WHITE PAPER

TROUBLESHOOTING SNA SWITCHING SERVICES: A GUIDE TO PROBLEM RESOLUTION

SNASw TROUBLESHOOTING OVERVIEW

SNA Switching Services (SNASw), like many network technologies that perform a protocol integration function, has characteristics that can make problem resolution difficult. Because the product operates both in an SNA environment as well as an IP environment, it is sometimes necessary to gather information from several sources to debug a particular problem. There are a number of good tools available to help diagnose and resolve any problem you might encounter. However, it is important to understand the specific nature and scope of the problem so that you can determine where to do your analysis.

This guide is designed to provide a strategy for dealing with problems related to SNASw, to explain the tools available to help diagnose problems, and to provide specific actions to take for various types of problems you may encounter. It is in no way meant to replace the IOS Command Reference and Configuration Guides, which should be used to find out more about the **snasw** commands referenced in this document.

OVERVIEW OF SNASw ENVIRONMENT

SNASw is the Cisco® recommended solution for supporting SNA-related devices and traffic in an IP-based network. SNASw is available as a component of the Cisco IOS® Software and is supported on a wide variety of router platforms.

SNASw implements an Advanced Peer-to-Peer Networking (APPN) branch network node (BrNN). As such, it appears as a network node (NN) to the downstream devices that connect through the node and as an end node (EN) to other upstream APPN nodes. SNASw also supports the Enterprise Extender (EE) transport option that transmits SNA traffic natively using IP/User Datagram Protocol (UDP). With EE, flow control and Layer 4 connection functions are handled by a protocol known as High Performance Routing (HPR)/IP.

The very nature of the software and its ability to support both SNA and IP transport protocols facilitates network designs that adhere to one of two main topologies: SNASw remote (see Figure 1) and SNASw with Data-Link Switching Plus (DLSw+) (see Figure 2).

Figure 1

SNASw Remote

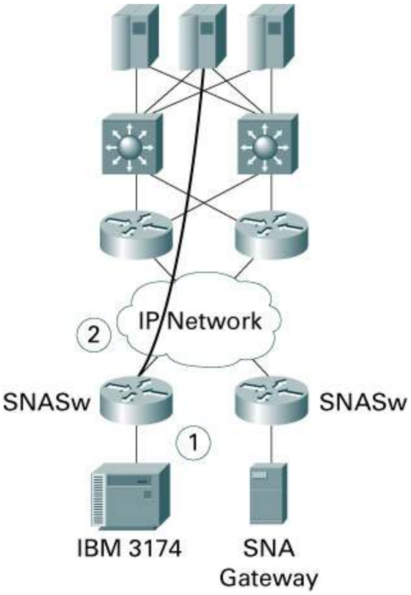
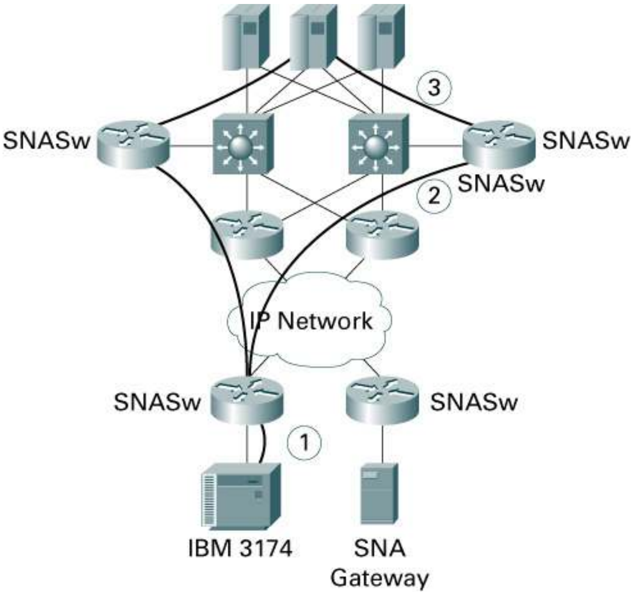


Figure 2

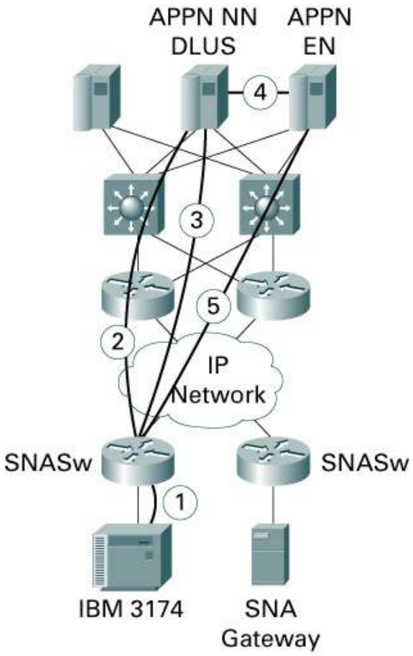
SNASw with DLSw+



There are various connection segments within the network, and this is where problems are likely to be seen and where diagnosis takes place. The type of problem dictates the information that needs to be gathered and from which points in the network information should be obtained. For example, Figure 1 shows a network with HPR/IP as the upstream connection from SNASw. In connection segment 1, a downstream physical unit (PU type 2 or 2.1) connects to an interface on the router using Logical Link Control, Type 2 (LLC2) or Synchronous Data Link Control (SDLC) protocol. Figure 2 shows a network that uses DLSw+ to transport SNA traffic over an IP network. SNASw is used at the data center to provide enhanced redundancy to the mainframe Parallel Sysplex environment. In connection segment 3, the upstream connection from SNASw can be HPR/IP or SNA HPR using LLC2. In connection segment 2, DLSw+ peering connects data center and branch routers. As before, downstream devices connect using LLC2 or SDLC in connection segment 1.

A number of general actions take place in the network to provide data transport services for downstream devices. Figure 3 depicts a typical network with SNASw deployed at the branch using Enterprise Extender (HPR/IP) as the transport protocol for SNA traffic. In this environment, several actions permit connectivity and subsequent data transfer to occur. First, it is common to define the primary NN server and backup NN server as upstream links from SNASw. One link must be in an Active state with a control point (CP)-to-CP session for subsequent connectivity to occur. If the links are not active, then follow the troubleshooting steps outlined in the section Uplink Fails to Connect. Downstream devices also connect to SNASw.

Figure 3
High-Level Data Flows for SNASw



For example, Figure 3 shows the high-level data flows that occur in SNASw as a series of steps. In step 1, a downstream PU 2 establishes an LLC2 connection by initiating a TEST request to a Media Access Control (MAC) address locally defined to SNASw, followed by an eXchange IDentifier (XID). In step 2, SNASw, acting as the Dependent Logical Unit Requestor (DLUR), establishes a DLUR/Dependent LU Server (DLUS) path with the DLUS. SNASw passes a REQACTPU (containing the XID from the downstream PU) over the DLUR/DLUS pipe and the downstream PU and LUs are then activated (System Services Control Point [SSCP]-to-PU/LU sessions via ACTPU/LU from the DLUS). An end user (LU) then requests a session with an application LU, named APPLA, which resides on the APPN EN host. In step 3, SNASw passes the INITSELF or USSLOGON to the DLUS over the DLUR/DLUS pipe. In step 4, the NN server informs the application of the session request and provides a route to the SNASw BrNN that handles the LU. Because a connection network has been defined, in step 5, the EN host is able to establish a direct link to the SNASw router over IP. The LU-to-LU session is then activated and data transfer begins.

This is a very simplistic description of the connectivity actions that are required to establish data transfer in this environment. When troubleshooting, try to determine the specific sequence and point in the flow where your problem occurs and then start your debug activities targeting that particular point.

TROUBLESHOOTING BASICS

Internetworking of IP and SNA can be complex and this particular environment imposes some difficulty because of the historical differences inherent in TCP/IP and SNA networks and the skills required in each area. When faced with a problem that requires detailed analysis, using a standard troubleshooting methodology reduces the time it takes to isolate and resolve the problem.

Troubleshooting Methodology Overview

It is important that you approach any internetworking problem using a problem-solving model. First, establish a clear understanding and definition of the problem. Next, gather all relevant information using the tools and techniques described in this document. After analyzing the information, create an action plan to address the likely cause of the problem. If the symptoms are not resolved, try another action plan or gather additional information that might lead to another conclusion.

The troubleshooting methodology adopted in this document follows these general steps:

- **Diagram the problem**—Begin with a detailed diagram of the network. Maintaining accurate diagrams of the physical and logical components and their relationships is important to ensure continued operation and availability. It helps to further illustrate the components involved in the data path specific to the problem at hand.
- **Isolate the problem**—Gather detailed information about the problem. This includes configurations, protocols, data paths, and historical performance data. Determine the starting point as well as fault isolation procedures.
- **Correct the problem**—Make appropriate hardware, software, or configuration changes to correct the problem.
- **Verify that the trouble is corrected**—Perform operational tests to verify that the trouble is corrected.

The troubleshooting steps presented in Troubleshooting SNASw Operational Problems and the example scenarios presented in the appendix, Diagnostic Output Examples, generally follow this methodology in listing typical symptoms and provide associated diagnostics measures.

Tools

SNASw was designed with support in mind. The product includes trace analysis and debugging tools to help you and Cisco diagnose any problem that might be encountered. These tools, in conjunction with various **show snasw** commands, enable problem diagnosis, isolation, and resolution of most problems. At times, additional trace and debug information, such as that available from IBM hosts or LAN analyzers, is required.

snasw pdlog

SNASw contains its own problem determination logging facility known as the pdlog. This is a cyclic buffer that provides detailed information on recent state transitions, traffic, and events for SNASw. The pdlog is always enabled (cannot be turned off), but the size of the buffer and the type of abbreviated pdlog messages written to the router log is controlled with the **snasw pdlog** command:

```
snasw pdlog [problem | exception | info] [buffer-size buffer-size-value] [file filename timestamp]
```

All detailed pdlog records (**problem**, **exception**, and **informational**) are written to the internal pdlog buffer *whether snasw pdlog is configured or not*. However, the pdlog configuration command determines which level of associated pdlog messages are written to the router log. If not configured, the default is **exception**, which means that only **problem** and **exception** pdlog messages will be seen in the router log.

The **buffer-size** keyword determines the size of the pdlog buffer (in processor memory). With IOS 12.1 and 12.2, the maximum **buffer-size** is 16,000 KB. With Cisco IOS Release 12.3 and above, the maximum **buffer-size** is 64,000 KB. If not coded, the default is a 500-KB buffer.

You can display information from the pdlog buffer at the router console using the **show snasw pdlog** command:

```
show snasw pdlog [brief | detail] [all] [last] [next] [filter filterstring] [id recordid]
```

You can also copy the entire pdlog file to a file server or flash using the **snasw dump** command (which is explained later in this document).

Note: The **snasw pdlog** is a very useful tool, and should be one of the first places you look when diagnosing a problem. The pdlog messages you see in the router log have an identifier that can be used to examine the detailed entry in the pdlog cyclic buffer. This detailed entry often contains resource names, session identifiers, sense codes, and so on that can lead you directly to the next step in resolving the problem.

snasw dlctrace

The **snasw dlctrace** command traces frames arriving and leaving the SNASw stack within IOS:

```
snasw dlctrace [buffer-size buffer-size-value] [file filename [timestamp]] [frame-size frame-size-value | auto-terse] [format [brief | detail | analyzer]] [nostart]
```

This trace facility is designed for use by network support personnel to troubleshoot connectivity problems. The trace can be stopped and started using the **snasw stop|start dlctrace** command.

The **buffer-size** keyword determines the size of the dlctrace buffer (in processor memory). With Cisco IOS Releases 12.1 and 12.2, the maximum **buffer-size** is 16,000 KB. With Cisco IOS Release 12.3 and above, the maximum **buffer-size** is 64,000 KB. The larger the buffer you configure, the better the chance that important trace records will not be lost. If not coded, the default is a 500-KB buffer.

Unless a problem requires you to see application data in the trace, it is recommended that you configure **frame-size auto-terse**. This trims all application data from the trace records, allowing more trace records to fit within the cyclic buffer. You can also filter which records are written to the buffer (thus allowing a longer duration of trace) by using the **snasw dlcfilter** configuration command.

You can use the **show snasw dlctrace** command to examine the dlctrace records (they are printed to the router log), but it is often easier to copy the dlctrace file to a file server (see the **snasw dump** command later in this document).

Note: The **snasw dlctrace** is a very powerful tool. Because it has very little overhead (between 2 and 8 percent), Cisco recommends that it be enabled when testing new implementations. Some customers also choose to leave it enabled in production to facilitate collecting documentation in the event that a problem is encountered.

snasw ipstrace

The **snasw ipstrace** command, or interprocess signal trace, is used for debugging internal SNASw software problems. It copies internal signal flows into a cyclic memory buffer, which can affect router performance by as much as 20 percent. Therefore, you should use this command only as directed by Cisco service personnel:

```
snasw ipstrace [buffer-size buffer-size-value] [file filename timestamp]
```

The impact on performance can be reduced by configuring the **snasw ipsfilter** command prior to enabling the **snasw ipstrace** command. This allows you to specify only those internal components identified by Cisco personnel as being related to the problem at hand.

The **buffer-size** keyword determines the size of the ipstrace buffer (in processor memory). With Cisco IOS Releases 12.1 and 12.2, the maximum **buffer-size** is 16,000 KB. With Cicsco IOS Release 12.3 and above, the maximum **buffer-size** is 64,000 KB. The larger the buffer you configure, the better the chance that important trace records will not be lost. If not coded, the default is a 500-KB buffer.

After the trace has been captured, it can be copied to a server using the **snasw dump** command covered in the next section of this document. This enables the Cisco engineer to perform additional processing of the data contained in the file. There is also a **show snasw ipstrace** command, but its use is not recommended except as advised by a Cisco engineer.

snasw summary-ipstrace

```
snasw summary-ipstrace [buffer-size buffer-size-value] [file filename timestamp]
```

There is an abbreviated version of the ipstrace called a summary-ipstrace. This trace is always enabled (cannot be turned off), but the size of the buffer and the file url are specified via the **snasw summary-ipstrace** command. Because of its limited information, the summary-ipstrace is rarely used.

snasw dump

```
snasw dump all | dlctrace | ipstrace | summary-ipstrace | pdlog
```

The **snasw dump** command copies the pdlog and dlc, ips, and summary-ips traces from their internal buffers to an external file server or to Flash memory. The command uses the file destinations previously specified using the **file** keyword on the related **snasw dlctrace, snasw ipstrace**, and **snasw pdlog** commands. For example, to copy the pdlog to a Trivial File Transfer Protocol (TFTP) server, you would use the following configuration:

```
snasw pdlog problem buffer-size 10000 file tftp://myhost/path/pdlogfilename
```

If no file was specified on the configuration and you issue **snasw dump dlctrace** or **ipstrace** or **summary-ipstrace** or **pdlog**, then you will be prompted for the file name. However, **snasw dump all** does not prompt for file names (they must have been previously configured for the command to succeed).

The files that are generated for the pdlog and dlctrace (in **format detail**) may be up to twice as large as the configured **buffer-size**. This is because the binary data in the buffer is converted to ascii text and then written to the file. In Cisco IOS Releases 12.1 and 12.2, **buffer-size** was limited to 16 MB to avoid the dumped ascii file size from exceeding the TFTP maximum size of 32 MB. Beginning with Cisco IOS Release 12.3, SNASw allows **buffer-size** to be specified to a maximum value of 64 MB. If TFTP is the transport protocol being used, SNASw copies the first 32 MB of ascii text to the configured file name and then copies subsequent 32-MB files with .01, .02, etc. appended to the name.

The files that are generated for the dlctrace (in **format analyzer** which is SnifferPro™-compatible) and ipstrace consist of binary data, so their size is the same or less than the configured **buffer-size**.

snasw msgdump

The **snasw msgdump** command can be used to enable automatic dumping of the dlctrace, ipstrace, and pdlog files (and optionally to execute a **write core** command) when a specified SNASw pdlog message is written to the router log:

```
snasw msgdump pdlog_message_id [writecore]
```

This can be very helpful to trigger trace information capture following a particular event, and is usually configured at the direction of Cisco support when trying to collect documentation for a service request. This is a one-time-only trigger—you must remove **snasw msgdump** from the configuration (using the **no** form of the command) and add it in again to re-enable the automatic dumping.

When using **snasw msgdump**, it is important that you correctly configure the **file** keyword on the respective **snasw pdlog**, **snasw dlctrace**, and **snasw ipstrace** commands, otherwise when the msgdump is triggered, the files will be lost. Also, you may find it helpful to configure the **timestamp** keyword, which appends the time the file was dumped to the end of the file name. This allows you to know when the file was written and to avoid the file copy from failing because of a duplicate file name.

An enhancement was made to the **snasw msgdump** processing in Cisco IOS Release 12.3 to add SNA alert support. In order to take advantage of this, SNASw must have an Alert focal point. Use the **show snasw node** command to see if there is a cpname in the Alert focal point field. If not, and if SNASw has an active Network Node Server (NNS), on the NetView host you can issue the command:

```
FOCALPT CHANGE,FPCAT=ALERT,TARGET=snasw-cpname | snasw-nns-cpname
```

When the SNASw router (or its NNS) is in NetView's alert sphere of control, then when a msgdump event is triggered, SNASw will send an MDS-MU alert. The alert will have an identifier of x'DAED5B0B', and will contain the pdlog entry which triggered the msgdump. This informs the network operator that a monitored event has occurred (so they know to retrieve the pdlog/trace files dumped by SNASw), and can trigger host automation to collect VTAM traces or take other appropriate action. This is especially useful when tracking down DLUR/DLUS-related issues.

If **writecore** is specified, a **write core** command is attempted whenever the **msgdump** condition is triggered (in addition to the dumping of the pdlog, dlc and ips traces). The **write core** command is issued using the existing configuration parameters: server host, transfer protocol, user name, and password. For the **write core** command to be successful, the **exception dump** statement must be configured to specify the destination server. Cisco also recommends that the **compress** option be used for the core file name in the **exception core** command to save space on the server.

```
exception dump <host name or address>
exception core-file <core file name> compress
```

If no exception protocol is configured, the **write core** operation would be attempted using tftp; the core file is written under the /tftpboot directory. If ftp is specified for exception, then the user name and password information must be configured:

```
ip ftp user <userid>
ip ftp password <password>
exception protocol ftp
```

Note: The user must be aware that the **write core** operation puts a load on the router and may momentarily cause some network disruption. Therefore, the **writecore** option should be used only at the explicit request from Cisco TAC.

snasw arbdata

The HPR protocol in SNASw utilizes the Adaptive Rate Based (ARB) algorithm to monitor the available bandwidth of the network and obtain the best throughput for HPR connections. When performance problems are detected with HPR connections, it is sometimes necessary to gather real-time values of ARB algorithm variables as the data flows through the HPR connection. This can be accomplished by issuing:

```
snasw start | stop arbdata local-tcid
```

Output from the **start** form of this command is written to the router log and can consist of many lines of text per second, so it is best to make sure that you have configured **logging buffered** and **no logging console** before issuing this command. You issue the **stop** form of the command to stop the messages from being written to the router log.

Note: Interpreting output from the **snasw arbdata** command requires a detailed understanding of the HPR Architecture and ARB algorithm. Also, this command can result in a high volume of messages being written to the router log. For these reasons, Cisco recommends this command only be used under the direction of Cisco service personnel.

snasw event

By default, only defined links and DLUS events are sent to the pdlog console. To get more information for debug purposes, use the **snasw event** global configuration command:

```
snasw event [cpcp] [dlc] [implicit-ls] [port]
```

SNASw Debug Commands

Output from Cisco IOS **debug** commands provides a valuable source of information and feedback concerning state transitions and functions when assessing problems. However, the **snasw dlctrace** and **snasw ipstrace** commands should be favored over **debug snasw dlc** and **debug snasw ips** commands in an SNASw environment. The **snasw** trace commands write directly to a cyclic buffer rather than to the router log, thereby avoiding flooding and providing flexibility in accessing the trace records.

Other debug commands, such as **debug dlsw** or **debug llc,** may be useful in environments where DLSw+ is used in conjunction with SNASw or to trace activity at the interface level.

Core Files

If your router crashes, it is sometimes useful to obtain a full copy of the memory image (called a core dump) to identify the cause of the crash. Not all crash types produce a core dump. The following example configures a router to use FTP to dump a core file named dumpfile to the FTP server at 172.17.92.2 when it crashes:

```
ip ftp username red
ip ftp password blue
exception protocol ftp
exception dump 172.17.92.2
exception core-file dumpfile
```

Details covering the procedure for obtaining a core dump can be found at:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf013.htm.

You can initiate transfer of a core dump manually by entering:

```
write core
```

```
cheney#wr core
Remote host [172.18.60.179]?
Base name of core files to write [cheney-core]?
writing compressed ftp://172.18.60.179/cheney-coreiomem.Z
!!!!!!!!!!!!!!
Writing cheney-coreiomem.Z
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
EOF-inputbuf 4000000! [OK]
5242880 bytes copied in 41.4 secs (127875 bytes/sec)
writing compressed ftp://172.18.60.179/cheney-core.Z
!
Writing cheney-core.Z
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
EOF-inputbuf 83B00000 [OK]
61865984 bytes copied in 321.672 secs (192728 bytes/sec)
cheney#
```

You might be requested to perform this action by the Cisco Technical Assistance Center (TAC) for debug purposes even if your router did not crash.

Note: The **snasw ipstrace** and **snasw dlctrace** commands provide additional important debug information for the development engineers. If these trace facilities are activated, stop them by issuing **snasw stop dlctrace** and **snasw stop ipstrace** before forcing **wr core**. If the traces are not stopped prior to the **wr core** command, some corruption of trace records can occur.

Host Commands and Traces

In some cases, it may be necessary or helpful to perform traces and displays from the host in addition to traces at the SNASw router. This section provides examples of various host-based trace facilities and associated job control information.

VTAM Internal Trace

Because VTAM is a NNS and Dependent Logical Unit Server (DLUS) for SNASw, it is often necessary to collect a VTAM Internal Trace (VIT) to diagnose problems. The VIT has many options and can be collected in several ways (GTF or Data Space), so it is best to refer to the VTAM Diagnosis Guide (a licensed manual) for details.

Collecting Buffer and CCW Traces Using the Generalized Trace Facility

Use JCL similar to the following statements to invoke the generalized trace facility (GTF):

```
//GTFNEW  PROC MEMBER=GTFPARM
//IEFPROC EXEC PGM=AHLGTF,PARM='MODE=EXT,DEBUG=NO,TIME=YES',           *
//  TIME=1440,REGION=2880K
//IEFRDER DD   DSNAME=SYS4.TRACE,DISP=SHR
//SYSLIB  DD   DSNAME=SYS1.PARMLIB(&MEMBER),DISP=SHR
```

Follow these steps to perform a buffer trace. First, start the GTF:

```
s gtf
AHL103I  TRACE OPTIONS SELECTED --USR,RNIO
  *10 AHL125A  RESPECIFY TRACE OPTIONS OR REPLY U
r 10,u
```

Then start the buffer trace by entering the statement:

```
f net,trace,type=buf,id=<resource>
```

Take action to recreate the problem you are tracing. When complete, stop the buffer trace with the statement:

```
f net,notrace,type=buf,id=<resource>
```

Then, stop the GTF by displaying the job and using the **purge** command:

```
d a,gtf

RESPONSE=DEREK
   IEE115I 12.02.03 2001.303 ACTIVITY 203
JOBS     M/S    TS USERS    SYSAS    INITS   ACTIVE/MAX VTAM    OAS
   00000    00011    00002      00024    00004    00002/00010     00001
    GTF      0342     IEFPROC  NSW  S  A=002C   PER=NO   SMC=000
                                       PGN=001  DMN=005  AFF=NONE
                                       CT=000.770S  ET=076.525S
                                       WUID=STC00229 USERID=++++++++
                                       ADDR SPACE ASTE=05323B00
   4020000 DEREK    01303 12:01:22.91 STC00229 00000090  AHL031I GTF INITIALIZATION         COMPLETE

p gtf.342
```

If you need to get a channel command word (CCW) trace, start the GTF and enter these statements where **addr** is the address to trace, **len** is how much of each datastream to collect (the default is 256), and **num ccws** is the number of CCWs to collect:

```
s gtf
r nn,trace=siop,iop,ccwp
r nn,io=sio=<addr>,ccw=(data=<len>,ccwn=<num ccws>),end
```

r nn,u

S GTF

```
 IRR813I NO PROFILE WAS FOUND IN THE STARTED CLASS FOR 214
         GTF WITH JOBNAME GTF. RACF WILL USE ICHRIN03.
 $HASP100 GTF      ON STCINRDR
 IEF695I START GTF      WITH JOBNAME GTF      IS ASSIGNED TO USER
 ++++++++
 $HASP373 GTF      STARTED
 IEF403I GTF - STARTED - TIME=13.32.44
 AHL121I  TRACE OPTION INPUT INDICATED FROM MEMBER GTFPARM  OF PDS
 SYS1.PARMLIB
 TRACE=RNIO,USR
 00010000
 AHL103I  TRACE OPTIONS SELECTED --USR,RNIO
*11 AHL125A  RESPECIFY TRACE OPTIONS OR REPLY U
```

R 11,TRACE=SIOP,IOP,CCWP

```
IEE600I REPLY TO 11 IS;TRACE=SIOP,IOP,CCWP
 TRACE=SIOP,IOP,CCWP
 AHL138I  SIO TRACE OPTION REPLACED BY SSCH TRACE OPTION
*12 AHL101A  SPECIFY TRACE EVENT KEYWORDS --IO=,SSCH=,CCW=,IO=SSCH=
```

R 12,IO=SIO=400,CCW=(DATA=1024,CCWN=50),END

```
 IEE600I REPLY TO 12 IS;IO=SIO=400,CCW=(DATA=1024,CCWN=50),END
IO=SIO=400,CCW=(DATA=1024,CCWN=50),END
AHL103I  TRACE OPTIONS SELECTED --IO=SSCH=(0400)
AHL103I  CCW=(SI,CCWN=50,DATA=1024)
13 AHL125A  RESPECIFY TRACE OPTIONS OR REPLY U
```

R 13,U

```
IEE600I REPLY TO 13 IS;U
```

Recreate your problem and then stop the trace facility. After you have trace data, you can format the trace information using interprocess communications subsystem (IPCS). The following example shows sample JCL to format a buffer trace with IPCS:

```
 //IPCSRUN JOB CLASS=A,MSGCLASS=X,NOTIFY=WINNETT
 //IPCS      EXEC PGM=IKJEFT01,DYNAMNBR=20,REGION=1500K
 //SYSPROC   DD  DSN=SYS1.SBLSCLI0,DISP=SHR
 //IPCSPRNT  DD  SYSOUT=*
 //IPCSTOC   DD  SYSOUT=*
 //SYSUDUMP  DD  SYSOUT=*
 //SYSTSPRT  DD  SYSOUT=*
 //SYSTSIN   DD  *
 DELETE 'SYS4.IPCS.DDIR.CLUSTER' PURGE CLUSTER
 BLSCDDIR DSNAME('SYS4.IPCS.DDIR.CLUSTER') VOLUME(OPWK01)
 IPCS NOPARM
 SETDEF DSNAME('SYS4.TRACE') LIST NOCONFIRM NOPRINT
```

```
GTF USR(FEF)
END
```

This example shows how to format a CCW trace with IPCS:

```
//IPCSRUN JOB CLASS=A,MSGCLASS=X,NOTIFY=WINNETT
//IPCS      EXEC PGM=IKJEFT01,DYNAMNBR=20,REGION=1500K
//SYSPROC   DD  DSN=SYS1.SBLSCLI0,DISP=SHR
//IPCSPRNT  DD  SYSOUT=*
//IPCSTOC   DD  SYSOUT=*
//SYSUDUMP  DD  SYSOUT=*
//SYSTSPRT  DD  SYSOUT=*
//SYSTSIN   DD  *
DELETE 'SYS4.IPCS.DDIR.CLUSTER' PURGE CLUSTER
BLSCDDIR DSNAME('SYS4.IPCS.DDIR.CLUSTER') VOLUME(OPWK01)
IPCS NOPARM
SETDEF DSNAME('SYS4.TRACE') LIST NOCONFIRM NOPRINT
GTF USR(ALL) CCW(SI) SSCHIO(400)
END
```

TROUBLESHOOTING SNASw OPERATIONAL PROBLEMS

Problems related to SNASw can be categorized into several basic areas:

- Upstream link activation problems
- Downstream device activation problems
- DLUR/DLUS problems
- Session failures
- Performance-related problems

In addition, problems can be categorized as being associated with particular types of equipment or issues with particular data paths. Because of similarities between symptoms and problems for these different situations, this document addresses these diagnostic topics collectively.

Begin troubleshooting by following the process suggested in the section Troubleshooting Methodology Overview. The diagnostics summaries in this section address the troubleshooting process using three basic stages:

1. Identifying symptoms

2. Isolating problems

3. Resolving problems

Each diagnostic section includes suggestions for identifying and isolating problems. It is assumed that relevant network topology diagrams have been obtained for reference prior to troubleshooting. Specific diagnostic output is included to illustrate how network entities react to failures and how to discern specific failures. Sample output for some of the commands is shown in Appendix B, Diagnostic Output Examples. If you need additional help in debugging or analyzing a particular problem, please contact the Cisco TAC at www.cisco.com.

Uplink Fails to Connect

If the uplink fails to connect, follow these troubleshooting steps:

Step 1. Verify the status of the defined uplinks using the **sh snasw link** command.

Step 2. Use **show snasw pdlog detail all | include** *linkname* to see if there are any entries specific to this link name in the pdlog. If so, you will need to show or dump the entire pdlog and find out which records apply.

Step 3. A defined uplink will attempt to establish connection when SNASw is started if the **nostart** parameter is not used. Issue the **sh run | include snasw** command to see the configuration for SNASw.

Step 4. If the link definition uses **ip-dest** *ip-address*, then the link is defined for HPR/IP EE. Verify IP connectivity to the host by issuing an extended **ping** originating from the interface associated with the hpr-ip port.

Step 5. If the ping fails, continue troubleshooting the IP connectivity issue using commands such as **trace, sh ip ospf**. Check neighbor connectivity to the host, Open Shortest Path First (OSPF) definitions on the host, and routing to the Virtual IP Addressing (VIPA) address.

Step 6. If the ping succeeds, then check the interaction between Virtual Telecommunications Access Method (VTAM) and the TCP/IP stack, including that **vtam TCPNAME** points to the correct stack (see **d net,vtamspts**) and VTAM external communication adapter (XCA) major node is set for **medium=HPRIP**.

Step 7. If the upstream link is SNA LLC2, then begin troubleshooting connectivity at Layer 2.

Step 8. Verify that the remote MAC and remote service access point (SAP) is defined on the **snasw** link.

Step 9. Trace the LLC2 layer using **debug llc2 state** and **debug llc2 packet**. Be sure to set **access-list 1100** to limit debug output.

Step 10. You can also use the SNASw trace facility to trace the SNASw DLC layer. Issue **snasw dlctrace**. Try the link again with the trace on. Display the trace using the **sh snasw dlctrace** or **snasw dump dlctrace** command.

Step 11. Examine and collect system or netlog information from the host network node.

Step 12. Use the information gathered to diagnose the cause of the failure.

Step 13. Check the VTAM definitions, node type, and CPNAME.

Downstream PU Does Not Activate

The downstream PU may be having trouble trying to connect to SNASw or the problem may be upstream of SNASw for DLUR PUs. Follow these troubleshooting steps:

Step 1. Issue the **sh snasw link** command.

Step 2. Examine the **pdlog** for error or exception data related to this link or PU.

Step 3. Issue the **sh snasw dlus** command. The DLUS will be active if, and only if, there is DLUR traffic.

Step 4. Issue the **sh snasw pu** command.

Step 5. Check to see if other PUs have established connectivity through this node.

Step 6. Gather host information, including **D NET,ID=puname; D NET,DLURS**.

Step 7. Issue the **sh snasw port** command. Determine the port through which the downstream PU connects and verify that it is active.

Step 8. If the port is not active, troubleshoot as a configuration problem or interface problem.

Step 9. Check that the MAC/SAP on the downstream device matches that defined for SNASw on interface.

Step 10. Ensure that you have enabled port event notifications using the **snasw event dlc implicit-ls port** command. This causes messages to be written to the router log for certain events.

Step 11. Examine **snasw dlctrace** data.

Problem Establishing Connection for Downstream End Node

You may encounter a problem with an APPN device downstream from SNASw. After you have established that no physical or lower layer problem exists, begin troubleshooting the connection establishment sequence using these steps:

Step 1. Issue the **sh snasw link** command.

Step 2. Try starting the link on the downstream device and observe **pdlog** messages. If there is a problem with the XID between the downstream device and snaswitch, the detailed pdlog message will have additional information, including the last sent and received XIDs.

Step 3. Check that the MAC/SAP on the downstream device matches that defined for SNASw on interface.

Step 4. Verify the node name and node type.

Step 5. Trace the link activation using the **snasw dlctrace** command.

Step 6. Examine the **snasw dlctrace** data.

User Cannot Connect to Application

The reason an end user cannot connect to the application may be due to a network problem in establishing a dynamic link to the EN host. In this case, use the following troubleshooting steps:

Step 1. Issue the **sh snasw link** command. Determine whether an active link has been established to the EN data host.

Step 2. If no link exists, perform **snasw dlctrace** on the upstream port.

Step 3. Verify the connection network definition (that is, the virtual routing node [VRN] name) between the SNASw and host definitions.

Step 4. Observe any error messages in **pdlog**, in the upstream NN server, and at the destination host.

Step 5. Examine information gathered for the cause of failure.

Intermittent Session Failures

Intermittent session failures are sometimes hard to troubleshoot, particularly if you cannot readily recreate the problem. You can use the **snasw msgdump** command to trigger a dump of trace files when a particular message occurs. If the problem is repeatable, follow these steps:

Step 1. Determine any messages related to the last occurrence of a problem.

Step 2. Use **snasw msgdump <msg-id>** to trigger a dump of **dlctrace** information on failure.

Step 3. Examine the **snasw dlctrace** data.

Poor Performance

There are many reasons that an end user may experience performance problems or observe high response time or low throughput. It is important to determine the correct cause of the poor performance. Try to determine whether poor performance results from excessive traffic rates (lack of router capacity) or if it is related to specific session parameters or connection types, using the following steps:

Step 1. Issue the **sh snasw port det** command.

Step 2. Examine the router for high CPU utilization (see the next section).

Step 3. Examine any historical and trending information that is available (Cisco Internet Performance Monitor data, for example).

Step 4. Examine the links along the path between the user and the host. Check the utilization and quality of service (QoS) settings.

Step 5. Issue the **sh interface** command and look for dropped packets.

Step 6. If using HPR, issue the **sh snasw rtp detail** command.

Step 7. Work with a specific user to isolate performance.

Step 8. Gather session information using **snasw dlctrace**.

Step 9. If using HPR, and as advised by Cisco service personnel, gather **snasw arbdata** log messages.

High CPU Utilization

If the router CPU utilization is above 95 percent, the performance of the router may be affected, and packets can be delayed or dropped. It is important to investigate the cause to determine if there is extraneous traffic, a misconfiguration, a need for a more powerful router platform, or a possible software defect. If you have access to the router and can enter **show** commands, follow these steps to determine if SNASw is the cause of the high CPU:

Step 1. Issue the **show processes cpu** command. If process switched IP traffic is causing problems, then the IP Input process will reflect this in the output. In this situation it would be important to collect the output from the **show interfaces**, **show interfaces stat**, and **show interface switching** commands to further diagnose the problem.

Step 2. If the high CPU is attributed to the process SNA Switch, then SNASw is using high CPU.

Step 3. Issue the **show snasw statistics** command to determine which SNASw component is responsible.

Step 4. Collect dlctrace, ipstrace, and sniffer traces and look for patterns. The ipstrace in particular can be useful in detecting software loops within SNASw.

Step 5 It may be that the traffic load is simply beyond the capability of the platform in use. See capacity planning and performance data at http://www.cisco.com/en/US/tech/tk331/tk336/technologies_design_guide09186a0080214a16.shtml.

SNASw CHARACTERISTICS AND KNOWN ISSUES

In some cases, the normal mode of operation is not immediately understood and a problem is perceived when there really is none. One particular case is observation of messages indicating a loss of DLUS connection. The DLUS connection is taken down as a normal course of operation if there are no downstream DLUR PUs that require the services of the DLUS. Therefore, the loss of connectivity to the DLUS does not always indicate a problem. Also, repeated activation and deactivation of the DLUR/DLUS session pipe may be the result of a single PU failure.

Another case is that of a REQACTPU failure. It may be that the PU is simply not defined to VTAM or is inactive rather than in a connectable state. Or it could be that the PU definition has the wrong control point name or station identifier. Always check for basic configuration problems before embarking on a full analysis session. In many cases, a quick look with the **sh snasw pdlog** command can determine the cause of the failure.

Session Pacing

You may encounter performance issues with interactive traffic if batch traffic is allowed to operate unpaced or with too large a variable pacing window. Cisco recommends that batch devices such as printers be configured with a fixed pacing window of 7. You can also adjust the maximum receive pacing window for variable pacing using the **max-pacing-window** parameter on the **snasw cpname** configuration command:

```
cheney(config)#snasw cpname NETIFD.CPNAME max-pacing-window ?
  <7-65535>  Maximum window size
```

For more information, refer to the SNASw documentation listed in Appendix A, Related Publications.

Production Recovery and Data Collection

Murphy’s Law states, “If anything can go wrong, it will,” and furthermore, it certainly will happen at the most inopportune time. For this reason, it is useful to establish a basic procedure for off-hours operations staff to follow in the event that a problem arises and no one is available to perform detailed troubleshooting.

In many cases, stopping and restarting SNASw on a specific router will clear up a problem. This can be done with several commands. Use the **snasw stop** command to terminate all sessions, stop all ports and links, and shut down SNASw. To start SNASw, use the **snasw start** privileged EXEC command. Before recycling SNASw, Cisco recommends that operations staff collect the following information at a minimum:

- **show tech**
- **snasw dump pdlog**
- **snasw dump dlctrace**

APPENDIX A: RELATED PUBLICATIONS

For Cisco publications, if you are using a version of Cisco IOS different than what is referenced below, you can find a matching version of the documentation by searching for the title at http://www.cisco.com/public/pubsearch.html.

SNASw Documentation

- Cisco SNASw Website, http://www.cisco.com/en/US/tech/tk331/tk897/tsd_technology_support_sub-protocol_home.html
- *Cisco IOS Bridging and IBM Networking Configuration Guide*, Release 12.3, http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ibm_vcg.htm
- *Cisco IOS Bridging and IBM Networking Command Reference*, Volume 2 of 2, Release 12.3, http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ibm_r2/index.htm
- "SNASw Messages," Release 12.3, http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123sup/123sems/123semv2/emgsnasw.htm

Related Troubleshooting Information

- "Troubleshooting High CPU Utilization on Cisco Routers," http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a00800a70f2.shtml
- "SDLC Debugging," http://www.cisco.com/en/US/tech/tk331/tk336/technologies_tech_note09186a0080094745.shtml
- "Troubleshooting DLSw," http://www.cisco.com/en/US/tech/tk331/tk336/technologies_tech_note09186a008009424a.shtml
- "Fine-Tuning the LLC2 Timers for Better Performance," http://www.cisco.com/en/US/tech/tk331/tk336/technologies_tech_note09186a0080093d89.shtml
- "Understanding and Troubleshooting Network Media Translation," http://www.cisco.com/en/US/tech/tk331/tk336/technologies_tech_note09186a0080093fa1.shtml
- "Understanding and Troubleshooting Local Source-Route Bridging," http://www.cisco.com/en/US/tech/tk331/tk660/technologies_tech_note09186a0080094742.shtml
- Tech Notes, http://www.cisco.com/en/US/tech/tk331/tk336/tech_tech_notes_list.html

Related IBM Documentation

- *TCP/IP Trace Guide*
- *IBM Systems Network Architecture: LU6.2 Reference: Peer Protocols* (SC31-6808)
- *IBM Systems Network Architecture: APPN Architecture Reference* (SC30-3422)
- *IBM Systems Network Architecture: Management Services* (SC30-3346)
- *IBM Systems Network Architecture: Formats* (GA27-3136)
- *IBM APPN Architecture and Product Implementations Tutorial* (GG24-3669)
- *IBM AS/400 Advanced Peer-to-Peer Networking* (GG24-3287)
- *IBM Communications Manager/2 System Management Programming Reference* (SC31-6173)
- *IBM Communications Manager/2 APPC Programming Guide and Reference* (SC31-6160)
- *IBM System/370 Principles of Operation* (GA22-7000)

- *IBM Systems Network Architecture: Technical Overview* (GC30-3073)
- *IBM Systems Network Architecture: VTAM Programming for LU Type 6.2* (SC30-3400)
- *IBM Systems Network Architecture Concepts and Products* (GC30-3072)
- *IBM Systems Network Architecture Format and Protocol Reference Manual: Architecture Logic or LU Type 6.2* (SC30-3269)
- *IBM Systems Network Architecture: Introduction to APPC* (GG24-1584)
- *IBM Systems Network Architecture: Transaction Programmer's Reference Manual for LU Type 6.2* (GC30-3084)
- *IBM Systems Network Architecture: Introduction to Sessions between Logical Units* (GC20-1869)
- *IBM Systems Network Architecture Format and Protocol Reference Manual: Architectural Logic* (SC30-3112)

AIW Documentation

- AIW publications, http://www.networking.ibm.com/app/aiwhome.htm

Many architecture references (including those listed above in **Related IBM Documentation**) can be found at this Website.

APPENDIX B: DIAGNOSTIC OUTPUT EXAMPLES

Show Commands

show snasw session

```
cheney#show snasw session
Number of local endpoint sessions 9
      SNA Local Endpoint Sessions
         PCID (hex)      Partner LU Name   Link/RTP    Mode     COS
      ----------------  -----------------  --------- -------- -------
   1> C193D9033CB91A56  NETA.IBDNT1        @I000013  CPSVCMG  CPSVCMG
   2> EB3FE7B419B132A3  NETA.IBDNT1        @I000013  CPSVCMG  CPSVCMG
   3> C193D9033CB91A50  NETA.MVSB          @R000024  #INTER   #INTER
   4> C193D9033CB91A4E  NETA.MVSB          @R000023  SNASVCMG SNASVCMG
   5> C193D9033CB91A4C  NETA.MVSA          @R000022  #INTER   #INTER
   6> C3BBDE1E415E9C29  NETA.MVSA          @R000021  CPSVRMGR SNASVCMG
   7> C193D9033CB91A3A  NETA.MVSA          @R000021  CPSVRMGR SNASVCMG
   8> C3BBDE1E415E9C05  NETA.MVSA          @R000002  CPSVCMG  CPSVCMG
   9> C193D9033CB91A01  NETA.MVSA          @R000001  CPSVCMG  CPSVCMG

Number of intermediate sessions 0

      SNA Intermediate Sessions
         PCID (hex)     Primary LU Name    Secondary LU Name   Mode      COS
      ----------------  -----------------  -----------------  -------- -------

Number of intermediate DLUR sessions 1

      SNA DLUR Assisted Intermediate Sessions
         PCID (hex)     Primary LU Name    Secondary LU Name   Mode      COS
      ----------------  -----------------  -----------------  -------- -------
   1> C3BBDE1E415E9C4F  NETA.TSOA0002      NETA.RW982303               #CONNECT
```

show snasw dlus

```
cheney#show snasw dlus
Number of Dependent LU Servers 1

      SNA Dependent LU Servers
          DLUS Name      Default?  Backup?  Pipe State         PUs
      -----------------  --------  -------  ----------------  -------
   1> NETA.MVSA          Yes       No       Active                2

cheney#

cheney#show snasw dlus det
Number of Dependent LU Servers 1

1>
DLUS name                                          NETA.MVSA
Is this the default DLUS                           Yes
Is this the backup default DLUS                    No
Pipe state                                         Active
Number of active PUs                               2
DLUS pipe statistics:
  REQACTPUs sent                                   11
  REQACTPU responses received                      11
  ACTPUs received                                  11
  ACTPU responses sent                             11
  DACTPUs received                                 9
  DACTPU responses sent                            9
  REQDACTPUs sent                                  9
  REQDACTPU responses received                     9
  ACTLUs received                                  9
  ACTLU responses sent                             9
  DACTLUs received                                 0
  DACTLU responses sent                            0
  SSCP-PU MUs sent                                 31
  SSCP-PU MUs received                             31
  SSCP-LU MUs sent                                 37
  SSCP-LU MUs received                             36
```

show snasw lu

```
cheney#sh snasw lu
Number of DLUR LUs 1

      SNA DLUR LUs
      LU Name   PU Name   DLUS Name          PLU Name
      --------  --------  -----------------  -----------------
   1> RW982303  IBDNT223  NETA.MVSA          NETA.TSOA0002

cheney#sh snasw lu det
Number of DLUR LUs 1

1>
LU name                                            RW982303
LU status                                          Active
SLU status                                         In Session
PU name                                            IBDNT223
DLUS name                                          NETA.MVSA
Primary LU name                                    NETA.TSOA0002
LU location                                        Downstream
LU  FSM history                                    (00,00)->(01,01)->(02,0E)->(0
3,03)->04
SLU FSM history                                    (00,00)->(01,01)->(02,03)->(0
3,06)->(03,05)->(04,07)->(00,0C)->(00,00)->(01,01)->02
```

show snasw port

```
cheney#show snasw port
Number of ports 3

      SNA Ports                HPR
        Name     State    SAP  SAP  Interface              Address
      --------  --------  ---  ---  ---------------------  --------------
   1> DNFE01    Active    x04  x00  FastEthernet0/1        4000.0195.0101
   2> HPRLO0    Active              Loopback0              10.88.192.13
   3> VTOK0     Active    x04  x00  Virtual-TokenRing0     4000.0195.0201

cheney#
```

show snasw pu

```
cheney#show snasw pu det
Number of DLUR PUs 2

1>
PU name                                            IBDNT223
Backup DLUS name
Active DLUS name                                   NETA.MVSA
PU ID (IDBLK/IDNUM)                                X'08198023'
PU location                                        Downstream
PU status                                          Active
DLUS session state                                 Active
Automatic Network Shutdown support                 Stop
DLUS retry timeout (seconds)                       0
DLUS retry limit                                   0
DLUS pipe PCID                                     X'C193D9033CB91A55'
DLUS pipe CP Name                                  NETA.CHENEY
PU FSM history                                     (00,01)->(01,03)->(02,04)->(0
2,06)->(03,11)->(03,07)->04

2>
PU name                                            RWTPA001
Backup DLUS name
Active DLUS name                                   NETA.MVSA
PU ID (IDBLK/IDNUM)                                X'08199001'
PU location                                        Downstream
PU status                                          Active
DLUS session state                                 Active
Automatic Network Shutdown support                 Stop
DLUS retry timeout (seconds)                       0
DLUS retry limit                                   0
DLUS pipe PCID                                     X'C193D9033CB91A39'
DLUS pipe CP Name                                  NETA.CHENEY
PU FSM history                                     (03,07)->(04,0C)->(06,0D)->(0
7,10)->(00,02)->(01,03)->(02,04)->(02,06)->(03,11)->(03,07)->04

cheney#
```

show snasw link

```
Number of links 3

    SNA Links                                                            HPR
    Link Name   State    Port Name Adjacent CP Name  Node Type     Sess  Sup
    ---------  --------  --------- ----------------  ------------  ----  ---
 1> @I000001   Active    VTOK      NETA.RW98P002     LEN Node         0  No
 2> EELNKA     Retrying  EEPORT                      Learn            0  No
 3> EELNKB     Inactive  EEPORT                      Learn            0  Yes
```

sh run | include snasw

```
roo#sh run | inc snasw
snasw cpname NETA hostname
snasw dlus NETA.MVSA prefer-active retry 300 10
snasw port VTOK Virtual-TokenRing0
snasw port EEPORT hpr-ip Loopback0
snasw port DLSW1 vdlc 100 mac 4000.1111.0001 conntype nohpr
snasw link EELNKB port EEPORT ip-dest 10.2.9.1 nostart
snasw link EELNKA port EEPORT ip-dest 10.2.8.1

cheney#sh run | inc snasw
snasw pdlog exception
snasw dlctrace
snasw cpname NETA.CHENEY
snasw port HPRLO0 hpr-ip Loopback0 vnname NETA.IBDCN
snasw port DNFE01 FastEthernet0/1 conntype nohpr
snasw port VTOK0 Virtual-TokenRing0 conntype nohpr
snasw link MVSA port HPRLO0 ip-dest 10.88.24.1 nns
cheney#

cheney#sh run | inc snasw
snasw pdlog exception file tftp://172.18.60.179/cheney-pdlog
snasw dlctrace file tftp://172.18.60.179/cheney-dlctrc
snasw event implicit-ls port dlc cpcp
snasw msgdump HPR_LOG_6
snasw cpname NETA.CHENEY
snasw port HPRLO0 hpr-ip Loopback0 vnname NETA.IBDCN
snasw port DNFE01 FastEthernet0/1 conntype nohpr
snasw port VTOK0 Virtual-TokenRing0 conntype nohpr
snasw link MVSA port HPRLO0 ip-dest 10.88.24.1 nns
cheney#
```

show process cpu

In this display example, the offered load is beyond the capability of the Cisco 2621 platform, resulting in high CPU:

```
cheney#sh proc cpu
CPU utilization for five seconds: 99%/5%; one minute: 98%; five minutes: 75%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1         796    363730          2  0.00%  0.00%  0.00%   0 Load Meter
   2        1156       353       3274  0.00%  0.00%  0.03%   0 Exec
   3     1113680    215280       5173  0.00%  0.06%  0.05%   0 Check heaps
   4           4         1       4000  0.00%  0.00%  0.00%   0 Chunk Manager
   5          44        23       1913  0.00%  0.00%  0.00%   0 Pool Manager
   6           0         2          0  0.00%  0.00%  0.00%   0 Timers
   7           0         2          0  0.00%  0.00%  0.00%   0 Serial Backgroun
   8        8600    362802         23  0.00%  0.00%  0.00%   0 ALARM_TRIGGER_SC
   9          48     60632          0  0.00%  0.00%  0.00%   0 Environmental mo
  10        1284     32887         39  0.00%  0.00%  0.00%   0 ARP Input
  11           4         2       2000  0.00%  0.00%  0.00%   0 DDR Timers
  12           0         2          0  0.00%  0.00%  0.00%   0 Dialer event
  13           8         3       2666  0.00%  0.00%  0.00%   0 Entity MIB API
  14           0         1          0  0.00%  0.00%  0.00%   0 SERIAL A'detect
  15           0         5          0  0.00%  0.00%  0.00%   0 Critical Bkgnd
  16        2544    236403         10  0.00%  0.01%  0.00%   0 Net Background
  17         188     42760          4  0.00%  0.00%  0.00%   0 Logger
  18       20464   1816849         11  0.00%  0.01%  0.00%   0 TTY Background
  19       14040   1816973          7  0.00%  0.01%  0.00%   0 Per-Second Jobs
  20           0         2          0  0.00%  0.00%  0.00%   0 Hawkeye Backgrou
  21       84416    679842        124  3.84%  3.59%  2.67%   0 HyBridge Input P
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
  22           0         1          0  0.00%  0.00%  0.00%   0 HDV background
  23           0         2          0  0.00%  0.00%  0.00%   0 VNM DSPRM MAIN
  24      167112   3731121         44  0.32%  0.22%  0.18%   0 Net Input
  25        3464    363730          9  0.00%  0.00%  0.00%   0 Compute load avg
  26      849868     30803      27590  0.00%  0.06%  0.00%   0 Per-minute Jobs
  27           0         1          0  0.00%  0.00%  0.00%   0 CES Line Conditi
  28           0         2          0  0.00%  0.00%  0.00%   0 AAA Dictionary R
  29     1023280   1589598        643  4.99%  4.02%  3.87%   0 IP Input
  30       38556    244756        157  0.00%  0.00%  0.00%   0 CDP Protocol
  31          16      3027          5  0.00%  0.00%  0.00%   0 MOP Protocols
  32           0         1          0  0.00%  0.00%  0.00%   0 X.25 Encaps Mana
  33          44     30317          1  0.00%  0.00%  0.00%   0 LDP Background
  34           0         1          0  0.00%  0.00%  0.00%   0 frr_tunnel
  35           0         2          0  0.00%  0.00%  0.00%   0 PASVC create VA
  36           0         1          0  0.00%  0.00%  0.00%   0 Asy FS Helper
  37           0         1          0  0.00%  0.00%  0.00%   0 PPP IP Add Route
  38        5824     30351        191  0.00%  0.00%  0.00%   0 IP Background
  39           0         1          0  0.00%  0.00%  0.00%   0 SNMP Timers
  40           0        61          0  0.00%  0.00%  0.00%   0 TCP Timer
  41          44        31       1419  0.00%  0.00%  0.00%   0 TCP Protocols
  42           0         1          0  0.00%  0.00%  0.00%   0 Probe Input
  43           4         1       4000  0.00%  0.00%  0.00%   0 RARP Input
```

```
PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
 44           0         1          0  0.00%  0.00%  0.00%   0 HTTP Timer
 45           0         1          0  0.00%  0.00%  0.00%   0 Socket Timers
 46           4         2       2000  0.00%  0.00%  0.00%   0 DHCPD Receive
 47        1808     30303         59  0.00%  0.00%  0.00%   0 IP Cache Ager
 48           0         1          0  0.00%  0.00%  0.00%   0 COPS
 49           0         1          0  0.00%  0.00%  0.00%   0 PAD InCall
 50           0         2          0  0.00%  0.00%  0.00%   0 X.25 Background
 51          28     30316          0  0.00%  0.00%  0.00%   0 TCP Intercept Ti
 52           0         2          0  0.00%  0.00%  0.00%   0 SPX Input
 53        2232     30322         73  0.00%  0.00%  0.00%   0 Adj Manager
 54           0         2          0  0.00%  0.00%  0.00%   0 Tag Input
 55       11540   1816935          6  0.00%  0.00%  0.00%   0 RUDPV1 Main Proc
 56           0         1          0  0.00%  0.00%  0.00%   0 bsm_timers
 57        5452   1816863          3  0.00%  0.00%  0.00%   0 bsm_xmt_proc
 58           0         1          0  0.00%  0.00%  0.00%   0 CES Client SVC R
 59           0         2          0  0.00%  0.00%  0.00%   0 TC-ATM Proc
 60       32388   2013930         16  0.00%  0.01%  0.00%   0 Tbridge Monitor
 61           8         2       4000  0.00%  0.00%  0.00%   0 CCVPM_HDSPRM
 62           0         1          0  0.00%  0.00%  0.00%   0 Router Autoconf
 63           4         1       4000  0.00%  0.00%  0.00%   0 TSP
 64           4         1       4000  0.00%  0.00%  0.00%   0 QOS_MODULE_MAIN
 65           4         1       4000  0.00%  0.00%  0.00%   0 CCVPM_HTSP
PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
 66           0         1          0  0.00%  0.00%  0.00%   0 CCVPM_R2
 67           0         1          0  0.00%  0.00%  0.00%   0 CCSWVOICE
 68           0         2          0  0.00%  0.00%  0.00%   0 Background Loade
 69           0         1          0  0.00%  0.00%  0.00%   0 sssapp
 70      253844     21525      11792  0.00%  0.00%  0.00%   0 Syslog Traps
 71        6816    181794         37  0.00%  0.00%  0.00%   0 BUSYOUT SCAN
 72       11996   1813957          6  0.00%  0.00%  0.00%   0 trunk conditioni
 73           0         1          0  0.00%  0.00%  0.00%   0 trunk conditioni
 74       22160     33087        669  2.37%  2.74%  2.11%   0 CLS Background
 75        7620   1820495          4  0.00%  0.00%  0.00%   0 DSPU Msg Proc
 76        3284   1818054          1  0.00%  0.00%  0.00%   0 SRB Background
 77        8476   1816860          4  0.08%  0.00%  0.00%   0 RSRB Background
 78      179680  36271901          4  0.40%  0.33%  0.28%   0 LLC2 Timer
 79      246304   3198429         77  0.08%  0.09%  0.08%   0 Spanning Tree
 80       22840   1816435         12  0.08%  0.03%  0.00%   0 DLSw Background
 81      115720   2356346         49  0.16%  0.07%  0.04%   0 IP-EIGRP Hello
 82          36        60        600  0.00%  0.00%  0.00%   0 DLSw msg proc
 83       53256    115026        462  0.00%  0.00%  0.00%   0 IP SNMP
 84       48512     46803       1036  0.00%  0.00%  0.00%   0 PDU DISPATCHER
 85      372488    190879       1951  0.00%  0.00%  0.00%   0 SNMP ENGINE
 86       31696       440      72036  0.00%  0.00%  0.00%   0 SNMP ConfCopyPro
 87          84        13       6461  0.00%  0.00%  0.00%   0 SNMP Traps
PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
 88           0         1          0  0.00%  0.00%  0.00%   0 Crash writer
 89        4736   1827811          2  0.00%  0.00%  0.00%   0 NTP
 90          16     15159          1  0.00%  0.00%  0.00%   0 DHCPD Timer
 91       26200    515136         50  0.00%  0.00%  0.00%   0 DHCPD Database
```

```
  92      114664    786662        145  0.00%  0.00%  0.00%   0 IP-EIGRP Router
  93           0         1          0  0.00%  0.00%  0.00%   0 DLSw Peer Proces
  94           0         1          0  0.00%  0.00%  0.00%   0 TCP Driver
  95        6972     26218        265  0.65%  0.83%  0.61%   0 VDLC Background
  96     8157192  22244960        366 80.08% 80.36% 62.65%   0 SNA Switch
  97       99052    311396        318  0.00%  0.00%  0.00%   0 SNASw NetMan
  98       13360      9624       1388  0.00%  0.00%  0.00%  67 SNA-NM Exec
```

show snasw statistics

```
cheney#sh snasw statistics
SNA Switch Subsystem Uptime                        21 days,  1 hrs,  2 mins,  7 secs

Directory Statistics:
  Maximum number of cache entries                  10000
  Current number of cache entries                  0
  Current number of home entries                   3
  Current number of registry entries               4
  Total number of entries in directory             7
  Total cache hits                                 0
  Total cache misses                               0
  Number of directed locates sent                  18
  Number of directed locates returned not found    0
  Number of directed locates received              0
  Number of broadcast locates sent                 0
  Number of broadcast locates returned not found   0
  Number of broadcast locates received             13
  Number of locates outstanding                    0

Toplogy Statistics:
  Maximum number of nodes                          0
  Current number of nodes                          2
  Total number of received TDUs                    0
  Total number of sent TDUs                        0
  Total received Node updates with lower RSN       0
  Total received Node updates with equal RSN       0
  Total received Node updates with higher RSN      0
  Total received Node updates with higher odd RSN  0
  Total node state changes requiring TDUs          0
  Total database inconsistencies detected          0
  Total number of timer based TDUs generated       0
  Total number of node records purged              0
  Total received TG updates with lower RSN         0
  Total received TG updates with equal RSN         0
  Total received TG updates with higher RSN        0
  Total received TG updates with higher odd RSN    0
  Total TG state changes requiring TG updates      1
  Total TG database inconsistencies detected       0
  Total number of timer TG updates generated       0
  Total number of TG records purged                0
  Total number of routes calculated                6
  Total number of routes rejected                  0
  Total number of cache hits in route calculation  0
  Total number of cache misses in rte calculation  7
  Total number of TDU wars detected                0


Number of processes 24
      CPU/Memory usage per SNA Switch process
      Process Name                         CPU Time (ms)  Memory Used (bytes)
      -----------------------------------  -------------  -------------------
   1> NOF API                                  36880                10
   2> N-Base allocated memory                      0             62569
   3> Buffer Manager (BM)                      21348               208
   4> Node Operator Facility (NOF)             24564             13117
   5> Address Space Manager (ASM)                100              1408
   6> Address Space (AS)                          92                 0
   7> Session Services (SS)                   881408              1824
   8> Directory Services (DS)                 578332            548736
   9> Configuration Services (CS)             122720             12063
  10> Management Services (MS)               2064564              7690
  11> Multiple Domain Support (MDS)               24                 0
  12> Topology & Routing Services (TRS)       146952             22816
  13> Session Connector Manager (SCM)            856              3957
  14> Session Connector (SCO)                  65900              2980
  15> Session Manager (SM)                    478684             16429
  16> Resource Manager (RM)                   583176                 0
  17> Presentation Services (PS)              577496                 0
  18> Half Session (HS)                        10280                 0
  19> Path Control (PC)                       359292             25052
  20> Data Link Control (DLC)                 153596              1760
  21> Dependent LU Requester (DR)             358360             17160
  22> High Performance Routing (HPR)             632              5315
  23> Rapid Transport Protocol (RTP)          144064             34904
  24> UDP stub                                117984               388

cheney#
```

show interface (busy router)

These interface displays were taken on an overloaded router:

```
cheney#sh int
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 0030.193e.78c0 (bia 0030.193e.78c0)
  Internet address is 10.88.194.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 187 drops
  5 minute input rate 748000 bits/sec, 136 packets/sec
  5 minute output rate 10000 bits/sec, 12 packets/sec
     1324128 packets input, 232077079 bytes
     Received 484517 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     1444001 packets output, 135351792 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
FastEthernet0/1 is up, line protocol is up
  Hardware is AmdFE, address is 0030.193e.78c1 (bia 0030.193e.78c1)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 19000 bits/sec, 71 packets/sec
  5 minute output rate 693000 bits/sec, 78 packets/sec
     10476356 packets input, 739980107 bytes
     Received 9906592 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     3185209 packets output, 352143821 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
FastEthernet0/1.1 is up, line protocol is up
  Hardware is AmdFE, address is 0030.193e.78c1 (bia 0030.193e.78c1)
  Internet address is 10.88.195.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  11.
  ARP type: ARPA, ARP Timeout 04:00:00
FastEthernet0/1.2 is up, line protocol is up
  Hardware is AmdFE, address is 0030.193e.78c1 (bia 0030.193e.78c1)
  Internet address is 10.88.196.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  22.
  ARP type: ARPA, ARP Timeout 04:00:00
Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 10.88.192.13/30
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input 00:00:02, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 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, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     393515 packets output, 23610900 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
Virtual-TokenRing0 is up, line protocol is up
  Hardware is Virtual-TokenRing, address is 4000.0195.0201 (bia 4000.0000.0004)
  MTU 8136 bytes, BW 16000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation SNAP, loopback not set
  ARP type: SNAP, ARP Timeout 04:00:00
  Last input 00:00:00, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 2 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     3638675 packets input, 95741279 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     7277657 packets output, 190414215 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 transitions
Virtual-TokenRing1 is up, line protocol is up
  Hardware is Virtual-TokenRing, address is 4000.0195.0202 (bia 4000.0000.0005)
  MTU 8136 bytes, BW 16000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation SNAP, loopback not set
  ARP type: SNAP, ARP Timeout 04:00:00
  Last input 00:00:00, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 2 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     3638955 packets input, 94672265 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     7277743 packets output, 190415695 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 transitions
```

show interface switching (busy router)

```
cheney#sh int switching
FastEthernet0/0
          Throttle count          0
        Drops         RP        187         SP          0
  SPD Flushes       Fast          0        SSE          0
  SPD Aggress       Fast          0
 SPD Priority     Inputs     785740      Drops          0

     Protocol       Path    Pkts In   Chars In   Pkts Out  Chars Out
        Other    Process      60635    3031750     182052   10923120
            Cache misses          0
                    Fast          0          0          0          0
               Auton/SSE          0          0          0          0
           IP    Process    1177647  220772721    1157116   98799561
            Cache misses          0
                    Fast      59494    3496772      71667   15502217
               Auton/SSE          0          0          0          0
      DEC MOP    Process          0          0       3027     233079
            Cache misses          0
                    Fast          0          0          0          0
               Auton/SSE          0          0          0          0
          ARP    Process        128       7680        133       7980
            Cache misses          0
                    Fast          0          0          0          0
               Auton/SSE          0          0          0          0
          CDP    Process      30343    7949866      30347    9923469
            Cache misses          0
```

```
                    Fast          0          0          0          0
               Auton/SSE          0          0          0          0
FastEthernet0/1
          Throttle count          0
        Drops         RP          0         SP          0
  SPD Flushes       Fast          0        SSE          0
  SPD Aggress       Fast          0
 SPD Priority     Inputs          0      Drops          0

     Protocol       Path    Pkts In   Chars In   Pkts Out  Chars Out
        Other    Process     142205    6809398     487526  155714244
            Cache misses          0
                    Fast          0          0          0          0
               Auton/SSE          0          0          0          0
           IP    Process     296549   34079257     786924   61376008
            Cache misses          0
                    Fast      71667   15502217      59494    3734748
               Auton/SSE          0          0          0          0
Trans. Bridge    Process          0          0          0          0
            Cache misses          0
                    Fast     249657   14997755          0          0
               Auton/SSE          0          0          0          0
      DEC MOP    Process          0          0       3026     233002
            Cache misses          0
                    Fast          0          0          0          0
               Auton/SSE          0          0          0          0
Spanning Tree    Process    1819333  105519542    1819246  123708728
            Cache misses          0
                    Fast          0          0          0          0
               Auton/SSE          0          0          0          0
          ARP    Process       2440     146400        601      38444
            Cache misses          0
                    Fast          0          0          0          0
               Auton/SSE          0          0          0          0
          CDP    Process      30337    7978631      30357    9925755
            Cache misses          0
                    Fast          0          0          0          0
               Auton/SSE          0          0          0          0
Loopback0
          Throttle count          0
        Drops         RP          0         SP          0
  SPD Flushes       Fast          0        SSE          0
  SPD Aggress       Fast          0
 SPD Priority     Inputs          0      Drops          0

     Protocol       Path    Pkts In   Chars In   Pkts Out  Chars Out
           IP    Process     393520   23611200     393520   23611200
            Cache misses          0
                    Fast          0          0          0          0
               Auton/SSE          0          0          0          0
Virtual-TokenRing0
```

```
          Throttle count          0
        Drops         RP          0         SP          0
  SPD Flushes       Fast          0        SSE          0
  SPD Aggress       Fast          0
 SPD Priority     Inputs          0      Drops          0

     Protocol       Path    Pkts In   Chars In   Pkts Out  Chars Out
        Other    Process         24       2400    7277753  190416711
            Cache misses          0
                    Fast          0          0          0          0
               Auton/SSE          0          0          0          0
    SR Bridge    Process          6        150          0          0
            Cache misses          0
                    Fast          0          0          0          0
               Auton/SSE          0          0          0          0
Virtual-TokenRing1
          Throttle count          0
        Drops         RP          0         SP          0
  SPD Flushes       Fast          0        SSE          0
  SPD Aggress       Fast          0
 SPD Priority     Inputs          0      Drops          0

     Protocol       Path    Pkts In   Chars In   Pkts Out  Chars Out
        Other    Process         24       1776    7277835  190418087
            Cache misses          0
                    Fast          0          0          0          0
               Auton/SSE          0          0          0          0
    SR Bridge    Process         64       1216          0          0
            Cache misses          0
                    Fast          0          0          0          0
               Auton/SSE          0          0          0          0
```

show interface statistics (busy router)

```
cheney#sh int stat
FastEthernet0/0
          Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor    1271430  233832865    1372900  119912472
             Route cache      59497    3496941      71672   15502531
                   Total    1330927  237329806    1444572  135415003
FastEthernet0/1
          Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor   10157328  709544152    3128881  352579691
             Route cache     321814   30529457      59497    3734929
                   Total   10479142  740073609    3188378  356314620
Loopback0
          Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor          0          0     393523   23611380
             Route cache          0          0          0          0
                   Total          0          0     393523   23611380
Virtual-TokenRing0
          Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor    3638747   95743151    7277801  190417959
             Route cache          0          0          0          0
                   Total    3638747   95743151    7277801  190417959
Virtual-TokenRing1
          Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor    3639027   94674137    7277887  190419439
             Route cache          0          0          0          0
                   Total    3639027   94674137    7277887  190419439
cheney#
```

Trace Commands

show snasw dlctrace

```
cheney#sh snasw dlctrace
DLC Trace Output

16625  MVSA     In  sz:45   HPR      Stat Rq Stat Rpy
16626  MVSA     Out sz:52   HPR      Stat Rpy
16627  MVSA     In  sz:68   SEND_MU
16628  MVSA     In  sz:45   HPR      Stat Rq Stat Rpy
16629  MVSA     Out sz:52   HPR      Stat Rpy
16630  MVSA     Out sz:52   HPR      Stat Rq Stat Rpy
16631  MVSA     In  sz:68   SEND_MU
16632  MVSA     In  sz:45   HPR      Stat Rpy
16633  MVSA     In  sz:45   HPR      Stat Rq Stat Rpy
16634  MVSA     Out sz:52   HPR      Stat Rpy
16635  MVSA     In  sz:45   HPR      Stat Rq Stat Rpy
16636  MVSA     Out sz:52   HPR      Stat Rpy
16637  MVSA     In  sz:68   SEND_MU
16638  MVSA     In  sz:45   HPR      Stat Rq Stat Rpy
16639  MVSA     Out sz:52   HPR      Stat Rpy
16640  MVSA     In  sz:45   HPR      Stat Rq Stat Rpy
16641  MVSA     Out sz:52   HPR      Stat Rpy
16642  MVSA     In  sz:68   SEND_MU
16643  MVSA     In  sz:45   HPR      Stat Rq Stat Rpy
16644  MVSA     Out sz:52   HPR      Stat Rpy
cheney#
```

ping sna

```
cheney#ping sna neta.mvsa
cheney#
SNA APING successful
Partner LU name            NETA.MVSA
Mode name                  #INTER
Allocate duration          92 ms
Duration statistics        Min = 8 ms   Ave = 10 ms   Max = 12 ms
cheney#
```

d net,vtamopts

```
* CNM21    D NET,VTAMOPTS
  CNM21    IST097I  DISPLAY  ACCEPTED
' CNM21
IST1188I  VTAM CSV2R8 STARTED AT 09:28:08 ON 10/29/01
IST1349I  COMPONENT ID IS 5695-11701-801
IST1348I  VTAM STARTED AS INTERCHANGE NODE
IST1189I  ALSREQ   = NO                   APPNCOS  = NONE
IST1189I  ASIRFMSG = OLUSSCP              ASYDE    = TERM
IST1189I  AUTHLEN  = YES                  AUTORTRY = AUTOCAP
IST1189I  AUTOTI   = 0                    BN       = YES
IST1189I  BNDYN    = FULL                 BNORD    = PRIORITY
IST1189I  BSCMDRS  = (STATS,INOPS)        BSCTMOUT = 286
IST1189I  CACHETI  = 8                    CDRDYN   = YES
IST1189I  CDRSCTI  = 480S                 CDSERVR  = YES
IST1189I  CDSREFER = ***NA***             CINDXSIZ = 8176
IST1189I  CMPMIPS  = 100                  CMPVTAM  = 0
IST1189I  CNMTAB   = *BLANKS*             COLD     = YES
IST1189I  CONFIG   = MA                   CONNTYPE = APPN
IST1189I  CPCDRSC  = YES                  CPCP     = YES
IST1189I  CSALIMIT = 90112K               CSA24    = 1024K
IST1189I  DATEFORM = MDY                  DIALRTRY = YES
IST1189I  DIRSIZE  = 0                    DIRTIME  = 691200S
IST1189I  DISCNTIM = (15,0)               DLRORDER = STATNID
IST1189I  DLRTCB   = 32                   DSPLYDEF = 300
IST1189I  DSPLYMAX = 16384                DSPLYWLD = FULLWILD
IST1189I  DUPDEFS  = ALL                  DYNADJCP = YES
IST1189I  DYNASSCP = YES                  DYNDLGMD = NONE
IST1189I  DYNHPPFX = *BLANKS*             DYNLU    = YES
IST1189I  DYNMODTB = NONE                 DYNPUPFX = *BLANKS*
IST1189I  DYNVNPFX = *BLANKS*             ENCRPREF = NONE
IST1189I  ENCRYPTN = 31                   ENHADDR  = YES
IST1189I  ESIRFMSG = ALLSSCP              FLDTAB   = MSGFLOOD
IST1189I  FSIRFMSG = OLUSSCP              GWSSCP   = YES
IST1189I  HNTSIZE  = 4080                 HOSTPU   = ISTPUS
IST1189I  HOSTSA   = 57                   HOTIOTRM = 20
IST1189I  HPR      = (RTP,RTP)            HPRARB   = RESPMODE
IST1189I  HPRNCPBF = NO                   HPRPST   = LOW          480S
IST1189I  HPRPST   = MEDIUM       240S    HPRPST   = HIGH         120S
IST1189I  HPRPST   = NETWRK        60S    HSRTSIZE = 9973
IST1189I  INITDB   = NONE                 INOPDUMP = OFF
IST1189I  IOINT    = 900                  IOMSGLIM = 2
IST1189I  IOPURGE  = 300S                 IPADDR   = 0.0.0.0
IST1189I  IRNSTRGE = 0                    ISTCOSDF = INDLU
IST1189I  LIMINTCP = 43200                LIST     = 00
IST1189I  MAINTLVL = *BLANKS*             MAXLOCAT = 5000
IST1189I  MAXLURU  = 6144                 MAXSSCPS = 10
IST1189I  MAXSUBA  = 63                   MIHTMOUT = 1800
IST1189I  MSGLEVEL = BASE                 MSGMOD   = NO
IST1189I  MXSAWBUF = 10000                MXSSCPRU = 4096
```

```
IST1189I  MXSUBNUM = 511                  NCPBUFSZ = 512
IST1189I  NETID    = NETA                 NMVTLOG  = NPDA
IST1189I  NNSPREF  = ***NA***             NODELST  = *BLANKS*
IST1189I  NODETYPE = NN                   NQNMODE  = NAME
IST1189I  NSRTSIZE = *BLANKS*             NUMTREES = 200
IST1189I  OSIEVENT = PATTERNS             OSIMGMT  = NO
IST1189I  OSITOPO  = ILUCDRSC             OSRTSIZE = 43
IST1189I  PDTRCBUF = 2                    PIUMAXDS = 200
IST1189I  PLUALMSG = NOSUPP               PPOLOG   = YES
IST1189I  PSRETRY  = LOW            0S    PSRETRY  = MEDIUM         0S
IST1189I  PSRETRY  = HIGH           0S    PSRETRY  = NETWRK         0S
IST1189I  PSSTRACE = NORB                 PSWEIGHT = LESSTHAN
IST1189I  RESUSAGE = 100                  ROUTERES = 128
IST1189I  SACONNS  = YES                  SAVERSCV = (NO,KEEP)
IST1189I  SAWMAXDS = 100                  SAWMXQPK = 0
IST1189I  SDLCMDRS = (STATS,INOPS)        SECLVLCP = ***NA***
IST1189I  SIRFMSG  = ALLSSCP              SLOWVAL  = (0,0)
IST1189I  SLUALMSG = NOSUPP               SMEAUTH  = DISCARD
IST1189I  SNAPREQ  = 1000                 SNVC     = 15
IST1189I  SONLIM   = (60,30)              SORDER   = APPN
IST1189I  SRCHRED  = OFF                  SRCOUNT  = 10
IST1189I  SRTIMER  = 30S                  SSCPDYN  = YES
IST1189I  SSCPID   = 57                   SSCPNAME = MVSA
IST1189I  SSCPORD  = PRIORITY             SSDTMOUT = 30
IST1189I  SSEARCH  = CACHE                STRGR    = ISTGENERIC
IST1189I  STRMNPS  = ISTMNPS              SUPP     = NOSUP
IST1189I  SWNORDER = CPNAME               TCPNAME  = *BLANKS*  ←  Must specify
IST1189I  TNSTAT   = NOCNSL,TIME=60       TRANSLAT = (0,1,2,3,4,5,6,7)
IST1189I  UPDDELAY = 60S                  USSTAB   = *BLANKS*
IST1188I  VTAM CSV2R8 STARTED AT 09:28:08 ON 10/29/01
IST1189I  VERIFYCP = NONE                 VFYRED   = YES
IST1189I  VFYREDTI = OFF                  VOSDEACT = NO
IST1189I  VRTG     = NO                   VRTGCPCP = YES
IST1189I  VTAMEAS  = 32001                WARM     = NO
IST1189I  XCFINIT  = YES                  XNETALS  = NO
IST314I  END
```

APPENDIX C: TROUBLESHOOTING COMMAND SUMMARY

Stopping SNASw and SNASw Ports and Links

Unless otherwise defined with the **nostart** operand, SNASw and SNASw port and link definitions are started automatically when SNASw starts. To stop SNASw or to stop SNASw ports and links when making configuration changes or when resetting the ports or links, use one of the commands in Table 1 in privileged EXEC mode, as needed.

Table 1. SNASw Start and Stop Commands

Command	Purpose
Router#**snasw start | stop**	Activates/Deactivates SNASw
Router#**snasw start | stop link** *linkname*	Activates/Deactivates the specified SNASw link
Router#**snasw start | stop port** *portname*	Activates/Deactivates the specified SNASw port

Note: Removing a CP name definition stops SNASw and deletes other SNASw configuration statements.

Verifying SNASw

To verify that you have connectivity between SNASw and other nodes supporting the APINGD transaction program, issue the **ping sna** command.

Monitoring and Maintaining SNASw

You can monitor the status and configuration of SNASw by issuing any of the commands listed in Table 2 in privileged EXEC mode.

Table 2. SNASw Commands

Command	Purpose
Router#**ping sna** [-*1*] [-**c** *consecutive packets*] [-**i** *number-iterations*] [-**m** *mode*] [-**n**] [-**r**] [-**s** *size*] [-**t** *tpname*] [-**u** *userid* -**p** *password*] **destination**	Initiates an Advanced Program-to-Program Communications (APPC) session with a named destination LU to run the APING transaction program to check network integrity and timing characteristics
Router#**show snasw class-of-service** [**brief** | **detail**]	Displays the predefined Class of Service (COS) definitions
Router#**show snasw connection-network** [**brief** | **detail**]	Displays the connection networks (virtual nodes) defined to the local node
Router#**show snasw directory** [**name** *resourcenamefilter*] [**brief** | **detail**]	Displays the SNASw directory entries
Router#**show snasw dlus** [**brief** | **detail**]	Displays the SNASw DLUS objects
Router#**show snasw link** [**brief** | **detail**] [**cpname** *cpnamefilter*] [**name** *linknamefilter*] [**port** *portnamefilter*] [**rmac** *macfilter*] [**xid** *xidfilter*]	Displays the SNASw link objects
Router#**show snasw lu** [**brief** | **detail**][**name** *luname*] [**pu** *puname*]	Displays the SNASw dependent LUs
Router#**show snasw mode**	Displays the SNASw modes
Router#**show snasw node**	Displays details of the SNASw operation
Router#**show snasw port** [**brief** | **detail**] [**name** *portnamefilter*]	Displays the SNASw port objects

Command	Purpose
Router#**show snasw pu** [**brief** | **detail**] [**dlus** *dlusfilter*] [**name** *punamefilter*]	Displays the SNASw PUs
Router#**show snasw rtp** [**brief** | **detail**] [**class-of-service** *cosname*] [**cpname** *netid.cpname*] [**name** *connectionnamefilter*] [**tcid** *tcidconnection*]	Displays the SNASw Rapid Transport Protocol (RTP) connections

You can troubleshoot SNASw by issuing any of the commands listed in Table 3 in privileged EXEC mode.

Table 3. SNASw Troubleshooting Commands

Command	Purpose
Router#**ping sna** [*-1*] [**-c** *consecutive packets*] [**-i** *number-iterations*] [**-m** *mode*] [**-n**] [**-r**] [**-s** *size*] [**-t** *tpname*] [**-u** *userid* **-p** *password*] **destination**	Initiates an APPC session with a named destination LU to run the APING transaction program to check network integrity and timing characteristics
Router#**show snasw dlctrace** [**all** | **last** | **next**] [**brief** | **detail**] [**filter** *filter-string*] [**id** *recordid*]	Displays the captured DLC trace information to the console
Router#**show snasw ipstrace** [**all** | **next** | **last**] [**filter** *filterstring*] [**id** *recordid*]	Displays the interprocess signal trace on the router console
Router#**show snasw pdlog** [**brief** | **detail**] [**all**] [**last**] [**next**] [**filter** *filterstring*] [**id** *recordid*]	Displays entries in the cyclical problem determination log to the console
Router#**show snasw summary-ipstrace** [**id** *recordid*] [**last** *number-records* | **filter** *number-records* | **all** | **next** | **last**]	Displays the special “footprint” summary interprocess signal trace on the router console
Router#**snasw dump**	Initiates file transfer of SNASw trace files from internal buffers to a file server
Router#**snasw pathswitch** [*rtp-connection-name* | **all**]	Forces an HPR pathswitch for an RTP connection
Router#**snasw start | stop arbdata** *local-tcid*	Starts/stops the display of arbdata router log messages for the specified SNASw rtp

You can also troubleshoot SNASw by issuing any of the commands listed in Table 4 in global configuration mode.

Table 4. SNASw Trace Commands

Command	Purpose
Router#**snasw dlcfilter** [**link** *linkname* [**session** *session-address*]] [**port** *portname*] [**rmac** *mac-address-value* [**session** *session-address*]] [**rtp** *rtpname* [**session** *session-address*]] [[**type** [**cls**] [**hpr-cntl**] [**hpr-data**] [**isr**] [**xid**]]	Filters frames captured by the **snasw dlctrace** or **debug snasw dlc** commands
Router#**snasw dlctrace** [**buffer-size** *buffer-size-value*] [**file** *filename*] [**frame-size** *frame-size-value*] [**format brief | detail | analyzer**] [**nostart**]	Traces frames arriving at and leaving SNASw
Router#**snasw event** [**cpcp**] [**dlc**] [**implicit-ls**] [**port**]	Indicates which events are logged to the console
Router#**snasw ipsfilter** [**as**] [**asm**] [**bm**] [**ch**] [**cpc**] [**cs**] [**di**] [**dlc**] [**dma**] [**dr**] [**ds**] [**es**] [**ha**] [**hpr**] [**hs**] [**lm**] [**mds**] [**ms**] [**nof**] [**pc**] [**ps**] [**pu**] [**px**] [**rm**] [**rtp**] [**ru**] [**scm**] [**sco**] [**sm**] [**spc**] [**ss**] [**trs**]	Filters interprocess signal trace elements being traced via the **snasw ipstrace** or **debug snasw ips** commands
Router#**snasw ipstrace** [**buffer-size** *buffer-size-value*] [**file** *filename*]	Sets up a trace buffer and begins tracing interprocess signal trace elements
Router#**snasw pdlog** [*problem* | *error* | *info*] [**buffer-size** *buffer-size-value*] [**file** *filename* **timestamp**]	Controls logging of messages to the console and the SNA problem determination log cyclic buffer

APPENDIX D: SENSE DATA

Messages may include “sense” data to describe particular types of failures and causes. Table 5 lists common sense codes and their meanings.

Table 5. Native IP DLC Link Activation Failure Sense Data

Error Description	Sense Data
The link specified in the RSCV is not available.	X'08010000'
The limit for null exchange identifier (XID) responses by a called node was reached.	X'0809003A'
A BIND was received over a subarea link, but the next hop is over a port that supports only HPR links. The receiver does not support this configuration.	X'08400002'
The contents of the DLC Signaling Type (X'91') subfield of the TG Descriptor (X'46') control vector contained in the RSCV were invalid.	X'086B4691'
The contents of the IP Address and Link Service Access Point (LSAP) Address (X'A5') subfield of the TG Descriptor (X'46') control vector contained in the RSCV were invalid.	X'086B46A5'
No DLC Signaling Type (X'91') subfield was found in the TG Descriptor (X'46') control vector contained in the RSCV.	X'086D4691'
No IP Address and Link Service Access Point Address (X'A5') subfield was found in the TG Descriptor (X'46') control vector contained in the RSCV.	X'086D46A5'
Multiple sets of DLC signaling information were found in the TG Descriptor (X'46') control vector contained in the RSCV. IP supports only one set of DLC signaling information.	X'08770019'
Link Definition Error: A link is defined as not supporting HPR, but the port only supports HPR links.	X'08770026'
A called node found no TG Identifier (X'80') subfield within a TG Descriptor (X'46') control vector in a prenegotiation XID for a defined link in an IP network.	X'088C4680'
The XID3 received from the adjacent node does not contain an HPR Capabilities (X'61') control vector. The IP port supports only HPR links.	X'10160031'
The RTP Supported indicator is set to 0 in the HPR Capabilities (X'61') control vector of the XID3 received from the adjacent node. The IP port supports only links to nodes that support RTP.	X'10160032'
The Control Flows over RTP Supported indicator is set to 0 in the HPR Capabilities (X'61') control vector of the XID3 received from the adjacent node. The IP port supports only links to nodes that support control flows over RTP.	X'10160033'
The LDLC Supported indicator is set to 0 in the HPR Capabilities (X'61') control vector of the XID3 received from the adjacent node. The IP port supports only links to nodes that support LDLC.	X'10160034'
The HPR Capabilities (X'61') control vector received in XID3 does not include an IEEE 802.2 LLC (X'80') HPR Capabilities subfield. The subfield is required on an IP link.	X'10160044'
Multiple defined links between a pair of switched ports is not supported by the local node. A link activation request was received for a defined link, but there is an active defined link between the paired switched ports.	X'10160045'
Multiple dynamic links across a connection network between a pair of switched ports is not supported by the local node. A link activation request was received for a dynamic link, but there is an active dynamic link between the paired switched ports across the same connection network.	X'10160046'
Link failure.	X'80020000'
Route selection services has determined that no path to the destination node exists for the specified COS.	X'80140001'

For other sense code information, issue the command **SENSE *xxxxxxxx*,** where *xxxxxxxx* is the sense code from the NetView console, or refer to the IBM SNA Formats manual.

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

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

DP/LW8458 05/05

Printed in the USA