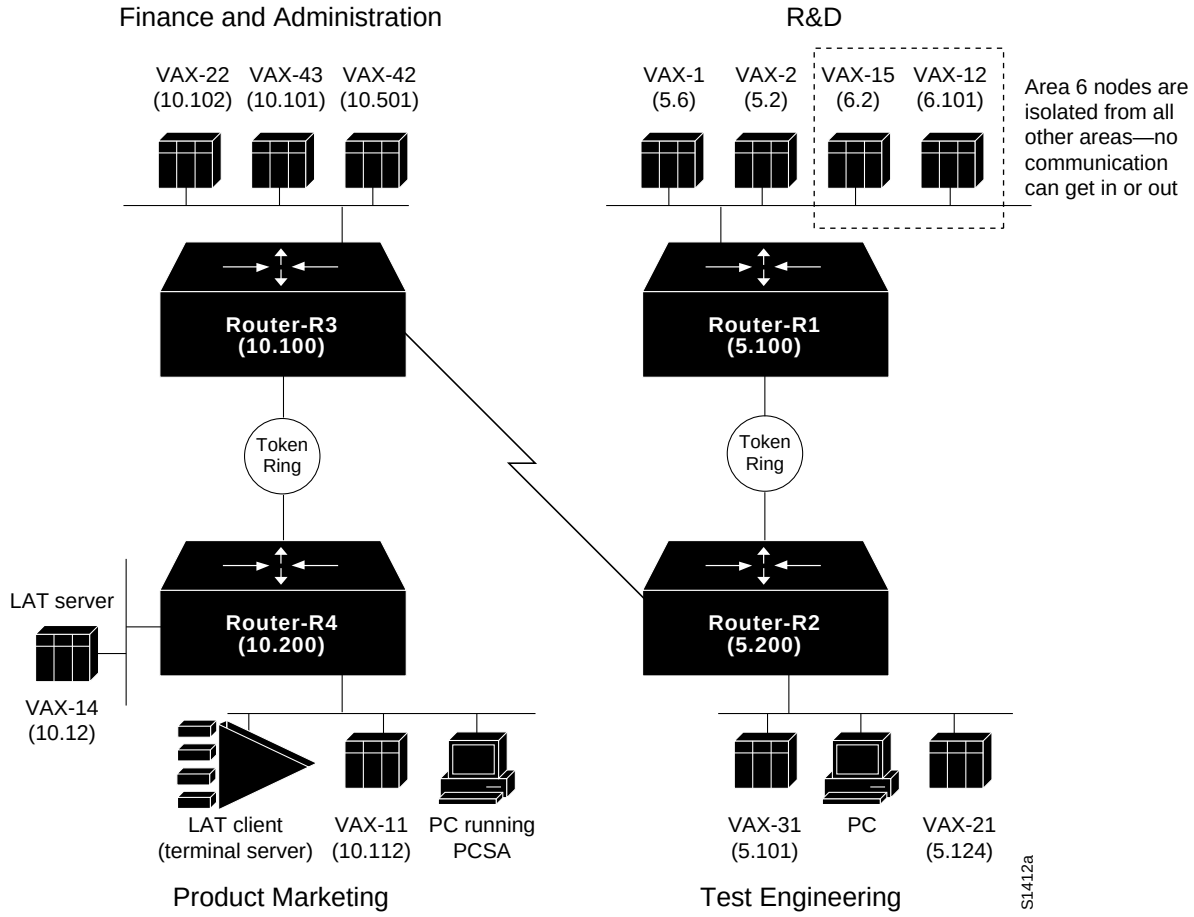
Step 2 If any partitioned areas exist, eliminate them by reconfiguring the physical network or reassigning network area addresses so that all the Level 2 areas are contiguous.

For the purposes of this implementation, assume that there are no partitioned areas.

Ensuring That Level 2 Routers Are in Place for All Areas

If a Level 2 DECnet router does not exist for a given area, the effect is similar to having a partitioned area. All traffic from the isolated area (that is, the area for which there is no Level 2 router) is ignored by all network devices that are not in the same area. This particular problem is suspected because there is no connectivity to or from nodes in DECnet area 6, as shown in Figure 7-2.

Figure 7-2 DECnet Scenario Map Illustrating Isolated DECnet Area



The following steps illustrate how to identify and remedy this problem:

Step 1 Use the **show decnet route** command at Router-R1 to determine whether a Level 2 router exists for DECnet area 6 in the route table. Figure 7-3 presents the output of the **show decnet route** command, which shows that there is not a Level 2 router for area 6.

Figure 7-3 Output of the show decnet route Command

```
  Area       Cost  Hops   Next Hop to Node       Expires  Prio

*5             0     0     (Local) -> 5.200
*10           10     1     Serial0 -> 10.100        31     64    A
 --More--
  Node       Cost  Hops   Next Hop to Node       Expires  Prio

*(Area)        0     0     (Local) -> 5.200
*5.100         4     1   Tokenring0 -> 5.100
*5.101         4     1    Ethernet0 -> 5.101
*5.105         4     1    Ethernet0 -> 5.105
*5.111         4     1    Ethernet0 -> 5.111
*5.124         4     1    Ethernet0 -> 5.124

*5.200         0     0     (Local) -> 5.200
```

S2612

Step 2 Because a Level 2 router is required to allow area 6 nodes to communicate with devices in other areas (even devices on the same physical cable), you must include an area 6 Level 2 routing node on the same cable with area 6 nodes.

You can set up one of the VAX hosts (such as DECnet node 6.101, VAX-12) as a Level 2 routing node, or you can add another router to the LAN segment as the Level 2 router for area 6.

Assume that after VAX-12 is reconfigured as a Level 2 router, area 6 nodes can communicate with nodes in other areas. However, VAX-31 still cannot communicate with VAX-42, and nodes in R&D still cannot communicate with nodes in Product Marketing. More troubleshooting remains to be done.

Determining Whether DECnet Parameters Are Misconfigured

Depending on the situation, connectivity loss can result from misconfigured values for a variety of DECnet parameter settings on a router. If the cost of a path to a node, the number of hops to a node, the cost to an area, or the hops to an area exceed the configured values for a given router, connectivity to the remote node will be blocked. Troubleshoot this problem as follows:

Step 1 Use the **show decnet interface** command to determine whether the various maximum parameter values are set (cost, hops, area cost, and area hops).

Step 2 If any of these values are set, compare the configured value with the value indicated in the DECnet routing table (obtained with the **show decnet route** command).

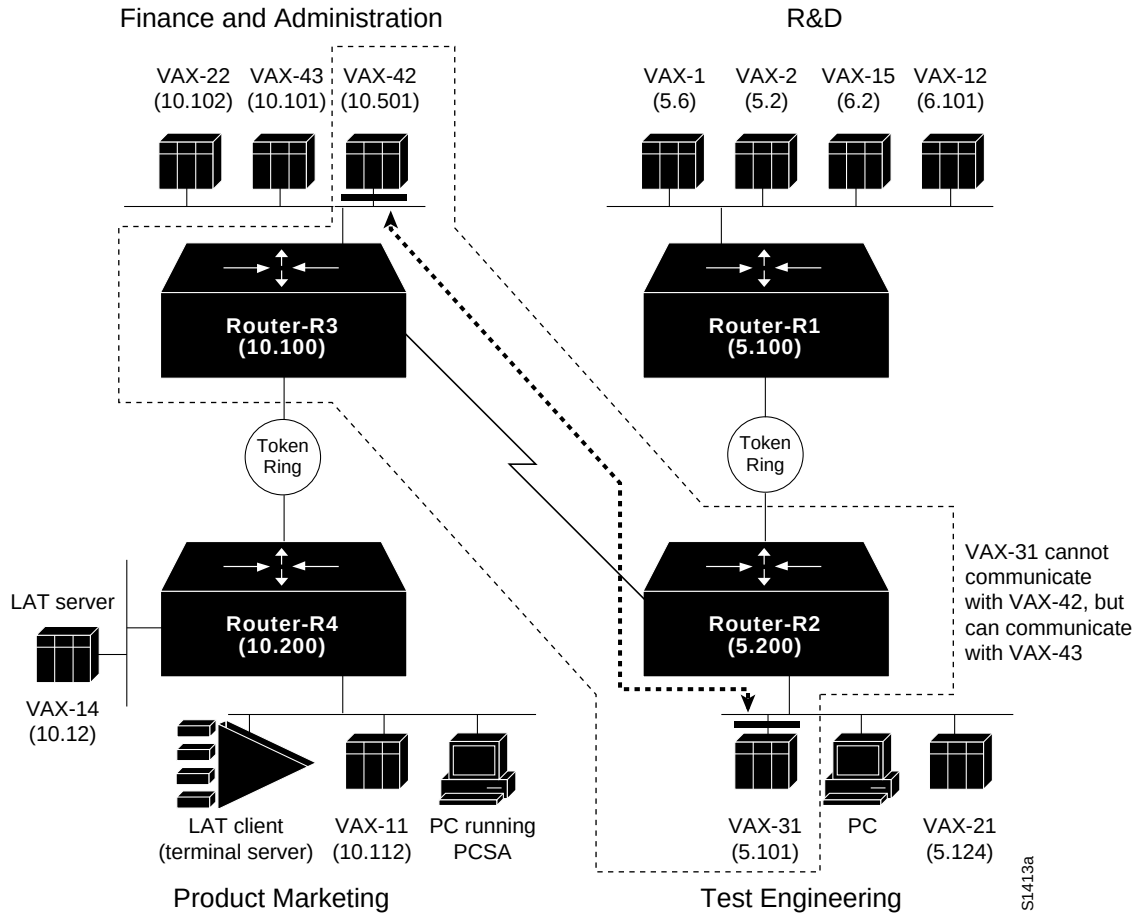
Step 3 If any of the actual values exceed the configured values, change the configuration of the router accordingly (with the **decnet max-cost**, **decnet area-max-cost**, **decnet max-hops**, and **decnet area-max-hops** commands).

For this scenario, assume that none of these values are explicitly configured, which means that the default values are in effect. (The default values are the maximum possible values for DECnet.)

Finding an Out-of-Range Node Number

One symptom cited at the beginning of this scenario is that VAX-31 cannot communicate with VAX-42. (See Figure 7-4.) However, VAX-31 *can* communicate with VAX-43. This situation indicates that some DECnet traffic is passing between Test Engineering and Finance through Router-R2 and Router-R3.

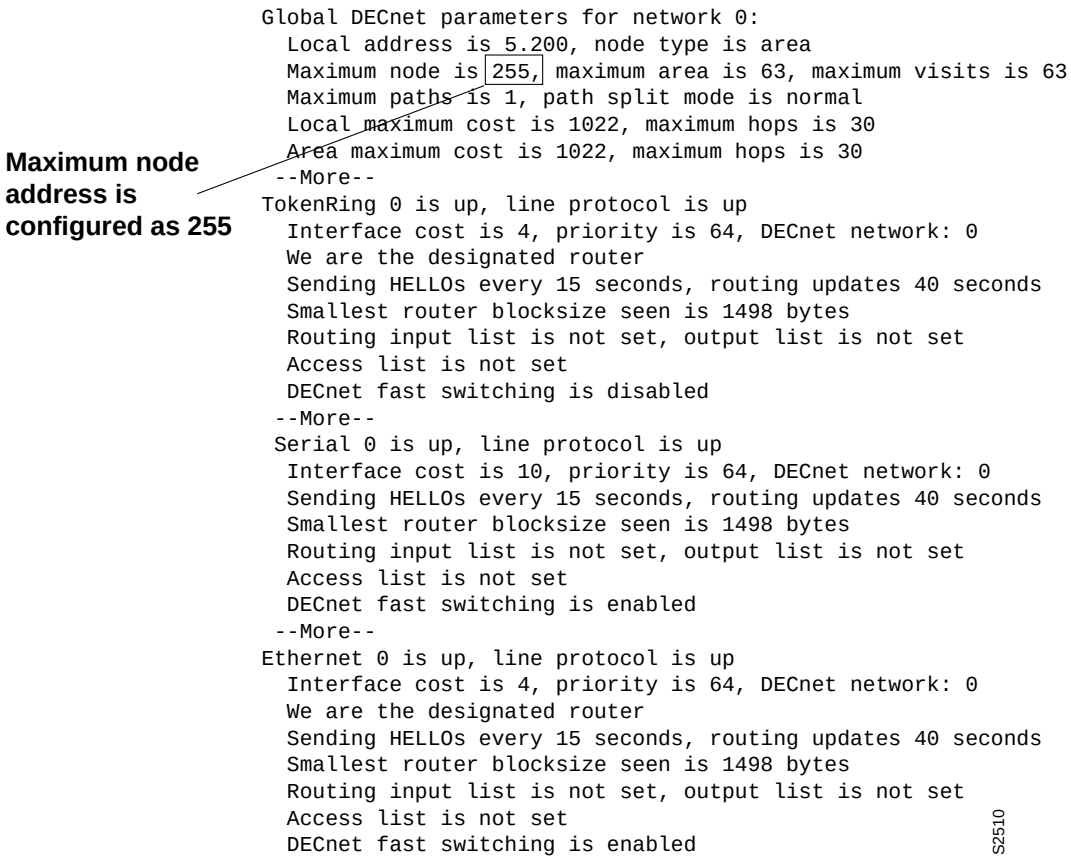
Figure 7-4 DECnet Scenario Map Illustrating Blocked Connectivity to Specific Host



One problem that can cause this symptom is an out-of-range DECnet node address. The easiest solution is to make sure that the router can accommodate the maximum allowable number of addresses (1023), as follows:

Step 1 Use the **show decnet interface** command at Router-R2 to determine the maximum address for the router. (See Figure 7-5.)

Figure 7-5 DECnet Maximum Node Address Display



Step 2 Reconfigure Router-R2 with a maximum address value of 1023 using the **decnet max-address** global configuration command.

Assume that when this change is made, connectivity is restored between VAX-31 and VAX-42. However, the hosts and users in R&D and Product Marketing still are unable to communicate.

Reconciling Encapsulation Differences for DECnet over Token Ring

For this scenario, remember that VAX-22, VAX-42, VAX-1, VAX-2, VAX-31, and VAX-21 are all able to communicate with each other over the router links (Router-R1, Router-R2, and Router-R3). However, none of these hosts can communicate with VAX-14 or VAX-11. These facts point to a problem between Router-R3 and Router-R4.

In prior diagnostic steps, the following possible problems were eliminated:

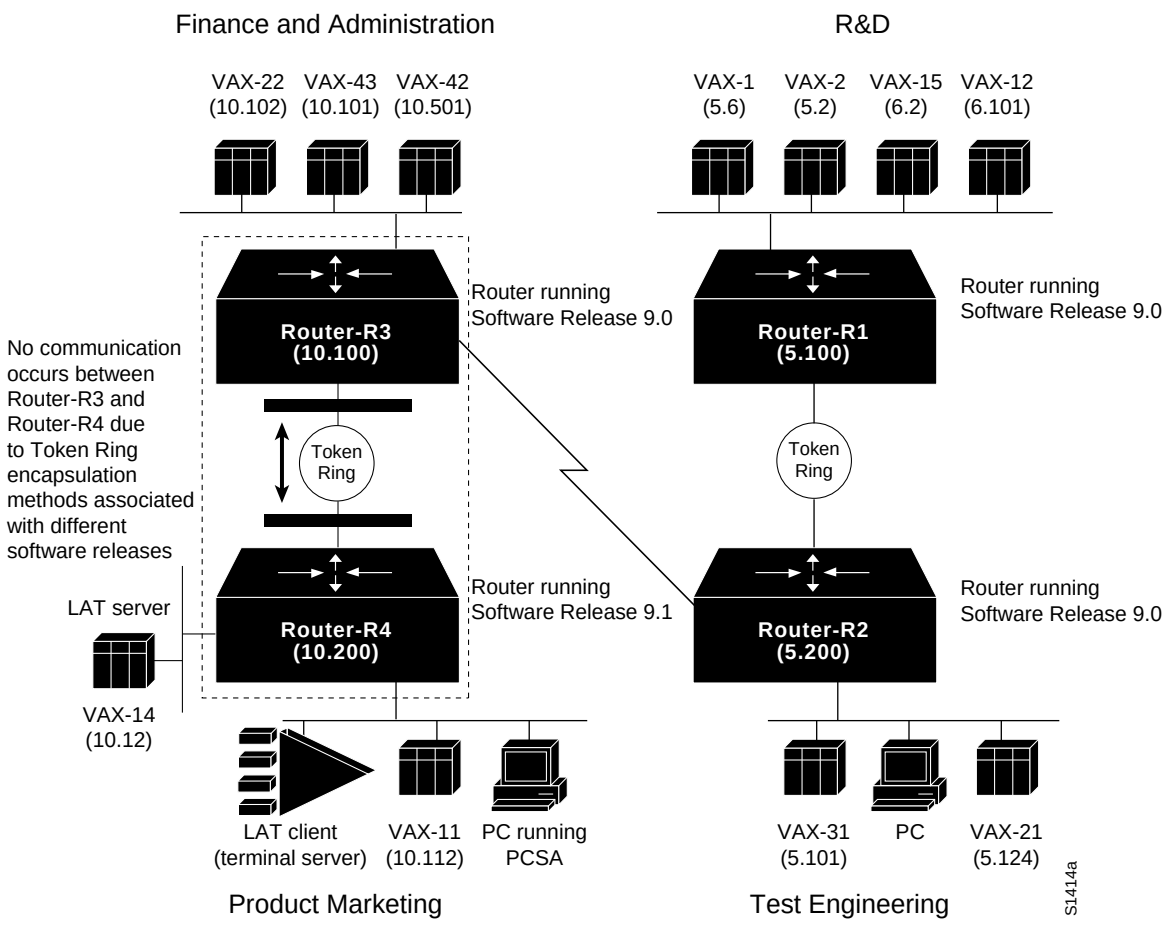
- DECnet is not enabled on certain routers.
- Routers are in different areas (no Level 2 routers).
- An area is partitioned.
- DECnet routing parameters (such as maximum cost or maximum hop) are incorrectly assigned.

One problem remains to be diagnosed: a possible configuration problem associated with DEC Token Ring implementations and differing router software versions.

The method of DECnet encapsulation over Token Ring differs between software releases. In particular, software prior to Software Release 9.1 uses an encapsulation method that does not interoperate with non-Cisco DECnet Token Ring nodes. Cisco routers that use Software Release 9.1 and later are, by default, configured to interoperate with non-Cisco nodes.

Assume that Router-R4 is running Software Release 9.1, while the other routers are running Software Release 9.0. In this situation, all 9.1 routers must be set to support the "pre-DEC" option in the **decnet encapsulation** interface configuration command. Figure 7-6 illustrates this problem and its effects on connectivity.

Figure 7-6 Scenario Map Showing Blocked Communication because of Differing Token Ring Encapsulations



Diagnose this problem as follows:

Step 1 Use the **show version** EXEC command on all Token Ring-attached routers in the path where connectivity is blocked. Check the software version string for the release number.

Step 2 Look for routers that have Software Release 9.1 (and later) and earlier releases. If both are found, the DECnet encapsulation type being used must be reconciled for all Token Ring-attached routers.

Step 3 All-Cisco internetwork only—Use the **write terminal** privileged EXEC command on each of the routers running Software Release 9.1 or later. Look for a **decnet encapsulation** interface configuration command. If it is not present (and if all routers in the network are Cisco routers), add the **decnet encapsulation pre-dec** command. As an alternative, you can upgrade routers running a software release prior to Software Release 9.1 to Software Release 9.1 or later.

Interoperation internetwork—If you must support interoperation between Cisco routers and non-Cisco devices over Token Ring, upgrade the software versions on routers running a software release prior to Software Release 9.1 or later.

When the **decnet encapsulation pre-dec** command is configured for Router-R4, connectivity between nodes in R&D and Product Marketing is reestablished and all symptoms for this scenario are eliminated.

Note If DECnet Phase IV Prime hosts are connected to your network, they will not be able to communicate with Cisco routers configured as DECnet Phase IV routers unless you upgrade the routers to Cisco Internetwork Operating System (Cisco IOS) Release 10.0, which supports DECnet Phase IV Prime.

Problem Solution Summary

This scenario focused on diagnosing blocked connectivity in DECnet internetworks. Three problems were discovered and resolved:

- Missing Level 2 router for an area
- End node number that was greater than maximum allowed on the router
- Token Ring encapsulation type mismatch

Figure 7-7 illustrates a complete configuration listing for Router-R4 as discussed in this scenario. In this configuration, the Token Ring encapsulation is set to the **pre-dec** option. Also note that bridging is configured on the Ethernet interfaces to support all nonroutable protocols (such as DEC Maintenance Operation Protocol [MOP], LAT, Local Area VAX Cluster [LAVC], and Local Area Disk Services [LAD]). This configuration also includes the change to increase the DECnet maximum address to 1023.

Figure 7-7 Complete DECnet Router-R4 Final Configuration

```
Current configuration:
version 9.1
!
hostname Router-R4
!
enable password sKrtalRt
!
decnet routing 10.200
decnet node-type area
decnet max-address 1023
!
interface ethernet 0
ip address 131.108.88.1 255.255.255.0
decnet cost 4
bridge-group 1
!
interface tokenring 1
ip address 131.108.101.18 255.255.255.0
decnet cost 4
decnet encapsulation pre-dec
!
interface ethernet 1
ip address 131.108.112.7 255.255.255.0
decnet cost 4
bridge-group 1
!
bridge 1 protocol dec
!
line aux 0
login
line vty 0 4
login
line con 0
exec-timeout 0 0
password WHiRLedPeAs
line aux 0
no exec
exec-timeout 0 0
password WHiRLedPeAs
line vty 0
exec-timeout 0 0
password WHiRLedPeAs
!
end
```

S2613

Configuring a DECnet Node to Log DECnet Events

In addition to the diagnostic tools available with your router, DECnet environments provide a wealth of diagnostic information. DECnet nodes can use the DECnet Event Logging Facility (EVL) to track DECnet events. EVL allows you to monitor significant network events, such as lost packets and circuit failures.

The following steps loosely outline the basic tasks required to enable event logging on a VMS system:

Step 1 Determine whether the Operator Communication Manager (OPCOM) process is running:

```
$ show system
```

Step 2 If OPCOM does not appear in the list of running processes, enter the following command to start it:

```
$ @sys$system:STARTUP.com OPCOM
```

Step 3 Use the Network Control Protocol (NCP) to enable event logging:

```
$ MCR NCP
NCP> SET logging MONITOR KNOWN Events
NCP> DEFINE logging MONITOR KNOWN Events
NCP> SET logging MONITOR STATE ON
NCP> DEFINE logging MONITOR STATE ON
```

Step 4 Exit NCP:

```
NCP> Exit
```

Step 5 To monitor network events from a console terminal, enter the following command at the VMS system prompt:

```
$ REPLY/ENABLE = NETWORK
```

(This command is equivalent to the **terminal monitor** privileged EXEC command.)

Note In some of the symptom discussions that follow, OPCOM messages are used to illustrate certain errors. These examples assume that OPCOM is running and event logging is enabled.

DECnet Connectivity Symptoms

The symptom modules in this section pertain to DECnet internetwork problems and cover the following topics:

- Connection Attempts to DEC Hosts Fail over Routers (Router Configuration)
- Connection Attempts to DEC Hosts Fail over Routers (End Nodes)
- End Nodes Cannot Find a Designated Router
- Router or End Node Sees Unexpected Designated Routers
- Intermittent DECnet Host Connectivity over Router
- Router Cannot Establish Adjacency with Another Router on the Same LAN
- No Phase IV Connectivity over Phase V Backbone
- Service Requests Are Aborted
- Routing Node Adjacencies Toggle Up and Down
- DECnet Phase IV Prime Host Cannot Communicate over Router

Note For more details about isolating problems for DECnet Phase V internetworks, see Chapter 9, "Troubleshooting ISO CLNS Connectivity."

Connection Attempts to DEC Hosts Fail over Routers (Router Configuration)

Symptom: DECnet nodes are unable to communicate when attempting to make connections over routers. This module focuses on possible causes related to router configuration. The next module, "Connection Attempts to DEC Hosts Fail over Routers (End Nodes)," addresses end node issues. Table 7-1 outlines possible causes and suggested actions when connection attempts to DEC hosts fail due to router configuration problems.

Table 7-1 DECnet: Connection Attempts to DEC Hosts Fail over Routers (Router Configuration)

Possible Causes	Suggested Actions
DECnet not enabled	**Step 1** Use the **write terminal** privileged EXEC command to determine whether appropriate DECnet global configuration and interface command specifications are included in the configuration of the router. **Step 2** Enable as required on router and interface.
End nodes not in the same area	**Step 1** Check the configuration for the address of the router. **Step 2** If end nodes are not in the same area, verify that routers with which these end nodes can communicate are able to reach a Level 2 router.
Actual cost to the destination area is more than the configured cost (Level 1 routers)	**Step 1** Use the **show decnet interface** EXEC command to determine the configured maximum cost. **Step 2** Use the **show decnet route** EXEC command to determine the actual cost to the destination. **Step 3** If the actual cost is more than the configured maximum cost, use the **decnet max-cost** global configuration command to increase the maximum cost.
Actual cost to the destination area is more than the configured cost (Level 2 routers)	**Step 1** Use the **show decnet interface** command to determine the configured maximum area cost. **Step 2** Use the **show decnet route** EXEC command to determine the actual cost to the destination area. **Step 3** If the actual cost is more than the configured cost, use the **decnet area-max-cost** global configuration command to increase the area maximum cost.
Actual number of hops to the destination is more than the configured maximum number of hops (Level 1 routers)	**Step 1** Use the **show decnet interface** command to determine the maximum number of hops allowed for intra-area routing. **Step 2** Use the **show decnet route** EXEC command to determine the actual number of hops to the destination as shown in the DECnet routing table. **Step 3** If the actual number of hops is more than the configured maximum allowed hops, use the **decnet max-hops** global configuration command to increase the maximum hops.

Possible Causes	Suggested Actions
Actual number of hops to the destination area is more than the configured maximum number of hops (Level 2 routers)	**Step 1** Use the **show decnet interface** command to determine the maximum number of hops configured for intra-area routing. **Step 2** Use the **show decnet route** EXEC command to determine the actual number of hops to the destination area as shown in the DECnet routing table. **Step 3** If the actual number of hops to an area is more than the configured maximum hops to an area, use the **decnet area-max-hops** global configuration command to increase the maximum number of hops.
Access list is improperly applied to DECnet interface	**Step 1** Use the **show decnet interface** EXEC command to determine whether an access list is set. **Step 2** If an access list is applied to the interface, use the **write terminal** privileged EXEC command to determine whether any access list entry in the list denies required access. **Step 3** Use the **debug decnet connects** privileged EXEC command to determine whether the relevant packets are being permitted. **Step 4** Use the **no decnet access-group** interface configuration command to disable the access list on the affected interface. **Step 5** Determine whether connectivity is restored. If so, the access list is probably the problem. **Step 6** Remove all the access list statements that apply to the interface, and use the **decnet access-group** interface configuration command to reenable the access control for the interface. **Step 7** Enter one access list statement, and test connectivity to the destination address. Repeat until connectivity is lost, at which point you have found the problem access list. **Step 8** Modify the access list as necessary.
Improperly enabled Address Translation Gateway (ATG)	**Step 1** Use the **show decnet map** EXEC command to determine whether address mapping is configured properly. **Step 2** If address mapping is not configured properly, modify mapping using the **decnet** *first-network* **map** *virtual-address second-network real-address* global configuration command.
Node address out of range	**Step 1** Use the **write terminal** privileged EXEC command to determine whether the DECnet maximum address has been set for any routers. **Step 2** Use the **decnet max-address** global configuration command to verify that the DECnet maximum address is 1023 (the default). If the node address is more than the **decnet max-address** value, increase the **decnet max-address** value.
Partitioned area	**Step 1** Review your network topology for any discontiguous areas. **Step 2** If any discontiguous areas exist, reconfigure the topology by changing area addresses or by adding a path (router) to create a contiguous network.

Connection Attempts to DEC Hosts Fail over Routers (End Nodes)

Symptom: Whenever a user attempts to connect to a DEC host over a router, the connection attempt fails. The previous module, "Connection Attempts to DEC Hosts Fail over Routers (Router Configuration)," focuses on issues relating to router configuration and implementation. This module focuses on possible causes associated with end nodes. Table 7-2 outlines possible causes and suggested actions when connection attempts to DEC hosts fail due to end node problems.

Table 7-2 DECnet: Connection Attempts to DEC Hosts Fail over Routers (End Nodes)

Possible Causes	Suggested Actions
Host access control rejects connection (Ultrix target system); user sees the following message: connect failed, access control rejected (typically a session layer problem)	**Step 1** Make sure that the following requirements are satisfied: User-supplied access control information is correct. Proxy access is set up correctly. Proxy database and proxy account are correct. **Step 2** Make sure that the user's security access matches the access specifications for the user on the remote systems. **Step 3** Make changes as necessary.
Unrecognized object (Ultrix target system); user sees the following message: connect failed, unrecognized object	**Step 1** Use the NCP **tell** command to determine whether the object is defined on the target node. The format of the **tell** command is as follows: **tell** *target-node-name* **show known** *objects* **Step 2** If the object is not defined, log in to the superuser account and run NCP to define the object with the NCP **set** command, as follows: **set object** *object-id* **Step 3** After the object is defined, use the NCP **tell** command to determine whether the object has a file specified: **tell** *target-node-name* **show object** *object-id* **character** **Step 4** Exit NCP and use the following command to determine whether the file specified for the object exists: **ls -l** **Step 5** If the file for the requested object does not exist, create the file. **Step 6** Make sure the protection for the specified file is correct. Example: # **chmod a+x /usr/etc/fal** # **chmod a+x /usr/etc**

Possible Causes	Suggested Actions
Insufficient resource error (VMS target system); VMS user sees the following message: % system-E-REMRSC, insufficient system resource at remote node (This error message may not indicate a problem. These parameter values can be set intentionally to prevent network connections beyond a certain number.)	**Step 1** Try tuning DEC target system parameters. SYSGEN parameters: - MAXPROCESSCNT NCP parameters: - MAXIMUM LINKS - ALIAS MAXIMUM LINKS AUTHORIZE parameters: - MAXJOBS - MAXACCTJOBS
Invalid login attempted	**Step 1** Determine whether access to a host is actually required. **Step 2** Ask the system manager at the target node to set up the user's account.

End Nodes Cannot Find a Designated Router

Symptom: When end nodes are unable to see a designated router, they cannot access any nodes that are on different LANs. Other nodes connected to the same LAN are accessible. Table 7-3 outlines possible causes and suggested actions when end nodes cannot find a designated router.

Table 7-3 DECnet: End Nodes Cannot Find a Designated Router

Possible Causes	Suggested Actions
DECnet not enabled on a router or not enabled on the interface	**Step 1** Use the **write terminal** privileged EXEC command to determine whether the router configuration includes the appropriate DECnet global configuration and interface command specifications. **Step 2** Enable DECnet as required on routers and interfaces.
Router not adjacent to the end node	**Step 1** At a router believed to be adjacent to the end node, use the **debug decnet packets** privileged EXEC command to determine whether hello packets are being exchanged between the end node and the router. If hello packets are not being exchanged, the router and the end node may not be adjacent. **Step 2** Make sure the router and end node are on the same LAN.
Routers and end node are not in the same area	**Step 1** Check DECnet addresses of the routers to determine whether they are in the same area. **Step 2** If not, use the **decnet routing** *decnet-address* global configuration command to reconfigure the appropriate routers to be in the same area.
Hello packets are not being exchanged	**Step 1** Use the **debug decnet packets** privileged EXEC command to determine whether the router is sending hello packets that are being received by the relevant end node. **Step 2** If no exchange is occurring, use the **show interfaces** command to determine whether the interface input and output queues are full. A full input queue is indicated by a value of 75/75, and a full output queue is indicated by a value of 40/40. **Step 3** If the queues are full and no hello packets are being exchanged, contact your router technical support representative.

Router or End Node Sees Unexpected Designated Routers

Symptom: If your network requires a specific router to be identified as the designated router, allowing another router to become a designated router can cause unpredictable network behavior and can block connectivity in and out of the area. Table 7-4 outlines possible causes and suggested actions when routers and end nodes see unexpected or incorrect designated routers.

Table 7-4 DECnet: Router or End Node Sees Unexpected Designated Routers

Possible Causes	Suggested Actions
Router is not adjacent to expected designated router	**Step 1** At a router believed to be adjacent to the expected designated router, use the **debug decnet packets** privileged EXEC command to determine whether hello packets are being exchanged between the routers. If hello packets are not being exchanged, the routers may not be adjacent. **Step 2** Make sure the router and end node are on the same LAN.
Priority of the expected designated router is not configured correctly	**Step 1** Use the **show decnet interface** EXEC command to determine which router is the designated router. Note the priority of the router. **Step 2** Use the **show decnet interface** command on the expected designated router and the actual designated router. Note the priority of the router. **Step 3** Compare the router priorities. The router that you want to be the designated router should have the highest priority. **Step 4** If a change is required, use the **decnet router-priority** interface configuration command to specify a particular router as the designated router.
Multiple routers have the same router priority	**Step 1** Use the **show decnet interface** command to determine which router is the designated router. **Step 2** Use the **show decnet interface** command on the expected designated router and the actual designated router. **Step 3** If the routers have the same priority, modify the configurations so that the router that is intended to be the designated router has the highest node number or router priority.
Adjacency with expected designated router is in a “down” or “initializing” state (adjacency between nodes is not bidirectional)	**Step 1** Use **debug decnet packets** privileged EXEC command to determine whether hello packets are being exchanged. **Step 2** If a router is not sending hello packets, use the **show interfaces** command to determine whether the interface input and output queues are full. A full input queue is indicated by a value of 75/75, and a full output queue is indicated by a value of 40/40. **Step 3** If the queues are full, and no hello packets are being exchanged, contact your router technical support representative. **Step 4** If routers are sending hello packets, contact end node administrators to determine why end nodes are rejecting hello packets.

Intermittent DECnet Host Connectivity over Router

Symptom: Connections sometimes drop unexpectedly, or hosts are sometimes inaccessible when connections are attempted over a router. Table 7-5 outlines possible causes and suggested actions for intermittent DECnet host connectivity over a router.

Table 7-5 DECnet: Intermittent DECnet Host Connectivity over Router

Possible Causes	Suggested Actions
Misconfigured router (timers improperly configured)	**Step 1** Use the **show decnet interface** EXEC command to verify that hello timers and routing update timers are consistent among all routers in the network. **Step 2** Use the **decnet hello-timer** and **decnet routing-timer** interface configuration commands to make any necessary configuration changes.
Disabled serial link or network media	**Step 1** Refer to the discussion of media problems in Chapter 2, "Troubleshooting Router Startup Problems," for a general discussion of media problems. **Step 2** Refer to Chapter 3, "Troubleshooting Serial Line Problems," for procedures that isolate serial interconnection problems.

Router Cannot Establish Adjacency with Another Router on the Same LAN

Symptom: Router will not establish adjacency with any other routers *known* to be on the same LAN. Table 7-6 outlines possible causes and suggested actions when a router cannot establish adjacency with another router on the same LAN.

Table 7-6 DECnet: Router Cannot Establish Adjacency with Another Router on LAN

Possible Causes	Suggested Actions
More than 32 routers on the network	**Step 1** Enable the **debug decnet routing** privileged EXEC command to determine whether the adjacency is being rejected. **Step 2** If the adjacency is being rejected, reduce the number of adjacent routers or change the priority of a router that you require to be adjacent so that it has a higher priority than one of the other neighboring routers. (Adjacency will be established with the target router instead of a router eliminated from the environment or assigned a lower priority.)
Node address out of range	**Step 1** Use the **write terminal** privileged EXEC command to determine whether the DECnet maximum address has been set for any routers. **Step 2** Use the **decnet max-address** global configuration command to verify that the DECnet maximum address is 1023 (the default). If the node address is higher than the **decnet max-address** value, increase the **decnet max-address** value.
Node area is more than **decnet max-area** configured	**Step 1** Use the **write terminal** privileged EXEC command to determine whether the DECnet maximum area has been set for any routers. **Step 2** Use the **decnet max-area** global configuration command to verify that the DECnet maximum area is more than the area of the node. If the area of the node is more than the **decnet max-area** value, the router will reset the adjacency.

No Phase IV Connectivity over Phase V Backbone

Symptom: Phase IV DECnet nodes are able to communicate with each other within a Phase IV area, but cannot access Phase IV nodes on the other side of a Phase V DECnet backbone. Table 7-7 outlines possible causes and suggested actions when there is no Phase IV connectivity over a Phase V backbone.

Table 7-7 DECnet: No DECnet Phase IV Connectivity over Phase V Backbone

Possible Causes	Suggested Actions
Misconfigured router (area addresses)	**Step 1** Enable the **debug clns packet** privileged EXEC command to determine whether packets are being converted and sent out to DECnet Phase V. **Step 2** Use the **write terminal** privileged EXEC command to verify that DECnet area address (specified by the **decnet routing** global configuration command) agrees with the CLNS area address (specified by the **network** router configuration command). (These addresses can be misconfigured easily. The area address for DECnet is specified in decimal, while the area address for CLNS is specified in hexadecimal.) **Step 3** If the area addresses do not agree, modify them as necessary.
Misconfigured router (ISO CLNS or DECnet not enabled on relevant interfaces)	**Step 1** Use the **write terminal** command to verify that DECnet and ISO CLNS are enabled on all interfaces where conversion will occur. **Step 2** Enable routing on relevant interfaces as necessary. (For DECnet, use the **decnet cost** interface configuration command; for ISO CLNS, use one of the valid variations of the **clns router** interface configuration commands.)

Service Requests Are Aborted

Symptom: When a node requests downline load services from a Maintenance Operation Protocol (MOP) server, a display similar to the following appears and repeats on the DEC system console:

```
%%%%%%%%%% OPCOM 30-JUN-1993 12:55:08.65 %%%%%%%%%%
Message from user DECNET on Wheel
DECnet event 0.7, aborted service request
From NODE 2.1 (Wheel), 30-JUN-1993 12:55:08.65
Circuit UNA-1, Line open error
```

The DEC node is unable to obtain its downline load from the MOP server. This symptom is commonly encountered by DEC terminal servers, MUX servers, and satellite nodes. Table 7-8 outlines a possible cause and suggested actions when service requests are aborted.

Table 7-8 DECnet: Service Requests Are Aborted

Possible Cause	Suggested Actions
Target system cannot locate matching hardware address, Ethernet address, or load file associated with node requesting service	**Step 1** At the DEC system console, look for an OPCOM message that indicates DECnet event 0.7. **Step 2** Check the node database on the MOP server for correct setup (proper hardware address, Ethernet address, and load file) for the requesting node. **Step 3** Add any missing information or correct errors in the database as needed. **Step 4** Power cycle the requesting node to determine whether it is able to obtain its downline load.

Routing Node Adjacencies Toggle Up and Down

Symptom: The following output appears repeatedly on the DEC system console:

```
%%%%%%%%%%% OPCOM 30-JUN-1993 1:25:07.45 %%%%%%%%%%%
Message from user DECNET on The Bay
DECnet event 4.16, adjacency rejected
From NODE 12.1 (The Bay), 30-JUN-1993 1:25:07.45
Circuit UNA-0, Adjacent node = 1.101 (Vax1)

%%%%%%%%%%% OPCOM 30-JUN-1993 1:25:07.46 %%%%%%%%%%%
Message from user DECNET on The Bay
DECnet event 4.15, adjacency up
From NODE 12.1 (The Bay), 30-JUN-1993 1:25:07.46
Circuit UNA-0, Adjacent node = 1.12 (Vax2)
```

In this example, the routers are constantly being added and removed from the routing table. Table 7-9 outlines possible causes and suggested actions when routing node adjacencies toggle up and down.

Table 7-9 DECnet: Routing Node Adjacencies Toggle Up and Down

Possible Causes	Suggested Actions
Hardware problem with routing node is causing a conflict between the designated router and another routing node	**Step 1** At the DEC system console, look for OPCOM message pairs that indicate DECnet events 4.16 (adjacency rejected) and 4.15 (adjacency up) for specific routing nodes. **Step 2** Find the routing node or nodes that are causing the adjacency to toggle. **Step 3** Troubleshoot the Ethernet cable or network interface card on the suspect nodes. (For details about isolating router hardware problems, refer to the hardware troubleshooting information in the "Troubleshooting Serial Line Problems" chapter.)
Total number of routing nodes in the network is more than 32	**Step 1** Enable **debug decnet routing** to determine whether the adjacency is being rejected. **Step 2** If the adjacency is being rejected, reduce the number of adjacent routers.

DECnet Phase IV Prime Host Cannot Communicate over Router

Symptom: End nodes attached to a Token Ring segment are unable to communicate with hosts on the other side of a router. These end nodes are PCs running Pathworks 4.1.a. The hosts on the other side of the router are Novell-based servers. Table 7-10 outlines a possible cause and suggested actions when a Phase IV Prime host cannot communicate over a router.

Note Pathworks 4.1.a enables DECnet Phase IV Prime by default.

Table 7-10 DECnet: DECnet Phase IV Prime Host Cannot Communicate over Router

Possible Cause	Suggested Actions
Router is unable to establish an adjacency with an end node	**Step 1** Upgrade to Cisco IOS Release 10.0, which supports DECnet Phase IV Prime.
	Step 2 If you cannot upgrade to Cisco IOS Release 10.0, disable DECnet Phase IV Prime on the end nodes. To disable DECnet Phase IV Prime on end nodes that are running Pathworks 4.1.a, add the following command to the DLCNDIS driver on each end node: **/P4P:N**
	Step 3 If the end nodes still cannot communicate with hosts over the router, contact your router technical support representative for assistance.

CHAPTER 8

Troubleshooting IBM Connectivity

This chapter focuses on a series of connectivity problems associated with routing and bridging in IBM-based networks, possible causes of those symptoms, and general suggestions for identifying, isolating, and resolving those causes.

This chapter consists of the following sections:

- Concurrent Routing and SRB Connectivity Scenario
- Translational Bridging, SRT Bridging, STUN, SDLC, and SDLLC Connectivity Scenario
- IBM Network and Token Ring Connectivity Symptoms
- Example STUN and SDLLC Diagnostic Sessions

The symptom modules consist of the following sections:

- Symptom statement—A specific symptom associated with IBM connectivity.
- Possible causes and suggested actions—A table for each symptom containing possible causes for the symptom and suggested actions for resolving each cause.

Note This chapter focuses on IBM-related and Token Ring problems. General diagnostic tools and techniques used for isolating serial line problems are discussed in the "Troubleshooting Serial Line Problems" chapter.

Concurrent Routing and SRB Connectivity Scenario

With multiprotocol internetworks, the chances of misconfiguration resulting in connectivity loss are substantially greater than with single-protocol networking environments. Along with the added efficiency and flexibility of multiprotocol internetworks comes an added level of management complexity.

The following connectivity-related scenario features both Novell and Sun networking systems sharing access to resources over Token Ring and serial media. This scenario illustrates problems facing internetworks characterized by concurrent bridging and routing.

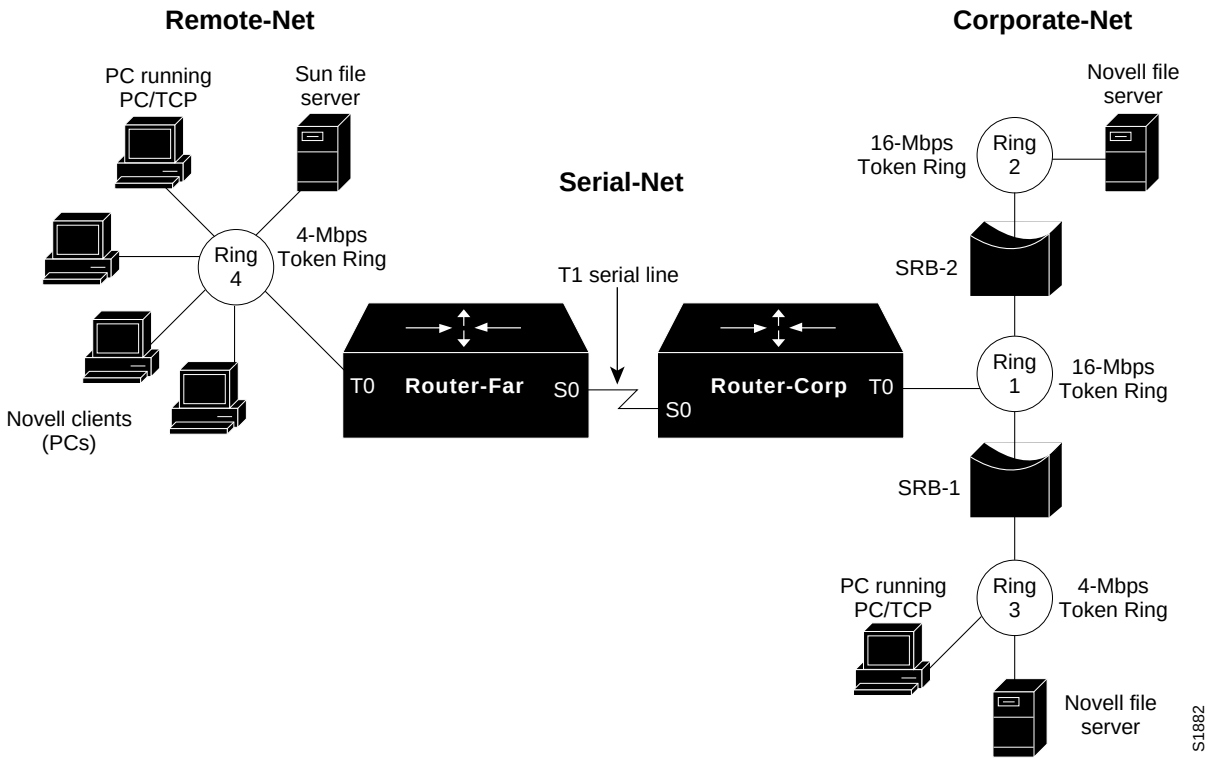
Symptoms

Consider a corporate network composed of Token Ring segments partitioned with source-route bridges (SRBs) as illustrated in Figure 8-1. Here, the personal computers (PCs) on Ring 4 are unable to connect to Novell servers on Rings 2 and 3, while a PC on Ring 3 cannot communicate with the Sun file server on Ring 4.

Environment Description

Figure 8-1 illustrates a map of the environment discussed in this case.

Figure 8-1 Initial SRB Problem Environment



The following summarizes the relevant elements of this internetworking environment:

- The primary corporate network (Corporate-Net) consists of one 4-Mbps and two 16-Mbps Token Rings separated by non-Cisco SRBs (SRB-1 and SRB-2).
- Users on the 4-Mbps Token Ring at a remote sales office (Remote-Net) are linked to the Corporate-Net over a T1 service (Serial-Net), with routers (Router-Corp and Router-Far) providing routing service for both TCP/IP and Novell IPX traffic between Corporate-Net and Remote-Net.
- The LANs are all IEEE 802.5 Token Rings.
- The network applications running over the WAN include X Windows, file transfer, mail, Novell NetWare file service, and virtual terminal connections.

Diagnosing and Isolating Problem Causes

Given the situation, the following possible problems are the most likely candidates for interconnection failure:

- Missing **multiring** interface configuration command
- Misconfigured IP network addresses
- No source-route bridging driver on a Novell server
- Software bug on some network device

The next step is to eliminate each potential cause as the problem source and then test the network to determine whether it is operational. The following discussion works through the process of problem isolation.

Finding Missing multiring Commands

Given the difficulties being experienced, router configuration problems are definite possibilities. In particular, if routed protocols are not making their way through an SRB environment, look for missing **multiring** interface configuration commands. The following steps outline actions to diagnose and remedy potential configuration problems in this kind of environment.

Step 1 Use the **write terminal** command on the two routers connected to the T1 serial line to look for a **multiring** interface configuration command for *each* routed protocol, or use the **all** keyword option (applied to the Token Ring interfaces). Note that the multiring command is only required when there are other SRB bridges on the LAN. Excessive use of multiring can lead to other problems.

Step 2 Assuming that the **multiring** command is not included or that it does not cover a particular protocol that is being routed and subsequently bridged as in this scenario, make any required changes. Figure 8-2 illustrates a specification of the **multiring** command that generates RIFs for IP frames, but not for Novell IPX frames. Refer to the *Router Products Configuration Guide* and *Router Products Command Reference* publications for more information about using the **multiring** command.

Figure 8-2 Example of Using the multiring Command

```
!
interface tokenring 0
multiring ip
ip address 131.108.2.4 255.255.255.0
ipx network 33                          S2614
!
```

Looking for a Misconfigured IP Address

The specification of IP network addresses is often the source of connectivity problems. An incorrect IP address can create a discontinuous network space, which results in a complete stoppage of all IP traffic at the point of discontinuity.

In this scenario, assume that Token Rings 1, 2, 3, and 4 are all configured for major net 131.108.0.0. The interfaces attached to the serial line linking the two sites are assigned IP addresses 192.1.100.1 (Router-Far) and 192.1.100.2 (Router-Corp). The discontinuity in this example results from the separation of segments in the same subnet (the four Token Rings) by a segment that belongs to a different major network (the serial network).

Step 1 Use the **write terminal** EXEC command to determine the address specifications associated with the Token Rings and serial lines to which the routers are attached.

Step 2 There are two solutions for this situation:

- Reconfigure the IP address assignments for the serial lines so that both interfaces attached to the link belong to the same major network as the Token Rings.
- Assign different network numbers to all three networks (Remote-Net, Serial-Net, and Corporate-Net).

Note For more information about assigning IP addresses and using subnet addressing, refer to the *Router Products Configuration Guide* and *Router Products Command Reference* publications.

Checking the End Systems

The end systems (PCs) attached to the various rings are another likely problem source in this scenario. The following steps outline actions to diagnose and remedy potential problems associated with the end systems in this kind of environment.

Step 1 Check the end systems for SRB drivers. Missing drivers might make end systems unable to participate in protocol exchanges.

Step 2 Reconfigure the end systems or replace them with systems that have the ability to handle SRB.

Step 3 In addition to missing SRB drivers, end systems may be unable to participate in protocol exchanges because of software problems. To isolate this problem in a TCP/IP environment, **ping** the end systems.

Step 4 If there is no response, the hardware address might be present. If so, the device was previously seen; if not, it was either never seen, or the entry timed out. Use the **show rif** and **show arp** EXEC commands to determine the hardware address of the end systems in the ARP and RIF tables. Figure 8-3 and Figure 8-4 illustrate the output of the **show rif** and **show arp** commands.

Figure 8-3 show rif EXEC Command Output

```
Codes: * interface, - static, + remote
Hardware Addr  How   Idle (min)  Routing Information Field
5C02.0001.4322 rg5           -   0630.0053.00B0
5A00.0000.2333 TR0           3   08B0.0101.2201.0FF0
5B01.0000.4444 -             -   -
0000.1403.4800 TR1           0   -
0000.2805.4C00 TR0           *   -
0000.2807.4C00 TR1           *   -
0000.28A8.4800 TR0           0   -
0077.2201.0001 rg5          10   0830.0052.2201.0FF0
```

S2398

Figure 8-4 show arp EXEC Command Output

```
Protocol  Address          Age (min)     Hardware Addr   Type      Interface
Internet  131.108.6.65           218     0000.0c02.710b  SNAP      Fddi0
Internet  131.108.6.69             -     0000.0c02.7aae  SNAP      Fddi0
Internet  131.108.134.69           -     0000.0c00.c0d3  ARPA      Ethernet1
Internet  131.108.181.69           -     0000.3040.e028  SNAP      TokenRing2
Internet  131.108.181.69         215     0000.3030.ee2b  SNAP      TokenRing2
```

S2399

Step 5 If the end system does not appear in the table, use the **clear rif-cache** and **clear arp-cache** commands. Be aware, however, that clearing caches causes network activity spikes while the caches are repopulated. If this high activity contributes to station problems, this might produce random results, which may be confusing to a user doing a "sample of one on a random result"—in other words, the station response gets lost and the user assumes it is still unavailable. Set the RIF timeout to a small value and **ping** the end system at intervals greater than the RIF timeout to see if the end system can respond.

Step 6 If the end system does not respond, use a network analyzer to look for the response of the end system to the Exchange ID (XID)-to-NULL SAP packet (DSAP value of 00) from the router.

The default timeout for Address Resolution Protocol (ARP) table entries is much larger than the Routing Information Field (RIF) entries (such as 4 hours for ARP and 15 minutes for RIF). The first time that a station is pinged, there are no ARP or RIF table entries for its hardware address, so both entries are updated with the ARP response from the end system. After the default timeout for RIF, the RIF entry is cleared, whereas the ARP entry remains. When this situation arises, if the end system is pinged again, the router generates an XID packet and sends it to the destination hardware address of the end system with a NULL SAP value (DSAP value of 00) to find the RIF.

Step 7 If you *do* see the router XID-to-NULL SAP packet, but the end system is unable to respond, there is probably a problem with the end system (host) SRB software, and you must upgrade the software on the end system.

(In one case, there was a bug in the IBM RS6000 where an RS6000 would not reply to an XID sent with a NULL SAP value.)

Note If an end system does not respond to the XID-to-NULL SAP packet (DSAP value of 00), and you are unable to upgrade its software, make the ARP time-out on the end system a little less than the RIF timeout. This setting causes the RIF and ARP to time out at about the same time and forces the routers to send an ARP instead of a XID-to-NULL SAP packet.

Resolving IP Cache Invalidations

Connectivity problems can be further complicated when the ARP cache contains so many entries that IP cache invalidations occur due to a constant stream of devices aging out. Any route change will result in a request to update the cache. If there are three or more simultaneous route-update requests for the cache, the Cisco device will invalidate the entire cache because doing so is faster than processing each one. The result is that each route that is invalidated (all of them in the case of three or more) will cause the next packet to be process switched and the route cache to be repopulated with up-to-date information.

The following steps outline actions to diagnose and remedy potential problems associated with the end systems in this kind of environment.

Step 1 Depending on the mix of network traffic, there will be a processor-load "spike" of random height and duration. The IP cache damping features may be used to reduce this effect in a LARGE routing table environment. In most corporate networks, the real cause of route flaps should be determined and overcome. In service provider environments with very large routing tables, it may be impossible to control the flapping route information received from outside sources; as a result, you might need to use the damping features (these are documented in the 10.2 manual). If you notice these symptoms, enable the IP cache damping features to extend the time at which devices time out (aging). To do so, enter the following command:

ip cache-invalidate-delay {20|60|30|50}

Step 2 Try using the **debug ip-icmp**, **debug arp** and **debug broadcast** commands.

Executing the **debug ip-icmp** command, in particular, can provide a quick indication on the health of your network. If you see time-to-live exceeded (TTL) messages, this is a sign that there are permanent or temporary routing loops in this network. If you see the router sending "redirects", end-stations might be responding improperly if the redirects are being constantly emitted toward one or more stations. Some users might constantly ping the routers as confirmation and reassurance that devices can be reached; unfortunately, this bogs down the routers with unnecessary overhead. In this case, you might want to ask users to limit their use of ping commands.

Execute the **debug arp** command to help you identify situations in which misconfigured end-stations are constantly running processes that attempt to reach non-existent (or powered-off) devices. These constantly running processes create a burden on the router, which must convert connection attempts into ARPs that are never answered. This also burdens all end-stations on the destination LAN with broadcast traffic, which must be evaluated and discarded

Execute the **debug broadcast** command after you check the relative broadcast "rate" on all interfaces of a router. After you enable debug broadcast, you can easily identify non-productive network traffic that is consuming bandwidth and router resources.

Step 3 Try using **egrep** on terminal output to quickly search for counts, errors, drops, and so forth.

Problem Solution Summary

Topics covered in this scenario addressed a number of common SRB and routing problems encountered in IBM internetworks. Procedures discussed included the following:

- Added missing **multiring** interface configuration commands to the Token Ring interfaces of interface of Router-Corp, as shown in Figure 8-1, to allow routing of protocols over multiple Token Rings in networks including SRBs.
- Ensured that the IP addressing of all interfaces created a contiguous network addressing scheme.
- Found and reconfigured or replaced Novell end systems that did not include SRB drivers.
- Used integrated router and third-party diagnostic tools to find software bugs on a network device.

Figure 8-5 and Figure 8-6 provide relevant configuration listings for Router-Corp and Router-Far. These configurations illustrate changes required to ensure proper RIF updating and a contiguous network addressing scheme.

Figure 8-5 Relevant Router-Corp Final Configuration

```
!Router-Corp configuration:
!
source-bridge ring-group 3
source-bridge remote-peer 3 tcp 150.136.139.1
source-bridge remote-peer 3 tcp 150.136.139.2
!
ipx routing 0000.3040.d065
!
interface serial 0
ip address 131.108.139.1 255.255.255.0
ipx network CC
!
interface tokenring 0
ip address 150.136.1.1
ring-speed 16
ipx network AA
source-bridge 1 2 3
source-bridge spanning
multiring ip
multiring ipx
!
```

S2615

Figure 8-6 Relevant Router-Far Final Configuration

```
!Router-Far configuration:
!
source-bridge ring-group 3
source-bridge remote-peer 3 tcp 150.136.139.1
source-bridge remote-peer 3 tcp 150.136.139.2
!
ipx routing 0000.3040.a043
!
!
interface serial 0
ip address 131.108.139.2 255.255.255.0
ipx network CC
!
interface tokenring 0
ip address 150.136.2.1
ring-speed 16
ipx network BB
source-bridge 4 5 3
source-bridge spanning
multiring ip
multiring ipx
!
```

S2616

Translational Bridging, SRT Bridging, STUN, SDLC, and SDLLC Connectivity Scenario

Cisco provides IBM connectivity options that range from support for source-route bridging (SRB) and source-route transparent (SRT) bridging to translational bridging and SDLC Transport over TCP/IP. Thus, network managers can tailor router configurations to the specific needs of existing networks and reconfigure routers to respond to network changes.

The scenario that follows illustrates some common pitfalls encountered in implementing internetworking solutions in complex IBM networks. This scenario focuses on potential problems associated with translational bridging, SRT bridging, serial tunneling (STUN), Synchronous Data Link Control (SDLC) Transport, and SDLC-to-Logical Link Control type 2 translation (SDLLC).

Symptoms

The large-scale corporate network illustrated in Figure 8-7 is composed of multiple Ethernet and Token Ring segments partitioned with SRBs, SRT bridges, a transparent bridge, and a translational bridge.

Connectivity problems on this network are as follows:

- Nonsource-route-capable end system (PC-2) on Ring 3 cannot communicate with either of the DEC Local Area Transport (LAT) Servers LAT-1 and LAT-2 on Ethernet 3 and Ethernet 1, respectively.
- Source-route-capable end system (PC-1) on Ring 3 cannot reach LAT-2 on Ethernet 1.
- IBM 3174 cluster controller (Cluster-2) attached to Router-5 cannot communicate with IBM 3745 front-end processor (FEP-2) attached to Router-4.
- IBM 3174 cluster controller (Cluster-1) cannot communicate with the IBM AS/400 attached to Ring 2.

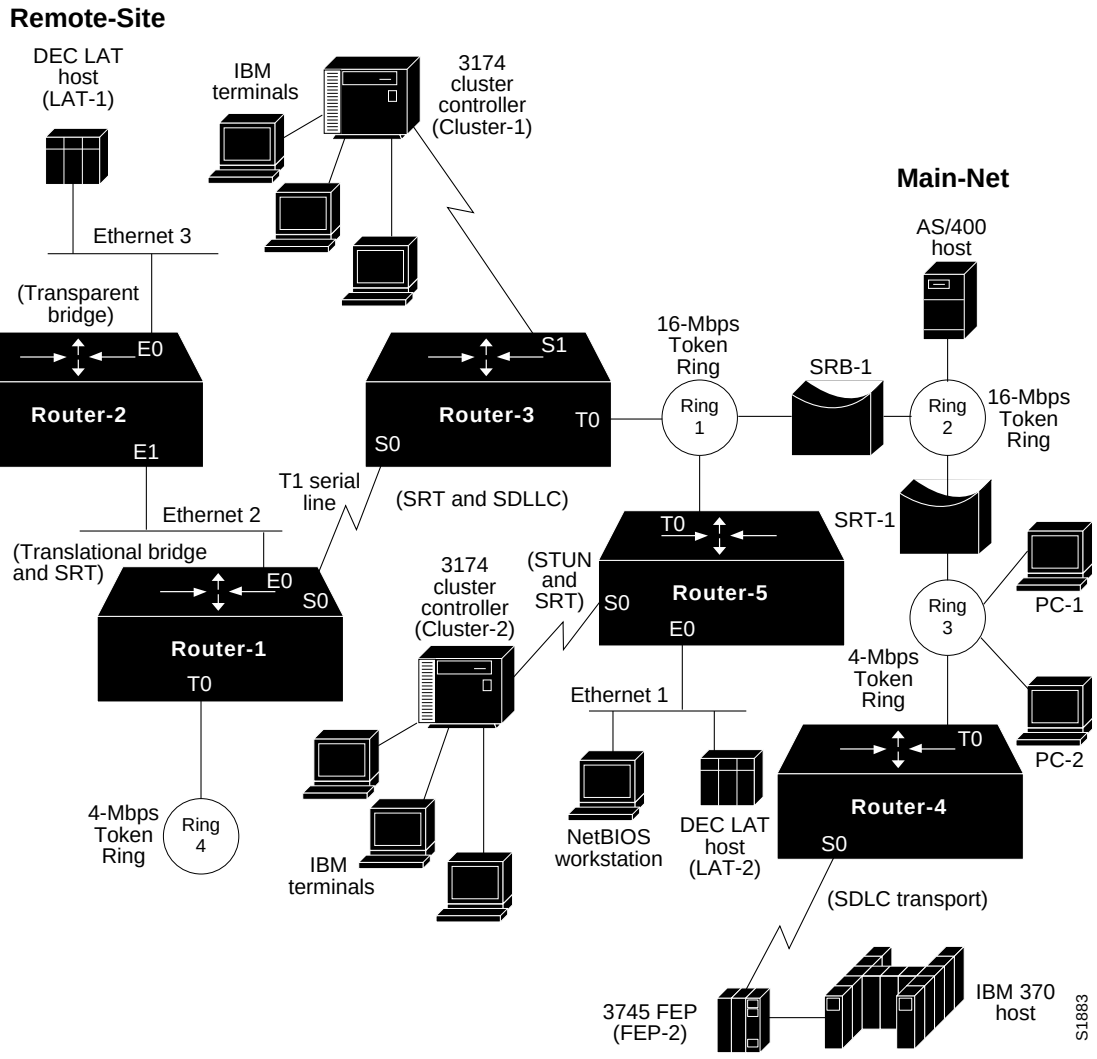
Environment Description

Figure 8-7 illustrates a map of the environment discussed in this scenario. The following summarizes the relevant elements of this internetworking environment:

- The corporate network (Main-Net) consists of an Ethernet and three Token Rings separated by both Cisco and non-Cisco internetworking devices.
- Remote-Site is interconnected via a T1 serial link between Router-1 and Router-3. Remote-Site includes two Ethernets (Ethernet 2 and Ethernet 3) and a single Token Ring.
- Cisco devices are configured as follows: Router-5 is configured for SRT bridging and STUN; Router-4 is configured for SDLC Transport; Router-3 is configured for SRT bridging and SDLLC; Router-1 is configured for translational bridging and SRT bridging; and Router-2 is configured for transparent bridging only.
- Non-Cisco internetworking devices at Main-Net are as follows: a source-route bridge (SRB-1) connects Ring 1 and Ring 2 and an SRT bridge (SRT-1) connects Ring 2 and Ring 3.
- Token Ring LANs are 4-Mbps and 16-Mbps, IEEE 802.5 compliant; Ethernets are IEEE 802.3 compliant.

- All the serial links from FEPs and cluster controllers to Cisco routers are 56-Kbps SDLC lines.
- The network applications running over the WAN include file transfer, mail, Novell, and both DEC LAT and IBM 3270 terminal connections.
- Other protocols can be routed within this environment, but the focus in this scenario is on mixed-technology bridging issues.

Figure 8-7 Initial IBM Internetwork Problem Environment



Diagnosing and Isolating Problem Causes

Before attempting to define a specific problem, it is important to identify the most likely causes and to then *systematically* eliminate each one. Given the situation, the following problems are the best candidates for interconnection failures:

- Incompatibilities between end systems and intermediate systems in mixed-media, multiprotocol environment.
- Packets with RIF being dropped by SRT bridges attached to Ethernets.

- Missing **ethernet-transit-oui** command.
- Missing **multiring** commands. Multiring is not needed in Router-[1|2].
- Missing **sdllc partner** or **sdllc xid** commands in SDLC-to-LLC translation configuration.

The next step is to eliminate each potential cause as the problem source and then test the network to determine whether it is operational. The following discussion works through the process of problem isolation.

Detecting Incompatibilities between End Systems and Intermediate Systems

In the first symptom, PC-2 is unable to access either of the target DEC LAT servers (LAT-1 and LAT-2). With an SRB in the path to both, PC-2 *itself* becomes a suspect. In particular, its ability to support SRB is in question. The following steps suggest ways to determine whether the system is source-route capable:

Step 1 Place a network analyzer on Ring 3 (the same ring to which end system PC-2 is connected).

Step 2 Look for any frames sent by the end system (PC-2) with the high-order bit of the source address set to 1. Figure 8-8 illustrates output from the network analyzer, with the high-order bit of the source address set to 1.

Figure 8-8 Output from a Network Analyzer Showing SRB-Capable End System Source Address

```
- - - - - - - - - - - - - - - - - - Frame 4 - - - - - - - - - - - - - - - - - -

SUMMARY  Delta T     Destination     Source        Summary
4        1.686       NetBIOS         VELA(00)      NETB Check name WWONG CISCO4

NETB: ----- NETBIOS Add Name Query -----
NETB:
NETB: Header length = 44, Data length = 0
NETB: Delimiter = EFFF (NETBIOS)
NETB: Command = 01
NETB: Response correlator = 0008
NETB: Name to be added = WWONG   CISCO4
NETB:

ADDR: HEX                                                  ASCII
0000  01 40 C0 00 00 00 00 80  90 00 5A DE 0D 8A C8 00  .@........Z.....
0010  00 11 00 A1 00 20 F0 F0  03 2C 00 FF EF 01 00 00  ..... ...,......
0020  00 00 00 08 00 00 00 00  00 00 00 00 00 00 00 00  ................
0030  00 00 00 00 00 57 57 4F  4E R7 20 20 20 43 49 53  .....WWONG   CIS
0040  43 4F 34 20 20                                   CO4
```

Hex value of 90 is binary 1001 0000—indicating that the high-order bit of the source address is set to 1

S2511

Step 3 If you cannot find a frame with the high-order bit of the source address set to 1, the end system does not support RIF and is not able to participate in source routing.

Step 4 If the end system supports source routing, replace SRB-1 with an SRT bridge to get its traffic through to LAT-1 and LAT-2. This network change is addressed later as part of a comprehensive solution; see Figure 8-10 for a revised map and a description of the network changes involved.

Note Make sure the end system (PC-2) is configured to point to the hardware addresses for servers on Ethernet (LAT-1 or LAT-2).

Detecting SRT Bridging/SRB Incompatibilities

In symptom number 2, PC-1 (which is SRB-capable) on Ring 3 can talk to DEC LAT server LAT-1, but cannot talk to DEC LAT server LAT-2. As with the preceding problem, the key here rests with technology differences between the internetworking devices in the path to the servers and the end system trying to make a connection.

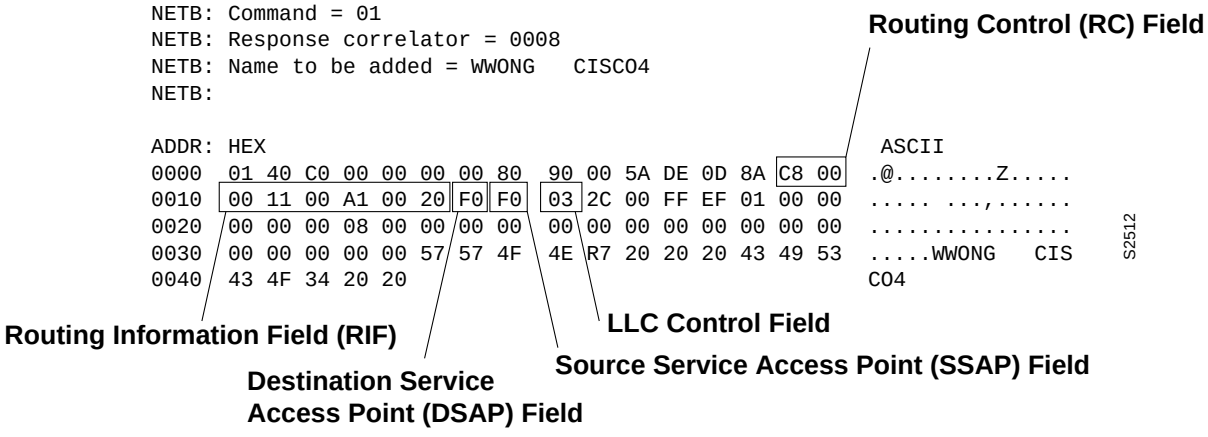
The likely stopping point for traffic in this case is Router-5, which is configured as an SRT bridge. Because Router-5 is attached to both a Token Ring and an Ethernet segment (and is configured for SRT bridging), it discards packets that include RIF data. Determine whether the end system (PC-1) is source-route capable. The steps to remedy this problem are analogous to the prior procedure, with some slight differences:

Step 1 Place a network analyzer on Ring 3 (the same ring to which end system PC-1 is connected).

Step 2 Look for frames sent by the end system (PC-1) with the RIF present. Figure 8-9 illustrates output from the network analyzer with RIF present.

Figure 8-9 Output from the Network Analyzer Showing an End System Packet with RIF

```
- - - - - - - - - - - - - - - - - Frame 4 - - - - - - - - - - - - - - - - -

SUMMARY  Delta T     Destination     Source        Summary
4        1.686       NetBIOS         VELA(00)      NETB Check name WWONG CISCO4

NETB: ----- NETBIOS Add Name Query -----
NETB:
NETB: Header length = 44, Data length = 0
NETB: Delimiter = EFFF (NETBIOS)
NETB: Command = 01
NETB: Response correlator = 0008
NETB: Name to be added = WWONG   CISCO4
NETB:

ADDR: HEX                                                    ASCII
0000  01 40 C0 00 00 00 00 80  90 00 5A DE 0D 8A C8 00  .@........Z.....
0010  00 11 00 A1 00 20 F0 F0  03 2C 00 FF EF 01 00 00  ..... ...,......
0020  00 00 00 08 00 00 00 00  00 00 00 00 00 00 00 00  ................
0030  00 00 00 00 00 57 57 4F  4E R7 20 20 20 43 49 53  .....WWONG   CIS
0040  43 4F 34 20 20                                   CO4
```



Step 3 If you find a frame with the high-order bit of the source address set to 1 (see Figure 8-8), PC-1 is source-route capable. The RIF illustrated in Figure 8-9 specifies that the frame came from Ring 001 (hexadecimal) over bridge 1 (hexadecimal), through Ring 00A (hexadecimal) over bridge 1 (hexadecimal) to Ring 002 (hexadecimal). Note that Bridge 0 *is* valid though not often seen.

Step 4 In this case, an end system with a RIF *is a problem*. When Router-5 sees the RIF in packets sent from PC-1, it will drop those packets rather than put them on the Ethernet interface.

Step 5 To get traffic from PC-1 through to LAT-2, you can enable translational bridging on Router-5 or replace SRB-1 with an SRT bridge. This network change is part of a comprehensive solution described in the section "Problem Solution Summary," later in this chapter.

Note Make sure the end system (PC-1) is configured to point to the hardware addresses for servers on Ethernet (LAT-1 or LAT-2) in order to be able to listen to their service advertisements.

Resolving Vendor Code Mismatch Problems

Older Token Ring implementations, such as the IBM 8209, expect the vendor code (OUI) field of the SNAP header to be 000000. Cisco routers modify this field to be 0000F8 to specify that the frame was translated from Ethernet Version 2 to Token Ring. Cisco's modification of this field can cause end systems that expect the SNAP header to be 000000 to drop packets. The **ethernet-transit-oui** interface configuration command forces the router to make the vendor code field 000000.

To determine whether you need to add the **ethernet-transit-oui** interface configuration command to the configuration of a router, follow these steps:

Step 1 On the router acting as a translational bridge (Router-1), use the **write terminal** EXEC command and look for the **ethernet-transit-oui** interface configuration command.

Step 2 If the **ethernet-transit-oui** interface configuration command is not present and if frames are getting through the translational bridge, but some workstations are dropping packets, specify the **ethernet-transit-oui** interface configuration command on Router-1. This command forces the router to make the vendor code field 000000.

For more information, refer to the *Router Products Configuration Guide* and *Router Products Command Reference* publications.

Finding Missing multiring Commands

If routed protocols are not making it through an environment consisting of SRBs, look for missing **multiring** Token Ring interface configuration commands.

Symptom number 3 is a 3174 cluster controller (Cluster-2) that cannot communicate with FEP-2. In this scenario, SDLC Transport (tunneling) is implemented via IP encapsulation. This configuration suggests that Router-4 or Router-5 is missing the **multiring** interface configuration command, which is required as a result of routing between Router-4 and Router-5.

The following steps outline actions for determining whether you should add the multiring interface configuration command to the configuration of a router:

Step 1 Use the **ping** EXEC command to determine whether Router-5 can communicate with Router-4.

Step 2 Use the **write terminal** EXEC command (on Router-4 and Router-5) to look for a **multiring** interface configuration command that includes the **ip** keyword option, or the **all** keyword option, for the Token Ring interfaces.

Step 3 Assuming that the **multiring** command is not included or does not cover a particular protocol that is being routed (and subsequently bridged over the SRB as in this scenario), you can add the **multiring ip** command to Router-4 (Token Ring interface T0) and Router-5 (Token Ring interface T0), as illustrated in Figure 8-7.

Step 4 Another option is to reconfigure to eliminate this problem. See Figure 8-10 for a revised map and a description of the network changes involved. Removing SRB-1 and SRT-1 remedies the problem without requiring the addition of the **multiring ip** command.

Enabling Access to the AS/400 on Ring 2

The last symptom in the scenario is the 3174 cluster controller (Cluster-1) that cannot communicate with the AS/400 host that is directly attached to Ring 2. The following procedure isolates and suggests ways to resolve this problem:

Step 1 Place a network analyzer on Ring 1 (the same ring to which Router-3 is connected), or use the **debug sdllc** EXEC command on Router-3.

Step 2 Determine whether Router-3 is generating explorer packets for the AS/400.

Step 3 If Router-3 is not generating explorer packets for the AS/400, check its configuration for inclusion of the **sdllc partner** interface command and **sdllc xid** interface configuration command.

Step 4 If not present, add the **sdllc partner** and **sdllc xid** commands. These commands force the router to generate explorer packets.

Problem Solution Summary

Several of the solutions in this scenario pointed to a redesign of the original network as illustrated in Figure 8-7. Figure 8-10 presents a suggested reconfiguration of the internetwork. The modification includes the replacement of SRB-1 and SRT-1 by an AGS+ Cisco router and the implementation of SRT bridging on all Main-Net Token Ring links.

This scenario addressed a number of common problems encountered in complex IBM internetworks. The solutions included the following:

- Resolving SRB-related and SRB/SRT bridging technology conflicts by replacing SRT-1 and SRB-1 with an AGS+ router (Router-4).
- Using third-party diagnostic tools to isolate problems based on traffic occurring on a network.
- Adding a missing **ethernet-transit-oui** command to applicable configurations to resolve vendor code mismatch problems (Router-1, global configuration change).
- Adding missing **sdllc partner** commands in SDLLC configurations (Router-3, interface Serial1).

Figure 8-10 Reconfigured IBM Internetwork Environment

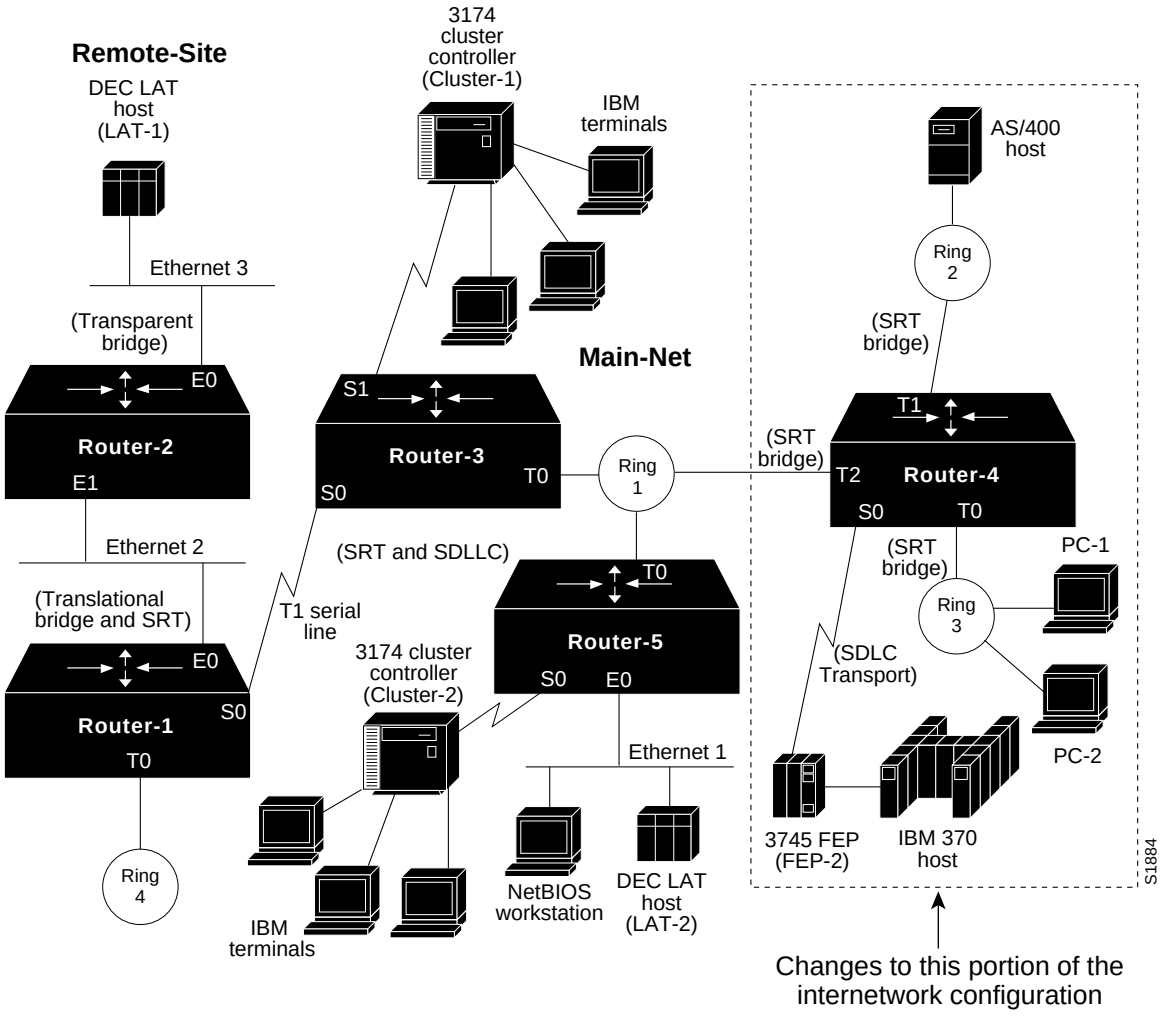


Figure 8-11 through Figure 8-14 provide the complete, final configuration listings for the key routers discussed in this scenario.

Figure 8-11 Relevant IBM Router-1 Final Configuration Listing

```
!
!
source-bridge ring-group 10
source-bridge remote-peer 10 tcp 131.108.1.1
source-bridge remote-peer 10 tcp 131.108.1.2
source-bridge remote-peer 10 tcp 131.108.2.2
source-bridge transparent 10 5 1 1
!
!
interface tokenring 0
ethernet-transit-oui standard
no ip address
ring-speed 16
source-bridge 4 1 10
source-bridge spanning
multiring all
bridge-group 1
!
!
interface ethernet 0
no ip address
bridge-group 1
!
interface serial 0
ip address 131.108.1.1 255.255.255.0
bridge-group 1
!
!
router igrp 109
network 131.108.0.0
!
ip name-server 255.255.255.255
snmp-server community
bridge 1 protocol ieee
!
```

S2617

Figure 8-12 Relevant IBM Router-3 Final Configuration Listing

```
!
!
source-bridge ring-group 10
source-bridge remote-peer 10 tcp 131.108.1.1
source-bridge remote-peer 10 tcp 131.108.1.2
!
!
!
interface tokenring 0
no ip address
ring-speed 16
source-bridge 1 1 10
source-bridge spanning
bridge-group 1
!
!
interface serial 0
ip address 131.108.1.2 255.255.255.0
bridge-group 1
!
!
interface serial 1
no ip address
encapsulation sdlc-primary
sdlc address c1
sdllc traddr 0110.2222.3300 8 1 10
sdllc partner 0000.2000.0400 c1
!
!
router igrp 109
network 131.108.0.0
!
ip name-server 255.255.255.255
snmp-server community
bridge 1 protocol ieee
!
```

S2618

Figure 8-13 Relevant IBM Router-4 Final Configuration Listing

```
stun peer-name 131.108.2.2
stun protocol-group 1 sdlc
!
!
source-bridge ring-group 10
source-bridge remote-peer 10 tcp 131.108.1.1
source-bridge remote-peer 10 tcp 131.108.2.2
!
!
interface tokenring 0
no ip address
ring-speed 16
source-bridge 3 1 10
source-bridge spanning
multiring all
bridge-group 1
!
interface tokenring 1
no ip address
ring-speed 16
source-bridge 2 1 10
source-bridge spanning
bridge-group 1
!
interface tokenring 2
ip address 131.108.2.2 255.255.255.0
ring-speed 16
source-bridge 1 2 10
source-bridge spanning
bridge-group 1
!
interface serial 0
encapsulation stun
no ip address
no keepalive
stun group 1
stun route address c2 tcp 131.108.2.3
!
!
router igrp 109
network 131.108.0.0
!
ip name-server 255.255.255.255
snmp-server community
bridge 1 protocol ieee
!
```

Figure 8-14 Relevant IBM Router-5 Final Configuration Listing

```
stun peer-name 131.108.2.3
stun protocol-group 1 sdlc
!
source-bridge ring-group 10
!
!
interface tokenring 0
ip address 131.108.2.3 255.255.255.0
ring-speed 16
bridge-group 1
!
interface ethernet 0
no ip address
bridge-group 1
!
interface serial 0
encapsulation stun
no ip address
no keepalive
stun group 1
stun route address c2 tcp 131.108.2.2
!
!
ip name-server 255.255.255.255
snmp-server community
bridge 1 protocol ieee
```

S2416

IBM Network and Token Ring Connectivity Symptoms

The symptom modules that follow pertain to IBM internetworking problems. There are modules for the following topics:

- Router Is Unable to Connect to Token Ring
- Routing Does Not Function in SRB Environment
- Routing in SRB Network Fails Unexpectedly
- No Communication over SRB
- Blocked Communication over Remote SRB
- Intermittent Communication Failures over Remote SRB
- NetBIOS Clients Cannot Connect to Servers over Remote SRB
- Users Cannot Communicate over Cisco Translational Bridge
- Traffic Cannot Get through Router Implementing SRT Bridging
- Intermittent Connectivity over Router Configured for SDLC
- Router Is Not Communicating with IBM SDLC Devices over EIA/TIA-232
- SDLC Sessions Fail over Router Running STUN
- Users Cannot Make Connections over Router Configured for SDLLC
- Router Cannot Be Linked from LAN Network Manager

Router Is Unable to Connect to Token Ring

Symptom: When installing a new router in a Token Ring environment, you find that the router will not connect to the ring. Table 8-1 outlines possible causes and suggested actions when a router fails to connect to a Token Ring.

Table 8-1 IBM: Router Is Unable to Connect to Token Ring

Possible Causes	Suggested Actions
Relay open in MAU	**Step 1** If, at system power-on, an "open lobe fault" message appears on the console (or VTY) connected to the router, check the cable connection to the Multistation Access Unit (MAU). **Step 2** Use the **clear interface** privileged EXEC command to reset the Token Ring interface and reinsert the router into the ring. For all Token Ring cards except the CTR and low-end routers, you must use the **clear interface** command to reinitialize the Token Ring interface if the interface is down. **Step 3** Use the **show interfaces token** EXEC command to verify that the interface and line protocol are up. **Step 4** If the interface is operational, but the "open lobe fault" message persists, and the router continues to be unable to connect to its ring, connect the router to a different MAU port. **Step 5** If the "open lobe fault" message continues to appear, disconnect all devices from the MAU and reset the MAUs relay with the tool provided by the MAU vendor. **Step 6** Reattach the router and determine whether it can connect to the ring. If resetting the relay does not remedy the problem, try replacing the MAU with one that is known to be operational. **Step 7** If the router is still unable to connect to the ring, check internal cable connections of the router Token Ring cards. Ensure that cables associated with the respective port numbers and applique numbers are correctly wired and that they are not swapped. **Step 8** If the router still cannot connect to the ring, replace the cables that connect the router to the MAU with working cables. **Step 9** Use the **clear interface** command to reset the interface and reinsert the router into the ring. Use the **show interfaces token** command to verify that the interface and line protocol are up. **Step 10** Alternatively, you can connect the router to a spare MAU to which no stations are connected. If the router is able to attach to the ring, the original MAU should be replaced.
Duplicate Media Access Control (MAC) address	**Step 1** Use a network analyzer to check all MAC addresses of stations on the ring. **Step 2** Change a MAC address by reinitializing one of the nodes that has a duplicate address. (This problem arises when routers attempt to generate a MAC address.)
LAN Network Manager (LNM) is blocking insertion	**Step 1** Disable LNM on the ring. **Step 2** Retry inserting the router into ring. **Step 3** If you are able to insert the router into the ring after disabling LNM, reconfigure your LNM table to include the address of the router as needed.

Possible Causes	Suggested Actions
Congested ring	**Step 1** Insert the router during an off-peak period. **Step 2** If insertion is successful during off-peak periods, but unsuccessful during peak load, segment your internetwork to distribute traffic.
Ring Parameter Server (RPS) conflict	**Step 1** Use the **no lnm rps** interface configuration command to disable the RPS function on the router that you are attempting to insert into the ring. **Step 2** Retry inserting the router into the ring. **Step 3** If you can insert the router with RPS disabled, a conflict exists between RPS implementations. Contact your router technical support representative for more information.
Bad ring speed specification	**Step 1** Use the **show interfaces token** EXEC command to determine the status of the interface. **Step 2** If status line indicates that the interface and line protocol are not up, check the cable from router to the MAU. Make sure that the cable is good; replace if necessary. **Step 3** If the **show interfaces token** EXEC command indicates that the interface and line protocol are up, use the **ping** command between routers to test connectivity. **Step 4** If the remote router does not respond, check the ring speed specification on all of the nodes that are attached to the Token Ring backbone. The ring speed for all of the nodes must be the same. (Ring speed conflicts cause the ring to beacon.) **Step 5** Modify ring speed specifications for clients, servers, and routers as necessary. For routers that support setting the ring speed in software, use the **ring-speed** interface configuration command. Change jumpers as needed for modular router platforms. For more information about ring speed specification, refer to the hardware installation and maintenance manual for your system.

Routing Does Not Function in SRB Environment

Symptom: SRBs are bridging traffic as they should, but routed protocols are not getting through a router. If this symptom occurs, you *must* route certain protocols (for example, Novell IPX) through an internetwork that is dominated by SRB links. Table 8-2 outlines a possible cause and suggested actions when routing does not function in an SRB environment.

Table 8-2 IBM: Routing Does Not Function in SRB Environment

Possible Cause	Suggested Actions
Misconfigured router; routing a protocol and attempting to communicate with host on another ring across an SRB bridge	**Step 1** Check the configuration for inclusion or absence of a **multiring** *protocol-name* interface configuration command. **Step 2** Add a **multiring** *protocol-name* interface configuration command to the router configuration if it is missing. **Step 3** For IP networks, make sure that the end system is pointing to the Token Ring address of the router as the default gateway. If a UNIX host is running *routed*, check its default routes. **Step 4** Determine whether a host can respond using the **ping** command. If it does not respond, use the **show arp** EXEC command to determine whether an entry for the host exists in the ARP table. If an entry exists, use the **show rif** EXEC command to match the RIF with the hardware address of the host. **Step 5** Try the steps outlined in the next symptom module, "Routing in SRB Network Fails Unexpectedly." **Step 6** Contact your router technical support representative if you still cannot get traffic intended to be routed to transit the router.

Note For illustrations and additional context-related information, refer to the section "Concurrent Routing and SRB Connectivity Scenario" earlier in this chapter.

Routing in SRB Network Fails Unexpectedly

Symptom: Routing is working in an environment dominated by SRB links, then halts without any known administrative changes in the network. Table 8-3 outlines a possible cause and suggested actions when routing in an SRB network fails unexpectedly.

Table 8-3 IBM: Routing in SRB Network Fails Unexpectedly

Possible Cause	Suggested Actions
Software bug in the end system software	**Step 1** Use the **show interfaces** EXEC command to determine whether the protocol is up. If the protocol is up, and the 5-minute input/output rate has not dropped to zero, and there are no input or output errors, check the ring status.
	Step 2 If the last ring status line shows a soft error, use the **show controllers token** EXEC command to determine whether there have been any line or burst errors on the ring. If no errors appear, skip the next step.
	Step 3 Place a network analyzer on the ring to determine which node is injecting errors into the ring. Contact your router technical support representative for additional assistance.
	Step 4 Use the **show rif** EXEC command to determine whether the MAC address for an end system is missing from the RIF table.
	Step 5 If a MAC address for an end system is missing, issue the **clear rif-cache** and **clear arp-cache** privileged EXEC commands. Then **ping** the end system to determine whether it can respond.
	Step 6 If the end system does not respond, use a network analyzer to look for XID-to-NULL SAP packets (LSAP value of 00) sent by the router to the end system. The XID-to-NULL SAP packets are generated when the router's RIF entry for a workstation ages out, and the RIF table is being updated. If you see the XID packet and the end system does not reply, there is probably a bug in the end system software.
	Step 7 Upgrade your host software or contact your end system technical support representative for more assistance.
	Step 8 If you do not see the XID packet, or if the station replies but you still cannot establish communication, contact your router technical support representative.
	Step 9 If the MAC address of the end system is present in the RIF table, use the **show arp** EXEC command to examine the ARP cache. If the IP address of the end system is not in the ARP cache, there probably is a problem with IP rather than with the SRB path to the router.
	Step 10 As a last resort, enable the **debug token ring** privileged EXEC command. This command can provide useful information, but generates traffic that can break poorly performing networks. Use this command with great care.

No Communication over SRB

Symptom: A router configured to operate as an SRB that connects two or more Token Rings is not forwarding SRB traffic. Table 8-4 outlines possible causes and suggested actions when no communication is occurring over an SRB.

Table 8-4 IBM: No Communication over SRB

Possible Causes	Suggested Actions
Misconfigured router; ring number mismatch	**Step 1** Get the ring number (specified in hexadecimal) from IBM SRBs. **Step 2** Use the **write terminal** privileged EXEC command to look for the **source-bridge** *local-ring bridge-number remote-ring* interface configuration command that assigns ring numbers (displayed in decimal) to the rings that are connected to the router's interfaces. (Although you can enter the ring number in hexadecimal or decimal, it always appears in the configuration as a decimal number. Also note that parallel bridges situated between the same two rings must have different bridge numbers.) **Step 3** Convert IBM SRB ring numbers to decimal and verify that the ring numbers for all internetworking nodes agree. **Step 4** If the ring numbers do not agree, reconfigure the router's interface so that its ring number matches the IBM SRB. **Step 5** If you still cannot communicate over the SRB, contact your technical support representative.
End system does not support RIF	**Step 1** Place a network analyzer on the same ring to which the end system is connected. **Step 2** Look for any frames sent from the end system with the first bit of the source MAC address set to 1. Refer to the section entitled "Translational Bridging, SRT Bridging, STUN, SDLC, and SDLLC Connectivity Scenario" earlier in this chapter for illustrations and additional context-related information. **Step 3** If no such frames are found, the end system does not support RIF and is not able to participate in source routing. **Step 4** If the protocol is routable, you can configure the router to act as an SRT bridge and route the protocol. **Step 5** If your environment requires SRB, contact your workstation or server vendor for SRB drivers or for information about setting up SRB on your workstation or server.

Possible Causes	Suggested Actions
End system configured to send spanning explorers, but router not configured to forward them (A spanning explorer is equivalent to a single-route broadcast.)	**Step 1** Place a network analyzer on the same ring to which the end system is connected. **Step 2** Look for any frames sent from the end system with the first bit of the source address set to 1. **Step 3** If such frames are found, determine whether the frames are spanning all-ring frames (that is, the first two bits are set to 1). **Step 4** If you find spanning all-ring frames, determine whether the router is configured to forward spanning explorers (using the **source-bridge spanning** interface configuration command). **Step 5** If necessary, add the **source-bridge spanning** interface configuration command to any router that is required to pass spanning explorers. **Step 6** Use the **show source-bridge** EXEC command to determine whether the explorer count is incrementing. **Step 7** If sessions still cannot be successfully established over the SRB, contact your technical support representative for more assistance.

Blocked Communication over Remote SRB

Symptom: Users are unable to communicate over a remote SRB. As a remote SRB, a router uses encapsulated Token Ring packets to allow interconnection of Token Ring networks over any non-Token Ring media type (such as a Fiber Distributed Data Interface [FDDI] backbone, point-to-point serial lines, or a packet-switched network). Table 8-5 outlines possible causes and suggested actions when communication over a remote SRB is blocked.

Table 8-5 IBM: Blocked Communication over Remote SRB

Possible Causes	Suggested Actions
Misconfigured **source-bridge remote-peer** global configuration commands on the router	**Step 1** Use the **write terminal** privileged EXEC command to verify that the **source-bridge remote-peer** command is pointing to the correct IP address on each router. **Step 2** Modify configuration as required. **Step 3** Use the **show source-bridge** EXEC command to check for the existence of remote peers.
End system does not support RIF	**Step 1** See Table 8-4 for suggested actions.
Hop count exceeded	**Step 1** Use the **show** *protocol* **route** command to check the hop count values on the routers and other bridges in the path. **Step 2** Alternatively, you can enable the **debug source event** privileged EXEC command to see whether packets are being dropped because the hop count has been exceeded.
No route to the remote peer (TCP/IP encapsulation)	**Step 1** Check the result of the **show ip route** EXEC command. If a route to the intended remote peer is not included in the list, create a route or check the state of devices and cabling in the path to the remote peer. **Step 2** Verify IP connectivity; try to **ping** from the router to the remote peer IP address. If the remote peer does not reply, the SRB frames cannot get through. If it does reply, IP routing is operational.
Serial link problem	**Step 1** Use the **show interfaces** EXEC command to verify that the interface and line protocol are up. Refer to Chapter 3, "Troubleshooting Serial Line Problems," if the status line indicates any other condition. **Step 2** Verify that the selected encapsulation type matches the requirements of the network to which the serial interface is attached.
Peer problems	**Step 1** Use the **show source-bridge** EXEC command to determine whether the peer is "open" between routers. If the peer is not open, routers cannot communicate. **Step 2** Use the **show source-bridge** command to determine whether the remote router can see the ring. If devices are not present on both rings, peers may not open, or peers may not appear in the **show source-bridge** display. **Step 3** If devices are present on both rings and peers are open, but communication is still blocked over the remote SRB connection, contact your router technical support representative for more assistance.

Intermittent Communication Failures over Remote SRB

Symptom: Sessions time out over a router configured for remote SRB. Table 8-6 outlines a possible cause and suggested actions when intermittent communication failures occur over a router configured as a remote SRB (encapsulated SRB over any non-Token Ring media).

Table 8-6 IBM: Intermittent Communication Failures over Remote SRB

Possible Cause	Suggested Actions
Sessions are timing out	**Step 1** Place a network analyzer on the ring local to the source station and look for acknowledgments that appear on the local ring after the transmission timeout period.
	Step 2 Perform a **ping** test to the remote router and note the round trip delay. Compare this value with the timeout value. If the round trip delay is close to or exceeds the timeout value, increase the timeout parameter. If the measured delay is close to or exceeds the timeout value, modify the timeout configuration at the source station.
	Step 3 Use the **show interfaces** EXEC command to check for dropped packets on all interfaces in the path.
	Step 4 If you are using TCP encapsulation, use the **show tcp** EXEC command to check the retransmission count for the peer in question.
	Step 5 Use a network analyzer to capture traffic for six or seven stations that have connectivity problems.
	Step 6 Adjust protocol parameters as described in the *Router Products Configuration Guide* and *Router Products Command Reference* publications. In particular, the various LLC2 timer values may need tuning.
	Step 7 On low-end routers, verify that the allocated buffers are adequate. Use the **show buffers** command, and look for misses in small, middle, or big buffers. Tune the number of buffers if there are many misses. For details, see the section "Adjusting Buffers to Ease Overutilized Serial Links" in the "Troubleshooting Serial Line Problems" chapter.

NetBIOS Clients Cannot Connect to Servers over Remote SRB

Symptom: Users on NetBIOS clients complain that they cannot establish connections to NetBIOS servers over routers acting as remote SRBs. Table 8-7 outlines possible causes and suggested actions when NetBIOS clients cannot connect to NetBIOS servers over a remote SRB.

Table 8-7 IBM: NetBIOS Clients Cannot Connect to Servers over Remote SRB

Possible Causes	Suggested Actions
Incorrect mapping of NetBIOS name cache server-to-client mapping	**Step 1** For each router on which NetBIOS name caching is enabled, use the **show rif** EXEC command to determine whether the RIF entry shows the correct path from the router to *both* the client and the server. **Step 2** Use the **write terminal** privileged EXEC command to ensure that the **source-bridge proxy-explorer** interface configuration command is included in the Token Ring configuration. Proxy explorers must be enabled on any interface that uses NetBIOS name caching. **Step 3** Use the **show netbios** EXEC command to see if the NetBIOS cache entry shows the correct mapping from server name and client name to MAC address. **Step 4** Use the **write terminal** privileged EXEC command at each router to examine the mapping of addresses specified in the **netbios name-cache** global configuration command. Change any mappings that are not correct.
Incorrect specification of remote peer parameters in **source-bridge** specification	**Step 1** For each router on which NetBIOS name caching is enabled, use the **show source-bridge** command to obtain the *version* of the remote connection. The value specified should be 2 or 3. If the value is 1, connections will not get through, and you must modify your configuration. **Step 2** If the router is running a software release prior to Cisco Internetwork Operating System (Cisco IOS) Release 10.0, specify either **version 2** or **version 3** in the **source-bridge remote-peer** interface configuration command. If the router is running Cisco IOS Release 10.0 or later, the specification of a version is ignored.

Note Whenever NetBIOS name caching appears not to be running between a particular client and server, capture traces of packets that apparently are not flowing. In addition, get the output of the **show rif**, **show netbios**, and **show source** EXEC commands for the routers at each end of the remote SRB cloud. The output of these commands can help diagnose a NetBIOS name caching problem by providing information about the state of the router.

Users Cannot Communicate over Cisco Translational Bridge

Symptom: Routers allow for the translation of transparent bridging and source-route bridging between Ethernet and Token Ring, respectively. Under certain circumstances, this translation may not work, which results in an apparent failure of translational bridging.

Caution In certain situations, replacing existing translational bridges with Cisco translational bridges can cause interoperability problems. Some translational bridge implementations map functional addresses between media (such as LAT functional address 0900.2B00.00FA on Ethernet) to a broadcast address on the Token Ring ring side (such as C000.FFFF.FFFF). Cisco does not support this functionality. Furthermore, you cannot use translational bridging with any protocol that embeds the MAC address of a station inside the information field of the MAC frames (examples include IP ARP and Novell IPX).

Table 8-8 outlines possible causes and suggested actions when users cannot communicate over Cisco routers configured for translational bridging.

Table 8-8 IBM: Users Cannot Communicate over a Translational Bridge

Possible Causes	Suggested Actions
Router does not support Ethernet-to-Token Ring address mapping	**Step 1** Use the **show bridge** EXEC command to verify the existence of the Ethernet station. (Ethernet and Token Ring addresses use opposite bit orderings. A Token Ring address of 0110.2222.3333 would be an Ethernet address of 8008.4444.cccc.) **Step 2** Use the **show spanning** EXEC command to determine whether the Ethernet port is in forwarding mode. **Step 3** Use the **show rif** EXEC command to determine whether the target Token Ring station is visible on the internetwork. (When configured for translational bridging, the router extracts the RIF of a packet received from the Token Ring side and saves it in a table. The router then transmits the packet on the Ethernet side. Later, the router reinserts the RIF when it receives a packet destined for the originating node on the Token Ring side.) **Step 4** If Ethernet and Token Ring end systems are visible, statically configure any relevant server MAC addresses in the client configurations, so the clients can listen to the server advertisements directly. (One case in which static mapping is required is when bridging DEC LAT traffic over a translational bridge. LAT services on Ethernet are advertised on a multicast address that is mapped by some translational bridges to a broadcast address on the Token Ring side. Routers do not support this mapping.)

Possible Causes	Suggested Actions
Vendor code mismatch	**Step 1** Specify the **ethernet-transit-oui** interface configuration command to force the router to make the vendor code field 000000. This change is frequently required when there are IBM 8209s (IBM Token Ring-to-Ethernet translating bridges) in the same network. (Older Token Ring implementations expect the vendor code [OUI field] of the SNAP header to be 000000. Cisco routers modify this field to be 0000F8 to specify that the frame was translated from Ethernet Version 2 to Token Ring.)
Adding Cisco translational bridging destabilizes network, blocks all traffic	**Step 1** Check for preexisting translational bridges in parallel with the Cisco translational bridge; any that are left in place will result in loops. **Step 2** Because implementing translational bridging defeats the spanning tree mechanism of both transparent bridging and SRB environments, you must eliminate all loops caused by inserting the translational bridge.
Trying to bridge protocols that embed MAC addresses in the Information field of the MAC frame (such as IP ARP and IPX)	**Step 1** Route these protocols. **Step 2** If you still cannot communicate over the router, contact your technical support representative.

Traffic Cannot Get through Router Implementing SRT Bridging

Symptom: Packets cannot traverse a router configured to support SRT bridging. Table 8-9 outlines possible causes and suggested actions when traffic cannot get through a router configured for SRT bridging.

Note SRT bridging allows you to implement transparent bridging in Token Ring environments. It is not a means of translating between SRB on a Token Ring and transparent bridging on Ethernet (or other) media. This confusion is sometimes the cause of blocked traffic in multimedia environments.

Table 8-9 IBM: Traffic Cannot Get through a Router Implementing SRT Bridging

Possible Causes	Suggested Actions
Trying to bridge frames containing RIF from the Token Ring side to the Ethernet side over an SRT bridge	**Step 1** Use translational bridging instead of SRT bridging to allow SRB-to-transparent bridging translation. Because SRT bridging only works between Ethernet and Token Ring, any packet containing a RIF is dropped when SRT bridging is used.
Hardware does not support SRT bridging	**Step 1** For each router interface configured to support SRT bridging, examine the output of the **show interfaces token** *number* EXEC command to determine whether the Token Ring interface is capable of SRT bridging. **Step 2** Check all other bridges in the network for SRT bridging support. **Step 3** Make sure that the software and microcode are compatible with SRT bridging for all internetworking devices; upgrade as needed.
Attempting to transfer large frame sizes (exceeding Ethernet MTU of 1500 bytes)	**Step 1** Configure hosts to generate frame sizes less than or equal to Ethernet MTU (1500 bytes).
Trying to bridge protocols that embed the MAC address in the Information field of the MAC frame (such as IP ARP and IPX)	**Step 1** Route these protocols. **Step 2** If you still cannot communicate over the router, contact your technical support representative.

Intermittent Connectivity over Router Configured for SDLC

Symptom: User connections to hosts time out over a router configured to support SDLC Transport. Table 8-10 outlines a possible cause and suggested actions when connectivity to hosts is intermittent over a router configured for SDLC.

Table 8-10 IBM: Intermittent Connectivity over Router Configured for SDLC

Possible Cause	Suggested Actions
SDLC timing problems	**Step 1** Place a serial analyzer on the serial line attached to the source station and monitor packets.
	Step 2 If duplicates appear, check the configuration for the **local-ack** keyword at the end of the **stun route address** interface configuration command.
	Step 3 If the **local-ack** keyword is missing, add it to both router configurations for SDLC interfaces.
	Step 4 Adjust the SDLC protocol parameters described in the *Router Products Configuration Guide* and *Router Products Command Reference* publications. These parameters are used to customize SDLC Transport over various network configurations. In particular, you may need to tune various LLC2 timer values.

Router Is Not Communicating with IBM SDLC Devices over EIA/TIA-232

Symptom: When installing a router, you find that the router is not able to communicate with an IBM SDLC device over an EIA/TIA-232 (formerly RS-232) cable.

Note When debugging serial line physical layer problems, it is important to observe indicator lights on appliques, LEDs on modems and modem eliminators, and line drivers. The indicator lights help you to determine whether the hardware is having any problems and can save debugging time.

Table 8-11 outlines a possible cause and suggested actions when a router is apparently not communicating with IBM SDLC devices over EIA/TIA-232.

Table 8-11 IBM: Router Is Not Communicating with IBM SDLC Devices over EIA/TIA-232

Possible Cause	Suggested Actions
Physical layer mismatch	**Step 1** Make sure that both the IBM device and the router implement the correct signal coding (NRZ or NRZI).
	Step 2 If the IBM device supports full-duplex NRZ, make sure that it is set for full-duplex NRZ (set Request to Send [RTS] high). For full-duplex configurations, set the signal high by strapping Data Terminal Ready (DTR) from the IBM side to RTS on the router side.
	Step 3 For AS/400 multidrop devices, make sure that Carrier Detect (CD) is tied to ground in the serial line that connects the router to the primary link station.
	Step 4 Use the **show interfaces** EXEC command to determine whether the interface and line protocol are up.
	Step 5 If the router is set up as a data terminal equipment (DTE) device, make sure that the clocking source configurations match for all devices. Also make sure that the modems and modem eliminators are properly configured.
	Step 6 When installing routers in IBM environments, make sure that the IBM devices are properly configured to communicate with each other. For example, make sure that cluster controllers can talk to FEPs before adding a router.
	Step 7 Make sure that the clock rate matches the network's externally derived clock.
	Step 8 Regardless of whether the router is configured as DTE or data communications equipment (DCE), try reducing the line speed to 9600 baud.
	Step 9 Because the EIA/TIA-232 clocking signal is weak, cable length must not exceed 50 feet (15.24 meters); 25 feet (7.62 meters) is the recommended length.

SDLC Sessions Fail over Router Running STUN

Symptom: SDLC sessions between two nodes are not coming up when they are attempted over a router that is running STUN. An underlying symptom is that the handshaking required to complete SDLC sessions is not occurring. Table 8-12 outlines possible causes and suggested actions when SDLC sessions fail over a router running STUN.

Table 8-12 IBM: SDLC Sessions Fail over Router Running STUN

Possible Causes	Suggested Actions
Broken physical connectivity of SDLC secondary stations and the STUN peer	**Step 1** Use the **show stun** EXEC command to check the STUN state. **Step 2** If the output of the **show stun** EXEC command indicates that the STUN is "closed," check physical connectivity as described in the "Router Is Not Communicating with IBM SDLC Devices over EIA/TIA-232" symptom module earlier in this chapter.
Misconfigured **stun route address** interface configuration command	**Step 1** Use the **show stun** EXEC command to check the STUN state. **Step 2** If the output of the **show stun** EXEC command indicates that the STUN is "open," use the **debug stun-packet** privileged EXEC command to look for Set Normal Response Mode (SNRM) and matching unnumbered acknowledgment (UA) packets. Ensure that the SNRMs and UAs that have SDLC addresses corresponding to the relevant secondary stations are getting to the correct router. **Step 3** If SNRMs are indicated in the **debug stun-packet** command output, but UAs are not indicated as returning, use the **write terminal** privileged EXEC command on the router to which the primary link station is attached. **Step 4** Look for the SDLC address specified in the **stun route address** interface configuration command. Entries for this command should point to relevant secondary link stations. (Routers do not support the **stun route all** functionality for SDLC; routers only support the basic STUN transport protocol.)
Misconfigured **stun peer-name** global configuration command	**Step 1** At the router to which the secondary link station is attached, enable the **debug stun-packet** privileged EXEC command and look for SNRMs for that peer. **Step 2** If no SNRMs appear in the output, check the **stun peer-name** commands on the router to which the primary link station is attached. Make sure that this command specifies the IP address of the router correctly.

Possible Causes	Suggested Actions
Physical connectivity problem from the secondary link station to the router; misconfigured **stun route address** interface configuration command on router to which the secondary link station is attached; or, broken IBM equipment	**Step 1** At the router to which the secondary link station is attached, enable the **debug stun-packet** privileged EXEC command and look for SNRMs for that peer. **Step 2** If you do see SNRMs, use the **show interfaces serial** EXEC command to see if output drops are accumulating. Accumulating output drops suggest that the router is not communicating with the secondary link station. **Step 3** For 3174s, if output drops are not accumulating, check the front panel display for values cycling between 505 and 532. This cycling of values indicates that SNRMs are getting to the 3174, but the receiver ready signal is not initializing. **Step 4** Check the output of the **debug stun-packet** privileged EXEC command to see if relevant UAs are being detected. If so, physical connectivity and broken IBM equipment can be eliminated as possible causes. If the **debug stun-packet** privileged EXEC command output at the router to which the primary link station is attached displays relevant UAs, the problem is isolated to a physical connectivity problem from that router *to* the primary link station. **Step 5** Check physical connectivity as described in the "Router Is Not Communicating with IBM SDLC Devices over EIA/TIA-232" symptom module earlier in this chapter.

Users Cannot Make Connections over Router Configured for SDLLC

Symptom: Users cannot make session connections to hosts on the other side of a router configured to support SDLLC.Table 8-13 outlines possible causes and suggested actions when users are unable to make host connections over a router configured for SDLLC.

Table 8-13 IBM: Users Cannot Make Connections over Router Configured for SDLLC

Possible Causes	Suggested Actions	
Missing **sdllc partner** command	**Step 1**	Configure the **sdllc partner** interface configuration command so that it points the router to the hardware address of the FEP on Token Ring. This command forces the transmission of explorer packets.
Missing **sdllc xid** command	**Step 1**	Include the **sdllc xid** interface configuration command. This command defines XID information (IDBLK and IDNUM) that must match host definitions when any 37X5 or 317X device is being used as a gateway.
	Step 2	Check with the system administrators of the hosts to ensure that the XID information is properly defined. If the 317X device is a channel-attached gateway, XID must be 0000000 for IDBLK and IDNUM.
Microcode incompatibility	**Step 1**	Use the **show controller mci** EXEC command to obtain the SCI microcode version of the serial card.
	Step 2	Upgrade to the latest microcode version.
Incorrect RTS signal in full-duplex implementation	**Step 1**	Insert a breakout box between the router and the IBM device and monitor the LEDs for correct signaling. EIA/TIA-232 signaling requirements are briefly described in the discussion following this table, "IBM EIA/TIA-232 Signaling Requirements Summary."
	Step 2	Check RTS for a continuously active signal from the router.
	Step 3	If the signal is not continuously active, set the signal high by strapping DTR from the IBM side to RTS on the router side. Open the RTS connection between the router and the IBM device. For more information concerning physical layer mismatches, see the "Router Is Not Communicating with IBM SDLC Devices over EIA/TIA-232" symptom module earlier in this chapter.
	Step 4	Configure the 3174 for permanent RTS by replying with a "1" to question number 340.
Incorrect V.35 applique jumper setting	**Step 1**	When using the V.35 dual-mode applique as a DCE, remove the SCT/SCTE jumper, which selects SCT and specifies that the timing signal come from the server.

IBM EIA/TIA-232 Signaling Requirements Summary

When connecting a router to an IBM device with a serial connection, you must verify that the signaling configurations are compatible. Figure 8-15 illustrates a typical serial connection between a router (Router-1) and an IBM device. Assume that the connection is full duplex. A breakout box is inserted to examine signal states on the cable.

Figure 8-15 Checking IBM Serial Link to Router with Breakout Box

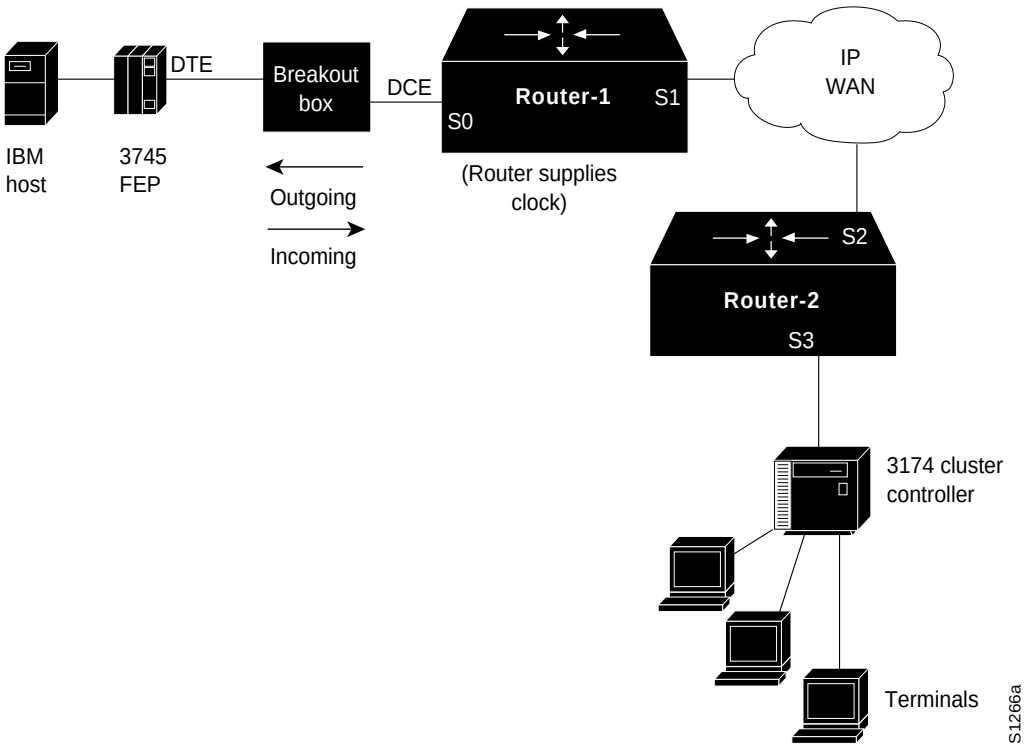


Table 8-14 outlines the key signaling requirements for the full-duplex link between Router-1 and the 3745 FEP. Figure 8-15 illustrates the direction of signals with respect to the router as listed in Table 8-14. This environment assumes that the router is configured for DCE, while the IBM FEP is configured for DTE.

Table 8-14 Key Full-Duplex EIA/TIA-232 Signaling Requirements for Router-to-IBM FEP Connection

Lead/Signal	State	Reference to Router
4/RTS	High	Incoming
5/CTS	High	Outgoing
6/DSR	High	Outgoing
8/CD	High	Outgoing
20/DTR	High	Incoming

Preventive Actions in SDLLC Environments

When configuring a router for SDLLC operation in IBM internetworking environments, try the following actions for preventing operational problems:

1. When configuring SDLLC, the **sdllc traddr** interface configuration command must point to the virtual ring, not to the physical ring. When using multiple interfaces, the **sdllc traddr** command specification must be unique for each interface. The virtual ring corresponds to the ring group number specified in the **source-bridge ring-group** global configuration command. This applies to single router configurations (where the Token Ring and the serial line are both tied to the same router) and multirouter configurations (where the routers are separated by WAN clouds). Also note that the specification of the virtual ring number is the last parameter in the **sdllc traddr** command.
2. SDLLC will not work between an IBM AS/400 and 5394. The AS/400 can only operate as a PU 2 device, while the 5394 can only operate as a PU 1 device. SDLLC only accommodates protocol and frame translation at the DLC level and does not participate in any SNA level exchange. To allow for this kind of translation, you must implement some kind of conversion device for translating PU 1 to PU 2. Routers only support PU 2 devices.

Virtual Token Ring Addresses and SDLLC Implementations

The **sdllc traddr** command requires the specification of a virtual Token Ring address for an SDLC-attached device (the device that you are spoofing to look like a Token Ring device). The last two hexadecimal digits of the virtual ring address must be 00 because the last byte of the address represents the SDLC address of the station on the serial link.

Assign virtual ring addresses carefully. Any virtual ring address that falls into the range xxxx.xxxx.xx00 to xxxx.xxxx.xxFF belongs to the associated SDLLC serial interface. An IBM locally administered address (LAA) is typically user-defined, and in practice these addresses tend to follow a logical ordering. As a result, there is a real chance that other IBM devices on an internetwork will have an LAA that falls in the same range. If this occurs, problems can arise because routers only examine the first 10 digits of the LAA address of a packet (not the last two, which are considered wildcards). If the router sees a match of the assigned SDLLC LAA address, it automatically forwards that packet to the SDLLC process. In certain cases, this can result in packets being incorrectly forwarded to the SDLLC process and sessions never being established.

Note Before assigning a virtual ring address for any SDLLC implementation, be certain you know the LAA naming convention used in the internetwork to avoid assigning conflicting addresses.

Router Cannot Be Linked from LAN Network Manager

Symptom: A specific router cannot be linked from the LAN Network Manager (LNM) in an SRB environment. Table 8-15 outlines possible causes and suggested actions when a router cannot be linked using LNM.

Table 8-15 IBM: Router Cannot Be Linked From LNM

Possible Causes	Suggested Actions
Misconfigured LNM MAC address specifications (universal)	**Step 1** Use the **show lnm config** EXEC command to determine the Token Ring MAC addresses. They must match the addresses entered on the LNM. **Step 2** If the addresses do not match, enter the Token Ring MAC addresses on the LNM platform.
MAC address mismatch when router is connected to a virtual ring (locally administered)	**Step 1** Use the **show lnm config** command on the router to determine the Token Ring MAC addresses. **Step 2** Make sure that the Token Ring address configured on the LNM matches the address administered on the router. Use the **mac-address** interface configuration command for each Token Ring interface. This command gives each Token Ring interface a locally administered address (such as 4000.0001.2345).

Example STUN and SDLLC Diagnostic Sessions

Troubleshooting STUN and SDLLC internetworks can involve a fairly complicated series of diagnostic steps. Even the simplest interconnection requires careful evaluation of each possible problem. This section outlines the basic diagnostic steps for representative STUN and SDLLC internetworking arrangements.

STUN Diagnostic Example

Consider the basic configuration illustrated in Figure 8-16. In this arrangement, an IBM mainframe is channel-attached to an FEP. The FEP is serial-attached to a router (Router-A), which is point-to-point connected over a serial connection to Router-B. Router-B is attached to a cluster controller. Assume that SDLC connections cannot be completed over the routed internetwork illustrated in Figure 8-16.

The following diagnostic tables (Table 8-16 through Table 8-19) outline a process for diagnosing blocked connectivity in this internetwork; the process starts at the FEP and moves to the cluster controller at the other end of the SDLC connection. The diagnostic steps outlined for this example are split into four parts:

- FEP connection diagnostics
- FEP configuration problem diagnostics
- Router STUN problem diagnostics
- Cluster controller problem diagnostics

Figure 8-16 Typical STUN Interconnection Illustrating Diagnostic Example

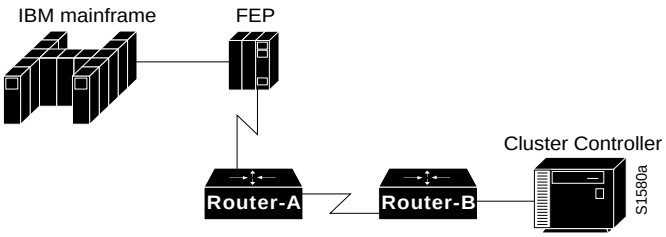


Table 8-16 FEP Serial Connection Diagnostics (STUN Example)

Possible Problem	Suggested Diagnostic Actions	
Failed serial connection from FEP to router	**Step 1**	Use the **show interfaces** EXEC command at Router-A; look for any indication of a possible problem. For more information about troubleshooting serial connections, refer to the "Troubleshooting Serial Line Problems" chapter.
Incorrect IBM cable	**Step 2**	Ensure that the correct cable is attached to the FEP. The V.35 cable and the EIA/TIA-232 IBM cable are similar in appearance. The chief difference is that the V.35 cable has three switches while the EIA/TIA-232 cable has only two.
	Step 3	Use the **show interfaces** command to determine whether the interface and line protocol are up, and that the reset counter is not changed. If everything appears normal, proceed to Table 8-17.
Incorrect RTS signal in full-duplex implementation	**Step 4**	Insert a breakout box between the router and the IBM device and monitor the LEDs for correct signaling.
	Step 5	Check RTS for a continuous active signal from the router.
	Step 6	If the signal is not continuously active, set the signal high by strapping DTR from the IBM side to RTS on the router side. Open the RTS connection between the router and the IBM device. For more information concerning physical layer mismatches, see the "Router Is Not Communicating with IBM SDLC Devices over EIA/TIA-232" symptom module earlier in this chapter.
	Step 7	When using the V.35 dual-mode applique as a DCE, remove the SCT/SCTE jumper, which selects SCT and specifies that the timing signal come from the server.
Microcode incompatibility	**Step 8**	Use the **show controller mci** EXEC command to obtain the SCI microcode version of the serial card.
	Step 9	Upgrade to the latest microcode version.

Table 8-17 FEP Configuration Problem Diagnostics (STUN Example)

Possible Problem	Suggested Diagnostic Actions
Misconfigured FEP	**Step 1** Check RTS and Clear to Send (CTS) signals; RTS should be active.
	Step 2 Check CD and ground; make sure that CD is strapped to ground.
	Step 3 Enable the **debug stun-packet** privileged EXEC command on Router-A.
	Step 4 Deactivate and then activate the SDLC lines at the host. Use the following VTAM commands: **VARY NET,INACT,LINE=***xx* **VARY NET,ACT,LINE=***xx* (where *xx* is the number of the line being toggled)
	Step 5 If SNRMs do not appear in the **debug stun-packet** output, check the line from the FEP to the serial interface on the router; the NCPGEN on the FEP, and the line number used with the **VARY** VTAM command as specified at the FEP.
	Step 6 If SNRMs appear in the **debug stun-packet** output, go to Table 8-18; otherwise, go to Table 8-19.

Table 8-18 Router STUN Problem Diagnostics (STUN Example)

Possible Problem	Suggested Diagnostic Actions
Misconfigured **stun peer-name** global configuration command and **stun route address** interface configuration command	**Step 1** Enable the **debug stun-packet** privileged EXEC command at Router-B.
	Step 2 If SNRMs appear in the **debug stun-packet** output at Router-B, misconfigured **stun peer-name** and **stun route address** commands might be blocking connectivity. Proceed to Table 8-19. (The **show stun** EXEC command can also provide a clue. It should indicate that the serial link between the routers is in "open" mode.)
Physical serial connection failed	**Step 3** Use the **show interfaces** EXEC command at Router-A and Router-B to determine whether they are operational. Make sure that the output indicates that both the interface and the line protocol are up.
	Step 4 If either the interface or the line protocol is not up, you may have a hardware problem. Check all your physical connections and refer to Chapter 2, "Troubleshooting Router Startup Problems," for hardware diagnostic information.
Mismatched SDLC (PU) address	**Step 5** If this serial connection uses direct HDLC encapsulation, verify that the SDLC address is correctly matched with the appropriate interface number. If not, modify as necessary.
IP connection is incorrectly defined	**Step 6** If this serial connection uses TCP/IP encapsulation, verify that the IP addresses of the **stun route address** interface configuration commands at both ends are matched with the IP addresses of the complementary **stun peer-name** global configuration commands.

Table 8-19 Cluster Controller Problem Diagnostics (STUN Example)

Possible Problem	Suggested Diagnostic Actions
Failed connection at cluster controller	**Step 1** Use the **show interfaces** EXEC command at Router-B to look for a possible problem. For more information about troubleshooting serial connections, refer to the "Troubleshooting Serial Line Problems" chapter.
Incorrect IBM cable	**Step 2** Ensure that the correct cable is attached to the FEP.
	Step 3 Use the **show interfaces** command to determine the status of the interface. If the output indicates that the interface and line protocol are up, and you still cannot establish connectivity, contact your router technical support representative.
Incorrect RTS signal in full-duplex implementation	**Step 4** Insert a breakout box between the router and the IBM device, and monitor the LEDs for correct signaling.
Incorrect V.35 applique jumper setting	**Step 5** Check RTS for a continuously active signal from the router. If the signal is not continuously active, set the signal high by strapping DTR from the IBM side to RTS on the router side. Open the RTS connection between the router and the IBM device. For more information concerning physical layer mismatches, see the "Router Is Not Communicating with IBM SDLC Devices over EIA/TIA-232" symptom module earlier in this chapter.
	Step 6 Configure the 3174 for permanent RTS by replying with a "1" to question number 340.
	Step 7 When using the V.35 dual-mode applique as a DCE, remove the SCT/SCTE jumper, which selects SCT and specifies that the timing signal come from the server.
Cluster controller configuration problem	**Step 8** Determine whether the cluster controller is operational.
	Step 9 If the cluster controller is not up, or if UAs are not returning from the controller, check the configuration of the controller and make sure that it is properly set; look for PU address, NRZI, and NRZ specification errors.
Microcode incompatibility	**Step 10** Use the **show controller mci** EXEC command to obtain the SCI microcode version of the serial card.
	Step 11 Upgrade to the latest microcode version.

SDLLC Diagnostic Example

Figure 8-17 illustrates an example SDLLC environment. An IBM mainframe is channel-attached to an FEP. The FEP and Router-A are both attached to a Token Ring. Router-A is point-to-point connected to Router-B, and Router-B is SDLC-attached to a cluster controller. For SDLLC troubleshooting, start with the SDLLC router—in this case Router-B. Assume that SDLLC connections cannot be completed over the routed internetwork illustrated in Figure 8-17.

The following diagnostic tables (Table 8-20 through Table 8-24) outline a process of diagnosing blocked connectivity starting from Router-B. The diagnostic steps outlined for this example are split into four parts:

- Router-to-router connectivity diagnostics
- FEP problem diagnostics
- SDLLC XID configuration problem diagnostics
- Router-to-cluster controller problem diagnostics

Figure 8-17 Typical SDLLC Interconnection Illustrating Diagnostic Example

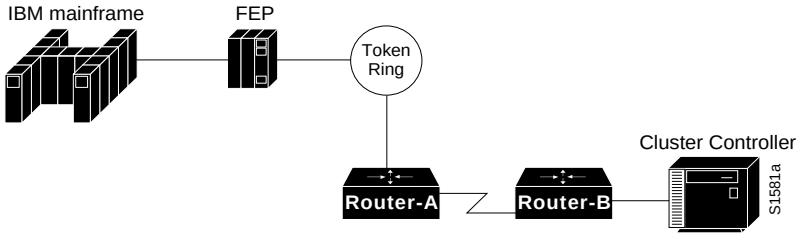


Table 8-20 Router-to-Router Connectivity Diagnostics (SDLLC Example)

Possible Problem	Suggested Diagnostic Actions
SDLLC configuration problems (general)	**Step 1** If the routers are running Cisco IOS Release 10.0, go to Table 8-21.
Incorrectly specified TIC address in the **sdllc partner** interface configuration command	**Step 2** Verify that the **sdllc partner** interface configuration command correctly specifies the TIC address in the configuration of the router. Make sure that the TIC address is the same as the LOCADDR defined on the FEP.
	Step 3 Enable the **debug sdllc** privileged EXEC command on Router-B.
	Step 4 To cause Router-B to display debug output on the console, turn the cluster controller off and on or apply the **shutdown** and **no shutdown** interface configuration commands to the SDLC serial interface that is connected to the cluster controller. If debug output does not appear, go to Step 7.
	Step 5 If a network analyzer is available, insert it into the FEP ring. (As a last resort, if a network analyzer is not available, use the **debug token ring** privileged EXEC command. However, use this command with extreme caution. This command generates a large number of messages. Unless you can capture this output using a UNIX script or some similar facility, it will scroll too quickly to be useful. In addition, this command uses substantial CPU bandwidth; just enabling it can disrupt traffic significantly.)
	Step 6 Check the output of the analyzer (or the output of the **debug token ring** privileged EXEC command) for a response from the FEP to a test message sent from Router-B.
	Step 7 If you do not get a response from the FEP, use a network analyzer to determine whether test frames are being placed on the ring.
Failed serial connection between routers	**Step 8** Check all physical connections between the routers (cables, connectors, interface cards, and appliques). Use the **show source-bridge** and **show interfaces serial** EXEC commands to identify any other serial connection problems.
	Step 9 Use the **show source-bridge** EXEC command to determine whether all peers are "open" and whether the relevant remote SRB peers appear in the listings for local SRB ports.
	Step 10 Use the **show interfaces** EXEC command to determine whether the interface and line protocol are up and whether the reset counter is unchanged; if so, go to Table 8-23.
	Step 11 If test frames appear in the output of the **debug token ring** privileged EXEC command, go to Table 8-22; otherwise, go to Table 8-23.

Table 8-21 Router-to-Router Connectivity Diagnostics for Cisco IOS Release 10.0 (SDLLC Example)

Possible Problem	Suggested Diagnostic Actions
Missing **sdllc partner** interface configuration command	**Step 1** Verify that the configuration of the router includes the **sdllc partner** interface configuration command, which points the router to the hardware address of the FEP on Token Ring. This command is required to initialize the SDLLC process.
Incorrectly specified TIC address in the **sdllc partner** interface configuration command	**Step 2** Verify that the TIC address is specified correctly in the configuration of the router. Make sure that this address is the same as the LOCADDR defined on the FEP.
	Step 3 Enable the **debug sdllc** privileged EXEC command on Router-B.
	Step 4 To cause Router-B to display debug output on the console, turn the cluster controller off and on or apply the **shutdown** and **no shutdown** interface configuration commands to the SDLC serial interface that is connected to the cluster controller. If debug output does not appear, go to Step 7.
	Step 5 Send a test message from Router-B. Check the output of the **debug sdllc** privileged EXEC command for a response from the FEP.
	Step 6 If you do not get a response from the FEP, use a network analyzer to determine whether a test frame was placed on the ring.
Failed serial connection between routers	**Step 7** Check all physical connections between the routers (cables, connectors, interface cards, and appliques). Use the **show source-bridge** and **show interfaces serial** EXEC commands to identify any other serial connection problems.
	Step 8 Use the **show source-bridge** command to determine whether all peers are "open" and whether the relevant remote SRB peers appear in the listings for local SRB ports.
	Step 9 Use the **show interfaces** EXEC command to determine whether the interface and line protocol are up and whether the reset counter is unchanged; if so, go to Table 8-23.
	Step 10 If test frames appear in the output of the **debug token ring** privileged EXEC command, go to Table 8-22; otherwise, go to Table 8-23.

Table 8-22 FEP Problem Diagnostics (SDLLC Example)

Possible Problem	Suggested Diagnostic Actions
Failed FEP Token Ring adapter	**Step 1** Check the network analyzer output (or **debug token ring** privileged EXEC command output) for a response to the null XID packet sent by the router.
	Step 2 If you do not see a response, check the Token Ring adapter of the FEP. If you see a response, go to Table 8-24.

Table 8-23 XID Configuration Problem Diagnostics (SDLLC Example)

Possible Problem	Suggested Diagnostic Actions
Missing **sdllc xid** interface configuration command	**Step 1** Check the network analyzer output (or **debug token ring** output) for an XID response for XID type 2. **Step 2** If not already configured, include the **sdllc xid** interface configuration command. This command defines XID information (IDBLK and IDNUM) that must match host definitions when any 37X5 or 317X device is used as a gateway. (If the 317X device is a channel-attached gateway, use the value 00000000 for IDNUM and IDBLK.) **Step 3** If you do not see an XID response for XID type 2, check the IDNUM and IDBLK found in the trace. **Step 4** Check with the system administrators of the hosts to ensure that XID information is properly defined. **Step 5** Check the network analyzer output (or **debug token ring** privileged EXEC command output) for a SABME message from the FEP and a UA from Router-B. **Step 6** Enable the **debug sdlc** command on Router-B. You should see SNRMs from Router-B arriving at the cluster controller. (If you do not see any UA responses to the SNRM messages in the **debug sdlc** command output, go to Table 8-24 or contact your technical support representative.)

Table 8-24 Router-to-Cluster Controller Problem Diagnostics (SDLLC Example)

Possible Problem	Suggested Diagnostic Actions
Failed serial connection from cluster controller to router	**Step 1** Check the physical connections from Router-B to the cluster controller.
Misconfigured cluster controller address or address configuration in router	**Step 2** Determine whether the cluster controller is operational. **Step 3** If the cluster controller is not up, or if UAs are not returning from the controller, check the configuration of the controller and make sure that it is properly set; look for PU address, NRZI, or NRZ specification errors.

CHAPTER 9

Troubleshooting ISO CLNS Connectivity

This chapter presents protocol-related troubleshooting information for the International Organization for Standardization (ISO) Connectionless Network Services (CLNS) protocol connectivity problems. ISO CLNS is a standard for the network layer of the Open Systems Interconnection (OSI) model.

This chapter consists of the following sections:

- ISO CLNS Connectivity Scenarios
- NCR/AT&T StarGroup Considerations
- ISO CLNS Connectivity Symptoms

The symptom modules consist of the following sections:

- Symptom statement—A specific symptom associated with ISO CLNS connectivity.
- Possible causes and suggested actions—A table for each symptom containing possible causes for the symptom and suggested actions for resolving each cause.

ISO CLNS Connectivity Scenarios

ISO CLNS networks are becoming increasingly complex as they gain wider use. Connectivity problems at the network layer, route redistribution problems in integrated networks, ISO CLNS links over WANs, and conversions between DECnet hosts are all sources of connectivity problems.

The connectivity-related scenarios in this section show environments that feature end systems (ESs) communicating through various ISO CLNS links. The scenarios include the following:

- ISO CLNS End System Connectivity
- ISO CLNS Connectivity over WANs
- ISO CLNS Route Redistribution Loops
- DECnet Phase IV and Phase V Connectivity

Note If your end system supports autoconfiguration, you can use it to prevent many of the most common problems that result from typing errors when entering Network Service Access Point (NSAP) addresses.

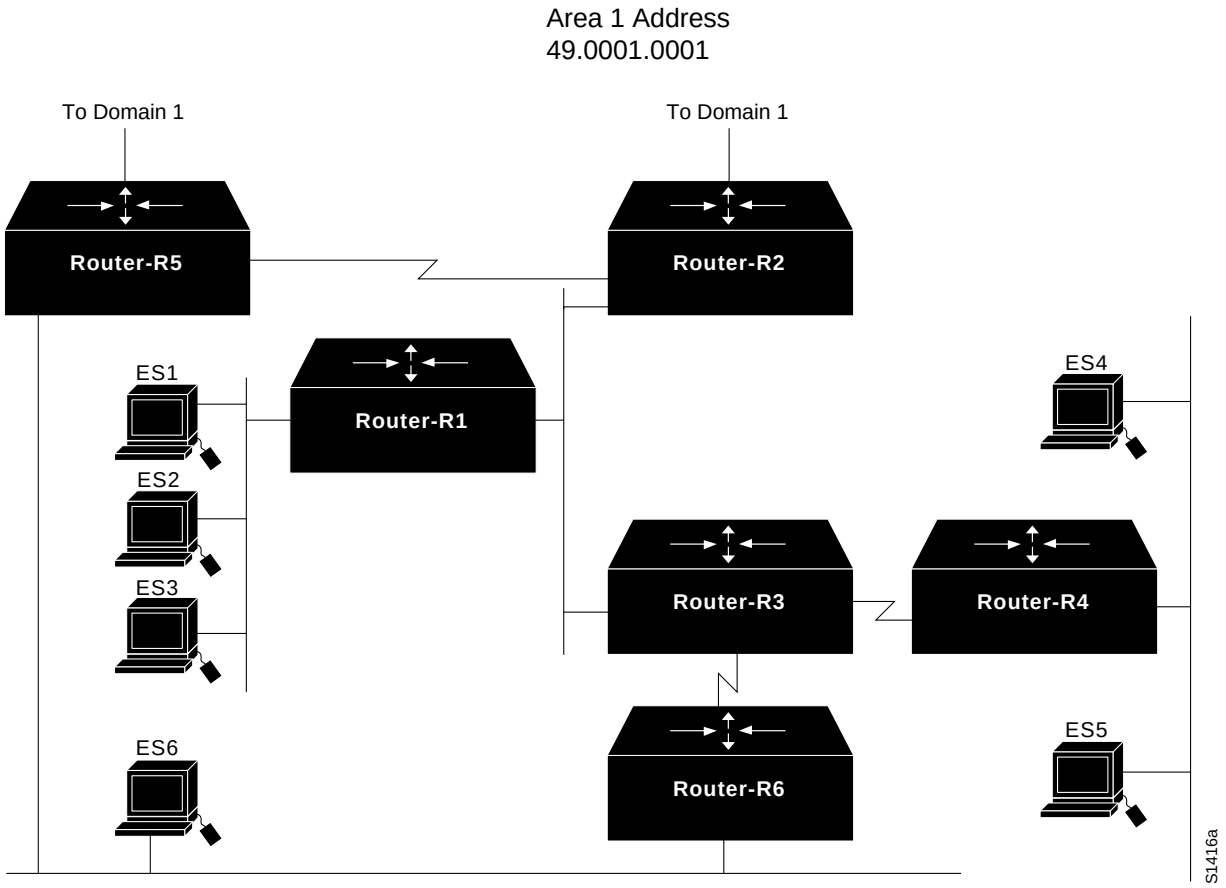
ISO CLNS End System Connectivity

Figure 9-1 illustrates Area 1 of Domain 1 in an ISO CLNS network segment that contains three domains. In Area 1, some end systems cannot communicate with other end systems. The following facts summarize the situation:

- ES1 cannot communicate with ES2, an end system that is on the same network segment.
- ES1 cannot communicate with ES4, an end system that is on a different network segment from ES1 but is in the same area as ES1.
- ES1 cannot communicate with an end system that is outside of area 1 but is in domain 1.

Many times, these symptoms are caused by simple configuration errors, such as inadvertently assigning duplicate addresses. By using debug and management tools, problems can be quickly isolated.

Figure 9-1 Initial ISO CLNS Connectivity Scenario Map



Environment Description

The relevant elements of the internetworking environment shown in Figure 9-1 can be summarized as follows:

- Area 1 consists of six routers (Router-R1 through Router-R6) and six end systems (ES1 through ES6). End systems ES1 through ES3 are on the same Ethernet segment, ES4 and ES5 share another Ethernet segment, and ES6 is on the same Ethernet segment as Router-R5 and Router-R6.
- Router-R2 and Router-R5 are connected by a point-to-point link. Both routers connect to the domain 1 backbone and are considered Level 2 routers, although in this discussion they participate in both Level 1 and Level 2 routing.
- Router-R3 has a point-to-point connection to Router-R4 and another point-to-point connection to Router-R6.
- The addressing scheme for domain 1, the areas within domain 1, and the systems within area 1 are based on the topology shown in Figure 9-2 and summarized in Table 9-1.

Figure 9-2 ISO CLNS Scenario Area and Domain Topology Map

.

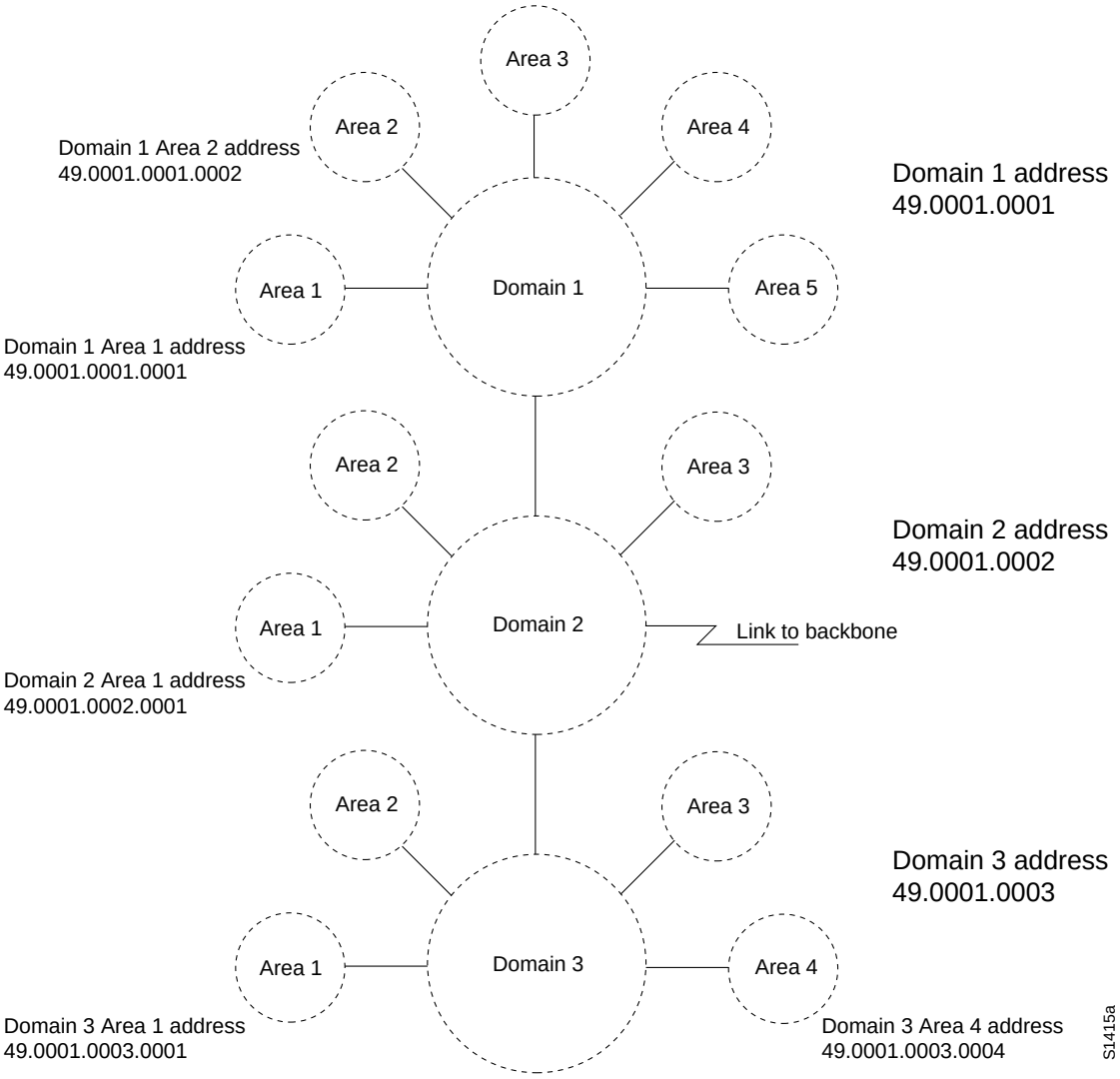


Table 9-1 Domain 1 Area 1 System IDs

End System/ Router	System ID (6 bytes)
ES1	0000.0000.0001
ES2	0000.0000.0002
ES3	0000.0000.0003
ES4	0000.0000.0004
ES5	0000.0000.0005
ES6	0000.0000.0006
Router-R1	0000.0000.1001
Router-R2	0000.0000.1002

End System/ Router	System ID (6 bytes)
Router-R3	0000.0000.1003
Router-R4	0000.0000.1004
Router-R5	0000.0000.1005
Router-R6	0000.0000.1006

Table 9-1 shows a simplified way of maintaining address consistency within an area. Given the domain 1 and area 1 addresses shown in Figure 9-2, the complete (NSAP) address for ES1 would be the following:

49.0001.0001.0001.0000.0000.0001.00

Note that the six-byte system ID *and* the one-byte n-selector are appended to the domain and area address. Similarly, the NSAP address for Router-R1 would be the following:

49.0001.0001.0001.0000.0000.1001.00

Diagnosing and Isolating Problem Causes between ES1 and ES2

The following problems are likely candidates for the first symptom. (ES1 cannot communicate with ES2, a host on the same network segment.)

- ES2 or ES1 does not support an implementation of the End System-to-Intermediate System (ES-IS) protocol that allows the two systems to dynamically discover one another and place the routing entries into the adjacency database.
- Static entries are missing or misconfigured in the end systems.

This list is ordered according to a combination of two criteria: ease of problem determination and the likelihood of being the *actual* problem. In general, it is useful to eliminate most likely problems first, and then to tackle more complex problems as necessary. The problem-solving process that follows illustrates this strategy.

Once you develop a list of possible problems, analyze each potential cause. The following discussion considers the problems for this scenario.

Checking Adjacency Databases in the End Systems

A number of mechanisms place system entries in adjacency databases. For a description of the various messages that end systems (ESs) and intermediate systems (ISs) use to advertise their presence on the network, see the *Internetworking Technology Overview* publication. These messages include the following:

- IS hello (ISH) packets
- ES hello (ESH) packets
- Redirect (RD) messages
- Link state packets (LSPs)

Common causes for a missing entry in the adjacency database are end systems that require manual installation of a static entry and end systems that do not fully support the ES-IS protocol, which means that they cannot dynamically discover other systems in the network.

To correct a missing entry in the adjacency database, follow these steps:

Step 1 Look in the adjacency database on each system and verify that addresses exist for the other systems that are directly attached. Create static entries in the adjacency database for the missing NSAP to Subnetwork Point of Attachment (SNPA) mappings.

Step 2 Check the ES-IS implementation on ES1 and ES2. Doing so may require contacting the software supplier or researching the system documentation.

Step 3 Depending on the ES-IS implementation on the end system, you might need to create static entries for other ESs that are on the same physical interface or ISs on the same interface.

If ES1 and ES2 have entries for one another in their adjacency databases, they should be able to directly communicate.

Diagnosing and Isolating Problem Causes Between ES1 and ES4

The following problems are likely candidates for the second symptom. (ES1 cannot communicate with ES4, a host on a different network segment in the same area.)

- Either ES1 or ES4 does not support an implementation of the ES-IS protocol that allows the systems to dynamically discover their intermediate systems (Router-R1 and Router-R4). This problem is described in the section "Checking Adjacency Databases in the End Systems" earlier in this section.
- There is a connectivity problem between ES1 and ES4.

Checking Connectivity from the Router to the End System

The steps that follow focus on using the EXEC **trace** and **show** EXEC commands to verify connectivity from the router to the end system. Systematically verify each link in the path.

Step 1 At Router-R1, use the **trace** EXEC command to verify connectivity to ES4. Based on the network installation map, which should resemble Figure 9-1, you can see that the path to ES4 is through Router-R3 and Router-R4. Use the **trace** command on the NSAP address for ES4. Figure 9-3 shows an example of the **trace** command output.

Figure 9-3 Output from the trace Command

```
Router-R2# trace 49.0001.0001.0001.0000.0000.0004.00

Type escape sequence to abort.
Tracing the route to 49.0001.0001.0001.0000.0000.0004.00
  1 49.0001.0001.0001.0000.0000.1003.00 0 msec ! 0 msec ! 0 msec !
  2 49.0001.0001.0001.0000.0000.1004.00 24 msec ! 24 msec ! 24 msec !
  3  *  *  *
```

S2620

It is most likely that connectivity problems will occur between ES4 and Router-R4, rather than between the routers.

Step 2 Use EXEC **show** commands to display the routing table and adjacency database information for the router.

If you get a response from Router-R3 but not from Router-R4, Router-R4 does not have an entry for ES4. Establish a connection to Router-R4 and display the routing table information.

If you are running ISO-Interior Gateway Routing Protocol (IGRP), use the **show clns route** EXEC command. (See Figure 9-4.)

Figure 9-4 Output of the show clns route Command

```
Router-R4# show clns route
ISO-IGRP Routing Table for Domain 49.0001.0001, Area 0001
System Id       Next-Hop        SNPA            Interface   Metric   State
0000.0000.0006  0000.0000.1003  *HDLC*          Serial1     10576    Up
0000.0000.0003  0000.0000.1003  *HDLC*          Serial1     8576     Up
0000.0000.0002  0000.0000.1003  *HDLC*          Serial1     8576     Up
0000.0000.0001  0000.0000.1003  *HDLC*          Serial1     8576     Up
0000.0000.0005  0000.0000.0005  0000.0c01.f331  Ethernet1   1100     Up
0000.0000.0004  0000.0000.0004  0000.0c00.ab41  Ethernet1   1100     Up
0000.0000.1005  0000.0000.1003  *HDLC*          Serial1     10576    Up
0000.0000.1002  0000.0000.1003  *HDLC*          Serial1     8576     Up
0000.0000.1003  0000.0000.1003  *HDLC*          Serial1     8476     Up
0000.0000.1001  0000.0000.1003  *HDLC*          Serial1     8576     Up
0000.0000.1004  0000.0000.0000  --              --          0        Up

ISO-IGRP Routing Table for Domain 49.0001.0001
Area Id         Next-Hop        SNPA            Interface   Metric   State
0001            0000.0000.0000  --              --          0        Up

CLNS Prefix Routing Table                                              S2621
49.0001.0001.0001.0000.0000.1004.00, Local NET Entry
```

If you are running IS-IS, use the **show isis routes** EXEC command. (See Figure 9-5.)

Figure 9-5 Output of the show isis routes Command

```
Router-R4# show isis routes

IS-IS Level-1 Routing Table - Version 46
System Id       Next-Hop        SNPA            Interface   Metric  State
0000.0000.0003  0000.0000.1003  *HDLC*          Serial1     30      Up
0000.0000.0002  0000.0000.1003  *HDLC*          Serial1     30      Up
0000.0000.0001  0000.0000.1003  *HDLC*          Serial1     30      Up
0000.0000.0006  0000.0000.1003  *HDLC*          Serial1     30      Up
0000.0000.1001  0000.0000.1003  *HDLC*          Serial1     20      Up
0000.0000.1002  0000.0000.1003  *HDLC*          Serial1     20      Up
0000.0000.1005  0000.0000.1003  *HDLC*          Serial1     30      Up
0000.0000.1006  0000.0000.1003  *HDLC*          Serial1     20      Up
0000.0000.1003  0000.0000.1003  *HDLC*          Serial1     10      Up    S2622
0000.0000.1004  0000.0000.0000  --              --          0       Up
```

Step 3 Next, use the **show clns neighbors** command to see whether Router-R4 has adjacency information for ES4. (See Figure 9-6.) If the **show clns neighbors** EXEC command shows a system ID for ES4 and its SNPA value is valid, there might be a problem with a misconfigured area address as described in the next step.

Figure 9-6 Output of the show clns neighbors Command

```
Router-R4# show clns neighbors
System Id       SNPA            Interface   State  Holdtime  Type  Protocol
0000.0000.0005  0000.0c01.f331   Ethernet1   Up     250       ES    ES-IS
0000.0000.0004  0000.0c00.ab41   Ethernet1   Up     282       ES    ES-IS
0000.0000.1003  *HDLC*          Serial1     Up     27        L1L2  IS-IS
```

S2623

Step 4 Use the **show clns neighbors detail** EXEC command to show which area address ES4 is advertising in its ESH packets. (See Figure 9-7.) If the area address being advertised is different from that of the area configured for Router-R4, the router has no indication that ES4 is in its area and therefore does not forward packets to it.

Figure 9-7 Output of the show clns neighbors detail Command

```
Router-R4# show clns neighbors detail
System Id       SNPA            Interface   State  Holdtime  Type  Protocol
0000.0000.0005  0000.0c01.f331   Ethernet1   Up     268       ES    ES-IS
  Area Address(es): 49.0001.0001.0001
0000.0000.0004  0000.0c00.ab41   Ethernet1   Up     299       ES    ES-IS
  Area Address(es): 49.0001.0001.0001
0000.0000.1003  *HDLC*          Serial1     Up     28        L1L2  IS-IS
  Area Address(es): 49.0001.0001.0001
```

S2624

Correct the area address entry on ES4.

Step 5 If the routing table entry for ES4 shows that it exists, but is on a different network, there are two possibilities: duplicate end system addresses exist within the area, or a routing loop exists. To check on duplicate end system addresses, use the **show clns route** EXEC command and the **show clns neighbors** EXEC command at each point in the path to the suspect ES4 until you locate the problem. In the case of a duplicate address that causes another end system to masquerade as ES4, reconfigure the duplicate system to its proper NSAP address.

Step 6 To see if there is a routing loop, you can check the conditions that follow. In general, a routing loop within an area is a transient condition caused by a topology change. However, if a loop persists, use the **trace route** EXEC command to discover where the loop occurs.

Step 7 If you are running the ISO-IGRP, turn on debugging with the **debug clns igrp packet** privileged EXEC command. Refer to the *Debug Command Reference* publication for a description of debug output.

Step 8 If you are running the IS-IS protocol, you can perform a quick check of the LSP databases and verify that they are synchronized, as follows:

- Look at all sequence numbers of all LSPs and see whether they are the same. LSPs are sorted, so it is fairly easy to perform a visual check on the LSP display for each router. Figure 9-8 shows a sample display emphasizing the LSP sequence numbers. This method is suitable for a small network.

Figure 9-8 Output of the show isis database Command Showing LSP Sequence Numbers

```
Router-R4# show isis database
IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0000.1001.00-00  0x0000000C   0xD69F        726           0/0/0
0000.0000.1001.0A-00  0x00000010   0xD539        726           0/0/0
0000.0000.1002.00-00  0x00000010   0x0B6B        1000          0/0/0
0000.0000.1002.0D-00  0x0000000D   0x6C7F        1000          0/0/0
0000.0000.1003.00-00  0x00000017   0x33CE        672           0/0/0
0000.0000.1003.09-00  0x00000002   0xABEA        672           0/0/0
0000.0000.1004.00-00* 0x00000011   0xEF3C        962           0/0/0
0000.0000.1005.00-00  0x0000001D   0xD98B        963           0/0/0
0000.0000.1006.00-00  0x0000000F   0x1B4C        546           0/0/0
0000.0000.1006.0A-00  0x0000000C   0x50A1        546           0/0/0

IS-IS Level-2 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0000.1001.00-00  0x0000000B   0xE0EA        755           0/0/0
0000.0000.1001.0A-00  0x00000007   0xA792        755           0/0/0
0000.0000.1002.00-00  0x00000011   0x29EC        1029          0/0/0
0000.0000.1002.0D-00  0x0000000D   0x6C7F        1029          0/0/0
0000.0000.1003.00-00  0x00000017   0x84D4        671           0/0/0
0000.0000.1003.09-00  0x00000002   0xABEA        671           0/0/0
0000.0000.1004.00-00* 0x00000010   0x903F        961           0/0/0
0000.0000.1005.00-00  0x0000001B   0x64A6        963           0/0/0
0000.0000.1006.00-00  0x0000000D   0x729B        546           0/0/0
0000.0000.1006.0A-00  0x0000000B   0x96F0        545           0/0/0
```

S2625

- You can use the **debug isis update packets** privileged EXEC command and look at the debug output to pinpoint the problem. Refer to the *Debug Command Reference* publication for a description of debug output.

Verifying IS-IS Connections

In IS-IS, use the following procedure to verify that connections exist between the routers and end systems:

Step 1 If the **show isis routes** EXEC command does not show ES4, yet it appears in the adjacency database displayed by **show clns neighbors**, there is no connectivity between Router-R4 and the pseudo node. The pseudo node is a fictitious node that reports all the end system and intermediate system nodes on a subnetwork. The node information is present in a pseudo node IS-IS LSP. Router-R4 will have a connection to the pseudo node, which provides a connection to all other reported end systems.

Use the **show isis database** EXEC command to verify that Router-R4 is generating both an LSP and a pseudo node LSP, as shown in Figure 9-9.

Figure 9-9 Output of the show isis database Command Showing LSP and Pseudo Node LSP

```
Router-R4# show isis database
IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0000.1001.00-00  0x0000000E   0xD2A1        1133          0/0/0
0000.0000.1001.0A-00  0x00000012   0xD13B        1133          0/0/0
0000.0000.1002.00-00  0x00000011   0x096C        507           0/0/0
0000.0000.1002.0D-00  0x0000000E   0x6A80        507           0/0/0
0000.0000.1003.00-00  0x0000001C   0x34C8        1080          0/0/0
0000.0000.1003.09-00  0x00000004   0xA7EC        1080          0/0/0
0000.0000.1004.00-00* 0x00000014   0x5B1C        515           0/0/0
0000.0000.1004.04-00* 0x00000002   0xBE5A        540           0/0/0
0000.0000.1005.00-00  0x0000001E   0xD78C        470           0/0/0
0000.0000.1006.00-00  0x00000011   0x174E        953           0/0/0
0000.0000.1006.0A-00  0x0000000E   0x4CA3        953           0/0/0

IS-IS Level-2 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0000.1001.00-00  0x0000000D   0xDCEC        1161          0/0/0
0000.0000.1001.0A-00  0x00000009   0xA394        1162          0/0/0
0000.0000.1002.00-00  0x00000012   0x27ED        536           0/0/0
0000.0000.1002.0D-00  0x0000000E   0x6A80        536           0/0/0
0000.0000.1003.00-00  0x0000001C   0x153F        1079          0/0/0
0000.0000.1003.09-00  0x00000004   0xA7EC        1079          0/0/0
0000.0000.1004.00-00* 0x00000012   0x1903        499           0/0/0
0000.0000.1005.00-00  0x0000001C   0x62A7        470           0/0/0
0000.0000.1006.00-00  0x0000000F   0x6E9D        951           0/0/0
0000.0000.1006.0A-00  0x0000000D   0x92F2        951           0/0/0
```

S2626

Step 2 Next, use the **show isis database detail 000.000.0004.01-00 level-1** command to display the contents of the pseudo node for ES4 Level 1 LSP. You are looking for the end system (ES4) to be listed in the LSP of the pseudo node. If the end system does not appear, there is probably a bug in the designated router.

If you use the **clns host** global configuration command to map the name ES4 to its associated NSAP address, you can use the name rather than the system ID in the **show isis database detail** EXEC command. Figure 9-10 shows how the **clns host** command is used.

Figure 9-10 Example of the clns host Command

```
Router-R4# clns host ES4 49.0001.0001.0001.0000.0000.0004
Router-R4# show isis database detail ES4.01-00 level-1
IS-IS Level-1 LSP 0000.0000.1004.04-00
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0000.1004.04-00* 0x00000003   0xBC5B        971           0/0/0
  Metric: 0    IS 0000.0000.0004.00
  Metric: 0    ES 0000.0000.0004
  Metric: 0    ES 0000.0000.0005
```

S2627

Step 3 If ES4 appears in the pseudo node LSP, verify that Router-R4 appears in the pseudo node LSP, as shown in Figure 9-11.

Figure 9-11 Output Showing Pseudo Nodes for ES and IS

```
Router-R4# show isis database detail 49.0001.0001.0001.0000.0000.1004 level-1
IS-IS Level-1 LSP 0000.0000.1004.04-00
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0000.1004.04-00* 0x00000003   0xBC5B        971           0/0/0
  Metric: 0    IS 0000.0000.1004.00
  Metric: 0    ES 0000.0000.1004
  Metric: 0    ES 0000.0000.0004                                        S2628
```

The pseudo node advertises all ESs and ISs on the subnetwork. By looking at the command output, you should see that the pseudo node has a link to ES4 and to Router-R4, and that Router-R4 has a connection back to the pseudo node. If all these pieces of the connection exist, there is connectivity between Router-R4 and ES4.

A pseudo node may exist, but Router-R4 is not yet in the pseudo node LSP because IS-IS was not configured on its Ethernet interface. The reason a pseudo node would exist for Router-R4 is because it may have been flooded through that path through another router.

Another problem not to be overlooked in this instance is that IS-IS routing was not enabled on Router-R4's Ethernet interface.

Step 4 Continue to work backward from Router-R4. Verify in an LSP from Router-R3 that a connection exists to Router-R4. Verify that Router-R3 has a connection to the pseudo node on the Ethernet shared with Router-R1 (and Router-R2) and that the pseudo node has a connection back to Router-R3, Router-R2, and Router-R1.

Step 5 Verify in the LSP for Router-R1 that it has a connection to the pseudo node in Router-R3. If there is no connection to the pseudo node, verify that the LSP sequence numbers are the same for Router-R1 as they are for Router-R3.

Step 6 After verifying that all the connections exist in the various LSP databases as shown by the **show isis database detail level1** EXEC command, connectivity should exist between ES1 and ES4. If there is a topology change—for example, a router is moved or wiring connections are changed—some time can pass before the change is detected, the new LSP is flooded throughout the network, and all the routers and end systems generate new routing tables with the updated information.

Verifying ISO-IGRP Connections

In ISO-IGRP, use the following steps to verify that connections exist between the routers and end systems along the path from ES1 to ES4:

Step 1 Turn on debugging in Router-R3 using the **debug clns igrp packet** privileged EXEC command and look at the update packets that are coming in from Router-R4. If you see that Router-R4 is advertising ES4, determine why Router-R3 is not putting ES4 in its routing table.

Step 2 At Router-R3, use the **trace** EXEC command to verify the path back to Router-R1.

Step 3 For each router in the path from Router-R1 to Router-R4, use the **show clns routes** EXEC command to verify the router is learning the path.

Step 4 After using the **debug** command, use the **no debug clns igrp packets** command to turn it off.

Diagnosing Problem Causes between ES1 and an End System outside Its Area

For the third connectivity symptom (ES1 cannot communicate with an end system outside its own area, such as ES8), the problem-solving steps are the same as those in the section "Diagnosing and Isolating Problem Causes Between ES1 and ES4" earlier in this chapter.

- Use the **trace** EXEC command to address the end system SNPA.
- Verify each link along the path and display the routing table contents by using the **show clns route** EXEC command (or the **show isis routes** EXEC command) and the **show clns neighbors** EXEC command.

End System Problem Solution Summary

This scenario focused on diagnosing end system connectivity problems.

- Misconfigured addresses were corrected.
- Connectivity was verified by displaying adjacency tables (IS-IS) and routing tables (ISO-IGRP).
- Routing for IS-IS or ISO-IGRP was enabled as required.

Figure 9-12, Figure 9-13, and Figure 9-14 provide representative configuration listings for routers discussed in this scenario.

Figure 9-12 Partial Configuration Listing for Router-R1

```
clns routing
router iso-igrp one
net 49.0001.0001.0000.0000.1001.00
interface ethernet 0
clns router iso-igrp one
interface ethernet 1
clns router iso-igrp one
```

S2629

Figure 9-13 Partial Configuration Listing for Router-R3

```
clns routing
router iso-igrp one
net 49.0001.0001.0000.0000.1003.00
interface ethernet 0
clns router iso-igrp one
interface serial 0
clns router iso-igrp one
interface serial 1
clns router iso-igrp one
```

S2630

Figure 9-14 Partial Configuration Listing for Router-R4

```
clns routing
router iso-igrp one
net 49.0001.0001.0000.0000.1004.00
interface ethernet 0
clns router iso-igrp one
interface serial 0
clns router iso-igrp one
```

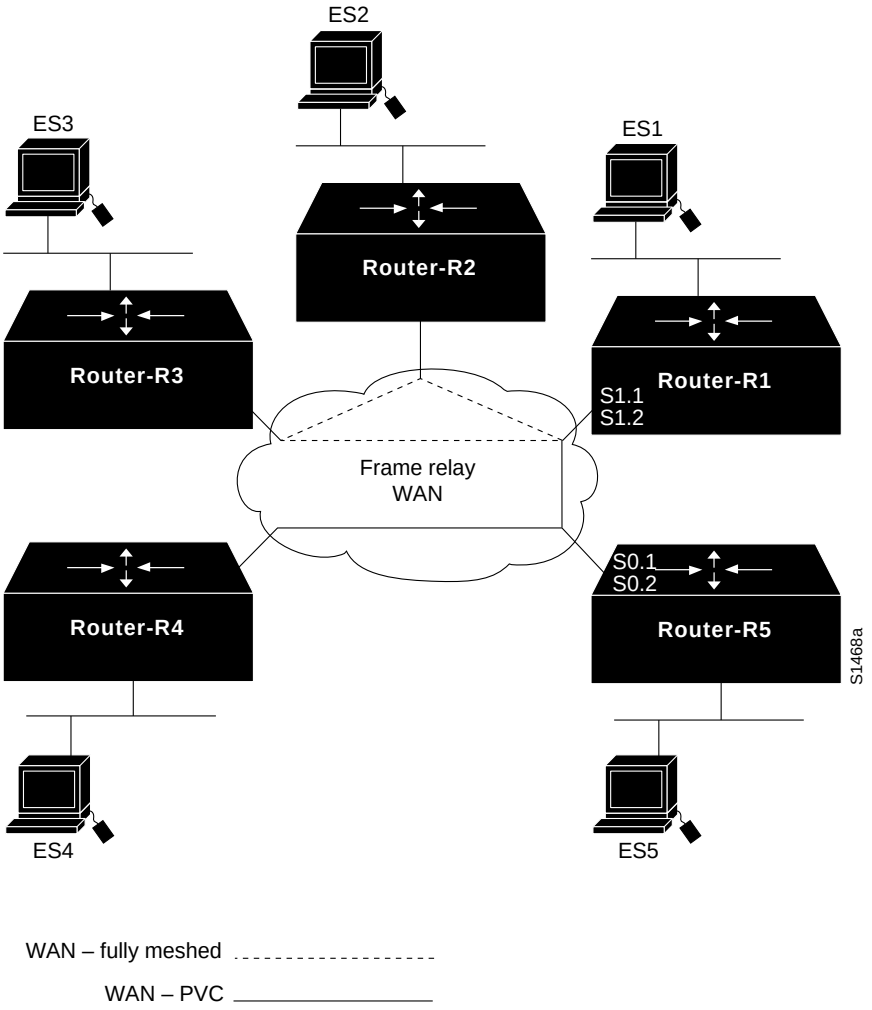
S2631

ISO CLNS Connectivity over WANs

Figure 9-15 illustrates various subnetworks that communicate through a Frame Relay cloud. The following facts summarize the situation:

- End system ES1 cannot communicate with ES2, an end system that is reached through the WAN, but is part of a fully meshed, logical network.
- ES4 cannot communicate with ES5, an end system that is reached through a permanent virtual circuit (PVC) on a subinterface.
- ES4 cannot communicate with ES1, an end system that is reached through ES5 and relies on subinterfaces and PVCs on both Router-R5 and Router-R1.

Figure 9-15 ISO CLNS Communication through a WAN Using Subinterfaces and PVCs



Environment Description

The relevant elements of the internetworking environment shown in Figure 9-15 can be summarized as follows:

- Router-R1, Router-R2, and Router-R3 are fully meshed and participate in multiaccess, broadcast communication.
- Router-R1 uses subinterfaces on its physical port S1 to communicate with the meshed network (S1.1) and to provide a PVC to Router-R5 (S1.2). A subinterface is occasionally referred to as a "virtual interface" or a "virtual port."
- Router-R5 uses subinterfaces on its physical port S0 to provide two PVCs: one to Router-R1 (S0.1) and one to Router-R4 (S0.2).
- Router-R1 and Router-R4 cannot communicate directly, but must have their packets forwarded by Router-R5.

Diagnosing and Isolating Problem Causes between ES1 and ES2 over a WAN

Given the situation, a number of problems might explain connectivity symptoms.

The following problems are likely candidates for the first symptom. (ES1 cannot communicate with ES2, a host reached through the WAN.)

- One of the routers (Router-R1 or Router-R2) does not have an entry in the adjacency database because the routers have missing or incorrect **frame-relay map** interface configuration commands.
- ES1 or ES2 does not support an implementation of the ES-IS protocol that allows the two systems to dynamically discover one another and place the entries into the adjacency database.
- Static entries are missing or misconfigured in the end systems.

IS-IS and ISO-IGRP protocols treat WANs as if they are multiaccess broadcast networks. In this situation, where a meshed network exists between the end systems, the routing protocol looks at the WAN as if it was a "solid wire" network like Ethernet. Other than the addition of **frame-relay map** commands in the routers, verifying ES-to-ES connectivity is the same as described in the section "Diagnosing and Isolating Problem Causes between ES1 and ES2," earlier in this chapter.

The information that follows explores the router as the cause of the connectivity problem.

Checking for Missing or Incorrect map Commands

A common cause for a missing entry in an adjacency database on the router is a missing or incorrect **frame-relay map** command. Assume the Data Link Connection Identifier (DLCI) values for routers are as shown in the following list:

- Router-R1: DLCI 16 to R2
- Router-R1: DLCI 17 to R3
- Router-R1: DLCI 18 to R4
- Router-R2: DLCI 21to R1
- Router-R2: DLCI 23 to R3
- Router-R3: DLCI 31 to R1
- Router-R3: DLCI 32 to R2

Step 1 If you are running ISO-IGRP, look in the adjacency database on each router and verify that entries exist for the other router that is accessed through the Frame Relay WAN. Use the **show clns neighbors** EXEC command to display the adjacency information, as shown in Figure 9-16.

Figure 9-16 Output of the show clns neighbors Command

```
Router-R1# show clns neighbors

System Id       SNPA            Interface   State  Holdtime  Type  Protocol
0000.0000.1002  DLCI 16         Serial1.1   Up     26        L1L2  IS-IS
0000.0000.1003  DLCI 17         Serial1.1   Up     20        L1L2  IS-IS
0000.0000.1005  DLCI 19         Serial1.2   Up     23        L1L2  IS-IS
```

S2632

Step 2 If the adjacency information is missing, check the router configuration and look for missing or incorrect **frame-relay map** commands. The **frame-relay map** commands are required whether you are running ISO-IGRP or IS-IS over the router interface.

At Router-R1 you must have interface configuration commands on the port that provide the connection to the WAN. For the DLCI values in this scenario, the commands would be the following.

```
interface serial 1
encapsulation frame-relay
interface serial 1.1 multipoint

frame-relay map clns 16 broadcast
frame-relay map clns 17 broadcast

interface serial 1.2
frame-relay interface-dlci 19
```

Similarly, Router-R2 must have interface configuration commands that point to Router-R1 and Router-R3.

```
frame-relay map clns 21 broadcast
frame-relay map clns 23 broadcast
```

And Router-R3 must have interface configuration commands that point to Router-R1 and Router-R2.

```
frame-relay map clns 31 broadcast
frame-relay map clns 32 broadcast
```

Step 3 Verify that ISO-IGRP or IS-IS routing is enabled for the router interface with the **clns router iso-igrp** or **clns router isis** interface configuration command on each router.

Note The IS-IS implementation differs slightly from the OSI specification in that in a multiaccess network, the Frame Relay WAN is treated as though it were a "solid wire" network like Ethernet. Designated router election is run over a Frame Relay network, and the designated router will have a pseudo node entry for the Frame Relay network. The same concepts of pseudo nodes and pseudo node links over an Ethernet described in the section "Checking Connectivity from the Router to the End System," earlier in this chapter, applies to problem diagnosis over a Frame Relay network.

If Router-R1 and Router-R2 have entries for one another in their adjacency databases, they should be able to communicate.

Diagnosing Problem Causes between ES4 and ES1 over a WAN

Several problems can cause connectivity symptoms between ES4 and ES1:

- The subinterfaces on Router-R5 that provide PVCs to Router-R4 and Router-R1 might be misconfigured.
- The subinterfaces on Router-R1 that provide connections to Router-R5 and to the meshed logical network that includes Router-R2 and Router-R3 might be misconfigured.
- There is a connectivity problem between Router-R1 and Router-R4.

Checking the Subinterface Configuration on Router-R5

A single physical interface can provide more than one connection by means of virtual interfaces, commonly called "subinterfaces." Subinterfaces are configured the same as interfaces and use the same set of interface configuration commands.

Assume that the DLCI values for Router-R4 and Router-R5 for routers are as follows:

- Router-R4: DLCI 45 to R5
- Router-R5: DLCI 51 to R1
- Router-R5: DLCI 54 to R4

Step 1 For Router-R5, verify that the configuration commands for interface serial 0, its physical interface to the WAN, include the commands that follow:

```
interface serial 0.1
clns router isis
! Or clns router iso-igrp
frame-relay map clns 51

interface serial 0.2
clns router isis
!Or clns router iso-igrp
frame-relay map clns 54

!PVC commands for R5 subinterfaces serial 0.1 and serial 0.2 follow.

interface serial 0
encapsulation frame-relay
interface serial 0.1 point-to-point
frame-relay interface-dlci 51
interface serial 0.2 point-to-point
frame-relay interface-dlci 54
```

Checking the Subinterface Configuration on Router-R1

On Router-R1, interface serial 0 provides two subinterfaces: an interface to the multiaccess network and an interface to the point-to-point PVC from Router-R5. To check the subinterface configuration, verify that the configuration commands for interface serial 1 of Router-R1 (its physical interface to the WAN), include the following commands:

```
interface serial 1.1 multipoint
clns router isis
!(OR clns router iso-igrp)
frame-relay map clns 12
frame-relay map clns 13

interface serial 1.2 point-to-point
clns router isis
!(OR clns router iso-igrp)
frame relay interface-dlci 1
```

The multipoint subinterface running IS-IS is treated as a multiaccess broadcast router. The point-to-point subinterface is treated as a "real" serial link, and the point-to-point IS-IS protocol is run on that link.

Checking Connectivity between Router-R1 and Router-R4

The following procedure for checking connectivity between Router-R1 and Router-R4 over a WAN is similar to the procedure for checking connectivity in which no WAN is involved:

Step 1 Use the **ping** EXEC command between Router-R1 and Router-R4 to verify that traffic is going through the WAN. Figure 9-17 illustrates output from the **ping** command.

Figure 9-17 Output from the ping Command

```
Router-R1# ping 49.0001.0001.0000.0000.1004.00
Type escape sequence to abort.
Sending 5, 100-byte CLNS Echos with timeout 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/40 ms
```

S2633

Step 2 Use the **trace** EXEC command to verify connectivity from Router-R4 to Router-R5 and from Router-R5 to Router-R1, as shown in Figure 9-18.

Figure 9-18 Output from the trace Command

```
Router-R4# trace 49.0001.0001.0000.0000.1001.00
Type escape sequence to abort.
Tracing the route to 49.0001.0001.0000.0000.1001.00
  1 49.0001.0001.0000.0000.1005.00 28 msec ! 28 msec ! 28 msec !
  2 49.0001.0001.0000.0000.1001.00 35 msec ! 35 msec ! 35 msec !
```

S2634

Step 3 Use EXEC **show** commands to display the routing table and adjacency database information for the routers. Figure 9-19 and Figure 9-20 illustrate the **show** command output for ISO-IGRP and IS-IS.

If you are running ISO-IGRP, use the **show clns route** EXEC command.

Figure 9-19 Output of the show clns route Command

```
Router-R4# show clns route
ISO-IGRP Routing Table for Domain 49.0001, Area 0001
System Id       Next-Hop        SNPA            Interface   Metric   State
0000.0000.1005  0000.0000.1005  DLCI 45         Serial1.1   8476     Up
0000.0000.1001  0000.0000.1005  DLCI 45         Serial1.1   9532     Up
0000.0000.1002  0000.0000.1005  DLCI 45         Serial1.1   9982     Up
0000.0000.1003  0000.0000.1005  DLCI 45         Serial1.1   9982     Up
0000.0000.1004  0000.0000.0000  --              --          0        Up

ISO-IGRP Routing Table for Domain 49.0001
Area Id         Next-Hop        SNPA            Interface   Metric   State
0001            0000.0000.0000  --              --          0        Up

CLNS Prefix Routing Table
49.0001.0001.0000.0000.1004.00, Local NET Entry
```

S2635

If you are running IS-IS, use the **show isis routes** EXEC command.

Figure 9-20 Output of the show isis routes Command

```
Router-R4# show isis routes
IS-IS Level-1 Routing Table - Version 9
System Id       Next-Hop        SNPA            Interface   Metric  State
0000.0000.1005  0000.0000.1005  DLCI 45         Serial1.1   10      Up
0000.0000.1001  0000.0000.1005  DLCI 45         Serial1.1   20      Up
0000.0000.1002  0000.0000.1005  DLCI 45         Serial1.1   30      Up
0000.0000.1003  0000.0000.1005  DLCI 45         Serial1.1   30      Up
0000.0000.1004  0000.0000.0000  --              --          0       Up
```

S2636

Step 4 Check the adjacency database entries by using the **show clns neighbors** and **show clns neighbors detail** EXEC commands to verify that the correct area address information is being advertised and that the routers contain entries in their adjacency databases.

Step 5 If there are no adjacency database entries, verify that the **frame relay map** interface configuration commands are correct for each interface or subinterface.

Step 6 If the **show isis routes** command does not show Router-R5, yet it appears in the adjacency database, there may be a problem in the IS-IS LSP. Use the **show isis database** EXEC command to verify that the LSPs between the routers point to one another and that they are synchronized.

Step 7 For ISO-IGRP, use the **debug clns igrp** privileged EXEC command to verify that the routers are receiving advertised routes.

After you correct the problems with the adjacencies and routes, you should have connectivity.

ISO CLNS Route Redistribution Loops

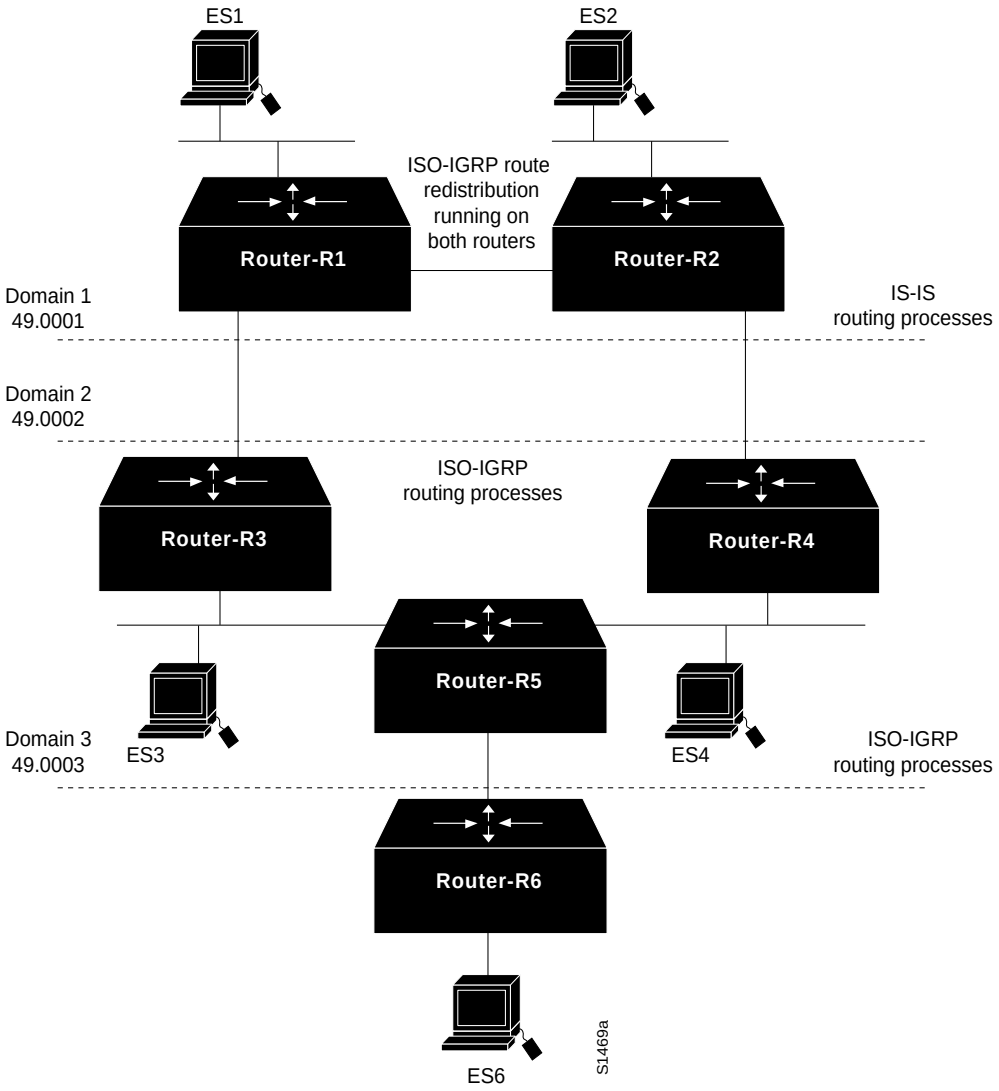
Figure 9-21 shows three domains, two of which are running ISO-IGRP and one that is running IS-IS. Domain 1 runs IS-IS routing processes internally, while routers R1 and R2 redistribute IS-IS and ISO-IGRP routes. Domain 2 and domain 3 run ISO-IGRP routing processes. To summarize the situation, a routing loop exists between Router-R1 and Router-R2 that blocks traffic between domain 1 and domain 3.

Environment Description

The relevant elements of the internetworking environment shown in Figure 9-21 can be summarized as follows:

- Domain 1 has two Level 1 and Level 2 border routers that perform route redistribution between IS-IS and ISO-IGRP.
- Domain 2 and domain 3 are running ISO-IGRP.

Figure 9-21 Route Redistribution Loops



Diagnosing and Isolating Route Redistribution Loops

This section describes how routing loops can occur in the topology shown in Figure 9-21, and gives specific recommendations for eliminating routing loops.

Initially, the redistributing routers (Router-R1 and Router-R2) have 49.0001 in their routing tables as an IS-IS route. This route is redistributed into ISO-IGRP, which causes 49.0001 to be advertised into domain 49.0002 at two points. The 49.0001 advertisement propagates throughout domain 49.0002 and returns to the redistributing routers. By default, the redistributing routers place the ISO-IGRP route in their routing tables with a next-hop pointing outside of the domain toward 49.0002. This pointer is erroneous because 49.0001 cannot be reached directly through domain 49.0002.

When an ES in domain 49.0002 originates a packet to an ES in 49.0001, the packet reaches one of the redistributing routers, which attempts to forward the packet back to domain 49.0002. A packet-forwarding loop occurs, and the packet is never delivered.

The manner in which the routing algorithms are run gives preference to ISO-IGRP routes over IS-IS routes when default route metrics are used. Because Router-R1 and Router-R2 both advertise an ISO-IGRP route to 49.0003, packets from 49.0001 (domain 1) to 49.0003 get caught in a loop because Router-R1 and Router-R2 use the preferred ISO-IGRP route to 49.0003 rather than the IS-IS route. That is, Router-R1 has a choice of sending a packet to 49.0003 through the ISO-IGRP route from Router-R3, or through the IS-IS route that has been redistributed by Router-R2. It chooses the ISO-IGRP route. Router-R2, upon receiving the packet faces the same choice of routes: ISO-IGRP to Router-R1 or IS-IS to Router-4. The packet never escapes this loop.

To prevent a route redistribution loop, you must make the IS-IS route win at Router-R2 and lose at Router-R1 by setting the administrative distance so that the IS-IS route is preferred. The steps that follow describe how to verify that a routing loop exists and how to correct it by modifying the router configuration:

Step 1 Use the **trace route** EXEC command to discover where the loop occurs.

Step 2 Use the **show isis database** EXEC command to display the LSP database and look at the routes in the suspect loop.

Step 3 Use the **debug isis update packets** privileged EXEC command and look at the debug output to pinpoint the problem. Refer to the *Debug Command Reference* publication for a description of debug output.

Step 4 After you find and verify the route redistribution loop, change the configuration of Router-R2 so that its IS-IS route to 49.0003 is preferred over the ISO-IGRP route back to Router-R1. Figure 9-22 shows the commands that resolve the routing loop.

Figure 9-22 Router Configuration That Resolves Routing Loop

```
router isis
network 49.0001.0001.1111.1111.1111.00
router iso-igrp emana
network 49.0002.0001.2222.2222.2222.00

interface ethernet 0
clns router isis

interface ethernet 1
clns router iso-igrp emana

router iso-igrp emana
redistribute isis

router isis
redistribute iso-igrp emana
!
!To break the loop
!
router isis
distance 90
```

S2637

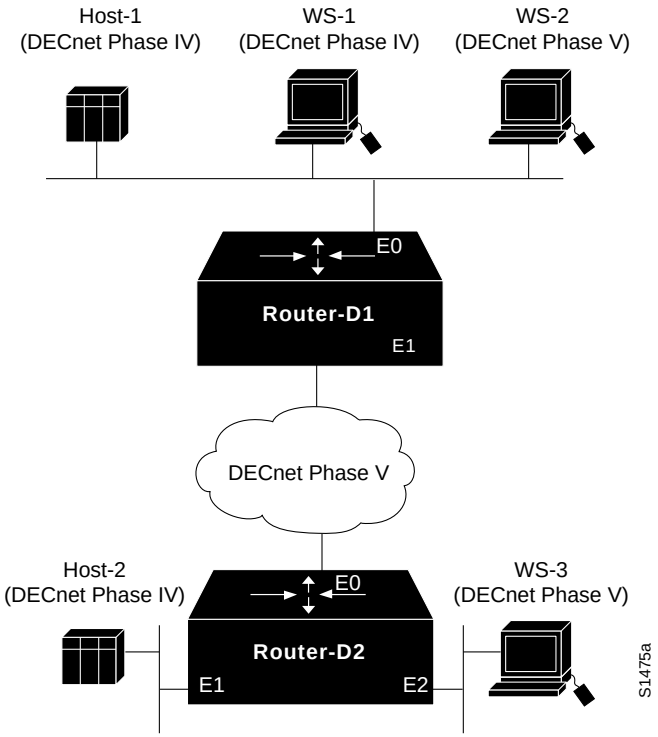
Add the distance metric as shown. The administrative distance of 90 for the IS-IS process in Router-R2 assures its precedence over the ISO-IGRP route back to Router-R1. Packets received by Router-R1 for 49.0003 are sent to Router-R2, where they are sent on to their destination, eliminating the routing loop.

DECnet Phase IV and Phase V Connectivity

Figure 9-23 illustrates a network that consists of both DECnet Phase IV and DECnet Phase V nodes. Some Phase IV nodes communicate through a DECnet Phase V cloud; others rely on DECnet Phase IV-to-Phase V conversion performed in the router. The following facts summarize the situation:

- The DECnet Phase IV node Host-1 cannot communicate with the DECnet Phase IV node Host-2 through the DECnet Phase V cloud.
- The DECnet Phase IV node WS-1 cannot communicate with the DECnet Phase V node WS-3.

Figure 9-23 DECnet Phase IV and Phase V Network



Environment Description

The relevant elements of the internetworking environment shown in Figure 9-23 can be summarized as follows:

- Router-D1 and Router-D2 perform DECnet Phase IV-to-Phase V conversion on all interfaces.
- All routers and nodes are in the same area.
- Other systems that make up the DECnet Phase V cloud are not relevant to the communication problems described in the scenario.

Diagnosing and Isolating Problem Causes for DECnet Phase IV Connectivity through a Phase V Cloud

The following problems are potential causes for the first symptom. (Two DECnet Phase IV nodes cannot communicate through a DECnet Phase V cloud.)

- DECnet conversion has not been enabled on the interfaces.
- The conversion prefix, which is required for packet conversion, is specified incorrectly.
- The DECnet Phase IV nodes are not configured to be in the same area.
- There is a connectivity problem.

In general, it is useful to eliminate most likely problems first and then to tackle more complex problems as necessary. The problem-solving process that follows illustrates this strategy.

Checking DECnet Conversion Processes and Prefixes on the Interface

In order for a DECnet Phase IV packet to pass through a DECnet Phase V cloud, DECnet conversion must be enabled on all router interfaces in the path, and the conversion prefixes must be specified correctly.

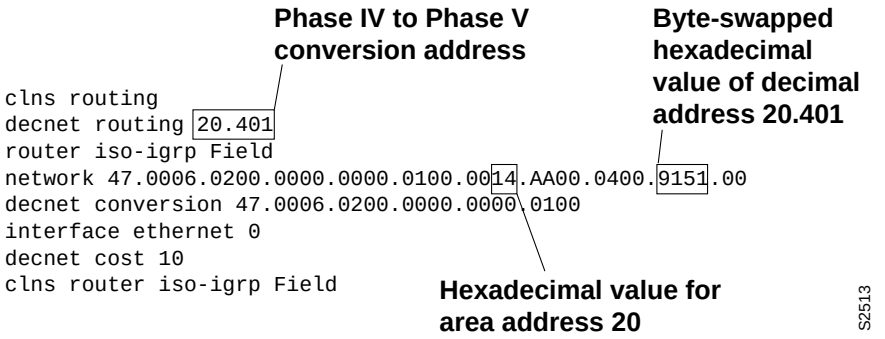
Use the following procedure to check the configuration of DECnet conversion prefixes:

Step 1 Use the **write terminal** EXEC command to list the configuration of the router. Verify that both ISO CLNS routing and DECnet routing are enabled on the router.

Step 2 Check that the **network** command correctly specifies the DECnet routing process node ID. You must enter, in hexadecimal, the *byte-swapped* address for the Phase IV-to-Phase V conversion address.

For example, the decimal Phase IV-to-Phase V conversion address 20.401 is converted as follows: (20 * 1024) + 401 = 20,881. The hexadecimal value of 20,881 is 5191. When the bytes are swapped, it becomes 9151. Figure 9-24 includes an example of the **network** command.

Figure 9-24 DECnet Conversion Commands



Step 3 Verify that the DECnet area ID is correctly converted to its hexadecimal value; in this case DECnet area 20 (decimal) equals 14 (hexadecimal).

Step 4 Use the debugging commands **debug decnet routing** and **debug clns packet** at Router-D1 to observe the Phase IV packet getting converted to Phase V (at Router-D1), going through the Phase V cloud, and reaching Router-D2, where it is converted back to Phase IV.

Checking Area Addresses

One of the requirements for DECnet Phase IV-to-Phase V conversion is that the DECnet node, which is an ES, and the converting router, which is an IS, must be in the same area. If the ES and IS are in different areas, no conversion takes place.

Use the following procedure to check area addresses:

Step 1 Use the **show decnet route** EXEC command to display the DECnet routing tables. The area ID for the DECnet node and for the router must be the same, as shown in Figure 9-25.

Figure 9-25 Output of the show decnet route Command

```
router-d1# show decnet route

  Node       Cost  Hops   Next Hop to Node       Expires  Prio

*1.1           4     1    (PhaseV)                 276
*1.2           4     1   Ethernet1 -> 1.2           44     64    V
*1.3           4     1   Ethernet1 -> 1.3           31     64    V
*1.5           0     0     (Local) -> 1.5                          S2639
```

Step 2 If the area IDs do not match, verify that the DECnet-to-CLNS address conversion was done correctly, or reconfigure the router with an area address that matches the DECnet host.

Step 3 Use the **show clns neighbors** EXEC command to display the CLNS adjacency database. This command shows the addresses of all CLNS neighbors and can indicate area address problems with adjacent systems.

Step 4 Use the **show clns route** EXEC command to display the CLNS routes. This command is useful when the routers are not adjacent. You should see an address entry for the Phase IV router. If not, proceed to the next section, "Checking Connectivity."

Checking Connectivity

After checking the most common problems (incorrect DECnet-to-CLNS address conversion and different area IDs for the DECnet host and the router), verify the connectivity between the routers and the hosts.

Use the following procedure to check connectivity:

Step 1 Use the **ping** EXEC command to see whether connectivity can be established between Router-D1 and Host-2 through the DECnet Phase V cloud, as shown in Figure 9-26.

Figure 9-26 Output of the ping Command for DECnet Phase IV

```
Router-D1# ping
Protocol [ip]: decnet
Target DECnet address: 1.7
Repeat count [5]:
Datagram size [10]:
Timeout in seconds [5]:
Verbose [n]:
Type escape sequence to abort.
Sending 5, DECnet echos to 1.7, timeout is 5 seconds:
.....                                                          S2640
Success rate is 0 percent (0/5)
```

Step 2 By using a combination of the **show clns route, show clns neighbors**, and **show decnet route** EXEC commands to display routing information and the **ping** command to check connectivity, you can quickly locate and diagnose connectivity problems.

Step 3 Correct any addressing errors or router configuration errors that you find.

Diagnosing and Isolating Problem Causes for DECnet Phase IV-to-Phase V End Systems

The following problems are potential causes for the second symptom. (A DECnet Phase IV node cannot communicate with a DECnet Phase V node.)

- The DECnet Phase V system ID is not compatible with DECnet Phase IV.
- DECnet conversion must be enabled on the interfaces.

Checking System IDs

DECnet Phase IV allows a maximum of 63 system IDs, numbered 1 through 63. When a DECnet Phase IV node communicates with a DECnet Phase V node, no problem exists for the system ID conversion. However, DECnet Phase V allows more than 63 system IDs, which causes problems if the node tries to communicate with a DECnet Phase IV node.

Use the following procedure to check system IDs:

Step 1 At the DECnet Phase V node, check the system ID entry in the CLNS address of the node. If it is larger than 3F hexadecimal (63 decimal), it cannot communicate with a DECnet Phase IV node.

Step 2 If necessary, reconfigure the system ID of the DECnet Phase V node to a value of 63 or less.

Checking DECnet Conversion

The conversion problems that you might encounter when a Phase IV system communicates with a Phase V system are nearly identical to those you might encounter when a Phase IV system communicates through a Phase V cloud.

Use the following procedure to verify that DECnet conversion is configured correctly:

Step 1 Check the router configuration and verify that both DECnet and CLNS routing processes are enabled.

Step 2 Verify that the host (ES) and the router (IS) that are performing the conversion are in the same area.

Step 3 Check that the DECnet Phase IV decimal addresses are correctly converted and entered in the byte-swapped hexadecimal conversion format.

Step 4 Use the **show clns route**, **show clns neighbors**, and **show decnet route** EXEC commands to display routing information and verify that the routes are being propagated.

Step 5 Use the **ping** EXEC command to verify connectivity throughout the path.

Problem Solution Summary

This scenario focused on diagnosing DECnet Phase IV-to-Phase V conversion problems. The solutions included the following:

- Conversion prefixes were verified for proper Phase IV decimal notation to Phase V byte-swapped hexadecimal notation.
- Router commands that enable the conversion processes were verified.
- Area addresses for ES to IS conversion were checked to make certain both systems were in the same area.
- System IDs were verified for DECnet Phase IV-to-Phase V compatibility, where a Phase V host communicates with a Phase IV host.

Figure 9-27 and Figure 9-28 provide representative configuration listings for routers discussed in this scenario.

Figure 9-27 Relevant DECnet Phase IV-to-Phase V Conversion Configuration for Router-D1

```
clns routing
!
decnet routing 1.5
decnet node-type routing-iv
decnet conversion 49
!
!
interface ethernet 0
ip address 160.89.48.9 255.255.255.0
!
interface ethernet 1
ip address 160.89.49.9 255.255.255.0
decnet cost 4
clns router iso-igrp

router iso-igrp                      S2641
network 49.0001.aa00.0400.0504.00
```

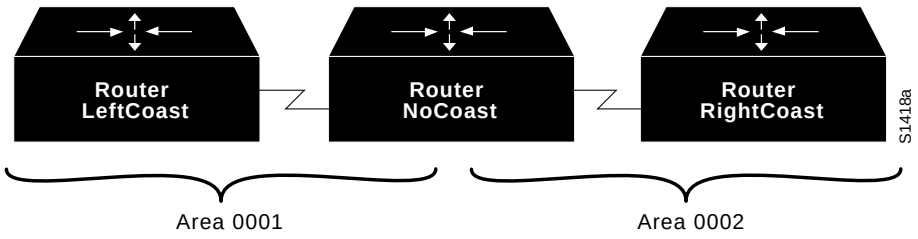
Figure 9-28 Relevant DECnet Phase IV-to-Phase V Conversion Configuration for Router-D2

```
clns routing
!
decnet routing 1.6
decnet node-type routing-iv
decnet conversion 49
!
!
interface ethernet 1
ip address 160.89.49.2 255.255.255.0
decnet cost 4
!
interface ethernet 3
ip address 160.89.35.2 255.255.255.0
clns router iso-igrp
!
interface ethernet 4
ip address 160.89.36.2 255.255.255.0
decnet cost 4
clns router iso-igrp
!
router iso-igrp                    S2642
network 49.0001.aa00.0400.0604.00
```

NCR/AT&T StarGroup Considerations

This section provides a configuration example that illustrates issues that are specific to the NCR/AT&T StarGroup implementation of ISO CLNS. In this example, three routers connect two areas via serial interfaces. Figure 9-29 represents the topology of the network.

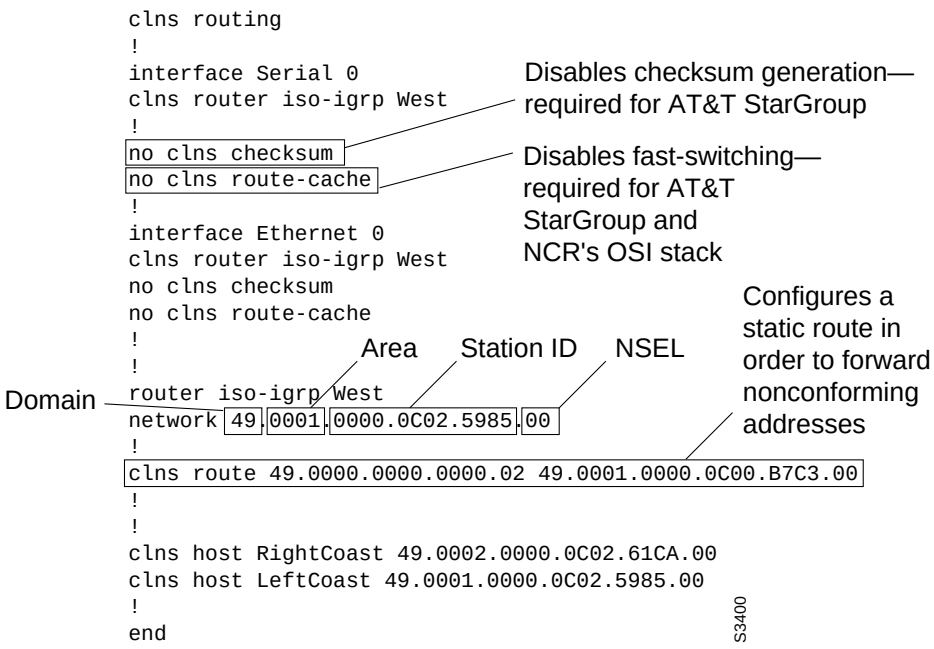
Figure 9-29 StarGroup Topology Example



Note Putting each router in its own area (for a total of three) would reduce the number of routing updates sent across the serial lines.

Figure 9-30 shows the configuration for Router LeftCoast.

Figure 9-30 Configuration for Router LeftCoast



Because of a problem in the AT&T StarGroup checksum calculation, checksum generation must be disabled on the router. Use the **no clns checksum** interface configuration command to disable checksum generation on the router.

Fast switching must be disabled as well, because the Cisco router will pad odd-length packets when fast switching. Both the AT&T StarGroup and the NCR ISO CLNS protocol stacks will discard packets in which the value of the 802.3 length field no longer matches the length calculated from the header information. Padding packets while fast switching causes this value to change, resulting in packet drops. Use the **no clns route-cache** interface configuration command to disable fast switching.

Note The AT&T StarGroup implementation requires that the station ID portion of the NSAP (see Figure 9-30) match the MAC address of that station. In order to interoperate, the Cisco router must make the same requirement. However, this is generally neither a Cisco nor an ISO requirement.

Another consideration when using the AT&T StarGroup implementation is the necessity of using the **clns route** global configuration command. StarGroup uses a 16-octet NSAP, which does not follow the ISO 8348/AD2 specification, in order to preserve backward compatibility with earlier versions of StarGroup. The **clns route** command, by configuring a static route, ensures that the router passes packets using the older StarGroup NSAP address prefix to the next neighbor in the path (in this case, NoCoast).

Figure 9-31 shows the output of the **show clns route** EXEC command for Router LeftCoast. This command displays all of the destinations to which the router knows how to route packets. Note that the static route entry shows the nonconforming NSAP (that is, the 16-octet NSAP) used by older

StarGroup software. The **show clns route** command is useful in determining the next-hop router and whether static routes have been configured. (For more information on the various fields in the **show clns route** command, see the *Router Products Command Reference* publication.)

Figure 9-31 show clns route Command Output for Router LeftCoast

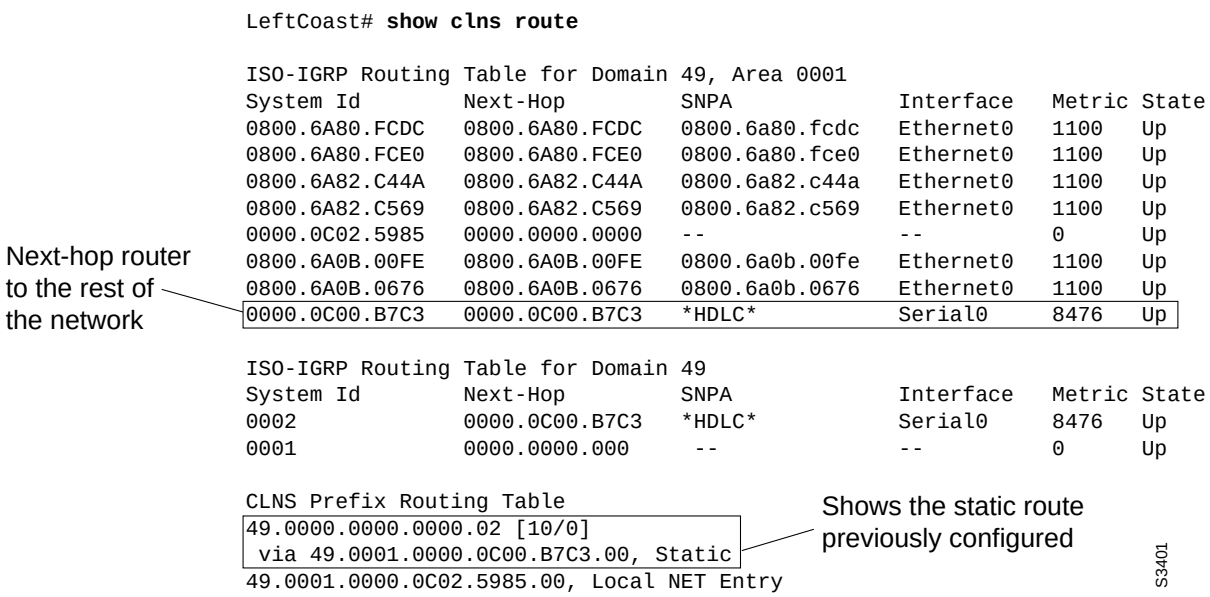
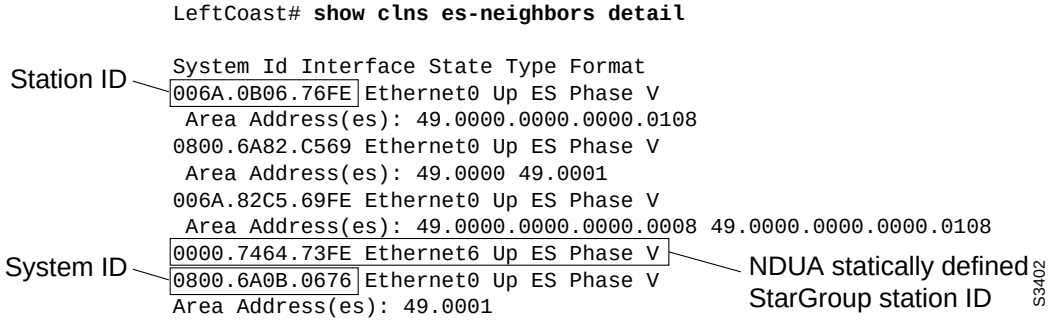


Figure 9-32 shows the output of the **show clns es-neighbors detail** EXEC command for Router LeftCoast. This command shows the table constructed by the router from Hellos sent by its end system neighbors. The **detail** keyword must be included if you want to see NSAP information for nonconforming neighbors.

Note The station ID and the system ID noted in Figure 9-32 actually match, but are parsed differently because they are StarGroup nonconforming NSAPs.

The **show clns es-neighbors detail** command also shows the statically defined NetBIOS Directory User Agent (NDUA) station ID. The NDUA is a special station ID and function as a sort of name-server for StarGroup. There must be at least one primary NDUA configured for each area.

Figure 9-32 show clns es-neighbors detail Command Output for Router LeftCoast



The configuration for Router NoCoast is shown in Figure 9-33. As was done with Router LeftCoast, static routes are configured to ensure that nonconforming StarGroup addresses are forwarded properly.

Figure 9-33 Configuration for Router NoCoast

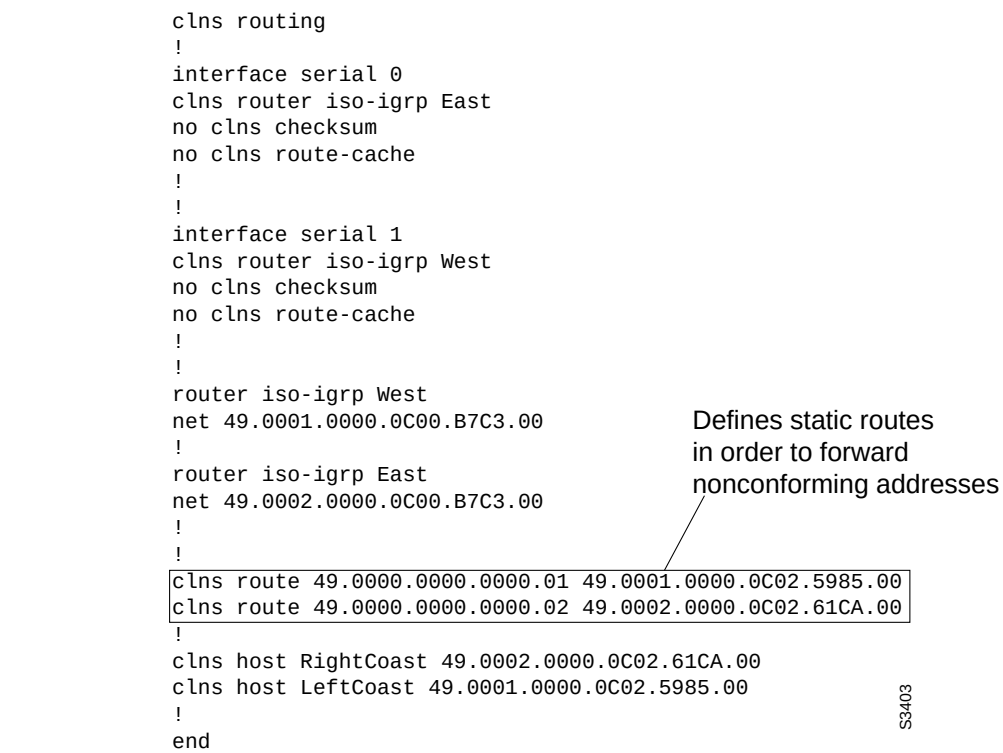


Figure 9-34 shows the output from the **show clns route** EXEC command. Note that adjacent areas and the static routes configured on the router appear in the routing table.

Figure 9-34 show clns route Command Output for Router NoCoast

```
NoCoast# show clns route

ISO-IGRP Routing Table for Domain 49, Area 0001
System Id           Next-Hop           SNPA         Interface    Metric    State
0800.6A80.FCE0      0000.0C02.5985      *HDLC*      Serial0      7476      Up
0800.6A80.FCDC      0000.0C02.5985      *HDLC*      Serial0      7476      Up
0800.6A82.C44A      0000.0C02.5985      *HDLC*      Serial0      7476      Up
0000.0C00.B7C3      0000.0000.0000      --          --           0         Up

ISO-IGRP Routing Table for Domain 49
System Id           Next-Hop           SNPA         Interface    Metric    State
0002                0000.0000.0000     --          --           0         Up
0001                0000.0000.0000     --          --           0         Up

ISO-IGRP Routing Table for Domain 49, Area 0002
System Id           Next-Hop           SNPA         Interface    Metric    State
0800.6A82.C36F      0000.0C02.61CA      *HDLC*      Serial1      8476      Up
0800.6A82.C3C8      0000.0C02.61CA      *HDLC*      Serial1      8476      Up
0800.6A82.C3D5      0000.0C02.61CA      *HDLC*      Serial1      8476      Up
0800.6A82.C415      0000.0C02.61CA      *HDLC*      Serial1      8476      Up
0800.6A82.C42F      0000.0C02.61CA      *HDLC*      Serial1      8476      Up
0800.6A81.DD6D      0000.0C02.61CA      *HDLC*      Serial1      8476      Up
0000.0C00.B7C3      0000.0000.0000      --          --           0         Up
0800.6A82.27C1      0000.0C02.61CA      *HDLC*      Serial1      8476      Up
0800.6A82.3CDB      0000.0C02.61CA      *HDLC*      Serial1      8476      Up

CLNS Prefix Routing Table
49.0001.0000.0C00.B7C3.00, Local NET Entry
49.0002.0000.0C00.B7C3.00, Local NET Entry
49.0000.0000.0000.01 [10/0]
 via 49.0001.0000.0C02.5985.00, Static
49.0000.0000.0000.02 [10/0]
 via 49.0002.0000.0C02.61CA.00, Static
```

Adjacent areas

Shows the static routes previously configured

S3404

The configuration for Router RightCoast is basically the reverse of Router LeftCoast.

NCR/AT&T StarGroup X.25 Encapsulation

When you choose X.25 encapsulation, you must manually enter the NSAP-to-X.121 address mapping. Assume that two routers, Router-A and Router-B, are communicating over an X.25 link through their serial interfaces. Configuration commands for interface serial 0 on Router-A are as follows:

```
interface serial 0
encapsulation x25
x25 address 777777022
clns router static area0099
no clns checksum
```

Replace the X.25 address in this example with your address.

Note When multiple switched virtual circuits are established between two routers, the packets can arrive out of sequence. Out-of-sequence packets will cause excessive delay. Use the **x25 nvc 1** interface configuration command to limit the number of virtual circuits that can be established between hosts.

Because no routing updates are sent over an X.25 link, the remainder of the interface configuration commands for Router-A define the address of Router-B and establish a static route:

```
clns is-neighbor 49.0001.0000.0c00.1b87.00 7777770020
clns route 49.0001 49.0001.0000.0c00.1b87.00
clns route 49.0000.0000.0000.01 49.0001.0000.0c00.1b87.00
```

Interface configuration commands for Router-B are as follows:

```
interface serial 0
encapsulation x25-dce
x25 address 777777020
clns router static area01
no clns checksum
clns is-neighbor 49.0099.0000.0c00.029e.00 7777770022
clns route 49.0099 49.0099.0000.0c00.029e.00
clns route 49.0000.0000.0000.99 49.0099.0000.0c00.029e.00
```

Note When you are configuring X.25 encapsulation on a serial interface, the interfaces must maintain a Data Communications Equipment (DCE)/Data Terminal Equipment (DTE) relationship. You must specify one router interface, such as interface serial 0 on Router-B, as DCE. Alternatively, if you use a switch to connect two routers, the switch presents a DCE interface to each router, and Router-A and Router-B are configured with DTE interfaces.

ISO CLNS Connectivity Symptoms

ISO CLNS connectivity symptoms are discussed in the following sections:

- Host Cannot Communicate with Offnet Hosts
- Host Cannot Access Certain Hosts in Same Area
- Host Cannot Access Certain Hosts in Different Area
- Users Can Access Some Hosts but Not Others
- Some Services Are Available While Others Are Not
- Users Cannot Make Any Connections when One Parallel Path Is Down
- Router Sees Duplicate Routing Updates and Packets
- Routing Not Working when Redistribution Is Used
- Redistribution route-map Commands Behave Unexpectedly

Note The symptoms that follow are generic in nature; however, discussions of host configuration problems assume that the host is a UNIX system. Equivalent kinds of actions may also be applicable to non-UNIX hosts, but the discussions do not address non-UNIX end station problems.

Host Cannot Communicate with Offnet Hosts

Symptom: Host cannot communicate with a host on another network. Attempts to make a connection to an intervening router might not be successful. Table 9-2 outlines possible causes and suggested actions when a host cannot communicate with offnet hosts.

Table 9-2 ISO CLNS: Host Cannot Communicate with Offnet Hosts

Possible Causes	Suggested Actions
No default gateway	**Step 1** Determine whether a default gateway is included in the adjacency table of the host attempting to make a connection (Host-A). Use the following UNIX command: **netstat -rn** **Step 2** Inspect the output of this command for a default gateway specification. **Step 3** If the specified default gateway is incorrect, or if it is not present at all, you can change or add a default gateway using the following UNIX command at the local host: **route add default** *address* **1** (The value of *address* is the ISO CLNS address of the default gateway; a value of 1 indicates that the specified node is one hop away.) **Step 4** To automate the addition of a default gateway as part of the boot process, specify the ISO CLNS address of the default gateway in the following file on the UNIX host: */etc/defaultrouter*
End system has no Level 1 router	**Step 1** Use the **show clns neighbors detail** EXEC command to show all end systems (ESs) and intermediate systems (ISs) to which the router is directly connected. **Step 2** Make sure that there is at least one Level 1 router on the same network as the end system.
Level 1 router or ES has bad address	**Step 1** At the Level 1 router, verify that it has the same address as the end system. **Step 2** Verify that all bytes of the NSAP address, up to but not including the system ID, are the same on both the router and the ES. The domain and area addresses must match, and the station IDs must be unique. The value of the n-selector byte has no impact.

Possible Causes	Suggested Actions
End system host is not running ES-IS protocol	**Step 1** Use appropriate host commands to verify that an ES-IS process is running. If necessary, initiate the ES-IS process. **Step 2** Check the adjacency database on the host and verify that it has an entry for its directly connected router. **Step 3** Use the **debug clns packet** privileged EXEC command to verify that the router sees and forwards the packet. **Step 4** If necessary, statically configure the router to recognize the ES by using the **clns es-neighbor** interface configuration command.
Router between hosts is down	**Step 1** Use the **trace** EXEC command to check connectivity between a router and an end system. **Step 2** If the trace fails at a router, use the **show clns neighbors** EXEC command to see which neighboring routers and ESs are recognized. **Step 3** If neighboring routers and end systems are up, perform one of the following procedures: • For ISO-IGRP, check the routing table and see whether the routes are being learned. Use the **show clns route** EXEC command to display the routing tables. • For IS-IS, check the LSP database to see whether the links are being reported in link state advertisements, then check the IS-IS routing table to see whether the routes are being installed in the routing table. Use the **show isis database detail** EXEC command to display the routing tables.

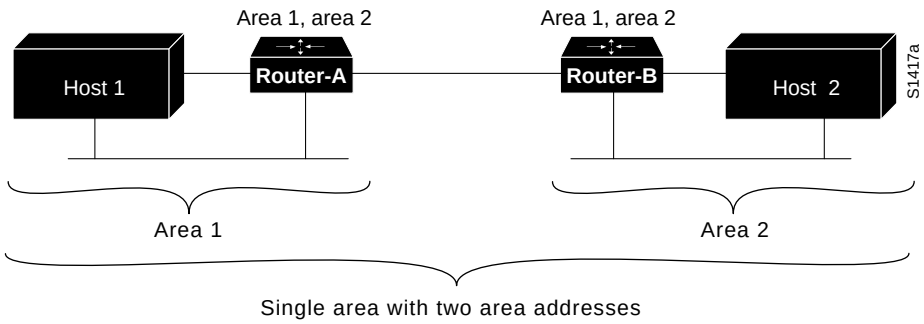
Host Cannot Access Certain Hosts in Same Area

Symptom: A host cannot access other hosts in the same area. The host is either on the same network or on a different network in the same area, but is unable to establish connectivity. Some networks might be accessible. Table 9-3 outlines possible causes and suggested actions when a host cannot access certain hosts in the same area.

Table 9-3 ISO CLNS: Host Cannot Access Hosts in Same Area

Possible Causes	Suggested Actions
Area address is configured incorrectly on the host	**Step 1** Check all Level 1 routing tables and link state databases. **Step 2** Verify that the hosts are in the same area. **Step 3** Check that the NSAP address is entered correctly on the hosts.
Different area addresses are merged into a single area, but the router is configured incorrectly	**Step 1** See whether your configuration includes multiple area addresses. **Step 2** Verify that the router is configured to support a multihomed area, which is a single area that has more than one area address. **Step 3** Figure 9-35 shows an example of a multihomed area. • In order to communicate, two routers must establish Level 1 adjacency. • For area 1 and area 2 to be considered a single area, Router-A must be configured to be in area 1 and area 2. Router-B can be configured in both areas as well. **Step 4** Alternatively, one router can be configured in both areas, while the other router remains configured for a single area. For example, Router-A is in both area 1 and area 2, while Router-B is in area 2 only. Area addresses must overlap to create Level 1 adjacency and establish connectivity.
End system host is not running ES-IS protocol	**Step 1** See Table 9-2 for suggested actions.
Router between hosts is down	**Step 1** See Table 9-2 for suggested actions.

Figure 9-35 Multiple Area Addresses in a Multihomed Area



Host Cannot Access Certain Hosts in Different Area

Symptom: A host cannot access a host in a different area. The host tries to access another host that is not in its adjacency database or link state database by going through a Level 2 router. Table 9-4 outlines possible causes and suggested actions when a host cannot access hosts in a different area.

Table 9-4 ISO CLNS: Host Cannot Access Hosts in Different Area

Possible Causes	Suggested Actions
Host is not really in a different area	**Step 1** Verify that the hosts are in different areas. **Step 2** Verify that the host is not part of a multihomed area. **Step 3** Reenter the host address and specify the correct area.
Level 2 routers are not routing packets to the correct area	**Step 1** Verify connectivity to the border of the area. Use the **trace** command to verify that Level 1 routers are routing packets to the nearest Level 2 router. **Step 2** Verify that the Level 2 routers are routing packets to the correct area. Use the **trace** EXEC command to check Level 2 routing. **Step 3** Check the Level 2 topology by inspecting the Level 2 routing tables (ISO-IGRP) or the Level 2 link state databases (IS-IS) to see that the routing is to the correct area. **Step 4** If necessary, reconfigure the router(s) with the correct area addresses and Level 2 (IS-IS) routing information.
End system host is not running ES-IS protocol	**Step 1** See Table 9-2 for suggested actions.
Router between hosts is down	**Step 1** See Table 9-2 for suggested actions.

Users Can Access Some Hosts but Not Others

Symptom: Users cannot access certain hosts that should be available. This type of problem results from router or host configuration errors or from a router that is down. For troubleshooting guidelines, refer to the sections “Host Cannot Communicate with Offnet Hosts,” “Host Cannot Access Certain Hosts in Same Area,” and “Host Cannot Access Certain Hosts in Different Area,” earlier in this chapter.

Some Services Are Available While Others Are Not

Symptom: In some cases, you might be able to get through to hosts using some protocols, but cannot get through using others. Table 9-5 outlines possible causes and suggested actions when some services are available while others are not.

Table 9-5 ISO CLNS: Some Services Are Available While Others Are Not

Possible Causes	Suggested Actions
Host is not configured to support the service	**Step 1** Verify that the needed services are running on the host system.
Misconfigured access list	**Step 1** Use the **trace** EXEC command to determine the path taken to reach remote hosts. **Step 2** (Optional) On each router in the path, enable the **debug clns routing** privileged EXEC command. Any router that returns "unreachables" is suspect. **Step 3** If you can verify the router that is stopping traffic, use the **write terminal** privileged EXEC command to see whether an access list is being used. You also can use the **show access-lists** and **show clns interface** EXEC commands in combination to determine whether access lists are being used. **Step 4** Disable the access list. **Step 5** See whether traffic can get through the router. **Step 6** If traffic can get through, carefully review the access list and its associated commands for proper authorization. In particular, look for an ISO port configured in the access lists. **Step 7** If ports are specified, be sure that all needed ports are explicitly permitted by access lists. **Step 8** Enable the access list and verify reachability of service.

Users Cannot Make Any Connections when One Parallel Path Is Down

Symptom: In configurations featuring multiple paths between networks, when one of the parallel links breaks, there is no communication through the alternative routes.

Note IS-IS has equal-cost load balancing for both Level 1 and Level 2 routes. If there are parallel paths in an IS-IS network and one goes down, the other is available as a "hot backup"; that is, it is ready to be used immediately.

Table 9-6 outlines possible causes and suggested actions when users cannot make connections over a parallel path.

Table 9-6 ISO CLNS: Users Cannot Make Connections over Parallel Path

Possible Causes	Suggested Actions	
Discontinuous network due to failure	**Step 1**	Restore the link.
Routing has not yet converged	**Step 1**	Examine the routing tables for routes listed as "possibly down." This entry indicates that the routing protocol has not converged.
	Step 2	Wait for the routing protocol to converge. Examine the routing table later. ISO-IGRP only does load balancing for domain prefix routes. If you are doing Level 1 or Level 2 routing in ISO-IGRP, only a single path is maintained. If that path goes down, you must wait for convergence before the alternative path is available.
Misconfigured access lists or other routing filters	**Step 1**	Check for access lists in the path.
	Step 2	If present, disable and determine whether traffic is getting through. If traffic is getting through, access lists and accompanying commands are probably causing traffic stoppage.
	Step 3	Evaluate and modify access lists as necessary.
Errors on serial link	**Step 1**	If the link is a serial link, look for input on the interface by using the **show interfaces serial** EXEC command.
	Step 2	Refer to the discussions regarding serial line debugging in Chapter 3, "Troubleshooting Serial Line Problems," and Chapter 1, "Troubleshooting Overview," for more information.
Errors on Ethernet link	**Step 1**	Use a time domain reflectometer (TDR) to find any unterminated Ethernet cables.
	Step 2	Check host cables and transceivers to determine whether any are incorrectly terminated, overly long, or damaged.
	Step 3	Look for a jabbering transceiver attached to a host; this might require a host-by-host inspection.

Possible Causes	Suggested Actions
Nonfunctional FDDI ring	**Step 1** Use the **show interfaces fddi** EXEC command to determine status of the interface. **Step 2** If **show interfaces fddi** EXEC indicates that the interface and line protocol are up, use the **ping clns** EXEC command between routers to test connectivity to routers. **Step 3** If the interface and line protocol are up, make sure that the addresses of upstream and downstream neighbors are as expected. If all zeros appear in either of the address fields for these neighbors, a physical connection problem is likely. **Step 4** In this case (or if status line does *not* indicate that interface and line protocol are up), check patch-panel connections. Use an optical TDR or light meter to check connectivity between routers; ensure that signal strength is within specification.
Nonfunctional Token Ring backbone	**Step 1** Use the **show interfaces token** EXEC command to determine status of the interface. **Step 2** If the status line indicates that the interface and line protocol are not up, check the cable from router to the Multistation Access Unit (MAU). Make sure that the cable is good; replace if necessary. **Step 3** If **show interfaces token** indicates that the interface and line protocol are up, use the **ping clns** EXEC command between routers to test connectivity to them. **Step 4** If the remote router does not respond, check the ring speed specification on all systems attached to the Token Ring backbone. Ring speed must be the same for all. **Step 5** If necessary, modify ring speed specifications for the ES and routers. **Step 6** Use the **ring-speed** interface configuration command to modify ring speed configuration for Token Ring cards that support software speed configuration. Change jumpers as needed for modular router platforms. For more information about ring speed specifications, refer to the hardware installation and maintenance documentation for your system. For additional hints on solving Token Ring problems, refer to the "Troubleshooting Router Startup Problems" chapter.

Router Sees Duplicate Routing Updates and Packets

Symptom: When the router sees duplicate routing updates, network users might experience sudden loss of connections and poor performance. Here, the router sees other routers and end systems on multiple interfaces. Table 9-7 outlines possible causes and suggested actions when routers see duplicate updates and packets.

Table 9-7 ISO CLNS: Router Sees Duplicate Routing Updates and Packets

Possible Causes	Suggested Actions
Bridge or repeater in parallel with router, causing updates and traffic to be seen from both sides of an interface	**Step 1** Use the **show clns is-neighbors detail** and the **show clns neighbors detail** EXEC commands to see through which routers and protocols the adjacencies were learned. **Step 2** Look for routers that are known to be remote to the network connected to the router. A router that is listed but is not attached to any directly connected network is a likely problem. **Step 3** Look for paths to the same networks (or areas) on multiple interfaces. **Step 4** If you determine that there is a parallel bridge, remove the bridge or configure access filters that block routing updates on the bridge.
Multiple ISO-IGRP processes are configured on a single interface	**Step 1** Use the **show clns interface** EXEC command to inspect the interface configuration. **Step 2** If multiple ISO-IGRP processes are configured on a single interface, different Level 2 updates are being sent out through the same interface. Multiple Level 2 updates on the same interface can cause congestion problems, especially if the network is large and links are flapping outside of the damping intervals. **Step 3** To remove the multiple ISO-IGRP processes, configure the suspect interface using the **no clns router iso-igrp** *tag* interface configuration command. The variable *tag* is the tag associated with the ISO-IGRP routing process that you want to remove.

Routing Not Working when Redistribution Is Used

Symptom: Traffic is not getting through a router that is redistributing routes between two different routing areas or domains—typically IS-IS and ISO-IGRP. Observed symptoms range from poor performance to no communication at all. Table 9-8 outlines possible causes and suggested actions when route redistribution causes routing problems.

Table 9-8 ISO CLNS: Routing Not Working when Redistribution Is Used

Possible Causes	Suggested Actions
Feedback loop exists	**Step 1** Be sure to perform redistribution between an IS-IS cloud and an ISO-IGRP cloud at a single point; otherwise, routing information is injected back into one of the clouds and causes routing feedback loops. **Step 2** If you must redistribute at another point, use metrics to perform the redistribution in one direction only. Refer to the *Router Products Command Reference* publication for information about adjusting ISO CLNS default metrics.
Incorrect metric is configured, or **distance** router configuration command is missing	**Step 1** Check the router configuration using the **write terminal** EXEC command. **Step 2** If the **default-metric** router configuration command or the **distance** router configuration command is missing, add the appropriate version of the missing command. Refer to the *Router Products Command Reference* publication for information about adjusting ISO CLNS default metrics.

Redistribution route-map Commands Behave Unexpectedly

Symptom: A series of **redistribute** and **route-map** router configuration commands allow some routes to be redistributed, but deny others. Also, some routes that are configured to deny redistribution are being redistributed. Table 9-9 lists possible causes and suggested actions when route redistribution problems occur with the **redistribute** and **route-map** router configuration commands.

Table 9-9 ISO CLNS: Redistribution route-map Commands Behave Unexpectedly

Possible Causes	Suggested Actions
Sequence numbers cause some conditions to be tested before others	**Step 1** Use the **write terminal** privileged EXEC command to display the router configuration. **Step 2** Look at the sequence numbers assigned to the **redistribute** router configuration commands. Lower sequence numbers are tested before higher sequence numbers, regardless of the order in which they are listed. **Step 3** Modify the sequence numbers so the conditions are tested in the desired order.
Missing condition in the series of router redistribution commands	**Step 1** Use the **write terminal** privileged EXEC command to display the router configuration. **Step 2** Verify that the conditions that permit or deny certain redistributions are included. **Step 3** Add or modify conditions that determine when a route is redistributed.
Current network is included in a deny condition	**Step 1** Use the **write terminal** privileged EXEC command to display the router configuration. **Step 2** Verify that the conditions that permit or deny certain redistributions are included. **Step 3** Add or modify conditions that determine when a route is redistributed.

Consider the example shown in Figure 9-36. The route map conditions are initially set to deny redistribution for all addresses with the prefix 47.005.

Figure 9-36 Configuration Example for Redistribution Using Route Maps

```
!Enable IS-IS routing and route-map redistribution

router isis
redistribute iso-igrp local route-map igrp-to-isis

!Set deny condition for prefix 47.0005

route-map igrp-to-isis deny 10
match clns address nsfnet

clns filter-set nsfnet permit 47.0005...
```

S2645

However, you realize that your own domain is 47.0005.80ff.ff00, and you have mistakenly excluded yourself from local route redistribution. In Figure 9-37, the commands with sequence number 5 ensure that the local domain will be redistributed before the larger class of 47.0005 is denied. The **redistribute** commands with their sequence numbers can be entered in any order, which makes it easy to modify a router configuration; you can add new permit and deny access lists at the end of the configuration file instead of having to reenter all access lists in their desired order.

Figure 9-37 Modified Configuration Example for Redistribution Using Route Maps

```
router isis
redistribute iso-igrp local route-map igrp-to-isis

route-map igrp-to-isis deny 10
match clns address nsfnet

clns filter-set nsfnet permit 47.0005...

!Add these commands to include local domain

route-map igrp-to-isis permit 5
match clns address my-domain

clns filter-set my-domain permit 47.0005.80ff.ff00...
```

S2646

The configuration in Figure 9-38 shows how route redistribution metrics can be set so that certain addresses are treated as special cases before general rules are applied.

Figure 9-38 Configuration Example for Setting Route Metrics

```
router isis
redistribute iso-igrp local route-map igrp-to-isis

!All routes arriving on ethernet 0 assigned metric 5 when redistributed
route-map igrp-to-isis permit 10
match interface ethernet 0
set metric 5

!All routes arriving on ethernet 1 assigned metric 6 when redistributed
route-map igrp-to-isis permit 20
match interface ethernet 1
set metric 6

!All routes arriving on ethernet 2 assigned metric 1 when redistributed
route-map igrp-to-isis permit 30
match interface ethernet 2
set metric 1

!Add metric 7 for all routes from 49.0001 and 49.0002 to be redistributed before
!the general interface redistribution

route-map igrp-to-isis permit 5
match clns address prefix-descrip
set metric 7

clns filter-set prefix-descrip permit 49.0001...
clns filter-set prefix-descrip permit 49.0002...
```

S2647

CHAPTER 10

Troubleshooting Novell IPX Connectivity

This chapter presents protocol-related troubleshooting information for Novell Internet Packet Exchange (IPX) connectivity problems. The chapter consists of the following sections:

- Changes in Default Novell IPX Behavior
- Novell Network Server Connectivity Scenario
- Example IPX Enhanced IGRP Diagnostic Session
- Novell IPX Internetworking Connectivity Symptoms

The symptom modules presented in this chapter consist of the following sections:

- Symptom statement—A specific symptom associated with Novell IPX connectivity.
- Possible causes and suggested actions—For each symptom, a table of possible symptom causes and suggested actions for resolving each cause.

Changes in Default Novell IPX Behavior

In order to conform to Novell specifications, Cisco has modified the behavior of two important Novell features. If left unaddressed, these changes could affect the functionality of existing networks. The following explanations describe the change that has been made, why it has been made, and what needs to be done to accommodate the new behavior.

GNS Delay

In Software Release 9.1(13), the default value of the **ipx gns-response-delay** command became *zero* milliseconds (ms). Prior software releases had a default delay of 500 ms (half a second). This value was assigned to fix a problem in NetWare 2.x associated with dual-connected servers running in parallel with a Cisco router. The implemented delay prevented the parallel Cisco from replying to a Get Nearest Server (GNS) request before the server itself.

This problem was resolved in NetWare 3.x, and a nonzero GNS response delay might cause problems in certain situations. If you are using a software prior to Software Release 9.1(13) with NetWare 3.x or later, you might have to manually decrease the GNS response delay, depending on your network topology. Conversely, if you are using Software Release 9.1(13) or later with NetWare 2.x or earlier, you might have to manually increase the GNS response delay to compensate for the problem in NetWare 2.x.

NetBIOS Broadcast Hops

In order to conform to the IPX Router Specification released by Novell, Software Releases 9.21 and later limit the forwarding of IPX NetBIOS broadcast packets (type-20 propagation packets) to a default maximum of 8 hops. In earlier system software releases, NetBIOS broadcasts were allowed up to 16 hops. The limitation imposed in Software Release 9.21 and later could have a problematic effect on networks with NetBIOS devices that are more than eight hops apart.

Cisco implemented the **ipx type-20-helpered** router configuration command in recent system software releases, allowing network administrators to force NetBIOS broadcast packets to be forwarded up to 16 hops. While the use of this command makes the forwarding of NetBIOS packets noncompliant with the IPX Router Specification, it might allow some networks to function more efficiently. For more information on system software releases that integrate this command, contact your Cisco sales representative.

Novell Network Server Connectivity Scenario

With the emergence of Novell NetWare as the dominant PC-based network operating environment, network administrators have encountered increasing requirements to interconnect and segment PC LANs running the IPX networking protocol. This scenario focuses on a variety of problems that can impair server access over a routed internetwork.

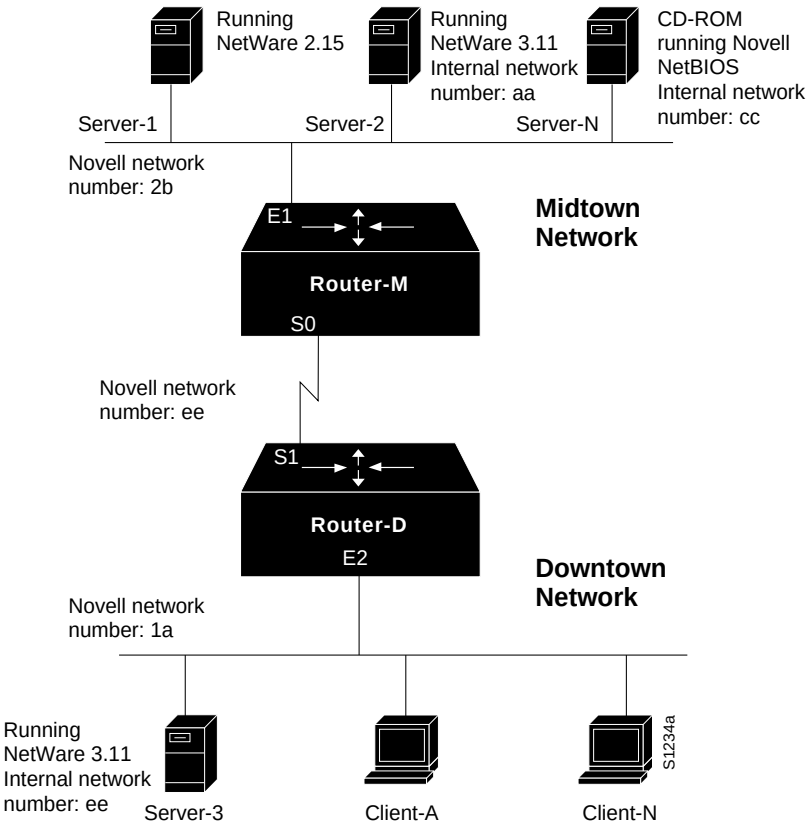
Symptoms

Figure 10-1 is a map of the Novell IPX internetwork for this scenario. It illustrates an interconnection between two sites over an arbitrary serial network. The following facts summarize the situation:

- Client-A cannot access Server-1 and Server-2 on the other side of the serial link. However, Client-A can access Server-3 on the local wire.
- Client-N (a NetBIOS client) cannot access Server-N (a NetBIOS-based CD-ROM server), which is also on the other side of the link.

Because no connections can be made over the serial link, it *initially* appears that there is a problem with traffic getting through the routers.

Figure 10-1 Initial Novell IPX Connectivity Scenario Map



Environment Description

The relevant elements of the internetworking environment shown in Figure 10-1 can be summarized as follows:

- Remote service is provided to a cross-town campus via a point-to-point serial link.
- Two routers (Router-M and Router-D) interconnect the Midtown and Downtown networks. The routers are MGS routers configured to route IPX. The clients are IBM PCs and compatibles.
- The LANs are Ethernets; the serial link is a dedicated T1 link (1.544 Mbps).
- The network applications intended to run over the T1 line include typical NetWare services.
- Server-1 is running NetWare 2.15, while Server-2 and Server-3 are running NetWare 3.11. Server-N is a CD-ROM running Novell NetBIOS.

Diagnosing and Isolating Problem Causes

Given this situation, several problems might explain both connectivity symptoms.

The following problems are likely candidates for the first symptom. (Client-A cannot access services on Server-1 and Server-2.)

- Client-A or target servers are not properly attached to their networks.
- Novell routing is not enabled on Router-D or Router-M.
- Network numbers are misconfigured.
- Router interfaces are not up or operational.
- Server-1 and Server-2 are running limited-user versions of NetWare.
- Encapsulation types are mismatched.
- Nonunique Media Access Control (MAC) addresses exist in the Novell routing configuration.
- Access lists are misconfigured.
- RIP or SAP updates from Server-2 are not being propagated correctly.

The following problems are likely candidates for the second symptom. (Client-N cannot access services on NetBIOS server.)

- Client-N or target server is not properly attached to its network.
- Novell routing is not enabled on Router-D or Router-M.
- Network numbers are misconfigured.
- Router interfaces are not up or operational.
- Server-N is running a limited-user version of NetWare.
- Encapsulation types are mismatched.
- Nonunique MAC addresses exist in the Novell routing configuration.
- Access list is misconfigured.
- **ipx type-20-propagation** interface configuration command is missing.

Both lists are ordered according to a combination of two criteria: ease of determining the problem and the likelihood of being the *actual* problem.

The problems identified as likely to block service access for Client-A and Client-N are essentially the same, with slight variations. In general, it is useful to eliminate the most likely problems first and tackle more complex problems as necessary. The problem-solving process that follows uses this strategy.

After you determine a possible problem list, you must analyze each potential cause. The following discussion considers the problems listed and illustrates the resolution of discovered problems.

Checking Physical Attachment of Clients to Network

The first step is to determine whether Client-A is attached to the network. This step also applies to Client-N and can be done at the same time.

Use the following procedure to verify that clients are physically attached to the network:

Step 1 Visually inspect the physical attachment of each client and attempt to connect to a local server. If a connection can be established, the client is obviously attached to the network.

Step 2 As of Cisco Internetwork Operating System (Cisco IOS) Release 10.3, you can **ping** Novell servers that are running NetWare Link Services Protocol (NLSP). (Some earlier versions can be updated to function in this manner as well.)

If you are unable to make a connection to the local server and you are using recent system software, **ping** the server to test connectivity.

Step 3 If a connection cannot be established to a local server (because a local server does not exist or because the connection attempt fails), use a protocol analyzer to determine whether clients are sending packets. Look for packets that have the hardware address of the client as the source address.

Step 4 As an alternative, use the **debug ipx packet** privileged EXEC command on the locally connected router (in this case Router-D) and look at the source address of each client.

Note Use caution when enabling the **debug ipx packet** command. Debugging can use a great deal of bandwidth and can cause performance problems on a busy network.

If packets appear that include the hardware address of the client as the source address, the client is active on the network and connectivity to Router-D is functional.

In order to use **debug ipx packet**, you must disable fast switching. (Use the **no ipx route-cache** interface configuration command on Ethernet interface E2.)

Note You also can use the Novell server console command **track on** to determine whether servers are broadcasting. Simple client/server activity can be viewed in this fashion.

In this case, assume that connectivity to Router-D is verified from both Client-A and Client-N.

Checking Physical Attachment of Servers to Network

The next step is to determine whether the remote servers are attached to their Ethernet segments. This process is very similar to determining whether the clients are attached to the Downtown segment. However, there are some slight differences.

Use the following procedure to verify the physical attachment of servers to the network:

Step 1 As in the previous procedure, start by visually inspecting the attachment of the servers to their networks.

Step 2 Using a protocol analyzer, determine whether the servers (in this case, Server-1, Server-2, and Server-N) are sending any packets on their local networks. Look for packets with the hardware address of each server as the source address.

Step 3 Check for connectivity between the servers and Router-M. To do this, use the **show ipx servers** EXEC command to see if the servers are included in list of Novell servers on the router. If they appear in the list, connectivity to Router-M is verified.

In this case, assume that connectivity to Router-M is verified from both Server-1 and Server-N; however, Server-2 does not appear in the **show ipx servers** output for Router-M.

Before continuing, you must determine why Server-2 is not appearing in the Novell server list on Router-M.

Enabling Novell IPX Routing

Use the **write terminal** privileged EXEC command to determine whether Novell routing is enabled on the routers. Use the **ipx routing** global configuration command if Novell routing is not enabled.

For the purposes of this scenario, assume that IPX routing is configured on the routers.

Checking Novell Network Number Specifications

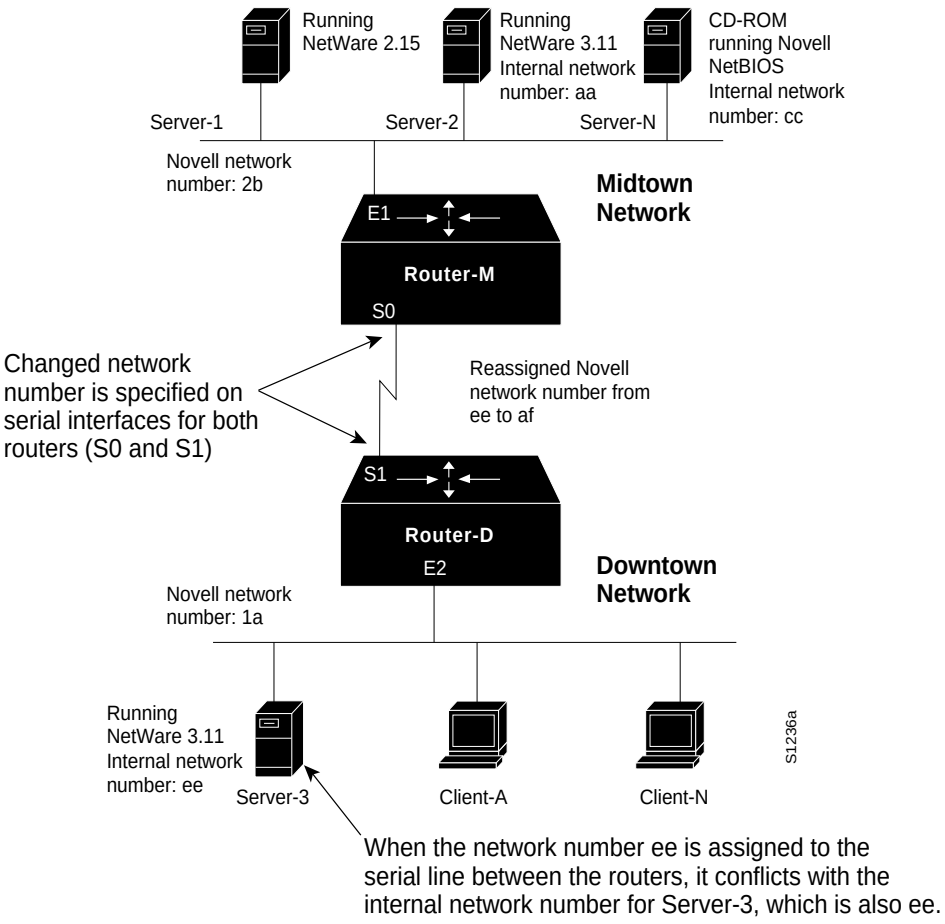
Next, examine the network number specifications for servers and routers on all networks in the internetwork, as follows:

Step 1 Assuming that IPX routing is enabled, compare the specifications for the Novell network number (using the **ipx network** *number* interface configuration command) on each router interface.

Step 2 Look for missing or duplicate network number specifications. If you find duplicates, assign unique network numbers for each network segment.

In this case, assume that there is a subtle conflict. The network number assigned for the serial link is “ee.” Unfortunately, this is also the internal network number assigned to Server-3. The result is that there is no connectivity over the serial line between Midtown and Downtown. The solution is to modify the serial line network number to something else (for example, “af”). Figure 10-2 illustrates this change. Note that when this change is made, there is no change to service availability.

Figure 10-2 IPX Connectivity Map Showing Revised Network Number Configuration



Checking Router Interface Status

In the process of eliminating the preceding problems, it is highly likely that the status of each router interface has been verified.

You can further confirm the status of the router interfaces using the following procedure:

Step 1 Issue the **show ipx interface** EXEC command on each router. The output should indicate that the interface is up and that the line protocol is up.

Step 2 You can also **ping** between the routers to confirm that the interfaces are operational.

Again, for the purposes of this scenario, assume that the interfaces are functional.

Checking for Limited-User Version of NetWare

In some cases, NetWare server software may limit the number of users that can access the server simultaneously. If your copy is a limited-user version, you should upgrade the version to support more users.

In this case, the version can be assumed to be a standard version supporting more users. Client-A is still unable to access Server-1 and Server-2, and Client-N is still unable to access Server-N.

Checking for Encapsulation Mismatch

The next problem on the list is an encapsulation mismatch. The default on Cisco routers is Novell Frame Type Ethernet_802.3 encapsulation. If there is a conflict (that is, if any entity is configured for different framing than the entities on the rest of the internetwork), you must modify the configurations so that they match.

Use the following procedure to check for an encapsulation mismatch:

Step 1 Determine the framing type that the clients and servers are running by changing the framing type on the local router (Router-D for the clients and Router-M for the servers) to **arpa** (for Novell's Frame Type Ethernet_II), **sap** (for Novell's Frame Type Ethernet_802.2), or **snap** (for Novell's Frame Type Ethernet_SNAP).

Step 2 Next, enable the **debug ipx packet** privileged EXEC command on the local router. (Remember to disable fast switching using the **no ipx route-cache** interface configuration command before enabling this **debug** command.) If you see a packet with the source address of a client or server, that node is using Frame Type Ethernet_II, Ethernet_802.2, or Ethernet_SNAP.

Step 3 You also can use the **show ipx traffic** EXEC command to look for an incrementing "format errors" counter. This counter suggests that there is an encapsulation mismatch.

Step 4 As an alternative to using these Cisco-specific commands, you can use a protocol analyzer to capture packets. Examine packets from clients, servers, and routers and determine whether they are all using the same framing type. If not, change configurations on nodes so that all nodes are using the same encapsulation type.

Different encapsulation types can coexist on the same wire and in the same internetwork, but each encapsulation type must be associated with a unique network number. If you require that Frame Type Ethernet_II and Ethernet_802.3 both be supported simultaneously, configure the interface using the **ipx network** *number* **encapsulation** *encapsulation-type* **secondary** interface configuration command.

Note Software Release 9.1 and earlier can translate between encapsulation types on the same segment only when *more than one* interface is attached to that segment. If you require that Frame Type Ethernet_II and Ethernet_802.3 both be supported simultaneously, you must have two separate interfaces attached to the same network segment—with each supporting different framing types. (Note that each interface must use a different network number.) In addition, Software Release 9.1 and earlier only support slow switched Subnetwork Access Protocol (SNAP) and Frame Type Ethernet_802.2 encapsulation over Ethernet. To avoid these problems, upgrade to Cisco IOS Release 10.0.

Table 10-1 lists encapsulation keywords for the **ipx encapsulation** interface configuration commands and their corresponding frame type.

Table 10-1 Router Interface and Novell IPX Frame Type Support

Router Interface Type	Keyword	Frame Type
Ethernet	novell-ether (default)	Ethernet_802.3
Ethernet	arpa	Ethernet_II
Ethernet	sap	Ethernet_802.2
Ethernet	snap	Ethernet_SNAP
Token Ring	novell-tr (default)	Token-Ring
Token Ring	snap	Token-Ring_Snap
FDDI	snap (default)	Fddi_Snap
FDDI	sap	Fddi_802.2

In this case, assume that all nodes are using Frame Type Ethernet_802.3.

Checking for Nonunique MAC Addresses on Routers

MAC addresses are obtained for Novell configurations in one of two ways: either from the router hardware address embedded in the system firmware or by random assignment (when the system software initializes before the interface is initialized). In some *rare* cases (usually involving serial links), the randomly generated MAC address for different routers will be the same. If these numbers are not unique, and the routers are on the same internetwork, communication will not occur. If Router-M and Router-D have the same MAC address, no traffic will traverse the serial link.

Step 1 Use the **write terminal** privileged EXEC command to examine the current configuration of each router in the path (Router-D and Router-M).

Step 2 Check the hardware address specified in the **ipx routing** global configuration command. If this system-generated number is the same for both routers, reinitialize one of the routers and see if connectivity over the link is reestablished.

Step 3 Test for connectivity between clients and servers.

Step 4 If connectivity is still blocked, reexamine the configuration of the routers.

Step 5 If the routers still have matching MAC addresses, use the **show controllers** *interface-type* EXEC command or the **show ipx interface [***interface unit***]** EXEC command to obtain an actual MAC address from each router.

Step 6 Use the **ipx routing** command to enter the selected MAC address (for example, **ipx routing 00aa.54f1.003e**).

In general, this problem is more likely to occur in Token Ring and serial link implementations. For the purposes of this case, assume that the MAC addresses are different.

Checking for Access List Problems

Access lists are the cause of many connectivity problems. Misconfigurations in access lists can produce disastrous results in a network. In a Novell IPX environment, make certain that access lists do not improperly deny RIP routing updates or SAP updates. While there are certain situations in which you might want to deny RIP or SAP traffic, implement your filters carefully. For details concerning access list issues, refer to the symptom modules, "Clients Cannot Communicate with NetWare Servers over Router" and "SAP Updates Not Propagated by Router," later in this chapter.

For the purposes of this case, assume that the **write terminal** privileged EXEC command output for both Router-D and Router-M indicates that there are no relevant access list specifications.

Determining Whether SAP Updates Are Being Propagated

Novell servers send Service Advertisement Protocol (SAP) updates to tell clients what services are available. If SAP updates are not properly propagated, clients might not be aware of the existence of the server. Clients might not receive SAP updates from a server for a number of reasons.

Use the following procedure to determine whether SAP updates are being propagated correctly:

Step 1 Determine whether the server is using special software that allows it to completely disable SAP updates. Certain third-party NetWare-loadable modules (NLMs) are available that allow a Novell server to be explicitly configured to withhold SAP updates. Consult the third-party documentation if you suspect that SAP updates have been disabled on the server.

Step 2 Assume that Server-1 and Server-2 were set to withhold SAP updates. Change this configuration.

Step 3 Again, check to see if Server-2 is seen by Router-M, using the **show ipx servers** EXEC command. Assume that Server-1 now appears in the **show ipx servers** output, and that connectivity between Client-A and Server-1 is restored. However, in spite of the fact that SAP updates are now being sent, Server-2 still does not appear in the **show ipx servers** output.

Determining Whether RIP Packets Are Being Propagated

Cisco routers look at the internal network numbers contained in Novell IPX RIP updates to determine the origin of the SAP updates sent from a server. If RIP packets are not being propagated correctly, the Cisco router is not seeing the internal network number of the server sending SAP updates. If this is the case, the server will not appear in the IPX servers table, despite the fact that it is sending SAP updates.

Use the following procedure to determine if RIP packets are being propagated correctly:

Step 1 Determine whether the server is using special software that allows it to disable RIP packets. Certain third-party NetWare-loadable modules (NLMs) are available that allow a Novell server to be explicitly configured to withhold RIP traffic. Consult the third-party documentation if you suspect that RIP updates have been disabled on the server.

Step 2 Assume that Server-2 was configured to withhold RIP traffic. Change this configuration.

Step 3 Again, check to see if Server-2 is seen by Router-M, using the **show ipx servers** EXEC command. Assume that Server-2 now appears in the **show ipx servers** output and that connectivity between Client-A and Server-2 is restored.

Unfortunately, Client-N is still unable to access the NetBIOS server (Server-N).

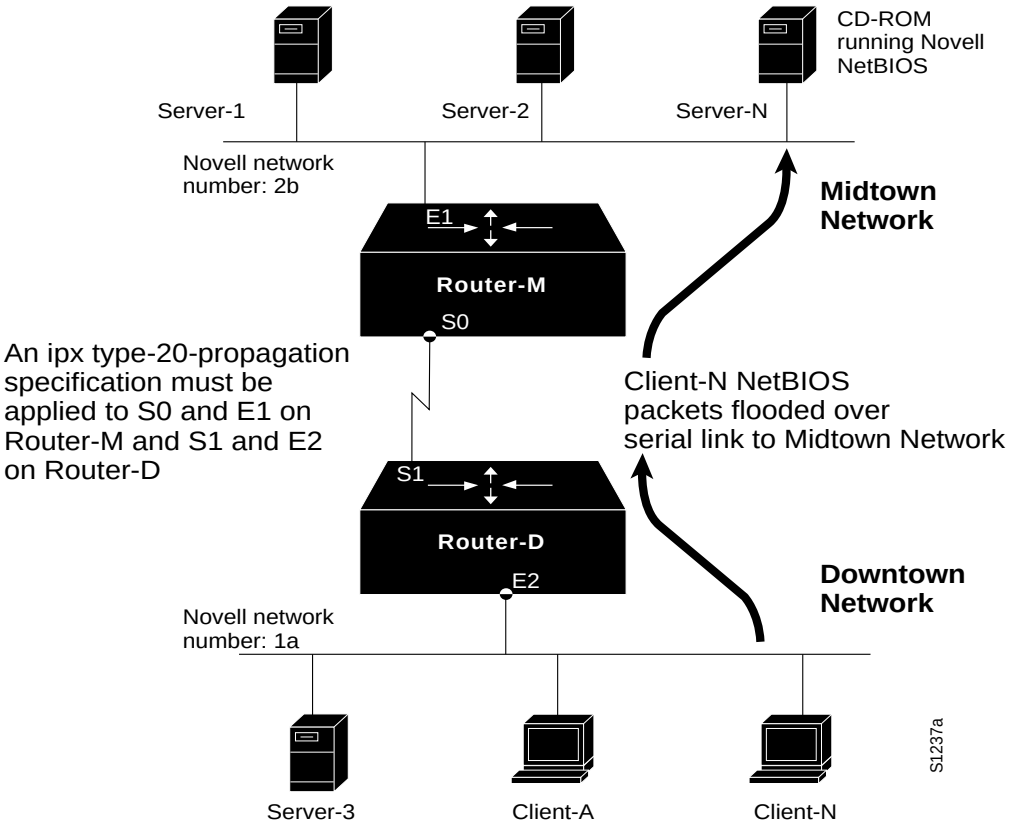
Determining Whether if the ipx type-20-propagation Command Is Missing

Next, check if the **ipx type-20-propagation** command is missing on either of the routers, using the following procedure:

Step 1 Use the **write terminal** EXEC command to look for **ipx type-20-propagation** interface configuration command entries.

The **ipx type-20-propagation** command must be specified on Router-M (Ethernet interface E1 and serial interface S0) and Router-D (Ethernet interface E2 and serial interface S1) to allow IPX type-20 (NetBIOS) broadcast traffic to be flooded through the routers. Figure 10-3 illustrates the flow of broadcast traffic from clients to the server.

Figure 10-3 ipx type-20-propagation Specification and Broadcast Traffic Flow



Step 2 Assume that the **ipx type-20-propagation** interface configuration command is not included in the original configuration and is added as a correction.

Assume that adding the **ipx type-20-propagation** interface configuration command restores connectivity between the NetBIOS devices on the network (Client-N and Server-N).

Problem Solution Summary

This scenario focused on diagnosing blocked connectivity in Novell IPX internetworks. Three problems were discovered and resolved:

- Misconfigured network numbers were corrected.
- Servers were reconfigured to properly produce RIP and SAP traffic.
- A number of **ipx type-20-propagation** interface configuration commands were included to propagate Novell NetBIOS client requests.

Figure 10-4 and Figure 10-5 provide representative configuration listings for Router-D and Router-M, as discussed in this scenario. These configurations illustrate the configuration commands required to interconnect the two Ethernet segments over the T1 line.

Figure 10-4 Relevant IPX Configuration Commands for Router-D

```
ipx routing
!
!
interface ethernet 2
ipx network 1a
ipx type-20-propagation
!
interface serial 1
ipx network af
ipx type-20-propagation
!
```

S2532

Figure 10-5 Relevant IPX Configuration Commands for Router-M

```
ipx routing
!
!
interface ethernet 1
ipx network 2b
ipx type-20-propagation
!
interface serial 0
ipx network af
ipx type-20-propagation
!
```

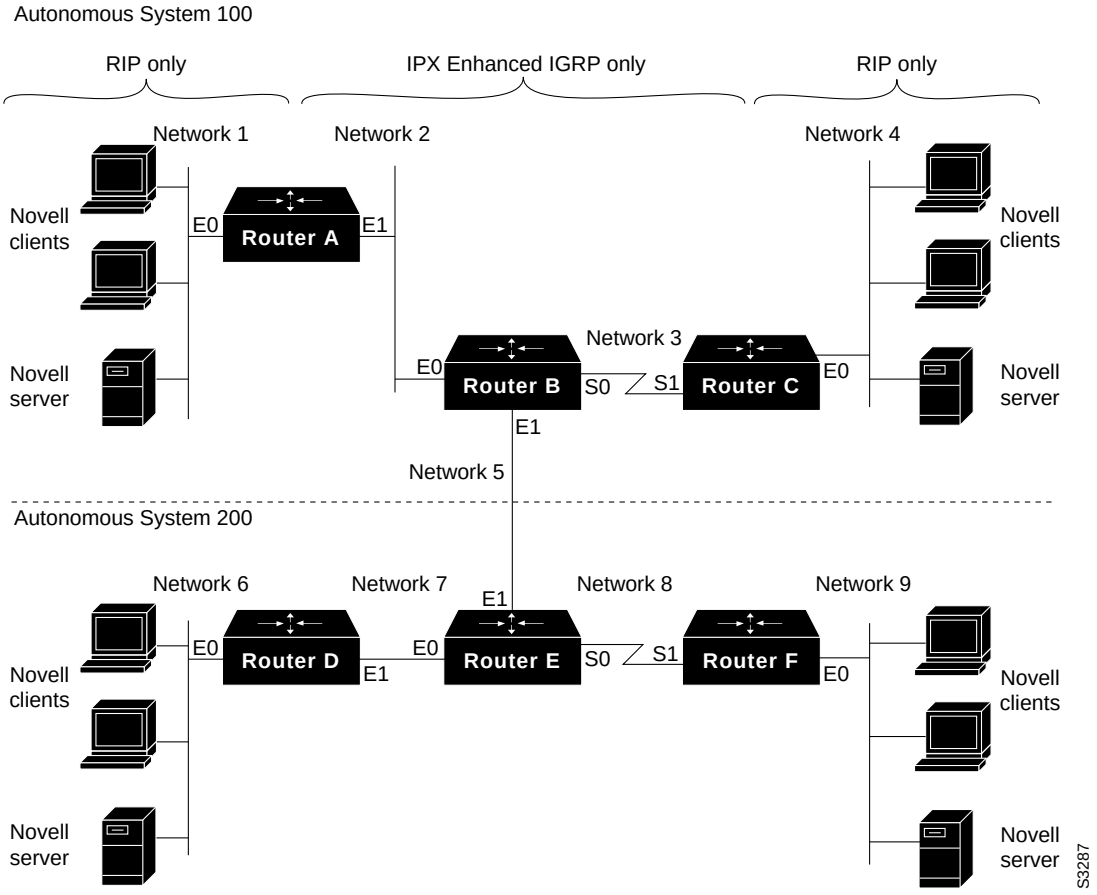
S2514

Note Remember to use the **ipx route-cache** command to reenable fast switching if it was disabled during troubleshooting.

Example IPX Enhanced IGRP Diagnostic Session

This section presents a sample diagnostic and troubleshooting session in an IPX Enhanced IGRP internetwork environment. In this example network, IPX Enhanced IGRP is running on the backbone while IPX RIP is running on the edges, on the LANs with connected Novell clients and servers. This network topology is illustrated in Figure 10-6.

Figure 10-6 Novell IPX Network Running IPX Enhanced IGRP and IPX RIP



In the network shown in Figure 10-6, Router A and Router D run IPX RIP on Ethernet interface 0, and IPX Enhanced IGRP on Ethernet interface 1. Router C and Router F run IPX RIP on Ethernet interface 0 and IPX Enhanced IGRP on serial interface 1. Router B and Router E run only IPX Enhanced IGRP on all interfaces.

It is important to note that Novell servers do not understand IPX Enhanced IGRP, so only IPX RIP should be enabled on interfaces with Novell servers on the connected LAN segment. Therefore, in the network shown in Figure 10-6, only IPX RIP should be enabled on Ethernet interface 0 of Router A, Router C, Router D, and Router F.

Furthermore, while it might be desirable or necessary in certain network topologies, Cisco recommends that you *not* enable IPX Enhanced IGRP and IPX RIP on the same interface because doing so produces unnecessary bandwidth and processor overhead that might affect network performance. In most cases, only one or the other should be enabled on each interface. Allow route redistribution to exchange routing information between the two routing processes.

The following diagnostic tables (Table 10-2 and Table 10-3) illustrate step-by-step procedures for troubleshooting poor or lost connectivity in an internetworking environment such as that shown in Figure 10-6. Potential trouble areas are identified and ordered based on the likelihood of their being the actual problem, and a series of actions is suggested for each problem. Table 10-2 encompasses diagnostic and troubleshooting procedures for the multiprotocol portions of the Novell IPX network shown in Figure 10-6, that is, the sections of the network that are running both IPX RIP and IPX Enhanced IGRP. Table 10-3 addresses the single-protocol backbone of the IPX network in which the routers are running only IPX Enhanced IGRP.

Note Table 10-2 and Table 10-3 do not address hardware problems that might contribute to network connectivity problems. For information on troubleshooting hardware problems, see the "Troubleshooting Router Startup Problems" chapter.

Table 10-2 Multiprotocol Novell IPX Internetwork Diagnostics (IPX RIP and IPX Enhanced IGRP)

Possible Problem	Suggested Actions
IPX Enhanced IGRP is not globally enabled.	**Step 1** Check the configuration of Router A using the **write terminal** privileged EXEC command. Look for the **ipx router eigrp** global configuration command.
	Step 2 If IPX Enhanced IGRP is not enabled on Router A, use the **ipx router eigrp 100** global configuration command to start the IPX Enhanced IGRP routing process on the router.
	Step 3 In IPX-router configuration mode, issue the command **network 2** to associate that network with the IPX Enhanced IGRP routing process.
	Step 4 Perform the same steps on Router C, Router D, and Router F. This ensures that the IPX Enhanced IGRP routing process is associated with the appropriate connected networks.
	NOTE: Unlike IPX RIP, IPX Enhanced IGRP is *not* enabled by default on all interfaces when the **ipx routing** global configuration command is issued. To properly configure IPX Enhanced IGRP you must issue the **ipx router eigrp** global configuration command and then associate the appropriate networks with the routing process using **network** commands.

Possible Problem	Suggested Actions
Routes are not being redistributed between IPX RIP and IPX Enhanced IGRP.	**Step 5** Use the **write terminal** privileged EXEC command on Router A to make certain that there are no explicit **no redistribute** IPX-router configuration commands. Such commands disable the default route redistribution behavior of a router configured with the **ipx routing** global configuration command. **Step 6** If **no redistribute** commands are present, use the **redistribute** IPX-router configuration command to start route redistribution between IPX RIP and IPX Enhanced IGRP. **Step 7** Perform the same actions on all routers that are running IPX RIP and IPX Enhanced IGRP. In the network shown in Figure 10-6, this includes Router C, Router D, and Router F. If, for example, there was a **no redistribute rip** command configured for autonomous system 200 on Router F, you would enter the **ipx router eigrp 200** global configuration command to enter IPX-router configuration mode. You would then enter the **redistribute rip** IPX-router configuration command to redistribute routing information from IPX RIP into IPX Enhanced IGRP. NOTE: Route redistribution between IPX RIP and IPX Enhanced IGRP is enabled by default when the **ipx routing eigrp** global configuration command is configured. It can, however, be disabled with the **no redistribute** IPX-router command.
IPX RIP and IPX Enhanced IGRP are enabled on the same interface.	**Step 8** The **ipx routing** global configuration command automatically enables IPX RIP on all interfaces. However, on a router running IPX Enhanced IGRP on some interfaces, Cisco recommends that you disable IPX RIP on those interfaces to avoid creating unnecessary traffic and processor overhead. Use the **write terminal** privileged EXEC command on Router A. Check the **network** router configuration commands associated with the **ipx router rip** global configuration command. Make sure that the IPX RIP routing process is only associated with Network 1, not Network 2. **Step 9** If the **network** commands associate the IPX RIP routing process with Network 2, issue the **no network 2** router configuration command to disable IPX RIP on the IPX Enhanced IGRP-only interface. **Step 10** Perform the same steps on Router C, Router D, and Router F. If IPX RIP was enabled on serial interface 1 of Router F, for example, you would first issue the **ipx router rip** global configuration command. Then, in router configuration mode, enter the **no network 8** command to disassociate the IPX RIP routing process from Network 8.

Possible Problem	Suggested Actions
Periodic SAP updates are using excessive bandwidth.	**Step 11** Issue the **write terminal** privileged EXEC command on Router A and look for **ipx sap-incremental eigrp** interface configuration command entries. To conserve bandwidth, configure the **ipx sap-incremental eigrp** interface configuration command on Ethernet interface 1 of Router A, which is running IPX Enhanced IGRP. This will change the default behavior of the SAP updates, sending them only when there is a change in the SAP table. NOTE: You should only have the **ipx sap-incremental eigrp** command enabled on interfaces that have no Novell clients or servers attached. **Step 12** Make certain that Ethernet interface 0 on Router A does *not* have the **ipx sap-incrementatal eigrp** enabled. This command should only be configured on an interface if all of the nodes out that interface are Enhanced IGRP peers. Because there are Novell servers on Network 1, SAP updates must be sent periodically instead of incrementally. NOTE: On Ethernet, Token Ring, and FDDI interfaces, SAP updates are sent periodically by default. **Step 13** Perform the same procedures on Router D to allow SAP updates to be sent on Ethernet interface 1 only when the SAP table has changed, but to ensure that periodic SAPs are sent out Ethernet interface 0. **Step 14** On serial interfaces, SAP updates are only sent when the SAP table changes. This is the preferable behavior on a serial interface because it conserves the limited bandwidth available. If network connectivity is still suffering after configuring Router A and Router D to send SAP updates incrementally, use the **write terminal** privileged EXEC command on Router C and Router F to make certain that there are not explicit **no ipx sap-incremental eigrp** interface configuration commands present. **Step 15** If this command is enabled, it is likely that periodic SAPs are causing network performance degradation. Configure the **ipx sap-incremental** interface configuration command on serial interface 1 of Router C and Router F to preserve bandwidth. Make certain that the Ethernet interfaces continue to send periodic SAP updates, which is necessary on network segments running Novell clients and servers.

Possible Problem	Suggested Actions
Neighboring Enhanced IGRP routers are not visible to other Enhanced IGRP routers.	**Step 16** Issue the **show ipx eigrp neighbors** EXEC command on Router A. Make sure that the directly connected IPX Enhanced IGRP router (Router B) appears in the output. **Step 17** Examine the Uptime field for each router in the **show ipx eigrp neighbors** output. If the uptime counter is continuously resetting, it is probably a result of Hello packets from the neighboring router arriving sporadically. This indicates connectivity problems that are most likely unrelated to IPX RIP and IPX Enhanced IGRP. **Step 18** Issue the **show interface** EXEC command to determine if the interface and line protocol are up. Look for high numbers in the queue fields and excessive drop counts. If there are many drops, if the queue count is high, or if the interface or line protocol are down, there is probably something wrong with the interface or other hardware. For more information on troubleshooting hardware, see the "Troubleshooting Router Startup Problems" and the "Troubleshooting Serial Line Problems" chapters. **Step 19** Use the **write terminal** privileged EXEC command on Router A. Look for **ipx hello-interval eigrp** and **ipx hold-time eigrp** interface configuration command entries. We recommend that the values configured by these commands be the same for all IPX routers on the network. **Step 20** Perform the same actions on all of the other routers in the network. If any of these routers have conflicting hello interval or hold time values, we recommend that you reconfigure them to bring them into conformance with the rest of the routers on the network. These values can be returned to their defaults with the **no ipx hello-interval eigrp** and the **no ipx hold-time interval eigrp** interface configuration commands.

Table 10-3 Single Protocol Novell IPX Internetwork Diagnostics (IPX Enhanced IGRP Only)

Possible Problem	Suggested Actions
IPX Enhanced IGRP is not globally enabled.	**Step 1** Check the configuration of Router B using the **write terminal** privileged EXEC command. Look for the **ipx router eigrp** global configuration command.
	Step 2 If IPX Enhanced IGRP is not enabled on Router A, use the **ipx router eigrp 100** global configuration command to start the IPX Enhanced IGRP routing process on the router.
	Step 3 Use **network** router configuration commands to associate the desired networks with the IPX Enhanced IGRP routing process. In the network environment shown in Figure 10-6, you would enter the IPX-router command **network all** to associate all of the attached networks with the IPX Enhanced IGRP routing process.
	Step 4 Perform the same steps on Router E to make certain that the appropriate networks are associated with the IPX Enhanced IGRP routing process. NOTE: Unlike IPX RIP, IPX Enhanced IGRP is *not* enabled by default on all interfaces when the **ipx routing** global configuration command is issued. To properly configure IPX Enhanced IGRP, you must enter the **ipx router eigrp** global configuration command and then associate the appropriate networks with the routing process using **network** commands.
IPX RIP is enabled on an IPX Enhanced IGRP-only router.	**Step 5** The **ipx routing** global configuration command automatically enables IPX RIP on all interfaces. However, on a router running IPX Enhanced IGRP exclusively, you should disable IPX RIP to avoid producing unnecessary traffic and processor overhead.
	Step 6 Use the **write terminal** privileged EXEC command on Router B. To determine if IPX RIP has been properly disabled on the router, check the configuration for the **no ipx router rip** global configuration command.
	Step 7 If the **no ipx router rip** global configuration command is not present, RIP is enabled on the router. Issue the **no ipx router rip** global configuration command to disable IPX RIP routing on the IPX Enhanced IGRP-only router.
	Step 8 Make certain that IPX RIP is disabled on Router E as well as Router B.

Possible Problem	Suggested Actions
Routes are not being redistributed between IPX Enhanced IGRP autonomous systems.	**Step 9** On Router B, use the **write terminal** privileged EXEC command and look for the **redistribute eigrp** IPX-router configuration command. **Step 10** If the command is not present, you must enter the **redistribute eigrp 200** IPX-router configuration command to allow route redistribution between IPX Enhanced IGRP autonomous systems. NOTE: While route redistribution between IPX Enhanced IGRP routers in the same autonomous system is enabled by default when the **ipx router eigrp** command is issued, you must manually configure redistribution between routers in different autonomous systems. **Step 11** Route redistribution must be configured for both autonomous systems if you want routing information to be exchanged reciprocally. On Router E, then, you would first enter the **ipx router eigrp 200** global configuration command, which places you in IPX-router configuration mode. Then enter the **redistribute eigrp 100** command to ensure that routing information from autonomous system 100 is redistributed into autonomous system 200.
Periodic SAP updates are using excessive bandwidth.	**Step 12** Issue the **write terminal** privileged EXEC command on Router B and look for **ipx sap-incremental eigrp** interface configuration command entries. On Ethernet, Token Ring, and FDDI interfaces, SAP updates are sent periodically by default, regardless of whether the SAP table has changed. To conserve bandwidth, you can change this default behavior using the **ipx sap-incremental eigrp** interface configuration command. Issue this command on the two Ethernet interfaces of Router B to configure these interfaces to send SAP updates only when the SAP table has changed. **Step 13** Unlike Ethernet interfaces, the default behavior of serial interfaces is to send SAP updates only when the SAP table changes. You need not explicitly configure serial interface 0 on Router B with the **ipx sap-incremental eigrp** command unless there is an explicit **no ipx sap-incremental eigrp** command in place. **Step 14** Perform the same procedures on Router E to allow SAP updates to be sent out the Ethernet interfaces only when the routing table has changed, and to make certain that the serial interface is also sending SAP updates in this manner. NOTE: Because there are only IPX Enhanced IGRP peers (and therefore no Novell servers) out all of the interfaces of Router B and Router E, incremental SAP updates are permissible.

Possible Problem	Suggested Actions
Neighboring Enhanced IGRP routers are not visible to other Enhanced IGRP routers.	**Step 15** Issue the **show ipx eigrp neighbors** EXEC command on Router B. Make sure that the directly connected Enhanced IGRP routers (Router A, Router C, and Router E) appear in the output. **Step 16** Examine the Uptime field for each router in the **show ipx eigrp neighbors** output. If the uptime counter is continuously resetting, it is probably a result of Hello packets from the neighboring router arriving sporadically. This indicates connectivity problems that are most likely unrelated to IPX RIP and IPX Enhanced IGRP. For more information, see the "Novell IPX Internetworking Connectivity Symptoms" section later in this chapter. **Step 17** Use the **write terminal** privileged EXEC command on Router B. Look for **ipx hello-interval eigrp** and **ipx hold-time eigrp** interface configuration command entries. Cisco recommends that the values configured by these commands be the same for all IPX routers on the network. **Step 18** Perform the same actions on all of the other routers in the network. If any of these routers have conflicting hello interval or hold time values, Cisco recommends that you reconfigure them to bring them into conformance with the rest of the routers on the network. These values can be returned to their defaults with the **no ipx hello-interval eigrp** and the **no ipx hold-time interval eigrp** interface configuration commands.

Novell IPX Internetworking Connectivity Symptoms

The following sections contain symptom modules that pertain to Novell IPX internetwork problems. Unless otherwise indicated, each module is presented as a set of general problems. Where there are special considerations associated with a situation, notes are included.

- Clients Cannot Communicate with NetWare Servers over Router
- SAP Updates Not Propagated by Router
- Novell NetBIOS Packets Cannot Get through Router
- Client Cannot Access Remote Servers over Frame Relay
- Clients Cannot Connect to Server over Packet-Switched Network
- Enhanced IGRP Router Stuck in Active Mode

Note Symptoms, problems, and actions associated with Novell NetWare 2.15 apply equally to NetWare 2.2, unless NetWare 2.2 is specifically excluded.

Clients Cannot Communicate with NetWare Servers over Router

Symptom: Clients might not be able to connect to servers on their directly connected networks. In either case, connections cannot be made to servers on the other side of the router. Table 10-4 outlines possible causes and suggested actions when clients cannot communicate with NetWare servers over a router.

Table 10-4 IPX: Clients Cannot Communicate with NetWare Servers over Router

Possible Causes	Suggested Actions
A client or a server is not attached to the network	**Step 1** Connect both the client and the server to the same network and verify that they can communicate with each other. **Step 2** If they cannot communicate, check the configurations. For troubleshooting information, refer to the documentation provided by the manufacturer. **Step 3** Attach a network analyzer to the network to which the client and server are temporarily connected. Look for the source addresses of both. **Step 4** If you find the source addresses, end stations are operating properly. If you do not find the addresses, check the configuration of the clients and servers. For troubleshooting information, refer to the documentation provided by the manufacturer.
Router interface is not functioning	**Step 1** Use the **show interfaces** EXEC command to check the operation of the router. Verify that the status line indicates that the interface and line protocol are up. **Step 2** If the interface is administratively down, add the **no shutdown** interface configuration command to the configuration for the that interface. **Step 3** If the interface or line protocol is down, check the cable connections from the router. If necessary, replace the cable. **Step 4** If, after replacing the cable, the output of the **show interfaces** EXEC command still indicates that the interface and line protocol are down, contact your router technical support representative.
Router network number specification is misconfigured for NetWare 2.15, causing problems for Routing Information Protocol (RIP), which relies on network numbers to route traffic	**Step 1** Check the router configuration to see whether Novell IPX routing is enabled. If not, add the **ipx routing** global configuration command and related commands as necessary. **Step 2** Get the network number from the target network server. **Step 3** Use the **write terminal** privileged EXEC or the **show ipx interface** EXEC command to get the network number of the server as it is specified on the router. **Step 4** Compare the network numbers. If they do not match, reconfigure the router with correct network number. **Step 5** If the network numbers match, check the router interface on the client side and make sure that the assigned network number is unique with respect to all network numbers in your Novell IPX internetwork. On the server side of the router, make sure that the network number assigned to the router interface matches the network number for the server.

Possible Causes	Suggested Actions
Router network number specification is misconfigured for NetWare 3.11 or 4.*x*, causing problems for RIP, which relies on network numbers to route traffic	**Step 1** Check the router configuration to see whether Novell IPX routing is enabled. If not, add the **ipx routing** global configuration command and related commands as necessary. **Step 2** Get the *external* network number of the server interface that is attached to the network to which the router is also attached. Do not use the *internal* network number of a 3.11 server. **Step 3** Use the **write terminal** privileged EXEC or the **show ipx interface** EXEC command to compare the *external* network number of the server with the network number specified on router. **Step 4** If the network numbers do not match, reconfigure the router with correct network numbers. **Step 5** If the network numbers match, check the router interface on the client side and make sure that the network number assigned is unique with respect to all of the network numbers in your Novell IPX internetwork.
NetWare 2.15 and 3.11 network number mismatch on the same network or backbone, causing problems for RIP, which relies on network numbers to route traffic	**Step 1** If NetWare 2.15 servers are on the same physical cable with NetWare 3.11 servers, the network number for the connected interface of any 2.15 server and the external network number for the connected interface of any 3.11 server must match. Compare the *external* network numbers for the 3.11 servers with the network numbers for the 2.15 servers. **Step 2** If these numbers do not match, reconfigure the servers to make them match. Refer to the server documentation for information concerning these modifications.
Misconfigured access list	**Step 1** Remove **ipx access-group** interface configuration command specifications on all relevant interfaces. **Step 2** See whether traffic can get through by testing connectivity between the client and the target server. If the connection now works, the access list needs modification. **Step 3** To isolate the location of the bad access list specification, apply one access list statement at a time until you can no longer create connections. **Step 4** Make sure that access lists are applied to the correct interface. Normally, filters are applied to *outgoing* interfaces.

Possible Causes	Suggested Actions
Backdoor bridge between segments	**Step 1** Use the **show ipx traffic** EXEC command to determine whether the "bad hop count" field is incrementing. **Step 2** If this counter is incrementing, use a network analyzer to look for packet loops on suspect segments. Look for RIP and SAP updates. If a backdoor bridge exists, you are likely to see hop counts that increment up to 16; the route then disappears and reappears unpredictably. **Step 3** Look for known *remote* network numbers that show up on the *local* network. Examine these packets, looking for packets whose source address is the MAC address of the remote node instead of the MAC address of the router. **Step 4** Use a fanout to isolate the local Ethernet into smaller segments. **Step 5** Examine packets on each segment. The back door is located on the segment on which a packet appears whose source address is the remote node's MAC address instead of the MAC address of the router.
Duplicate network numbers on Novell servers	**Step 1** Use the **show ipx servers** EXEC command to look for duplicate network numbers. This command generates a list of servers by type, name, network number, MAC address, hop count, and interface. **Step 2** If you see duplicate network numbers, modify server configurations to eliminate duplicate network numbers from your internetwork.
Nonfunctional FDDI ring	**Step 1** Use the **show interfaces fddi** EXEC command to determine the status of interface. **Step 2** If the **show interfaces fddi** EXEC command indicates that the interface and line protocol are up, use the **ping ipx** privileged EXEC command to test connectivity between routers. **Step 3** If the interface and line protocol are up, make sure that the MAC addresses of upstream and downstream neighbors are as expected. If all zeros appear in either of the address fields for these neighbors, a physical connection problem is likely. **Step 4** In this case (or if the status line does *not* indicate that the interface and line protocol are up), check patch-panel connections. Use an optical time domain reflectometer (TDR) or light meter to check connectivity between routers; ensure that the signal strength is within specification.
Nonfunctional serial link	**Step 1** Use the **show interfaces serial** EXEC command to determine the status of the interface. **Step 2** If the **show interfaces serial** EXEC command indicates that the interface and line protocol are up, use the **ping ipx** privileged EXEC command to test connectivity between routers. **Step 3** If routers do not respond to the ping test, refer to the "Troubleshooting Serial Line Problems" chapter.

Possible Causes	Suggested Actions
Nonfunctional Ethernet backbone	**Step 1** Use the **show interfaces ethernet** EXEC command to determine the status of the interface. **Step 2** If the status line does not indicate that the interface and line protocol are up, check the physical attachment of the router to Ethernet backbone. **Step 3** If the **show interfaces ethernet** EXEC command indicates that the interface and line protocol are up, use the **ping ipx** privileged EXEC command to test connectivity between routers. **Step 4** Obtain analyzer traces and look for packets from target servers, client, and routers. **Step 5** Any known nodes that do not appear as expected are suspects for being problem nodes. Locate and determine whether the node and its cables are functional. If not, replace or reconfigure as needed.
Nonfunctional Token Ring backbone	**Step 1** Use the **show interfaces token** EXEC command to determine the status of the interface. **Step 2** If the status line indicates that the interface and line protocol are not up, check the cable from the router to the Multistation Access Unit. Make sure that the cable is functional; replace it if necessary. **Step 3** If the **show interfaces token** EXEC command indicates that the interface and line protocol are up, use the **ping ipx** privileged EXEC command to test connectivity between routers. **Step 4** If the remote router does not respond, check the ring specification on all nodes attached to the Token Ring backbone. The ring speed for all of the nodes must be the same. **Step 5** If necessary, modify ring speed specifications for clients, servers, and routers. On routers that support setting the ring speed in software, use the **ring-speed** interface configuration command. Change jumpers as needed for modular router platforms. For more information about ring speed specification, refer to the hardware installation and maintenance manual for your system.

Possible Causes	Suggested Actions
Mismatched Ethernet encapsulation methods	**Step 1** Check the encapsulation type that is being used by clients and servers. **Step 2** Compare the encapsulation types with the encapsulation type specified in the configuration of the router. By default, Cisco routers use Novell's Frame Type Ethernet_802.3 encapsulation. Cisco refers to this as "novell-ether" encapsulation.) **Step 3** If servers and clients are using what Novell refers to as "Frame Type Ethernet _II," use the **ipx encapsulation arpa** interface configuration command to make sure that the router also uses this form. (This particular encapsulation mismatch problem also applies to DEC/VMS hosts and servers that are running Novell server software.) **Step 4** If clients and servers on a particular interface are using Frame Type Ethernet_II, Ethernet_SNAP, or Ethernet_802.2 encapsulation, change the encapsulation type of the router to match. **Step 5** As a last resort, disable Novell IPX routing and enable bridging. Note that Cisco routers running Software Release 9.21 and later can translate Frame Type Ethernet_802.2, Ethernet_802.3, Ethernet_II, and Ethernet_SNAP encapsulation types on the same interface or between different interfaces. Each encapsulation type requires a unique network number.

SAP Updates Not Propagated by Router

Symptom: SAP updates do not appear to be propagated by a router. Novell servers use SAP updates to broadcast the Novell services that they offer. Table 10-5 outlines possible causes and suggested actions when SAP updates are not being propagated by a router.

Table 10-5 IPX: SAP Updates Are Not Propagated by Router

Possible Causes	Suggested Actions
Novell server is not sending SAP updates	**Step 1** Use a protocol analyzer to look for SAP updates from the server. **Step 2** If the server is not sending SAP updates, make sure the server is attached to the network. **Step 3** In Ethernet environments, if the server is sending SAP updates, check the encapsulation type in the router configuration. The encapsulation type must match the Novell server encapsulation specification (Frame Type Ethernet_802.2, Frame Type Ethernet_802.3, Frame Type Ethernet_II or Frame Type Ethernet_SNAP). **Step 4** Certain third-party NLMs are available that allow SAP updates to be disabled entirely. If you are using such software on your servers, make certain that the necessary SAP updates are being sent. Consult your third-party documentation for more information.
Ring speed specification mismatch	**Step 1** Check the ring speed specifications on Novell servers and routers (4 or 16 Mbps). **Step 2** If the ring speeds do not match, use the **ring-speed** interface configuration command to make the router configuration match server specifications.
Misconfigured access lists	**Step 1** Disable any SAP-specific access lists by removing **ipx input-sap-filter** and **ipx output-sap-filter** interface configuration commands as appropriate. **Step 2** Use the **display servers** command on the server to verify that the server is advertising services, or, if there is a Novell client on the other side of router, use the **slist** command on the client. **Step 3** Use the **debug ipx sap activity** privileged EXEC command to look for server name, network number, and MAC address. If the SAP information of the Novell server is included in the updates from the router, an access list is causing SAP updates to be dropped at the router. **Step 4** Revise access lists or filter statements as necessary and apply them individually to ensure that updates are being distributed appropriately.

Possible Causes	Suggested Actions
Misconfigured network number on router or Novell server, causing problems for RIP, which relies on network numbers to route traffic	**Step 1** Use the **show ipx route** or the **show ipx servers** EXEC command to determine whether there are any duplicate network numbers in the internetwork. If the routers or Novell servers have duplicate network numbers, the router might not send out SAP updates. **Step 2** Check the server console for error messages. The system console log will indicate that there are misconfigured routers in the network if network numbers conflict. **Step 3** If you find duplicate network numbers, modify server configurations or the **ipx network** interface configuration command on the router as appropriate.
Novell servers are unable to handle the rate at which routers generate SAP updates	**Step 1** Compare the output of the **show ipx servers** EXEC command from the router with the output of the **slist** command from Novell servers. If the **slist** output for a Novell server shows only a partial listing of SAP entries, it is possible that the Novell servers are unable to handle the rate at which the router is generating SAP updates. This problem is more likely in older servers or servers with older LAN card drivers. **Step 2** Use the **ipx output-sap-delay** interface configuration command to specify the delay between packets in a multipacket SAP update. Novell recommends a delay of 55ms. However, a delay of as little as of 5 ms may work. Use the lowest possible delay that corrects the problem.
SAP or RIP timers mismatch	**Step 1** SAP and RIP timer values can be changed on servers running NetWare 4.x or later. Examine the configuration of the server and the routers to determine if the timer values are the same. **Step 2** If the timer value configured on the server is more than 3 minutes greater than that configured on the router, the router will remove the server from the IPX servers table. This will result in clients being unable to see the services available on that server. **Step 3** Bring the timer values within 3 minutes of each other to ensure that the router does not remove the server from its IPX servers table.
Limited-user version of NetWare software	**Step 1** Check the software running on the server. If the software is a limited-user version, you must upgrade the version to support more users.

Possible Causes	Suggested Actions
Nonunique MAC address on routers	**Step 1** Use the **write terminal** privileged EXEC command to examine the current configuration of each router in the path. **Step 2** Check the MAC address specified in the **ipx routing** global configuration command. **Step 3** If this router-generated number matches for both routers, reinitialize one of the routers and see whether connectivity over the link is reestablished. **Step 4** If the numbers still match, use the **show interfaces** EXEC command to get the real MAC address of one of the interfaces. Use the **ipx routing** command to assign the real MAC address to the router. In general, this problem is more likely to occur in Token Ring implementations. If the routers are interconnected over a serial line, no connection can be made over the serial line.

Novell NetBIOS Packets Cannot Get through Router

Symptom: Clients are unable to get response from servers running Novell NetBIOS when connections are attempted over a router. Table 10-6 outlines a possible cause and suggested actions when Novell NetBIOS packets cannot get through a router.

Table 10-6 IPX: Novell NetBIOS Packets Cannot Get through Router

Possible Cause	Suggested Actions
Missing **ipx type-20-propagation** interface configuration command	**Step 1** Use the **debug ipx packet** privileged EXEC command to look for Novell packets with an unknown specification as type 20. **Step 2** Use the **write terminal** privileged EXEC command to check for an **ipx type-20-propagation** interface configuration command configured for the incoming and outgoing interface for Novell NetBIOS traffic from stations. **Step 3** If the **ipx type-20-propagation** command is not present, add it as appropriate.

Client Cannot Access Remote Servers over Frame Relay

Symptom: In a hub-and-spoke environment, Novell clients are unable to connect to remote Novell servers across a Frame Relay network. Connections can be made to local servers. Table 10-7 describes possible causes and suggested actions when Novell clients cannot access remote servers over Frame Relay.

Table 10-7 IPX: Novell Client Cannot Access Remote Servers over Frame Relay

Possible Causes	Suggested Action
The hub router is not forwarding Service Advertisement Protocol (SAP) packets because of the split horizon rule.	**Step 1** If you are running Software Release 9.1 or earlier, use the **novell sap** interface configuration command to configure a static SAP at each spoke site indicating the Frame Relay interface of the hub router as the next hop. For information on the exact usage of the **novell sap** interface configuration command, see the "Router Products Command Reference." **Step 2** If you are running Software Release 9.21 or later, configure subinterfaces on the Frame Relay interface of the hub router. Assign a subinterface to each spoke site. The hub router will treat each subinterface as a physical interface, allowing it to advertise SAPs without violating split horizon. For specific information on configuring subinterfaces, see the "Router Products Configuration Guide."
Frame Relay map statements and data link connection identifier (DLCI) assignments are misconfigured	**Step 1** Examine the Frame Relay map assignments currently configured, using the **show frame-relay map** EXEC command. **Step 2** Check each Frame Relay map statement to ensure that the DLCI assignments are correctly configured.
Novell servers are unable to handle the rate at which routers generate multi-packet SAP updates	**Step 1** Compare the output of the **show ipx servers** EXEC command from the router with the output of the **slist** command from Novell servers. If the **slist** output for a Novell server shows a partial listing of SAP entries, it is possible that the Novell servers are unable to handle the rate at which the router is generating SAP updates. This problem is more likely in older servers or servers with older LAN card drivers. **Step 2** Use the **ipx output-sap-delay** interface configuration command to specify the delay between packets in a multipacket SAP update. Novell recommends a delay of 55ms. However, a delay of as little as of 5 ms may work. Use the lowest possible delay that corrects the problem.

Possible Causes	Suggested Action
Slow serial line causes SAP updates to be dropped from the output queue of hub router	**Step 1** Issue the **show interfaces serial** EXEC command and examine the value indicated in the output queue "drops" field. A large number of dropped packets may indicate that SAP updates are not reaching clients across the serial link. **Step 2** Re-evaluate implemented SAP filtering. Eliminate the forwarding of any SAP updates that are not absolutely necessary. Use the **access-list** global configuration command and the **ipx input-sap-filter**, **ipx output-sap-filter**, and **ipx router-sap-filter** interface configuration commands, as appropriate. **Step 3** Increase the available bandwidth if possible. Add a second serial line or obtain a single link with more available bandwidth. **Step 4** Increase the output hold queue on the serial interface using the **hold-queue** *length* **out** interface configuration command. **Step 5** Use the **ipx output-sap-delay** interface configuration command to specify the delay between packets in a multipacket SAP update. Use the lowest possible delay that corrects the problem.

Clients Cannot Connect to Server over Packet-Switched Network

Symptom: Local servers are responding, but servers on the other side of a packet-switching network that interconnects routers do not respond. A router *appears* to block IPX over the packet-switched network (PSN). Table 10-8 outlines possible causes and suggested actions when clients cannot connect to servers over a PSN.

Table 10-8 IPX: Clients Cannot Connect to Server over Packet-Switched Network

Possible Cause	Suggested Actions
X.25 address mapping error	**Step 1** Use the **write terminal** privileged EXEC command to examine the configuration of the router. **Step 2** Make sure that the MAC addresses and X.121 addresses specified in any **x25 map ipx** interface configuration commands match the addresses associated with the respective destination routers. Refer to the following section, "Notes about Packet-Switched Network Address Map Specifications," for address-mapping information.
Misconfigured network number specification on servers or routers	**Step 1** See Table 10-4 for suggested actions.
Encapsulation mismatch	**Step 1** Use the **write terminal** privileged EXEC or the **show interfaces** EXEC command to determine the encapsulation type being used. **Step 2** Look for a relevant packet-switching encapsulation type (such as **encapsulation x25**). If an encapsulation command is not present, the default is High-Level Data Link Control (HDLC) encapsulation. **Step 3** For PSN interconnection, you must explicitly specify an encapsulation type.

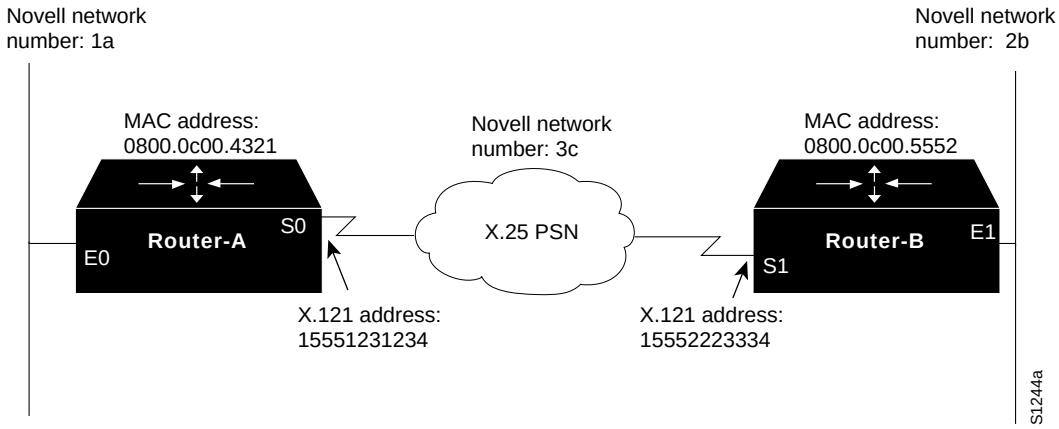
Notes about Packet-Switched Network Address Map Specifications

When routing Novell IPX (or any protocol) over a PSN, you must specify mapping between the protocol and PSN addresses. Consider the two examples illustrated in Figure 10-7 and Figure 10-8. Figure 10-7 illustrates an address map specification for routing Novell IPX over an X.25 PSN, while Figure 10-8 illustrates an address map specification for routing Novell IPX over a Frame Relay network. Relevant configurations and a brief explanation of command variables are provided in the following discussions.

Address Mapping for Novell-to-X.25 Interconnection

As illustrated in Figure 10-7, Novell-to-X.25 address map specifications are required for both Router-A and Router-B.

Figure 10-7 Network Diagram Illustrating Novell-to-X.25 Mapping



The interface specifications are as follows:

```
!Router-A X.25 mapping configuration
!Specifies Novell-to-X.121 address map configuration for Router-A
!
interface serial 0
x25 map ipx 3c.0800.0c00.5552 15552223334 broadcast

!Router-B X.25 mapping configuration
!Specifies Novell IPX-to-X.121 address map configuration for Router-B
!
interface serial 1
x25 map ipx 3c.0800.0c00.4321 15551231234 broadcast
```

Use the **write terminal** privileged EXEC command on the target router to obtain the MAC address. Look for the **ipx routing** global configuration command in the configuration listing. It is displayed with the auto-generated MAC address appended to the command. For example, for Router-A in Figure 10-7, you would see the following:

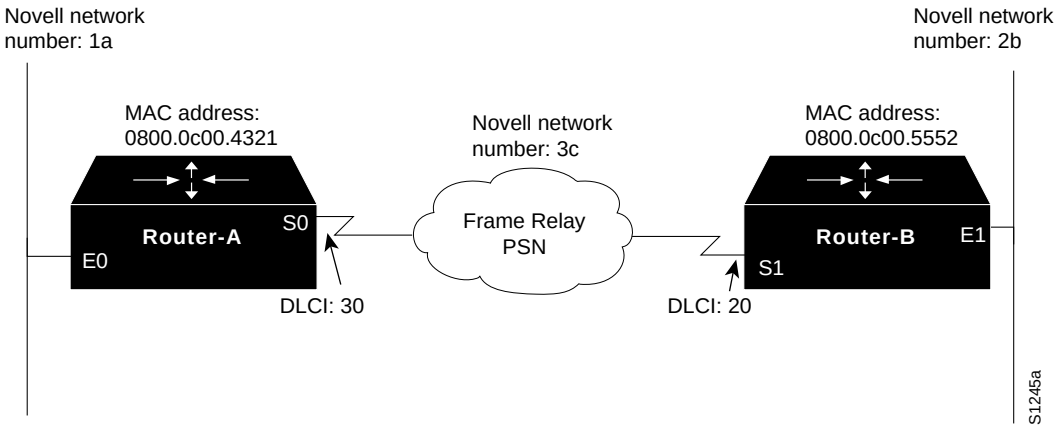
```
ipx routing 0800.0c00.4321
```

Note For IPX routing over an X.25 PSN, a static MAC address is recommended. Choose the MAC address of any local Ethernet, Token Ring, or FDDI interface and specify it with the **ipx routing** *address* global configuration command.

Address Mapping for Novell-to-Frame Relay Interconnection

Figure 10-8 shows essentially the same interconnection arrangement as shown in Figure 10-7, except that the PSN is a Frame Relay network. In an analogous manner, Novell-to-Frame Relay address map specifications are required for both Router-A and Router-B.

Figure 10-8 Network Diagram Illustrating Novell-to-Frame Relay Mapping



The interface configurations are as follows:

```
!Router-A Frame Relay mapping configuration
!Specifies Novell-to-DLCI address map configuration for Router-A
!
interface serial 0
frame-relay map ipx 3c.0800.0c00.5552 20 broadcast

!Router-B Frame Relay mapping configuration
!Specifies Novell-to-DLCI address map configuration for Router-B
!
interface serial 1
frame-relay map ipx 3c.0800.0c00.4321 30 broadcast
```

Use the **write terminal** privileged EXEC command on the target router to obtain the MAC address. Look for the **ipx routing** global configuration command in the configuration listing. It is displayed with the auto-generated MAC address appended to the command.

Note For IPX routing over a Frame Relay PSN, a static MAC address is recommended. Choose the MAC address of any local Ethernet, Token Ring, or FDDI interface and specify it with the **ipx routing** *address* global command.

Enhanced IGRP Router Stuck in Active Mode

Symptom: An IPX Enhanced IGRP router is stuck in Active mode. An Enhanced IGRP router can be in either Passive or Active mode. A router is said to be Passive for Network A when it has an established path to Network A in its routing table.

If the Enhanced IGRP router loses the connection to Network A, it becomes Active for that network. The router sends out queries to all of its neighbors in order to find a new route to Network A. The router remains in Active mode until it has either received replies from *all* of its neighbors or until the active timer, which determines the maximum period of time a router will stay Active, has expired.

If the router receives a reply from each of its neighbors, it computes the new next hop to Network A and becomes Passive for that network. However, if the active timer expires, the router removes from its neighbor table any neighbors that did not reply, again enters Active mode, and issues a "Stuck-in-Active" message to the console:

```
%DUAL-3-SIA: Route 3c.0800.0c00.4321 Stuck-in-Active
```

Note It is essential to note that the occasional appearance of these messages is *not* cause for concern. This is simply the manner in which an Enhanced IGRP router recovers if it does not receive replies to its queries from all of its neighbors. However, if these error messages occur frequently, the problem should be investigated.

Table 10-9 describes possible causes and suggested actions when an IP Enhanced IGRP router is stuck in Active mode.

Table 10-9 IPX: Enhanced IGRP Router Stuck in Active Mode

Possible Causes	Suggested Actions
Active timer value is misconfigured	**Step 1** The active timer determines the maximum period of time that an Enhanced IGRP router will wait for replies to its queries. If the active timer value is set too low, there might not be enough time for all of the neighboring routers to send their replies to the Active router.
	Step 2 Check the configuration of each Enhanced IGRP router using the **write terminal** privileged EXEC command. Look for the **timers active-time** router configuration command associated with the **ipx router eigrp** global configuration command.
	Step 3 The value set by the **timers active-time** command should be consistent among routers in the same autonomous system. We strongly recommend configuring a value of 3 (3 minutes, which is the default value) to allow all Enhanced IGRP neighbors to reply to queries.

Possible Causes	Suggested Actions
Interface or other hardware problem	**Step 1** If queries and replies are not sent and received properly, the active timer will time out and cause the router to issue an error message. Issue the **show ipx eigrp neighbors** EXEC command and examine the Uptime and Q Cnt (queue count) fields in the output. If the uptime counter is continually resetting or if the queue count is consistently high, there might be a problem with hardware. **Step 2** Determine where the problem is occurring by looking at the output of the stuck in Active error message, which will indicate the IPX address of the problematic node. **Step 3** Make sure the suspect router is still functional. Check the interfaces on the suspect router. Make sure the interface and line protocol are up and determine whether the interface is dropping packets. For more information on troubleshooting hardware, see the "Troubleshooting Router Startup Problems" and the "Troubleshooting Serial Line Problems" chapters. **Step 4** Make sure the suspect router has not had its configuration changed in a manner that could effect the convergence of the Enhanced IGRP routing protocol. Static routes, for example, can cause problems. **Step 5** Try jumpstarting the Enhanced IGRP router using the **clear ipx eigrp neighbors** privileged EXEC command. This causes the router to clear its neighbor table, enter Active mode, and attempt to reaquire its neighbor information.
Flapping route	**Step 1** If there is a flapping serial route (caused by heavy traffic load), queries and replies might not be forwarded reliably. Route flapping caused by heavy traffic on a serial link can cause queries and replies to be lost, resulting in the active timer timing out. **Step 2** Take steps to increase the bandwidth of the link.

CHAPTER 11

Troubleshooting TCP/IP Connectivity

This chapter presents protocol-related troubleshooting information for Transmission Control Protocol/Internet Protocol (TCP/IP) connectivity problems. The chapter consists of the following sections:

- TCP/IP Route Redistribution and Access Control Scenario
- TCP/IP Connectivity Symptoms

Each symptom module is divided into the following sections:

- Symptom statement—A specific symptom associated with TCP/IP connectivity
- Possible causes and suggested actions—A table for each symptom containing possible causes for the symptom and suggested actions for resolving each cause

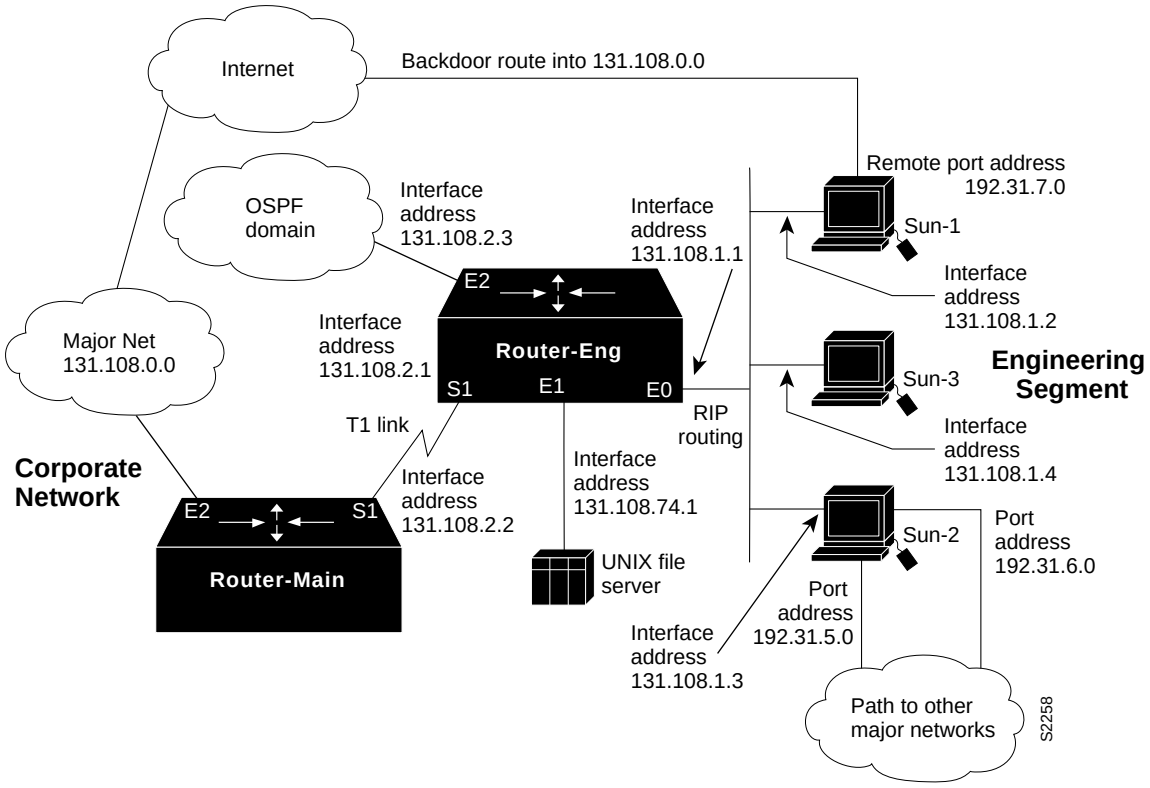
TCP/IP Route Redistribution and Access Control Scenario

Many of the largest internetworks employ TCP/IP as their backbone network protocol. However, this does not mean that these networks employ universal internetworking implementations. In fact, TCP/IP internetworks—sometimes comprising thousands of internetworking nodes—can span organizational domains that employ completely different topologies, routing protocols, and possibly conflicting administrative objectives. The challenge is to provide the requisite level of connectivity between hosts in different domains and on different major networks, while providing adequate security for each organization attached to the internetwork. This scenario focuses on the issue of balancing connectivity and security.

Symptoms

This scenario addresses connectivity problems in TCP/IP internetworks. Figure 11-1 illustrates interconnections from one subnet to a corporate network as well as interconnections to external networks.

Figure 11-1 TCP/IP Internetwork Connectivity Scenario Map



Sun-1, Sun-2, and Sun-3 on the Ethernet segment attached to Router-Eng are unable to communicate with hosts in the main corporate network or outside the organization through Router-Eng. Several backdoor routes also exist, which allow other networks to access the engineering segment.

Because external access is not being reliably controlled and because users on the engineering segment are unable to get through to the corporate network via Router-Eng, this scenario represents a security problem as well as a connectivity problem.

Environment Description

The relevant elements of the internetworking environment shown in Figure 11-1 can be summarized as follows:

- Remote service is provided to a geographically separated network via a point-to-point serial link.
- Two routers (Router-Main and Router-Eng) interconnect the engineering segment with the corporate network and an Open Shortest Path First (OSPF) domain.
- The corporate network is interconnected to a large internetwork.
- Several backdoor routes into the engineering segment are available through serial connections to two of the UNIX hosts.

- The LANs are all IEEE 802.3 Ethernets; the serial link from the engineering segment to the corporate network is a dedicated T1 link (1.544 Mbps). The backdoor links to the UNIX workstation-based routers are asynchronous lines.
- The only network layer protocol running in this network is IP; the engineering segment is using Routing Information Protocol (RIP) locally. An OSPF domain is reachable through the Router-Eng router. The corporate network uses Interior Gateway Routing Protocol (IGRP).
- The network applications intended to run over the T1 line are limited to file transfer (File Transfer Protocol [FTP]), mail (Simple Mail Transfer Protocol [SMTP]), and virtual terminal connections (Telnet).

Diagnosing and Isolating Problem Causes

Given the situation, the following candidates are likely causes for interconnection problems:

- Misconfigured route redistribution
- Misconfigured access lists

The next step is to analyze each potential cause as the problem source and then test the network to determine whether it is operational after each modification is made. The following discussion considers these possible problems and alternatives for providing the proper access and security.

Isolating Router Software Configuration Problems

Because the UNIX workstation-based routers on the engineering segment are using RIP to route among themselves, while the corporate network uses IGRP, the first configuration issue to consider is route redistribution.

Step 1 Use the **write terminal** privileged EXEC command to review the configuration on Router-Eng. In order for RIP routes and IGRP routes to be passed between the engineering segment and the corporate network, Router-Eng must be configured for redistribution.

Step 2 Assuming that Router-Eng does not have redistribution configured, add appropriate redistribution commands.

Figure 11-2 illustrates a partial configuration for Router-Eng that establishes RIP-to-IGRP route redistribution for this network and prevents IGRP-to-RIP route redistribution.

Figure 11-2 RIP-to-IGRP Route Redistribution Configuration Example

```
router rip
distance 255
network 131.108.0.0
passive-interface serial 1
default-metric 2
redistribute igrp 101
!
router igrp 101
network 131.108.0.0
passive-interface ethernet 0
!
```

S2419

Note the following points about Figure 11-2:

- The **passive-interface** router configuration command prevents RIP from running on the serial network (serial 1) and blocks IGRP from running on the Ethernet network (ethernet 0).
- The **default-metric** value is assigned for the redistribution of IGRP routes sent into the RIP domain.

Figure 11-3 shows a partial configuration for Router-Eng that redistributes IGRP routes into the OSPF domain and OSPF routes back into IGRP.

Figure 11-3 IGRP-to-OSPF Route Redistribution Configuration Example

```
router igrp 101
network 131.108.0.0
passive-interface ethernet 2
default-metric 10000 100 255 1 1500
redistribute ospf 1
!
router ospf 1
network 131.108.0.0
default-metric 2 0.0.0.255 area0
redistribute igrp 101 subnets
!
```

S2643

Note the following points about Figure 11-3:

- The **passive-interface** command prevents IGRP from running on the Ethernet network (ethernet 2).
- The **default-metric** value is assigned for the redistribution of OSPF routes sent into the IGRP domain.

Step 3 At this point, you might perform an extended **ping** from Router-Main to one or more of the UNIX nodes on the engineering segment. Assuming that no access controls are in place, the ping should be successful, and Sun-1, Sun-2, and Sun-3 should be able to communicate with the corporate network resources.

However, setting up redistribution does not provide any means of blocking the uncontrolled backdoor access available through the asynchronous lines on the UNIX routers (Sun-1 and Sun-2).

Step 4 The next step is to set up access lists to allow Sun-1, Sun-2, and Sun-3 on the engineering segment to access the corporate network but to block access from outside the corporation to resources on the corporate network.

Step 5 Figure 11-4 illustrates additional commands for Router-Eng to control access to the corporate network.

Figure 11-4 Access Control Additions to Router-Eng Configuration

```
interface serial 1
ip access-group 20
!
access-list 20 permit 131.108.1.2
access-list 20 permit 131.108.1.3
access-list 20 permit 131.108.1.4
```

S2420

Access list 20 and the **ip access-group 20** interface configuration command (applied to serial 1) permit Sun-1, Sun-2, and Sun-3 on Ethernet0 to make connections *through* serial 1. However, other access via serial 1 is blocked.

Figure 11-5 illustrates a modification to the access list specification for Router-Eng that provides a slightly different access control. Access list 21 also illustrates how order can be crucial in access list specifications. Here, the first line of access list 21 specifies that if the packet comes from address 131.108.1.4, it will be blocked (denied). If the packet is not from this source address, the next line is read. This line indicates that any packets from any other node on subnet 131.108.1.0 are permitted on serial 1—specifically packets from 131.108.1.2 and 131.108.1.3.

If the **permit** and **deny** statements for access list 21 are swapped, all packets on subnet 131.108.1.0 are permitted. The second line is never applied, because 131.108.1.4 has *already passed* the first list entry. All other traffic is denied.

Figure 11-5 Standard Access Control for Router-Eng Configuration

```
interface serial 1
ip access-group 21
!
access-list 21 deny 131.108.1.4
access-list 21 permit 131.108.1.0 0.0.0.255
```

S2421

Another access list variation is an extended access list. Figure 11-6 illustrates an extended access list that is used to limit access to resources by Sun-1 and Sun-2. This access lists uses source and destination filtering to control traffic from the UNIX nodes on Ethernet0. As specified, Sun-1 and Sun-2 only can access resources directly connected to 131.108.0.0. Traffic intended for any other network will not be allowed out Serial1.

Figure 11-6 Extended Access Control for Router-Eng Configuration

```
ip access-group 101
!
access-list 101 permit ip 131.108.1.2 0.0.0.0 131.108.0.0 0.0.255.255
access-list 101 permit ip 131.108.1.3 0.0.0.0 131.108.0.0 0.0.255.255
```

S2422

Problem Solution Summary

This scenario focused on solving two problems in TCP/IP internetworks:

- Allowing the proper redistribution of routing information between different domains
- Providing appropriate access to network resources while establishing controls that limit access to networks from external hosts

Of these two, implementing redistribution is relatively straightforward, while access lists can be fairly complicated and can yield unexpected results.

Figure 11-7 illustrates a complete router configuration for Router-Eng (obtained by using the **write terminal** privileged EXEC command).

Figure 11-7 Complete Example Configuration for Router-Eng

```
Current configuration:
!
enable password noBuGZ
!
boot host Router-Eng-confg 131.108.2.20
boot system gs3-bf.shell 131.108.2.20
!
interface ethernet 0
ip address 130.108.1.1 255.255.255.0
!
interface ethernet 1
ip address 130.108.74.1 255.255.255.0
!
!
interface serial 1
ip address 131.108.2.1 255.255.255.0
ip access-group 20
!
router rip
default-metric 2
network 131.108.0.0
distance 255
redistribute igrp 101
passive-interface serial 1
!
router igrp 101
network 131.108.0.0
passive-interface ethernet 0
!
!
ip domain-name cisco.com
ip name-server 255.255.255.255
snmp-server community
snmp-server community dink RO
snmp-server host 131.108.2.30 dink
access-list 20 permit 131.108.1.4
access-list 20 permit 131.108.1.2
access-list 20 permit 131.108.1.3
hostname Router-Eng
!
!
line vty 0 4
login
line con 0
exec-timeout 0 0
password nErdKnoBs
line aux 0
no exec
line vty 0
password nErdKnoBs
line vty 1
password nErdKnoBs
line vty 2
!
end
```

S2423

TCP/IP Connectivity Symptoms

The symptom modules in the following sections pertain to TCP/IP internetwork problems. Unless otherwise indicated, each module is presented as a set of general problems. Where there are special considerations associated with a situation, notes are included.

- Host Cannot Access Offnet Hosts
- Host Cannot Access Certain Networks
- Connectivity Available to Some Hosts but Not Others
- Some Services Are Available, Others Are Not
- Users Cannot Make Connections when One Parallel Path Is Down
- Router Sees Duplicate Routing Updates and Packets
- Routing Works for Some Protocols, Not for Others
- Router or Host Cannot Reach Nodes on the Same Network
- OSPF Networks Are Not Advertised
- OSPF Routers Do Not Communicate
- OSPF Protocols Fail to Work on New Interfaces
- OSPF Routers Are Not Receiving Routing Information from Other Areas
- OSPF Routers Are Not Communicating Dynamically
- OSPF External Routes Incorrectly Advertised into Stub Area
- IGRP Routers Do Not Communicate
- Traffic Is Not Getting through Router Using Redistribution
- IGRP or RIP Fail to Work on New Interfaces
- Redistribution route-map Commands Behave Unexpectedly
- Poor or Lost Connectivity in Multiprotocol Network Running Enhanced IGRP
- Poor or Lost Connectivity on Internetwork Running Enhanced IGRP Exclusively
- Enhanced IGRP Router Stuck in Active Mode

Note The symptoms are generic in nature. However, when host configuration problems are discussed, they are addressed assuming UNIX end systems. Equivalent kinds of actions may be applicable to non-UNIX hosts as well, but the discussion here does not address non-UNIX end station problems.

Host Cannot Access Offnet Hosts

Symptom: Host-A is unable to communicate with Host-B on another network. When you attempt to make a connection to an intervening router, you may or may not be able to make a successful connection. For example, you can ping Router-X but not Router-Y. In either case, you are unable to connect to the target host on the other side of the router. This situation is illustrated in Figure 11-8.

Figure 11-8 Host-A Cannot Communicate with Host-B over Routers

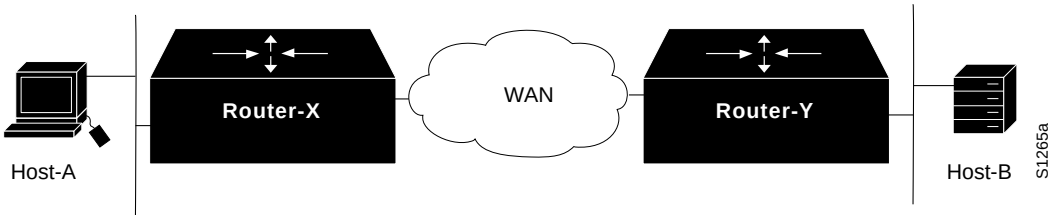


Table 11-1 outlines possible causes and suggested actions when a host cannot access offnet hosts.

Table 11-1 TCP/IP: Host Cannot Access Offnet Hosts

Possible Causes	Suggested Actions
No default gateway specification	**Step 1** Determine whether a default gateway is included in the routing table of the host attempting to make a connection (Host-A in Figure 11-8). Use the following UNIX command: **netstat -rn** **Step 2** Look at the output of this command for a default gateway specification. **Step 3** If the default gateway specification is incorrect, or if it is not present at all, you can change or add a default gateway using the following UNIX command at the local host: **route add default** *address* **1** (*address* is the IP address of the default gateway; the value 1 indicates that the specified node is one hop away) You may need to reboot the host for this change to take effect. **Step 4** To automate this as part of the boot process, specify the default IP address of the gateway in the following UNIX host file: */etc/defaultrouter* This filename may be different for your particular version of UNIX. Or, if you working with a PC or a Macintosh, consult the corresponding documentation to determine how to set the default gateway.

Possible Causes	Suggested Actions
Misconfigured subnet mask	**Step 1** Check the following two locations on the local host for possible subnet mask errors: */etc/netmasks* */etc/rc.local* **Step 2** Fix the netmask if is specified incorrectly, or add the netmask if it is missing. Or, if you working with a PC or a Macintosh, consult the corresponding documentation to determine how to set the subnet mask.
Host interface is down	**Step 1** Verify that the host interface is working.
Router between hosts is down	**Step 1** Use the **ping** command to determine whether the router is reachable. **Step 2** If the router does not respond, isolate the problem and repair the broken interconnection. **Step 3** For more information, refer to the section “Developing a Strategy for Isolating Problems” in the “Troubleshooting Overview” chapter, and to the “Troubleshooting Router Startup Problems” chapter.

Host Cannot Access Certain Networks

Symptom: Host cannot access certain networks on the other side of a router. Some networks might be accessible. Table 11-2 outlines possible causes and suggested actions when a host cannot access certain networks.

Table 11-2 TCP/IP: Host Cannot Access Certain Networks

Possible Causes	Suggested Actions
No default gateway	**Step 1** Check the host for proper default gateway specification and modify or add a default gateway specification as required. For more information, see Table 11-1.
Misconfigured access list (getting routing information for some routes, but not others)	**Step 1** Use the **show ip routes** EXEC command to check routing table and use the appropriate **debug** command (such as **debug ip igrp events** and **debug ip rip**) to check protocol exchanges. **Step 2** Look for information concerning the network with which you are unable to communicate. **Step 3** Check the use of access lists on the routers in the path and make sure that a **distribute-list** or **distance** router configuration command does not filter out the route. **Step 4** Temporarily remove **ip access-group** interface configuration commands to disable access lists, and use the **trace** or **ping** EXEC command with the Record Route option set to determine whether traffic can get through when the access list is removed.
Discontinuous network addressing due to network design	**Step 1** Use the **show ip route** EXEC command to determine which routes are known and how they are being learned. **Step 2** Use the **trace** or **ping** command to see where traffic is stopping. **Step 3** Fix topology or reassign addresses to include all appropriate network segments in the same major network. For additional information, refer to the "Users Cannot Make Connections when One Parallel Path Is Down" symptom module, later in this chapter.
Discontinuous network addressing due to link failure	**Step 1** Restore disabled link. **Step 2** If a link failure occurs, and you cannot use a parallel path, examine network address assignments. **Step 3** If the link failure results in a discontinuous network because one network has different points of contact with two now isolated subnets of a different major network, assign secondary addresses along the backup path to restore major network connectivity.

Connectivity Available to Some Hosts but Not Others

Symptom: Hosts on a network can communicate with specific hosts on the other side of a router, but are unable to communicate with certain other hosts. Table 11-3 outlines possible causes and suggested actions when connectivity is not available to all hosts.

Table 11-3 TCP/IP: Connectivity Not Available to all Hosts

Possible Causes	Suggested Actions
Misconfigured subnet mask	**Step 1** Check subnet masks on hosts and routers. **Step 2** Look for a mismatch between subnet masks. What may be a specific host address to one host may become a subnet broadcast when a different mask is applied at a router. **Step 3** Fix the subnet mask on the host or router as required. See Table 11-1 and Table 11-8 for additional information.
Misconfigured access list (host is denied by some router in the path)	**Step 1** Determine where packets are being dropped by using the **trace** or **ping** EXEC command out through the path. **Step 2** If you can identify the router that is stopping traffic, use the **write terminal** privileged EXEC command to see whether an access list is being used. You also can use the **show access-lists** and **show ip interface** EXEC commands in combination to determine whether access lists are being used. **Step 3** Temporarily disable the access list. **Step 4** Use **ping** or **telnet** to see whether traffic can get through the router. **Step 5** If traffic can get through, review the access list and its associated commands for proper authorization.
Missing default gateway specification on remote host	**Step 1** Have someone log in to the remote host and try to access an offnet host. **Step 2** Check the remote host for the proper default gateway specification and modify or add a default gateway specification as required. For more information, see Table 11-1.

Some Services Are Available, Others Are Not

Symptom: In some cases, you might be able to get through to hosts using some protocols, but cannot get through using others. For instance, you might be able to ping a host and FTP to a host, but Telnet does not get through. Table 11-4 outlines a possible cause and suggested actions when not all services are available.

Table 11-4 TCP/IP: Not All Services Are Available

Possible Cause	Suggested Actions
Misconfigured extended access list	**Step 1** Use the **trace** command to determine the path taken to reach remote hosts.
	Step 2 (Optional) On each router in the path, enable **debug ip icmp** command.
	Any router that returns “unreachable” is suspect.
	Step 3 If you can identify the router that is stopping traffic, use the **write terminal** privileged EXEC command to see whether an access list is being used. You also can use the **show access-lists** and **show ip interfaces** EXEC commands in combination to determine whether access lists are being used.
	Step 4 Temporarily disable the access list.
	Step 5 Determine whether traffic can get through the router.
	Step 6 If traffic can get through, review the access list and its associated commands for proper authorization.
	In particular, look for extended access lists that specify TCP ports.
	Step 7 If an extended access list specifies a TCP port, make sure that the access list explicitly permits all the necessary TCP ports.

For information on how to create access-lists, refer to the *Router Products Configuration Guide.*

Users Cannot Make Connections when One Parallel Path Is Down

Symptom: In configurations that feature multiple paths between networks, there is no communication over the alternative routes when one of the parallel links breaks.

Figure 11-9 illustrates one example of a situation in which this lack of communication can occur. Here, one major network (Net-B) has two or more access points into another major network (Net-C), while a third link joins two separate subnets of Net-C. Details are provided in Table 11-5.

Figure 11-9 Problem Parallel Path Topology Example

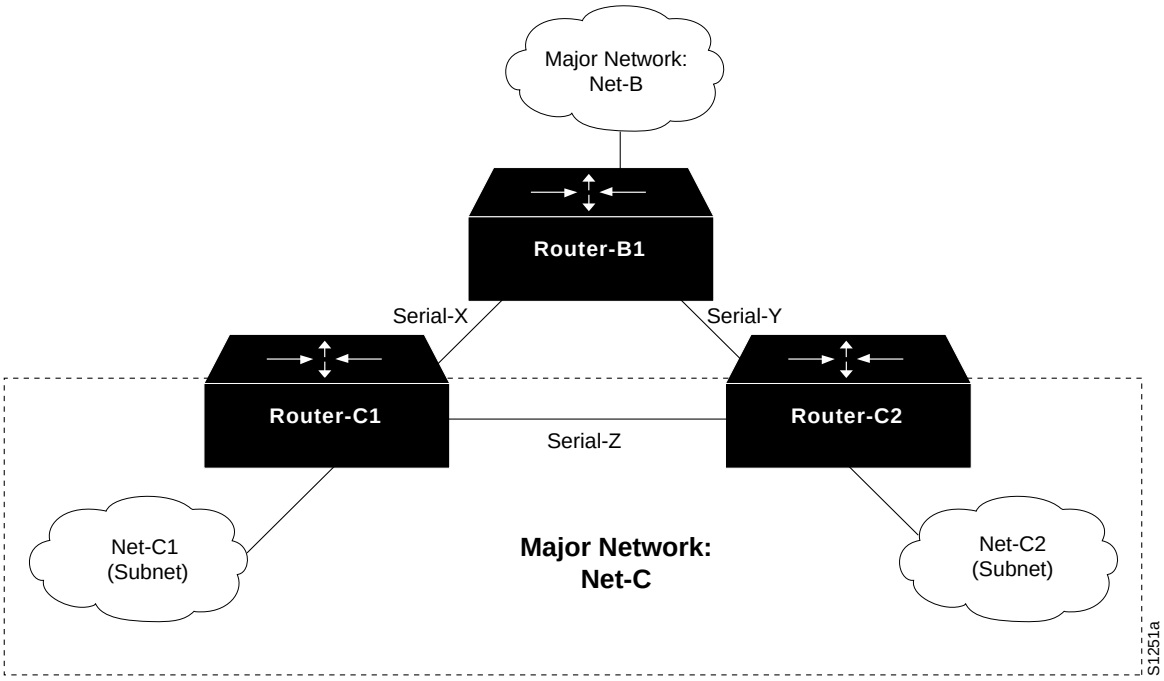


Table 11-5 outlines possible causes and suggested actions when users cannot make connections when one parallel path is down.

Table 11-5 TCP/IP: Users Cannot Make Connections when One Parallel Path Is Down

Possible Causes	Suggested Actions
Discontinuous network due to failure. If Serial-Z is lost, traffic cannot traverse from Net-C1 to Net-C2 through Router-B1	**Step 1** Bring the link back up. **Step 2** As an alternative, use a secondary IP address configuration to ensure that all interfaces are included in the same major network. Refer to Figure 11-9. If Serial-Z is lost, Major Network Net-C becomes a discontinuous network because Router-B1 is separating the two Net-C subnets (Net-C1 and Net-C2). Traffic between Router-C1 and Router-C2 will not get through Router-B1 because Router-B1 assumes that they are directly connected.
Routing has not converged	**Step 1** Assuming that you have used secondary addresses, examine routing tables for routes that are listed as "possibly down." If this entry is found, the routing protocol has not converged. **Step 2** Wait for the routing protocol to converge. Examine the routing table later.
Misconfigured access lists or other routing filters	**Step 1** Check for access lists in the secondary path. **Step 2** If present, disable and determine whether traffic is getting through. If traffic is getting through, an access list and accompanying commands may be causing traffic stoppage. **Step 3** Evaluate and reconfigure access lists as necessary.
Errors on serial link	**Step 1** Use the **show interfaces serial** EXEC command to look for input on the serial interface. **Step 2** For more information, see the "Troubleshooting Serial Line Problems" chapter.
Errors on Ethernet link	**Step 1** Use a time domain reflectometer (TDR) to find any unterminated Ethernet cables. **Step 2** Check host cables and transceiver cables to determine whether any are incorrectly terminated, overly long, or damaged. **Step 3** Look for a jabbering transceiver attached to a host.

Router Sees Duplicate Routing Updates and Packets

Symptom: Router sees duplicate routing updates on different interfaces. Network users might experience sudden loss of connections and extremely poor performance. Router sees other routers and hosts on multiple interfaces. Table 11-6 outlines a possible cause and suggested actions when a router sees duplicate routing updates and packets.

Table 11-6 TCP/IP: Router Sees Duplicate Routing Updates and Packets

Possible Cause	Suggested Actions
Bridge or repeater in parallel with a router, causing updates and traffic to be seen as coming from both sides of an interface	**Step 1** Use the **show ip routes** EXEC command to examine routes for each interface. **Step 2** Look for routers that are known to be remote to the network connected to the router. Routers that are listed but are not attached to any directly connected networks are a likely problem. **Step 3** Look for paths to the same networks with the same cost on multiple interfaces. **Step 4** Another test is to use **debug** EXEC commands to examine protocol routes for each interface, which will identify both the source of the routing update and the inbound interface. For example, **debug ip rip** shows RIP-specific events. **Step 5** If you determine that there is a parallel bridge, disable the bridge or configure the bridge with access filters that block routing updates.

Routing Works for Some Protocols, Not for Others

Symptom: Some protocols are routed, others are not. Telnet, for example, works from a host on one network to a host on another network on the other side of a router, but FTP does not. Perhaps Domain Name Service (DNS) works with your own domain, but does not work for external domains. Table 11-7 outlines a possible cause and suggested actions when routing does not work for all protocols.

Table 11-7 TCP/IP: Routing Does Not Work for All Protocols

Possible Cause	Suggested Actions
Misconfigured access list	**Step 1** Use the **ping** and **trace** EXEC commands to help determine which routers are in the path and should be investigated for misconfigured access lists.
	Step 2 Use the **write terminal** privileged EXEC command on a router that may be stopping traffic.
	Step 3 Look for any access list in the configuration.
	Step 4 Temporarily disable the access list and monitor traffic to and through the suspect router. If the router is allowing previously blocked traffic through, the problem is probably in the access list.
	Step 5 Make sure that you explicitly permit desired traffic; otherwise, unpermitted traffic is blocked by the implicit deny statement that ends all access lists.

Router or Host Cannot Reach Nodes on the Same Network

Symptom: A router or host is unable to communicate with other routers or hosts known to be connected to the same network. Table 11-8 outlines possible causes and suggested actions when a router or host cannot reach nodes on the same network.

Table 11-8 TCP/IP: Router or Host Cannot Reach Nodes on the Same Network

Possible Causes	Suggested Actions
Subnet mask configuration mismatch between router and host	**Step 1** Test connectivity to the destination using the **ping** command at the router or host, as discussed in the section "Developing a Strategy for Isolating Problems" in the "Troubleshooting Overview" chapter. **Step 2** If you can **ping** from the local host to the local router (but not to a remote host), and if you can **ping** from the local router to the remote host, there is probably a subnet mask configuration problem on your local host or router. **Step 3** Check host and router configurations for a subnet mask mismatch. Make sure that all subnet masks match. NOTE: Masks might not match if proxy ARP is being used. Refer to Request for Comments (RFC) 1027 for more information about using proxy ARP. For notes about host subnet masks, refer to the "Host Cannot Access Offnet Hosts" symptom module, earlier in this chapter. For information about subnet mask conflicts, refer to the section "Note about IP Addresses and Subnet Masks" later in this chapter.
Misconfigured access list	**Step 1** See Table 11-7 for suggested actions.
No default gateway specified	**Step 1** Check the remote host for the proper default gateway specification and add or modify the specification as necessary. For more information, see Table 11-1. **Step 2** Check host and router configurations for static routes. **Step 3** If static routes exist and no default gateway is specified, access to some hosts and routers might be possible, while others are unavailable. You have several options for resolving this inconsistency: • Specify a default gateway on your host as described in Table 11-1. • Enable proxy ARP on the router; make the local cable the default network (network 0 for RIP). • Run the Gateway Discovery Protocol (GDP), which allows dynamically defined default gateways, on the host (Berkeley Software Distribution [BSD] UNIX host only). • Run a routing protocol (such as RIP) on the host. Note that there might be high host processing overhead associated with this option.

Possible Causes	Suggested Actions
Incorrect network specified	**Step 1** Enable debug arp and ping hosts. Look for responses that indicate you are on the incorrect network. For example, you believe you are on the physical network attached ethernet 0, but you are really on the physical network attached ethernet 1. In such a case, you might be able to reach all devices on your local network (ethernet 1), and the router might forward your packets. However, because of your network address, the router is operating as if you are on ethernet 0 instead of your correct location on ethernet 1. **Step 2** Move your host so that its address corresponds to the correct network. Or, change the address of your host to match the cable to which it is attached.

Note about IP Addresses and Subnet Masks

In most IP networks, routers and hosts should agree on their common subnet mask. If a router and a host disagree on the length of the subnet mask, packets might not be routed correctly. Consider the situation described in Table 11-9.

A host interprets a particular address (192.31.7.49) as being Host 1 on the third subnet (subnet address 48). However, because it is using a different subnet mask, the router interprets the address as belonging to Host 17 on the first subnet (subnet address 32). Depending on its configuration, the router drops any packet destined for 192.31.7.49 or sends it out on the wrong interface.

Table 11-9 Comparison of Host and Router Subnet Mask Effects

Routing Info	Host Value	Router Value
Destination IP address	192.31.7.49	192.31.7.49
Subnet mask	255.255.255.240	255.255.255.224
Interpreted address	Subnet address 48, host 1	Subnet address 32, host 17

OSPF Networks Are Not Advertised

Symptom: OSPF routes and networks are not being advertised to other routers. Routes are not in the routing table, and hosts are unable to communicate. Table 11-10 lists a possible cause and suggested actions when OSPF networks are not being advertised.

Table 11-10 TCP/IP: OSPF Networks Are Not Advertised

Possible Cause	Suggested Actions
Improper OSPF mask specification	**Step 1** Use the **show ip ospf** EXEC command to determine which interfaces are configured to run OSPF. **Step 2** Use the **write terminal** privileged EXEC command to check the configuration of the router. **Step 3** Look for **network** router configuration commands. Make certain the network masks match the network requirements. For example: `network 131.108.0.0 0.0.255.255 area 0` With this network mask, an interface with an address of 120.110.7.2 is not in any area and is not advertised, which prevents other routers from seeing this network. Adding the following configuration command configures OSPF on this interface and allows network advertisements over this interface: **network 120.110.7.2 0.0.255.255 area 0**

OSPF Routers Do Not Communicate

Symptom: Connectivity fails for OSPF routers and networks. Hosts or routers do not communicate with one another. Table 11-11 lists possible causes and suggested actions for OSPF routers that do not communicate.

Table 11-11 TCP/IP: OSPF Routers Do Not Communicate

Possible Causes	Suggested Actions
Network is down	**Step 1** Use the **ping** command to determine whether the router is reachable. **Step 2** If the router does not respond, isolate the problem and repair the broken interconnection. **Step 3** For more information, refer to the section "Developing a Strategy for Isolating Problems" in the "Troubleshooting Overview" chapter, and to the "Troubleshooting Router Startup Problems" chapter.
Misconfigured access list	**Step 1** See Table 11-7 for suggested actions.

OSPF Protocols Fail to Work on New Interfaces

Symptom: New interfaces are added to a router, but the protocol configured for the router does not work on the new interfaces. New interfaces in the router are assigned to a different major network than existing interfaces, and the routing protocol fails. Table 11-12 lists a possible cause and suggested actions when OSPF routing protocols fail to work on new interfaces.

Table 11-12 TCP/IP: OSPF Protocols Fail to Work on New Interfaces

Possible Cause	Suggested Actions
Missing **network** router configuration command	**Step 1** Use the **show ip ospf interfaces** EXEC command to find out which interfaces have OSPF enabled. **Step 2** Use the **write terminal privileged** EXEC command to list the router configuration if the **show ip ospf interfaces** output does not show OSPF running on the new interface. **Step 3** Look for the **network** router configuration command. Make sure that the networks on which OSPF runs include the new interfaces and that they define the area IDs for those interfaces.

OSPF Routers Are Not Receiving Routing Information from Other Areas

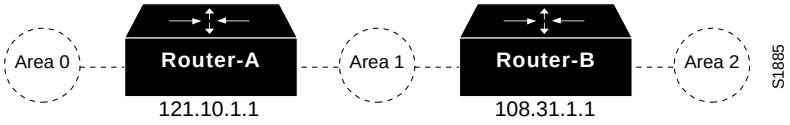
Symptom: OSPF nodes in one area are not seeing routing information for other areas. Some hosts being are unable to communicate with hosts in other areas, and routing table information is incomplete. Table 11-13 lists possible causes and suggested actions when OSPF routers are not receiving routing information from other areas.

Table 11-13 TCP/IP: OSPF Routers Not Receiving Routing Information from Other Areas

Possible Causes	Suggested Actions	
A specific area is isolated from the OSPF backbone	**Step 1**	Use the **write terminal** privileged EXEC command to verify that at least one border router exists for each area. Area border routers must have **area 0** defined by the **network** router configuration command, and the backbone area (area 0) must not be partitioned.
	Step 2	If no area border router exists in an area, add one where appropriate.
Hello timer or dead timer intervals are mismatched in the OSPF domain	**Step 1**	Use the **write terminal** privileged EXEC command at each router and make sure that values for the Hello timer and dead timer match for all routers in the OSPF domain.
	Step 2	Change timer values as required. Note that timer values are extremely important when Cisco routers interoperate with routers from other vendors.
A virtual link is configured through a stub area	**Step 1**	A stub area cannot be used as a transit area for virtual links. Use the **write terminal** privileged EXEC command and look for the following router configuration commands: **area** *area-id* **stub** **area** *area-id* **virtual-link** *router-id*
	Step 2	Verify that no virtual link is configured through a router defined as an area stub.
IGRP or RIP is not redistributed correctly into OSPF	**Step 1**	The **subnet** keyword must be included when IGRP or RIP is redistributed into OSPF; otherwise, only major routes (not subnet routes) are redistributed.
	Step 2	Use the **write terminal** privileged EXEC command to check that the **subnet** keyword is used with the **redistribute** router configuration command.
	Step 3	Add the **subnet** keyword as appropriate.

Possible Causes	Suggested Actions
A virtual link is misconfigured	**Step 1** A virtual link requires that the routers at each area boundary of the transit area point to one another. (See Figure 11-10.) **Step 2** Use the **show ip ospf** EXEC command to get the border router ID on each side of the transit area (area 1). **Step 3** Add or modify the **area** *area-id* **virtual-link** *router-id* router configuration command. For example, in Router-A create a virtual link to Router-B: **area 1 virtual-link 108.31.1.1** And in Router-B, create a virtual link to Router-A: **area 1 virtual-link 121.10.1.1**

Figure 11-10 Virtual Links and Transit Areas



OSPF Routers Are Not Communicating Dynamically

Symptom: OSPF routers are not communicating dynamically with their neighbors. Some routers can communicate, but some routers are unreachable. Table 11-14 lists possible causes and suggested actions when OSPF routers are not communicating dynamically.

Table 11-14 TCP/IP: OSPF Routers Not Communicating Dynamically

Possible Causes	Suggested Actions
Hello timer or dead timer intervals are mismatched in the OSPF domain	**Step 1** Use the **show ip ospf neighbor** EXEC command to identify the OSPF neighbors of the router. **Step 2** If the output does not list an expected neighbor, use the **show ip ospf interfaces** EXEC command to see the Hello and dead timer intervals configured on the interface. Compare these values with the configured value on the expected neighbor. If there is a mismatch, reconfigure the timer values, so they are the same on the router and its neighbor. Note that timer values are extremely important when Cisco routers interoperate with routers from other vendors.
A virtual link is configured through a stub area	**Step 1** See Table 11-13 for suggested actions.

OSPF External Routes Incorrectly Advertised into Stub Area

Symptom: OSPF external routes are incorrectly advertised into a stub area. Some routers can communicate, but specific routers or hosts are unreachable. Table 11-15 lists a possible cause and suggested actions when OSPF external routes are incorrectly advertised into a stub area.

Table 11-15 TCP/IP: OSPF External Routes Incorrectly Advertised into Stub Area

Possible Cause	Suggested Actions
Not all routers in stub area are configured as stubs	**Step 1** Use the **write terminal** privileged EXEC command to list the configuration for each router in the stub area. **Step 2** Verify that the configuration of all routers in the stub area includes the **area** *area-id* **stub** command.

IGRP Routers Do Not Communicate

Symptom: Connectivity fails for IGRP routers and networks. Hosts or routers do not communicate with one another. Table 11-16 lists possible causes and suggested actions when IGRP routers are not communicating.

Table 11-16 TCP/IP: IGRP Routers Not Communicating

Possible Causes	Suggested Actions
Network is down	**Step 1** Use the **ping** command to determine whether the router is reachable. **Step 2** If the router does not respond, isolate the problem and repair the broken interconnection. **Step 3** For more information, refer to the section "Developing a Strategy for Isolating Problems" in the "Troubleshooting Overview" chapter, and to the "Troubleshooting Router Startup Problems" chapter.
Misconfigured access list	**Step 1** See Table 11-7 for suggested actions.

Traffic Is Not Getting through Router Using Redistribution

Symptom: Traffic is not getting through a router that is redistributing routes between two different routing domains—typically RIP and IGRP. Observed symptoms range from poor performance to no communication at all. Poor performance can occur when nonoptimal routes are used because the best path is blocked by a misconfigured redistribution. Table 11-17 outlines possible causes and suggested actions when traffic is not getting through a router using route redistribution.

Table 11-17 TCP/IP: Traffic Not Getting through Router Using Redistribution

Possible Cause	Suggested Actions
Missing **default-metric** command	**Step 1** Use the **write terminal** privileged EXEC command to check the router configuration for the **default-metric** router configuration command. **Step 2** If the **default-metric** router configuration command is missing, add it to the configuration, using appropriate values.
Problem with the default administrative distance	**Step 1** Determine the policy for identifying how much you *trust* routes derived from different domains. Problems occur when a particular route is, by default, trusted less than another, but actually is the preferred route. **Step 2** Use the **distance** router configuration command to vary the level of trust associated with specific routing information as necessary.
Missing **redistribute** command	**Step 1** Check router configuration using the **write terminal** privileged EXEC command. **Step 2** If the **redistribute** router configuration command is missing, add it to the configuration. For more information, refer to the *Router Products Configuration Guide* and *Router Products Command Reference* publications.
Misconfigured access list	**Step 1** See Table 11-7 for suggested actions.
Misconfigured **distribute-list** command	**Step 1** Use the **write terminal** privileged EXEC command to check the configuration of the router. **Step 2** Verify that any **distribute-list** router configuration command specifies the correct access list.

IGRP or RIP Fail to Work on New Interfaces

Symptom: New interfaces are added to a router, but the protocol configured for the router does not work on them. The new interfaces are assigned to a different major network than existing interfaces, and the routing protocol fails. Table 11-18 lists a possible cause and suggested actions when IGRP or RIP fail to work on new interfaces.

Table 11-18 TCP/IP: IGRP or RIP Fail on New Interfaces

Possible Cause	Suggested Actions

Missing **network** router configuration command	**Step 1** Use the **write terminal** privileged EXEC command to list the configuration of the router.
	Step 2 When more than one major network is configured in a router, add the **network** router configuration command. For example, a router that runs IGRP and that supports two major networks, such as 128.10.0.0 and 192.31.7.0, must have the following commands in its configuration:
	`router igrp 109`
	`network 128.10.0.0`
	`network 192.31.7.0`

Redistribution route-map Commands Behave Unexpectedly

Symptom: A series of **redistribute** and **route-map** router configuration commands allow some routes to be redistributed but deny others. Also, some routes that are configured to deny redistribution are redistributed. Table 11-19 lists possible causes and suggested actions when redistribution problems occur with the **redistribute** and **route-map** router configuration commands.

Table 11-19 TCP/IP: Redistribution route-map Commands Behave Unexpectedly

Possible Causes	Suggested Actions
Sequence numbers cause some conditions to be tested before others	**Step 1** Use the **write terminal** privileged EXEC command to display the configuration of the router. **Step 2** Look at the sequence numbers assigned to the **redistribute** router configuration commands. Lower sequence numbers are tested before higher sequence numbers, regardless of their listed order. **Step 3** Modify the sequence numbers so the conditions are tested in the desired order.
Missing condition in the series of router redistribution commands	**Step 1** Use the **write terminal** privileged EXEC command to display the router configuration. **Step 2** Look at the configuration and be sure that conditions to permit or deny certain redistributions are included. **Step 3** Add or modify conditions that determine when a route is redistributed.

Consider the example configuration shown in Figure 11-11 and the modified configuration shown in Figure 11-12. In Figure 11-11, a router is configured to redistribute RIP and ISO-IGRP routes into an Intermediate System-to-Intermediate System (IS-IS) level-2 LSP with a metric of 5. All destinations on the RIP network with address 160.89.0.0 are redistributed, as are all ISO-IGRP routes with a prefix of 49.0001.0002.

Figure 11-11 Configuration Example for Redistribution Using Route Maps

```
router isis
redistribute rip route-map 1
redistribute iso-igrp remote route-map 1

route-map 1 permit
match ip address 1
match clns address 2
set metric 5
set level level-2

access-list 1 permit 160.89.0.0 0.0.255.255
clns filter-set 2 permit 49.0001.0002...
```

S2648

However, you want to exclude a particular subnet from RIP route redistribution. The additional configuration commands shown in Figure 11-12 exclude subnet 160.89.111.0. By assigning a sequence number of 5, you ensure that this address will be excluded before the more general access for 160.89.0.0 is processed. The **redistribute** router configuration commands, with their sequence numbers, can be entered in any order, making it easier to modify a router configuration. You can add new permit and deny access lists at the end of the configuration file instead of having to reenter all access lists in the desired order.

Figure 11-12 Modified Configuration Example for Redistribution Using Route Maps

```
router isis
redistribute rip route-map 5
redistribute rip route-map 10
redistribute iso-igrp remote route-map 10

route-map 5 deny
match ip address 5

route-map 10 permit
match ip address 10
match clns address 20
set metric 5
set level level-2

access-list 5 permit 160.89.111.0 0.0.0.255
access-list 10 permit 160.89.0.0 0.0.255.255
clns filter-set 20 permit 49.0001.0002...
```

S2649

Poor or Lost Connectivity in Multiprotocol Network Running Enhanced IGRP

Symptom: Nodes on a multi-protocol internetwork running IP Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) and any combination of IGRP, RIP, OSPF, or other typically used routing protocols experience poor connectivity or lost connectivity with other nodes on the network. Table 11-20 describes possible causes and suggested actions when connectivity problems occur between nodes in a multiprotocol and IP Enhanced IGRP environment.

Table 11-20 TCP/IP: Poor or Lost Connectivity in Multiprotocol Internetwork Running IP Enhanced IGRP

Possible Causes	Suggested Actions

IGRP, RIP, OSPF or other routing protocols are not enabled on boundary routers.	**Step 1** Issue the **write terminal** privileged EXEC command on the boundary routers. Look for the **router** global configuration commands associated with the routing protocols you are running.
	Step 2 If the applicable commands are not present, enable the routing protocols you want to use with the correct **router** global configuration command.
	Step 3 In router configuration mode, enter the appropriate **network** commands to associate networks with the routing process, as applicable. For example, to enable IGRP routing on networks 193.166.66.12 and 193.168.25.25, enter the following configuration commands:
	`Router(config)# router igrp 100`
	`Router(config-router)# network 193.166.66.0`
	`Router(config-router)# network 193.168.25.0`
	Step 4 For complete information on configuring IGRP, RIP, OSPF, Border Gateway Protocol (BGP), or IS-IS, see the *Router Products Configuration Guide* and the *Router Products Command Reference* publications.

Enhanced IGRP routing is not enabled on boundary routers.	**Step 1** Issue the **write terminal** privileged EXEC command on the boundary routers. Look for the **router eigrp** global configuration command. **Step 2** If the command is not present, enable Enhanced IGRP routing using the **router eigrp** global configuration command. **Step 3** In router configuration mode, enter the appropriate **network** commands to associate networks with the Enhanced IGRP routing process. For complete information on configuring Enhanced IGRP, see the *Router Products Command Reference* and the *Router Products Configuration Guide* publications.

Possible Causes	Suggested Actions
Routes are not being redistributed between routing protocols.	**Step 1** Issue the **write terminal** privileged EXEC command on the boundary routers. Examine the **router** global configuration command entries for the enabled routing protocols (such as IGRP, OSPF, Enhanced IGRP, and so forth) to see if the autonomous system designated for each protocol is the same. **Step 2** If the **router** commands indicate autonomous systems, routes will not be automatically redistributed between the routing protocols. Route redistribution must be manually configured using the **redistribute** router configuration command. NOTE: Only Enhanced IGRP, OSPF, BGP, and IS-IS are capable of understanding redistributed subnet routing information. In the case of IGRP and RIP, subnet information is summarized at the network boundaries. **Step 3** Static routes are not redistributed automatically. If you want static routes to be redistributed between Enhanced IGRP and other routing protocols, you must use the **redistribute static** router configuration command to be sure that static routes are properly redistributed. For more information on the use of the **redistribute** router configuration command for IP Enhanced IGRP and other protocols, see the *Router Products Command Reference* and the *Router Products Configuration Guide* publications.
Default routing metrics are incorrectly configured.	**Step 1** Use the **write terminal** privileged EXEC command on suspect routers. Look for **default-metric** router configuration command entries for any of the enabled routing protocols. This command changes the default metric values assigned to redistributed routes. **Step 2** If a **default-metric** statement appears in the configuration, examine the values that it defines. Be certain that these values will reliably and accurately translate routing metrics between the routing protocols implemented on your network. To restore the default values for the routing metrics, use the **no default-metric** router configuration command for the appropriate routing protocol. **Step 3** For more information on the IP Enhanced IGRP **default-metric** router configuration command, see the *Router Products Command Reference* and the *Router Products Configuration Guide* publications.

Poor or Lost Connectivity on Internetwork Running Enhanced IGRP Exclusively

Symptom: Nodes on an internetwork running IP Enhanced IGRP exclusively experience poor connectivity or lost connectivity with other nodes on the network. Table 11-21 describes possible causes and suggested actions for connectivity problems in an IP Enhanced IGRP-exclusive environment.

Table 11-21 TCP/IP: Poor or Lost Connectivity on IP Enhanced IGRP-Exclusive Network

Possible Causes	Suggested Actions
Neighboring Enhanced IGRP routers are not visible to other Enhanced IGRP routers.	**Step 1** Issue the **show ip eigrp neighbors** EXEC command on the Enhanced IGRP-only router. Make sure that all directly connected Enhanced IGRP routers appear in the output. **Step 2** Examine the Uptime field in the **show ip eigrp neighbors** output. A continuously resetting uptime counter indicates that Hello packets from the neighboring router are arriving sporadically. **Step 3** Enable the **debug ip packet** and **debug eigrp packets** privileged EXEC commands. The former command indicates whether IP packets are being sent and received, and whether there are encapsulation problems. The latter command indicates whether Enhanced IGRP hello packets are being sent and received properly. (CAUTION: These **debug** commands can use considerable bandwidth. Do not enable them if your network is already heavily congested.) **Step 4** If one router appears to be sending IP and Enhanced IGRP packets correctly, but a connected router does not receive them, check the configuration of the connected router for access-lists that might be filtering out packets. Make certain these access lists are not filtering out Enhanced IGRP packets. **Step 5** In a Frame Relay or other WAN environment, be certain that static maps configured for the WAN protocol specify mapping for multicast and broadcast traffic. If they do not, Enhanced IGRP broadcast hello packets will be dropped. For more troubleshooting procedures for WAN environments, see the "Troubleshooting WAN Connectivity" chapter. **Step 6** Issue the **show interfaces** EXEC command and make sure the interface and line protocol are up. Look for drops, input errors, bad packets, high queue counts, and other indicators of interface problems. For information on troubleshooting hardware problems, see the chapters "Router Startup Problems" and "Troubleshooting Serial Line Problems."
Routes are not being redistributed between two Enhanced IGRP autonomous systems.	**Step 1** Issue the **write terminal** privileged EXEC command. Look for **router eigrp** global configuration commands that indicate different autonomous systems. **Step 2** Route redistribution must be explicitly configured to occur between two different autonomous systems. Examine the configuration to see if the **redistribute** router configuration command is enabled. If it is not, you must enable redistribution between the two autonomous systems. Use the **redistribute eigrp** router configuration command to allow routes to be redistributed between two autonomous systems. NOTE: You do not need to configure **default-metric** commands in a strictly Enhanced IGRP network.

Possible Causes	Suggested Actions
Hello interval or hold time value mismatch	**Step 1** Use the **write terminal** privileged EXEC command on all routers in the network. Look for **ip hello-interval eigrp** and **ip hold-time eigrp** interface configuration command entries. The values configured by these commands should be the same for all IP routers on the network. At the very least, backbone routers should be configured with the same hello interval and hold time values. **Step 2** If there are routers with conflicting hello interval or hold time values, reconfigure them to bring them into conformance with the rest of the routers on the network. These values can be returned to their defaults with the **no ip hello-interval eigrp** and the **no ip hold-time interval eigrp** interface configuration commands.

Enhanced IGRP Router Stuck in Active Mode

Symptom: An IP Enhanced IGRP router is stuck in Active mode. An Enhanced IGRP router can be in either Passive or Active mode. A router is Passive for Network A when it has an established path to Network A in its routing table.

If the Enhanced IGRP router loses the connection to Network A, it becomes Active for that network. The router sends out queries to all of its neighbors in order to find a new route to Network A. The router remains in Active mode until it has either received replies from *all* of its neighbors or until the active timer, which determines the maximum period of time a router will stay Active, has expired.

If the router receives a reply from each of its neighbors, it computes the new next hop to Network A and becomes Passive for that network. However, if the active timer expires, the router removes from its neighbor table any neighbors that did not reply, again enters Active mode, and issues a "Stuck-in-Active" message to the console:

```
%DUAL-3-SIA: Route 198.169.52.51 Stuck-in-Active
```

Note The occasional appearance of these messages is *not* cause for concern. This is simply the manner in which an Enhanced IGRP router recovers if it does not receive replies to its queries from all of its neighbors. However, if these error messages occur frequently, the problem should be investigated.

Table 11-22 describes possible causes and suggested actions when an IP Enhanced IGRP router is stuck in Active mode.

Table 11-22 TCP/IP: Enhanced IGRP Router Stuck in Active Mode

Possible Causes	Suggested Actions
Active timer value is misconfigured	**Step 1** The active timer determines the maximum period of time that an Enhanced IGRP router will wait for replies to its queries. If the active timer value is set too low, there might not be enough time for all of the neighboring routers to send their replies to the Active router.
	Step 2 Check the configuration of each Enhanced IGRP router using the **write terminal** privileged EXEC command. Look for the **timers active-time** router configuration command associated with the **router eigrp** global configuration command.
	Step 3 The value set by the **timers active-time** command should be consistent among routers in the same autonomous system. We strongly recommend configuring a value of 3 (3 minutes, which is the default value) to allow all Enhanced IGRP neighbors to reply to queries.

Possible Causes	Suggested Actions
Interface or other hardware problem	**Step 1** If queries and replies are not sent and received properly, the active timer will time out and cause the router to issue an error message. Issue the **show ip eigrp neighbors** EXEC command and examine the Uptime and Q Cnt (queue count) fields in the output. If the uptime counter is continually resetting or if the queue count is consistently high, there might be a problem with hardware. **Step 2** Determine where the problem is occurring by looking at the output of the stuck in Active error message, which will indicate the IP address of the problematic node. **Step 3** Make sure the suspect router is still functional. Check the interfaces on the suspect router. Make sure the interface and line protocol are up and determine whether the interface is dropping packets. For more information on troubleshooting hardware, see the "Troubleshooting Router Startup Problems" and the "Troubleshooting Serial Line Problems" chapters. **Step 4** Make sure the suspect router has not had its configuration changed in a manner that could effect the convergence of the Enhanced IGRP routing protocol. Static routes, for example, can cause problems. **Step 5** Try jumpstarting the Enhanced IGRP router using the **clear ip eigrp neighbors** privileged EXEC command. This causes the router to clear its neighbor table, enter Active mode, and attempt to reaquire its neighbor information.
Flapping route	**Step 1** If there is a flapping serial route (caused by heavy traffic load), queries and replies might not be forwarded reliably. Route flapping caused by heavy traffic on a serial link can cause queries and replies to be lost, resulting in the active timer timing out. **Step 2** Take steps to increase the bandwidth of the link.

CHAPTER 12

Troubleshooting WAN Connectivity

This chapter presents symptoms and problems associated with wide-area network (WAN) connectivity.

This chapter consists of the following sections:

- X.25 WAN Router Initial Installation Scenario
- Using the show interfaces Command in an X.25 WAN Environment
- WAN and Serial Line Connectivity Symptoms

Each symptom module is divided into the following sections:

- Symptom statement—A specific symptom associated with WAN connectivity
- Possible causes and suggested actions—For each symptom, a table of possible symptom causes and suggested actions for resolving each cause

X.25 WAN Router Initial Installation Scenario

A common problem when bringing new internetworking nodes online is that systems on one side of the new node often are unable to communicate with systems on the other side. The problem scenario that follows explores this kind of situation in the context of a private X.25 WAN. In this case, several problems are uncovered during troubleshooting before a final resolution is achieved.

Symptoms

No traffic of any kind can pass through a newly installed router used to interconnect an Ethernet-based network segment with a private X.25 WAN. Local-area networks (LANs) previously interconnected with the X.25 WAN continue to communicate without disruption of service. However, users trying to make connections cannot get through to resources on the new segment.

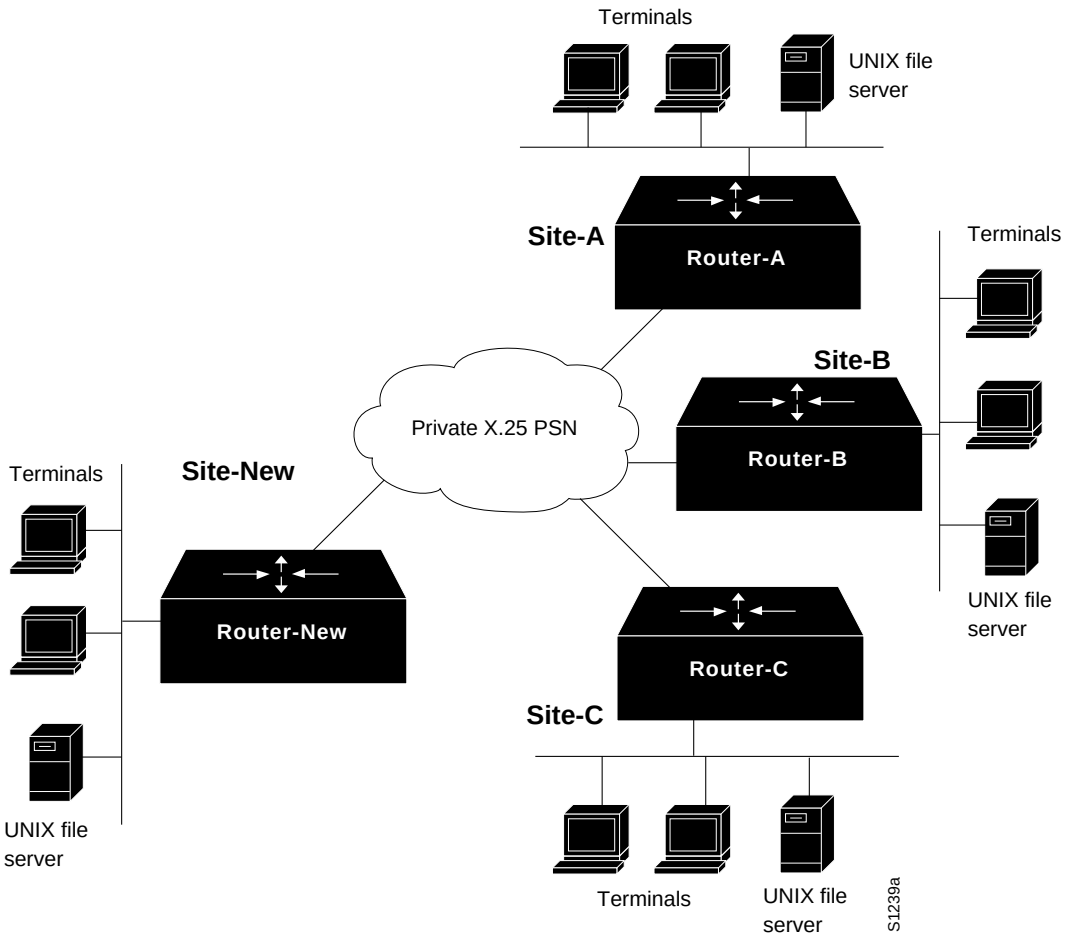
Environment Description

Figure 12-1 illustrates a map of an X.25 WAN. The following list summarizes relevant elements of this internetworking environment:

- WAN service is provided to geographically separated networks via a private X.25 packet-switching network.
- Three routers (Router-A, Router-B, and Router-C) provide WAN interconnection for hosts and users at three sites (Site-A, Site-B, and Site-C).

- A fourth router (Router-New) has been added to provide WAN interconnection service between a fourth location (Site-New) and the other three sites.
- All four sites are connected to the X.25 network via a fractional T1 service providing 56 kbps of bandwidth. The routers attach to a Channel Service Unit (CSU) or Data Service Unit (DSU) with an RS-449 cable.
- The LANs are all IEEE 802.3 Ethernets.
- The only network layer protocol running in this network is IP; the network uses the Interior Gateway Routing Protocol (IGRP) to route traffic among IP subnets, with traffic routed over the X.25 links using static address mapping.
- The network applications running over the WAN are limited to file transfer, mail, and virtual terminal connections.

Figure 12-1 X.25 WAN Connectivity Scenario Map



Diagnosing and Isolating Problem Causes

Given this situation, the following problems are the best candidates for interconnection failure:

- Cabling problem to the switch or to the LAN
- Wrong applique (must be data terminal equipment [DTE] for CSU/DSU connectivity)
- Router hardware problem
- Disabled port on the X.25 switch
- Bad T1 digital link
- Mismatched Ethernet version configurations
- Misconfigured hosts
- Misconfigured router

Next, eliminate each potential cause as a problem source and then test the network to determine whether it is operational. The following discussion works through the problem isolation process.

Isolating Serial Hardware and Media Problems

The following procedure illustrates the process of isolating hardware-related problems:

Step 1 Use the **show version** EXEC command to determine the condition of the router. Figure 12-2 illustrates the typical output that the system returns when interfaces are minimally operational, and the system can communicate with them. In this case, the interface of interest is associated with an MCI controller.

Figure 12-2 show version Command Output

```
Cisco Internetwork Operating System Software
IOS (tm) GS Software (GS3), Version 10.2(2), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1994 by cisco Systems, Inc.
Compiled Thu 15-Dec-94 15:39 by kmac
Image text-base: 0x00001000, data-base: 0x003BCF00

ROM: System Bootstrap, Version 4.6(5), SOFTWARE

depechemode uptime is 2 minutes
System restarted by reload
System image file is "gs3-k.102-2", booted via tftp from 171.69.1.129

CSC4 (68040) processor with 16384K bytes of memory.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
Bridging software.
2 MCI controllers (4 Ethernet, 4 Serial).
4 Ethernet/IEEE 802.3 interfaces.
4 Serial network interfaces.
32K bytes of non-volatile configuration memory.

Configuration register is 0x0
```

S3308

Step 2 In addition to the basic information provided in the **show version** output, use the **show controllers** EXEC command to examine the types of appliques on a router and the status of the appliques. Figure 12-3 illustrates an example output of the **show controllers mci** EXEC command. In this case, the environment requires a DTE applique to attach the router to a CSU/DSU device. In contrast, a data circuit-terminating equipment (DCE) applique typically would be required if the router were connecting directly to a host (DTE interface). Figure 12-4 illustrates an example output of the **show controllers cbus** (Cisco 7000) EXEC command. Figure 12-5 illustrates an example output of the **show controllers** EXEC command (Cisco 2500, Cisco 4000).

Figure 12-3 show controllers mci Command Output

```
MCI 1, controller type 1.1, microcode version 1.8
  128 Kbytes of main memory, 4 Kbytes cache memory
16 system TX buffers, largest buffer size 1520
  Restarts: 0 line down, 0 hung output, 0 controller error
  Interface 0 is Ethernet0, station address 0000.0c00.2be9
    22 total RX buffers, 9 buffer TX queue limit, buffer size 1520
    Transmitter delay is 0 microseconds
  Interface 1 is Serial0, electrical interface is RS-449 DTE
    22 total RX buffers, 9 buffer TX queue limit, buffer size 1520
    Transmitter delay is 0 microseconds
    High speed synchronous serial interface
  Interface 3 is Serial1, electrical interface is RS-449 DTE
    22 total RX buffers, 9 buffer TX queue limit, buffer size 1520
    Transmitter delay is 0 microseconds
    High speed synchronous serial interface
```

S2425

Figure 12-4 Show controllers cbus Command Output

```
Harold>show controllers cbus
Switch Processor 5, hardware version 11.1, microcode version 10.7
Microcode loaded from system
512 Kbytes of main memory, 128 Kbytes cache memory
4 256 byte buffers, 4 1024 byte buffers, 312 1520 byte buffers
1024 byte system buffer
Restarts: 0 line down, 0 hung output, 0 controller error
FSIP 0, hardware version 1.0, microcode version 175.0
Microcode loaded from system
Interface 0 - Serial 0/0, electrical interface is Universal (cable unattached)
22 buffer RX queue threshold, 23 buffer TX queue limit, buffer size 1520
TX queue length is 0
ift 0001, rql 12, tq 0000 0000, tql 23
Transmitter delay is 0 microseconds
Interface 1 - Serial 0/1, electrical interface is Universal (cable unattached)
22 buffer RX queue threshold, 23 buffer TX queue limit, buffer size 1520
TX queue length is 0
ift 0001, rql 12, tq 0000 0000, tql 23
Transmitter delay is 0 microseconds
Interface 2 - Serial 0/2, electrical interface is Universal (cable unattached)
22 buffer RX queue threshold, 23 buffer TX queue limit, buffer size 1520
TX queue length is 0
ift 0001, rql 12, tq 0000 0000, tql 23
Transmitter delay is 0 microseconds
Interface 3 - Serial 0/3, electrical interface is Universal (cable unattached)
22 buffer RX queue threshold, 23 buffer TX queue limit, buffer size 1520
TX queue length is 0
ift 0001, rql 12, tq 0000 0000, tql 23
Transmitter delay is 0 microseconds
```

S3395

Figure 12-5 Show Controllers Command Output (Cisco 2500, Cisco 4000)

```
Maude>show controllers
BRI unit 0
D Chan Info:
Layer 1 is DEACTIVATED

[. . .]
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns

B1 Chan Info:
Layer 1 is DEACTIVATED

[. . .]
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns

B2 Chan Info:

[. . .]
LANCE unit 0, idb 0x9515C, ds 0x96F00, regaddr = 0x2130000, reset_mask 0x2
IB at 0x40163F4: mode=0x0000, mcfilter 0000/0000/0000/0000
station address 0000.0c0a.28a7  default station address 0000.0c0a.28a7
buffer size 1524

[. . .]
0 missed datagrams, 0 overruns, 0 late collisions, 0 lost carrier events
0 transmitter underruns, 0 excessive collisions,  0 tdr, 0 babbles
0 memory errors, 0 spurious initialization done interrupts
0 no enp status, 0 buffer errors, 0 overflow errors
0 one_col, 0 more_col, 3 deferred, 0 tx_buff
0 throttled, 0 enabled
Lance csr0 = 0x73

HD unit 0, idb = 0x98D28, driver structure at 0x9AAD0
buffer size 1524  HD unit 0, RS-232 DTE cable

[. . .]
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns

HD unit 1, idb = 0x9C1B8, driver structure at 0x9DF60
buffer size 1524  HD unit 1, No DCE cable

[. . .]
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns
```

S3396

Step 3 Next, determine whether the interface is operational using the **show interfaces serial** EXEC command. Figure 12-6 illustrates the output from this command, the first line of which indicates that the serial interface and line protocol are down. These symptoms suggest a router hardware problem or a cabling problem. If the output specifies the line is down, the most likely cause is no Carrier Detect. In new installations, a cabling error is most likely. However, you should check both possibilities.

If the command output indicates that line is up and protocol is down, the likely causes are either that the switch is down, or the device is operating in the correct mode. For example, the device might be operating as an X.25-DCE when it should be operating as an X.25. Consult with your X.25 provider to learn whether the device should be operating as X.25-DCE or X.25 DTE.

Note In general, when using X.25, you cannot ping your own interface.

Figure 12-6 show interfaces serial Command Output Indicating a Possible Wrong Cable or Disabled CD

```
Serial0 is down, line protocol is down
  Hardware is MCI Serial
  Internet address is 131.63.125.10, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation X25, loopback not set
  LAPB DTE, state SABMSENT, modulo 8, k 7, N1 12048, N2 20
      T1 3000, interface outage (partial T3) 0, T4 0
      VS 0, VR 0, Remote VR 0, Retransmissions 0
      IFRAMEs 0/0 RNRs 0/0 REJs 0/0 SABM/Es 35/1 FRMRs 0/0 DISCs 0/0
  X25 DTE, address 408026201500, state R1, modulo 8, timer 0
      Defaults: cisco encapsulation, idle 0, nvc 1
        input/output window sizes 2/2, packet sizes 128/128
      Timers: T20 180, T21 200, T22 180, T23 180, TH 0
      Channels: Incoming-only none, Two-way 1-1024, Outgoing-only none
      RESTARTs 0/0 CALLs 0+0/0+0/0+0 DIAGs 0/0
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     1 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 1 abort
     35 packets output, 152 bytes, 0 underruns
     0 output errors, 0 collisions, 39 interface resets, 0 restarts
     1 carrier transitions
```

S3306

Step 4 The next step is to check the hardware. Specific tests to determine whether the hardware is operating normally depend on the system type. For instance, you would inspect the applique LEDs on an AGS+, but with an IGS, you would attach a breakout box to the serial port and check the breakout box status LEDs. For other devices, verify that the Carrier Detect is functioning by using the **show interface** command.

For general information about interpreting hardware LEDs and other diagnostics, refer to the "Troubleshooting Router Startup Problems" chapter. For specific information, refer to your hardware installation and maintenance documentation.

In this case, assume that the router hardware is operational, but that the transmit clock (obtained from the CSU/DSU) is not active. The cable is the most likely problem candidate.

Step 5 To determine whether it is the cable from the modem to the router or from the modem to the switch, configure the CSU/DSU to operate in local loop mode. This mode terminates use of the line clock (from the T1 service) and forces the CSU/DSU to use the local clock.

Note A loopback test should be performed using HDLC mode. X.25 does not support loopbacks.

Step 6 Next, use the **show interfaces serial** EXEC command to inspect the interface status. If the line remains down, a bad cable connection is extremely likely.

To remedy this problem, replace the cable and inspect the interface. Repeat the **show interfaces serial** command and assume that you see the output shown in Figure 12-7. The first line of the output indicates that the interface is operational and that the cable is working properly.

Figure 12-7 show interfaces serial Command Output Indicating That Link Is Up after a Cable Swap

```
Serial0 is up, line protocol is up
  Hardware is MCI Serial
  Internet address is 131.63.125.10, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation X25, loopback not set
  LAPB DTE, state CONNECT, modulo 8, k 7, N1 12048, N2 20
      T1 3000, interface outage (partial T3) 0, T4 0
      VS 1, VR 1, Remote VR 1, Retransmissions 0
      IFRAMEs 1/1 RNRs 0/0 REJs 0/0 SABM/Es 1/0 FRMRs 0/0 DISCs 0/0
  X25 DTE, address 170093, state R1, modulo 8, timer 0
      Defaults: cisco encapsulation, idle 0, nvc 1
        input/output window sizes 2/2, packet sizes 128/128
      Timers: T20 180, T21 200, T22 180, T23 180, TH 0
      Channels: Incoming-only none, Two-way 5-1024, Outgoing-only none
      RESTARTs 1/1 CALLs 0+0/0+0/0+0 DIAGs 0/0
  Last input 0:37:35, output 0:37:33, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     4 packets input, 13 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     4 packets output, 33 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets, 0 restarts
     1 carrier transitions                                          S3307
```

For more information about troubleshooting serial connections, see the "Troubleshooting Serial Line Problems" chapter.

Isolating Interface, LAN, and Local Host Configuration Problems

At this point, hardware problems associated with the serial connection to the X.25 WAN have been eliminated; however, traffic is still unable to get through Router-New.

Use the following procedure to determine if there is a problem with the LAN interface, the LAN in general, or network hosts:

Step 1 First determine the status of the LAN interface, the LAN media, and the resources on the LAN. Use the **show interfaces** command to inspect the condition of the interface and determine whether it is communicating with devices on the Ethernet. Figure 12-8 illustrates the output from the **show interfaces ethernet** EXEC command. In this case, the interface is alive and properly connected.

Figure 12-8 show interfaces ethernet Command Output Indicating an Operational Interface

```
Ethernet0 is up, line protocol is up
  Hardware is MCI Ethernet, address is 0000.0c02.5f4b (bia 0000.0c02.5f4b)
  Internet address is 131.63.152.20, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 4:00:00
  Last input 0:00:03, output 0:00:03, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 2/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     774229 packets input, 130286376 bytes, 0 no buffer
     Received 515472 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     301232 packets output, 20716867 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets, 0 restarts
```

S3386

Step 2 The output in Figure 12-8 indicates that the interface is operational and sees traffic on the network. However, the output does not indicate whether the router is able to communicate with specific end nodes on the Ethernet or whether the host configuration allows the host to communicate with the router. To determine whether the host can reach the router, use the **ping** and **clear** commands to test connectivity with the UNIX end system.

First, use the **ping** privileged EXEC command to verify that the router can communicate with each host on the local Ethernet. Figure 12-9 illustrates a successful acknowledgment (Echo Reply) to the Internet Control Message Protocol (ICMP) Echo Request (ping).

Figure 12-9 Successful First ping Communication from Router-New to Target Host

```
Router-New# ping 131.63.152.21
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.63.152.21, timeout is 2 seconds:
!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/3/4 ms
```

S2429

Step 3 Step 2 verified that the router is able to communicate with a specific host. However, to verify that the host configuration is correctly specified, **ping** the router from the host.

Step 4 Next, use the **clear arp-cache** privileged EXEC command on the router to clear the Address Resolution Protocol (ARP) cache, and **ping** from the router to the host again. Figure 12-10 illustrates the successful ping transmission and acknowledgment.

Figure 12-10 Transmission of Second ping Communication to Target Host after Clearing ARP Cache

```
Router-New# ping 131.63.152.21
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.63.152.21, timeout is 2 seconds:
.!!!!
Success rate is 80 percent, round-trip min/avg/max = 1/3/4 ms
```

S2430

Figure 12-11 and Figure 12-12 illustrate the effect of the ping exchange on the ARP cache of Router-New (*after* the **clear arp-cache** command was executed). Figure 12-11 illustrates that before the ping transmission, the ARP cache does not include the target host. After the ping, the ARP entry for the host is included in the ARP cache for Router-New. (See Figure 12-12.)

In the second ping exchange (refer to Figure 12-10), only 80 percent of the returns are successful. This is the *expected* behavior. Because the end system is not in the original ARP table, the first ping packet is dropped, and an ARP request is substituted instead. After the station replies, the subsequent pings work.

Figure 12-11 show arp Command Output before Running the ping Command

```
Router-New# show arp

Protocol  Address          Age (min)     Hardware Addr   Type      Interface
Internet  131.63.152.20           0     0000.0c00.f614  ARPA      Ethernet0
```

S2431

Figure 12-12 show arp Command Output after Running the ping Command

```
Router-New# show arp

Protocol  Address          Age (min)     Hardware Addr   Type      Interface
Internet  131.63.152.21           0     0000.0c00.4dbb  ARPA      Ethernet0
Internet  131.63.152.20           0     0000.0c00.f614  ARPA      Ethernet0
```

S2432

The success of the ping demonstrates that the host can reply to the router. All LAN-related and host configuration problems are now eliminated; however, traffic still is not traversing the router. It is time to examine the router's configuration.

Isolating Router Software Configuration Problems

After eliminating all serial hardware problems, LAN problems, and host configuration problems, a router configuration problem may exist. In fact, there may be more than one problem.

Use the following procedure to isolate router software configuration problems:

Step 1 Use the **debug x25 events** privileged EXEC command to enable X.25 debugging on the router. Given the situation, the router is likely to immediately report events. Connection attempts appear as *call* packets; communication problems can cause *clear* or *reset* packets for individual circuits or, in more severe cases, *restart* or *diagnostic* packets for the X.25 service. The clear, reset and restart packets commonly encode cause and diagnostic codes, and diagnostic packets contain a diagnostic code. See the *Debug Command Reference* for an explanation of these codes. *Call* and *call confirm* packets can encode user facility information, which can also be informative when troubleshooting.

Step 2 Compare the configuration files of the various routers in the WAN with the configuration file for Router-New.

There are a number of configurable X.25 parameters that must match those defined for the WAN connection. These key parameters, which you must get from your X.25 network provider, follow:

- X.121 address specification
- Default packet sizes
- Default window sizes
- Switched virtual circuit channel ranges.
- X.25 modulo
- X.25 DTE/DCE identity
- LAPB parameters

Note The LAPB parameters must match in order for the WAN connection to work, but the default values are commonly sufficient. These parameters are: LAPB window size (*k*), LAPB acknowledgment timer (*T1*), LAPB modulo and LAPB DTE/DCE identity. Similarly, in the postulated setup the X.25 DTE/DCE identity will be DTE, but in other configurations this parameter should be checked.

In this case, assume that the switched virtual circuit channel ranges are not correctly defined in the configuration for Router-New.

The values that define the outgoing-only range (LOC and HOC, the lowest and highest channel respectively), the two-way range (LTC and HTC) and the incoming-only range (LIC and HIC) are all set to the default in Router-New. However, the WAN requires that these be specifically configured. Because of this mismatch, the router is unable to complete any virtual circuits. In Software Release 9.1 and greater, you generally only need to set LTC and HTC.

Fixing these errors allows the router to successfully perform ICMP pings, but regular traffic is still not getting through.

Note The configuration requirement for the LTC in this case is driven by the specification of permanent virtual circuits (PVCs). The PVC channel specifications must be lower than any SVC range. The default is a two-way range between 1 and 1024, so the LTC value must be raised to define any PVCs.

Step 3 Use the **write terminal** privileged EXEC command to examine the configuration of the router. In this case, the **x25 map** command does not include the **broadcast** keyword. Because the IP internetwork uses IGRP (a dynamic routing protocol), the **broadcast** keyword is required. Figure 12-13 summarizes the changes made to the configuration file that finally allow traffic through the router.

If X.25 payload compression is used for encapsulation traffic, the two encapsulating routers must run Cisco Internetwork Operating System (Cisco IOS) Release 10.2 or later; this feature is not available in earlier versions and can cause problems if the two routers are not configured correctly. The two routers must agree to use X.25 payload compression, either by using a Call User Data (CUD) preamble when establishing an SVC or by configuring compression for both ends of a PVC. Because there is no standard for compressing X.25 data, this feature can only be used to encapsulate traffic between two Cisco routers.

Software releases prior to Cisco IOS Release 10.2 will not recognize the CUD of a received compression call and will, by default, clear the call. The call will be accepted, however, if the interface is configured with a default protocol (using the **x25 default** command) but no connectivity will result because neither of the two routers will understand the traffic received from the other. Similarly a PVC that is connected to a router that is compressing its encapsulation traffic will not do anything useful.

Cisco IOS Release 10.2 and later will recognize the CUD of a received call (so an interface that configures a default protocol will not accept an unusable call), but will only accept a compression call if the encapsulation map is configured for compression. Both routers must be configured for compression because the feature consumes significant memory and computational resources. An uncompressed call can, however, use a map configured for compression, so connectivity can be established by one station despite mismatched configurations.

In all cases, an encapsulation PVC must be correctly configured on both routers to establish connectivity, because there is no X.25 protocol procedure that can be used to identify the traffic carried.

Problem Solution Summary

Introducing new internetworking systems into LAN-to-WAN internetworks is not a simple matter. The key to resolving multilayered problems is to address each possible problem individually. In this case, multiple causes involved both media problems and software misconfigurations. Connectivity to Site-New was established after making the following changes:

- A bad cable was replaced with a new cable.
- The router configuration was modified to match the X.25 parameters defined for the WAN connection, specifically the SVC ranges.
- The **x25 map** command was modified to include the **broadcast** option required to handle dynamic routing over X.25.

Figure 12-13 show the final X.25 configuration that allows traffic to pass through the internetwork. Internetworking problems are rarely one-dimensional. Isolating a problem requires a certain amount of patience and a methodical approach. It is also important to note that subtle protocol variations can wreak havoc in networks if these variations are not fully accounted for during the initial configuration. Thus, it is critical to coordinate efforts with all responsible organizations—especially when third parties, such as WAN service vendors, are involved.

Figure 12-13 Complete X.25 Configuration Showing Changes Needed to Pass Traffic

```
interface ethernet 0
ip address 131.63.152.20 255.255.255.0
!
interface serial 0
ip address 131.63.125.10 255.255.255.0
encapsulation X25
x25 win 7
x25 wout 7
x25 ips 1024
x25 ops 1024
x25 address 408026201500
x25 ltc 4
x25 htc 127
x25 facility windowsize 7 7
x25 facility packetsize 1024 1024
x25 map IP 131.63.125.108 40803010123000 broadcast
x25 map IP 131.63.125.12 40802126001000 broadcast
x25 map IP 131.63.125.132 40802121203200 broadcast
x25 pvc 1 IP 131.63.125.77 44820635287300 broadcast
x25 idle 3
!
router igrp 109
network 131.63.0.0
!
!
ip name-server 255.255.255.255
snmp-server community
snmp-server community public RO
hostname Router-New
logging 129.14.87.76
scheduler-interval 1500
!
end
```

S3388

Using the show interfaces Command in an X.25 WAN Environment

Depending on the WAN encapsulation (such as X.25, Switched Multimegabit Data Service [SMDS]), or Frame Relay) that is being used, the **show interfaces serial** EXEC command provides specialized diagnostic information. This section examines the additional diagnostic information provided by the **show interfaces serial** EXEC command for troubleshooting X.25 WAN connections. For information about the output of the **show interfaces serial** EXEC command that is pertinent to SMDS and Frame Relay, see the *Router Products Configuration Guide* and *Router Products Command Reference* publications.

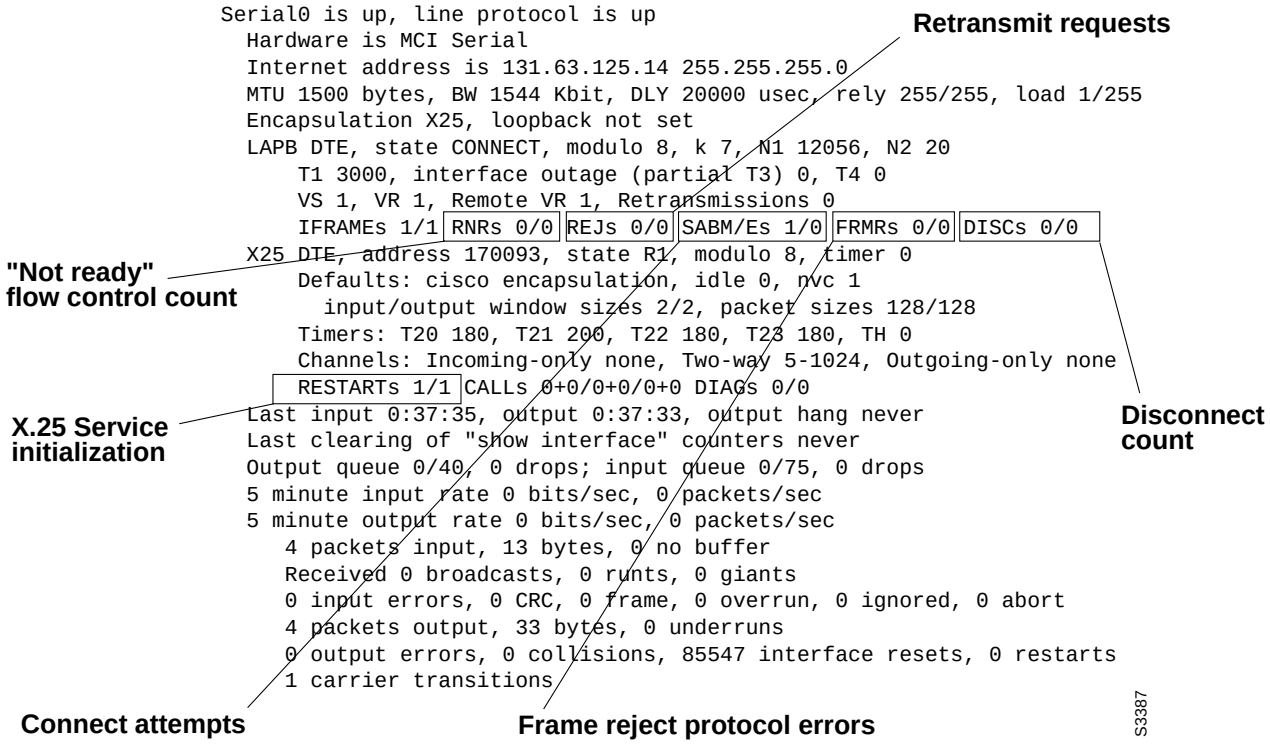
In addition to the general fields discussed in the section "Developing a Strategy for Isolating Problems" in the "Troubleshooting Overview" chapter, the **show interfaces serial** output for X.25 internetworks provides additional accounting information that can indicate serial problems. These fields provide the following information:

- Number of rejects (REJs)
- Number of Set Asynchronous Balance Mode requests (SABMs)
- Number of Receiver Not Ready (RNR) events
- Number of protocol frame errors (FRMRs)
- Number of restarts (RESTARTs)
- Number of disconnects (DISCs)

All but the X.25 restart count are LAPB events; because X.25 requires a stable data link, LAPB problems will commonly cause an X.25 restart event that implicitly clears all virtual connections. If unexplained X.25 restarts occur, examine the underlying LAPB connection for problems.

Figure 12-14 highlights each field in the X.25 version of output from the **show interfaces serial** EXEC command.

Figure 12-14 Output from the X.25 Version of the show interfaces serial Command



Note If any of these fields are increasing and represent more than 0.5 percent of the number of information frames (IFRAMEs), there is probably a problem somewhere in the X.25 network. There should always be at least one SABM; however, if there are more than 10, the packet switch probably is not responding.

Symptom Recorded REJs, RNRs, FRMRs, RESTARTs, or DISCs in excess of 0.5 percent of IFRAMEs

Possible Cause The following causes can result in this symptom:

- Faulty switch
- Bad cabling
- Bad CSU/DSU
- Failed router hardware
- Misconfigured protocol parameters

Recommended Action The following steps are suggested when this symptom is encountered:

Step 1 Enable the **debug lapb** privileged EXEC command. If the LAPB protocol seems stable, disable the **debug lapb** command and enable the **debug x25 events** privileged EXEC command.

Step 2 Look for restarts or RESTART messages or CLEAR REQUESTS with non-zero cause codes.

Step 3 To interpret the X.25 cause and diagnostic codes provided by the output, see the "X.25 Cause and Diagnostic Codes" appendix in the *Debug Command Reference* manual.

Step 4 Verify that the critical LAPB parameters (modulo, T1, N1, N2 and k) and the critical X.25 parameters (modulo, X.121 address, SVC ranges, default window and packet sizes and PVC definitions) match the parameters required by the WAN connection.

Step 5 Use a serial analyzer to check the hardware at both ends of the link and to determine whether the SABMs are being responded to with unnumbered acknowledge (UA) packets, or to examine any other anomalous protocol event.

Step 6 If the analyzer cannot identify any external problems, check the router hardware.

Step 7 Swap faulty equipment as necessary.

WAN and Serial Line Connectivity Symptoms

The symptom modules in this section pertain to serial and WAN problems. Unless otherwise indicated, each module is presented as a set of general problems applying to all WAN types (such as X.25, point-to-point serial, SMDS, and Frame Relay). Any special considerations for a specific network type are noted.

WAN connectivity symptoms are discussed in the following sections:

- Intermittent WAN Connectivity
- WAN Connections Fail as Load Increases
- WAN Connections Fail at a Particular Time of Day
- Connections Fail after a Period of Normal Operation
- WAN Users Cannot Connect to Resources over a New HDLC Link
- WAN Users Cannot Connect to Resources over a New X.25 WAN Link
- WAN Users Cannot Connect to Resources over a New Frame Relay Link
- WAN Users Cannot Connect to Resources over a New SMDS Link
- Some Users Cannot Connect to Resources over a WAN

Intermittent WAN Connectivity

Symptom: Connections can be made between some nodes, while other nodes cannot connect.
Table 12-1 outlines possible causes and suggested actions when intermittent connectivity in serial and WAN interconnections is experienced.

Table 12-1 WAN: Intermittent WAN Connectivity

Possible Causes	Suggested Action	
Faulty interface card or cable	**Step 1**	Use the **show interfaces serial** and **show controllers** EXEC commands to check the status of the interface.
	Step 2	Look for a line down condition and version level.
	Step 3	Upgrade microcode (firmware) if the current code is older than Version 1.7.
	Step 4	Swap any nonoperational cards or cables.
CSU/DSUfailure	**Step 1**	Use the **show interfaces serial** EXEC command to check for input errors.
	Step 2	Replace the modem.
	Step 3	Observe behavior after the modem is changed.
Timing problem	**Step 1**	Check the CSU/DSU configuration to verify that SCTE/Terminal timing is enabled; enable serial clock transmit external (SCTE)/terminal timing if it is not already enabled.
	Step 2	If the CSU/DSU is properly configured, or if intermittent connectivity persists after enabling SCTE/Terminal timing on the CSU/DSU, verify that the correct network entity is generating the system clock; reconfigure nodes and modems if clocking is not properly configured.
	Step 3	If intermittent problems persist, check cable length; if the cable is longer than 25 feet (7.62 meters), you might need to invert the clock on the MCI/SCI.
	Step 4	Invert the data on the DSU/CSU on both ends of the connection.
	Step 5	Lower the line speed to 56 KB or derivative of that speed.
	Step 6	Check for possible routing loops, or misconfigurations of routing protocols.
Network generating invalid PRs (X.25)	**Step 1**	Verify that the interface default flow control values match the values defined for the switch.
	Step 2	Run diagnostics at the switch.
	Step 3	Swap switch hardware if necessary.

Possible Causes	Suggested Action
Router generating invalid PRs (X.25)	**Step 1** Verify that the interface default flow control values match the values defined for the WAN connection. **Step 2** Enable the **debug x25 events** EXEC command and examine the cause and diagnostic codes. For more information, see the "X.25 Cause and Diagnostic Codes" appendix in the *Debug Command Reference* manual.
Serial line congestion	**Step 1** Adjust the hold queue. **Step 2** Tune buffer sizes. For more information, see the section "Adjusting Buffers to Ease Overutilized Serial Links" in the "Troubleshooting Serial Line Problems" chapter. **Step 3** Apply a priority list. **Step 4** Reduce broadcast traffic.

WAN Connections Fail as Load Increases

Symptom: Users continually complain about lost connections at peak periods. One example of this problem is in an environment that features bridged DEC local-area transport (LAT) traffic and multiple routed protocols. Data entry input from users (or other application requests) might be getting buffered at the end of an already long input queue; eventually one end of the connection times out. Table 12-2 outlines possible causes and suggested actions when WAN connections fail as load increases.

Table 12-2 WAN: Connections Fail as Load Increases

Possible Causes	Suggested Actions
Noisy serial line	**Step 1** Determine whether input errors are increasing.
	Step 2 If input errors appear, diagnose the serial line as described in the section “Special Serial Line Tests” in the “Troubleshooting Serial Line Problems” chapter.
Overutilized serial line	**Step 1** If input errors do not appear, there is a congestion problem.
	Step 2 Increase the bandwidth.
	Step 3 Include an appropriate priority queuing configuration statement.
	Step 4 Tune buffer sizes. For more information, see the section “Adjusting Buffers to Ease Overutilized Serial Links” in the “Troubleshooting Serial Line Problems” chapter.
	Step 5 Reduce unnecessary broadcast traffic.

WAN Connections Fail at a Particular Time of Day

Symptom: This symptom is generally an example of connections dying under load. In this case, traffic on a serial link approaches saturation at specific times during the day: for instance, around 8:30 a.m., noon, and 5:30 p.m. The result is a lost connections or an inability to make connections. Table 12-3 outlines possible causes and suggested actions when connections fail at a particular time of day.

Table 12-3 WAN: Connections Fail at a Particular Time of Day

Possible Causes	Suggested Action
Overutilized bandwidth	**Step 1** Check the applications that are being run. Look for very large file transfers scheduled at particular times of the day. **Step 2** If you find large file transfers that are scheduled for the time of day at which saturation occurs, set up a priority queue based on packet size to allow higher amounts of small-packet traffic. (The protocol must support flow control.) **Step 3** Rearrange the timing of file transfers so that links are not overused during normal business hours. **Step 4** Add bandwidth and consider dial backup over the new link for applications that are taking excessive bandwidth on existing links.
Unshielded cable runs are too close to electromagnetic interference (EMI) sources	**Step 1** Use the **show interfaces serial** EXEC command to look for input errors. **Step 2** If loading is not the problem, and input errors are being registered, inspect cable runs for proximity to EMI sources. **Step 3** Relocate or shield cables if they are found to be near EMI sources.

Connections Fail after a Period of Normal Operation

Symptom: Connections suddenly fail and cannot be restored after relatively normal, error-free operation. Table 12-4 outlines possible causes and suggested actions when connections fail suddenly after a period of normal operation.

Table 12-4 WAN: Connections Fail after Normal Operation

Possible Causes	Suggested Action
Hardware failure somewhere in the serial link	**Step 1** Use the **show interfaces serial** EXEC command to determine whether the link is down. **Step 2** If the link is down, refer to the section "CSU and DSU Loopback Tests" in the "Troubleshooting Serial Line Problems" chapter or use a serial analyzer to troubleshoot the failure.
Routing tables are incorrect	**Step 1** If the link is up, use the appropriate **show** *protocol* **route** EXEC command. **Step 2** Determine whether routes are correct; if not, look for the source of bad routes, such as a flapping link, a backdoor bridge between the routed segments, or an incorrect configuration of route redistribution between routing protocols.
Buffer misses or other software problem	**Step 1** If the routing table is correct and the link is up, use the **show buffers** EXEC command to evaluate buffer status. **Step 2** Refer to the section "Adjusting Buffers to Ease Overutilized Serial Links," in the "Troubleshooting Serial Line Problems" chapter. Modify buffers as necessary to prevent dropped connections. **Step 3** Contact your technical support representative if all actions fail to resolve the problem.

WAN Users Cannot Connect to Resources over a New HDLC Link

Symptom: Traffic does not pass through a newly installed router interconnecting broadcast networks via a High-Level Data Link Control (HDLC) point-to-point link. Table 12-5 outlines possible causes and suggested actions when users cannot connect to resources over a new HDLC link.

Table 12-5 WAN: Users Cannot Connect to Resources over a New HDLC Link

Possible Causes	Suggested Action
Link is down	**Step 1** Use **the show interfaces serial** EXEC command to determine whether the link is down. **Step 2** If the link is down, refer to the "CSU and DSU Loopback Tests" section in the "Troubleshooting Serial Line Problems" chapter or use a serial analyzer to troubleshoot the failure.
Keepalive packets not being received	**Step 1** Use the **debug serial interface** privileged EXEC command to determine the status of keepalive packets. **Step 2** If keepalive packets are not incrementing, refer to the section "CSU and DSU Loopback Tests" in the "Troubleshooting Serial Line Problems" chapter.

WAN Users Cannot Connect to Resources over a New X.25 WAN Link

Symptom: Traffic does not pass through a newly installed router interconnecting broadcast networks via an X.25 WAN. Look for problems associated with the new installation, especially when LANs previously interconnected via the WAN continue to communicate with no disruption of service. Table 12-6 outlines possible causes and suggested actions when users cannot connect to resources over a new X.25 link.

Note The process of problem isolation for Defense Data Network (DDN) X.25 networks is essentially the same, except for the DDN-defined dynamic mapping capability.

Table 12-6 WAN: Users Cannot Connect to Resources over New X.25 WAN Link

Possible Causes	Suggested Actions
Link is down	**Step 1** Use the **show interfaces serial** EXEC command to determine whether the link is down. **Step 2** If the link is down, refer to the "CSU and DSU Loopback Tests" section in the "Troubleshooting Serial Line Problems" chapter.
Switch is misconfigured	**Step 1** Check the configuration of the switch; look for bad address specifications, incorrect VC parameter settings, or other configuration errors. **Step 2** If you find errors, modify the configuration and use the **show interfaces serial** EXEC command to check the status of the line.
Misconfigured router, incorrect cabling, or bad router hardware	**Step 1** Use the **show interfaces serial** EXEC command to determine the status of the interface. If the interface is up, but the line protocol is down, check the Link Access Procedure, Balanced (LAPB) state. **Step 2** If the LAPB state is *not* CONNECT, attach a serial analyzer. **Step 3** Use the serial analyzer to look for UA packets sent in reply to SABMs. If UAs are not being sent, one of the possible causes described in this table is the likely problem. **Step 4** Reconfigure equipment or replace equipment as required. **Step 5** If the **show interfaces serial** EXEC command indicates that the interface and line protocol are up, but no connections can be made, use the **write terminal** privileged EXEC command to check the router configuration. **Step 6** Look for **x25 map** interface configuration commands and ensure that the correct addresses are specified. **Step 7** If dynamic routing is being used in the network, verify that the **broadcast** keyword is included in the **x25 map** command. **Step 8** Ensure that all router configuration options match switch settings. **Step 9** Modify router configuration as needed to resume operation.

WAN Users Cannot Connect to Resources over a New Frame Relay Link

Symptom: Traffic does not pass through a newly installed router interconnecting broadcast networks via a Frame Relay WAN. Look for problems associated with the new installation, especially when LANs previously interconnected via the WAN continue to communicate with no disruption of service. Table 12-7 outlines possible causes and suggested actions when users cannot connect to resources over a new Frame Relay link.

Table 12-7 WAN: Users Cannot Connect to Resources over New Frame Relay Link

Possible Causes	Suggested Actions
Frame Relay switch is misconfigured (dynamic Data Link Connection Identifier [DLCI] and protocol address mapping)	**Step 1** Use the **show interfaces serial** EXEC command to determine the status of the line and to determine whether Local Management Interface (LMI) updates are being received. **Step 2** If LMI updates have not been received, enable the **debug frame-relay lmi** privileged EXEC command; look for LMI information to determine whether the switch and router are sending and receiving LMI packets. **Step 3** Confirm that the DLCI numbers provided by your vendor match the PVC output resulting from the **debug frame-relay lmi** privileged EXEC command. **Step 4** Check the configuration of the Frame Relay switch; make sure LMI matches the router.
Router is misconfigured (wrong keepalive setting)	**Step 1** Use the **write terminal** privileged EXEC command to check for LMI keepalive setting (dynamic mode). Ten seconds is the default (not displayed). **Step 2** Compare LMI keepalive setting with the Frame Relay switch setting. The LMI keepalive setting should be equal to or less than the Frame Relay switch. **Step 3** Make sure that the router speed does not match the switch, which is normally set 2–5 seconds slower than the router.
Misconfigured access list	**Step 1** Evaluate access lists at both ends of the connection. **Step 2** Make sure there are no inadvertent access denials. **Step 3** Modify access lists as needed or remove to test connectivity.
Cabling problem	**Step 1** Use the **show interfaces serial** EXEC command to determine the status of the interface. **Step 2** Check cabling. Refer to the "Developing a Strategy for Isolating Problems" section in the "Troubleshooting Overview" chapter. **Step 3** Replace any incorrectly configured or failed cables.
Failed hardware	**Step 1** Use the **show interfaces serial** command to determine the status of the interface. Frame Relay does not support Loop Back, but if Local DSU is placed into Local Loopback, the input packets will equal output packets. These packets are the LMI updates the router sends out. **Step 2** Replace hardware as necessary.

Possible Causes	Suggested Actions
Router is misconfigured (dynamic DLCI and protocol address mapping)	**Step 1** Check the output of the **show interface serial** EXEC command to determine the status of the interface. **Step 2** Determine whether DLCI-to-protocol mapping is dynamic or static; set to the correct mode if it is not correct. **Step 3** If dynamic mapping is implemented and if the interface and line protocol are up, but no connections can be made, examine the output of the **show frame-relay map** EXEC command. **Step 4** Determine whether any of the far end networks have been learned by the local router. **Step 5** If far end networks have been learned and if the protocol supports ping, **ping** the nearest interface of the remote router to verify that you can reach that point. **Step 6** If the interface and line protocol are up, and you *cannot* ping, the Frame Relay network is probably misconfigured. **Step 7** If you can ping, **ping** through to the other side of the router, working out to end stations. **Step 8** Reconfigure equipment as necessary. (At the router, be sure that the remote DLCI number is mapped to the protocol address at the far end.) **Step 9** If the output of the **show frame-relay map** EXEC command indicates that no far end networks have been learned, enable the **debug frame-relay events** EXEC command and run the appropriate **show route** EXEC command. **Step 10** Identify the exchanges that are occurring between the router and the switch and determine whether any routing protocol information is being learned. **Step 11** Change the router configuration as necessary.
Router is misconfigured (static Frame Relay address mapping)	**Step 1** Use the **show interfaces serial** EXEC command to determine the status of the interface. **Step 2** Determine whether DLCI-to-protocol mapping is dynamic or static; set to correct mode if not correct. **Step 3** If the interface and line protocol are up and if static mapping is implemented, but no connections can be made, examine the output of the **show frame-relay map** EXEC command. **Step 4** The status should be active. If not, compare the configurations on the switch and the router and make sure they match. **Step 5** If the **show frame-relay map** EXEC command indicates that the status is active, examine the output of the **show route** EXEC command for the appropriate protocol to determine whether routing information is accumulating. Misconfigured access lists might be a cause. **Step 6** Make sure BROADCAST tag is set on your map statements if your are running a routing protocol. **Step 7** Double-check that the NETWORK ADDRESS and DLCI are set correctly in your configuration.

Note You cannot ping the local router's frame-relay interface unless a static map is configured to permit this action.

WAN Users Cannot Connect to Resources over a New SMDS Link

Symptom: No traffic of any kind is passing through a newly installed router interconnecting broadcast networks via an SMDS WAN link. Look for problems associated with the new installation, especially when LANs previously interconnected via the WAN continue to communicate without disrupted service.

If you are having difficulty establishing connections over an SMDS cloud, obtain the following information as a preliminary step before beginning the problem isolation process:

- Use the **show arp** EXEC command to determine whether any SMDS devices were detected on the switch.
- Use the **debug serial interface** privileged EXEC command to determine whether packets are being sent and received.
- Use the **debug serial packet** privileged EXEC command to obtain the entire SMDS header and payload data when SMDS packets are transmitted or received on an interface.
- Use the **debug arp** privileged EXEC command to determine other SMDS devices that are being detected on the switch.
- Use the **show smds traffic** EXEC to verify errors and packets transmitted and received.

Table 12-8 outlines possible causes and suggested actions when users cannot connect to resources over a new SMDS link.

Table 12-8 WAN: Users Cannot Connect to Resources over New SMDS Link

Possible Causes	Suggested Actions
SMDS switch is misconfigured	**Step 1** Check the router and switch configurations for an address mismatch. **Step 2** Make sure that the SMDS switch is configured for multicast or static mapping (depending on the intended network setup).
Router misconfigured (general SMDS)	**Step 1** Use the **write terminal** privileged EXEC command to evaluate the configuration of the router. **Step 2** Compare the configuration with requirements for the switch. Look for bad address specifications, an incorrect mode specification (multicast versus static), or a missing **encapsulation smds** interface configuration command. **Step 3** Modify the configuration as necessary to make the router match SMDS network requirements. Verify that SMDS DXI is enabled or disabled as required by the SDSU. In Cisco IOS Release 10.0 and later, SMDS DXI is enabled by default.

Possible Causes	Suggested Actions
Misconfigured SMDS interface or multicast addresses	**Step 1** Use the **show arp** EXEC command to determine what other devices, if any, have been detected on the switch. **Step 2** If none have been detected, make sure that the SMDS address specified in the **smds address** interface configuration command matches the address of the attached switch. **Step 3** Make sure that the SMDS multicast addresses specified in the **smds multicast** interface configuration command match the addresses configured on the switch. **Step 4** Make sure that the **smds enable-arp** interface configuration command is present so that higher layers learn about the router. **Step 5** Check the static maps configured on the router. To allow the SMDS software to translate a destination address into a proper SMDS address for outgoing packets, make sure that static maps are configured for all nonlearning protocols. **Step 6** If SMDS data is still not being received, even when packets are being sent, check all connections for physical connectivity. **Step 7** If the physical connections are operational, and packets still are not being received, check the SDSU configuration.
Router misconfigured (static SMDS address mapping)	**Step 1** Use the **show interfaces serial** EXEC command to determine the status of the interface. **Step 2** Use the **show smds map** EXEC command to determine whether the mapping mode is multicast or static; reconfigure the mode if it is incorrect. All network protocols, with the exception of IP and ISO Connectionless Network Service (CLNS), require static mapping from protocol addresses to SMDS addresses. **Step 3** If IP or ISO CLNS is being routed, check the multicast group specification. Make any necessary address changes. **Step 4** If static mapping is implemented, if the interface and line protocol are up, and if connections cannot be made, enable the **debug serial interface** privileged EXEC command. **Step 5** Based on the **debug** output, determine whether the correct destination address is being used. **Step 6** Make configuration changes as necessary to the mapping, mode, or encapsulation specification.
Misconfigured access list	**Step 1** See Table 12-7 for suggested actions.

Possible Causes	Suggested Actions
Cabling problem	**Step 1** Use the **show interfaces serial** EXEC command to determine the status of the interface. **Step 2** Check cabling. Refer to the sections “Using the show interfaces Command to Troubleshoot Serial Lines” and “Special Serial Line Tests” in the “Troubleshooting Serial Line Problems” chapter. **Step 3** Replace any incorrectly configured or failed cables.
Failed hardware	**Step 1** Use the **show interfaces serial** EXEC command to determine the status of the interface. To isolate specific problem equipment, perform loopback and ping tests as described in the section “CSU and DSU Loopback Tests,” and “Using Extended ping Tests to Troubleshoot Serial Lines” in the “Troubleshooting Serial Line Problems” chapter. **Step 2** Replace hardware as necessary.

Some Users Cannot Connect to Resources over a WAN

Symptom: Some users or applications are able to reach resources over a serial/WAN link through a router while other users cannot. Table 12-9 outlines possible causes and suggested actions when some users cannot connect to resources over a WAN.

Table 12-9 WAN: Some Users Cannot Connect to Resources over WAN

Possible Causes	Suggested Actions
Misconfigured access list	**Step 1** See Table 12-7 for suggested actions.
Host configuration is not set up to send ARPs	**Step 1** Verify that the host is configurated to send ARPs. **Step 2** Modify as necessary.
Host configuration points at wrong router	**Step 1** Check host configuration for default gateway specification. **Step 2** Modify host configuration as necessary.
Discontinuous subnet addressing (IP)	**Step 1** Check the network configuration for discontinuous network address space assignment. **Step 2** If you find discontinuous network address space assignments, use secondary IP addresses to accommodate physical discontinuity.

CHAPTER 13

Troubleshooting XNS Connectivity

This chapter presents protocol-related troubleshooting information for Xerox Network Systems (XNS) connectivity problems and consists of the following sections:

- XNS Network Server Connectivity Scenario
- XNS Internetworking Connectivity Symptoms

The symptom modules consist of the following sections:

- Symptom statement—A specific symptom associated with the XNS connectivity
- Possible causes and suggested actions—A table for each symptom containing possible causes for the symptom and suggested actions for resolving each cause.

XNS Network Server Connectivity Scenario

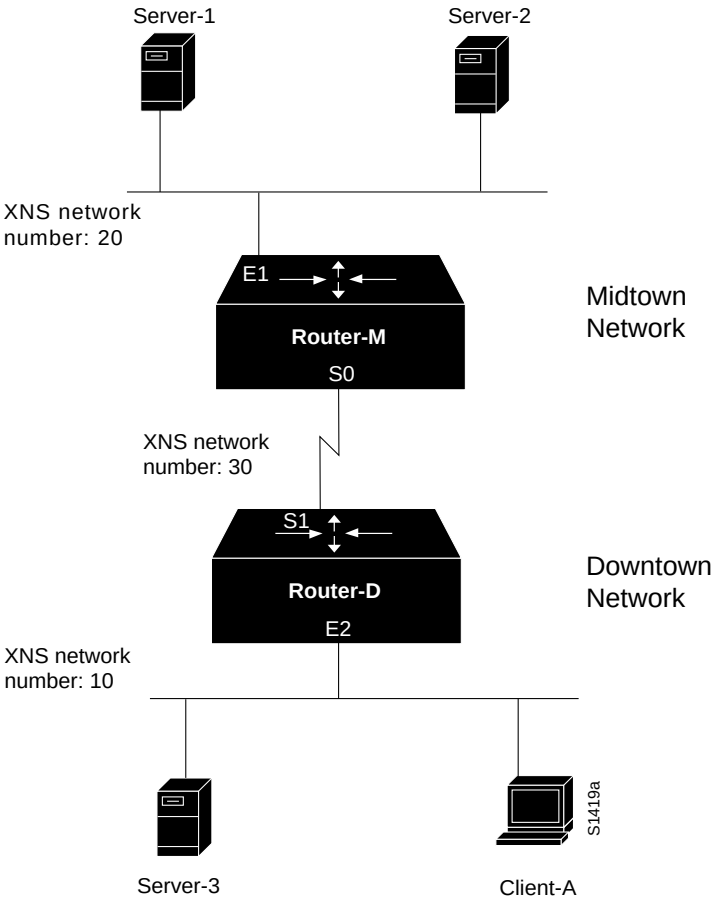
With the emergence of XNS as an important PC-based network operating environment, network administrators have had increasing requirements to interconnect and segment PC LANs running the XNS networking protocol. This scenario focuses on a variety of problems that can impair server access over a routed internetwork.

Symptoms

Figure 13-1 is a map of the XNS internetwork discussed in this case. It illustrates an interconnection between two sites over an arbitrary serial network. The symptom encountered in this scenario is that Client-A cannot access Server-1 and Server-2 on the other side of the serial link. However, Client-A can access Server-3 on the local wire.

Because no connections can be made over the serial link, it *initially* appears that there is a problem with traffic getting through the routers.

Figure 13-1 Initial XNS Connectivity Scenario Map



Environment Description

The relevant elements of the internetworking environment shown in Figure 13-1 can be summarized as follows:

- Remote service is provided to a cross-town campus via a point-to-point serial link.
- Two routers (Router-M and Router-D) interconnect the Midtown and Downtown networks. Routers are MGS routers configured to route XNS. The clients are IBM PCs and compatibles.
- LANs are Ethernets. The serial link is a dedicated T1 link (1.544 Mbps).
- Network applications are intended to run over the T1 line.

Diagnosing and Isolating Problem Causes

Given the situation, several problems could explain connectivity symptoms.

The following problems are likely candidates for the first symptom. (Client-A cannot access services on Server-1 and Server-2.)

- Client-A or target servers are not properly attached to their networks.
- XNS routing is not enabled on Router-D or on Router-M.

- Network numbers are misconfigured.
- Router interfaces are not up or operational.
- Access lists are misconfigured.
- Nonunique Media Access Control (MAC) addresses are in XNS routing configuration.
- XNS helper-addresses are incorrect or missing.
- XNS forward-protocol is incorrect or missing.

This list is loosely ordered according to a combination of two criteria: ease of problem determination and likelihood of being the *actual* problem.

In general, it is useful to eliminate the most likely problems first and then to tackle the more complex problems as necessary. The problem-solving process that follows illustrates this strategy.

After you determine a possible problem list, you must analyze each potential cause. The following discussion considers the problems listed and illustrates the resolution of discovered problems.

Checking Physical Attachment of Clients to Network

The first step is to determine whether clients are physically attached to the network, as follows:

Step 1 Visually inspect the physical attachment of each client and attempt to connect to a local server. If a connection can be established, the client obviously is attached.

Step 2 If a connection cannot be established to a local server (either one does not exist or the connection attempt fails), use a protocol analyzer to determine whether clients are sending any packets. Look for packets with the hardware address of each client as the source address.

Step 3 As an alternative, use the **debug xns packet** privileged EXEC command on the locally connected router (in this case Router-D) and look for each client's source address. If packets appear that include the hardware address of the respective client as the source address, the client is active on the network, and connectivity to Router-D is functional.

In order to use **debug xns packet**, you must disable fast switching. (Use the **no xns route-cache** interface configuration command on Ethernet interface E2.)

In this case, assume that connectivity is verified up to Router-D from Client-A.

Checking Physical Attachment of Servers to Network

The next step is to determine whether the remote servers are attached to their Ethernet segments. This process is very similar to determining whether the clients are attached to the Downtown segment.

Step 1 As in the prior procedure, start by visually inspecting the attachment of the servers to their Network.

Step 2 Using a protocol analyzer, determine whether the servers (in this case, Server-1 and Server-2) are sending any packets on their local networks. Look for packets with the hardware address of each server as the source address.

In this case, assume that connectivity is verified up to Router-M from Server-1.

Enabling XNS Routing

Use the **write terminal** privileged EXEC command to determine whether XNS routing is enabled. Use the **xns routing** global configuration command if it is not. Use the **show protocols** EXEC command to determine what protocols are running on which interfaces.

Checking XNS Network Numbers

Use the **write terminal** privileged EXEC command to determine whether the network number matches the client or the server network number. Use the **xns network** interface configuration command to change or assign the proper network number to the interface.

Checking Router Interface Status

In the process of eliminating the preceding problems, it is highly likely that the status of each router interface has been verified. You can further confirm the status of the router interfaces using the following procedure:

Step 1 Issue the **show xns interface** EXEC command on each router. The interfaces should indicate that the interface and line protocol are up. The **show xns interface** command displays additional information about the status of an interface.

Step 2 You also can **ping** between the routers to confirm that the interfaces are operational.

Again, for the purposes of this scenario, assume that all of the interfaces are functional.

Checking for Access List Problems

Access list problems are commonly the cause of connectivity problems. For details concerning access list issues, refer to Table 13-1 in the "Clients Cannot Communicate with XNS Servers over Routers" symptom module later in this chapter.

For the purposes of this scenario, assume that the **write terminal** privileged EXEC command output for both Router-D and Router-M indicates that there are no relevant access list specifications.

Checking for Nonunique MAC Addresses on Routers

MAC addresses for XNS configurations are obtained in one of two ways: either from the router hardware address embedded in the system firmware or by random assignment (when the system software initializes before the interface is initialized). In some *rare* cases, the randomly generated MAC address for different routers will be the same. If these numbers are not unique, and the routers are on the same internetwork, communication will not occur. If Router-M and Router-D have the same MAC address, no traffic will traverse the serial link.

Use the following procedure to check for nonunique MAC addresses:

Step 1 Use the **write terminal** privileged EXEC command to examine the current configuration of each router in the path (Router-D and Router-M).

Step 2 Check the hardware address specified in the **xns routing** global configuration command. If this system-generated number matches for both routers, reinitialize one of the routers and see if connectivity over the link is reestablished. To reinitialize a router, you may need to turn XNS routing off then turn it back on.

Step 3 Test for connectivity between clients and servers.

Step 4 If connectivity is still blocked, reexamine the configuration of the routers.

Step 5 If the routers still have matching MAC addresses, use the **show controllers** *interface-type* EXEC command to obtain an actual MAC address from each router.

Step 6 Use the **xns routing** global configuration command to enter the selected MAC address (for example, **xns routing 00aa.54f1.003e**).

In general, this problem occurs more frequently in Token Ring implementations. For the purposes of this scenario, assume that the MAC addresses are different.

Checking for Misconfigured xns forward-protocol Command

Next, look for a missing or misconfigured **xns forward-protocol** global configuration command, as follows:

Step 1 To diagnose this configuration problem, use the EXEC **write terminal** privileged EXEC command. In the output, look for the global command **xns forward-protocol**. This command must include the proper type number.

Step 2 To discover the type number, use the EXEC **debug xns packet** command or use a protocol analyzer to capture the trace.

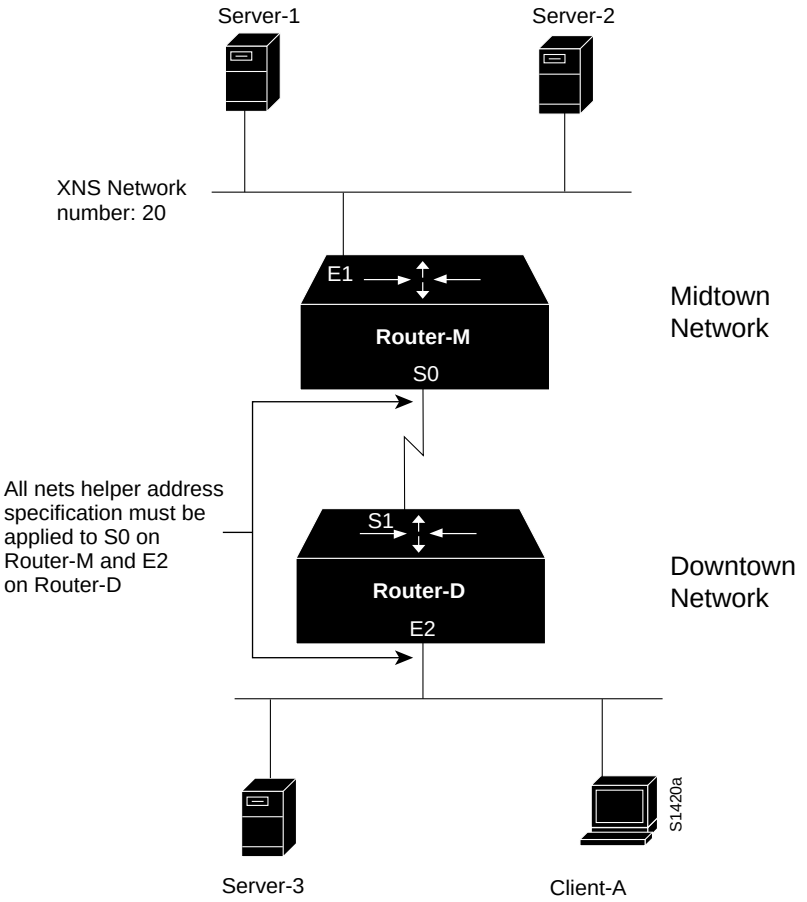
Assume for the purposes of this scenario that the **xns forward-protocol** command is properly configured. Unfortunately, connectivity to the remote hosts from Client-A is still blocked when test connections are attempted.

Checking for Misconfigured Helper Addresses

Next, look for a missing or misconfigured XNS helper address specification. On each of the routers, issue the **write terminal** EXEC command to look for **xns helper-address** interface configuration command specifications. The **xns helper-address** command must include either an *all nets* specification (-1.ffff.ffff.ffff) or *directed broadcast* specification (20.ffff.ffff.ffff).

If the all nets specification is used, it must be specified on Router-M (serial interface S0) and Router-D (Ethernet interface E2). Figure 13-2 illustrates the flow of broadcast traffic from clients and the application of the all nets broadcast specification. If a directed broadcast specification is used, it is only required on Router-D (Ethernet interface E2).

Figure 13-2 All Nets Helper Address Specification Illustration



Assume that the helper address is not included in the original configuration and is added as a correction. This restores connectivity between Client-A and the remote hosts.

Problem Solution Summary

This scenario focused on diagnosing blocked connectivity in XNS internetworks. The problem that was discovered was that the helper address specification was not present in the configuration. This was resolved with the addition of a directed-broadcast helper address which allowed the routers to forward XNS broadcast packets.

Figure 13-3 and Figure 13-4 provide representative configuration listings for Router-M and Router-D as discussed in this scenario. These configurations illustrate the configuration commands required to interconnect the two Ethernet segments over the T1 line.

Figure 13-3 Relevant XNS Configuration Commands for Router-D

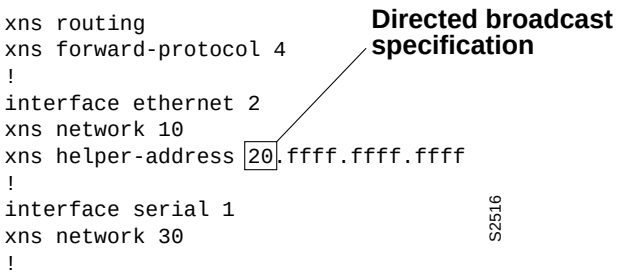
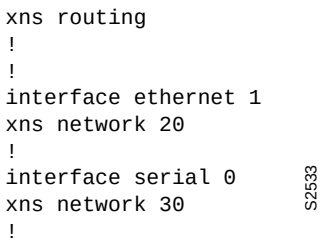


Figure 13-4 Relevant XNS Configuration Commands for Router-M



Note Remember to reenable fast switching using the **xns route-cache** interface command if it was disabled during troubleshooting.

XNS Internetworking Connectivity Symptoms

The symptom modules in this section pertain to XNS internetwork problems. Specific XNS connectivity symptoms are discussed in the following sections:

- Clients Cannot Communicate with XNS Servers over Routers
- XNS Broadcast Packets Cannot Get through Router
- Clients Cannot Connect to Server over Packet-Switched Network

Clients Cannot Communicate with XNS Servers over Routers

Symptom: Clients might not be able to connect to servers on their directly connected networks. In either case, no connections can be made to servers on the other side of the router. Table 13-1 outlines possible causes and suggested actions when clients cannot communicate with XNS servers over routers.

Table 13-1 XNS: Clients Cannot Communicate with XNS Servers over Router

Possible Causes	Suggested Actions
Clients or servers are not attached to network	**Step 1** Connect both clients and servers to the same network and verify that they can communicate. **Step 2** If they cannot communicate, check the configuration of the client and the server. For troubleshooting information, refer to the software documentation for the host. **Step 3** Attach a network analyzer to the network to which the clients and servers are temporarily connected. Look for the source addresses of both. **Step 4** If you find the source addresses, the end stations are operating properly. If you do not find their addresses, check the configuration of the clients and servers (consult your client and server documentation for more information).
Router interface is not functioning	**Step 1** Use the **show interfaces** EXEC command to check the status of the router. **Step 2** If the interface is administratively down, specify the **no shutdown** interface configuration command on the interface. **Step 3** If the interface or line protocol is down, check cable connections from the router. If necessary, replace the cable. **Step 4** If, after replacing the cable, the **show interfaces** EXEC command indicates that the interface and line protocol are not up, contact your router technical support representative.
Router network number specification is misconfigured for XNS server, causing problems for RIP	**Step 1** Use the **write terminal** privileged EXEC command to verify that XNS routing is enabled. If not, add the **xns routing** router configuration command and related commands as necessary. **Step 2** Get the network number from the target network server. **Step 3** Use the **write terminal** privileged EXEC command or **show xns interface** EXEC command to obtain the network number specified on the server side of the router. **Step 4** Compare the network numbers. If they do not match, reconfigure the router with the correct network number. **Step 5** If the network numbers match, check the router interface on the client side and make sure that the assigned network number is unique with respect to all network numbers in your XNS internetwork.

Possible Causes	Suggested Actions
Misconfigured access list	**Step 1** Remove any **xns access-group** interface configuration command specifications on all relevant interfaces. **Step 2** See whether traffic can get through by testing the connectivity of the client to the target server. If the connection now works, the access list needs modification. **Step 3** To isolate the location of the bad access list specification, apply one access list statement at a time until you can no longer create connections. **Step 4** Make sure that access lists are applied to the correct interface. Normally, filters are applied to *outgoing* interfaces.
Backdoor bridge between segments	**Step 1** Use the **show xns traffic** EXEC command to determine whether the bad hop count field is incrementing. **Step 2** If this counter is increasing, use a network analyzer to look for packet loops on suspect segments. Look for routing updates. If a backdoor bridge exists, you are likely to see hop counts that increment up to 15; the route will disappear and can reappear unpredictably. **Step 3** Use a protocol analyzer to examine the traffic on each segment. Look for known remote network numbers that show up on the local network. That is, look for packets from a remote network whose source address is not the source address of the router. **Step 4** Use a fanout or similar device to isolate the local Ethernet into smaller segments. **Step 5** The back door is located on the segment on which a packet from a remote network appears whose source address is not the source address of the router.
Nonfunctional Fiber Distributed Data Interface (FDDI) ring	**Step 1** Use the **show interfaces fddi** EXEC command to determine the status of the interface. **Step 2** If **show interfaces fddi** EXEC command indicates that the interface and line protocol are up, use the **ping xns** EXEC command to test connectivity between routers. **Step 3** If the interface and line protocol are up, make sure the MAC addresses of upstream and downstream neighbors are as expected. If all zeros appear in either of the address fields for these neighbors, a physical connection problem is likely. **Step 4** In this case (or if status line does *not* indicate that the interface and line protocol are up), check patch-panel connections. Use an optical time domain reflectometer (TDR) or light meter to check connectivity between routers. Ensure that signal strength is within specification.
Nonfunctional serial link	**Step 1** Use the **show interfaces serial** EXEC command to determine the status of the interface. **Step 2** If the **show interfaces serial** EXEC command indicates that the interface and line protocol are up, use the **ping xns** command to test connectivity between routers. **Step 3** If the routers do not respond to the ping test, follow the serial line troubleshooting techniques described in the "Troubleshooting Serial Line Problems" chapter.

Possible Causes	Suggested Actions
Nonfunctional Ethernet backbone	**Step 1** Use the **show interfaces ethernet** EXEC command to determine the status of the interface. **Step 2** If the status line does not indicate that the interface and line protocol are up, check the physical attachment of the router to the Ethernet backbone. **Step 3** If the **show interfaces ethernet** EXEC command indicates that the interface and line protocol are up, use the **ping xns** command to test connectivity between routers. **Step 4** Obtain analyzer traces and look for packets from target servers, clients, and routers. **Step 5** Any known nodes that do not appear as expected are suspects for being problem nodes. Locate the node and determine whether the node and its cables are functional. If not, replace or reconfigure the node and its cables as needed.
Nonfunctional Token Ring backbone	**Step 1** Use the **show interfaces token** EXEC command to determine the status of the interface. **Step 2** If the status line indicates that the interface and line protocol are not up, check the cable from the router to the Multistation Access Unit. Make sure that the cable is good; if necessary, replace the cable. **Step 3** If the **show interfaces token** EXEC command indicates that the interface and line protocol are up, use the **ping xns** EXEC command to test connectivity between routers. **Step 4** If the remote router does not respond, check the ring specification on all nodes that are attached to the Token Ring backbone. The ring speed for all nodes must be the same. **Step 5** If necessary, modify ring speed specifications for clients, servers, and routers. **Step 6** On routers that support setting the ring speed in software, use the **ring-speed** interface configuration command. On modular router platforms, change jumpers as needed. For more information about ring speed specification, refer to the hardware installation and maintenance documentation for your system.

XNS Broadcast Packets Cannot Get through Router

Symptom: Clients are unable to get response from servers using XNS broadcast when they attempt to connect over a router. Table 13-2 outlines possible causes and suggested actions when XNS broadcast packets cannot get through a router.

Table 13-2 XNS: XNS Broadcast Packets Cannot Get through Router

Possible Causes	Suggested Actions
Missing **xns helper-address** interface configuration command	**Step 1** Enable the **debug xns packet** privileged EXEC command and look for XNS packets that have an unknown type xx specification. **Step 2** Use the **write terminal** privileged EXEC command to verify that the **xns helper-address** interface configuration command is configured for the incoming interface (for XNS broadcast traffic from stations). **Step 3** If the **xns helper-address** command is not present, add it as appropriate. Depending on the network configuration, the specification of the helper address may differ. For more information, refer to the section "Helper Address Specification Hints" later in this chapter and to the *Router Products Configuration Guide* and *Router Products Command Reference* publications.

Misconfigured **xns helper-address** specification	**Step 1** Check the router interface configuration on the client side for the **xns helper-address** interface configuration command.
	Step 2 Make sure that the MAC address field specified in this command is a type of broadcast.
	Example of an all nets broadcast:
	`interface ethernet 0`
	`xns helper-address -1.ffff.ffff.ffff`
	Example of a directed broadcast:
	`interface ethernet 1`
	`xns helper-address 40.ffff.ffff.ffff`

Missing **xns forward-protocol** router configuration command	**Step 1** Enable the **debug xns packet** privileged EXEC command and look for XNS packets with the unknown type xx. **Step 2** Use the **write terminal** privileged EXEC command to look in the router configuration for the **xns forward-protocol** global configuration command. **Step 3** If the command is not present, add it as appropriate.
Misconfigured access list	**Step 1** Refer to Table 13-1 for suggested actions.

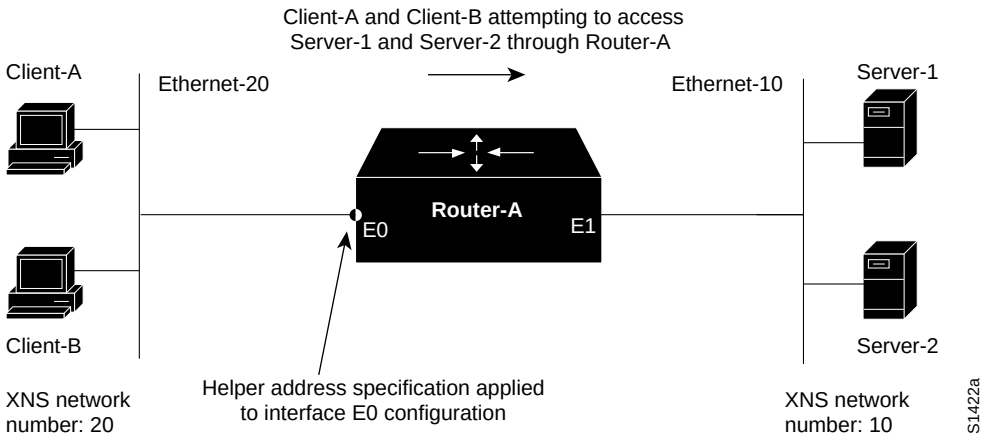
Helper Address Specification Hints

The following illustrations and accompanying text discuss some of the implications of XNS helper address assignment, some potential pitfalls, and general behavioral characteristics. The *Router Products Command Reference* and *Router Products Configuration Guide* publications provide details about configuration commands associated with helper address assignment.

Basic Helper Address Assignment

Consider the simple configuration illustrated in Figure 13-5. In this case, Router-A separates two Ethernet segments (Ethernet-20 and Ethernet-10). Clients on Ethernet-20 must be able to access services from Server-1 and Server-2 on Ethernet-10.

Figure 13-5 Basic Helper Address Network



The helper address specification is as follows:

```
interface ethernet 0
xns network 20
xns helper-address -1.ffff.ffff.ffff
```

Here, -1 is used to specify flooding to all nets.

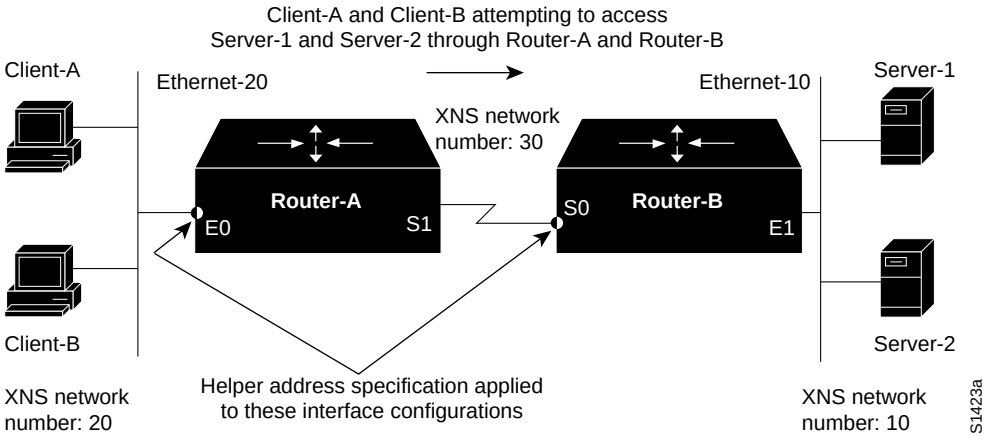
As an alternative, you can specify a network number. In this case, specify XNS network 10 as follows:

```
interface ethernet 0
xns network 20
xns helper-address 10.ffff.ffff.ffff
```

Helper Address Configuration over a Single Serial Interconnection

The network configuration illustrated in Figure 13-6 is similar to that illustrated in Figure 13-5, except that Ethernet-20 and Ethernet-10 are separated by a serial network and two routers (Router-A and Router-B). As before, clients on Ethernet-20 must be able to access services from Server-1 and Server-2 on Ethernet-10.

Figure 13-6 Single Serial Interconnection Helper Address Network



Assuming the use of the all nets broadcast address, the helper address specifications for the two routers would be as follows:

```
!Router-A helper address specification:
!
interface ethernet 0
xns network 20
xns helper-address -1.ffff.ffff.ffff

!Router-B helper address specification:
!
interface serial 0
xns network 30
xns helper-address -1.ffff.ffff.ffff
```

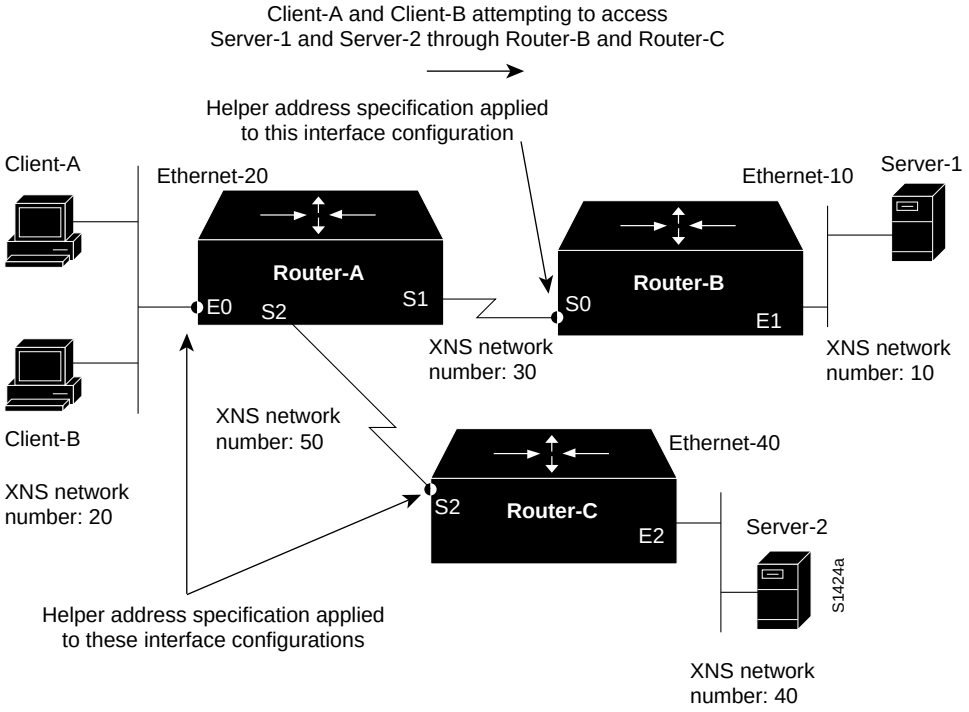
As in the prior example, -1 is used to specify flooding to all nets. Note that the helper address specification is required on Router-B because of the use of the all nets (-1) network specification (on Router-A). You can specify a specific network number as an alternative. In this case, you would specify XNS network 10 on Router-A only as follows:

```
!Router-A helper address specification:
!
interface ethernet 0
xns network 20
xns helper-address 10.ffff.ffff.ffff
```

Helper Address Configuration over Multiple Serial Interconnections

The key difference between the following example and prior examples is that Server-1 and Server-2 are now on separate Ethernet segments, and clients access Server-1 and Server-2 via different routers (Router-B and Router-C). Refer to Figure 13-7.

Figure 13-7 All Nets Multiple Serial-Line Helper Address Specification



The all nets broadcast configurations for the routers follow:

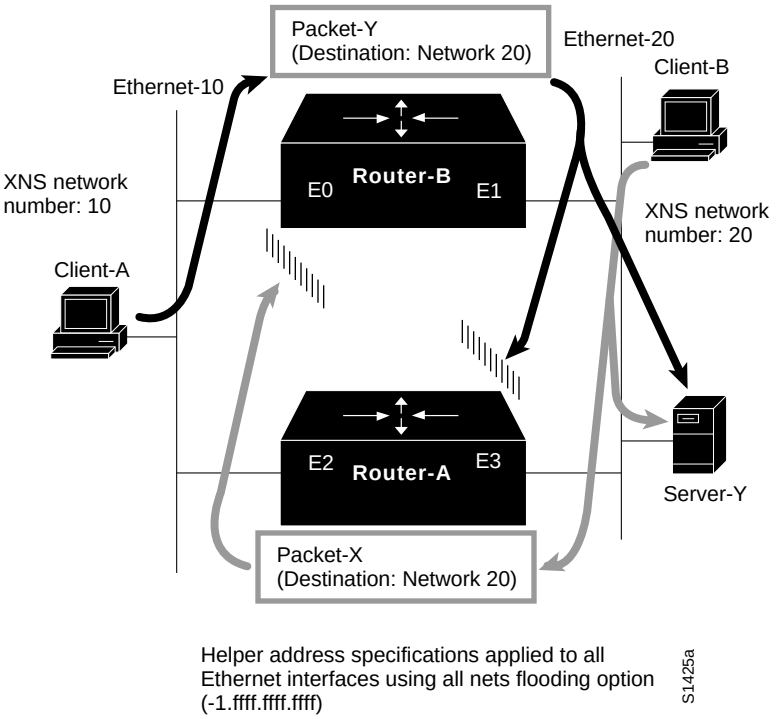
```
!Router-A helper address specification:
!
interface ethernet 0
xns network 20
xns helper-address -1.ffff.ffff.ffff

!Router-B helper address specification:
!
interface serial 0
xns network 30
xns helper-address -1.ffff.ffff.ffff

!Router-C helper address specification:
!
interface serial 2
xns network 50
xns helper-address -1.ffff.ffff.ffff
```

Note that the helper address specification is *required* on both Router-B and Router-C because of the use of the all nets (-1) network specification on Router-A.

Helper Behavior with Parallel Routers

Use care in assigning broadcast-type helper addresses when XNS networks are interconnected over multiple routers and when clients are using XNS broadcast. Although traffic will not permanently loop, local client queries can leak out through a router, resulting in excess traffic. Consider the situation illustrated in Figure 13-8.

Figure 13-8 XNS Helper Address Handling with Parallel Routers



In this example, helper addresses are assigned to the Ethernet interfaces on Router-A and Router-B. The interface configurations might be as follows:

```
!Router-B helper address specifications:
!
interface ethernet 0
xns network 10
xns helper-address -1.ffff.ffff.ffff
!
interface ethernet 1
xns network 20
xns helper-address -1.ffff.ffff.ffff

!Router-A helper address specifications:
!
interface ethernet 2
xns network 10
xns helper-address -1.ffff.ffff.ffff
!
interface ethernet 3
xns network 20
xns helper-address -1.ffff.ffff.ffff
```

Consider what happens to Packet-Y from Client-A that is destined for Server-Y on XNS network 20. Assume that no access lists are in place and that Router-B is the first to get a query from Client-A. Because the query is intended for an offnet host, Router-B broadcasts the query out of Ethernet interface E1 and onto XNS network 20. The broadcast finds its way to Server-Y (causing a response, assuming that Server-Y is operational) and also lands at Ethernet interface E3 on Router-A. There, the packet is dropped. This is the expected behavior.

Note Server-Y actually receives two copies of Packet-Y, one via Router-A and one via Router-B. The response of the server depends on its application implementation.

Now consider Packet-X, a client query from Client-B that is also intended for Server-Y. In this case, the broadcast packet finds its server on the same wire to which it is connected. However, Router-A forwards this broadcast because the source address is local—which puts the locally targeted packet onto XNS network 10. This packet will continue to propagate outward through the network until the internetwork terminates (or until the packet has traversed 15 routers), but it will not leak back into XNS network 20 because the routers see that the source network in the packet is 20. In no case is the packet sent back along the path to its source network. In the preceding example, the packet would be dropped when it reaches Ethernet interface E0 on Router-B.

This situation is a type of *partial* loop. True routing loops are prevented, but some excess traffic is created.

Note To prevent loops from occurring, you can use network-specific broadcasts. However, you may not be able to do so if many clients and servers must access each other on segments separated by parallel routers. Depending on your configuration, increasing the number of paths the router can store for each destination may reduce the amount of excess traffic. Use the **xns maximum-paths** interface configuration command to do this.

Clients Cannot Connect to Server over Packet-Switched Network

Symptom: Local servers are responding, but servers on the other side of a packet-switched network (PSN) that interconnects routers do not respond. A router *appears* to block XNS over the PSN. Table 13-3 outlines possible causes and suggested actions when clients cannot connect to a server over a PSN.

Table 13-3 XNS: Clients Cannot Connect to Server over PSN

Possible Causes	Suggested Actions
X.25 address mapping error	**Step 1** Use the **write terminal** privileged EXEC command or the **show x25 map** EXEC command to examine the configuration of the router. **Step 2** Make sure that the MAC addresses and X.121 addresses specified in any **x25 map xns** interface configuration commands match the addresses associated with the respective destination routers. For information about address mapping, refer to the section, "Notes about PSN Address Map Specifications," later in this chapter.
Frame Relay address mapping error	**Step 1** Use the **write terminal** privileged EXEC command to examine the configuration of the router. **Step 2** Make sure that the MAC addresses and DLCI addresses specified in any **frame-relay map xns** interface configuration commands match the addresses associated with the respective destination routers. For information about address mapping, refer to the section, "Notes about PSN Address Map Specifications," later in this chapter.
Misconfigured network number specification on servers or routers	**Step 1** See Table 13-1 for suggested actions.
Encapsulation mismatch	**Step 1** Use the **write terminal** privileged EXEC command or the **show interfaces** EXEC command to look for an **encapsulation** interface configuration command, such as **encapsulation x25** or **encapsulation frame-relay**. If an **encapsulation** command is not present, the default is High-Level Data Link (HDLC) encapsulation. **Step 2** For PSN interconnections, you must explicitly specify the encapsulation type.

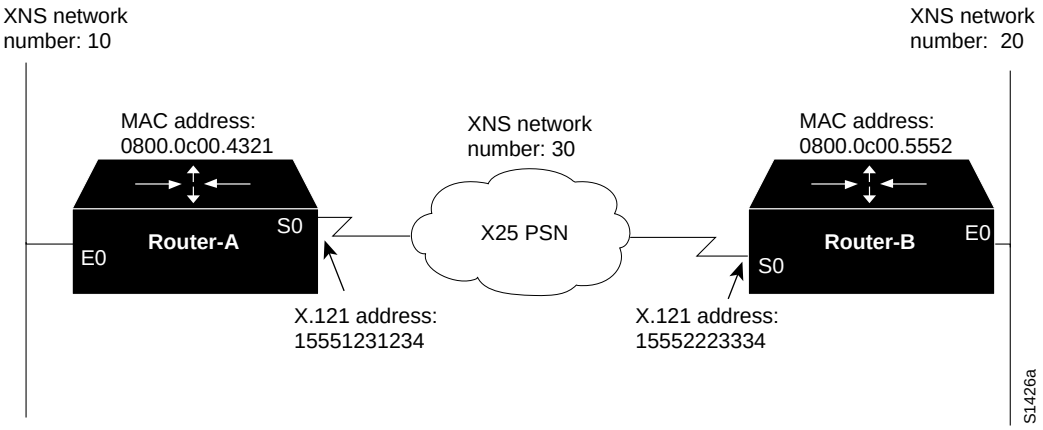
Notes about PSN Address Map Specifications

When routing XNS (or any protocol) over a PSN, you must specify mapping between the protocol and the PSN addresses. Consider the two examples illustrated in Figure 13-9 and Figure 13-10. Figure 13-9 illustrates an address map specification when routing XNS over an X.25 PSN, while Figure 13-10 illustrates an address map specification when routing XNS over a Frame Relay network. Relevant configurations and a brief explanation of command variables are provided in the following discussions. For more information about address map specifications, refer to the *Router Products Configuration Guide* and *Router Products Command Reference* publications.

Address Mapping for XNS-to-X.25 Interconnection

As illustrated in Figure 13-9, XNS-to-X.25 address map specifications would be required for both Router-A and Router-B.

Figure 13-9 Network Diagram Illustrating XNS-to-X.25 Mapping



The specific interface configurations are as follows:

```
!Router-A
interface serial 0
x25 map xns 30.0800.0c00.5552 15552223334 broadcast
! Above specifies XNS-to-X.121 address map configuration for Router-A

!Router-B
interface serial 1
x25 map xns 30.0800.0c00.4321 15551231234 broadcast
! Above specifies XNS-to-X.121 address map configuration for Router-B
```

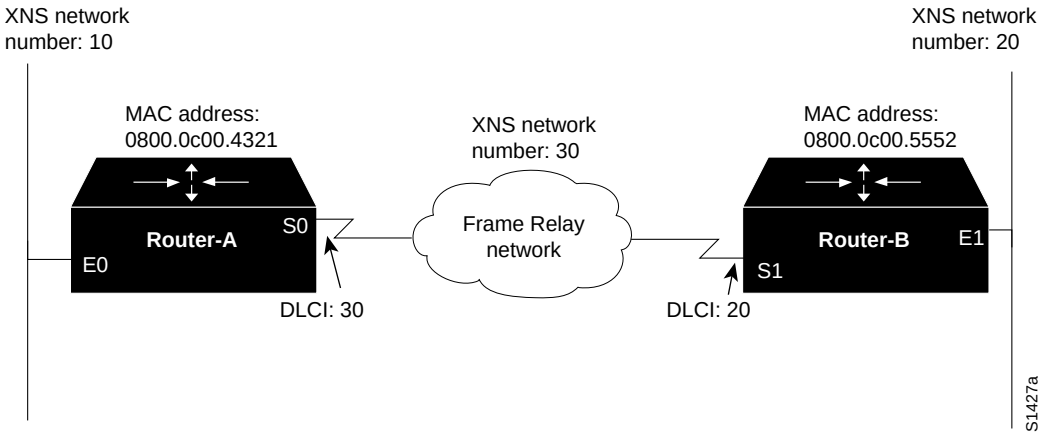
In the preceding configurations, the MAC address is obtained using the **write terminal** privileged EXEC command on the target router. Look for the **xns routing** router configuration command in the configuration listing. It is displayed with the auto-generated MAC address appended to the command. For Router-A in Figure 13-9, you would see the following listing:

```
xns routing 0800.0c00.4321
```

Address Mapping for XNS-to-Frame Relay Interconnection

Figure 13-10 illustrates essentially the same interconnection arrangement as Figure 13-9, except that the PSN used is a Frame Relay network. In an analogous manner, XNS-to-Frame Relay address map specifications would be required for both Router-A and Router-B.

Figure 13-10 Network Diagram Illustrating XNS-to-Frame Relay Mapping



The specific interface configurations would be as follows:

```
!
interface serial 0
frame-relay map xns 30.0800.0c00.5552 20 broadcast
! Above specifies XNS-to-DLCI address map configuration for Router-A

interface serial 0
frame-relay map xns 30.0800.0c00.4321 30 broadcast
! Above specifies XNS-to-DLCI address map configuration for Router-B
```

In these example configurations, the MAC address is obtained in the same manner as described in the X.25 example: use the **write terminal** privileged EXEC command on the target router and look for the **xns routing** router configuration command in the configuration listing.

PART 3

Troubleshooting Performance

CHAPTER 14

Performance Problem Scenarios

This chapter presents problem-solving scenarios for identifying, isolating, and solving problems that impede throughput performance in internetworks.

These problem-solving scenarios address specific situations and illustrate the process of problem isolation and resolution. The scenarios span different protocols, media, and problem types. The objective is to illustrate a problem-solving method based on the model defined in the section "General Problem-Solving Model" in the "Troubleshooting Overview" chapter. The scenarios focus on situations in which traffic is getting to its intended destination, but network users complain about slow host response, connections dropping, or sporadic resource availability.

Each scenario includes the following components:

- Symptom statement
- Description of the internetworking environment
- Discussion of the problem isolation process
- Summary of the solution

The "Troubleshooting Internetwork Performance" chapter presents a series of symptom modules that provide snapshots of common symptoms, possible causes, and suggested actions for the protocols and technologies addressed in this publication.

For an overview of scenarios and symptom modules, see the section "Using This Publication" in the "Troubleshooting Overview" chapter.

Performance Scenario Overview

In general, performance slowdowns are considered lower-priority problems than reachability issues. However, poorly performing internetworks can degrade organizational productivity and can effectively halt operation of network applications. Performance problems manifest themselves in many ways. Slow host response, dropped connections, and high error counts all suggest that network performance is not optimal. Unfortunately, the actual sources of performance problems are often difficult to detect.

This chapter presents a series of situational discussions, including the application of various diagnostic tools. Every possible scenario cannot be covered. Indeed, the scenarios included here only scratch the surface of possible situations. However, certain common themes typically tie all connectivity problems together. This chapter illustrates the use of troubleshooting tools and techniques to identify those common themes.

The following problem-solving scenarios are presented in this chapter:

- Novell Performance Scenarios—Several performance-related scenarios illustrate typical configuration and network design problems that lead to poor performance in Novell IPX internetworks.
- Poor Performance over TCP/IP Serial Network—This scenario focuses on performance in a TCP/IP internetwork in which Cisco routers and parallel serial links join two geographically separated locations.
- Serial Link Performance Scenario—This scenario illustrates the resolution of problems associated with poor host response over a 56-kbps High-Level Data Link Control (HDLC) link.
- XNS Performance Scenarios—Several short performance-related case examples illustrate typical configuration and network design problems that can lead to poor performance in XNS internetworks.

Performance Problems in Novell IPX Internetwork after Bandwidth Upgrade

The following case illustrates a situation in which performance degrades significantly after a Novell IPX internetwork is upgraded from a 2400-baud link over a telephone line to a 9600-baud synchronous serial line.

Symptoms

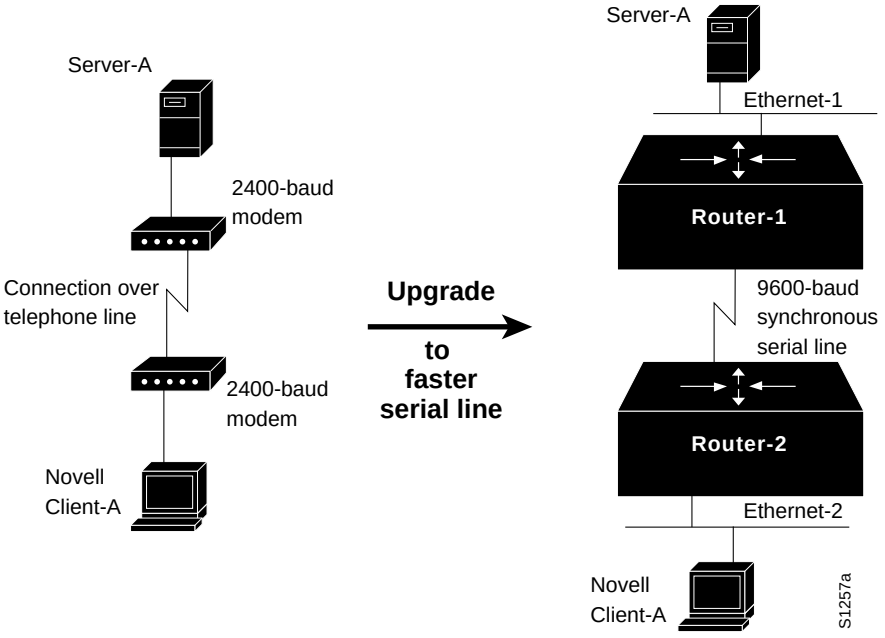
Server responsiveness noticeably slows following an upgrade from a 2400-baud, direct dial-up interconnection between a client and a server to a router-based link over a 9600-baud synchronous serial line.

Environment Description

Figure 14-1 shows a map of the environment for this scenario. The following characteristics represent the relevant elements of this internetwork:

- Initial communication between Client-A and Server-A is acceptable when provided over a direct dial-up link.
- In order to share resources, Client-A is attached to an Ethernet, and the dial-up access is replaced by a 9600-baud synchronous serial line separated by two routers.
- LANs are IEEE 802.3 Ethernets.
- Novell IPX is the only protocol being routed over the point-to-point link.

Figure 14-1 Upgrade from Dial-Up Link to 9600-Baud Connection



Diagnosing and Isolating Problem Causes

Insufficient bandwidth is the best candidate for poor server responsiveness.

In the original configuration, Server-A communicates with Client-A without any encapsulation. Although the modems attach a header to each transmission, information exchanged between Server-A and Client-A is essentially all data and varies in size depending on the kind of communication that is occurring.

In the upgraded configuration, the Ethernet segments to which Server-A and Client-A are attached require a minimum packet size of 60 bytes (which includes a 6-byte destination address, a 6-byte source address, a 2-byte type or length field, and data). The overhead associated with Ethernet encapsulation (for packets smaller than 60 bytes) can easily overwhelm the 9600-baud line, resulting in communication that is actually slower than the original direct, dial-up interconnection.

Problem Solution Summary

One solution is to disable fast switching, which uses the link-layer packet size. When fast switching is disabled, the router uses the network layer packet size. In addition, when fast switching is disabled, more buffers are available for handling peak loads.

However, with such a narrow serial pipe, the best solution is to add bandwidth. The amount of additional bandwidth required will vary depending on the situation. Certainly, if multiple clients are trying to access multiple servers, converting the 9600-baud line to a 56-kbps line would be reasonable.

Performance Problems in Novell IPX Internetwork after Switching to Routing

The following scenario illustrates a situation in which performance degrades significantly after a bridged Novell IPX internetwork is converted to routing.

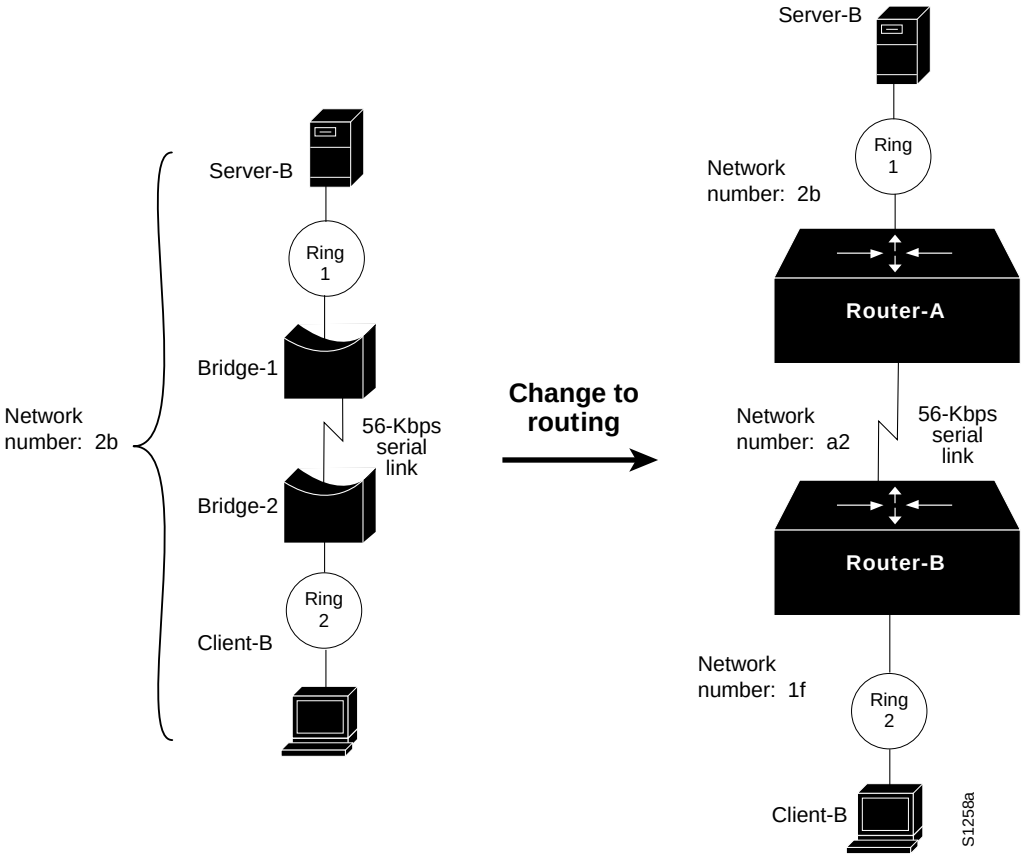
Symptoms

Server responsiveness slows by an approximate factor of four after Novell IPX routing is implemented in place of bridging.

Environment Description

Figure 14-2 shows a map of the internetwork before and after the conversion.

Figure 14-2 Novell IPX Interconnection Converted from Bridging to Routing



The following characteristics represent the relevant elements of this internetwork:

- Previously, communication between Client-B and Server-B was provided via two remote bridges over a 56-kbps link.
- In order to ensure a more manageable interconnection, Bridge-1 and Bridge-2 are replaced with routers (Router-1 and Router-2) over the same 56-kbps link.
- LANs are IEEE 802.5 Token Rings.
- Novell IPX is the only protocol being routed over the point-to-point link.

Diagnosing and Isolating Problem Causes

The maximum packet size limitation associated with standard NetWare in a routed environment is the best candidate for poor server responsiveness.

In a bridged environment, Server-B allows transmission of the maximum packet size associated with the media in the internetwork (1130 bytes for Ethernet, and 4202 bytes for 4-Mbps Token Ring and 16-Mbps Token Ring).

However, in a router-based internetwork, standard NetWare 3.11 and earlier Novell servers only allow for a maximum packet size of 576 bytes, regardless of media. Packet routing defaults to this smallest common size whenever multiple network numbers are detected. In addition, prior to Software Release 8.3(3), Cisco routers did not support the Novell Large Internet Packet Exchange (LIPX) NetWare-loadable module (PBURST.NLM) for Token Ring. (This module was previously known as BIGPACK.) Novell 3.12 and 4.*x* servers automatically find the largest packet size.

Problem Solution Summary

Two actions can help improve performance between Server-B and Client-B in this router-based internetwork:

- Implement the Novell PBURST.NLM NetWare-loadable module on the server to accommodate the transmission of packets of any size requested by clients, or upgrade Novell servers to 3.12 or 4.*x*.

Caution Be sure that all media and transport protocols are accounted for when implementing PBURST.NLM. If any segment does not support the larger packets, connectivity can be disrupted throughout the internetwork.

- Implement BNETX.COM at clients to support burst mode. This software implements a windowing capability that allows for larger individual units of data transfer. Alternatively, you can upgrade to NetWare 3.12 or 4.*x*.

Slow Novell IPX Performance over Router Connecting 16-Mbps Rings

The following scenario illustrates a situation in which performance over a router interconnecting two 16-Mbps Token Rings is slower than a comparable interconnection of two Ethernet segments.

Symptoms

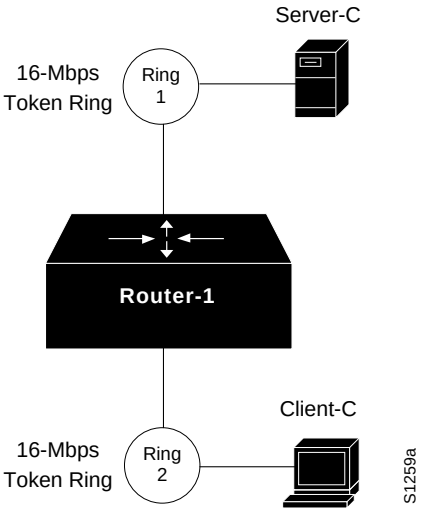
Server responsiveness is slow over a router that separates two 16-Mbps rings.

Environment Description

Figure 14-3 shows a map of the environment for this scenario. The following characteristics represent the relevant elements of this internetwork:

- Router-1 separates two Token Ring segments.
- Client-C (on Ring 2) accesses services on Server-C (on Ring 1).
- LANs are 16-Mbps Token Rings.
- Novell IPX is the only protocol being routed.

Figure 14-3 Novell IPX Interconnection over Router Joining 16-Mbps Rings



Diagnosing and Isolating Problem Causes

A likely candidate for poor server response is that PBURST.NLM is not implemented on the server. PBURST.NLM allows the server to transmit packets of any size.

Problem Solution Summary

Implement the PBURST.NLM NetWare-loadable module on the server.

Caution Be sure that all media and transport protocols are accounted for when implementing PBURST.NLM. If any segment does not support the larger packets, connectivity can be disrupted throughout the internetwork.

Implement BNETX.COM at clients to support burst mode. This software implements a windowing capability that allows the transfer of larger individual units of data.

Slow Novell IPX Performance over Ethernet Backbone

The following scenario illustrates a situation in which performance is extremely slow over an Ethernet backbone that separates two routers.

Symptoms

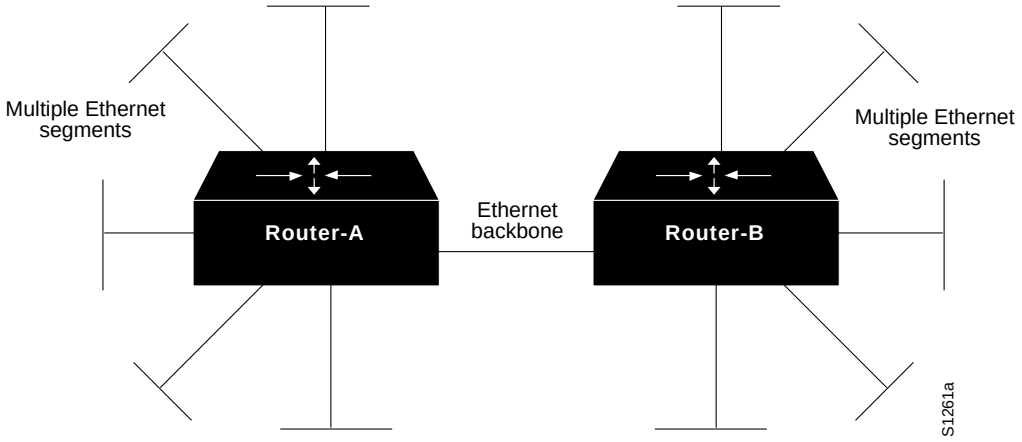
Slow server response among multiple Ethernet segments separated by two routers and an Ethernet backbone.

Environment Description

Figure 14-4 shows a map of the environment for this scenario. The following characteristics represent the relevant elements of this internetwork:

- Router-A and Router-B interconnect multiple Ethernets over an Ethernet backbone.
- LANs are IEEE 802.3 Ethernets.
- Novell IPX is the only protocol being routed.

Figure 14-4 Novell IPX Routers Joining Multiple Ethernets over an Ethernet Backbone



Diagnosing and Isolating Problem Causes

Congestion is the best candidate for poor performance over the backbone.

You can use the following procedure to determine whether there is a congestion problem over the backbone:

Step 1 Examine the output of the **show interfaces** EXEC command for relative load, high and increasing levels of input errors, and drops.

Step 2 Attach a network analyzer to the backbone. Look for high levels of collisions and for bandwidth utilization in excess of 30 percent.

For information about general troubleshooting of performance problems in a routed internetwork, refer to the section "Slow Host Response over a 56-kbps HDLC Link," later in this chapter. For more information about diagnosing congestion problems, refer to the "Troubleshooting Serial Line Problems" and the "Troubleshooting Internetwork Performance" chapters.

If you determine that congestion over the Ethernet backbone is high, the only real option is to increase bandwidth. You can do this by adding additional Ethernet segments or by replacing the Ethernet backbone with a faster media, such as Fiber Distributed Data Interface (FDDI).

Problem Solution Summary

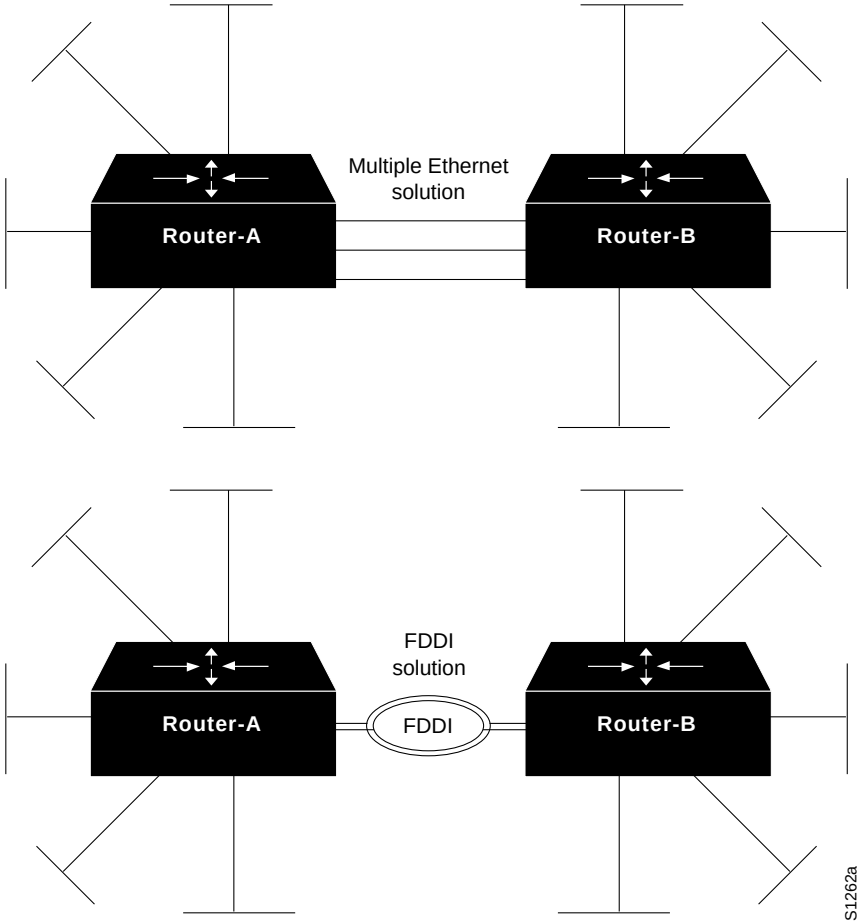
This scenario focused on improving performance over a backbone that segments multiple Ethernets by increasing bandwidth using one of two options:

- Replacing the single Ethernet backbone with multiple Ethernet segments.
- Replacing the single Ethernet backbone with an FDDI backbone.

Figure 14-5 illustrates these options.

Note If you adopt a multiple Ethernet option, remember to implement the **ipx maximum-paths** global configuration command. For more information about this requirement, refer to the section "Slow Novell IPX Performance over Equal Parallel Links" later in this chapter. Also note that each segment must have its own network address. For more information about duplicate network number problems, refer to the "Troubleshooting Novell IPX Connectivity" chapter.

Figure 14-5 Alternative Solutions to Ethernet Backbone Bottleneck



Slow Novell IPX Performance over Equal Parallel Links

The following scenario illustrates a situation in which performance is less than optimal over parallel T1 links that join two routers.

Symptoms

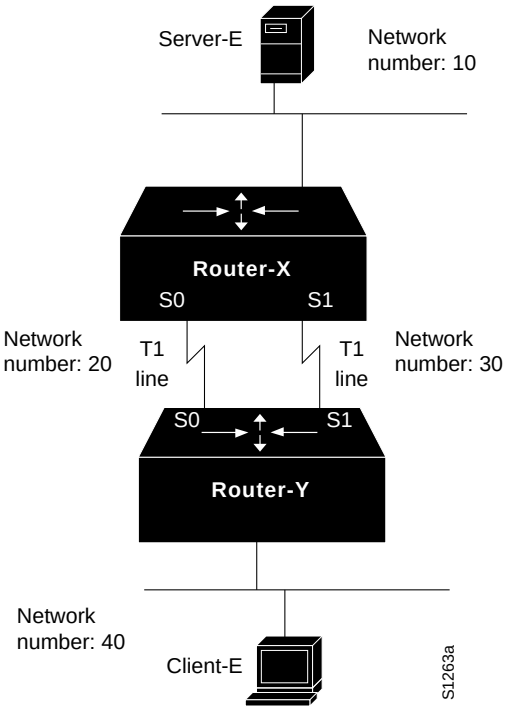
One line appears to be heavily loaded, while the other line is either idling or indicates very low load. Users complain of slow response and intermittent connection drops.

Environment Description

Figure 14-6 shows a map of the environment for this scenario. The following characteristics represent the relevant elements of this internetwork:

- Router-X and Router-Y interconnect two sites over parallel T1 lines running at 1.544 Mbps.
- Client-E needs to access Server-E on the other side of the serial interconnections.
- LANs are IEEE 802.3 Ethernets.
- Novell IPX is the only protocol being routed.

Figure 14-6 Routers Joining Novell IPX Networks over Parallel T1 Lines



Diagnosing and Isolating Problem Causes

The router probably is keeping only one routing table entry per target network. This is likely to cause poor performance over the parallel serial lines. In the worst case, traffic is routed through only one line, while the second line is idle.

You can use the following procedure to determine whether traffic is being unevenly distributed between the parallel lines:

Step 1 Use the **show interfaces** EXEC command to examine the load for each interface. Also examine the number of input and output drops and the 5-minute output and input packet counts. Record the observed values.

Step 2 Use the **clear counters** privileged EXEC command and continue to monitor changes in the counters over time with the **show interfaces** EXEC command.

Step 3 Look for values that are substantially uneven. (For example, interface serial 0 indicates 300,000 packets total input, while interface serial 1 indicates only 1000.)

Step 4 If you determine that traffic is unevenly distributed over the serial links, use the **ipx maximum-paths** global configuration command to set the number of multiple paths for the router to use when transmitting traffic to any particular destination. Instead of keeping only one routing table entry, the router will use up to the specified number of paths when it determines how to route traffic. In essence, the **ipx maximum-paths** global configuration command forces load balancing over two lines when the number of paths is specified as 2.

Note This problem is the same for any parallel media. The suggested solution would be the same for parallel FDDI, Ethernet, or Token Ring links, as well as for parallel serial interconnections.

Problem Solution Summary

This scenario focused on improving performance over parallel links. The recommended solution is to implement the **ipx maximum-paths** global configuration command with the number of paths specified as 2.

Slow Novell IPX Performance over Unequal Parallel Links

The following scenario illustrates a situation in which performance is slow over parallel links of differing speeds that join two routers.

Symptoms

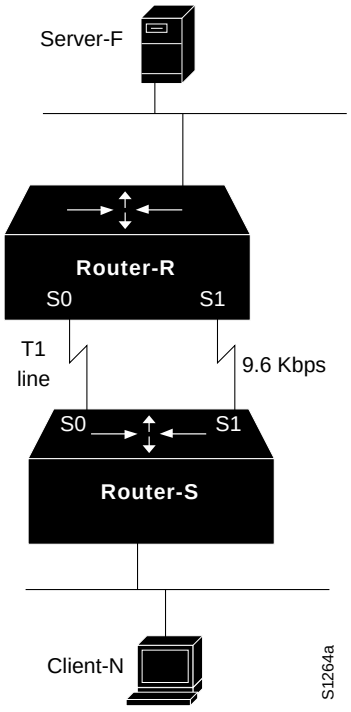
One line appears to be heavily loaded, while the other is either idling or indicates very low load. Users complain of slow response and intermittent connection drops.

Environment Description

Figure 14-7 shows a map of the environment for this scenario. The following characteristics represent the relevant elements of this internetwork:

- Router-R and Router-S interconnect two sites over parallel lines. One line runs at T1 speed (1.544 Mbps) and the other line runs at 9.6 kbps.
- The **ipx maximum-paths** global configuration command is enabled on both routers.
- Client-N needs to access Server-F on the other side of the serial interconnections.
- LANs are IEEE 802.3 Ethernets.
- Novell IPX is the only protocol being routed.

Figure 14-7 Routers Joining Novell IPX Networks over Unequal Parallel Lines



Diagnosing and Isolating Problem Causes

Because the Novell Routing Information Protocol (RIP) does not take line speed into consideration, load cannot be balanced effectively between these two links. For this reason, it is probable that traffic is only being routed through one line, while the second line is idle. And, because RIP does not consider line speed, the 9.6-kbps line could be completely overwhelmed, while the T1 line is relatively unused. A load-balancing problem is probably causing poor performance over the parallel serial lines.

You can use the following procedure to determine whether traffic is being unevenly distributed between the unequal parallel lines:

Step 1 Use the **show interfaces** EXEC command and examine the load for each interface. Also examine the number of input and output drops and the 5-minute output and input error counts. Record the observed values.

Step 2 Use the **clear counters** privileged EXEC command and continue to monitor changes in the counters over time with the **show interfaces** EXEC command.

Step 3 Look for values that are substantially uneven. (For example, interface serial 0 indicates 0 output drops, while interface serial 1 indicates 300 output drops.)

Step 4 If you determine that traffic is being unevenly distributed over the serial links, and the **ipx maximum-paths** global configuration command is already implemented, one solution is to make the speed on both lines match. Another solution is to use the **ipx delay** interface configuration command to set the tick value of the slow-speed line to a high value, which causes the slow-speed line to be used only as a backup.

Note This problem is the same for any unequal parallel media. The suggested solution would be the same for unevenly matched FDDI, Ethernet, or Token Ring links, as well as for uneven parallel serial interconnections.

Problem Solution Summary

This scenario focused on improving performance over uneven parallel links. The recommended solution is to force the speed of the parallel links to match or to use the **ipx delay** interface command to cause the slow-speed line to be used only as a backup.

Poor Performance over TCP/IP Serial Network

This scenario focuses on performance in a TCP/IP internetwork that uses Cisco routers and parallel serial links to join two geographically separated locations.

Symptoms

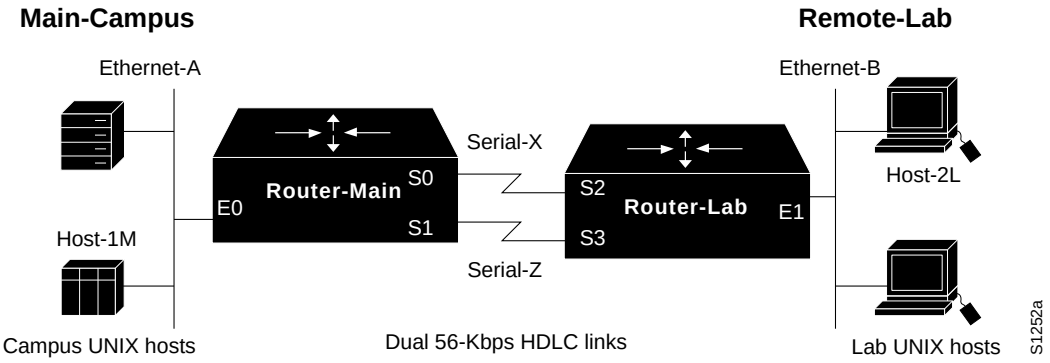
Users at Remote-Lab complain of poor host response and slow performance when connecting to hosts at the Main-Campus. In addition, during certain times of the day, large files are being transferred over the serial network. At these times, traffic becomes especially slow, but does not stop. Figure 14-8 illustrates this network topology.

Environment Description

Figure 14-8 shows a map of the environment for this scenario. The following characteristics represent the relevant elements of this internetwork:

- A remote research lab (Remote-Lab) is linked to a campus network (Main-Campus) over two parallel 56-kbps HDLC lines (Serial-X and Serial-Z).
- Two routers (Router-Main and Router-Lab) join the two sites. The routers are attached to channel service units (CSUs) or data service units (DSUs) with V.35 cables.
- LANs are IEEE 802.3 Ethernets.
- UNIX workstations are used at the Remote-Lab; traffic to the Main-Campus consists of File Transfer Protocol (FTP), Telnet, and mail.
- Transmission Control Protocol (TCP/IP) is being routed over the point-to-point links.

Figure 14-8 Dual 56-kbps Serial Link TCP/IP Internetwork Scenario Map



Diagnosing and Isolating Problem Causes

Given the situation, the following problems are the most likely candidates for poor performance between Main-Campus and Remote-Lab:

- Bad Ethernet or serial line
- Congestion

The following procedure illustrates the process of investigating potential hardware problems:

Step 1 Use the **show interfaces serial** EXEC command to determine the condition of the serial lines. Figure 14-9 shows output that indicates that the interfaces are minimally operational and the router can communicate with them.

Figure 14-9 show interfaces serial Command Output

```
Serial 0 is up, line protocol is up
  Hardware is MCI Serial
  MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:04, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 0/75, 40 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
     240 packets input, 15768 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     174 packets output, 11432 bytes, 0 underruns
     0 output errors, 0 collisions,40 interface resets, 0 restarts
     0 carrier transitions
```

S2440

Output queue drops

Input errors

Look for input errors and high numbers of output drops, which suggest that the serial line is being overutilized.

Step 2 Assume that the serial line is basically functional. That is, the router reports that the interface and line protocol are up. Now, use an extended **ping** test to isolate the point where traffic is being slowed. Look for drops, failures, and timeouts. Figure 14-10 illustrates an example of an extended ping test that detects failures.

Figure 14-10 ping Command Output

```
dingus# ping
Protocol [ip]:
Target IP address: 131.108.25.75
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address: dingus
Translating "DINGUS"...domain server (255.255.255.255) [OK]

Type of service [0]: ftp
Set DF bit in IP header? [no]: n
Data pattern [0xABCD]: ffff
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.108.25.75, timeout is 2 seconds:
Packet has data pattern 0xFFFF
.....
Success rate is 0 percent
```

Status of ping test

S2441

Step 3 Starting with the router closest to the remote hosts, **ping** various nodes in the path, looking for the point at which drops start to occur. For instance, **ping** from Router-Lab to Host-2L. If pings are successful, you can eliminate Ethernet-B as the source of congestion problems. Next, **ping** from Router-Main to Host-1M. If pings are successful, you can eliminate Ethernet-A as the source of congestion problems.

Step 4 If these tests indicate no problems, **ping** between the routers. First, **ping** from Router-Main to the IP address associated with interface Ethernet1 on Router-Lab. Next, **ping** each of the serial interfaces on Router-Lab. If you find any ping failure on the serial lines, refer to serial debugging as discussed in the "Troubleshooting Serial Line Problems" chapter and to the additional information provided in the "Troubleshooting Router Startup Problems" chapter.

Step 5 If you determine that the problem is indeed one of congestion because of bandwidth overutilization, you must decide whether it is more effective to add bandwidth (in the form of another serial circuit) or to adjust the router configuration.

Step 6 If you see load values of about 50 percent and high numbers of input errors and output drops, consider implementing priority queuing to force Telnet to be given higher precedence over other packet types. Priority queuing helps ensure reasonable connection service to users, even during periods when file transfers are taking place. Figure 14-11 illustrates a configuration for Router-Lab that establishes priority queuing and assigns port 23 (Telnet) a higher priority than other TCP/IP protocols, such as mail (port 25).

Figure 14-11 Configuration Showing Priority Queuing Specification

```
priority-list 4 protocol ip medium tcp 23
!
interface serial 2
ip-address 131.108.155.21 255.255.255.0
priority-group 4
!
interface serial 3
ip-address 131.108.156.22 255.255.255.0
priority-group 4
```

S2442

Note One reason why Telnet traffic can be bumped from the buffer queues is the tendency of larger FTP packet types to collect in buffers. When FTP traffic is high, the smaller Telnet packets are squeezed out of the output queues, resulting in retransmissions, session timeouts, and generally slower connection performance. Priority queuing can relieve marginal cases of this kind.

Step 7 If you see a consistent load of close to 90 percent, as well as input errors and output drops, priority queuing is not likely to help. With consistently high congestion, the best solution is additional or faster serial links.

Problem Solution Summary

This scenario focused on the following performance problems in TCP/IP internetworks:

- Isolating problem nodes and eliminating potential problems using extended **ping** tests
- Determining when to enable priority queuing and when to add bandwidth
- Specifying priority queuing to force the router to give a specific TCP/IP socket a higher priority than other protocols

Slow Host Response over a 56-kbps HDLC Link

When designing and implementing internetworks, it is important to factor in any potential changes and expectations of growth. This is especially important when certain network elements are at risk of becoming bottlenecks—such as point-to-point serial links. Bandwidth that appears to be sufficient today may be inadequate in a year. And the budget may not exist to add another drop or replace the existing service. This scenario explores a situation in which a router can be used to improve performance over a serial link that does not meet user requirements.

Symptoms

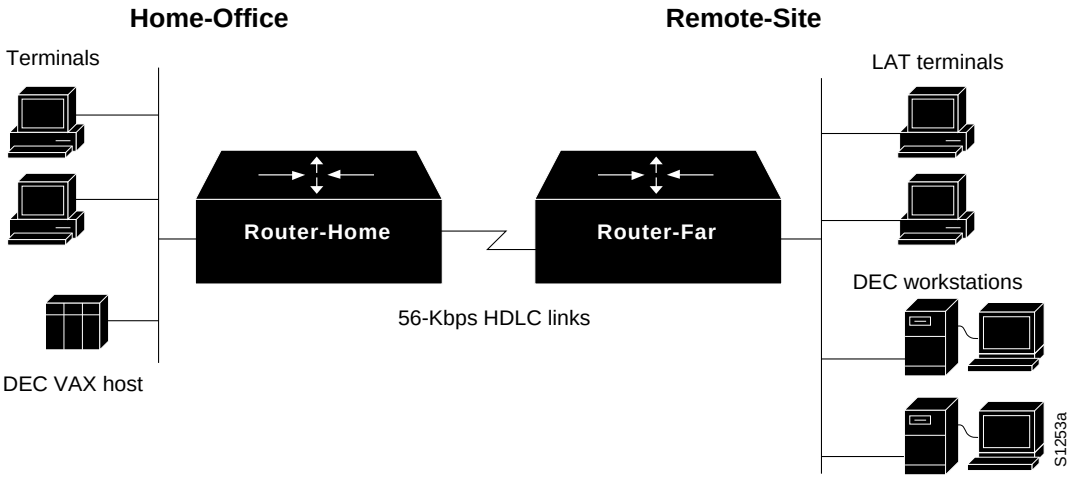
Users at a remote site complain of consistently degraded performance when they connect to hosts at the home office. Performance previously was acceptable, but now slows substantially during peak use periods.

Environment Description

Figure 14-12 shows a map of the environment for this scenario. The following characteristics represent the relevant elements of this internetwork:

- A single remote sales office (Remote-Site) is linked to the corporate network (Home-Office) over a 56-kbps HDLC line.
- Two routers (Router-Home and Router-Far) join the two sites over a 56-kbps link. The local router attachment is to a CSU/DSU using a V.35 cable.
- LANs implemented are IEEE 802.3 Ethernets.
- DEC workstations and various ASCII terminals are used at the Remote-Site. Traffic to the Home-Office consists of file transfers, virtual terminal connections, and electronic mail.
- Native DECnet is routed over the point-to-point link, while DEC local-area transport (LAT) protocol is the sole protocol being bridged.
- In this situation, the observed level of traffic is very high on the serial link. Spikes of 80 to 90 percent of bandwidth are commonly detected.

Figure 14-12 Scenario Map for a 56-kbps Point-to-Point Performance Problem



Diagnosing and Isolating Problem Causes

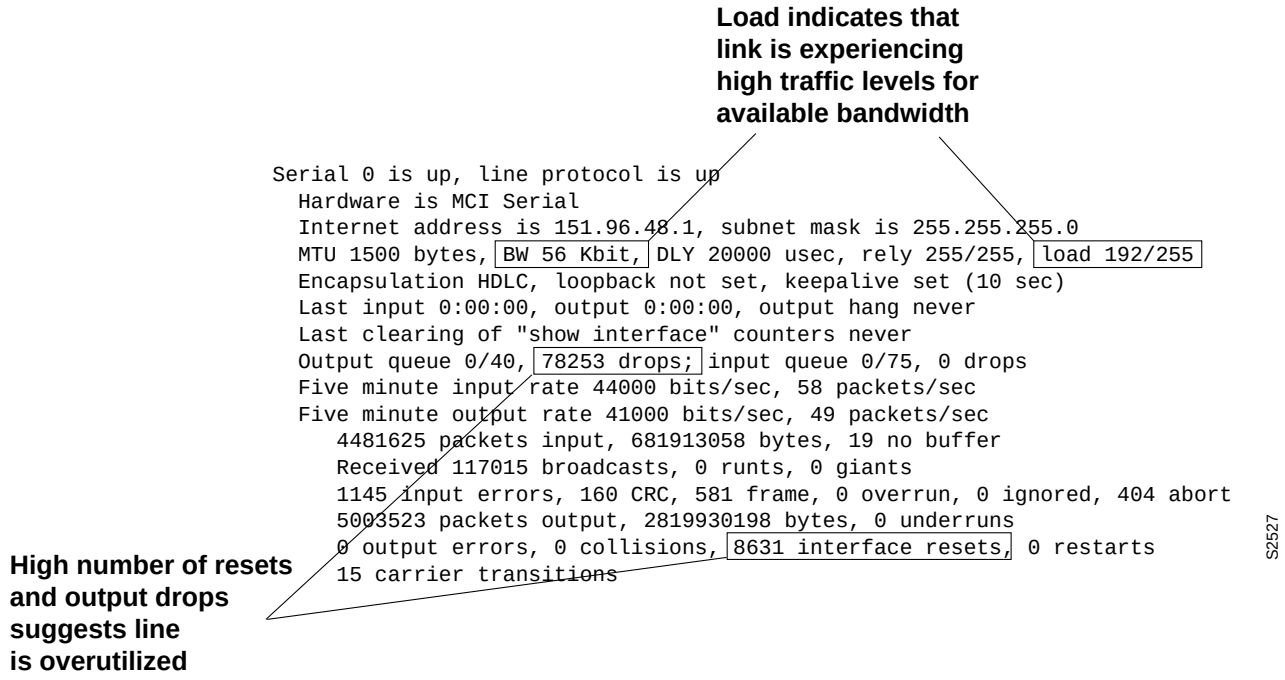
Given the situation, the following problems are the best candidates for poor performance:

- Bad serial line
- Overutilized serial line
- Interface card out of buffers
- Misconfigured hosts

The following procedure illustrates the process of investigating potential hardware problems:

Step 1 Use the **show interfaces serial** EXEC command to determine the condition of the serial line. Figure 14-13 shows output indicating that the interfaces are minimally operational and the that router can communicate with them.

Figure 14-13 show interfaces serial Command Output



Of interest in this display is the fact that the value for input errors is relatively low, but the values for interface resets and output drops are both high. Another clue is that the load field indicates that the link is experiencing a load of about 75 percent of available bandwidth (the value is shown as a “percentage” of 255, such that a link seeing one third utilization (33/100) would have a load value of 85/255). This information combines to suggest that the serial line is functional but is being overutilized.

Note The value displayed in the load field is based on a 5-minute weighted average of traffic activity on the interface. This means that all traffic values for the last 5 minutes are taken into account, but the more recent values are weighted more heavily. Large fluctuations in this number over time usually indicate that the interface is experiencing periodic congestion, which is common on low-speed interfaces.

Note that the value shown in the load field is based on the figure shown in the BW (bandwidth) field on the same line. The BW field normally displays a default value (typically 56 or 1544 kbps) that correlates to the type of interface. If you know that the amount of bandwidth actually available differs from the default value, and you want the load to be calculated more accurately, use the **bandwidth** interface configuration command to change the BW value.

To monitor changes in the number of dropped packets, follow these steps:

Step 1 Obtain the **show interfaces serial** EXEC command output. (See Figure 14-13.)

Step 2 Write down the number of output drops. (See Figure 14-13.)

Step 3 Use the **clear counters** privileged EXEC command to reset counters on the target interface.

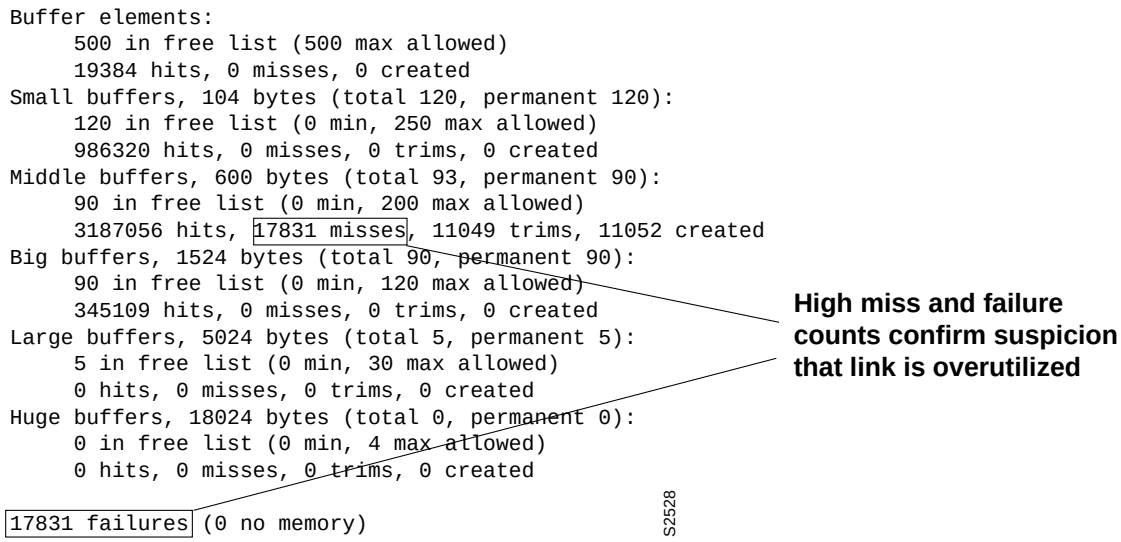
Step 4 Check the change to the output drops field in an hour; if the value is around 1000 or more, the link is probably overutilized.

Note The DECnet protocol is particularly sensitive to drops. If your internetwork involves handling of DECnet traffic, you must ensure that drops are eliminated.

To further confirm that the serial link is overutilized, use the **show buffers** EXEC command. Figure 14-14 illustrates the output from this command. In this example, there are a large number of failures and misses, which suggests a problem with the system-level buffers, and that the router is trying to transmit traffic that exceeds the interface bandwidth.

Note An interface reset on one end of a serial link causes aborts on the other end; these appear as input errors (as well as aborts). This is why it is essential to inspect both ends of the serial link (using the **show interfaces** EXEC command).

Figure 14-14 show buffers Command Output



Step 5 Next, look at the router configuration files for clues. If fast switching is *not* explicitly disabled for all protocols, disable fast switching, which is enabled by default. For DECnet, use the **no decnet route-cache** interface configuration command to disable fast switching. This change forces the router to use system-level memory buffers (instead of board-level buffers), which, under certain conditions, can improve overall throughput.

Step 6 Although disabling fast switching can improve performance over the serial link, assume that problems still persist during peak demand times. The next step is to prioritize traffic using the priority queuing function. By assigning a high priority to bridged (LAT) packets, the LAT traffic takes precedence over any other traffic. Again, this enhances performance, but might not entirely eliminate peak period sluggishness.

Step 7 Tune system buffers. By setting a minimum number of system buffers as available at all times, you can significantly reduce the bottleneck at the serial link.

Figure 14-15 illustrates a complete configuration listing for Router-Home (obtained using the **write terminal** privileged EXEC command) that includes the changes suggested in Steps 2 through 4.

Note When customizing buffer settings, you must carefully match the buffer specifications with the hold-queue limits. For more information about managing buffers and specifying hold-queue limits, refer to the "Troubleshooting Serial Line Problems" chapter.

Figure 14-15 Complete Configuration Showing Changes Needed to Improve Performance over a 56-kbps Line

```
buffers small min-free 20
buffers middle min-free 20
buffers big min-free 5
buffers small max-free 300
buffers middle max-free 400
!
!
decnet routing 21.12
decnet node area
decnet max-address 1023
!
!
interface ethernet 0
ip address 129.14.87.123 255.255.255.0
decnet cost 5
bridge-group 1
!
interface serial 0
ip address 151.96.48.1 255.255.255.0
no ip route-cache
decnet cost 20
no decnet route-cache
bridge-group 1
priority-group 1
!
!
router igrp 109
network 129.14.0.0
network 151.96.0.0
!
!
!
ip name-server 255.255.255.255
snmp-server community
snmp-server community public RO
hostname Router-Home
scheduler-interval 1500
bridge 1 protocol dec
!
priority-list 1 protocol bridge high list 201
priority-list 1 protocol decnet medium
priority-list 1 protocol ip normal
priority-list 1 queue-limit 40 40 20 10
!
!
access-list 201 permit 0x6004 0x0000
!
!
end
```

S2445

Problem Solution Summary

This scenario revolved around an interface that was overworked. The immediate reaction to this situation might be to add another link in parallel. Ultimately, adding bandwidth is probably required. But that might not be an immediately available option. Perhaps the protocol being used cannot handle load balancing, or you simply cannot afford the added expense of another physical link in your current budget.

The actions offered in this example explore options that use the existing physical configuration, but reconfigure the way traffic is handled. The following modifications can help optimize traffic over an overloaded 56-kbps link:

- Disabling fast switching.
- Enabling priority queuing for bridged (LAT) traffic. Note that the configuration in Figure 14-15 includes an access list that permits bridging of LAT packets, but blocks bridging of any other packets.

  The configuration also shows specific queue depths for high, medium, normal, and low priority packets. If you implement priority queuing, try these as a starting point. Your actual implementation will take some tuning. With LAT, reducing the number of drops will improve performance; however, avoid assigning arbitrarily large queue limits, because there can be performance side effects. Excessively large queues can cause timing problems when packets are buffered for too long a time.

  As you tune the **queue-limit** values assigned in the **priority-list** global configuration command, check the interface activity with the **show interfaces** EXEC command to monitor the number of drops. A typical **queue-limit** value for the high-priority packets is 50.

  This solution is particularly applicable to situations involving routing of DECnet traffic and bridging of LAT traffic. Set DECnet queues to 100 to help prevent drops if necessary.
- Tuning system buffers.

Note If an interface is dropping packets at a traffic load near or approaching100 percent (255/255 load), you must add bandwidth in the form of another line or a higher-capacity line.

Slow XNS Performance over Ethernet Backbone

This scenario illustrates a situation in which performance is extremely slow over an Ethernet backbone that separates two routers.

Symptoms

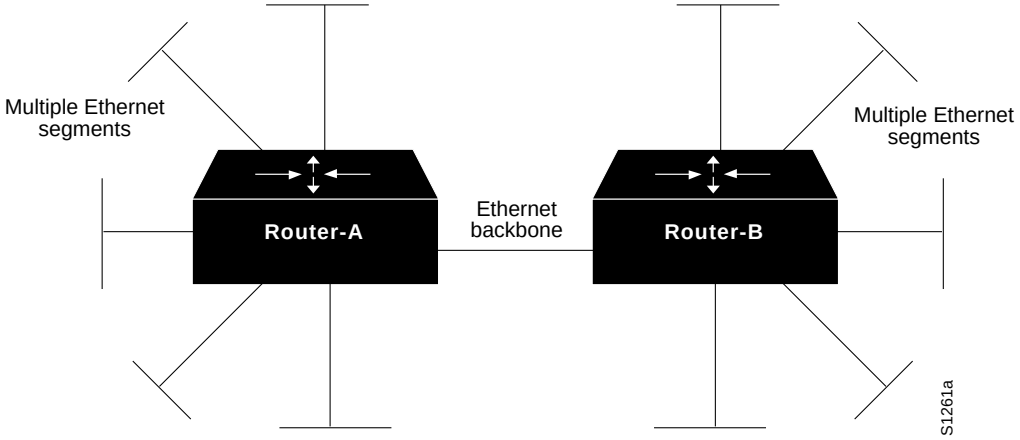
Slow server response among multiple Ethernet segments separated by two routers and an Ethernet backbone.

Environment Description

Figure 14-16 shows a map of the environment for this scenario. The following characteristics represent the relevant elements of this internetwork:

- Router-A and Router-B interconnect multiple Ethernets over an Ethernet backbone.
- LANs are IEEE 802.3 Ethernets.
- XNS is the only protocol being routed.

Figure 14-16 XNS Routers Joining Ethernets over Ethernet Backbone



Diagnosing and Isolating Problem Causes

Congestion is the best candidate for poor performance over the backbone. You can use the following two methods to determine whether the backbone has a congestion problem:

- Issue the **show interfaces** EXEC command and examine the output for relative load, increasingly high levels of input errors, and drops.
- Attach a network analyzer to the backbone and look for high levels of collisions, and bandwidth utilization in excess of 30 percent.

For information about general troubleshooting of performance problems in a routed internetwork, refer to the section "Slow Host Response over a 56-kbps HDLC Link," earlier in this chapter. For more information about diagnosing congestion problems, refer to the "Troubleshooting WAN Connectivity" and the "Troubleshooting Internetwork Performance" chapters.

If you do determine that congestion over the Ethernet backbone is high, the only option is to increase bandwidth. You can do this by either adding additional Ethernet segments or by replacing the Ethernet backbone with a faster media, such as FDDI.

Problem Solution Summary

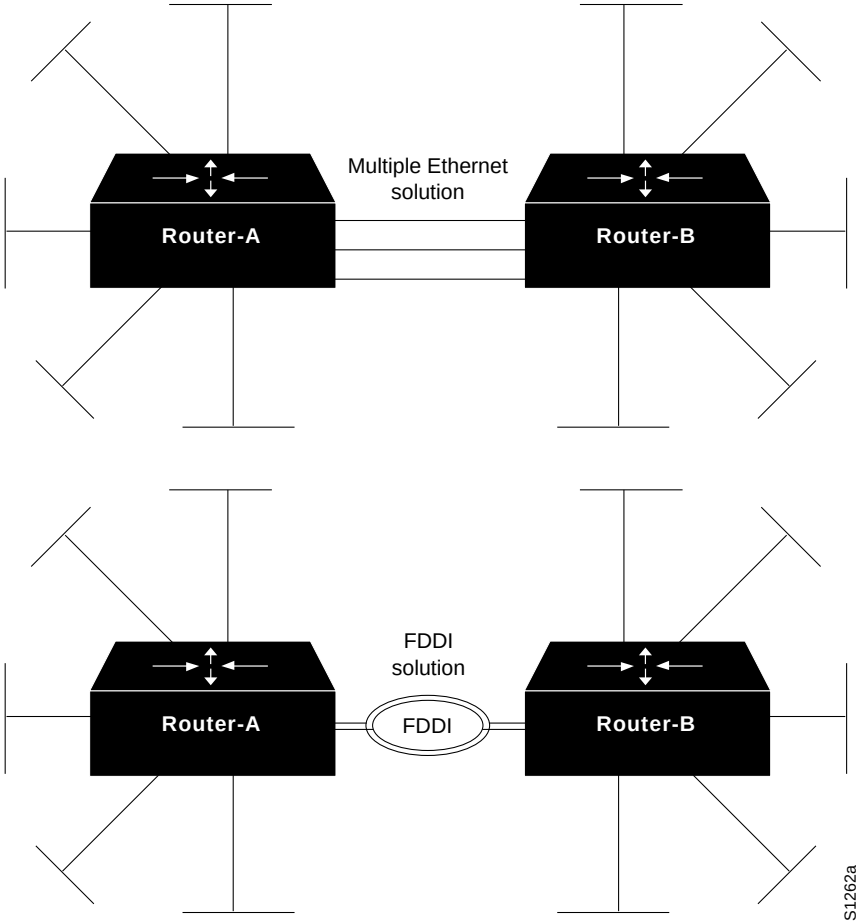
This scenario focused on improving performance over a backbone segmenting multiple Ethernets by increasing bandwidth using one of two options:

- Replacing the single Ethernet backbone with multiple Ethernet segments
- Replacing the single Ethernet backbone with an FDDI backbone

Figure 14-17 illustrates these options.

Note If you adopt a multiple Ethernet option, remember to implement the **xns maximum-paths** global configuration command. For more information about this requirement, refer to the beginning of the section "Slow XNS Performance over Equal Parallel Links," earlier in this chapter. Also note that each segment must have its own network address. For more information about duplicate network number problems, refer to the "Troubleshooting XNS Connectivity" chapter.

Figure 14-17 Alternative Solutions to Ethernet Backbone Bottleneck in XNS Network



Slow XNS Performance over Equal Parallel Links

This scenario illustrates a situation in which performance is less than optimal over parallel T1 links joining two routers.

Symptoms

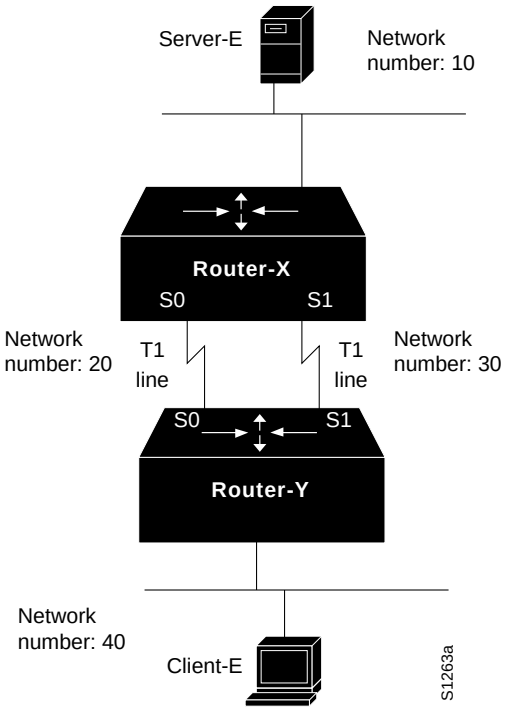
One line appears to be heavily loaded, while the other is either idling or indicates very low load. Users complain of slow response and intermittent connection drops.

Environment Description

Figure 14-18 shows a map of the environment for this scenario. The following characteristics represent the relevant elements of this internetwork:

- Router-X and Router-Y interconnect two sites over parallel T1 lines running at 1.544 Mbps.
- Client-E needs to access Server-E on the other side of the serial interconnections.
- LANs are IEEE 802.3 Ethernets.
- XNS is the only protocol being routed.

Figure 14-18 Router Joining XNS Networks over Parallel T1 Lines



Diagnosing and Isolating Problem Causes

A likely cause for poor performance over parallel serial lines is that the router is keeping only one routing table entry per target network. In the worst case, traffic is only routed through one line, while the second line is idle.

Use the following procedure to determine whether traffic is being unevenly distributed between the parallel lines:

Step 1 Issue the **show interfaces** EXEC command and examine the load for each interface. Also examine the number of input and output drops and the 5-minute output and input packet counts. Record the observed values.

Step 2 Use the **clear counters** privileged EXEC command and continue to monitor changes in the counters over time with the **show interfaces** EXEC command.

Step 3 Look for values that are substantially uneven. (For example, interface serial 0 indicates 500 packets total input, while interface serial 1 indicates 10.)

Step 4 If you determine that traffic is unevenly distributed over the serial links, use the **xns maximum-paths** global configuration command to set the number of multiple paths for the routers to use when transmitting traffic to any particular destination. Instead of keeping only one routing table entry, each router will use up to the specified number of paths when it determines how to route traffic. In essence, the **xns maximum-paths** global configuration command forces load balancing over two lines when the number of paths is specified as 2.

Note This problem is the same for any parallel media. Therefore, the suggested solution would be the same for parallel FDDI, Ethernet, or Token Ring links, as well as for parallel serial interconnections.

Problem Solution Summary

This scenario focused on improving performance over parallel links. The recommended solution is to implement the **xns maximum-paths** global configuration command on the routers with the number of paths specified as 2.

Slow XNS Performance over Unequal Parallel Links

This scenario illustrates a situation in which performance is slow over parallel links of differing speeds that join two routers.

Symptoms

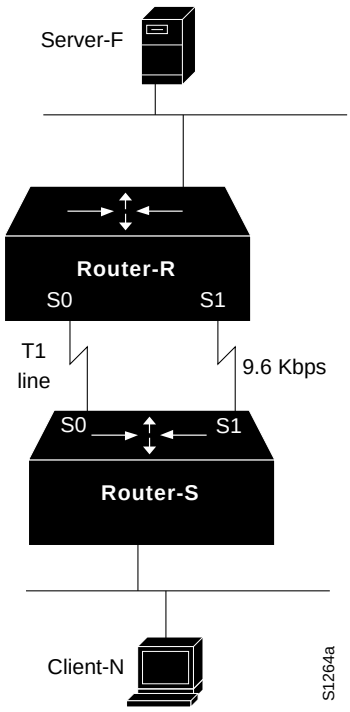
One line appears to be heavily loaded, while the other is either idling or indicates very low load. Users complain of slow response and intermittent connection drops.

Environment Description

Figure 14-19 shows a map of the environment for this scenario. The following characteristics represent the relevant elements of this internetwork:

- Router-R and Router-S interconnect two sites over parallel lines with one line running at T1 speed (1.544 Mbps) and the other line running at 9.6 kbps.
- **xns maximum-paths** global configuration command is enabled on both routers.
- Client-N needs to access Server-F on the other side of the serial interconnections.
- LANs are IEEE 802.3 Ethernets.
- XNS is the only protocol being routed.

Figure 14-19 Router Joining XNS Networks over Unequal Parallel Lines



Diagnosing and Isolating Problem Causes

Because the XNS RIP routing protocol does not take line speed into consideration, the load cannot be balanced effectively between the two links. Lack of load balancing is probably causing poor performance over the parallel serial lines. It is quite possible that traffic is only being routed through one line, while the second line is idle. Because RIP does not consider line speed, the 9.6-kbps line could be completely overwhelmed, while the T1 line is relatively unused.

You can use the following procedure to determine whether traffic is being unevenly distributed between the parallel lines:

Step 1 Issue the **show interfaces** EXEC command and examine the displayed load for each interface. Also examine the number of input and output drops and the 5-minute output and input packet counts. Record the observed values.

Step 2 Use the **clear counters** privileged EXEC command and continue to monitor changes in the counters over time with the **show interfaces** EXEC command.

Step 3 Look for values that are substantially uneven. (For example, interface serial 0 indicates 10 packets total input, while interface serial 1 indicates 500.)

Step 4 If you determine that traffic is being unevenly distributed over the serial links, and the **xns maximum-paths** *paths* global configuration command is already implemented, you can make the speed on both lines match, or you can eliminate the slow-speed line altogether.

Note This problem is the same for any differing parallel media. Therefore, the suggested solution would be the same for unevenly matched FDDI, Ethernet, or Token Ring links, as well as for uneven parallel serial interconnections.

Problem Solution Summary

This scenario focused on improving performance over uneven parallel links. The recommended solution is to force the speed of the parallel links to match or to eliminate the slow-speed link.

CHAPTER 15

Troubleshooting Internetwork Performance

This chapter focuses on common symptoms associated with poor performance in internetworks, possible causes of those symptoms, and general suggestions for identifying, isolating, and resolving problem causes. The symptom modules in this chapter pertain to performance-related problems for the various protocols and technologies addressed in this publication.

Performance symptoms discussed in this chapter include the following:

- Sporadic Service Availability and Poor AppleTalk Internetwork Performance
- Poor Bridging Performance over Serial Lines or LANs
- Poor DECnet Performance over Serial Lines or LANs
- Slow Performance and Intermittent Loss of Connections over RSRB
- Slow Performance over ISO CLNS
- Poor Novell Server Performance over Router in an IPX LAN Internetwork
- Poor Novell Server Performance over Router in a WAN
- Slow Performance in TCP/IP Internetworks
- Slow TCP/IP Performance Despite Multiple Paths
- Slow Host or Network Response over a WAN or Serial Link
- Dropped Connections over a WAN or Serial Link
- Poor XNS Server Performance over Router in a LAN Internetwork
- Poor XNS Server Performance over Router in a WAN
- Switching-Support Matrices

Sporadic Service Availability and Poor AppleTalk Internetwork Performance

Symptom: Connectivity to AppleTalk services over an internetwork is unpredictable and generally slow. Table 15-1 outlines possible causes and suggested actions when service availability is unpredictable and performance is slow on an AppleTalk internetwork.

Table 15-1 AppleTalk: Sporadic Service Availability and Poor Performance

Possible Causes	Suggested Actions
ZIP storm	**Step 1** Examine the output of the **show appletalk traffic** EXEC command to determine the number of ZIP requests being sent; repeat after 30 seconds.
	Step 2 If the number of ZIP requests is greater than 10 and increasing, a ZIP storm is probably occurring.
	Step 3 Use the **show appletalk route** EXEC command to see whether there is a network that is described as having "no zone set." If you find such a network, a node in that network is probably not responding to ZIP requests, which results in a ZIP storm.
	Step 4 Determine why the node is not responding to ZIP requests.
Duplicate network numbers	**Step 1** The network that exhibits this symptom is likely to contain duplicate network numbers equidistant from the point at which problems are observed. Either change the network number of the afflicted network or remove AppleTalk from the associated interface. In either case, the original network number associated with the interface should disappear from the internetwork within a few minutes. If it persists, you probably have found the duplicate network.
	Step 2 If you changed the network number on the interface, no further action is required. If not, change it now (making sure it is unique). Remember to reenter the zone name and any other interface configurations for AppleTalk on that interface.
Unexpected back door	**Step 1** Inspect the internetwork for any bridges that may link networks that are routing AppleTalk.
	Step 2 If any bridges (including routers configured for bridging) are found, set all bridges to forward nonrouted protocols and filter routed protocols.
	Step 3 Use the **show appletalk route** and **show interfaces** EXEC commands to monitor routes and neighbors.
	Step 4 If networks continue to be associated with the wrong interfaces, consult your router technical support representative for more assistance.

Poor Bridging Performance over Serial Lines or LANs

Symptom: Users complain of slow host response and dropped connections. Bridging traffic itself might not be heavy, but links also might be routing other protocols. Measurable symptoms include input and output drops, increasing 5-minute input/output rates, and unusually high increases in collision counts. Table 15-2 outlines possible causes and suggested actions when bridging performance is poor over WAN links.

Table 15-2 Bridging: Poor Performance over Serial or WAN Links

Possible Causes	Suggested Actions
Overutilized serial line bandwidth	**Step 1** Use **the show interfaces** EXEC command to determine whether output drops are occurring; check the output for high values in the 5-minute input and output packet rate fields. If any output drops are found, bandwidth is probably insufficient. If the input and output rates indicate values close to the media maximum throughput for the line, the line is saturated. **Step 2** Use bridging filters to reduce traffic. **Step 3** If local-area transport (LAT) is being bridged and the problem persists, try LAT compression. **Step 4** Increase bandwidth or add parallel lines (combined with the **bridge-group** *group* **circuit** *number* interface configuration command) to increase available bandwidth.
Excessive traffic on LAN	**Step 1** Use the **show interfaces** EXEC command to determine whether output drops are occurring; check the 5-minute input and output packet rate for unusually high values; see if the collision counter is incrementing at a high rate. If any output drops are found, bandwidth is probably insufficient. Collisions and unusually high 5-minute input and output rates also indicate that the media is saturated. **Step 2** Segment the network using internetworking devices (either routers or bridges, depending on your network and the situation). **Step 3** Implement bridging filters to prevent unnecessary traffic from flooding local segments.
Unstable media, or network device has hardware problem	**Step 1** Use the **show interfaces** EXEC command to determine whether interface resets are occurring or whether transition counters are incrementing. **Step 2** Check the physical connections of all suspect devices; check modems for proper attachment and functionality; check for noisy lines; check appliques and other router or bridge hardware. Refer to the media and hardware troubleshooting discussions in the “Troubleshooting Router Startup Problems” and the “Troubleshooting Serial Line Problems” chapters. **Step 3** Remove and replace defective network interface cards or other devices.

Poor DECnet Performance over Serial Lines or LANs

Symptom: Users complain of slow host response and dropped connections. Table 15-3 outlines possible causes and suggested actions when DECnet performance is poor over serial lines or LAN.

Table 15-3 DECnet: Poor Performance over Serial Lines or LANs

Possible Causes	Suggested Actions
Overutilized bandwidth	**Step 1** Use the **show interfaces** EXEC command to determine whether input and output queues are full. **Step 2** Use the **show decnet traffic** EXEC command to determine whether packets are being received and forwarded. If the number of received packets is greater than the number of forwarded packets and if the queues are full, congestion is probably the problem. **Step 3** To reduce traffic overhead, increase hello timer or update timers to the same value on all routers in the network. **Step 4** Implement the priority queuing and buffer changes described in the section "Slow Host or Network Response over a WAN or Serial Link" later in this chapter.
Network device has hardware problem and is sending out large amounts of incorrect data over LAN	**Step 1** Use a LAN traffic monitor to collect information about the amount and type of data transferred from and received by each node in the network for a period of time. **Step 2** Compare data from all systems. **Step 3** Use a network analyzer (or perform a binary search) to isolate the problem nodes that are generating excessive data. **Step 4** Remove and replace defective network interface cards or devices.

Slow Performance and Intermittent Loss of Connections over RSRB

Symptom: Users complain about connection loss at peak traffic periods when trying to connect to resources on the other side of a router configured for remote source-route bridging (RSRB). Table 15-4 outlines a possible cause and suggested actions when performance is slow and connectivity is intermittent over RSRB connections.

Table 15-4 Bridging: Slow Performance and Intermittent Loss of Connections over RSRB

Possible Cause	Suggested Actions
Busy router; high CPU utilization when using TCP encapsulation	**Step 1** Use the **show processes** EXEC command to determine CPU utilization. Look for CPU utilization higher than 50 percent. High CPU utilization can cause RSRB sessions to time out when TCP encapsulation is used. **Step 2** Check the configuration for the **local-ack** keyword in the **source-bridge remote-peer** global configuration command. **Step 3** If it is missing, add the **local-ack** keyword. **Step 4** Consider using the **source-bridge fst-peername** global configuration command to implement fast sequenced transport (FST) on the link.

Slow Performance over ISO CLNS

Symptom: Users complain about poor performance and slow response in a large ISO Connectionless Network Service (CLNS) network. Table 15-5 lists possible causes and suggested actions when performance is slow over an ISO CLNS network.

Table 15-5 ISO CLNS: Slow Performance over ISO CLNS Network

Possible Causes	Suggested Actions
Busy router; duplicate routing updates; congested network	**Step 1** Use the **show processes** EXEC command to see CPU utilization. Look for CPU utilization higher than 50 percent. **Step 2** Check the configuration for multiple ISO-Interior Gateway Routing Protocol (IGRP) processes configured on a single interface. Multiple ISO-IGRP processes on a single interface cause different Level 2 routing updates to be sent out on the interface. In a large network, the additional bandwidth of these unnecessary updates can degrade performance. **Step 3** In the router configuration, remove all but one IGRP routing process per interface.
Multihomed area is too large; busy router	**Step 1** Use the **write terminal** privileged EXEC command to look for the assignment of multiple area addresses. **Step 2** Use the **show clns routes** and **show clns neighbors** EXEC commands (for ISO-IGRP) or **show isis database** EXEC command (for Intermediate System-to-Intermediate System [IS-IS]) to display areas and routes. **Step 3** Verify that your network topology does not extend multihomed areas farther than necessary. When an area extends farther than necessary, Level 1 traffic increases. The additional packet processing can degrade performance. **Step 4** Reconfigure the areas as required.

Poor Novell Server Performance over Router in an IPX LAN Internetwork

Symptom: Users complain that sessions drop at peak traffic periods when they are trying to connect to resources on the other side of a router configured to route Novell Internetwork Packet Exchange (IPX). Table 15-6 outlines possible causes and suggested actions when a Novell server performs poorly over a router in a Novell IPX LAN internetwork.

Table 15-6 IPX: Poor Novell Server Performance over Router in an IPX LAN Internetwork

Possible Causes	Suggested Actions
Excessive traffic; collisions causing session drops (Ethernet problem only)	**Step 1** Use a protocol analyzer to look for collisions in excess of normal acceptable conditions (varies for specific site). As an alternative, use the **show interfaces** EXEC command to get a rough estimate of the collision count. **Step 2** Examine the protocol analyzer output to determine bandwidth utilization. The protocol analyzer output will provide the most accurate reading of dynamic traffic information. As an alternative, you can run the Novell **load monitor** command at a server console to get an approximate idea of bandwidth utilization. If bandwidth utilization detected by the analyzer averages 15 to 20 percent or higher, you are likely to have a load-related performance problem. **Step 3** If you see that collisions are increasing steadily with a higher-than-expected bandwidth utilization, consider segmenting the network with additional bridges or routers.
Insufficient bandwidth on Token Ring to handle traffic	**Step 1** Upgrade from 4- to 16-Mbps Token Ring throughout the network. **Step 2** If performance is still inadequate, consider segmenting the network with additional bridges or routers.

Poor Novell Server Performance over Router in a WAN

Symptom: Users complain about sessions dropping at peak traffic periods when trying to connect to resources on the other side of a router configured to route Novell IPX over a WAN or serial link. Table 15-7 outlines a possible cause and suggested actions when a Novell server performs poorly over a router in a Novell IPX WAN internetwork.

Table 15-7 IPX: Poor Novell Server Performance over Router in an IPX WAN Internetwork

Possible Cause	Suggested Actions
Other protocol dominates CPU time	**Step 1** Use the **show processes** EXEC command to look for large numbers appearing in the Runtime (ms) and Invoked fields for certain protocols. A protocol that has a value that is 10 times or greater than the value indicated for Novell traffic is a likely suspect. When this kind of condition exists, Novell traffic is not getting adequate access to the CPU, and performance is affected. **Step 2** Use the **show interfaces** EXEC command to look for a high level of output drops. **Step 3** If you see output drops, and another protocol is dominating CPU time (indicated in the **show processes** Runtime (ms) field), use priority queuing to force the router to give priority to Novell traffic. More information about priority queuing is provided in the "Troubleshooting Serial Line Problems" chapter. **Step 4** If priority queuing does not improve performance, add bandwidth by implementing a higher-speed line or by adding additional lines of the same speed. If you add additional lines, use the **ipx maximum-paths** global configuration command to specify the number of paths.

Slow Performance in TCP/IP Internetworks

Symptom: TCP/IP internetwork performance is slow, with poor host response, spotty connection service, and generally slow file transfers. Packets might be dropped. Table 15-8 outlines possible causes and suggested actions when performance is slow in a TCP/IP internetwork.

Table 15-8 TCP/IP: Slow Performance in TCP/IP Internetworks

Possible Causes	Suggested Actions
Bad network link, which results in dropped or lost packets	**Step 1** Issue the **ping** command along entire length of the path to determine where packets are being dropped. **Step 2** Perform serial debugging or other media debugging. For media and hardware diagnostic information, refer to the "Troubleshooting Router Startup Problems" chapter. For more specific information about serial debugging, refer to the "Troubleshooting Serial Line Problems" chapter. **Step 3** Replace hardware or add bandwidth as necessary.
Access list applied to one link, but not another (when there are multiple paths to a destination)	**Step 1** Refer to the section "Slow TCP/IP Performance Despite Multiple Paths" later in this chapter.
Congested link	**Step 1** Determine whether the link is indeed congested. For media and hardware diagnostic information, refer to the "Troubleshooting Router Startup Problems" chapter. For more specific information about serial debugging, refer to the "Troubleshooting Serial Line Problems" chapter. **Step 2** Apply priority queuing if feasible. **Step 3** If you cannot implement priority queuing or if priority queuing does not help, add bandwidth or additional routers.

Slow TCP/IP Performance Despite Multiple Paths

Symptom: Despite multiple paths from one network to another and apparently sufficient bandwidth, performance over the links is poor, and traffic does not appear to be getting through some of the links. Although this can be considered a connectivity problem, it manifests itself as a performance issue. Table 15-9 outlines possible causes and suggested actions when TCP/IP performance is slow despite multiple paths.

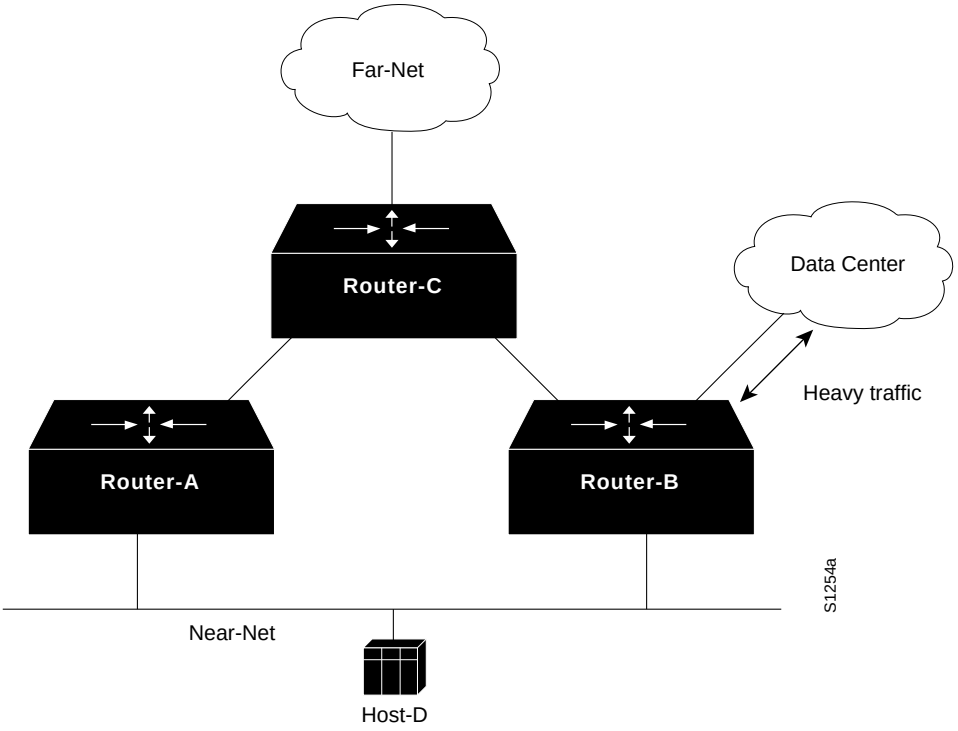
Table 15-9 TCP/IP: Slow TCP/IP Performance Despite Multiple Paths

Possible Causes	Suggested Actions
Misconfigured access lists where multiple paths and one or more access lists block access to one or more routes	**Step 1** Use the **ping** and **trace** EXEC commands to determine where traffic is stopping. This procedure works best when standard access lists are used. **Step 2** If ping or trace packets are stopped along the way, check the specific router for access lists. **Step 3** If an access list is found, disable the list and monitor traffic through the router, using the **ping** and **trace** EXEC commands. **Step 4** If ping and trace packets get through after removing the access list, you might need to add explicit permit statements to the access list to allow the blocked traffic type. If extended access lists are specified, ping and trace packets might get through, even though intended traffic is not getting through. **Step 5** If ping packets get through, attach a network analyzer along the path where problems occur to see where the dropped packet type was last seen. The next node is the most likely suspect. **Step 6** Remove any access list, use the protocol being blocked, and monitor traffic through the router.
Bad interface or media hardware	**Step 1** For media and hardware diagnostic information, refer to the "Troubleshooting Router Startup Problems" chapter. For more information about serial debugging, refer to the "Troubleshooting Serial Line Problems" chapter. **Step 2** Perform serial debugging or other media debugging. **Step 3** Replace hardware or add bandwidth as necessary.
Load balancing problem (see Figure 15-1, following this table)	**Step 1** Use the **show interfaces** and **show ip traffic** EXEC commands and **ping** out to the destination to determine where traffic is being dropped. **Step 2** At the point of congestion, relieve traffic problems by adding a router in parallel or by increasing the bandwidth of the link. **Step 3** If you cannot add a router or bandwidth, try adjusting the hop count on the congested router. This is done using the **offset-list** router configuration command to add a hop to a route received from a particular router. **Step 4** Use the **distance** router configuration command to set the administrative distance for a particularly slow route.

Load Balancing Problem Example

Figure 15-1 illustrates a situation where two routes might be equivalent in terms of hop count from Host-D to Far-Net, but due to the level of traffic (associated with Router-B and the Data Center), the route through Router-A is administratively preferred. In this case, both routes look equally good to Host-D, so without any configuration modifications, Host-D can use either Router-A or Router-B to communicate with Far-Net. However, as outlined in the load balancing problem discussion in Table 15-9, several options are available to force traffic from Host-D (intended for Far-Net) to go through Router-A.

Figure 15-1 Load Balancing Problem Map



Slow Host or Network Response over a WAN or Serial Link

Symptom: As with similar loss of connection problems, users complain about very slow host and network responsiveness at peak traffic periods over a WAN or serial link.

Obtain the following information when troubleshooting load-related connection problems:

- Observe the output of the **show interfaces serial** EXEC command on both ends of the serial line, and evaluate error counters.
- If you see input errors, refer to the section "Evaluating Input Errors" in the "Troubleshooting Serial Line Problems" chapter for details about isolating the sources of input errors.

Table 15-10 outlines possible causes and suggested actions when host or network response is slow over a WAN or serial link.

Table 15-10 WAN: Slow Host or Network Response over a WAN or Serial Link

Possible Causes	Suggested Actions
Noisy serial line	**Step 1** Use the **show interfaces serial** EXEC command to determine whether input errors are increasing. **Step 2** If input errors appear and are increasing, diagnose the serial line as described in the "Troubleshooting Serial Line Problems" chapter.
Overutilized bandwidth	**Step 1** Use the **show interfaces serial** EXEC command to determine whether input errors are increasing. **Step 2** If input errors do not appear, the problem is related to congestion. **Step 3** Turn off fast switching on the affected interface. **Step 4** Check the applications that are being run, especially for very large file transfers scheduled at particular times of day. **Step 5** If large transfers occur, set up priority queuing. (Priority queuing requires that the protocol allow flow control.) **Step 6** Rearrange the timing of file transfers so that links are not overused during normal business hours. **Step 7** Add bandwidth and consider using dial backup over the new link for applications that are taking excessive bandwidth on existing links. **Step 8** Adjust buffer size. For details, see the section "Adjusting Buffers to Ease Overutilized Serial Links," in the "Troubleshooting Serial Line Problems" chapter.
Hardware in the serial link is unreliable	**Step 1** Use a serial analyzer to troubleshoot the serial line or perform the tests described in the sections "Using Extended ping Tests to Troubleshoot Serial Lines" and "CSU and DSU Loopback Tests" in the "Troubleshooting Serial Line Problems" chapter. **Step 2** Replace hardware as necessary.
Carrier is automatically rerouting T1 trunk lines	**Step 1** Contact the long-line carrier service to determine whether rerouting is occurring. **Step 2** Ensure that the carrier provides a dedicated circuit if automatic switching is causing performance problems.

Dropped Connections over a WAN or Serial Link

Symptom: Users complain about dropped connections and the inability to make host connections at peak traffic periods. One example of this problem is in an environment that features bridged DEC LAT traffic and multiple routed protocols. Data entry input (or other application requests) from users might be getting buffered at the end of an already long input queue and eventually one end of the connection times out. Table 15-11 outlines possible causes and suggested actions when connections are dropped over a serial or WAN interconnection.

Table 15-11 WAN: Dropped Connections over a WAN or Serial Link

Possible Cause	Suggested Actions
Noisy serial line	**Step 1** Use the **show interfaces serial** EXEC command to determine whether input errors are increasing.
	Step 2 If input errors appear and are increasing, diagnose the serial line as described in the "Troubleshooting Serial Line Problems" chapter.
Overutilized bandwidth	**Step 1** If input errors do not appear, the problem is related to congestion.
	Step 2 Turn off fast switching on the affected interface.
	Step 3 Check the applications being run, especially for very large file transfers scheduled at particular times of day.
	Step 4 If you find large, scheduled file transfers, set up priority queuing. (Priority queuing requires that the protocol allow flow control.)
	Step 5 When bridging LAT, consider using the **bridge-group** *group* **lat-compression** interface configuration command to reduce bandwidth by implementing LAT compression.
	Step 6 Rearrange the timing of file transfers so that links are not overused during normal business hours.
	Step 7 Add bandwidth and consider using dial backup over the new link for applications that are taking excessive bandwidth on existing links.
	Step 8 Adjust buffer size. For details, see "Adjusting Buffers to Ease Overutilized Serial Links," in the "Troubleshooting Serial Line Problems" chapter.
Hardware in the serial link is unreliable	**Step 1** Use a serial analyzer to troubleshoot the serial line or perform the tests described in the sections "Using Extended ping Tests to Troubleshoot Serial Lines" and "CSU and DSU Loopback Tests" in the "Troubleshooting Serial Line Problems" chapter.
	Step 2 Replace hardware as necessary.
Inadequate bandwidth	**Step 1** After checking all of the above, examine the output of the **show interfaces serial** EXEC command. If, after these actions, load is still about 80 percent, the line is inadequate for traffic requirements.
	Step 2 Add another serial line.

Poor XNS Server Performance over Router in a LAN Internetwork

Symptom: Users complain about sessions dropping at peak traffic periods when trying to connect to resources on the other side of a router configured to route XNS. Table 15-12 outlines possible causes and suggested actions when XNS server performance is poor over a router in a LAN internetwork.

Table 15-12 XNS: Poor XNS Server Performance over Router in a LAN Internetwork

Possible Causes	Suggested Actions
Excessive traffic; collisions causing session drops (Ethernet only)	**Step 1** Use a protocol analyzer to examine traffic to look for collisions in excess of normal acceptable conditions (varies for specific site). As an alternative, use the **show interfaces** EXEC command to get a rough estimate of the collision count. **Step 2** Examine the output of the protocol analyzer to determine bandwidth utilization. Output from a protocol analyzer will provide a more accurate reading of dynamic traffic information. If the protocol analyzer detects bandwidth utilization of 15 to 20 percent (on average) or higher, you are likely to have a load-related performance problem. **Step 3** If you see a higher-than-expected bandwidth utilization and if collisions are increasing steadily, consider segmenting the network with additional bridges or routers.
Insufficient bandwidth on Token Ring to handle traffic	**Step 1** Upgrade from 4- to 16-Mbps Token Ring throughout network. **Step 2** If performance is still inadequate, consider segmenting the network with additional bridges or routers.

Poor XNS Server Performance over Router in a WAN

Symptom: Users complain that sessions drop at peak traffic periods when they are trying to connect to resources on the other side of a router that is configured to route XNS over a WAN or serial link. Table 15-13 outlines a possible cause and suggested actions when an XNS server performs poorly over a router in a WAN internetwork.

Table 15-13 XNS: Poor XNS Server Performance over Router in a WAN

Possible Cause	Suggested Actions
Another protocol dominates CPU time	**Step 1** Use the **show processes** EXEC command to look for large numbers in the Runtime (ms) and Invoked fields for certain protocols. An example would be a protocol that has a value that is 10 times or greater than the value indicated for XNS traffic. When this kind of condition exists, XNS traffic is not getting adequate access to the CPU, and performance is affected. **Step 2** Use the **show interfaces** EXEC command to look for a high level of output drops. **Step 3** If you see output drops and another protocol is dominating CPU time (indicated in the **show process** Runtime [ms] field), use priority queuing to force the system to handle XNS traffic over other protocols. More information about priority queuing is provided in the "Troubleshooting Serial Line Problems" chapter. **Step 4** If priority queuing does not improve performance, add bandwidth by implementing a higher-speed line or by adding additional lines of same speed. If you add additional lines, use the **xns maximum-paths** global configuration command to specify the number of paths

Switching-Support Matrices

The overall performance of the network can vary according to the switching mechanism used for a given protocol, interface type, software version, or encapsulation method. Furthermore, the type of switching that is available on a particular platform depends on the version of the installed software and on the individual cards installed in the router.

The following matrices compare protocols and network media types, and define the switching methods available for each combination based on the particular Cisco Internetwork Operating System (Cisco IOS) release you are running.

Note Switching support is dependent on the encapsulation used on a given media. The switching support indicated in the following tables is general and applies to most common encapsulations, but might not hold true for all possible encapsulations on that type of interface for the specified protocol. If you are uncertain about the switching support in your particular networking environment, contact your technical support representative.

Table 15-14 Cisco 3000 Switching Matrix for Cisco IOS Release 10.2

	Ethernet	Token Ring	Serial
IP	Fast	Fast	Fast
IPX	Fast	Fast	Fast
DECnet	Fast	Process	Fast
OSI	Fast	Process	Fast
AppleTalk	Fast	Fast	Fast
Bridging	Fast	Fast	Fast
SRB/RSRB	Fast	Fast	Fast
VINES	Fast	Fast	Fast

Table 15-15 Cisco 4000 Switching Matrix for Cisco IOS Release 10.2

	Ethernet	Token Ring	FDDI	Serial
IP	Fast	Fast	Fast	Fast
IPX	Fast	Fast	Fast	Fast
DECnet	Fast	Process	Fast	Fast
OSI	Fast	Process	Process	Fast
AppleTalk	Fast	Fast	Process	Fast
Bridging	Fast	Fast	Fast	Fast
SRB/RSRB	Fast	Fast	Fast	Fast
VINES	Fast	Fast	Fast	Fast

Table 15-16 Cisco 7000 Switching Matrix for Cisco IOS Release 10.2

	Ethernet Interface Processor (EIP)	Token Ring Interface Processor (TRIP)	FDDI Interface Processor (FIP)	Fast Serial Interface Processor (FSIP)	HSSI Interface Processor (HIP)	ATM Interface Processor (AIP)
IP	Silicon/ Autonomous	Silicon/ Autonomous	Silicon/ Autonomous	Silicon/ Autonomous	Silicon/ Autonomous	Silicon/ Autonomous
IPX	Silicon/ Autonomous	Silicon/ Autonomous	Silicon/ Autonomous	Silicon/ Autonomous	Silicon/ Autonomous	Fast
DECnet	Fast	Process	Fast	Fast	Fast	Process
OSI	Silicon	Silicon	Silicon	Silicon	Silicon	Process
AppleTalk	Fast	Fast	Fast	Fast	Fast	Process
Bridging	Silicon/ Autonomous	Fast	Silicon/ Autonomous	Silicon/ Autonomous	Silicon/ Autonomous	Process
SRB/RSRB	Fast	Silicon/ Autonomous	Fast	Fast	Fast	Process
VINES	Fast	Fast	Fast	Fast	Fast	Fast

Table 15-17 Cisco AGS+ Switching Matrix for Cisco IOS Release 10.2

	Multiport Ethernet Controller (MEC)	ciscoBus Token Ring Card (CTR)	FDDI Communications Interface Translational (FCIT)	High-Speed Communications Interface (HSCI)
IP	Autonomous	Autonomous	Autonomous	Autonomous
IPX	Autonomous	Autonomous	Autonomous	Autonomous
DECnet	Fast	Process	Fast	Fast
OSI	Fast	Fast	Fast	Fast
AppleTalk	Fast	Fast	Fast	Fast
Bridging	Autonomous	Fast	Autonomous	Autonomous
SRB/RSRB	Fast	Autonomous	Fast	Fast
VINES	Fast	Fast	Fast	Fast

Table 15-18 Cisco 3000 Switching Matrix for Cisco IOS Release 10.0

	Ethernet	Token Ring	Serial
IP	Fast	Fast	Fast
IPX	Fast	Fast	Fast
DECnet	Fast	Process	Fast
OSI	Fast	Process	Fast
AppleTalk	Fast	Process	Fast
Bridging	Fast	Fast	Fast
SRB/RSRB	Fast	Fast	Fast
VINES	Fast	Fast	Fast

Table 15-19 Cisco 4000 Switching Matrix for Cisco IOS Release 10.0

	Ethernet	Token Ring	FDDI	Serial
IP	Fast	Fast	Fast	Fast
IPX	Fast	Fast	Fast	Fast
DECnet	Fast	Process	Fast	Fast
OSI	Fast	Process	Process	Fast
AppleTalk	Fast	Process	Process	Fast
Bridging	Fast	Fast	Fast	Fast
SRB/RSRB	Fast	Fast	Fast	Fast
VINES	Fast	Fast	Fast	Fast

Table 15-20 Cisco 7000 Switching Matrix for Cisco IOS Release 10.0

	Ethernet Interface Processor (EIP)	Token Ring Interface Processor (TRIP)	FDDI Interface Processor (FIP)	Fast Serial Interface Processor (FSIP)	HSSI Interface Processor (HIP)	ATM Interface Processor (AIP)
IP	Silicon/ Autonomous	Silicon/ Autonomous	Silicon/ Autonomous	Silicon/ Autonomous	Silicon/ Autonomous	Silicon/ Autonomous
IPX	Silicon/ Autonomous	Silicon/ Autonomous	Silicon/ Autonomous	Silicon/ Autonomous	Silicon/ Autonomous	Process
DECnet	Fast	Process	Fast	Fast	Fast	Process
OSI	Silicon	Silicon	Silicon	Silicon	Silicon	Process
AppleTalk	Fast	Fast	Fast	Fast	Fast	Process
Bridging	Silicon/ Autonomous	Fast	Fast	Silicon/ Autonomous	Silicon/ Autonomous	Process
SRB/RSRB	Fast	Silicon/ Autonomous	Fast	Fast	Fast	Process
VINES	Fast	Fast	Fast	Fast	Fast	Process

Table 15-21 Cisco AGS+ Switching Matrix for Cisco IOS Release 10.0

	Multiport Ethernet Controller (MEC)	ciscoBus Token Ring Card (CTR)	FDDI Communications Interface Translational (FCIT)	High-Speed Communications Interface (HSCI)
IP	Autonomous	Autonomous	Autonomous	Autonomous
IPX	Autonomous	Autonomous	Autonomous	Autonomous
DECnet	Fast	Process	Fast	Fast
OSI	Fast	Fast	Fast	Fast
AppleTalk	Fast	Fast	Fast	Fast
Bridging	Autonomous	Fast	Autonomous	Autonomous
SRB/RSRB	Fast	Autonomous	Fast	Fast
VINES	Fast	Fast	Fast	Fast

Appendixes

APPENDIX A

Technical Support Information List

When a problem arises that you are unable to resolve, the resource of last resort is your router technical support representative. To analyze a problem, your technical support representative will need certain information about the situation and the symptoms you are experiencing. To speed the problem isolation process, present this data when you contact your representative.

Gathering Information about Your Internetwork

Before gathering any specific data, the first thing to do is compile a list of all symptoms that users have reported on the internetwork (such as connections dropping or slow host response).

The next step is to gather specific information. Typical information needed to troubleshoot internetworking problems falls into two general categories: information required for any situation and information specific to the topology/problem.

Information always required by technical support engineers includes the following:

- Configuration listing of all routers involved
- Complete specifications of all routers involved
- Version numbers of software (obtained with **show version** command) and firmware (obtained with the **show controllers** command) on all routers
- Network topology map, including any suspected back doors
- List of hosts and servers (host and server type, number on network, description of host operating systems implemented)
- List of network layer protocols, versions, vendors

Specific requirements that vary depending on the situation include the following:

- Output from general **show** commands:

  show interfaces

  show controllers {**serial** | **token** | **mci** | **cbus** | **fddi**}

  show processes

- Output from protocol-specific **show** commands:

  show *protocol-type* **route**

  show *protocol-type* **traffic**

  show *protocol-type* **interfaces**

  show *protocol-type* **arp**

  show appletalk globals (AppleTalk only)

  show ipx servers (Novell only)

- Output from relevant **debug** privileged EXEC commands.
- Output from protocol-specific **ping** (Echo Request/Echo Reply) and **trace** diagnostic tests as appropriate.
- Network analyzer traces.
- Core dumps (use the **exception dump** router configuration command). You also can use the **write core** router configuration command if the system is operational.

Getting the Data from Your Router

You must tailor the way you obtain information from the router to the systems you are using to get that information. A few hints are outlined as follows (organized by an information-gathering tool).

For PC and Macintosh

Connect a PC or Macintosh to the console port of the router and log all output to a disk file. The exact procedure varies depending on the communication package used with the PC.

For Terminal Connected to Console Port or Remote Terminal

The only way to get information with this configuration is to attach a printer to the AUX port on the terminal (if one exists) and force all screen output to go to the printer. Using a terminal is undesirable because there is no way to capture the data to a file.

For UNIX Workstation

At your UNIX prompt, enter the command **script** *filename*, then Telnet to the router. The UNIX **script** command causes all screen output to be captured to the specified filename. To stop capturing output and close the file, enter the end-of-file character for your UNIX system.

Note To get your system to automatically log specific error messages or operational information to a UNIX syslog server, use the **logging** *internet-address* router configuration command. For more information about using the **logging** command and setting up a syslog server, refer to your *Router Products Configuration Guide* and *Router Products Command Reference* publications.

Presenting Data to Your Technical Support Representative

Your technical support representative will accept information in any format that you can provide. Common forms include data sent via file transfer, electronic mail, magnetic media, and hard copy.

The order of preference is as follows:

1. The preferred method of information delivery is via the File Transfer Protocol (FTP) service over the Internet. If your environment supports FTP, you can place your file in the "incoming" directory on the host named *ftp.cisco.com*.
2. The next best method is to send data by electronic mail. Before trying this method, be sure to contact your router technical support representative, especially when transferring binary core dump files.
3. Transfer via a PC-based communications protocol, such as *Kermit*. Again, be sure to contact your technical support representative before attempting any transfer.
4. Transfer by disk or tape.
5. The least favorable method is hard copy transfer by physical mail or fax.

APPENDIX B

Problem-Solving Checklist and Worksheet

To isolate problems in your internetwork, you must first compile all the relevant facts and then methodically address each suspect problem. This appendix provides a troubleshooting checklist and general worksheet to help you in this process. Use the checklist and worksheet as *initial guidelines* to assist you in developing your own checklist and worksheet—one tailored to your own internetworking environment.

Troubleshooting Checklist

Before you start making any changes to your internetwork, be sure you can answer the following questions positively:

1. Have you identified and compiled a list of all the reported symptoms on your internetwork?
2. Do you know your internetwork? Do you have an accurate physical and logical map of your internetwork?
3. Do you have a list of all the network protocols implemented in your network?
4. Do you know which protocols are being routed?
5. Do you know which protocols are being bridged?
6. Do you know all the points of contact to external networks?
7. Do you know all the internetwork equipment in your network?
8. Have you identified an end system or internetwork node that might be the cause of a problem?
9. Do you know the applications that are being used in your network?
10. For every symptom, have you developed a list of potential problems and causes?
11. For each problem, do you have a plan of action?

If you can answer *yes* to these questions, you can begin the process of isolating problems. Remember to eliminate one problem at a time.

Troubleshooting Worksheet

1 Symptoms reported:

2 Network topology map—attach separate sheet(s)

3 Network protocols implemented:

4 Protocols routed:

5 Protocols bridged:

6 Points of contact to external networks:

7 Internetwork equipment (including network address, vendor, model, and function):

8 Suspect end system and internetwork nodes (including network address, vendor, model, and function):

9 Applications being used on the network (FTP, sendmail, NFS, NetWare, and so forth):

10 Symptoms and possible problems:

Symptom **Possible Problems**

11 Action plan for each problem:

Problem	**Action Plan**

12 Action outcomes:

Problem/Action	Result/Outcome

APPENDIX C

Creating Core Dumps

When a router crashes, it can be useful to obtain a full copy of the memory image (core dump) to analyze the cause of the crash. Core dumps generally are only useful to your router technical support representative.

Caution Use the commands discussed in this appendix only in coordination with a technical support representative. The resulting binary file must be directed to a specific Trivial File Transfer Protocol (TFTP) server and subsequently interpreted by technical personnel who have access to source code and detailed memory maps.

Exception Commands

The **exception** class of configuration commands should be used only after consulting with a technical support representative. These commands are useful for debugging purposes, but they can result in unexpected behavior.

Creating a Core Dump

To obtain a core dump when a router crashes, use the **exception dump** *IP-address* router configuration command. *IP-address* is the address of your TFTP server. The core dump is written to a file named *hostname*-core on your TFTP server, where *hostname* is the name of the router (assigned using the **hostname** router configuration command). Using this command causes the router to attempt to make a core dump when it crashes.

This procedure cannot be guaranteed to work. It can fail for certain classes of system crashes. If successful, the core dump file will be the size of the memory available on the processor (for example, 4 MB for a CSC/3).

In addition you can use the **exception core-file** *filename* command to create a name for the core dump on your host.

Creating an Exception Memory Core Dump

During the debugging process, you can cause the router to create a core dump and reboot when certain memory size parameters are violated. The **exception memory** commands define a minimum contiguous block of memory in the free pool and a minimum size for the free memory pool.

[**no**] **exception memory fragment** *size*
[**no**] **exception memory minimum** *size*

The value of *size* is in bytes and is checked every 60 seconds. If you enter a size that is greater than the free memory, a core dump and router reload is generated after 60 seconds only when the **exception dump** command has been configured; otherwise, the router reloads without generating a core dump. The following example configures the router to monitor the free memory. If it falls below 250,000 bytes, it will dump the core and reload.

```
exception dump 131.108.92.2
exception core-file memory.overrun
exception memory minimum 250000
```

write core Command

You can test core dumps by using the EXEC command **write core**. This command causes the router to generate a dump without reloading and is useful if the router is malfunctioning, but has not crashed.

Depending on your TFTP server, you may need to create a target file before the router can write to it. You can test whether a target file is needed by attempting to use the TFTP **put** command from a workstation.

show Commands

When a router fails with an unexpected reload, and you report the problem to a technical support representative, always include a copy of the output from the **show stacks** and **show version** EXEC commands, so the representative can learn as much information about the state of your router when it failed.

show stacks Command

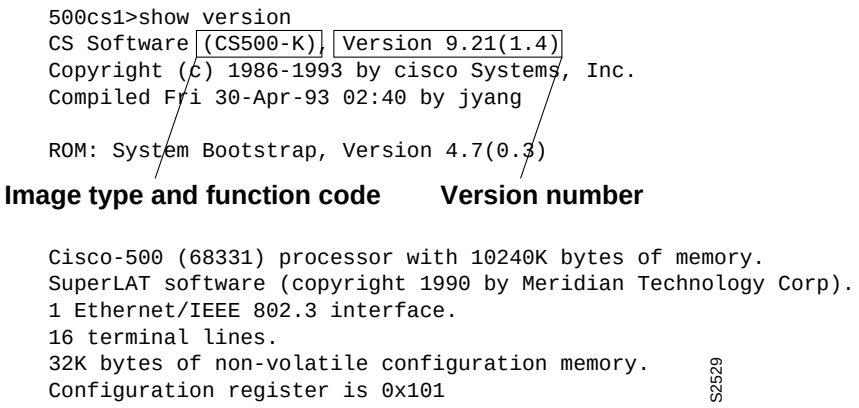
A useful EXEC command is **show stacks**. This command displays data saved by the ROM monitor, which includes a failure type, an operand address, and a failure program counter. This data is overwritten when the system is reloaded, so check your configuration register settings and decide how you want to recover from system crashes.

The "Memory Maps" appendix provides an example of **show stacks** output and memory map information that can help you determine whether a system crash is due to a software or hardware problem.

Software Version Identification

Much useful information is contained in the output of the **show version** command. (See Figure C-1.) The image type, version number, and function sets included in the image pinpoint the exact software that is running on your router.

Figure C-1 show version Command Output



Version Numbering

A version number consists of a major version part, a minor version part, and an edit level, written in the form <major>.<minor>(<edit>). For Software Release 9.1(5), the major version is 9; the minor version is 1; and the edit level is 5. The major version number is changed when very extensive changes are made to the software. The minor number is changed whenever new functionality is added; and the edit level is changed when any change is made to the software.

For some versions, the edit level might also be divided into parts, as in Software Release 9.1(3.5). This convention identifies interim versions created between software maintenance releases. Software Release 9.1(3.5) would be the fifth 9.1 interim version created after Release 9.1(3). When a full-fledged field release in this progression is made, it would be numbered 9.1(4). Interim releases are distributed for special situations only, so most users see integer edit levels only.

Maintenance and interim releases progress linearly; 9.1(4) contains all the changes that were in Software Release 9.1(3) and all changes introduced in 9.1(3.x) versions. This linear progression is guaranteed for maintenance and interim releases, but not for major releases. For example, 9.17 does not contain all the functionality of 9.14; they are two separate products.

Beta test releases have two-part edit levels with zero as the first part; Software Release 9.1(0.11), for example, is a beta test release of 9.1. The first full field release of a software version always has edit level 1; for example, the first full field release of 9.1 is 9.1(1).

Experimental or early field test software may not follow edit-level numbering conventions. Such software often has single-number edit levels greater than 100, as in Software Release 9.1(12345). Also common are edit levels with more than two parts, edit levels that have nonnumeric components, and identifiers in brackets following the edit level. If you work with such software, pay careful attention to everything displayed by the **show version** command.

Image Types

The image type indicates which hardware platforms the image supports and the functions present in it, as shown in Table C-1. The version number indicates the source code version used to create the image. In addition, the version number indicates the release level of the image.

Table C-1 Image Types

Image Type	Description
GS7	Cisco 7000 series router software (GS stands for "Gateway Server" and is used for historical reasons).
GS2	Router software that runs on CSC/2 processors. Later GS2 images also will run on CSC/3 processors.
GS3	Software that runs on AGS+, AGS, MGS, and CGS routers with CSC/3 and CSC/4 processors.
XX	Cisco 4000 series router software (XX comes from the internal project code name used during Cisco 4000 development).
IGS	IGS and Cisco 3000 series router software and software for hub-based router products.
TS2	Older communication server (terminal server) software for CSC/2 processors.
TS3	Older communication server (terminal server) software for CSC/3 and CSC/4 processors.
CS3	Newer communication server software for CSC/3 and CSC/4 processors.
CS500	500-CS communication server software.
PT2	Protocol translator software for CSC/2 processors. Protocol translation is now available for many router and communication server products. In those products, the feature code P is used to denote the presence of protocol translation.
PT3	Protocol translator software for CSC/3 and CSC/4 processors.
STS	STS-10 terminal server software (the STS-10 is now obsolete).
BT2	Secondary bootstrap images for CSC/2 processors. Now largely obsolete.

Function Codes

Table C-2 describes function codes. Codes are often combined for images that have multiple optional function sets; for example, XX-RXBOOT is a Cisco 4000 image that executes from ROM, includes support for WAN connections, and includes only functions that are necessary for bootstrapping.

Table C-2 Function Types

Function Type	Description
B	Bridging support.
D	DDN X.25 support in very old images. Newer images include DDN X.25 with general X.25 support.
F	Full support. Used for older AGS+ images to denote the presence of support for the ciscoBus complex. Also used on Cisco 2000 series and Cisco 3000 series platforms to denote images that execute from Flash memory.
K	K images support all optional features (except for protocol translation) applicable to the platforms they run on. Note that even if all features are compiled into an image, most versions may require special licensing steps to enable the use of optional features.
P	Telnet/LAT/X.29 protocol translation.
R	Software that executes directly from ROM. R images cannot be network booted on any platform.
S	Standard software images without bridging, X.25, or other optional functionality.
X	X.25 and other WAN protocols.
BOOT	Minimal bootstrap images whose only function is to allow loading of other images over the network or from Flash memory.

APPENDIX D

Memory Maps

This appendix presents memory maps for selected product platforms, processors, and interface cards. Memory map information is useful for technically qualified users who understand concepts of low-level operating systems and have a basic understanding of bus structures and address mapping in computer systems.

When using this appendix, be aware of the distinct difference between program counter values and operand addresses. The addresses that appear in this appendix are operand values and should not be confused with program counter values.

Note Unless otherwise noted, all memory addresses are in hexadecimal.

Memory Maps and Troubleshooting

Memory map information can be useful when you are determining whether a problem exists in the software or in the hardware. The system software can provide information on the reasons for a system crash. This information appears in the form of error messages issued by the read-only memory (ROM) monitor when an exception is encountered.

Failure Types

When a system crashes, the ROM monitor reports a failure type. The failure type is important both in its own right and as a guide to interpreting the other information the system provides. Failure types are usually one of the following:

- Bus errors
- Address errors
- Watchdog timeouts
- Parity errors
- Emulator traps

Bus Errors

The system encounters a bus error when the processor tries to use a device or a memory location that either does not exist or does not respond properly. Bus errors indicate either a software bug or a hardware problem. The address the processor was trying to access when the system crashed provides a key as to whether the failure is due to software or hardware.

If the operand address is valid, the problem is probably in the hardware. The address maps list addresses for selected hardware platforms.

Bus errors on an address not in the map usually indicate a software bug.

Address Errors

Address errors occur when the software tries to access data on incorrectly aligned boundaries. For example, 2- and 4-byte accesses are allowed only on even addresses. An address error usually indicates a software bug.

Watchdog Timeouts

Cisco processors have timers that guard against certain types of system hangs. The central processing unit (CPU) periodically resets a watchdog timer. If the timer is not reset, a trap will occur. Failure to service the watchdog timer indicates either a hardware or a software bug.

Parity Errors

Parity errors indicate that internal hardware error checks have failed. A parity failure is almost certainly a hardware problem. Use the address map to locate the affected hardware.

Emulator Traps

Emulator traps indicate that the processor has executed an illegal instruction. Emulator traps can be caused either by software taking illegal branches or by hardware failures, notably ROM failures.

Error Addresses

By observing the operand address, you can locate the general area of the router where the error occurred. Hardware problems can be inferred only from a bus error on a legal address, not from an emulator trap or illegal instruction trap. When looking at the bus error, the operand address—not the program counter address—provides the memory map location of the error.

show stacks Command

By using the **show stacks** EXEC command, you can display data saved by the ROM monitor, which includes a failure type, an operand address, and a failure program counter. This data is overwritten when the system is reloaded, so you might want to check your configuration register settings and decide how you want to recover from system crashes. Stack traces can be used by qualified technical support representatives who have access to symbol tables, object files, and source code.

Figure D-1 shows an example of the **show stacks** output from a software failure. The message "Software forced crash" indicates that the software detected a condition it did not expect and from which it could not recover. When investigated by a technical support representative, the listed program counter provides a trace to the code responsible for the failure.

Figure D-2 shows output from a hardware error and includes an example of a hardware operand address that can be used with the memory maps in this appendix. The operand address points to the register space for MCI unit 0 and indicates a hardware or microcode problem with that unit.

Figure D-1 show stacks Command Output Showing the Software Program Counter Address

```
ROUTER> show stacks

Minimum process stacks:
Free/Size  Name
 972/1000  env delay init
 866/1000  Router Init
 556/1000  Init
 638/1000  RSRB Connector
1230/2000  Virtual Exec

Interrupt level stacks:
Level    Called Free/Size  Name
  1      306611  952/1000  env-flash
  3    22294573  496/1000  Multiport Communications Interfaces
  5        2986  968/1000  Console UART

System was restarted by error - Software forced crash, PC 0x4854E
GS Software (GS3-K), Version 9.1(4) [fc1], SOFTWARE
Compiled Thu 25-Mar-93 09:49 by daveu
Stack trace from system failure:
FP: 0x2B0424, RA: 0x3B04
FP: 0x2B0458, RA: 0xF39C2
FP: 0x2B046C, RA: 0xF4566
FP: 0X2B0490, RA: 0x112F0
FP: 0x2B04B0, RA: 0x2560
```

program counter address

S2530

Figure D-2 show stacks Command Output Showing the Hardware Address

```
Minimum process stacks:
Free/Size  Name
 970/1000  env delay init
 866/1000  Router Init
 554/1000  Init
1500/2000  Exec

Interrupt level stacks:
Level    Called Free/Size  Name
  1       16803  956/1000  env-flash
  3     4827380  772/1000  cBus Interfaces
  5        5627  968/1000  Console UART

System was restarted by bus error at PC 0x71EAE, address 0x210C008
GS Software (GS3-K), Version 9.1(5), RELEASE SOFTWARE
Compiled Wed 19-May-93 18:35 by daveu
Stack trace from system failure:
FP: 0x2B6BA0, RA: 0xF496
FP: 0x2B6BCC, RA: 0xABDFA
FP: 0x2B6C2C, RA: 0xABA2C
FP: 0x2B6C40, RA: 0xAB338
FP: 0x2B6C68, RA: 0x258C
```

Hardware address in the bus controller address space

S2531

Memory Maps

The following tables summarize memory map information for the various Cisco platforms:

- Table D-1 describes the Cisco 2000 memory map.
- Table D-2 describes the Cisco 2500 memory map.
- Table D-3 describes the Cisco 3000 memory map.
- Table D-4 describes the memory map for the Cisco 3104 and Cisco 3204; Table D-5 describes the Cisco 3104 and Cisco 3204 memory map of onboard registers and chips.
- Table D-6 describes the Cisco 4000 memory map; Table D-7 describes the Cisco 4000 memory map of onboard resources.
- Table D-8 describes the Cisco 4500 memory map; Table D-9 describes the Cisco 4500 memory map of onboard resources.
- Table D-10 describes the Cisco 7000 memory map.
- Table D-11 describes the Cisco 500-CS memory map.
- Table D-12 describes Multibus memory space assignment; Table D-13 describes Multibus I/O space assignment.
- Table D-14 describes the Cisco Cx-RP memory map.
- Table D-15 describes the Cisco CSC/3 memory map.
- Table D-16 describes the Cisco CSC/4 memory map.
- Table D-17 describes the processor memory map for the Cisco CSC/2, CSC/3, CSC/4 cards, including the IGS and Cisco 3000.

Table D-1 Cisco 2000 Memory Map

Address	Description	Comments
00000000 - 0017FFFF	CPU and packet memory (dynamic random-access memory [DRAM])	1.5 MB
01000000 - 011FFFFF	ROM monitor and system image code space (erasable programmable read-only memory [EPROM])	2 MB
02000000 - 02007FFF	Configuration random-access memory (RAM)	32 KB
02100000 - 0213FFFF	Control registers and input/output (I/O) devices	Details follow
02110000	Control register 1	–
02110002	Control register 2	–
02110040	Programmable read-only memory (PROM) cookie	–
02110100	Status register	–
02120040	Timer control register	–
02130000 - 02130003	Ethernet controller	–
02130000 - 0213000F	Token Ring controller	–
02130040 - 02130043	Serial controller	–
02130080	Serial control register 1	–
02130081	Serial control register 2	–

Table D-2 Cisco 2500 Memory Map

Address	Bit Width	Description	Comments
00000000 - 00FFFFFF	32	DRAM	2, 4, 8, or 16 MB
00000000 - 001FFFFF	32	DRAM 2 MB	–
00000000 - 003FFFFF	32	DRAM 4 MB	–
00000000 - 007FFFFF	32	DRAM 8 MB	–
00000000 - 00FFFFFF	32	DRAM 16 MB	–
00000000 - 001FFFFF	8/16	Boot Flash memory	1 or 2 MB, when Flash memory PCMCIA card is not installed
00000000 - 001FFFFF	16	Flash memory PCMCIA card	Boot Mode
01000000 - 011FFFFF	16	Boot EPROMs for ROM monitor and RXBOOT images	1 or 2 MB ROM; 2 MB Flash memory
01000000 - 011FFFFF	16	Flash memory PCMCIA card	When installed
02000000 - 0201FFFF	8	Configuration non-volatile random-access memory (NVRAM)	32 or 128 KB
02000000 - 02007FFF	8	Configuration NVRAM (32 KB)	–
02000000 - 0201FFFF	8	Configuration NVRAM (128 KB)	–
02100000 - 0213FFFF	8/16	Onboard I/O registers and chips	–
03000000 - 03FFFFFF	32	Flash memory RAM (SIMMs)	4, 8, or 16 MB
03000000 - 033FFFFF	32	Flash memory RAM (4 MB)	–
03000000 - 037FFFFF	32	Flash memory RAM (8 MB)	–
03000000 - 03FFFFFF	32	Flash memory RAM (16 MB)	–
08000000 - 081FFFFF	8/16	Onboard boot EPROMs (remapped)	1 or 2 MB, when PCMCIA Flash memory card is installed

Table D-3 Cisco 3000 Memory Map

Address	Description	Comments
00000000 - 00FFFFFF	Main memory DRAM	–
01000000 - 011FFFFF	Secondary DRAM	–
02000000 - 0201FFFF	NVRAM	–
02100000 - 02100FFF	Channel B: 68302 registers	–
02101000 - 02101FFF	Channel B: 63802 RAM	–
02110000	System control register 1	–
02110002	System control register 2	–
02110100	System status register	–
02110040 - 0211005F	Cookie	–
02120000 - 02120003	Counter/timer (CNTR)	–
02120040	Counter control register (CCTL)	–
02120100 - 0212013F	Console ports	–
02130000 - 02130003	Channel A: LANCE chip	–

Address	Description	Comments
02130040 - 02130043	Channel B: LANCE/serial chip	–
02130080 - 02130083	Channel B: serial DTR register	–
03000000 - 03FFFFFF	Flash memory	–
04000000 - 042FFFFF	Secondary RAM	When main memory = 16 MB

Table D-4 Cisco 3104 and Cisco 3204 Memory Map

Address	Description	Comments
00000000 - 00FFFFFF	Main DRAM	1-, 4-, 8-, and 16-MB sizes
01000000 - 010FFFFF	Boot EPROMs for ROM monitor and bootstrap image	–
01000000 - 011FFFFF	Boot Flash memory for ROM monitor and bootstrap image	Onboard Flash memory or PCMCIA Flash memory card, 2 MB
02000000 - 0201FFFF	Configuration NVRAM	32 or 128 KB size
02100000 - 0213FFFF	Onboard registers and chips	–
03000000 - 03FFFFFF	Flash memory single in-line memory module (SIMM)	Up to 16 MB
04000000 - 041FFFFF	I/O memory (packet memory)	512 KB or 2 MB sizes
08000000 - 081FFFFF	Remapped onboard boot Flash memory	Remapped when PCMCIA Flash memory card is installed

Table D-5 Cisco 3104 and Cisco 3204 Onboard Registers and Chips

Address	Description	Comments
021000F2 - 021000F3	Base address register for 68302	–
021000F4 - 021000F7	System control register for 68302	–
02101000 - 021013FF	System RAM for 68302	–
02101400 - 021017FF	Parameter RAM for 68302	–
02101800 - 02101FFF	Internal registers for 68302	–
02110000	System control register 1	–
02110002	System control register 2	–
02110004	System control register 3	–
02110006	System interrupt register	–
02110060	Serial NVRAM control register	–
02120000 - 02120003	Timer counter	–
02120040	Counter control register	–
02120100 - 0212013F	Console interfaces	–
02130000 - 0213003	Ethernet controller	–
02131000 - 0213100F	Token Ring controller	–
02131010 - 02131011	Hardware map register 0	–
02131012 - 02131013	Hardware map register 1	–

Address	Description	Comments
02132000 - 021320FF	Serial controller	–
02132100 - 02132101	Serial 0 device register	–
02132102 - 02132103	Serial 1 device register	–

Table D-6 Cisco 4000 Memory Map

Address	Bit Width	Description	Comments
00000000 - 0003FFFF	32	System static random-access memory (SRAM)	256 KB, fixed; 0 wait read, 1 wait write
00040000 - 00FFFFFF	32	System DRAM memory (SIMMs)	8-, 16-, 32-bit unaligned access supported; 4, 8, 16, or 32[1] MB
00040000 - 003FFFFF		4 MB	–
00040000 - 00FFFFFF		16 MB	–
01000000 - 01FFFFFF	16	Boot EPROM	2 MB, fixed
01000000 - 010FFFFF		1 MB	–
01000000 - 011FFFFF		2 MB	–
01000000 - 013FFFFF		4 MB	–
01000000 - 017FFFFF		8 MB	–
02000000 - 02FFFFFF	8 or 32	Onboard resources	–
02020000		System I/O	–
03000000 - 03FFFFFF	32	Flash memory EPROM or EPROM	32 bit read/write access
03000000 - 031FFFFF		2 MB	–
03000000 - 033FFFFF		4 MB	–
03000000 - 037FFFFF		8 MB[2]	–
05000000		System DRAM	Upper 16 MB of 32 MB configuration
06000000 - 06FFFFFF	32	Shared (I/O) memory	8-, 16-, 32-bit unaligned access supported; 1–16 MB
06000000 - 060FFFFF		1 MB	–
06000000 - 063FFFFF		4 MB	–
06000000 - 067FFFFF		8 MB	–
04000000 - 05FFFFFF		Undefined	–
07000000 - 07FFFFFF		Undefined	–
08000000 - 08FFFFFF	32	I/O expansion	Network interface module (NIM) slots
08000000 - 080FFFFF	16	NIM at I/O expansion slot 1	16 bit aligned access only
08100000 - 081FFFFF	16	NIM at I/O expansion slot 2	16 bit aligned access only
08200000 - 082FFFFF	16	NIM at I/O expansion slot 3	16 bit aligned access only

1. Only the Cisco 4000-M supports 32-MB DRAM. The 32-MB configuration is split into two discontiguous pieces, with the upper 16 MB mapped to begin at location 05000000.
2. Only the Cisco 4000-M supports 8-MB Flash memory.

Table D-7 Cisco 4000 Memory Map of Onboard Resources

Address	Bit Width	Description	Comments
02000000 - 0201FFFF	8	NVRAM battery backed up CMOS SRAM	128 KB, fixed; also accommodates 32 KB x 8 and 8 KB x 8
02110000	32	System status and control registers	–
02110002		Hardware revision	–
02110040 - 0211005F	8	System ID PROM cookie	24 bytes
02110100	32	Shared memory control register	–
02120000	8	Counter timer	–
02120040	8	Counter interrupt control register	–
02120100 - 0212013F	8	Control serial I/O	–

Table D-8 Cisco 4500 Memory Map

Address	Bit Width	Description	Comments
60000000 - 61FFFFFF	64	System DRAM	Capable of 8–64 bit access, cached
60000000 - 607FFFFF		8 MB	–
60000000 - 60FFFFFF		16 MB	–
60000000 - 61FFFFFF		32 MB	–
BFC00000 - BFC7FFFF	8	Boot EPROM	–
BFC00000 - BFC1FFFF		128 KB	–
BFC00000 - BFC7FFFF		512 KB	–
3E000000 - 3EFFFFFF	8	Onboard resources	–
30000000 - 30FFFFFF	32	System Flash memory EPROM	–
30000000 - 303FFFFF		4 MB	–
30000000 - 307FFFFF		8 MB	–
30000000 - 30FFFFFF		16 MB	–
38000000 - 387FFFFF	32	Boot Flash memory EPROM	–
38000000 - 383FFFFF		4 MB	–
38000000 - 387FFFFF		8 MB	–
40000000 - 40FFFFFF	32	Shared memory	8-, 16-, 32-bit access
40000000 - 403FFFFF		4 MB	–
40000000 - 40FFFFFF		16 MB	–

Table D-9 Cisco 4500 Memory Map of Onboard Resources

Address	Bit Width	Description	Comments
3E000000 - 3E07FFFF	8	NVRAM	Battery backed up SRAM
3E000000 - 3E01FFFF	8	128 KB	–
3E000000 - 3E07FFFF	8	512 KB	–
3E000000	8	Time of day clock	–
3E800400	8	System ID PROM cookie	–

Table D-10 Cisco 7000 Memory Map

Address	Description	Comments
11110100	System status register	–
11110400	Flash memory card status	–
11110C00	I/O address base	SwitchBus address space. Each unit occupies 64 bytes (0x40).
11120040	Timer control register	–
11120200	Environmental monitor control	16 bits
11120300	Environmental monitor status	32 bits
11130000	Diagnostic bus	–
11131000	ID PROM	–
11140000	NVRAM	–
1115FC00	Environmental monitor NVRAM base address	–
1115FFFF	Real time calendar bit	–
11200000 - 11FFFFFF	Reserved	14 Mb reserved
12000000	Onboard Flash memory	–
14000000	External Flash memory	–

Table D-11 Cisco 500-CS Memory Map

Address	Description	Comments
000000 - 3FFFFF	ROM	4 MB or less
400000 - 407FFF	Electronically erasable programmable read-only memory (EEPROM) (NVRAM)	32 KB
420000 - 427FFF	LCD registers (not used)	–
428000 - 42FFFF	Future hardware	–
430000 - 440000	Reserved	–
460000 - 460004	LANCE registers	Ethernet controller registers
500000 - 50007F	Octal Universal Asynchronous Receiver/Transmitter (UART) 0	–
500400 - 50047F	Octal UART 1	–

Address	Description	Comments
600000 - 7FFFFF	Onboard RAM	–
800000 - BFFFFF	2-MB SIMM expansion	–
800000 - FFFFFF	8-MB SIMM expansion	–

Table D-12 Multibus Memory Space Assignment

Address	Description	Comments
20000000 - 2000FFFF	Memory card	64 KB
20010000 - 2002FFFF	CSC-R16 card	Unit 0 address, 128 KB
20030000 - 2004FFFF	CSC-R16 card	Unit 1 address, 128 KB
20050000 - 2006FFFF	CSC-R16 card	Unit 2 address, 128 KB
20070000 - 2008FFFF	CSC-R16 card	Unit 3 address, 128 KB
20090000 - 200AFFFF	CSC-R16 card	Unit 4 address, 128 KB
200B0000 - 200BFFFF	NVRAM	64 KB
200C0000 - 200DFFFF	CSC-R16 card	Unit 5 address, 128 KB
200E0000 - 200FFFFF	CSC-R16 card	Unit 6 address, 128 KB (shared)

Table D-13 Multibus I/O Space Assignment

Address	Description	Size (in hex)	Comments
20100000	Environmental Monitor (ENVM) card	2	Environmental monitor
20100002 - 2010008F	Unused		
20100090		2	CSC-R16M Ethernet mailbox, Unit 0
20100092		2	CSC-R16M Ethernet mailbox, Unit 1
20100098	CSC-R16 card	2	Unit 0
2010009A	CSC-R16 card	2	Unit 1
201000A0	CSC-R card	4	Unit 0
201000A4	CSC-R card	4	Unit 1
201000A8	CSC-R card	4	Unit 2
201000AC	CSC-R card	4	Unit 3
201000B0	CSC-R16M card	2	Unit 0
201000B2	CSC-R16M card	2	Unit 1
201000B4	CSC-R16M card	2	Unit 2
201000B6	CSC-R16M card	2	Unit 3
201000B8	CSC-R16M card	2	Unit 4
201000BA	CSC-R16M card	2	Unit 5
201000BC	CSC-R16M card	2	Unit 6
201000BE	CSC-R16M card	2	Unit 7

Address	Description	Size (in hex)	Comments
201000C0	MLP	20	Unit 0
201000E0	MLP	20	Unit 1
20100100	3MB	100	Unit 0
20100200	3MB	100	Unit 1
20100300	3MB	100	Unit 2
20100400	3MB	100	Unit 3
20100500	Interlan	10	Unit 0
20100510	Interlan	10	Unit 1
20100520	Interlan	10	Unit 2
20100530	Interlan	10	Unit 3
20100540	Interlan	10	Unit 4
20100550	Interlan	10	Unit 5
20100560	Interlan	10	Unit 6
20100570 - 201005FF	Unused		
20100600	ACC	100	Unit 0
20100700	ACC	100	Unit 1
20100800	ACC	100	Unit 2
20100900	ACC	100	Unit 3
20100A00	HUB	100	Unit 0
20100B00	HUB	100	Unit 1
20100C00 - 20101FFF	Unused		
20102000	3COM	2000	Unit 0
20104000	3COM	2000	Unit 1
20106000	3COM	2000	Unit 2
20108000	3COM	2000	Unit 3
2010A000	3COM	2000	Unit 4
2010C000	CSC-MCI card	40	Unit 0
2010C040	CSC-MCI card	40	Unit 1
2010C080	CSC-MCI card	40	Unit 2
2010C0C0	CSC-MCI card	40	Unit 3
2010C100	CSC-MCI card	40	Unit 4
2010C140	CSC-MCI card	40	Unit 5
2010C180	CSC-MCI card	40	Unit 6
2010D000 - 2010 FFFF	Unused	–	–

Table D-14 Cx-RP Memory Map

Address	Bit Width	Description	Comments
00000000 - 0FFFFFFF		DRAM	–
10000000 - 100FFFFF		ROML	–
10400000 - 104FFFFF		ROMU	–
11000000 - 110FFFFF		Multibus memory	–
11100000 - 1110FFFF		Multibus I/O	–
11110000 - 1112FFFF		Local I/O	–
11130000 - 11130FFF		Diagnostic bus	–
11131000 - 111314FF		ID PROM	–
11140000 - 1115FFFF		NVRAM	–
12000000 - 13FFFFFF		Internal Flash memory	–
14000000 - 15FFFFFF		External Flash memory card	–
11110000	16	System control	–
11110100	32	System status	–
11120000	8	Counter timer	–
11120040	8	Counter control register	–
11120100 - 1112013F	8	Serial I/O ports	–
11120200	16	Environmental monitor control	–
11120300	32	Environmental monitor status	–
1115FFFF	1	Calender	1 bit (bit 0)
11110400	8	Flash memory card status	–

Table D-15 CSC/3 Memory Map

Address	Bit Width	Description	Comments
00000000 - 003FFFFF		RAM	–
01000000 - 0107FFFF		ROML	–
0108FFFF - 010FFFFF		ROMH	–
02000000 - 020FFFFF		Multibus memory	–
02100000 - 0210FFFF		Multibus I/O	–
02110000 - 02110001	16	System control register	–
02110100 - 02110103	32	System status register	–
02120000	8	Counter timer	–
02120040	8	Counter control register	–
02120100 - 0212013F		Serial ports	–
020B0000 - 020B7FFF		NVRAM	Over Multibus

Table D-16 CSC/4 Memory Map

Address	Bit Width	Description	Comments
00000000 - 00FFFFFF		RAM	–
01000000 - 013FFFFF		ROML	–
01400000 - 017FFFFF		ROMH	–
02000000 - 020FFFFF		Multibus memory	–
02100000 - 0210FFFF		Multibus I/O	–
02110000 - 02110001	16	System control register	–
02110100 - 02110103	32	System status register	–
02120000	8	Counter timer	–
02120040	8	Counter control register	–
02120100 - 0212013F		Serial ports	–
020B0000 - 020B7FFF		NVRAM	Over Multibus

Table D-17 Processor Memory Map for CSC/2, CSC/3, and CSC/4 Cards, Including IGS and Cisco 3000

Address	Description	Comments
D0D0D0D	"Poisoned free" address	Used by the "poisoned free" code to make sure the system is not accessing freed memory. An error at or near this location usually indicates a software bug.
2100000 - 21FFFFF	Multibus I/O space	Not all I/O space is occupied by interface cards. Bus errors that do not correspond to a real interface card are probably software bugs.
210C000 - 210C200	MCI and ciscoBus controllers (CSC-CCTL and CSC-CCTL2)	Common failures result from attempts to access the command and argument registers that occupy the first 4 bytes of the address space of each board.
21000A0 - 21000AF	Netrionix 4 Mbps Token Ring card	Each card occupies 4 bytes.
21000B0 - 21000BD	CSC-C2CTR card	Each card occupies 2 bytes.
2100000 - 2100003	Control register for the ENVM	Environmental monitor card.
2000000 - 20FFFFF	Multibus memory space	Used by interface cards and by shared Multibus memory.
20C0000 - 20FFFFF	Shared memory on CSC-R16 cards	Token Ring units 5 and 6. Each card has 0x20000 bytes of memory.
20B0000 - 20BFFFF	Multibus NVRAM (CSC/2, CSC/3, CSC/4 cards)	Cards with 32 KB RAM only go through 0x20B7FFF.
2040000 - 20405FF	CSC-16 card asynchronous lines (CSC/2, CSC/3, CSC/4 cards)	Each UART is 0x20 bytes; there are two lines per UART.
2010000 - 20AFFFF	Shared memory on CSC-R16 cards	Units 0–4. Each card has 0x20000 bytes of memory.
2000000 - 2007FFF	Shared Multibus memory primarily used by CSC-R Token Ring cards	Each card has a system control area within this memory, but the address of each area is decided at runtime and is difficult to predict.

Address	Description	Comments
–	System ROM address space	The ROM monitor starts at the bottom of ROM and is followed by the system image. The location of the system image is not always known and is important only for images that are run from ROM. A bus error in valid ROM space might indicate bad ROMs, a bad processor card, or in the case of run-from-ROM images, a software bug in which the software tries to write into ROM.
1000000 - 107FFFF	System ROM address space	512-KB system ROMs on the CSC/2, CSC/3, and CSC/4 cards, IGS, CS-3000. Run from ROM, system images exist only on the CSC/2 card.
1000000 - 10FFFFF	System ROM address space	1-MB system ROMs on the CSC/2, CSC/3, and CSC/4 cards, IGS, CS-3000. Run from ROM, system images exist only on the CSC/2 card.
1000000 - 11FFFFF	System ROM address space	2-MB system ROMs on the CSC/2, CSC/3, and CSC/4 cards and the IGS. Run from ROM, system images exist only on the CSC/2 card.
–	Main processor RAM	Bus errors here are usually caused by a hardware failure on the processor card.
0000 - 0FFFFF	Main processor RAM	CSC/2 card and IGS with 1 MB. On the IGS, the top 0.5 MB is shared packet memory.
0000 - 17FFFF	Main processor RAM	IGS with 1.5 MB. The top 0.5 MB is shared packet memory.
0000 - 3FFFFF	Main processor RAM	CSC/3 card
0000 - FFFFFF	Main processor RAM	CSC/4 card
0000 - 47FFFF	Main processor RAM	IGS with 4.5 MB. The top 0.5 MB is shared packet memory.
0000 - 0FFF	System page	The system page contains several processor and ROM monitor data structures, primarily the trap and interrupt vectors. If the low page gets corrupted, the system might hang rather than crash.

APPENDIX E

References and Recommended Reading

This appendix lists technical publications—many of which are available commercially—that you might find useful when troubleshooting internetworks.

Commercially Available Publications

Chappell, L. *Novell's Guide to NetWare LAN Analysis*. Novell Press; 1993.

Held, G. *Data Communications Testing and Troubleshooting*. Second Ed. Van Nostrand Reinhold; 1992.

Jones, N.E.H., and D. Kosiur. *Macworld Networking Handbook*. IDG Books Worldwide, Inc.; 1992.

Malamud, C. *Analyzing DECnet/OSI Phase V*. Van Nostrand Reinhold; 1991.

Malamud, C. *Analyzing Novell Networks*. Van Nostrand Reinhold; 1990.

Malamud, C. *Analyzing Sun Networks*. Van Nostrand Reinhold; 1992.

Miller, M.A. *LAN Protocol Handbook*. M&T Publishing; 1990.

Miller, M.A. *LAN Troubleshooting Handbook*. M&T Publishing; 1989.

Miller, M.A. *Troubleshooting Internetworks*. M&T Publishing; 1991.

Perlman, R. *Interconnections: Bridges and Routers*. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1992.

Technical Publications and Standards

IBM. *Token-Ring Problem Determination Guide*. SX27-3710-04; 1990.

Apple Computer, Inc. *Inside AppleTalk*. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1991.

Apple Computer, Inc. *Planning and Managing AppleTalk Networks*. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc.; 1991.

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Z