



Configuring CSNA and CMPC

Cisco SNA (CSNA) and Cisco Multipath Channel (CMPC) are software features that enable a Cisco router to establish channel connections with a mainframe host. This chapter provides information about configuring the Cisco SNA (CSNA) and Cisco Multipath Channel support on the CIP and CPA types of CMCC adapters on a Cisco router.

This information is described in the following sections:

- [Overview of CSNA and CMPC, page 1](#)
- [Preparing to Configure CSNA and CMPC, page 3](#)
- [CSNA Support Configuration Task List, page 5](#)
- [CMPC Support Configuration Task List, page 20](#)
- [Monitoring and Maintaining CSNA and CMPC, page 38](#)
- [CSNA and CMPC Configuration Examples, page 39](#)

For a complete description of the CSNA and CMPC commands in this chapter, refer to the “CSNA, CMPC, and CMPC+ Commands” chapter of the *Cisco IOS Bridging and IBM Networking Command Reference* (Volume 2 of 2). To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the [“Identifying Platform Support for Cisco IOS Software Features” section on page 1v](#) in the “Using Cisco IOS Software” chapter.

Overview of CSNA and CMPC

This section provides an overview of the architectural and implementation considerations when configuring a CIP or CPA adapter for connection to a mainframe host using the Cisco SNA or Cisco Multipath Channel features. The following topics are included in this section:

- Cisco SNA Environments
- Cisco Multipath Channel Environments



Cisco SNA Environments

The CSNA feature provides support for Systems Network Architecture (SNA) protocols to the IBM mainframe from Cisco 7500, Cisco 7200, and Cisco 7000 with RSP7000 series routers, using CMCC adapters (over both ESCON and parallel interfaces). As an IBM 3172 replacement, a CMCC adapter in a Cisco router supports the External Communications Adapter (XCA) feature of the Virtual Telecommunications Access Method (VTAM).

Support for the XCA feature allows Logical Link Control (LLC) downstream physical units (PUs) to be defined as switched devices. XCA support also allows the CMCC adapter to provide an alternative to front-end processors (FEPs) at sites where the Network Control Program (NCP) is not required for SNA routing functions.

The CSNA feature supports communication between a channel-attached mainframe and the following types of devices attached to a LAN or WAN:

- Physical Unit (PU) 2.0 SNA node
- PU 2.1 SNA node
- PU 5/4 SNA node

CSNA also supports communication between two mainframes running VTAM that are either channel-attached to the same CMCC adapter card, or channel-attached to different CMCC adapter cards.

The CSNA feature provides SNA connectivity through a Media Access Control (MAC) address that is defined on an internal adapter in a CMCC. The internal adapter is a virtual adapter that emulates the LAN adapter in an IBM 3172 Interconnect Controller. Each internal adapter is defined in a corresponding XCA major node in VTAM, which provides an access point (LAN gateway) to VTAM for SNA network nodes.

The internal adapter is configured on an internal (virtual) Token Ring LAN located in the CMCC. Each CMCC can be configured with multiple internal Token Ring LANs and internal adapters. Each internal Token Ring LAN must be configured to participate in source-route bridging to communicate with the LAN devices attached to the router.

By providing Cisco Link Services (CLS) and the Logical Link Control type 2 (LLC2) protocol stack on the CMCC adapter card, all frames destined to or from the CMCC adapter card are switched by the router. The presentation of LAN media types allows the CSNA feature to take advantage of current source-route bridging (SRB), remote source-route bridging (RSRB), data-link switching plus (DLSw+), Source-Route Translational Bridging (SR/TLB), internal SDLC-LLC2 translational bridging (SDLLC), Qualified Logical Link Control (QLLC) services, and APPN functionality such as SNA Switching Services (SNASw).

Cisco Multipath Channel Environments

CMPC is Cisco's implementation of IBM's MultiPath Channel (MPC) feature on Cisco 7500, Cisco 7200, and Cisco 7000 with RSP7000 series routers. CMPC allows VTAM to establish Advanced-Peer-to-Peer Networking (APPN) connections using both High Performance Routing (HPR) and Intermediate Session Routing (ISR) through channel-attached router platforms.

Routers configured for CMPC can be deployed in Parallel MVS Systems Complex (sysplex) configurations.

CMPC can be used to establish an APPN connection between VTAM and the following types of APPN nodes:

- VTAM on another host that is channel-attached to the same CMCC adapter
- VTAM on another host that is channel-attached to a different CMCC adapter in the same router
- TN3270 server using Dependent LU Requester (DLUR) in the same CMCC adapter
- SNASw in the router with the CMCC adapter
- Other APPN nodes external to the CMCC adapter and router such as Communications Server/2, AS/400, other LAN- or WAN-attached VTAM hosts, or remote routers

One read subchannel and one write subchannel are supported for each MPC transmission group (TG). The read subchannel and write subchannel may be split over two physical channel connections on the same CMCC adapter.

CMPC insulates VTAM from the actual network topology. The MPC protocols are terminated on the CMCC adapter and converted to LLC protocols. After they are converted to LLC protocols, other Cisco features can be used to connect VTAM to other APPN nodes in the network. CMPC can be used in conjunction with DLSw+, RSRB, SR/TLB, SRB, SDLLC, QLLC, ATM LAN emulation, and FRAS host to provide connectivity to VTAM.

CMPC supports connections to PU 2.1 nodes: APPN NN, APPN EN, and LEN. Subarea connections are not supported.

The CMPC feature can coexist with the CLAW, TCP/IP Offload, IP host backup, CSNA, CMPC+, and TN3270 server features on the same CMCC adapter.

Preparing to Configure CSNA and CMPC

The following topics in this section provide information that is useful when you are planning to configure CSNA or CMPC support:

- [Hardware and Software Requirements, page 3](#)
- [Mainframe Host Configuration Considerations, page 4](#)

Hardware and Software Requirements

This section provides information about the router and mainframe requirements to support CSNA and CMPC. The router requirements are the same to support either CSNA or CMPC. However, the minimum level of VTAM required on the mainframe varies by whether you are configuring CSNA or CMPC.

Router Requirements

Both the CSNA and CMPC features are supported on the following router platforms:

- Cisco 7500 series—Supports CIP adapters
- Cisco 7200 series—Supports the ECPA and PCPA adapters
- Cisco 7000 series with RSP7000—Supports CIP adapters

You must configure the CSNA and CMPC features on the physical interface of a CMCC adapter. For a CIP, the physical interface is either 0 or 1. For the CPA adapters, ECPA and PCPA, the physical interface is port 0.

Mainframe Requirements

CSNA and CMPC establish channel connectivity to a mainframe host using VTAM on the host. For questions about the required maintenance level or for information about Program Temporary Fixes (PTFs), consult your IBM representative.

The following versions of VTAM are required to configure CSNA and CMPC on a CMCC adapter:

CSNA VTAM Requirement

- VTAM V3.4 and later

CMPC VTAM Requirements

- MPC APPN ISR connections—VTAM V4.2 and later
- MPC APPN HPR connections—VTAM V4.3 and later

Mainframe Host Configuration Considerations

Configuring CSNA or CMPC support requires that you perform tasks for configuration of the mainframe and the router sides of the network environment.

Often in the mixed network environment of mainframes and LANs, an MVS systems programmer installs and maintains the mainframe side of the network, while a network engineer manages the routers on the LAN side of the network. In such an environment, the successful configuration of CSNA or CMPC support requires the close coordination between these job functions at a customer site.

This chapter contains information for both the network engineer and the MVS systems programmer to properly configure the network devices for CSNA or CMPC support. The tasks for configuring CSNA or CMPC support are organized by whether they are host-related configuration tasks or router-related configuration tasks. In addition, a topic for correlating the mainframe and router configuration is provided so that you can identify the dependencies between the host and router configuration elements and be sure that they are set up correctly.

Defining the Channel Subsystem for the Router

To establish the path and allocate the range of subchannel addresses that the CMCC adapter can use for the CSNA or CMPC features, you need to specify the channel subsystem definitions in the Input/Output Control Program (IOCP) or Hardware Configuration Definition (HCD).

For more information about the statements that might be defined in an IOCP file for parallel channels and ESCON channels on the CIP or CPA, see the “Defining the Channel Subsystem for the Router” section in the “Configuring Cisco Mainframe Channel Connection Adapters” chapter of this publication.

Disabling the Missing Interrupt Handler

Because the appropriate configuration of the missing interrupt handler (MIH) varies according to the protocols and software releases used, Cisco offers the following guidance:

- For OS/390 releases Version 2 Release 4 and earlier, set the MIH to zero.
- For OS/390 releases later than Version 2 Release 4 and z/OS releases, refer to the following section of the z/OS Communications Server IP Configuration Reference:
<http://publibfp.boulder.ibm.com/cgi-bin/bookmgr/BOOKS/f1a1b420/1.2.13?SHELF=f1a1bk31&DT=20020604120755#HDRMOLLY>

For information about how to disable the MIH for the unit addresses being used for your CMCC adapter configuration, see the section “Disabling the Missing Interrupt Handler” section in the “Configuring Cisco Mainframe Channel Connection Adapters” chapter of this publication.

CSNA Support Configuration Task List

CSNA allows CMCC adapters to communicate directly with a mainframe host through VTAM. In this capacity, a CMCC adapter running CSNA can replace the functions of a Token Ring subsystem on a channel-attached front-end processor (FEP) or IBM 3172 Interconnect Controller.

This section describes the configuration tasks required to install CSNA support on the mainframe and router and includes the following topics:

- [CSNA Configuration Guidelines, page 5](#)
- [CSNA Host Configuration Task List, page 6](#)
- [CSNA Router Configuration Task List, page 8](#)
- [Correlating the Router and Mainframe Configuration Elements, page 14](#)
- [CSNA Verification Configuration Task List, page 14](#)

See the “CSNA and CMPC Configuration Examples” section on page 39 for examples.

CSNA Configuration Guidelines

To configure the CSNA feature, you must configure the host VTAM parameters and the CMCC adapter. Consider the following guidelines as you begin to configure CSNA support:

- The CMCC adapters communicate with remote SNA nodes using internal LANs (called virtual or pseudo-rings). An internal LAN can have multiple internal adapters and MAC addresses.
- The CMCC adapters support only the Token Ring type of internal LAN.
- A CMCC adapter can have multiple internal LANs, up to a maximum of 18.



Note Although a CMCC adapter can technically support up to 32 internal LANs, the limit of up to 18 internal adapters on a CMCC adapter makes 18 internal LANs the practical limit.

- A CMCC adapter can have multiple internal adapters, up to a maximum of 18.
- To define the host subchannel (or path) and device, use the **csna** command on the router. The **csna** command is configured on the router’s physical channel interface. On a CIP, the physical interface is on ports 0 and 1. On a CPA, the physical interface is always port 0.

- To configure the internal LANs and adapters, use the following ports on a CMCC interface:
 - On a CIP, configure port 2 which is the virtual channel interface.
 - On a CPA, configure port 0 which is the physical channel interface.
- To define the internal LAN adapter used by CSNA on the router, create an XCA major node in VTAM. The XCA major node controls the activation and deactivation of subchannels and SAPs associated with the CMCC internal adapters that are configured for CSNA. One XCA major node is required for each internal LAN adapter to be used by the CSNA feature in the router.
- CSNA can coexist with CLAW, TCP/IP offload, CMPC, CMPC+, and TN3270 server features on the router. When you configure multiple entities on a CMCC adapter, it is important to be sure that you do not introduce SAP conflicts.

For more information about configuring SAPs, see the “SAP Configuration Guidelines” section in the “Configuring Cisco Mainframe Channel Connections” chapter in this publication.

- CSNA has a limit of 128 SAPs total on the CMCC. So, if you are configuring the TN3270 server using a CSNA connection, the total number of SAPs open on the host plus the number of SAPs defined for PUs on the TN3270 server must be less than or equal to 128.
- If you are configuring CSNA and the TN3270 server on a CMCC, it is good design practice to configure each feature on a separate internal adapter.
- The adapter number that you specify in the **adapter** command on the router must match the adapter number defined in the CSNA XCA major node.
- The host IOCP and HCD parameters must coordinate with the **csna** command parameters on the router and the XCA major node definition to specify the subchannel path, device, and control unit address.
- The unique routing information is determined by a combination of the adapter number, control unit address, and SAP.

CSNA Host Configuration Task List

Configuring CSNA on the mainframe host requires that you establish a path for the CSNA connection by defining the channel subsystem to allocate subchannel addresses, according to the type of router channel connection in use. The tasks in this section assume that the channel subsystem has already been defined to support the CMCC adapter connection.

To establish a SAP for the adapter configured for CSNA in the router, you need to define a VTAM XCA major node. To support the PU type 2.0 and 2.1 connections used in CSNA communication, you need to configure the PU definitions in a switched major node.

This section provides an overview of the primary components needed to implement CSNA on the host. Mainframe systems programmers can use this information as an aid to determine the required parameters to configure CSNA.

The following topics describe the required tasks to configure CSNA on the host:

- [Defining the XCA Major Node, page 7](#)
- [Defining the Switched Major Node, page 7](#)

Defining the XCA Major Node

To configure the internal LAN adapter that is used for CSNA support on the router and to specify the subchannel and SAP to be used by the host to communicate with the router, you need to define an XCA major node.

To configure the XCA major node for CSNA support in VTAM, you must know the following information:

- A valid subchannel configured in the IOCP or HCD on the host that can be used for CSNA.
In the following sample configuration, the subchannel address 584 is shown for the CUADDR parameter. In this example, 584 must be one of the available addresses in the IODEVICE statement for the corresponding CMCC channel connection.
- The adapter number configured in the router that identifies the internal LAN adapter. You must define a separate XCA major node for each internal LAN adapter that is configured for CSNA in the router.

In the following sample configuration, the adapter number 0 is shown for the ADAPNO parameter. In this example, 0 must be the number of the adapter defined on the internal LAN for CSNA use in the CMCC.

VTAM allows SAPs to be defined in multiples of 4. SAP 4 is the most commonly used number for SNA. If you need to define multiple XCA major nodes for multiple internal LAN adapters that are configured for CSNA, you can use the same SAP number of 4 in the XCA major node definition because the ADAPNO parameter uniquely identifies the path.

The following sample configuration shows a sample XCA major node definition (labeled JC27A04) that configures an internal LAN adapter numbered 0 on the router with control unit address 584, and defines a SAP of 4:

```
JC27A04 VBUILD TYPE=XCA
*****
PJEC27A PORT ADAPNO=0, X
CUADDR=584, X
MEDIUM=RING, X
SAPADDR=04, X
TIMER=255
*****
JEC27A GROUP DIAL=YES, X
ANSWER=ON, X
CALL=INOUT, X
AUTOGEN=(3,F,E), X
ISTATUS=ACTIVE
```



Note

The primary configuration elements are shown in bold. All parameters followed by a comma in the PORT and GROUP macros require an X in column 72 as a continuation character.

Defining the Switched Major Node

To support Token Ring PU connections to the host through a CMCC adapter in the router, you need to define switched (dial) connections in VTAM in a switched major node. The remote PUs, defined as PU type 2.0 or 2.1 in the VTAM switched major node, represent the remote SNA controllers (such as an IBM 3174). These PUs can include entities such as a PC running 3270 or APPC emulation packages, PUs configured on DSPU, or a TN3270 server.

The following sample configuration shows a sample switched major node definition labeled C0SWN for a CSNA PU:

```

COSWN VBUILD TYPE=SWNET
COPU1 PU  ADDR=01, X
          PUTYPE=2, X
          IDBLK=05D, X
          IDNUM=C0AA1, X
          MODETAB=ALAMODE, X
          DLOGMODE= SX32702S X
          DISCNT=(NO), X
          USSTAB=USSSNA, X
          ISTATUS=ACTIVE, X
          MAXDATA=521, X
          IRETRY=YES, X
          MAXOUT=7, X
          PASSLIM=5, X
          MAXPATH=4
C0LU101LU LOCADDR=02
C0LU102LU LOCADDR=03
C0LU103LU LOCADDR=04
C0LU104LU LOCADDR=05

```

**Note**

The primary configuration elements are shown in bold. All parameters followed by a comma in the PU macro require an X in column 72 as a continuation character.

CSNA Router Configuration Task List

The following sections describe how to configure a CMCC interface for CSNA support. This procedure requires the configuration of both the physical and virtual interfaces on a CIP.

- [Configuring the CSNA Subchannels, page 9](#)
- [Configuring the Internal LAN, page 10](#)
- [Configuring Internal Adapters, page 10](#)
- [Configuring the Source Bridge, page 12](#)
- [Enabling the Router Configuration, page 13](#)

Configuring the CSNA Subchannels

Configuring the CSNA subchannels establishes the physical path between the CMCC interface and the mainframe channel.

To define an SNA subchannel supported by the CSNA feature, use the following commands beginning in global configuration mode:

Command	Purpose
Step 1 Router(config)# interface channel slot/port	Selects the interface on which to configure CSNA. The <i>port</i> value differs by the type of CMCC adapter: <ul style="list-style-type: none"> • CIP—<i>port</i> value corresponds to the physical interface, which is port 0 or 1. • CPA—<i>port</i> value corresponds to port 0.
Step 2 Router(config-if)# csna path device [maxpiu value] [time-delay value] [length-delay value]	Defines the CSNA subchannel device with the following arguments: <ul style="list-style-type: none"> • <i>path</i>—Four-digit value that represents the channel path for the device. The path value is always 0100 for parallel channels. • <i>device</i>—Unit address for the device on the subchannel. The available options for this command are: <ul style="list-style-type: none"> • maxpiu—(Optional) Maximum packet size (in the range 4096 to 65535 bytes) that the CMCC adapter sends to the host in one I/O operation. The default is 20470 bytes. Note Values for a maxpiu less than 819 bytes are not recommended because of potential LONGREC errors produced by VTAM. <ul style="list-style-type: none"> • time-delay—(Optional) Maximum allowable delay (in the range 0 to 100 ms) before the CMCC adapter sends packets to the host. The default is 10 ms. • length-delay—(Optional) Minimum data length (in the range 0 to 65535 bytes) to accumulate before the CMCC adapter sends packets to the host. The default is 20470 bytes.

Use the **no csna** command to remove the CSNA subchannel device.

Mainframe Configuration Tip

Configuring the subchannel information in the router requires that you correlate the *path* and *device* information from the IOCP or HCD file on the host.


- The *path* argument is a four-digit hexadecimal value that concatenates the path value (2 digits), EMIF partition number (1 digit), and control unit logical address (1 digit).
- The *device* argument is a valid number in the UNITADD range of the IOCP CNTLUNIT statement for the CSNA internal LAN adapter.

For detailed information about how to determine the *path* and *device* values for the **csna** command, see the “Correlating Channel Configuration Parameters” section in the “Configuring Cisco Mainframe Channel Connection Adapters” chapter in this publication.

Configuring the Internal LAN

The CSNA feature resides on an internal LAN and adapter in the CMCC on the router. The internal LAN is a virtual Token Ring LAN that is defined within the CIP or CPA on the router. Unlike the CSNA subchannel path that you define on the physical interface of the CMCC, you define the internal LAN on the virtual interface of the CIP. For the CPA, you can only configure the physical interface port.

To configure an internal LAN, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface channel slot/port	Selects the interface on which to configure the internal LAN. The <i>port</i> value differs by the type of CMCC adapter: <ul style="list-style-type: none"> • CIP—<i>port</i> value corresponds to the virtual interface, which is port 2. • CPA—<i>port</i> value corresponds to port 0.
Step 2	Router(config-if)# lan tokenring lan-id	Selects a Token Ring internal LAN interface identified by <i>lan-id</i> and enters internal LAN configuration mode.
		 <p>Note Token Ring is the only type of internal LAN supported on channel interfaces.</p>

Configuring Internal Adapters

To configure CSNA on the internal LAN, you also need to configure an internal adapter for CSNA use on the LAN. Naming the internal adapter is optional. However, selecting meaningful names for the internal adapters that you configure can simplify identification of the adapter in **show** command output and when troubleshooting is required.

You can configure multiple internal adapters (up to 18) on a CMCC. If you want to support internal adapters with duplicate MAC addresses, you must define the adapter on a different internal LAN and use a unique relative adapter number (RAN). Each internal adapter that is configured for CSNA must have a corresponding XCA major node definition on the host.

To select or configure an internal adapter, use the following commands in internal LAN configuration mode:

	Command	Purpose
Step 1	Router(cfg-lan)# adapter <i>adapno mac-address</i>	Selects the internal adapter to configure for CSNA with the following arguments: <ul style="list-style-type: none"> • <i>adapno</i>—Relative adapter number (RAN). • <i>mac-address</i>—MAC address for the adapter on the internal LAN. The MAC address cannot be a duplicate on the same internal LAN.
Step 2	Router(cfg-adap)# name <i>name</i>	(Optional) Specifies a name for the internal adapter.

Use the **no adapter** command to remove an internal adapter.

Mainframe Configuration Tip

The value for the *adapno* argument in the **adapter** command on the router must match the value specified for the ADAPNO parameter in the corresponding XCA major node definition in VTAM for CSNA. Each internal adapter that is configured for CSNA must have its own XCA major node definition.

Configuring an Internal Adapter's Link Characteristics

To configure the LLC link characteristics of an internal adapter, use the following commands in internal adapter configuration mode, as needed:

Command	Purpose
Router(cfg-adap)# llc2 n1 <i>bytes</i>	(Optional) Specifies the maximum size (up to 4105 bytes) of an I-frame. The default is 4105 bytes.
Router(cfg-adap)# llc2 n2 <i>retry-count</i>	(Optional) Specifies the maximum retry count (up to 255). The default is 8.
Router(cfg-adap)# llc2 nw <i>window-size-increase</i>	(Optional) Increases the window size for consecutive good I-frames received (0 is disabled). The default is 0.
Router(cfg-adap)# llc2 ack-delay-time <i>milliseconds</i>	(Optional) Specifies the maximum time (up to 60000 ms) for incoming I-frames to stay unacknowledged. The default is 100 ms.
Router(cfg-adap)# llc2 ack-max <i>frame-count</i>	(Optional) Specifies the maximum number of I-frames received (up to 127) before an acknowledgment must be sent. The default is 3.
Router(cfg-adap)# llc2 idle-time <i>milliseconds</i>	(Optional) Specifies the frequency of polls (up to 60000 ms) during periods of idle traffic. The default is 60000 ms.
Router(cfg-adap)# llc2 local-window <i>frame-count</i>	(Optional) Specifies the maximum number of I-frames to send (up to 127) before waiting for an acknowledgment. The default is 7.
Router(cfg-adap)# llc2 recv-window <i>frame-count</i>	(Optional) Controls the number of frames in the receive window. The default is 7.

Command	Purpose
Router(cfg-adap)# llc2 t1-time <i>milliseconds</i>	(Optional) Specifies the amount of time to wait (up to 60000 ms) for an acknowledgment to send I-frames. The default is 1000 ms.
Router(cfg-adap)# llc2 tbusy-time <i>milliseconds</i>	(Optional) Specifies the amount of time to wait (up to 60000 ms) while the other LLC2 station is in a busy state before attempting to poll the remote station. The default is 9600 ms.
Router(cfg-adap)# llc2 tpf-time <i>milliseconds</i>	(Optional) Specifies the amount of time to wait (up to 60000 ms) for a final response to a poll frame before resending the original poll frame. The default is 1000 ms.
Router(cfg-adap)# llc2 trej-time <i>milliseconds</i>	(Optional) Specifies the amount of time to wait (up to 60000 ms) for resending a rejected frame before sending the reject command. The default is 3200 ms.

Configuring the Source Bridge

Source-route bridging (SRB) is required to get packets from the LANs that are external to the CMCC adapter, to the internal LAN on the CIP or CPA and the CSNA feature. The **source-bridge** command identifies the interfaces in the same ring group. Frames are sent only to interfaces in the same ring group.

When you configure the source bridge, you can assign the following types of priorities:

- **LOCADDR** priority—Allows you to map LUs to queuing priorities for the internal LAN by specifying a defined LOCADDR priority using the **locaddr-priority** command. The LOCADDR priorities are defined using the **locaddr-priority-list** command in global configuration mode.
- **SAP** priority—Allows you to assign priorities for the internal LAN according to the service access point and MAC address in an LLC2 session by specifying a defined SAP priority using the **sap-priority** command. The SAP priorities are defined using the **sap-priority-list** command in global configuration mode.

To configure the bridging characteristics for the internal LAN, use the following commands in internal LAN configuration mode:

Command	Purpose
Step 1 Router(cfg-lan)# source-bridge source-ring-number bridge-number target-ring-number	Configures source-route bridging for the selected internal LAN interface with the following arguments: <ul style="list-style-type: none"> • <i>source-ring-number</i>—Number for the Token Ring on the internal LAN for the CIP or CPA. • <i>bridge-number</i>—Bridge number connecting the source and target Token Rings. • <i>target-ring-number</i>—Number of the destination ring number on the router. The target ring can also be a ring group.

	Command	Purpose
Step 2	Router(cfg-lan)# locaddr-priority <i>list-number</i>	(Optional) Assigns a LOCADDR priority for the internal LAN, where <i>list-number</i> is a value defined from the locaddr-priority-list command.
Step 3	Router(cfg-lan)# sap-priority <i>list-number</i>	(Optional) Assigns a SAP priority for the internal LAN, where <i>list-number</i> is a value defined from the sap-priority-list command.

Use the **no source-bridge** command to disable source-route bridging.

Enabling the Router Configuration

After you complete the tasks to configure CSNA on the router, be sure that you enable the configuration using the **no shut** command on all of the applicable interfaces. For the CIP, this means that you need to run the **no shut** command on the selected physical interface, and again for the virtual interface.

For the CPA, you only need to run the **no shut** command on the physical interface.

To enable the router configuration for CSNA, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface channel <i>slot/port</i>	Selects the interface. The <i>port</i> value differs by the type of CMCC adapter: <ul style="list-style-type: none"> • CIP—<i>port</i> value corresponds to 0 or 1 for the physical interface, and 2 for the virtual interface. • CPA—<i>port</i> value corresponds to port 0.
Step 2	Router(config-if)# no shut	Restarts the selected interface.

Correlating the Router and Mainframe Configuration Elements

Table 1 shows a summary of the configuration elements on the router and host that must be correlated for proper operation of CSNA. The column labeled “Configuration Element” identifies the type of entity to be configured. The columns labeled “Router Configuration” and “Mainframe Configuration” identify the related parameters on the router and the mainframe whose values must be compatible or match.

Table 1 Relationship of Router and Mainframe Configuration Elements for CSNA

Configuration Element	Router Configuration	Mainframe Configuration
Subchannels	<i>path</i> and <i>device</i> arguments of the csna command	RESOURCE PARTITION, CHPID, and CNTLUNIT statements of the IOCP definition defining the following parameters for the CSNA channel path: <ul style="list-style-type: none"> • LPAR number (if defined) in the RESOURCE PARTITION and CHPID statements—Specify in the third digit of the <i>path</i> argument in the router csna command. • CUADD value (if defined) in the CNTLUNIT statement—Specify in the fourth digit of the <i>path</i> argument in the router csna command. • Available device address in the UNITADD parameter of the CNTLUNIT statement—Specify in the <i>device</i> argument of the router csna command.
Internal adapter number	<i>adapno</i> argument of the adapter command	ADAPNO parameter in the XCA major node definition for the corresponding CSNA internal adapter

CSNA Verification Configuration Task List

Configuring CSNA includes tasks for both the mainframe and the router. This section describes the steps to verify that you have successfully configured CSNA on a CIP. It provides procedures to verify connectivity from the router perspective and from the host perspective, and includes troubleshooting tips as a guide when the configuration verification fails.

This section includes the following topics:

- [Initial Host and Router Configuration, page 15](#)
- [Verifying CSNA Channel Connectivity, page 16](#)
- [Verifying Communication with VTAM, page 18](#)

Initial Host and Router Configuration

Consider that you begin the verification procedures with the following sample XCA major node definition, switched major node definition, and initial router configuration:

XCA Major Node Definition

```
JC27A04  VBUILD  TYPE=XCA
PJEC27A  PORT  ADAPNO=0,                X
          CUADDR=27A,                    X
          SAPADDR=04,                    X
          MEDIUM=RING,                   X
          TIMER=244
JEC27A   GROUP ANSWER=ON,                X
          AUTOGEN=(3,F,3),                X
          CALL=INOUT,                     X
          DIAL=YES,                        X
          ISTATUS=ACTIVE
```

Switched Major Node Definition

```
C0SWN  VBUILD  TYPE=SWNET
COPU1  PU      ADDR=01,                  X
          PUTYPE=2,                       X
          IDBLK=05D,                       X
          IDNUM=C0AA1,                     X
          MODETAB=ALAMODE,                 X
          DLOGMODE= SX32702S,              X
          DISCNT=(NO),                     X
          USSTAB=USSSNA,                   X
          ISTATUS=ACTIVE,                  X
          MAXDATA=521,                     X
          IRETRY=YES,                      X
          MAXOUT=7,                        X
          PASSLIM=5,                       X
          MAXPATH=4
C0LU101LU  LOCADDR=02
C0LU102LU  LOCADDR=03
C0LU103LU  LOCADDR=04
C0LU104LU  LOCADDR=05
```



Note

The verification procedures assume that the XCA major node and switched major node are defined, but not yet activated.

Router Configuration for Internal LAN on a CIP

```
interface channel 2/1
 no ip address
 no ip directed-broadcast
 no keepalive
!
interface channel 2/2
 no ip redirects
 no ip directed-broadcast
 no keepalive
 lan Token Ring 0
  source-bridge 100 1 400
  adapter 0 4000.8001.0100
```

**Note**

The initial router configuration in the [“Router Configuration for Internal LAN on a CIP”](#) section on page 15 shows the internal LAN, source-bridge, and internal adapter configuration in preparation for configuration of CSNA.

Verifying CSNA Channel Connectivity

If you have defined the channel paths for the router at the mainframe host in the IOCP or HCD, you can begin to configure the router for CSNA support and verify connectivity at the channel level first. Isolating this level of verification is useful when the VTAM configuration is not completed, but you want to establish that the router can successfully communicate with the host.

Verifying channel connectivity confirms the following aspects of the router configuration:

- Microcode is loaded on the CMCC
- CMCC adapter is functional
- CMCC can communicate with the host over the channel path

Verifying CSNA Channel Connectivity from the Router

The steps in this section show how to verify the CSNA channel configuration beginning with running the **csna** command on the router’s physical interface. The following assumptions are made for the procedure described in this section:

- The router’s virtual interface is already configured with the required internal LAN, source-bridge, and internal adapter statements as shown in the initial router configuration for a CIP in the [“Router Configuration for Internal LAN on a CIP”](#) section on page 15.
- The router has the recommended CMCC hardware and microcode versions to support the CSNA feature. You can use the **show version**, **show controllers cbus**, and **show controllers channel** commands to verify the Cisco IOS software and CMCC microcode versions.

**Note**

Before you begin on the router, run the **debug channel events** command so that you can verify the messages on the router console.

To verify CSNA channel connectivity, perform the following steps:

- Step 1** From the router, configure the **csna** command on the physical interface according to your site’s requirements as shown in the following example:

```
interface channel 2/1
csna C190 7A
```

Confirm that you receive a message stating “Device Initialized,” similar to the following display:

```
C190-7A Device Initialized
```

- Step 2** To verify that the channel is up and the line protocol is up, go to EXEC command mode and run the **show interfaces channel** command as shown in the following example:

```
show interfaces channel 2/1
```


- Step 3** To verify that the physical channel is up, run the **show extended channel statistics** command as shown in the following example:

```
show extended channel 2/1 statistics
```

Verify that the path field in the output for the CSNA device shows “ESTABLISHED,” which means that the physical channel is up.

- Step 4** If your **show** command output matches the values described in [Step 2](#) and [Step 3](#), then the channel connection between the mainframe and the router is established. If you cannot confirm the values, see the [“Troubleshooting Tips for Channel Connectivity”](#) section on page 17.
-

Verifying CSNA Channel Connectivity from the Host

After CSNA has been configured on the router, you can also verify channel connectivity from the host by performing the following steps:

- Step 1** From the host, verify that the device is online using the following sample command to display the device:

```
d u,,,27A
```

- Step 2** If the device is offline, then vary the device online according to your site’s configuration as shown in the following sample command:

```
v 27A,online
```



Note The CHPID for the device should already be active on the host.

- Step 3** If the device comes online, then the channel connection between the mainframe and the router is established. If the device does not come online, or you receive the message “No paths physically available,” see the [“Troubleshooting Tips for Channel Connectivity”](#) section on page 17.
-

Troubleshooting Tips for Channel Connectivity

There are several indicators on the router and the mainframe that indicate that the channel connection is not available.

- From the router, you might see the following things:
 - The output from the **show interfaces channel** command shows that the channel or line protocol is down.
 - The output from the **show interface channel statistics** command shows that the path is not established (the physical channel is not up).
- From the host, you might see the following things:
 - The device is not online.
 - When you vary the device online, you receive the message “No paths physically available.”

Recommended Action

If you determine that the channel connection is not available, review the following tasks to be sure that you have performed them correctly:

- Be sure that you enabled the CSNA router configuration using the **no shut** command to restart the interface. If you configured both the physical and virtual interface on a CIP, be sure to run the **no shut** command on both interfaces.
- Be sure that the CSNA device (and path) are online at the host.
- Verify that the *path* and *device* arguments that you specified in your **csna** configuration command correlate properly to the host IOCP or HCD configuration.

If none of these recommended actions allow you to establish the channel connection, check your CMCC LED indicators and the physical channel connection.

Verifying Communication with VTAM

After the VTAM XCA major node is installed, you can verify communication between the router and VTAM using CSNA. If you have installed a switched major node, you can also verify a session from a network device to the host.

This section includes the following verification procedures:

- [Verifying Communication with VTAM from the Host, page 18](#)
- [Verifying Communication with VTAM from the Router, page 19](#)
- [Troubleshooting Tips for VTAM, page 20](#)

Verifying Communication with VTAM from the Host

This procedure describes how to verify from the host that the XCA major node and switched major node are configured and activated.

To verify communication with VTAM from the host, perform the following steps:

-
- Step 1** If you have configured a switched major node, activate the switched major node from the host using the following sample command:

```
v net,act,id=C0SWN
```

Verify that you receive the following console messages:

```
IST097I VARY ACCEPTED
IST093I C0PU1 ACTIVE
IST093I C0SWN ACTIVE
```

- Step 2** From the host, activate the XCA major node using the following sample command:

```
v net,act,id=JC27A04
```

Verify that you receive the following console messages:

```
IST097I VARY ACCEPTED
IST093I JC27A04 ACTIVE
IST093I C0SWN ACTIVE
```

If you receive a message similar to the following display, see the [“Troubleshooting Tips for VTAM” section on page 20](#):

```
IST380I ERROR FOR ID=F027A000 - REQUEST: ACTLINK, SENSE: 081C003C
IST380I ERROR FOR ID=F027A001 - REQUEST: ACTLINK, SENSE: 081C003C
IST380I ERROR FOR ID=F027A002 - REQUEST: ACTLINK, SENSE: 081C003C
```

Step 3 (Optional) Using a network station defined with the proper settings, establish a session with the host. In our example, the station should specify the following parameters:

- MAC address of the adapter on the internal LAN as the destination address—4000.8001.0100
- IDBLK/IDNUM (XID) combination for the destination PU, as defined in the switched major node—05DC0AA1
- Destination SAP, as defined in the XCA major node—4

Display the switched major node using the following sample command, and verify that the PU is active and the corresponding LU shows ACT/S:

```
d net, id=C0SWN,e
```

If the PU for the device is not active, see the [“Troubleshooting Tips for VTAM” section on page 20](#).

Verifying Communication with VTAM from the Router

This procedure describes how to verify communication with the VTAM XCA major node for CSNA from the router.

To verify communication with VTAM from the router, perform the following steps:

Step 1 Run the **show extended channel statistics** command as shown in the following example:

```
show extended channel 2/1 statistics
```

Verify that the following is displayed in these fields of the output for the CSNA device:

- Path—The CSNA path is “ESTABLISHED,” which means that the physical channel is up.
- Con—The connection value is “Y,” which means that the subchannel is up and the CSNA connection is established between the router and the mainframe.

Step 2 To verify that the CMCC adapter has opened a SAP, run the **show extended channel connection-map llc2** command as shown in the following example:

```
show extended channel 2/2 connection-map llc2
```

Step 3 To verify the operational status of the CSNA device, run the **show extended channel csna oper** command as shown in the following example:

```
show extended channel 2/1 csna oper
```

For information about other commands that are useful when diagnosing or monitoring your CSNA connection, see the [“Monitoring and Maintaining CSNA and CMPC” section on page 38](#).

Troubleshooting Tips for VTAM

This section describes recommended actions for the following problems that might occur during verification of communication with VTAM.

- From the router, you might see the following output:
 - The **show interface channel statistics** command shows the field Con=N (the subchannel is not allocated). This output is normal if the XCA major node is not active.
- From the host, you might see the following output:
 - The IST380I message with sense code 081C003C is displayed when you activate the XCA major node.
 - The PU is not active when you display the switched major node after attempting to establish a session.

Recommended Actions

If you encounter problems during verification of communication with VTAM, perform the following tasks to recover:

- If the **show interface channel statistics** command shows that the path is established (the physical channel is up), but the subchannel is not allocated (Con=N), verify that the XCA major node is activated.
- If you receive the sense code 081C003C when activating the XCA major node at the host, review the following tasks to be sure that you have performed them correctly:
 - If you have not already verified channel connectivity, follow the procedure described in the [“Verifying CSNA Channel Connectivity”](#) section on page 16.
 - If the channel connectivity is established, verify the configuration values for the adapter number, control unit address, and SAP.

Be sure that the adapter number that you specified in the XCA major node matches the adapter number on the internal LAN in the router. Verify that the control unit address corresponds to the CSNA device configured on the router and in the IOCP or HCD, and that the SAP is a valid multiple of 4. Be sure that you do not have any SAP conflicts within the router configuration.
- If the PU is not active after attempting to establish a session, verify the values for the following configuration elements in the network device:
 - XID value for the destination device matches the IDBLK/IDNUM value in the switched major node.
 - Destination MAC address matches the MAC address of the internal adapter in the CMCC.
 - Destination SAP address matches the SAP value in the XCA major node. Remember that the SAP address in the XCA major node is in decimal format.

CMPC Support Configuration Task List

CMPC implements the full-duplex IBM channel protocol for SNA, APPN, and HPR traffic. CMPC allows VTAM to establish APPN connections using HPR or ISR through a channel-attached router using a CMCC adapter. CMPC also supports TN3270 using DLUR.

To configure the CMPC feature, you must configure the host VTAM parameters and the CMCC adapter. Consider the following guidelines as you prepare to configure CMPC support:

- The CMCC adapters communicate with remote SNA nodes using internal LANs (called virtual or pseudo-rings). An internal LAN can have multiple internal adapters and MAC addresses.
- The CMCC adapters support only the Token Ring type of internal LAN.
- A CMCC adapter can have multiple internal LANs, up to a maximum of 18.



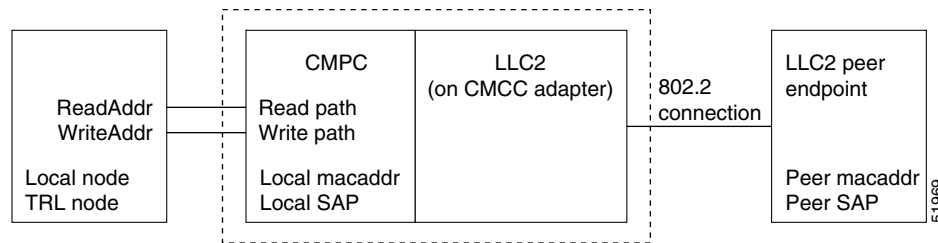
Note Although a CMCC adapter can technically support up to 32 internal LANs, the limit of up to 18 internal adapters on a CMCC adapter makes 18 internal LANs the practical limit.

- A CMCC adapter can have multiple internal adapters, up to a maximum of 18.
- To configure the internal LANs and adapters, use the following ports on a CMCC interface:
 - On a CIP, configure port 2 which is the virtual channel interface.
 - On a CPA, configure port 0 which is the physical channel interface.
- A CMPC link uses two subchannels: one read and one write. Some IBM implementations of MPC allow multiple read and multiple write subchannels within a link. CMPC does not support multiple read and write subchannels. Only one read subchannel and one write subchannel can be configured for each CMPC link. A CMPC link is also referred to as a CMPC TG.
- On the router a CMPC TG consists of one read subchannel definition, one write subchannel definition, and a TG definition, associated by a unique *tg-name*.
- A CMCC adapter can have multiple CMPC links (TGs), up to a maximum of 64.
- To configure the LLC2 interface for the CMCC adapter, use the **tg** (CMPC) command and specify the internal adapter number (which is used to derive the source, or local MAC address) and local SAP address for VTAM. In the **tg** (CMPC) command, you must also identify the remote MAC address and remote SAP of the LLC2 peer with which CMPC communicates. Though this is called the “remote” MAC and SAP, the peer might reside within the router.
- To define the host subchannel (or path) and device, use the **cmpr** command on the router. One **cmpr** command defines the read subchannel, and one **cmpr** command defines the write subchannel. The **cmpr** command is configured on the CMCC adapter’s physical interface (port 0 or 1 on a CIP; port 0 on a CPA).
- The two subchannels in a CMPC link do not need to be adjacent devices. Either channel can be the read subchannel or the write subchannel. The two subchannels can be on separate channel process IDs (CHPIDs) in the host.
- The two subchannels must be connected to the same CMCC adapter, however they do not have to be connected to the same physical channel interface on a CIP. On a CIP it is possible to connect a read subchannel to channel interface 0, while the write subchannel is connected to channel interface 1.
- The host IOCP or HCD parameters must coordinate with the **cmpr** command parameters on the router and the transport resource list major node definition to specify the subchannel path, device, and subchannel address.
- To configure MPC on the host, define the Transport Resource List (TRL) and the local SNA major nodes. If you do not plan to support HPR, then you need to disable support in the TRL major node by configuring HPR=NO.

- CMPC can coexist with CLAW, TCP/IP offload, IP host backup, CSNA, CMPC+, and TN3270 server features on the router.
- Only APPN connections are supported across CMPC. For this reason when you configure TN3270 server with CMPC, you must configure the TN3270 server as an APPN end node with DLUR.

As an overview of the configuration process, refer to [Figure 1](#), which shows the CMPC link between the VTAM host, the router, and CMCC adapter card, and the communication to the LLC2 endpoint. The read and write addresses defined in the VTAM host correspond to the read and write paths defined for CMPC. CMPC communicates with the LLC2 stack, which communicates to the endpoint of the connection by means of the IEEE 802.2 link.

Figure 1 Logical View of CMPC Link



This section describes the configuration tasks required to install CMPC support on the mainframe and router and includes the following topics:

- [Configuring CMPC on the Host, page 22](#)
- [Configuring CMPC on the Router, page 24](#)
- [Correlating the Mainframe and Router Configuration Elements, page 29](#)
- [CMPC Verification Configuration Task List, page 30](#)

See the “[CSNA and CMPC Configuration Examples](#)” section on [page 39](#) for examples.

Configuring CMPC on the Host

Configuring CMPC on the mainframe host requires that you define the TRL and local SNA major nodes. One TRL major node might include several transport resource list entries (TRLEs). The local SNA major node references the TRLE to be used for a specific connection to the control point (CP) in the CMCC.

This section provides an overview of the primary components needed to implement CMPC on the host. Mainframe systems programmers can use this information as an aid to determine the required parameters to configure CMPC.

The following topics describe the required tasks to configure CMPC on the host:

- [Configuring the VTAM Transport Resource List Major Node, page 23](#)
- [Configuring the VTAM Local SNA Major Node, page 23](#)

Configuring the VTAM Transport Resource List Major Node

To configure MPC on the host, you need to define a Transport Resource List (TRL) major node. To define the TRL, you must have two valid subchannel addresses configured in the IOCP or HCD on the host that can be used for the read and write subchannels. The read/write subchannels that you configure in the TRL should correlate with the unit addresses configured in the *device* argument of the **cmpc** commands.

For details on how to configure the TRL major node, see the following IBM documents:

- *VTAM Resource Definition Samples*, SC31-6554
- *VTAM Operation*, SC31-6549
- *VTAM Network Implementation Guide*, SC31-6548

The following example shows a typical TRL major node configuration:

```
LAGTRLA  VBUILD TYPE=TRL
LAGTRLEA  TRLE  LNCTL=MPC,MAXBFRU=8,REPLYTO=3.0,          X
READ=(2F0),                                           X
WRITE=(2F1)
```

In this example, device 2F0 has been configured for read and 2F1 has been configured for write. 2F0 and 2F1 must be available subchannels in the IOCP or HCD definition for the CMCC adapter connection.

You should activate the TRL before activating the corresponding local major node. The following example shows the command to activate a TRL, where the ID parameter specifies the name of the TRL, LAGTRLA:

```
v net,act,id=lagtrla,update=add
```

Note that “update=add” is preferred and is the default for later versions of VTAM. The argument “update=all” can cause inactive TRLEs to be deleted unexpectedly from ISTTRL. However, “update=all” must be used if you change an active TRL major node and want the changes to become active.

The following commands are useful for displaying the current list of TRLEs:

- **d net,trl**
- **d net,id=isttrl,e**
- **d net,trl,trle=trle_name**

Configuring the VTAM Local SNA Major Node

To configure the MPC channel link on the VTAM host, define the local SNA major node.

The following is an example of a typical configuration:

```
LAGLNA  VBUILD TYPE=LOCAL
LAGPUA  PU  TRLE=LAGTRLEA,          X
        ISTATUS=ACTIVE,           X
        XID=YES, CONNTYPE=APPN, CPCP=YES, HPR=YES
```

The TRLE parameter in the local node specifies the label on the TRLE statement from the TRL major node LAGTRLA. If you do not want to run HPR be sure to specify HPR=NO.

Before you activate the local SNA major node, you must activate the TRL node. The following example shows the command to activate a local node, where the ID parameter specifies the name of the local node, LAGLNA:

```
v net,act,id=laglna
```

Configuring CMPC on the Router

The following sections describe how to configure a CMCC interface for CMPC support. This procedure requires the configuration of both the physical and virtual interfaces on a CIP.

- [Configuring the CMPC Subchannels, page 24](#)
- [Configuring the CMPC Transmission Groups, page 25](#)
- [Configuring the Internal LAN, page 26](#)
- [Configuring Internal Adapters, page 26](#)
- [Configuring the Source Bridge, page 28](#)
- [Enabling the Router Configuration, page 28](#)

Configuring the CMPC Subchannels

Configuring the CMPC subchannels establishes the physical path between the CMCC interface and the mainframe channel.

To define a CMPC read subchannel and CMPC write subchannel, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface channel slot/port	Selects the interface on which to configure CMPC. The <i>port</i> value differs by the type of CMCC adapter: <ul style="list-style-type: none"> • CIP—<i>port</i> value corresponds to the physical interface, which is port 0 or 1. • CPA—<i>port</i> value corresponds to port 0.
Step 2	Router(config-if)# cmcp path device tg-name read	Defines the CMPC read subchannel device with the following arguments: <ul style="list-style-type: none"> • <i>path</i>—Four-digit value that represents the channel path for the device. The path value is always 0100 for parallel channels. • <i>device</i>—Unit address for the device on the subchannel. • <i>tg-name</i>—Name of the CMPC TG, up to eight characters.
Step 3	Router(config-if)# cmcp path device tg-name write	Defines the CMPC write subchannel device with the following arguments: <ul style="list-style-type: none"> • <i>path</i>—Four-digit value that represents the channel path for the device. The path value is always 0100 for parallel channels. • <i>device</i>—Unit address for the device on the subchannel. This unit address must be a different address than the unit address for the CMPC read subchannel. • <i>tg-name</i>—Name of the CMPC TG, up to eight characters.

Use the **no cmcp path device** command to remove the definition of a subchannel.

Mainframe Configuration Tips

- Configuring the subchannel information in the router requires that you correlate the *path* and *device* information from the IOCP or HCD file on the host.
 - The *path* argument is a four-digit hexadecimal value that concatenates the path value (two digits), EMIF partition number (one digit), and control unit logical address (one digit).
 - The *device* argument is a valid number in the UNITADD range of the IOCP CNTLUNIT statement for the CMPC internal LAN adapter.

For detailed information about how to determine the *path* and *device* values for the **cmpc** command, see the “Correlating Channel Configuration Parameters” section in the “Configuring Cisco Mainframe Channel Connection Adapters” chapter in this publication.

- The **cmpc** commands on the router define the subchannel addresses that CMPC will use to connect to the host, and correspond to the definitions in the TRL major node on the host. Normally, the last two hexadecimal digits in the READ parameter of the TRL match the value of the *device* argument in the corresponding **cmpc read** command. Similarly, the last two hexadecimal digits in the WRITE parameter of the TRL match the value of the *device* argument in the **cmpc write** command.

Configuring the CMPC Transmission Groups

Configuring the CMPC TG defines the MAC/SAP quadruple addressing of an LLC connection. CMPC TGs are configured on the virtual interface of a CIP, and the physical interface of a CPA.

To define a CMPC TG by name and specify its connection to the LLC2 stack, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface channel slot/port	Selects the interface on which to configure the CMPC TG. The <i>port</i> value differs by the type of CMCC adapter: <ul style="list-style-type: none"> • CIP—<i>port</i> value corresponds to the virtual interface, which is port 2. • CPA—<i>port</i> value corresponds to port 0.
Step 2	Router(config-if)# tg name llc token-adapter adapter-number lsap [rmac rmac] [rsap rsap]	Defines the LLC connection parameters for the CMPC TG with the following arguments: <ul style="list-style-type: none"> • <i>name</i>—Name (up to eight characters) of the TG. This name must match the name specified in the cmpc command. • <i>adapter-number</i>—Relative adapter number of the internal adapter on the CMCC’s internal Token Ring LAN. • <i>lsap</i>—Local SAP number (multiple of four, from 04 to FC in hexadecimal) to open on the adapter for the connection to VTAM. This SAP number must not conflict with another SAP on the internal adapter for the CMCC. • rmac rmac—MAC address of a partner link station. • rsap rsap—SAP address of a partner link station.

The local SAP, remote MAC, and remote SAP parts of the addressing are defined explicitly in the corresponding parameters of the **tg** (CMPC) command. The local MAC address is derived from the internal adapter number that you specify in the *adapter-number* argument. Be sure that you specify a unique local SAP that does not conflict with other SAPs on the same internal adapter.

Use the **no tg** command to remove a CMPC TG from the configuration, which will deactivate the named CMPC TG. To change any parameter of the **tg** statement, the statement must be removed by using the **no tg tg-name** command.

Router Configuration Tip

The *name* that you specify for the CMPC TG must match the name that you specify in the *tg-name* argument of the **cmpc** command on the physical interface of the same CMCC adapter.

Configuring the Internal LAN

The CMPC feature resides on an internal LAN and adapter in the CMCC on the router. The internal LAN is a virtual Token Ring LAN that is defined within the CIP or CPA on the router. Unlike the CMPC subchannel path that you define on the physical interface of the CMCC, you define the internal LAN on the virtual interface of the CIP. For the CPA, you can only configure the physical interface port.

To configure an internal LAN, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface channel slot/port	Selects the interface on which to configure the internal LAN. The <i>port</i> value differs by the type of CMCC adapter: <ul style="list-style-type: none"> • CIP—<i>Port</i> value corresponds to the virtual interface, which is port 2. • CPA—<i>Port</i> value corresponds to port 0.
Step 2	Router(config-if)# lan tokenring lan-id	Selects a Token Ring internal LAN interface identified by <i>lan-id</i> and enters internal LAN configuration mode.

Configuring Internal Adapters

To configure CMPC on the internal LAN, you also need to configure an internal adapter for CMPC use on the LAN. Naming the internal adapter is optional. However, selecting meaningful names for the internal adapters that you configure can simplify identification of the adapter in **show** command output and when troubleshooting is required.

You can configure multiple internal adapters (up to 18) on a CMCC. If you want to support internal adapters with duplicate MAC addresses, you must define the adapter on a different internal LAN and use a unique relative adapter number (RAN).

To select or configure an internal adapter, use the following command in internal LAN configuration mode:

	Command	Purpose
Step 1	Router(cfg-lan)# adapter adapno mac-address	Selects the internal adapter to configure for CSNA with the following arguments: <ul style="list-style-type: none"> • <i>adapno</i>—Relative adapter number (RAN). • <i>mac-address</i>—MAC address for the adapter on the internal LAN. The MAC address cannot be a duplicate on the same internal LAN.
Step 2	Router(cfg-adap)# name name	(Optional) Specifies a name for the internal adapter.

Use the **no adapter** command to remove an internal adapter.

Router Configuration Tip

The value for the *adapno* argument in the **adapter** command on the router must match the value specified in the **tg** (CMPC) command for the CMPC TG.

Configuring an Internal Adapter's Link Characteristics

To configure the LLC link characteristics of an internal adapter, use the following commands in internal adapter configuration mode, as needed:

Command	Purpose
Router(cfg-adap)# llc2 n1 <i>bytes</i>	(Optional) Specifies the maximum size (up to 4105 bytes) of an I-frame. The default is 4105 bytes.
Router(cfg-adap)# llc2 n2 <i>retry-count</i>	(Optional) Specifies the maximum retry count (up to 255). The default is 8.
Router(cfg-adap)# llc2 nw <i>window-size-increase</i>	(Optional) Increases the window size for consecutive good I-frames received (0 is disabled). The default is 0.
Router(cfg-adap)# llc2 ack-delay-time <i>milliseconds</i>	(Optional) Specifies the maximum time (up to 60000 ms) for incoming I-frames to stay unacknowledged. The default is 100 ms.
Router(cfg-adap)# llc2 ack-max <i>frame-count</i>	(Optional) Specifies the maximum number of I-frames received (up to 127) before an acknowledgment must be sent. The default is 3.
Router(cfg-adap)# llc2 idle-time <i>milliseconds</i>	(Optional) Specifies the frequency of polls (up to 60000 ms) during periods of idle traffic. The default is 60000 ms.
Router(cfg-adap)# llc2 local-window <i>frame-count</i>	(Optional) Specifies the maximum number of I-frames to send (up to 127) before waiting for an acknowledgment. The default is 7.
Router(cfg-adap)# llc2 recv-window <i>frame-count</i>	(Optional) Controls the number of frames in the receive window. The default is 7.
Router(cfg-adap)# llc2 t1-time <i>milliseconds</i>	(Optional) Specifies the amount of time to wait (up to 60000 ms) for an acknowledgment to send I-frames. The default is 1000 ms.
Router(cfg-adap)# llc2 tbusy-time <i>milliseconds</i>	(Optional) Specifies the amount of time to wait (up to 60000 ms) while the other LLC2 station is in a busy state before attempting to poll the remote station. The default is 9600 ms.
Router(cfg-adap)# llc2 tpf-time <i>milliseconds</i>	(Optional) Specifies the amount of time to wait (up to 60000 ms) for a final response to a poll frame before resending the original poll frame. The default is 1000 ms.
Router(cfg-adap)# llc2 trej-time <i>milliseconds</i>	(Optional) Specifies the amount of time to wait (up to 60000 ms) for resending a rejected frame before sending the reject command. The default is 3200 ms.

Configuring the Source Bridge

Source-route bridging (SRB) is required to get packets from the LANs that are external to the CMCC adapter, to the internal LAN on the CIP or CPA and the CMPC feature. The **source-bridge** command identifies the interfaces in the same ring group. Frames are sent only to interfaces in the same ring group.

When you configure the source bridge, you can assign the following types of priorities:

- **LOCADDR priority**—Allows you to map LUs to queuing priorities for the internal LAN by specifying a defined LOCADDR priority using the **locaddr-priority** command. The LOCADDR priorities are defined using the **locaddr-priority-list** command in global configuration mode.
- **SAP priority**—Allows you to assign priorities for the internal LAN according to the service access point and MAC address in an LLC2 session by specifying a defined SAP priority using the **sap-priority** command. The SAP priorities are defined using the **sap-priority-list** command in global configuration mode.

To configure the bridging characteristics for the internal LAN use the following commands in internal LAN configuration mode:

Command	Purpose
Step 1 Router(cfg-lan)# source-bridge <i>source-ring-number bridge-number</i> <i>target-ring-number</i>	Configures source-route bridging for the selected internal LAN interface with the following arguments: <ul style="list-style-type: none"> • <i>source-ring-number</i>—Number for the Token Ring on the internal LAN for the CIP or CPA. • <i>bridge-number</i>—Bridge number connecting the source and target Token Rings. • <i>target-ring-number</i>—Number of the destination ring number on the router. The target ring can also be a ring group.
Step 2 Router(cfg-lan)# locaddr-priority <i>list-number</i>	(Optional) Assigns a LOCADDR priority for the internal LAN, where <i>list-number</i> is a value defined from the locaddr-priority-list command.
Step 3 Router(cfg-lan)# sap-priority <i>list-number</i>	(Optional) Assigns a SAP priority for the internal LAN, where <i>list-number</i> is a value defined from the sap-priority-list command.

Use the **no source-bridge** command to disable source-route bridging.

Enabling the Router Configuration

After you complete the tasks to configure CMPC on the router, be sure that you enable the configuration using the **no shut** command on all of the applicable interfaces. For the CIP, this means that you need to run the **no shut** command on the selected physical interface, and again for the virtual interface.

For the CPA, you only need to run the **no shut** command on the physical interface.

To enable the router configuration for CMPC, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface channel slot/port	Selects the interface. The <i>port</i> value differs by the type of CMCC adapter: <ul style="list-style-type: none"> • CIP—<i>port</i> value corresponds to 0 or 1 for the physical interface, and 2 for the virtual interface. • CPA—<i>port</i> value corresponds to port 0.
Step 2	Router(config-if)# no shut	Restarts the selected interface.

Correlating the Mainframe and Router Configuration Elements

Table 2 shows a summary of the configuration elements on the router and host that must be correlated for proper operation of CMPC. The column labeled “Configuration Element” identifies the type of entity to be configured. The columns labeled “Router Configuration” and “Mainframe Configuration” identify the related parameters on the router and the mainframe whose values must be compatible or match.

Table 2 Relationship of Router and Mainframe Configuration Elements for CMPC

Configuration Element	Router Configuration	Mainframe Configuration
Subchannels	<i>path</i> and <i>device</i> arguments of the cmpc command	RESOURCE PARTITION, CHPID, and CNTLUNIT statements of the IOCP definition defining the following parameters for the CMPC channel path: <ul style="list-style-type: none"> • LPAR number (if defined) in the RESOURCE PARTITION and CHPID statements—Specify in the 3rd digit of the <i>path</i> argument in the router cmpc command. • CUADD value (if defined) in the CNTLUNIT statement—Specify in the 4th digit of the <i>path</i> argument in the router cmpc command. • Available device address in the UNITADD parameter of the CNTLUNIT statement—Specify in the <i>device</i> argument of the router cmpc command.
Read/write subchannels	<i>device</i> argument for the cmpc read command <i>device</i> argument for the cmpc write command	Subchannel for the READ parameter of the TRL major node. Subchannel for the WRITE parameter of the TRL major node.

CMPC Verification Configuration Task List

Configuring CMPC includes tasks for both the mainframe and the router. This section describes the steps to verify that you have successfully configured CMPC with the TN3270 server on a CIP. It provides procedures to verify connectivity from the router perspective and from the host perspective, and includes troubleshooting tips as a guide when the configuration verification fails.

This section includes the following topics:

- [Initial Host and Router Configuration, page 30](#)
- [Verifying CMPC Channel Connectivity, page 32](#)
- [Verifying Communication with VTAM, page 34](#)

Initial Host and Router Configuration

Consider that you begin verification with the following configurations on the host and router:

- [TRL Major Node Definition, page 30](#)
- [Local SNA Major Node Definition, page 30](#)
- [Switched Major Node Definition, page 30](#)
- [LUGROUP Major Node Definition, page 31](#)
- [Router Configuration for Internal LAN on a CIP with TN3270 Server, page 31](#)



Note

The verification procedures assume that the VTAM major nodes are defined, but not yet activated.

TRL Major Node Definition

```
JECTR LG VBUILD TYPE=TRL
JC TR LG70 TRLE LNCTL=MPC, X
          MAXBF RU=16, X
          REPLYTO=25.5, X
          MPCLEVEL=NOHPDT, X
          READ=(270), X
          WRITE=(271) X
```

Local SNA Major Node Definition

```
JECLNA VBUILD TYPE=LOCAL
JECPU70 PU TRLE=JC TR LG70, X
        ISTATUS=ACTIVE, X
        XID=YES, X
        CONNTYPE=APPN, X
        CPCP=YES, X
        HPR=YES
```

Switched Major Node Definition

```
SWTNPAN VBUILD TYPE=SWNET,MAXDLUR=4
PANTNPU PU ADDR=01, X
        PUTYPE=2, X
        IDBLK=415, X
        IDNUM=AAAAA, X
        LUGROUP=DDDJECLU, X
        LUSEED=TNPAN###, X
        ISTATUS=ACTIVE, X
```

```

MAXDATA=4096,
MAXPATH=1

```

X

LUGROUP Major Node Definition

```

LUJEC  VBUILD TYPE=LUGROUP
DDDJEC  LUGROUP
DYNAMIC LU DLOGMOD=D4C32XX3,
           MODETAB=ISTINCLM,
           USSTAB=USSL3270,
           SSCPFM=USS3270
@      LU DLOGMOD=D4C32784,
           MODETAB=ISTINCLM,
           USSTAB=USSL3270,
           SSCPFM=USS3270

```

X
X
X
X
X
X

Router Configuration for Internal LAN on a CIP with TN3270 Server

```

interface channel 2/1
no ip address
no ip directed-broadcast
no keepalive
!
interface channel 2/2
ip address 172.18.20.49 255.255.255.248
no ip redirects
no ip directed-broadcast
no keepalive
lan Token Ring 6
source-bridge 106 1 400
adapter 6 4000.8001.0106
lan Token Ring 7
source-bridge 107 1 400
adapter 7 4000.8001.0107
tn3270-server
dlur NETA.PANTN32 NETA.MVSG
lsap token-adapter 6 04
link HOST2 rmac 4000.8001.0107
pu PANTNPU 415AAAAA 172.18.20.58

```



Note

The initial router configuration shows the internal LAN, source-bridge, and internal adapter configuration in preparation for configuration of CMPC.

Verifying CMPC Channel Connectivity

If you have defined the channel paths for the router at the mainframe host in the IOCP or HCD, you can begin to configure the router for CMPC support and verify connectivity at the channel level first. Isolating this level of verification is useful when the VTAM configuration is not completed, but you want to establish that the router can successfully communicate with the host.

Verifying channel connectivity confirms the following aspects of the router configuration:

- Microcode is loaded on the CMCC
- CMCC adapter is functional
- CMCC can communicate with the host over the channel path

Verifying CMPC Channel Connectivity from the Router

The steps in this section show how to verify the CMPC channel configuration beginning with running the **cmpr** command on the router's physical interface. The following assumptions are made for the procedure described in this section:

- The router's virtual interface is already configured with the required internal LAN, source-bridge, and internal adapter statements as shown in the initial router configuration for a CIP shown in [Figure 1](#).
- The router has the recommended CMCC hardware and microcode versions to support the CMPC feature. You can use the **show version**, **show controllers cbus**, and **show controllers channel** commands to verify the Cisco IOS software and CMCC microcode versions.



Note

Before you begin on the router, run the **debug channel events** command so that you can verify the messages on the router console.

To verify CMPC channel connectivity, perform the following steps:

- Step 1** From the router, configure the **cmpr** commands on the physical interface according to your site's requirements as shown in the following example:

```
interface channel 2/1
cmpr C190 70 MVSG-TN READ
cmpr C190 71 MVSG-TN WRITE
```

Confirm that you receive messages stating "Device Initialized," similar to the following displays:

```
PA1 MPC C190-70 Device initialized
PA1 MPC C190-71 Device initialized
```

- Step 2** Configure the CMPC TG according to your site's requirements as shown in the following example:

```
interface channel 2/2
tg MVSG-TN llc token-adapter 7 04 rmac 4000.8001.0106
```

Confirm that you receive a message stating that the CMPC TG is "Initialized," similar to the following display:

```
CMPC-TG MVSG-TN initialized
```

- Step 3** To verify that the channel is up and the line protocol is up, go to EXEC command mode and run the **show interfaces channel** command as shown in the following example:


```
show interfaces channel 2/1
```

- Step 4** To verify that the physical channel is up, run the **show extended channel statistics** command as shown in the following example:

```
show extended channel 2/1 statistics
```

Verify that the path field in the output for the CMPC devices shows “ESTABLISHED,” which means that the physical channel is up.

- Step 5** If your **show** command output matches the values described in [Step 3](#) and [Step 4](#), then the channel connection between the mainframe and the router is established. If you cannot confirm the values, see the [“Troubleshooting Tips for Channel Connectivity”](#) section on page 34.
-

Verifying CMPC Channel Connectivity from the Host

After CMPC has been configured on the router, you can also verify channel connectivity from the host by performing the following steps:

- Step 1** From the host, verify that the devices are online using the following sample command to display the device 270 for a range of two (or 270-271):

```
d u,,,270,2
```

- Step 2** If the devices are offline, then vary the devices online according to your site’s configuration as shown in the following sample commands:

```
v 270,online  
v 271,online
```



Note The CHPID for the device should already be active on the host.

- Step 3** If the devices come online, then the channel connection between the mainframe and the router is established. If the device does not come online, or you receive the message “No paths physically available,” see the [“Troubleshooting Tips for Channel Connectivity”](#) section on page 34.
-

Troubleshooting Tips for Channel Connectivity

There are several indicators on the router and the mainframe that indicate that the channel connection is not available.

- From the router, you might see the following things:
 - The output from the **show interfaces channel** command shows that the channel or line protocol is down.
 - The output from the **show interface channel statistics** command shows that the path is not established (the physical channel is not up).
- From the host, you might see the following things:
 - The device is not online.
 - When you vary the device online, you receive the message “No paths physically available.”

Recommended Actions

If you determine that the channel connection is not available, review the following tasks to be sure that you have performed them correctly:

- Be sure that you enabled the CMPC router configuration using the **no shut** command to restart the interface. If you configured both the physical and virtual interface on a CIP, be sure to run the **no shut** command on both interfaces.
- Be sure that the CMPC devices (and paths) are online at the host.
- Verify that the *path* and *device* arguments that you specified in your **cmpc** configuration command correlate properly to the host IOCP or HCD configuration.

If none of these recommended actions allow you to establish the channel connection, check your CMCC LED indicators and the physical channel connection.

Verifying Communication with VTAM

After all of the VTAM major node definitions are installed, you can verify communication between the router and VTAM using CMPC. You can also verify a session from a TN3270 client network device to the host.

This section includes the following verification procedures:

- [Verifying Communication with VTAM from the Host, page 35](#)
- [Verifying Communication with VTAM from the Router, page 36](#)

Verifying Communication with VTAM from the Host

This procedure describes how to verify from the host that all of the VTAM major node definitions are configured and activated.

To verify communication with VTAM using CMPC, perform the following steps:

Step 1 From the host, activate the switched major node using the following sample command:

```
v net,act,id=SWTNPAN
```

Verify that you receive the following console messages:

```
IST097I VARY ACCEPTED
IST093I PANTNPU ACTIVE
IST093I SWTNPAN ACTIVE
```

Step 2 Activate the LUGROUP major node using the following sample command:

```
v net,act,id=DDDJEC
```

Verify that you receive the following console messages:

```
IST097I VARY ACCEPTED
IST093I DDDJEC ACTIVE
```

Step 3 Activate the TRLE using the following sample command:

```
v net,act,id=JCTRLG70,update=add
```

Verify that you receive the following console messages:

```
IST097I VARY ACCEPTED
IST093I ISTTRL ACTIVE
```

Step 4 Display the TRLE status using the command:

```
d net,trl
```

Verify that the TRLE is present but not active, as shown in the following console message:

```
IST1314I TRLE=JCTRLG70 STATUS=INACT CONTROL=MPC
```



Note If the local SNA major node is activated before the TRLE, the TRLE will be active.

Step 5 Activate the local SNA major node using the following sample command:

```
v net,act,id=JCLS270
```

Verify that you receive the following console messages:

```
IST097I VARY ACCEPTED
IST093I JCLS270 ACTIVE
IEF196I IEF237I 0271 ALLOCATED TO TP0271
IEF196I IEF237I 0270 ALLOCATED TO TP0270
IST1086I APPN CONNECTION FOR NETA.PANTN32 IS ACTIVE - TGN = 165
IST093I JECPU70 ACTIVE
IST1096I CP-CP SESSIONS WITH NETA.PANTN32 ACTIVATED
```

Verifying Communication with VTAM from the Router

This procedure describes how to verify communication with the VTAM TRL and local SNA major nodes for CMPC from the router.

To verify communication with VTAM from the router, perform the following steps:

Step 1 Run the **show extended channel statistics** command as shown in the following example:

```
show extended channel 2/1 statistics
```

Verify that the following is displayed in these fields of the output for the CMPC devices:

- Path—The CMPC path is “ESTABLISHED,” which means that the physical channel is up.
- Con—The connection value is “Y,” which means that the subchannel is up and the CMPC connection is established between the router and the mainframe.

Step 2 To verify that the CMPC subchannels are active, run the **show extended channel cmpc** command as shown in the following example:

```
show extended channel 2/0 cmpc
```

Step 3 To verify the operational status and configuration of the CMPC TGs, run the **show extended channel tg** command as shown in the following example:

```
show extended channel 2/2 tg detailed MVSG-TN
```

For information about other commands that are useful when diagnosing or monitoring your CMPC connection, see the [“Monitoring and Maintaining CSNA and CMPC” section on page 38](#).

Troubleshooting Tips for VTAM

This section describes recommended actions for the following problems that might occur during verification of communication with VTAM.

- When you activate the local SNA major node, you receive the following messages:

```
IST259I INOP RECEIVED FOR JECPU70 CODE=01
IST619I ID = JECPU70 FAILED - RECOVERY IN PROGRESS
IST129I UNRECOVERABLE OR FORCED ERROR ON NODE JECPU70 - VARY INACT SCHED
IST105I JECPU70 NODE NOW INACTIVE
```

Recommended Actions

- Be sure that the CMPC devices (and paths) are online at the host.
- Verify that the *path* and *device* arguments that you specified in your **cmpc** configuration commands correlate properly to the host IOCP or HCD configuration and to the TRL major node.
- The local SNA major node activates and the subchannels are allocated, but you receive a message similar to the following display on the router console:

```
MPC-6-NODE_NOT_ACTIVE: Host attempted activation of MVSG-TN but TG not configured
```

Recommended Actions

- Verify that the TG is defined on the router.
- Verify that you specified the same TG name in the **tg** (CMPC) command and in each of the **cmpc** commands.
- When you activate the local SNA major node, you receive the following messages at the host:

```
IST097I VARY ACCEPTED
IST093I JCLS270 ACTIVE
IEF196I IEF237I 0271 ALLOCATED TO TP0271
IEF196I IEF237I 0270 ALLOCATED TO TP0270
IST222I READ DEVICE 0271 IS INOPERATIVE, NAME ISJCTRLG70 446
IST1578I DEVICE INOP DETECTED FOR JCTRLG70 BY ISTTSCXI CODE = 200
IST314I END
IST1222I WRITE DEVICE 0270 IS INOPERATIVE, NNAME IS JCTRLG70 447
IST1578I DEVICE INOP DETECTED FOR JCTRLG70 BY ISTTSCXI CODE = 200
IST314I END
IST1578I SOFT INOP DETECTED FOR JCTRLG70 BY ISTTSC8X CODE = 007
IST259I INOP RECEIVED FOR JECPU70 CODE = 01
IST619I ID = JECPU70 FAILED - RECOVERY IN PROGRESS
IST129I UNRECOVERABLE OR FORCED ERROR ON NODE JECPU70 - VARY INACT SCHED
IST105I JECPU70 NODE NOW INACTIVE
```

In addition, you receive messages similar to the following display on the router console:

```
MPC-6-BAD_DIRECTION:PA1 MPC C190-70 configured for READ
MPC-6-BAD_DIRECTION:PA1 MPC C190-71 configured for WRITE
```

Recommended Action

Verify that the direction (read versus write) that you specified for the subchannel in the TRLE matches the direction that you specified in the **cmpc** commands. So, the host READ subchannel matches the **cmpc read** device and the host WRITE subchannel matches the **cmpc write** device.

Monitoring and Maintaining CSNA and CMPC

The following topics in this section provide information about the different commands that you can use to monitor and maintain the CMCC interfaces that are configured for CSNA and CMPC:

- [Monitoring Interface Status, page 38](#)
- [Clearing Counters for CSNA and CMPC, page 39](#)

Monitoring Interface Status

To monitor CMCC adapter interface status, you can display information about the interface, including the version of the software and the hardware, the controller status, and statistics about the interfaces. In addition, you can display information about feature-related statistics on the CMCC adapter. This section lists some additional commands that are useful when monitoring CMCC adapter interfaces that are configured for CSNA and CMPC.

For a complete list of the **show** commands that are related to monitoring CMCC adapter interfaces, see the “Configuring Cisco Mainframe Channel Connection Adapters” chapter in this publication. To display the full list of **show** commands, enter **show ?** at the EXEC prompt.

To display information related to CSNA and CMPC configurations, use the following commands in EXEC mode:

Command	Purpose
Router# show extended channel slot/port csna [admin oper stats] [path [device]]	Displays information about the CSNA subchannels configured on the specified CMCC adapter interface.
Router# show extended channel slot/port cmpc [path [device]]	Displays information about each CMPC (and CMPC+) subchannel configured on the specified CMCC adapter interface.
Router# show extended channel slot/port tg [oper stats] [detailed] [tg-name]	Displays configuration, operational, and statistics information for CMPC (and CMPC+) TGs configured on a specified CMCC adapter internal LAN interface.
Router# show extended channel slot/port connection-map llc2	Displays the number of active LLC2 connections for each SAP and the mapping of the internal MAC adapter and the SAP to the resource that activated the SAP.
Router# show extended channel slot/port llc2 [admin oper stats] [lmac [lsap [rmac [rsap]]]]	Displays information about the LLC2 sessions running on the CMCC adapter interfaces.
Router# show extended channel slot/port max-llc2-sessions	Displays information about the number of LLC2 sessions supported on the CMCC adapter.

Clearing Counters for CSNA and CMPC

You can reset the statistics counters that are displayed in the output of the **show extended channel** commands. You can reset the counters associated with an interface or a particular feature on the interface. If you are monitoring a particular threshold or statistic for CSNA or CMPC and need to reset a related counter, you can clear all those counters related to the feature.

For information about clearing other counters on the CMCC adapter interface, see the “Configuring Cisco Mainframe Channel Connection Adapters” chapter in this publication.

To clear the counters associated with CSNA and CMPC on the CMCC adapters, use the following commands in privileged EXEC mode:

Command	Purpose
<pre>router# clear extended counters channel slot/port csna</pre>	<p>Clears counters for statistics associated with the CSNA feature on the specified <i>slot/port</i>. The port value differs by the type of CMCC adapter:</p> <ul style="list-style-type: none"> • CIP—<i>port</i> value corresponds to the physical interface, which is port 0 or 1. • CPA—<i>port</i> value corresponds to the physical interface, which is port 0.
<pre>router# clear extended counters channel slot/port tg</pre>	<p>Clears counters for statistics associated with TGs in the CMPC (and CMPC+) features on the specified <i>slot/port</i>. The port value differs by the type of CMCC adapter:</p> <ul style="list-style-type: none"> • CIP—<i>port</i> value corresponds to the virtual interface, which is port 2. • CPA—<i>port</i> value corresponds to the physical interface, which is port 0.
<pre>router# clear extended counters channel slot/port llc2</pre>	<p>Clears counters for LLC2 statistics on the specified <i>slot/port</i>. The port value differs by the type of CMCC adapter.</p> <ul style="list-style-type: none"> • CIP—<i>port</i> value corresponds to the virtual interface, which is port 2. • CPA—<i>port</i> value corresponds to the physical interface, which is port 0.



Note

These commands will not clear counters retrieved using Simple Network Management Protocol (SNMP), but only those seen with the EXEC **show extended channel** commands.

CSNA and CMPC Configuration Examples

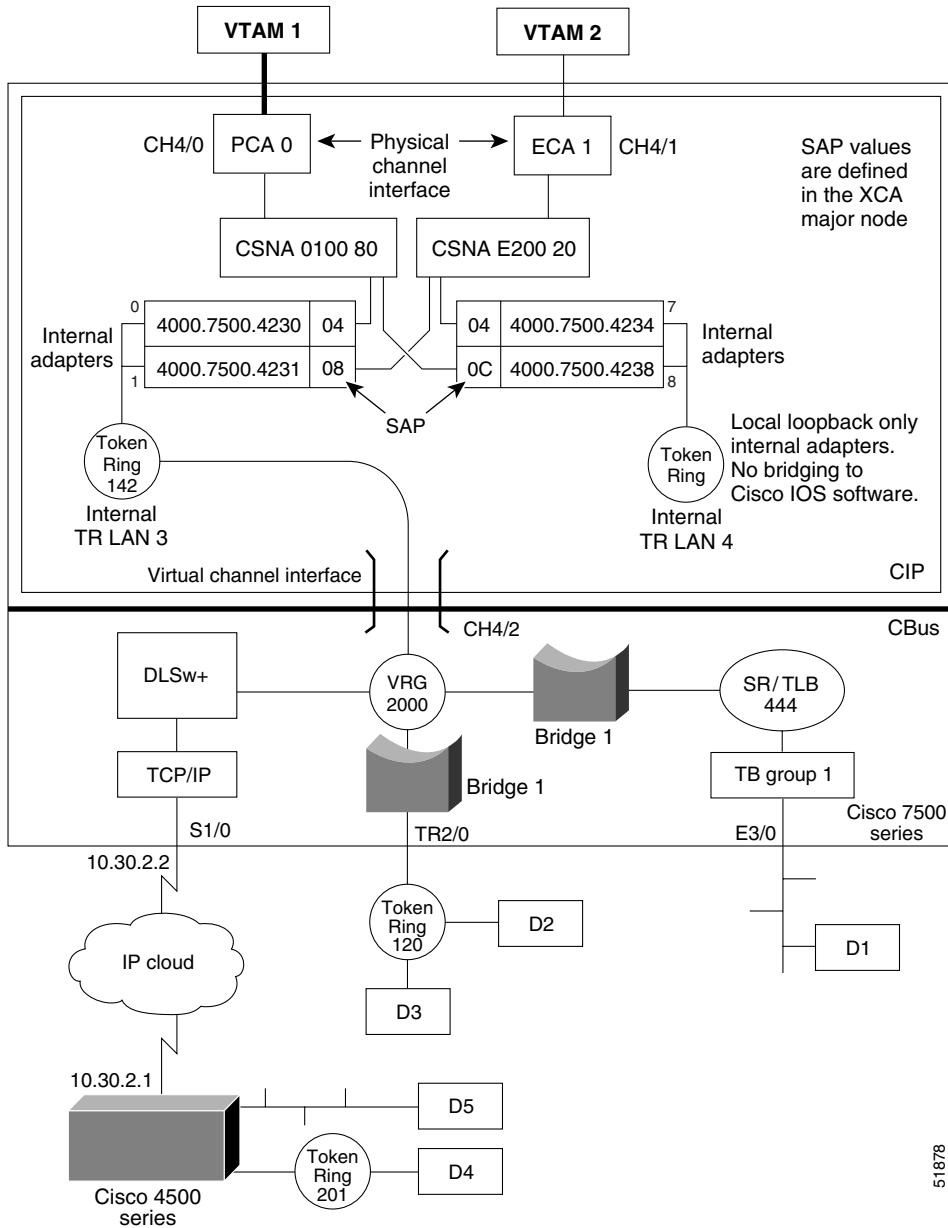
The configuration examples in this section are organized by the following categories:

- [CSNA Configuration on a CIP Example, page 39](#)
- [CSNA Configuration on an ECPA Example, page 41](#)
- [CMPC Configuration Examples, page 43](#)

CSNA Configuration on a CIP Example

[Figure 2](#) illustrates an example of configuring CSNA on a Cisco 7500 router with a CIP.

Figure 2 CIP CSNA Source-Route Translational Bridging Configuration



51878

```

source-bridge ring-group 2000
source-bridge transparent 2000 444 1 1
dlsw remote-peer 0 tcp 10.30.2.1
dlsw local-peer peer-id 10.30.2.2
!
interface serial 1/0
ip address 10.30.2.2 255.255.255.128
clockrate 56000
!
interface tokenring 2/0
mac-address 4000.7500.0200
no ip address
ring-speed 16
source-bridge 120 1 2000
source-bridge spanning
    
```

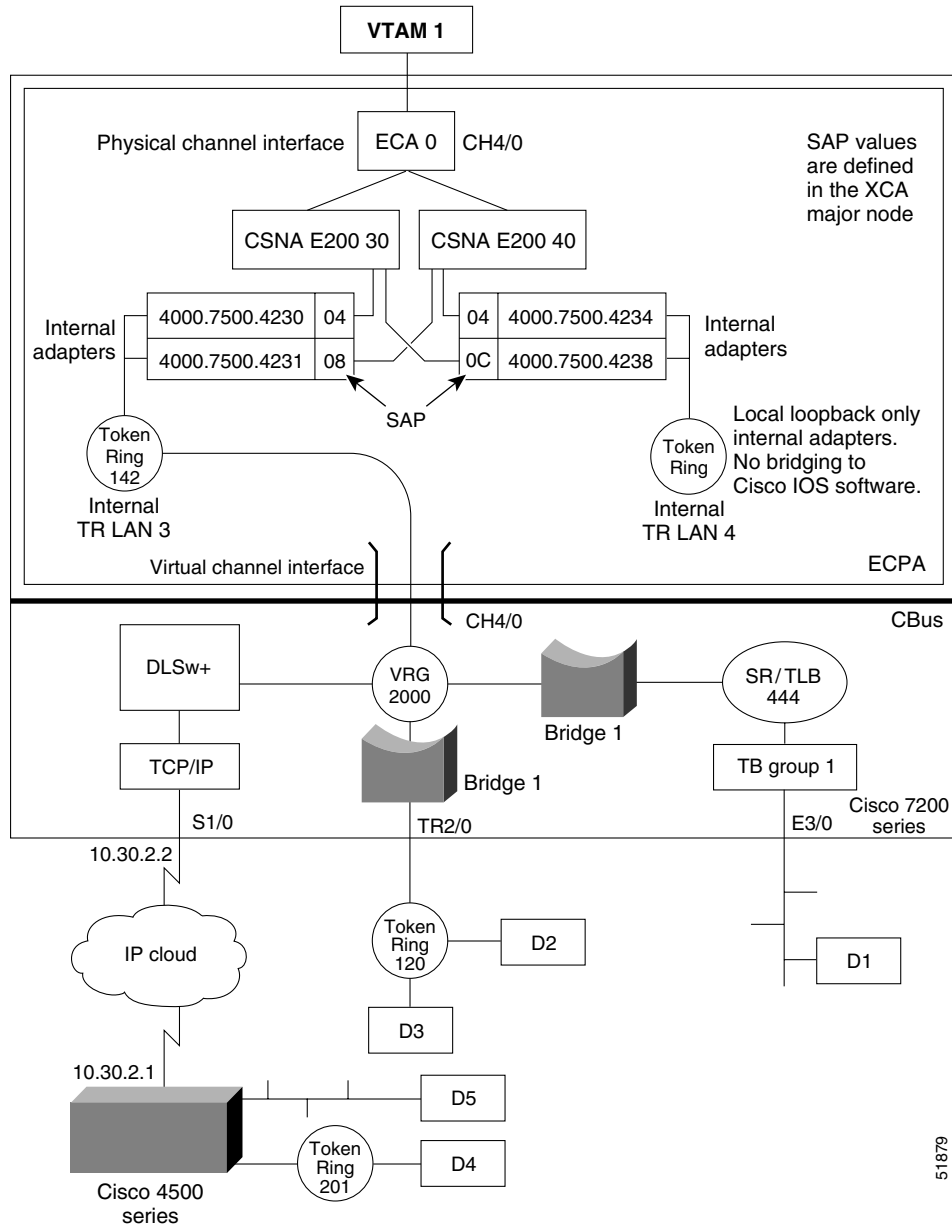


```
!  
interface ethernet 3/0  
  mac-address 0200.ae00.c000  
  no ip address  
  bridge-group 1  
!  
interface channel 4/0  
  no ip address  
  no ip directed-broadcast  
  no keepalive  
  csna 0100 80  
!  
interface channel 4/1  
  no ip address  
  no ip directed-broadcast  
  no keepalive  
  csna E200 20 maxpiu 65535 time-delay 100  
!  
interface channel 4/2  
  no ip address  
  no ip directed-broadcast  
  no keepalive  
  max-llc2-sessions 2500  
  lan TokenRing 3  
    source-bridge 142 1 2000  
    adapter 0 4000.7500.4230  
      llc2 local-window 1  
      llc2 ack-max 1  
    adapter 1 4000.7500.4231  
  lan TokenRing 4  
    adapter 7 4000.7500.4234  
    adapter 8 4000.7500.4238  
!  
bridge 1 protocol ieee
```

CSNA Configuration on an ECPA Example

The following configuration is an example of configuring CSNA on a Cisco 7200 router with a ECPA. [Figure 3](#) illustrates this configuration example.

Figure 3 ECPA CSNA Source-Route Translational Bridging Configuration



51879

```

source-bridge ring-group 2000
source-bridge transparent 2000 444 1 1
dlsw remote-peer 0 tcp 10.30.3.1
dlsw local-peer peer-id 10.30.2.2
!
interface serial 1/0
ip address 10.30.2.2 255.255.255.128
clockrate 56000
!
interface tokenring 2/0
mac-address 4000.7500.0200
no ip address
ring-speed 16
source-bridge 120 1 2000
source-bridge spanning
    
```

```
!  
interface ethernet 3/0  
  mac-address 0200.ae00.c000  
  no ip address  
  bridge-group 1  
!  
interface channel 4/0  
  no ip address  
  no ip directed-broadcast  
  no keepalive  
  csna E200 30 maxpiu 65535  
  csna E200 40 maxpiu 65535  
  max-llc2-sessions 2500  
  lan TokenRing 3  
    source-bridge 142 1 2000  
    adapter 0 4000.7500.4230  
      llc2 local-window 1  
      llc2 ack-max 1  
    adapter 1 4000.7500.4231  
  lan TokenRing 4  
    adapter 7 4000.7500.4234  
    adapter 8 4000.7500.4238  
!  
bridge 1 protocol ieee
```

CMPC Configuration Examples

This section provides sample configurations for the CMPC feature. Throughout these configuration samples, a Cisco 7500 router with an RSP is used to illustrate the configurations. The configurations also apply to a Cisco 7000 router with an RP or an RSP installed. All SAP values are written in hexadecimal form.

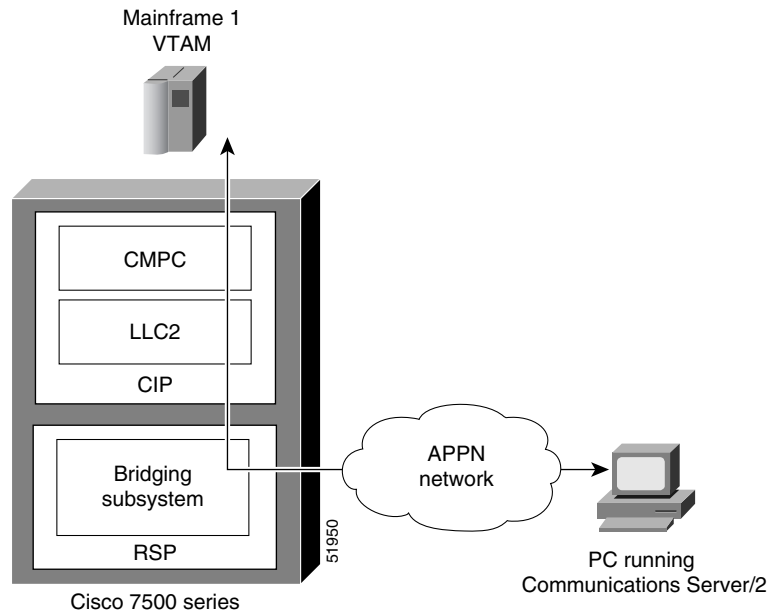
This sections includes the following configuration examples:

- [Connecting VTAM to a Remote PC with Communications Server/2 Using CMPC Example, page 44](#)
- [Connecting VTAM to SNA Switching Services \(SNASw\) on the RSP Using CMPC Example, page 46](#)
- [Connecting Two VTAM Nodes Using Two CIPs in the Same Router and CMPC Example, page 48](#)
- [Connecting VTAM to SNASw on a Remote Router with DLUR Using CMPC Example, page 52](#)

Connecting VTAM to a Remote PC with Communications Server/2 Using CMPC Example

Figure 4 shows the physical components for this example. Figure 5 shows the various parameters for each component in the configuration example.

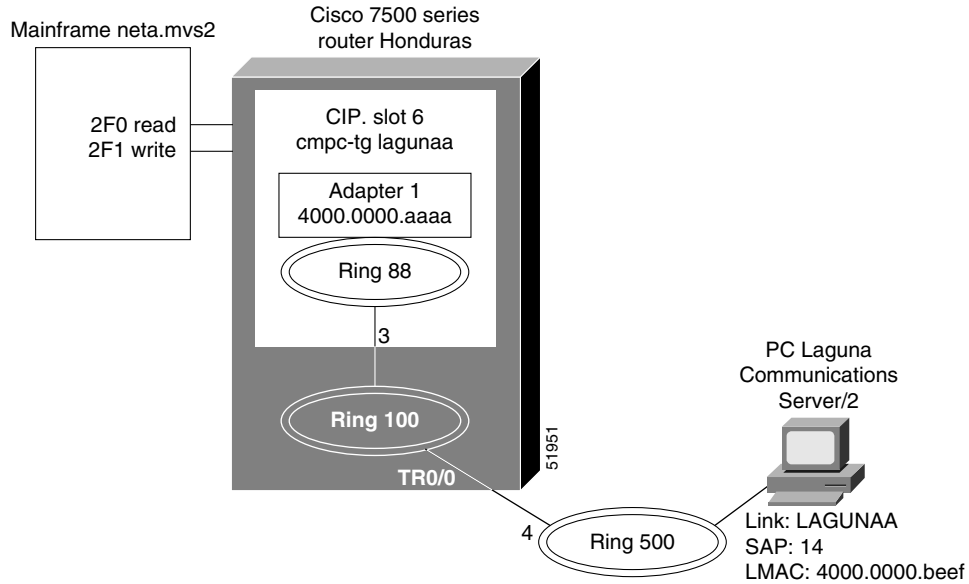
Figure 4 *Topology for VTAM-to-Remote PC with Communications Server/2*



In Figure 4, the following activity occurs:

- VTAM connects to the CMPC driver on the CIP.
- The CMPC driver converts the data to an LLC data stream and passes the data to the LLC2 stack on the CIP.
- The LLC2 stack on the CIP passes the data to the bridging code on the RSP.
- The bridging code on the RSP passes the data to the APPN network.

Figure 5 Parameters for VTAM-to-Remote PC with Communications Server/2



The example in [Figure 5](#) shows CMPC running on the CIP and communicating with a PC running Communications Server/2. APPN is not running on the router. It is only running in VTAM and on the PC.

The configuration examples for the VTAM host and the router follow.

TRL Node LAGTRLA on MVS2

```
LAGTRA  VBUILD TYPE=TRL
LAGTRLA  TRLE  LNCTL=MPC,MAXBFPU=8,REPLYTO=3.0,
          READ=(2F0),
          WRITE=(2F1)
```

Local Node LAGLNA on MVS2

```
LAGLNA  VBUILD TYPE=LOCAL
LAGPUA  PU    TRLE=LAGTRLA,
          ISTATUS=ACTIVE,
          XID=YES,CONNTYPE=APPN,CPCP=YES,HPR=YES
```

Configuration for Honduras Router

```
source-bridge ring-group 100
!
interface TokenRing0/0
 no ip address
 ring-speed 16
 source-bridge 500 4 100
!
interface Ethernet1/0
 ip address 172.18.3.24 255.255.255.0
!
interface Channel6/1
 no ip address
 no keepalive
 cmpc C020 F0 LAGUNAA READ
 cmpc C020 F1 LAGUNAA WRITE
!
```

```

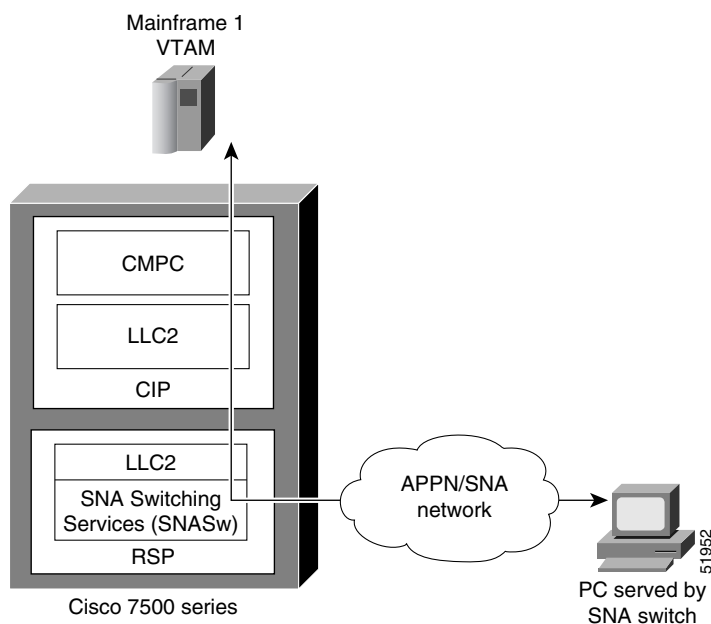
interface Channel16/2
no ip address
no keepalive
lan TokenRing 0
source-bridge 88 3 100
adapter 1 4000.aaaa.aaaa
tg LAGUNAA llc token-adapter 1 18 rmac 4000.0000.beef rsap 14

```

Connecting VTAM to SNA Switching Services (SNASw) on the RSP Using CMPC Example

Figure 6 shows the physical components for this example. Figure 7 shows the various parameters for each component in the configuration example.

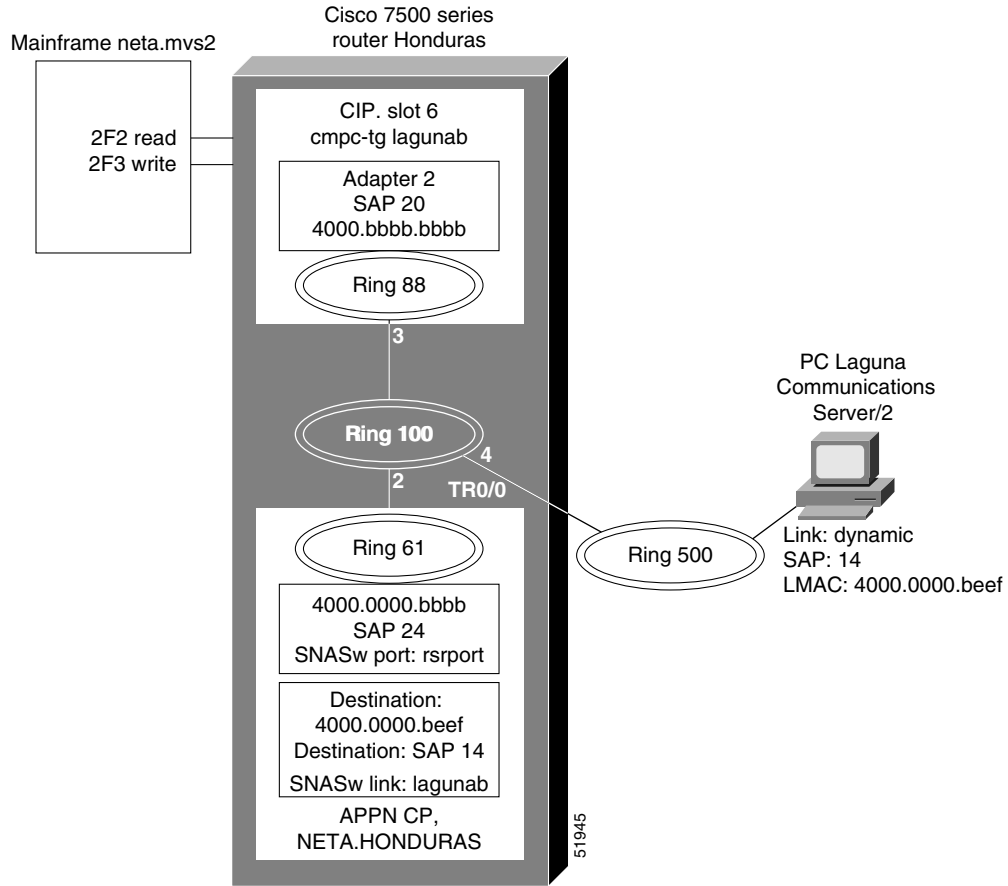
Figure 6 Topology for VTAM-to-SNASw Connection on the CIP



In Figure 7, the following activity occurs:

- VTAM connects to the CMPC driver on the CIP.
- The CMPC driver converts the data to an LLC data stream and passes the data to the LLC2 stack on the CIP.
- The LLC2 stack on the CIP passes the data to the LLC2 stack on the RSP.
- The LLC2 stack on the RSP passes the data to SNA Switching Services on the RSP.
- SNA Switching Services on the RSP sends the data to the APPN/SNA network.

Figure 7 Parameters for VTAM-to-SNASw Connection on the CIP



The configuration illustrated in Figure 7 is more complex because you must configure SNASw on the router. There are many different ways to configure SNASw. The example is a simple SNASw configuration in which SRB is used to connect the SNASw on the RSP to VTAM and the Token Ring attached PC.

It is possible to connect directly to the Token Ring port, which is not shown in the example.

Configuration for TRL Node LAGTRLB

```
LAGTRB  VBUILD TYPE=TRL
LAGTRLB TRLE LNCTL=MPC,MAXBFRU=8,REPLYTO=3.0, X
        READ=(2F2), X
        WRITE=(2F3)
```

Local SNA Major Node LAGLNB

```
LAGNNB  VBUILD TYPE=LOCAL
LAGPUB  PU TRLE=LAGTRLB, X
        ISTATUS=ACTIVE, X
        XID=YES,CONNTYPE=APPN,CPCP=YES
```

Honduras Router

```

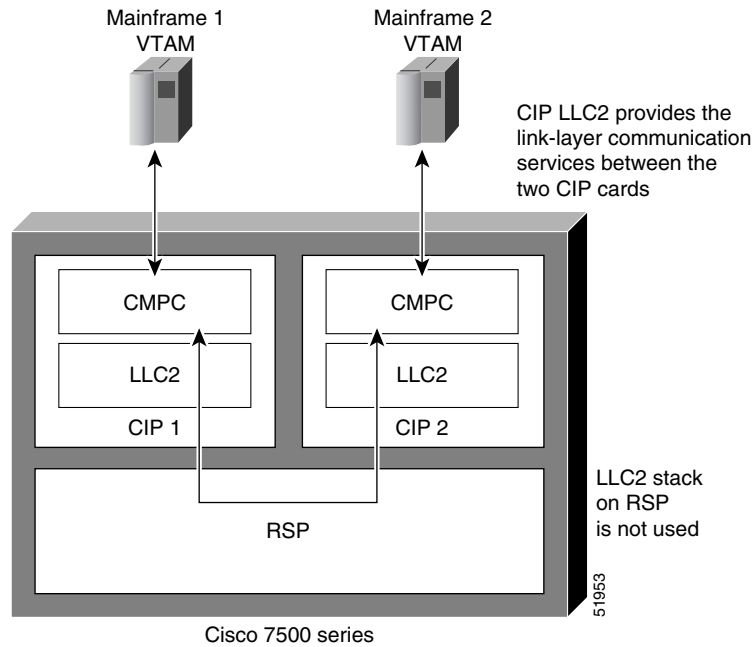
source-bridge ring-group 100
!
interface Channel6/1
  no ip address
  no keepalive
  cmpc C020 F2 LAGUNAB READ
  cmpc C020 F3 LAGUNAB WRITE
!
interface Channel6/2
  no ip address
  no keepalive
  lan TokenRing 0
    source-bridge 88 3 100
    adapter 2 4000.bbbb.bbbb
  lan TokenRing 2
    tg LAGUNAB 11c token-adapter 2 20 rmac 4000.0000.bbbb rsap 24
!
!
interface Virtual-TokenRing0
  mac-address 4000.0000.bbbb
  no ip address
  no ip directed-broadcast
  ring-speed 16
  source-bridge 61 2 100
!
snasw cpname NETA.HONDURAS
snasw port VTOK Virtual-TokenRing0
snasw link MVS2D port VTOK rmac 4000.bbbb.bbbb

```

Connecting Two VTAM Nodes Using Two CIPs in the Same Router and CMPC Example

[Figure 8](#) shows the physical components for this example. [Figure 9](#) shows the various parameters for each component in the configuration example.

Figure 8 **Topology for VTAM-to-VTAM Connection**



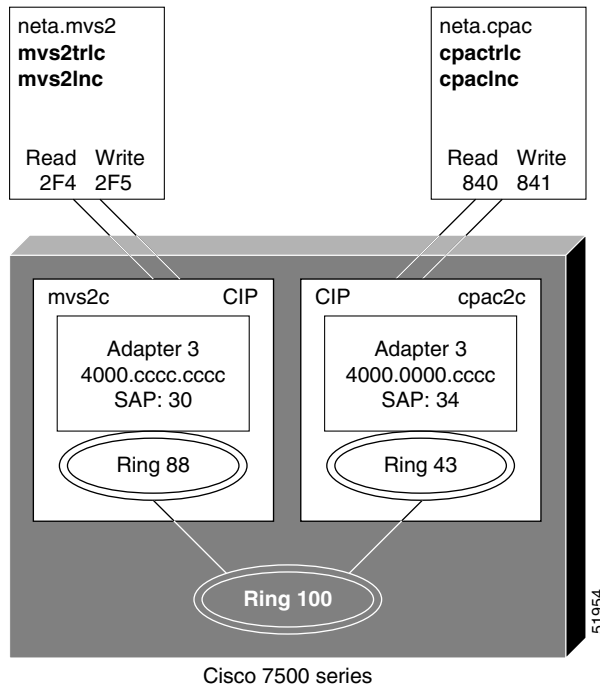
In [Figure 8](#), the following activity occurs:

- VTAM on Mainframe 1 passes MPC data to the CMPC driver on CIP 1.
- The CMPC driver on CIP 1 passes the data to the LLC2 stack.
- LLC2 sends the data to CIP 2 in the same router via IEEE 802.2.
- The LLC2 stack on CIP 2 passes the data to the CMPC driver on CIP 2, which passes the data to VTAM on Mainframe 2.

The CIPs could be in different routers or both VTAM connections could be to the same CIP.

Figure 9 shows parameters for VTAM-to-VTAM connection.

Figure 9 Parameters for VTAM-to-VTAM Connection



Differing solutions can be configured for the example shown in Figure 9. For example, you can have two CIPs in different routers connected via LLC2. You can also configure host connections going into the same CIP card rather than two separate CIP cards.

mvs2trlc

```
MVS2TRC  VBUILD  TYPE=TRL
MVS2TRLC TRLE  LNCTL=MPC, MAXBFPU=8, REPLYTO=3.0,      X
          READ= (2F4) ,                                X
          WRITE= (2F5)
```

mvs2lnc

```
MVS2NNC  VBUILD  TYPE=LOCAL
MVS2PUC  PU      TRLE=MVS2TRLC,                          X
          ISTATUS=ACTIVE,                                X
          XID=YES, CONNTYPE=APPN, CPCP=YES
```

cpactrlc

```
CPACTRC  VBUILD  TYPE=TRL
CPACTRLC TRLE  LNCTL=MPC, MAXBFPU=8, REPLYTO=3.0,      X
          READ= (840) ,                                X
          WRITE= (841)
```

cpacInc

```

CPACNNC  VBUILD TYPE=LOCAL
CPACPUC  PU      TRLE=CPACTRLC,           X
          ISTATUS=ACTIVE,                 X
          XID=YES, CONNTYPE=APPN, CPCP=YES

```

Router

```

source-bridge ring-group 100
!
interface Channel4/1
  no ip address
  no keepalive
  cmpc C010 40 CPACC READ
  cmpc C010 41 CPACC WRITE
!
interface Channel4/2
  no ip address
  no keepalive
  lan TokenRing 0
  source-bridge 43 5 100
  adapter 3 4000.0000.cccc
  tg CPACC llc token-adapter 3 34 rmac 4000.cccc.cccc rsap 30
!
interface Channel6/1
  no ip address
  no keepalive
  cmpc C020 F4 MVS2C READ
  cmpc C020 F5 MVS2C WRITE
!
interface Channel6/2
  lan TokenRing 0
  source-bridge 88 3 100
  adapter 3 4000.cccc.cccc
  tg MVS2C llc token-adapter 3 30 rmac 4000.0000.cccc rsap 34

```

Connecting VTAM to SNASw on a Remote Router with DLUR Using CMPC Example

Figure 10 shows the physical components for the DLUS-to-DLUR configuration. Figure 11 shows the various parameters for each component in the configuration example.

Figure 10 *Topology for VTAM-to-SNASw on a Remote Router with DLUR Connection*

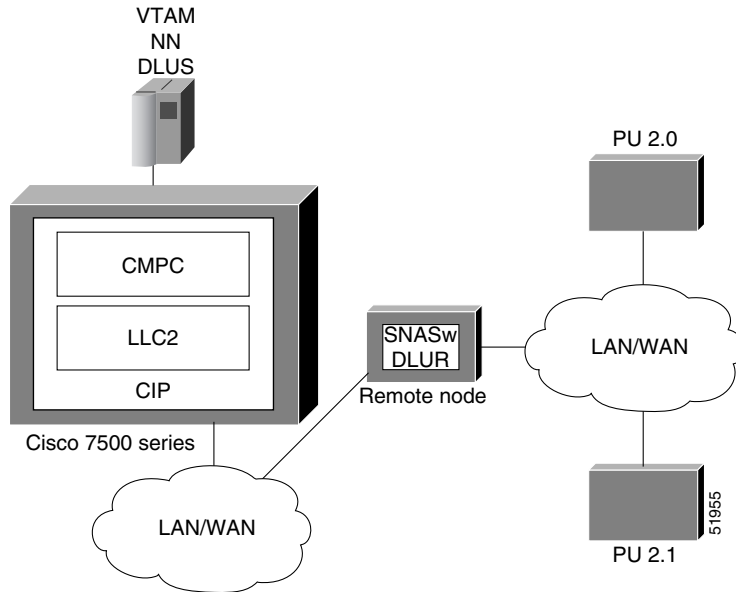
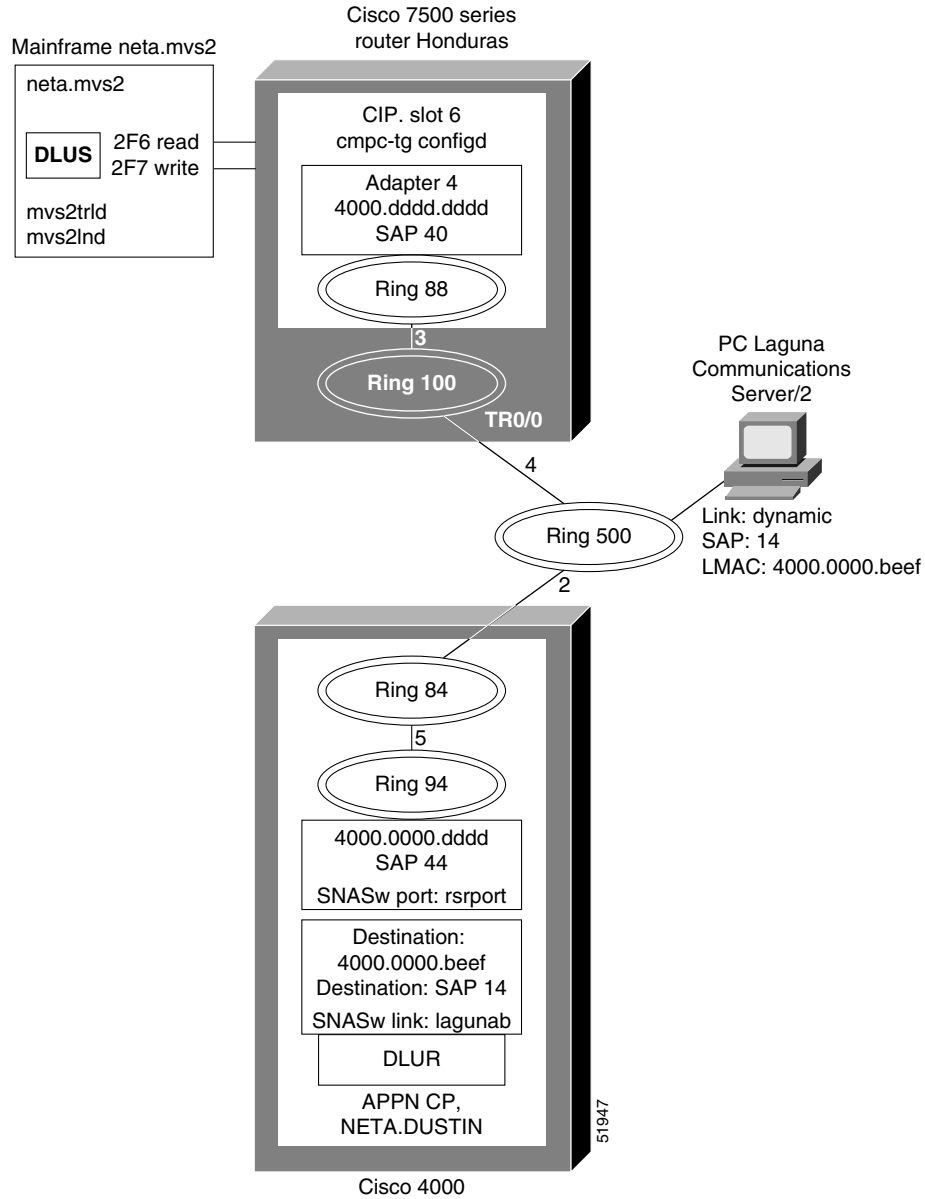


Figure 11 Parameters for VTAM-to-SNASw on a Remote Router with DLUR Connection



In the example shown in [Figure 11](#), DLUS is running on the MVS host. DLUR is running on a remote Cisco 4000 router. The connection from MPC to the APPN stack on the Cisco 4000 is via LLC2. There is no NN on the Cisco 7500. The PC is running Communications Server/2.

mvs2trld

```

MVS2TRD  VBUILD TYPE=TRL
MVS2TRLD TRLE  LNCTL=MPC, MAXBFRTU=8, REPLYTO=3.0,           X
                                     READ=(2F6),                X
                                     WRITE=(2F7)
    
```

mvs2lnd

```

MVS2NND  VBUILD TYPE=LOCAL
MVS2PUD  PU      TRLE=MVS2TRLD,           X
          ISTATUS=ACTIVE,                 X
          XID=YES, CONNTYPE=APPN, CPCP=YES

```

Additional Configuration for Router Honduras

```

interface Channel6/1
  cmpc C020 F6 CONFIGD WRITE
  cmpc C020 F7 CONFIGD READ
!
interface Channel6/2
  lan TokenRing 0
  source-bridge 88 3 100
  adapter 4 4000.dddd.dddd
  tg CONFIGD llc token-adapter 4 40 rmac 4000.0000.dddd rsap 44

```

Router Dustin

```

source-bridge ring-group 84
interface Ethernet0
  ip address 172.18.3.36 255.255.255.0
  media-type 10BaseT
!
interface TokenRing0
  no ip address
  ring-speed 16
  source-bridge 500 2 84
!
interface Virtual-TokenRing0
  mac-address 4000.0000.dddd
  no ip address
  no ip directed-broadcast
  ring-speed 16
  source-bridge 94 5 84
!
snasw cpname NETA.DUSTIN
snasw port VTOK Virtual-TokenRing0
snasw link MVS2D port VTOK rmac 4000.dddd.dddd

```

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.