

Configuring IBM Channel Attach

This chapter describes how to configure the Cisco 7000 with RSP7000 and Cisco 7500 series mainframe Channel Interface Processor (CIP), which supports the IBM channel attach feature.

For hardware technical descriptions and information about installing the router interfaces, refer to the hardware installation and maintenance publication for your product. For command descriptions and usage information, refer to the “IBM Channel Attach Commands” chapter of the *Bridging and IBM Networking Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Cisco’s Implementation of the IBM Channel Attach Interface

Support for IBM channel attach is provided on the Cisco 7000 with RSP7000 and Cisco 7500 series routers by the Channel Interface Processor (CIP) and an appropriate interface adapter card. With a CIP and the ESCON Channel Adapter (ECA) or bus-and-tag Parallel Channel Adapter (PCA), a Cisco 7000 with RSP7000 and Cisco 7500 series router can be directly connected to a mainframe, replacing the function of an IBM 3172 interconnect controller. This connectivity enables mainframe applications and peripheral access from LAN-based workstations.

A single CIP can support up to two channel adapter cards in any combination. Because of this flexibility, upgrading from parallel bus-and-tag to ESCON is simplified. The CIP can be configured for ESCON support by replacing a PCA with an ESCON adapter. Note that this upgrade procedure must be done by authorized service personnel.

The CIP provides support for the environments discussed in the following sections:

- TCP/IP Environments Using CLAW
- TCP/IP Offload Environments
- CIP SNA (CSNA) Environments
- TN3270 Server Environments under CSNA

TCP/IP Environments Using CLAW

TCP/IP mainframe protocol environments for IBM operating systems Multiple Virtual Storage (MVS) and Virtual Machine (VM) are supported. This support includes TCP/IP-based applications such as terminal emulation (Telnet), the File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) and Network File System (NFS), a distributed file access system. In addition, Internet Control Message Protocol (ICMP) and User Datagram Protocol (UDP) are supported.

A CIP configured with 8 megabytes (MB) of memory can support up to 128 CLAW connections, or 256 devices. Because each CLAW connection requires two devices, that allows a maximum of 128 CLAW connections per interface adapter card. However, a maximum of 32 CLAW connections is recommended.

TCP/IP Offload Environments

TCP/IP mainframe protocol environments for IBM operating systems MVS and VM are supported.

The CIP TCP/IP offload feature delivers the same function as the TCP/IP “offload” function on the 3172 Interconnect Controller (Model 3), but without the performance penalty. This feature implements the 3172 offload protocol for transporting application requests over the IBM ESCON or bus-and-tag channels.

All functionality provided in the CLAW environment is also supported in the TCP/IP offload environment because the function ships TCP/IP application calls over the mainframe channel using the CLAW channel protocol.

CIP SNA (CSNA) Environments

The CSNA feature provides support for SNA protocols over both ESCON and PCA interfaces to the IBM mainframe. As an IBM 3172 replacement, the CIP must support the External Communications Adapter (XCA) feature of VTAM, which allows VTAM to define Token Ring devices attached to the 3172 as switched devices.

In SNA environments, support for the XCA feature of VTAM allows the CIP to provide an alternative to front-end processors (FEPs) at sites where NCP is not required for SNA routing functions.

By providing CLS and the Logical Link Control, type 2 (LLC2) protocol stack on the CIP card, all frames destined to the CIP or from the CIP card can be fast switched by the router. The presentation of multiple “virtual” 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+), transparent bridging, SDLC-LLC2 translation (SDLLC), and Qualified Logical Link Control (QLLC) services.

Note In the implementation of CSNA, the multiple virtual LAN media types available are referred to as *internal LAN* types, because they exist as internal processes on the CIP card.

The CSNA feature supports the following communication through a Cisco 7000 with RSP7000 and Cisco 7500 series router:

- Communication between a channel-attached mainframe running VTAM and a LAN/WAN attached PU 2.0 SNA node
- Communication between a channel-attached mainframe running VTAM and a LAN/WAN attached PU 2.1 SNA node
- Communication between a channel-attached mainframe running VTAM and a LAN/WAN attached PU 5/4 SNA node
- Communication between two mainframes running VTAM channel-attached to the same CIP card or different CIP cards in a Cisco 7000 with RSP7000 and Cisco 7500 series router

The CSNA feature provides SNA connectivity through the use of MAC addresses configured for internal MAC adapters on the Cisco 7000 with RSP7000 and Cisco 7500 series router. These internal MAC adapters correspond to XCA major node definitions in VTAM, providing access points (LAN gateway) to VTAM for SNA network nodes. The internal MAC adapters are configured to exist on internal LANs located on a CIP card. Each CIP card can be configured with multiple internal LANs where an internal LAN can be a Token Ring, Ethernet, or FDDI LAN. Each internal Token Ring or FDDI LAN must be configured to participate in either source-route or transparent bridging and each internal Ethernet LAN must be configured for transparent bridging. Each internal Token Ring or FDDI LAN can be configured with up to 32 internal MAC adapters. An Ethernet internal LAN can support a single internal MAC adapter. The internal MAC adapter is an emulation of LAN adapters in an IBM 3172 interconnect controller.

TN3270 Server Environments under CSNA

The TN3270 server feature on a CIP card provides mapping between an SNA 3270 host and a TN3270 client connected to a TCP/IP network as shown in Figure 146. Functionally, it is useful to view the TN3270 server from two different perspectives: SNA functions and Telnet Server functions.

- SNA Functions

From the perspective of an SNA 3270 host connected to the CIP, the TN3270 server is an SNA device that supports multiple physical units (PUs), with each PU supporting up to 255 logical units (LUs). The LU can be Type 1, 2, or 3. The SNA host is unaware of the existence of the TCP/IP extension on the implementation of these LUs.

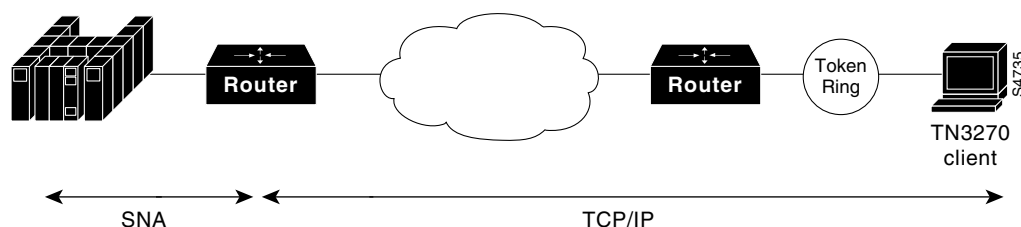
The LUs implemented by TN3270 server are dependent LUs. To route these dependent LU sessions to multiple virtual telecommunications access method (VTAM) hosts connected to the server in the CIP card, rather than routing in the VTAM hosts, the TN3270 server implements a SNA session switch with end node dependent LU requester (DLUR) function. Using the DLUR is optional so that the TN3270 server can be used with VTAM versions prior to version 4.2, which provide no APPN support.

SNA session switch allows you to eliminate SNA subarea routing between hosts of TN3270 traffic by establishing APPN links with the primary LU hosts directly.

- Telnet Server Functions

From the perspective of a TN3270 client, the TN3270 server is a Telnet server that can support approximately 8000 concurrent Telnet sessions. The server on the CIP card supports Telnet connection negotiation and data format as specified in RFC 1576 (referred to as “traditional TN3270”) and RFC 1647 (referred to as “TN3270E”).

Figure 146 TN3270 Implementation



Because the TN3270 server configuration is performed after an interface is configured for CSNA support, TN3270 configuration issues and tasks are addressed separately from the interface configuration tasks. The description of TN3270 configuration issues and tasks begins in the section “Configuring TN3270 on a Channel Interface Processor,” later in this chapter.

Note To enable the TN3270 server feature, you must have a CIP installed in a Cisco 7000 with RSP7000 or Cisco 7500 series router. The TN3270 server is very different from the TN3270 terminal emulation access feature described in the “Configuring Dial-In Terminal Services” chapter of the *Dial Solutions Configuration Guide*.

Interface Configuration Task List

You can perform the tasks in the following sections to configure and maintain IBM channel attach interfaces. In addition, several examples show how host configuration settings correlate to values used in the configuration commands.

Note After you select an interface to configure, you can configure that interface for the specific features you prefer: CLAW support, offload support, or CSNA support.

Not all tasks are required. Your CIP image may be preloaded. You must select an interface, after which you configure the features you want supported on that interface.

- Load the CIP Image
- Select the Interface
- Configure IBM Channel Attach for TCP/IP CLAW Support
- Configure IBM Channel Attach for TCP/IP Offload Support
- Configure IBM Channel Attach for CSNA Support
- Select Host System Parameters
- Monitor and Maintain the Interface

See the end of this chapter for “IBM Channel Attach Interface Configuration Examples.”

Note You can configure a CIP interface for any or all of the supported modes. If you want only CSNA support, for example, you need not configure TCP/IP support.

Because the TN3270 server configuration is performed after an interface is configured for CSNA support, TN3270 configuration issues and tasks are addressed separately from the interface configuration tasks. The of TN3270 configuration task list begins in the section “TN3270 Configuration Task List,” later in this chapter.

Load the CIP Image

Beginning with Cisco IOS Software Release 11.1, the CIP microcode (or CIP *image*) no longer is bundled with the Cisco IOS software. You must have Flash memory installed on the Route Processor (RP) card and 8 MB of RAM installed on your CIP card to use the IBM channel attach features in Cisco IOS Software Release 11.1 and later.

The CIP image is preloaded on Flash cards for all Cisco 7000 with RSP7000 and Cisco 7500 series routers ordered with the CIP option for Cisco IOS Software Release 11.1 and later. Perform the tasks in this section if you are upgrading the CIP image in your router.

To prepare the CIP, perform the following tasks beginning in privileged EXEC command mode:

Task	Command
Copy the CIP image from a server to the Flash memory. Use the appropriate command for your system. You must be running Cisco IOS Release 11.1 or later prior to executing a copy tftp command.	copy tftp flash <i>cipxxx-yy</i> (embedded Flash) copy tftp slot0: (Flash card) copy tftp slotn: (Flash card on 7500 series router) copy tftp bootflash: (onboard Flash on 7500 series router)
Configure your router to load the Flash image to the CIP:	
Step 1 Enter global configuration mode and specify that the CIP microcode load from a Flash card in router slot <i>n</i> or from embedded Flash.	configure microcode cip flash slotn: <i>cipxxx-yy</i> or microcode cip flash <i>cipxxx-yy</i>
Step 2 Load the image from Flash to the CIP card.	microcode reload
Exit configuration mode and display images loaded on the CIP card.	show controllers cbus

Rather than as a single image (named *cipxxx-yy*), the CIP image appears as a directory (*cipxxx-yy*) that contains the various image segments to be loaded into the CIP.

The router configuration process takes longer than when using features, because the initial loading of a CIP configuration feature results in the loading of the applicable code and includes any necessary processing.

Select the Interface

Before you configure your channel attach interface, you must select the interface. Perform the following task in global configuration mode:

Task	Command
Select the channel attach interface and enter interface configuration mode.	interface channel <i>slot/port</i>

You need not add a space between the interface type (**channel**) and the slot and port number. For example, you can specify **interface channel 3/0** or **interface channel3/0**.

Use the **show extended channel subchannel** EXEC command to display current CIP status. This command provides a report for each physical interface configured to support IBM channel attach.

The following section describes how to configure your channel attach interface.

See the section “IBM Channel Attach Interface Configuration Examples” at the end of this chapter for example configuration commands.

Configure IBM Channel Attach for TCP/IP CLAW Support

The following sections describe how to configure the IBM channel attach interface for TCP/IP CLAW support. All tasks, except for configuring other interface support, are required:

- Define the Routing Process
- Assign an IP Address
- Configure the IBM Channel Attach Interface
- Select a Data Rate for the Parallel Channel Adapter (PCA)
- Configure Other Interface Support

See the section “Select Host System Parameters” for guidelines on matching interface configuration values with host system values.

Define the Routing Process

You must configure the routing process that will be used by the Cisco IOS software. We recommend using the Enhanced IGRP routing process to perform IP routing on the IBM channel attach interface. Perform the following steps beginning in global configuration mode:

Task	Command
Step 1 Enter router configuration mode by selecting the routing process, preferably Enhanced IGRP, and the autonomous system the router belongs to.	router eigrp <i>process-id</i> or router igrp <i>process-id</i>
Step 2 Define the directly connected networks that are part of the autonomous system.	network <i>network-number</i>

Assign an IP Address

You must assign an IP address to the ECA or PCA interface so that it can communicate with other devices (or tasks) on the network. The IP address you assign to the interface must be in the same subnet as the hosts with which you wish to communicate. Perform the following task in interface configuration mode:

Task	Command
Assign an IP address and network mask to the selected interface.	ip address <i>address mask</i>

Configure the IBM Channel Attach Interface

You must define the devices, or tasks, supported on the interface. Some information you need to perform this task is derived from the following host system configuration files: MVSIOCP, IOCP, and the TCPIP configuration. Refer to the section “Select Host System Parameters” for guidelines on matching interface configuration values with host system values.

Perform the following task in interface configuration mode:

Task	Command
Define the CLAW parameters for this device.	claw <i>path device-address ip-address host-name device-name host-app device-app</i> [broadcast]

See the section “IBM Channel Attach Interface Configuration Examples” for samples of **claw** commands for different configurations.

Select a Data Rate for the Parallel Channel Adapter (PCA)

When you configure a channel attach interface that supports a PCA card, you must define a data rate of either 3 MBps or 4.5 MBps. Perform the following task in interface configuration mode:

Task	Command
Define the PCA data transfer rate.	channel-protocol [s s4]

Configure Other Interface Support

To enhance the usefulness of IBM channel attach support, you can further define how the interface and the router interoperate by performing any of the following tasks in interface configuration mode:

Task	Command
Disable fast switching (IP route cache switching). Fast switching is on by default, but access lists can inhibit fast switching. Always include this command when configuring host-to-host communications through the same ECA interface.	no ip route-cache
Use access lists to filter connections.	access-list access-list-number {permit deny} source source-wildcard
Enable autonomous switching through either the silicon switching engine (SSE) or the CxBus controller.	ip route-cache [cbus sse] or ip route-cache sse
Include autonomous switching support for multiple IP datagram applications running on the same CIP, as required. Always include this command when configuring host-to-host communications through the same ECA interface.	ip route-cache same-interface

Configure IBM Channel Attach for TCP/IP Offload Support

The following sections describe how to configure the IBM channel attach interface for TCP/IP offload support. All tasks, except for configuring other interface support, are required:

- Define the Routing Process
- Assign an IP Address
- Configure the IBM Channel Attach Interface
- Select a Data Rate for the Parallel Channel Adapter (PCA)
- Configure Other Interface Support

See the section “Select Host System Parameters” for guidelines on matching interface configuration values with host system values.

Define the Routing Process

You must configure the routing process that will be used by the Cisco IOS software. We recommend using the Enhanced IGRP routing process to perform IP routing on the IBM channel attach interface. Perform the following steps beginning in global configuration mode:

Task	Command
Step 1 Enter router configuration mode by selecting the routing process, preferably Enhanced IGRP, and the autonomous system the router belongs to.	router eigrp <i>process-id</i>
Step 2 Define the directly connected networks that are part of the autonomous system.	network <i>network-number</i>

Assign an IP Address

You must assign an IP address to the ECA or PCA interface so that it can communicate with other devices (or tasks) on the network. The IP address you assign to the interface must be in the same subnet as the hosts with which you wish to communicate. Perform the following task in interface configuration mode:

Task	Command
Assign an IP address and network mask to the selected interface.	ip address <i>address mask</i>

Configure the IBM Channel Attach Interface

You must define the devices, or tasks supported on the interface. Some information you need to perform this task is derived from the following host system configuration files: MVSIOCP, IOCP, and the TCP/IP configuration. Refer to the section “Select Host System Parameters” for guidelines on matching interface configuration values with host system values.

Perform the following task in interface configuration mode:

Task	Command
Define the offload parameters for this device.	offload <i>path device-address ip-address host-name device-name host-app device-app host-link device-link</i> [broadcast]

See the section “IBM Channel Attach Interface Configuration Examples” for samples of **offload** commands for different configurations.

Select a Data Rate for the Parallel Channel Adapter (PCA)

When you configure a channel attach interface that supports a PCA card, you must define a data rate of either 3 MB per second or 4.5 MB per second. Perform the following task in interface configuration mode:

Task	Command
Define the PCA data transfer rate.	channel-protocol [<i>s</i> <i>s4</i>]

Configure Other Interface Support

You can further define how the interface and the router interoperate. You can perform any of the following tasks in interface configuration mode to enhance the usefulness of IBM channel attach support:

Task	Command
Disable fast switching (IP route cache switching). Fast switching is on by default, but access lists can inhibit fast switching. Always include this command when configuring host-to-host communications through the same ECA interface.	no ip route-cache
Use access lists to filter connections.	access-list <i>list</i> { permit deny } <i>source source-wildcard</i>
Enable autonomous switching through either the silicon switching engine (SSE) or the CxBus controller.	ip route-cache [cbus] or ip route-cache sse
Include autonomous switching support for multiple IP datagram applications running on the same CIP, as required. Always include this command when configuring host-to-host communications through the same ECA interface.	ip route-cache same-interface

Configure IBM Channel Attach for CSNA Support

The following sections describe how to configure the IBM channel attach interface for CSNA support. The last task, “Name the Internal Adapter,” is optional. All other tasks are required.

- Configure the Channel Information
- Configure the Internal LAN Interfaces
- Configure Bridging
- Configure the Internal Adapter’s Link Characteristics
- Name the Internal Adapter

Note Internal LAN interfaces can be configured only on port 2 of a CIP. Port 0 and port 1 represent physical interface ports; port 2 is always reserved for the internal interface.

Configure the Channel Information

To define the SNA channels supported by the CSNA feature, perform the following task in interface configuration mode:

Task	Command
Define the CSNA interface.	csna path <i>device</i> [maxpiu <i>value</i>] [time-delay <i>value</i>] [length-delay <i>value</i>]

Note The CSNA interface is configured on port 0 or port 1, one of the physical interfaces.

Configure the Internal LAN Interfaces

To select an internal LAN interface, perform the following tasks beginning in global configuration mode:

Task	Command
Step 1 Select the channel attach interface and enter interface configuration mode.	interface channel <i>slot/2</i>
Step 2 Select the maximum number of concurrent LLC2 sessions.	max-llc2-sessions <i>number</i>
Step 3 Select the LAN interface and enter internal LAN configuration mode.	lan type <i>lan-id</i>

Configure Bridging

Select the bridging characteristics for Token Ring and FDDI, or Ethernet. Perform either of the following tasks in internal LAN configuration mode:

Task	Command
Select source-route bridging for Token Ring or FDDI.	source-bridge <i>local-ring bridge-number target-ring</i>
Select transparent bridging for Ethernet.	bridge-group <i>bridge-group</i>

Configure the Internal Adapter's Link Characteristics

To configure the link characteristics of the internal LAN adapter, perform the following tasks in internal LAN configuration mode:

Task	Command
Step 1 Enter internal adapter configuration mode.	adapter <i>adapter-number mac-address</i>
Step 2 Configure the link characteristics.	llc2 ack-delay time <i>milliseconds</i> llc2 ack-max <i>packet-count</i> llc2 idle-time <i>milliseconds</i> llc2 local-window <i>packet-count</i> llc2 n1 <i>maximum-size</i> llc2 n2 <i>retry-count</i> llc2 nw <i>window-size</i> llc2 rcv-window <i>size</i> llc2 t1-time <i>milliseconds</i> llc2 tbusy-time <i>milliseconds</i> llc2 tpf-time <i>milliseconds</i> llc2 trej-time <i>milliseconds</i>

Name the Internal Adapter

Select a name for the internal adapter. Perform the following task in internal adapter configuration mode:

Task	Command
Select a name for the internal adapter.	name <i>name</i>

Select Host System Parameters

This section describes how to correlate values found in the VM and MVS system I/O configuration program (IOCP) files with the fields in the **claw** interface configuration command and the **offload** interface configuration command. In addition, you will need configuration information from the host TCP/IP application configuration file. Refer to the following IBM operating system manuals for specific IOCP configuration statement details:

- *Transmission Control Protocol/Internet Protocol TCP/IP Version 2 Release 2.1 for MVS: Planning and Customization*, SC31-6085 (or later version)
- *Transmission Control Protocol/Internet Protocol TCP/IP Version 2 Release 2 for VM: Planning and Customization*, SC31-6082 (or later version)

Values from the Host IOCP File

When you define CLAW or offload parameters, you must supply path information and device address information to support routing on an IBM channel. The path information can be simple, in the case of a channel directly attached to a router, or more challenging when the path includes an ESCON director switch or multiple image facility support.

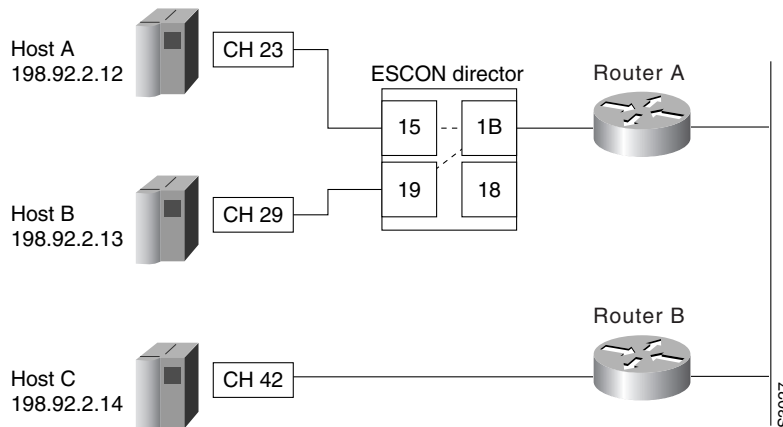
The *path* argument is a concatenation of three hexadecimal numbers that represent the values listed in Table 6.

Table 6 CLAW Path Argument Values

CLAW Path Argument Breakdown	Values	Description
Path	01–FF	For a directly attached ESCON channel or any parallel channel, this value is 01 <i>unless</i> the system administrator has configured another value. For a channel attached through an ESCON director switch, this value will be the path that, from the Cisco IOS software point of view, exits the switch and attaches to the host.
Channel logical address	0–F	For a parallel channel, this value is 0. For a directly attached ESCON channel, the value may be non-zero. If the host is running in Logical Partition (LPAR) mode and the CHPID is defined as shared, this is the partition number associated with the devices configured in the IOCP. The default for this part of the path argument is 0. Otherwise, the channel logical address associated with the channel is defined in the IOCP.
Control unit logical address	0–F	For a parallel channel, this value is 0. For a directly attached ESCON channel, the value may be non-zero. If this value is specified in the IOCP, match that value here. Otherwise, the control unit logical address is specified in the IOCP CNTLUNIT statement for the host channel in the CUADD parameter.

In Figure 147, two host systems connect to the ESCON director switch, on paths 23 and 29. The channels both exit the switch on path 1B and attach to Router A.

Figure 147 System with an ESCON Director Switch and a Directly Attached Channel



Note that the path between Host A and Host B is dynamically switched within the ESCON director. A third host is attached directly to Router B through path 42. The IOCP control unit statements would look something like the following examples:

- Host A


```
CNTLUNIT CUNUMBER=0001, PATH=(23), LINK=1B, UNITADD=((00,64)), UNIT=SCTC, CUADD=F
```
- Host B


```
CNTLUNIT CUNUMBER=0002, PATH=(29), LINK=1B, UNITADD=((00,64)), UNIT=SCTC, CUADD=A
```
- Host C


```
CNTLUNIT CUNUMBER=000A, PATH=(42), UNIT=SCTC, UNITADD=((00,64))
```

Note If you use the Hardware Configuration Definition (HCD) program to generate an IOCP and your release of HCD does not support the value RS6K, you might need to set the control unit and device value to SCTC for your ESCON channels. A device mismatch error message will be displayed, but the device will come online and operate correctly.

The system administrator can provide you with the values, for example 15 and 19, for the return channel attachment from the switch to each host. Given these values, the **claw** command *path* argument for the two channel attachments to Router A becomes:

```
claw 150F
claw 190A
```

The **offload** command *path* argument for the two channel attachments to Router A becomes:

```
offload 150F
offload 190A
```

The **claw** command *path* argument for the directly attached channel to Router B is easy to determine:

```
claw 0100
```

Similarly, the **offload** command *path* argument for the directly attached channel to Router B is as follows:

```
offload 0100
```

Next, determine the **claw** or **offload** command *device-address* argument value, which is shown as 00 in the UNITADD parameter for all three devices. This value can be any even value between 00 and 3E, as long as it matches an allowed UNITADD value in IOCP. The **claw** (or **offload**) commands now become:

- Router A (for the **claw** command)

```
claw 150F 00
claw 190A 00
```

- Router A (for the **offload** command)

```
offload 150F 00
offload 190A 00
```

- Router B (for the **claw** command)

```
claw 0100 02
```

- Router B (for the **offload** command)

```
offload 0100 02
```

Values from the Host TCP/IP File

The remainder of the **claw** and **offload** command arguments are derived from the DEVICE, LINK, and HOME statements in the host TCP/IP configuration files. The statements will be similar to the following:

- Host A

```
DEVICE EVAL CLAW 500 VMSYSTEM C7000 NONE 20 20 4096 4096
LINK EVAL1 IP 0 EVAL
HOME 198.92.2.12 EVAL1
```

- Host B

```
DEVICE EVAL CLAW 600 STSYSTEM C7000 NONE 20 20 4096 4096
LINK EVAL1 IP 0 EVAL
HOME 198.92.2.13 EVAL1
```

- Host C

```
DEVICE EVAL CLAW 700 RDUSYSTEM C7000 NONE 20 20 4096 4096
LINK EVAL1 IP 0 EVAL
HOME 198.92.2.14 EVAL1
```

The DEVICE statement lists the *host-name* and *device-name* values to use, which follows the CLAW 500 entry in the DEVICE statement.

The LINK statement links the device name, EVAL, to EVAL1. The IP address for EVAL1 appears in the HOME statement.

Based on this example, you can supply the remainder of the arguments for the sample **claw** commands:

- Router A

```
claw 150F 00 198.92.2.12 VMSYSTEM C7000 TCPIP TCPIP
claw 190A 00 198.92.2.13 STSYSTEM C7000 TCPIP TCPIP
```

- Router B

```
claw 0100 02 198.92.2.14 RDUSYSTM C7000 TCPIP TCPIP
```

Similarly, the sample **offload** commands are as follows:

- Router A

```
offload 150F 00 198.92.2.12 VMSYSTEM C7000 TCPIP API
offload 190A 00 198.92.2.13 STSYSTEM C7000 TCPIP API
```

- Router B

```
offload 0100 02 198.92.2.14 RDUSYSTM C7000 TCPIP API
```

Example of a Derived Value

When you have a directly attached channel, the system administrator may provide you with a system IODEVICE ADDRESS that you can use. In this case, you must work backwards through the IOCP file to locate the proper *device-address* argument value for the **claw** command.

In this first example, the IODEVICE ADDRESS value is 800. Using this number, you locate the IODEVICE ADDRESS statement in the IOCP file, which points you to the CNTLUNIT statement that contains the *device-address* argument value for the **claw** or **offload** command:

```
IODEVICE ADDRESS=(0800,256),CUNUMBR=(0012),UNIT=SCTC
**** Address 800 points to CUNUMBR 0012 in the following statement

CNTLUNIT CUNUMBR=0012,PATH=(28),UNIT=SCTC,UNITADD=((00,256))
**** The device-address is the UNITADD value of 00
```

From this example, the **claw** or **offload** command would be similar to the following:

```
claw 0100 00 197.91.2.12 CISCOVM EVAL TCPIP TCPIP
```

In the next example, the system administrator has given you an IODEVICE ADDRESS of 350, which does not correspond exactly to a value in the IOCP file. In this instance you must calculate an offset *device-address* argument value for the **claw** or **offload** command:

```
IODEVICE ADDRESS=(0340,64),CUNUMBR=(0008),UNIT=SCTC
IODEVICE ADDRESS=(0380,64),CUNUMBR=(0009),UNIT=SCTC
**** Address 350 (340 + 10) is in the range covered by CUNUMBER 0008

CNTLUNIT CUNUMBR=0008,PATH=(24),UNIT=SCTC,UNITADD=((40,64)),SHARED=N, X
**** The device-address is the UNITADD value of 40, offset by 10
**** The device-address to use is 50
```

From this example, the **claw** or **offload** command would be similar to the following:

```
claw 0100 50 197.91.2.12 CISCOVM EVAL TCPIP TCPIP
```

Note In the IOCP examples for the IODEVICE and CNTLUNIT statements, UNIT=SCTC is the usual value for ESCON channels. Parallel channels will have UNIT=3088 in the CNTLUNIT statement and UNIT=CTC in the IODEVICE statement.



Caution When you are running MVS, you must disable the missing interrupt handler (MIH) to avoid introducing errors into the CLAW algorithm. Refer to the IBM publication *Transmission Control Protocol/Internet Protocol TCP/IP Version 2 Release 2.1 for MVS: Planning and Customization* (publication SC31-6085 or later) for information on disabling the MIH.

Monitor and Maintain the Interface

You can perform the tasks in the following sections to monitor and maintain the interfaces:

- Monitor Interface Status
- Clear and Reset an Interface
- Shut Down and Restart an Interface
- Run CIP Interface Loopback Diagnostics

Monitor Interface Status

The software allows you to display information about the interface, including the version of the software and the hardware, the controller status, and statistics about the interfaces. The following table lists some of the interface monitoring tasks. To display the full list of **show** commands, enter **show ?** at the EXEC prompt.

Perform the following commands in privileged EXEC mode:

Task	Command
Display information about the CIP interfaces on the Cisco 7000 with RSP7000 and Cisco 7500 series. These commands display information that is specific to the interface hardware.	show extended channel slot/port connection-map llc2
	show extended channel slot/port csna [admin oper stats] [path [device-address]]
	show extended channel slot/port icmp-stack [ip-address]
	show extended channel slot/port ip-stack [ip-address]
	show extended channel slot/port llc2 [admin oper stats] [lmac [lsap [rmac [rsap]]]]
	show extended channel slot/port max-llc2-sessions
	show extended channel slot/port statistics [path [device-address]]
	show extended channel slot/port subchannel
	show extended channel slot/port tcp-stack [ip-address]
	show extended channel slot/port udp-listeners [ip-address]
	show extended channel slot/port udp-stack [ip-address]
	show interfaces channel slot/port [accounting]

Task	Command
Display current internal status information for the interface controller cards in the Cisco 7000 with RSP7000 and Cisco 7500 series.	show controllers { <i>cxbus</i> <i>fdi</i> <i>serial</i> <i>t1</i> <i>token</i> }
Display the number of packets for each protocol type that has been sent through the interface for the Cisco 7000 with RSP7000 and Cisco 7500 series.	show interfaces channel <i>slot/port</i>
Display the hardware configuration, software version, names and sources of configuration files, and boot images.	show version

Clear and Reset an Interface

To clear the interface counters shown with the **show interfaces** command, enter the following command in EXEC mode:

Task	Command
Clear interface counters for router.	clear counters [<i>type slot/port</i>]

Note This command will not clear counters retrieved using Simple Network Management Protocol (SNMP), but only those seen with the EXEC **show interfaces** command.

Complete the following task in EXEC mode to clear and reset interfaces. Under normal circumstances, you do not need to clear the hardware logic on interfaces.

Task	Command
Reset the hardware logic on an interface.	clear interface <i>type number</i>

Shut Down and Restart an Interface

You can disable an interface. Doing so disables all functions on the specified interface and marks the interface as unavailable on all monitoring command displays. This information is communicated to other network servers through all dynamic routing protocols. The interface will not be mentioned in any routing updates. On the CIP with an ECA interface adapter, a command is sent to the host to inform it of the impending shutdown. On the CIP with a PCA interface adapter, the **shutdown** command disables the adapter card's transceivers and the PCA stops responding to all commands. A select-out bypass relay must be manually set at the cable connecting to the PCA.

One reason to shut down an interface is if you want to change the interface type of a Cisco 7000 with RSP7000 or Cisco 7500 port online. To ensure that the system recognizes the new interface type, shut down the interface, then reenble it after changing the interface. Refer to your hardware documentation for more details.

To shut down an interface and then restart it, perform the following tasks in interface configuration mode:

Task	Command
Shut down an interface.	shutdown
Reenable an interface.	no shutdown

To check whether an interface is disabled, use the EXEC command **show interfaces**. An interface that has been shut down is shown as administratively down in the **show interfaces** command display.

Run CIP Interface Loopback Diagnostics

The CIP does not provide software loopback support. You can use special loopback wrap plugs to perform hardware loopback with the ECA and PCA interface cards. Hardware loopback information is included in the hardware installation notes for the CIP.

Configuring TN3270 on a Channel Interface Processor

The following sections describe additional features of TN3270 server support on the CIP. The features discussed include the following:

- Dynamic LU Allocation
- Formation of LU Model Type and Number
- Specific LU Allocation
- SNA Switching—End Node DLUR
- Multiple Hosts Support
- IP Type of Service and Precedence Setting

You will also need to understand the following information before proceeding with TN3270 configuration tasks:

- VTAM Host Configuration Considerations for Dynamic LU Allocation
- LU Address Mapping
- TN3270 Configuration Modes

Dynamic LU Allocation

This will be the most common form of request from TN3270 clients emulating a TN3270 terminal. The user typically wants to specify emulating a particular terminal type and normally is not interested in what LOCADDR or LU name is allocated by the host, as long as a network solicitor logon menu is presented. The server will perform the following on such a session request:

- Form an EBCDIC string based on the model type and number requested by the client (see “Formation of LU Model Type and Number” on the algorithm used). This string is used as a field in a Reply product set ID (PSID) network management vector transport (NMVT).
- Allocate a LOCADDR from the next available LU in the generic LU pool. This LOCADDR is used in the NMVT.
- Send the formatted Reply PSID NMVT to VTAM.

When VTAM receives the NMVT, it will use the EBCDIC model type and number string to look up an LU template under the LUGROUP. For example, the string “327802E” will find a match in the sample configuration shown in Figure 148. An ACTLU will be sent and a terminal session with the model and type requested by the client can be established.

Formation of LU Model Type and Number

VTAM requires a model type and number from the Reply PSID NMVT to use as a key to look up in the LU group to find an LU template. The model type is a four character string; the model number is a two or three character string. The server will accept the following formats of terminal type string from the client:

- IBM-<XXXX>-<Y>[-E]: This will be formatted as “XXXX0Y” or “XXXX0YE” in the model type and number field in the Reply PSID NMVT.
- IBM-DYNAMIC: This will result in “DYNAMIC” being put in the model type and number field. The VTAM configuration will need to have “DYNAMIC” defined as a template in the LU group. In fact “IBM-ZZ..Z,” where “ZZ..Z” does not match the preceding syntax, will be forwarded as “ZZ..Z.”

Note The “E” in the model string refers to 3270 Extended Datastream. It has no connection with the “E” in “TN3270E”.

- Any other string is forwarded as is.
- In all cases, the string forwarded is translated from ASCII to EBCDIC and truncated at seven characters.

A complication arises with TN3270E clients that request a copy of the Bind Image. Such clients require SCS datastream on the SSCP-LU flow. All other clients require 3270 datastream on that flow. Therefore, these two kinds of client must be directed to different LUGROUP entries at the host. To make this as easy as possible, the SCS requirement is also encoded into the model string sent to the host. Following the previously described terminal type string formats accepted by the server, this additional condition is applied:

- If the client has negotiated to receive BIND-IMAGE, the character “S” is overlaid on the fifth character of the string, or appended if the string is less than five characters. See Table 7.

Table 7 Examples of Model String Mapping

String from Client (ASCII)	BIND-IMAGE Requested?	String to Host (EBCDIC)
IBM-3278-4	No	327804
IBM-3279-5E	No	327905E
IBM-3279-3-E	Yes	3279S5E
IBM-DYNAMIC	Yes	DYNASIC
ABC	Yes	ABCS
ABCDEFGH	Yes	ABCDSFG

Specific LU Allocation

A TN3270E client can request a specific LU name by using the TN3270E command CONNECT as documented in RFC 1647. The name requested must match the name by which the TN3270 server knows the LU (see the section “LU Names in the TN3270 Server”), and the host must have activated the LU (with ACTLU).

LU Names in the TN3270 Server

Where SNA session switching is configured (that is, on DLUR PUs) the TN3270 server learns the LU names from the ACTLUs.

For direct PUs, a “seed” name can be configured on the PU. TN3270 server uses this name in conjunction with the LOCADDRS to generate names for the LUs. It is best to use the same naming convention as the host.

SNA Switching—End Node DLUR

An end node DLUR function is implemented as part of the TN3270 server. The purpose of the DLUR is to allow the routing of TN3270 LUs to multiple VTAM hosts to be performed in the CIP card rather than on the VTAM hosts. The need for this feature will increase with the introduction of the new multi-CPU CMOS mainframe which comprises up to 16 CPUs that appear as separate VTAMs.

The implementation of TN3270 server LUs under DLUR also allows the server to learn about the LU names on the ACTLU, which greatly simplifies the configuration to support specifically requestable LUs such as printers.

Multiple Hosts Support

The TN3270 server supports access to multiple hosts via the configuration on a PU basis (Table 8). PUs connected to different hosts/applications can be configured with different IP address.

Table 8 Direct PU Configuration in Router

Command	PU		IP-address	Type	Adapter		Lsap	RMAC	RMAC	Lu-seed	Lu-name
	Name	ldblk			number						
PU	X1	05D30001	192.195.80.40	tok	1	4	RMAC	4100.cafe.0001	lu-seed	TN3X1###	
PU	X2	05D30002	171.69.176.43	tok	1	8	RMAC	4100.cafe.0002	lu-seed	TN3X2###	

From the **pu (direct)** TN3270 configuration command values shown in Table 8, PU X2 establishes a link to a host at SAP 4 (the default) on MAC address 4100.cafe.0002. A client connecting to IP address 171.69.176.43 is allocated an LU from that PU and is routed to that host.

Note that by using the DLUR function, all the LUs in the server can be defined and owned by a controlling VTAM. When a client requests an application residing on a different VTAM host, the controlling VTAM will issue the request to the target host which will send a BIND directly to the client. All LU-LU data will then flow directly between the target host and the client without needing to go through the controlling VTAM.

IP Type of Service and Precedence Setting

The TN3270 server supports IP type of service (TOS) precedence setting. TOS is used in router networks to make routing decisions for the generated IP packets. The TN3270 server generates packets that comply to IP TOS and IP precedence values. (Refer to RFC 1349 for a description of IP TOS and IP precedence.)

The Cisco implementation of IP precedence allows values of 0 to 7 while TOS allows values from 0 to 15. You must choose appropriate values for TN3270 screens and printers consistent with your organization’s policy.

At the protocol level, IP precedence allows a router network to discriminate between different types of traffic by giving different priorities to them. IP TOS allows router networks to discriminate between different types of traffic by giving different routing characteristics to them. Precedence and TOS values complement one another and provide flexibility in managing your network traffic.

In TN3270 server, two types of TN3270 clients connect: interactive screens or printers. Screens are interactive while printers need bulk data transfer. IP TOS and IP precedence allows you to discriminate between those two types of sessions and assign different precedence values to the interactive connection and the bulk data connection.

IP TOS and IP precedence values can be specified either at the TN3270 server command level or on the individual PU command level. Values can be specified on both levels, in which case siftdown will be used to determine value on individual PU. Siftdown is used when you configure values in TN3270 server configuration mode that apply to all entities in the server, yet you still can configure individual PUs at the PU configuration mode to alternative values. PU values not specifically changed use the values configured at the TN3270 server configuration mode. This flexibility provides a powerful, yet efficient, way to manage the values.

VTAM Host Configuration Considerations for Dynamic LU Allocation

Other non-Cisco implementations of TN3270 support depend on predefined, static pools of LUs to support different terminal types requested by the TN3270 clients. The CIP TN3270 server implementation removes the static nature of these configurations by using a VTAM release 3.4 feature, dynamic definition of dependent LU (DDDLU). (Refer to the VTAM operating system manuals for your host system, under the descriptions for LUGROUP for additional information.) DDDLU dynamically requests LUs using the terminal type provided by TN3270 clients. The dynamic request eliminates the need to define any LU configuration in the server to support TN3270 clients emulating a generic TN3270 terminal.

To support DDDLU, the PUs used by the TN3270 server have to be defined in VTAM with LUSEED and LUGROUP parameters as shown in Figure 148.

Figure 148 VTAM Host Values Defining LUSEED and LUGROUP

Example VTAM host values defining LUSEED and LUGROUP name parameters:

```

TN3270PU      PU      .      *      define other PU parameters
              IDBLK=05D,
              IDNUM=30001,
              LUSEED=TN3X1###,      *      define the seed component of the LU names
                                      created by DDDLU (e.g. LOCADDR 42 will have
                                      the name TN3X1042)
              LUGROUP=AGROUP      *      define the LU group name
*
TN3X1100      LU      LOCADDR=100,      *      define a terminal which requires a
              MODETAB=AMODETAB      specific LU name
*
TN3X1101      LU      LOCADDR=101,      *      define a printer which requires a specific
              DLOGMODE=M3287CS      LU name
    
```

Example VTAM host values defining LUGROUPname, AGROUP:

```

AGROUP      LUGROUP      *      define LU group to support various
                                      terminal types
    
```

327802E	LU	USSTAB=USSXXX, LOGAPPL=TPXP001, DLOGMOD=SNX32702, SSCPFM=USS3270	*	define template to support IBM 3278 terminal model 2 with Extended Data Stream. Note that the USS messages in USSXXX should be in 3270 datastream.
3278S2E	LU	USSTAB=USSYYY, LOGAPPL=TPXP001, DLOGMOD=SNX32702, SSCPFM=USSSCS	*	define template to support IBM 3278 terminal model 2 with Extended Data Stream, for TN3270E clients requesting BIND-IMAGE.
327805	LU	USSTAB=USSXXX, LOGAPPL=TPXP001, DLOGMOD=D4C32785, SSCPFM=USS3270	*	define template to support IBM 3279 terminal model 5
@	LU	USSTAB=USSXXX, LOGAPPL=TPXP001, DLOGMOD=D4A32772, SSCPFM=USS3270		this is the default template to match any other terminal types

With the configuration shown in Figure 148 defined in the host, the ACTPU sent by VTAM for the PU TN3270PU will have the “Unsolicited NMVT Support” set in the system services control point (SSCP) capabilities control vector. This allows the PU to dynamically allocate LUs by sending network management vector transport (NMVT) with a “Reply Product Set ID” control vector.

After the TN3270 server sends a positive response to the ACTPU, it will wait for VTAM to send ACTLUs for all specifically defined LUs. In the sample configuration shown in Figure 148, ACTLUs will be sent for TN3X1100 and TN3X1101. The server sends a positive response and sets SLU DISABLED. The LOCADDR of these LUs are put into the specific LU cache and reserved for specific LU name requests only.

To allow sufficient time for the VTAM host to send all the ACTLUs, a 30-second timer is started and restarted when an ACTLU is received. When the time expires, it is assumed all ACTLUs defined in VTAM for the PU have been sent. All LUs that have not been activated are available in a generic LU pool to be used for DDDLUs unless they have been reserved by the configuration using the **generic-pool deny** TN3270 configuration command.

After the VTAM activation, the server can support session requests from clients using dynamic or specific LU allocation.

Note If your host computer is customized for a character set other than U.S. English EBCDIC, you might need to code some VTAM configuration tables differently than indicated in the examples provided by Cisco.

Some VTAM configurations include the number sign (#) and at symbol (@). In the U.S. English EBCDIC character set, these characters are stored as the hexadecimal values 7B and 7C, respectively. VTAM will look for those hexadecimal values when processing the configuration file.

The characters used to enter these values are different in other EBCDIC National Language character sets. Table 9 lists the languages that have different characters for the 7B and 7C hexadecimal values and the corresponding symbols used to enter the characters.

For example, the value for the LUSEED parameter in the PU definition called TN3270PU in Figure 148 has a value of TN3X1###. To properly code this value for LUSEED for the French National Language character set, the value should be TN3X1£££.

Table 9 International Character Sets for Hexadecimal Values

Language	Symbol	Hexadecimal value		
		7B		7C
	Symbol	Description	Symbol	Description
German	#	Number sign	§	Section symbol
German (alternate)	Ä	A-dieresis	Ö	O-dieresis
Belgian	#	Number sign	à	a-grave
Brazilian	Õ	O-tilde	Ã	A-tilde
Danish/Norwegian	Æ	AE-ligature	Ø	O-slash
English (U.S./UK)	#	Number sign	@	At symbol
Finnish/Swedish	Ä	A-dieresis	Ö	O-dieresis
French	£	Pound sterling	à	a-grave
Greek	£	Pound sterling	§	Section symbol
Icelandic	#	Number sign	Ð	Uppercase eth
Italian	£	Pound sterling	§	Section symbol
Portuguese	Õ	O-tilde	Ã	A-tilde
Spanish	Ñ	N-tilde	@	At symbol
Turkish	Ö	O-dieresis	Ş	S-cedilla

LU Address Mapping

Logical unit (LU) address mapping allows a client IP address to be mapped, or “nailed,” to one or more LU local addresses on one or more physical units (PUs) by means of router configuration commands. You can control the relationship between the TN3270 client and the LU.

Clients from traditional TN3270 (non-TN3270E) devices can connect to specific LUs, which overcomes a limitation of TN3270 devices that cannot specify a “CONNECT LU.” LU nailing is useful for TN3270E clients, because you can perform the configuration at the router, providing central control, rather than at the client.

Handling Large Configurations

The largest size nonvolatile random-access memory (NVRAM) planned for the Cisco 7000 and 7500 series routers is 128 KB. The maximum number of nailing commands that can be stored in a 128 KB NVRAM is approximately 4000. However, large configurations may map as many as 10,000 IP addresses to LUs.

To maintain a configuration file that exceeds 128 KB there are two alternatives. The configuration file can be stored compressed in NVRAM. Or, the configuration file can be stored in Flash memory that is either internal Flash or on a PCMCIA card.

NVRAM Configuration File Compression

The **service compress-config** global command specifies that the configuration file is to be stored compressed in NVRAM. Once the configuration file has been compressed, the router functions normally. A **show startup-config EXEC** command expands the configuration before displaying it. When the system is booted, it recognizes that the configuration file is compressed and will expand it and proceed normally.

The example below compresses a 129 KB configuration file to 11 KB.

```
router# copy running-config startup-config
Building configuration...
Compressing configuration from 129648 bytes to 11077 bytes
[OK]
```

The size of the configuration must not exceed three times the NVRAM size. For a 128 KB size NVRAM, the largest expanded configuration file size is 384 KB.

Note This compression facility is only available with Cisco IOS Software Release 10 boot ROMs or later.

If the boot ROMs do not recognize a compressed configuration, the following message is displayed:

```
Boot ROMs do not support NVRAM compression Config NOT written to NVRAM
```

Store Configuration File in Flash

Store the startup configuration file in Flash memory by entering the **boot config slot0:router-config** global command. This command sets the environment variable CONFIG_FILE to load the startup configuration (router-config) from Flash memory, which is PCMCIA slot0 in this case. The buffer that holds the configuration file is usually the size of NVRAM. Larger configurations need larger buffers. To adjust the buffer size, use the **boot buffersize bytes** global command.

Note that you must first do a **copy startup-config slot0:router-config** prior to the **boot config slot0:router-config** to create the Flash configuration file. After you have created the Flash configuration file, update the Flash again.

For example, the following commands store the configuration file in Flash memory:

```
copy startup-config slot0:router-config
conf t
  boot buffersize <bytes>
  boot config slot0:router-config
copy running-config startup-config
```

Care must be taken when editing or changing a large configuration. Flash memory space is used every time a **copy running-config startup-config** is issued. Because file management for Flash memory, such as optimizing free space, is not done automatically you must pay close attention to available Flash memory. Cisco recommends that you use a large-capacity Flash card of at least 20 MB.

LU Nailing and Model Matching

The “model matching” feature of the CIP TN3270 server is designed for efficient use of dynamic LUs. Each client specifies a terminal model type at connection. When a non-nailed client connects and does not request a specific LU, the LU allocation algorithm attempts to allocate an LU that operated with that terminal model the last time it was used. If no such model is available, the next choice is an LU that has not been used since the PU was last activated. Failing that, any available LU is used; however, for dynamic LUs only, there is a short delay in connecting the session.

Where a client or set of clients is nailed to a set of more than one LU, the same logic applies. If the configured LU nailing maps a screen client to a set of LUs, the LU nailing algorithm attempts to match the client to a previously used LU that was most recently used with the same terminal model type as requested by the client for this connection. If a match is found, that LU is used. If a match is not found, any LU in the set that is not currently in use is chosen. If there is no available LU in the set, the connection is rejected.

For example, the following LUs are nailed to clients at address 192.195.80.40, and LUs BAGE1004 and BAGE1005, which were connected but are now disconnected.

lu	name	client-ip:tcp	nail	state	model	frames in	out	idle for
1	BAGE1001	192.195.80.40:3822	Y	P-BIND	327904E	4	4	0:22:35
2	BAGE1002	192.195.80.40:3867	Y	ACT/SESS	327904E	8	7	0:21:20
3	BAGE1003	192.195.80.40:3981	Y	ACT/SESS	327803E	13	14	0:10:13
4	BAGE1004	192.195.80.40:3991	Y	ACT/NA	327803E	8	9	0:0:7
5	BAGE1005	192.195.80.40:3997	Y	ACT/NA	327805	8	9	0:7:8

If a client at IP address 192.195.80.40 requests a terminal model of type IBM-3278-5, LU BAGE1005 will be selected over BAGE1004.

lu	name	client-ip:tcp	nail	state	model	frames in	out	idle for
1	BAGE1001	192.195.80.40:3822	Y	P-BIND	327904E	4	4	0:23:29
2	BAGE1002	192.195.80.40:3867	Y	ACT/SESS	327904E	8	7	0:22:14
3	BAGE1003	192.195.80.40:3981	Y	ACT/SESS	327803E	13	14	0:11:7
4	BAGE1004	192.195.80.40:3991	Y	ACT/NA	327803E	8	9	0:1:1
5	BAGE1005	192.195.80.40:4052	Y	ACT/SESS	327805	13	14	0:0:16

TN3270 Configuration Modes

The TN3270 configuration modes and router command prompts are described in the following sections and displayed in Figure 149. The TN3270 server can be configured only on Port 2, the internal LAN port, of a CIP card.

Some configuration commands create entities on the CIP. For most of these, the command changes to the mode associated with that entity (for example, a PU). In general, the parameters provided to create the entity come in two sets: those which identify the specific instance of the entity (for example, a PU name) and those that merely set operating parameters. To return to the mode later, the same command is used but with only the first set of parameters. The following example tasks clarify how to return to a command mode without necessarily creating a new entity:

To create a DLUR LSAP and enter DLUR LSAP configuration mode, perform the following task beginning in TN3270 DLUR configuration mode:

Task	Command
Create a DLUR LSAP and enter DLUR LSAP configuration mode.	lsap token-adapter 1 84

To return later to the DLUR LSAP configuration mode on the same entity, perform the following task beginning in TN3270 DLUR configuration mode:

Task	Command
Enter DLUR LSAP configuration mode on the same LSAP.	lsap token-adapter 1

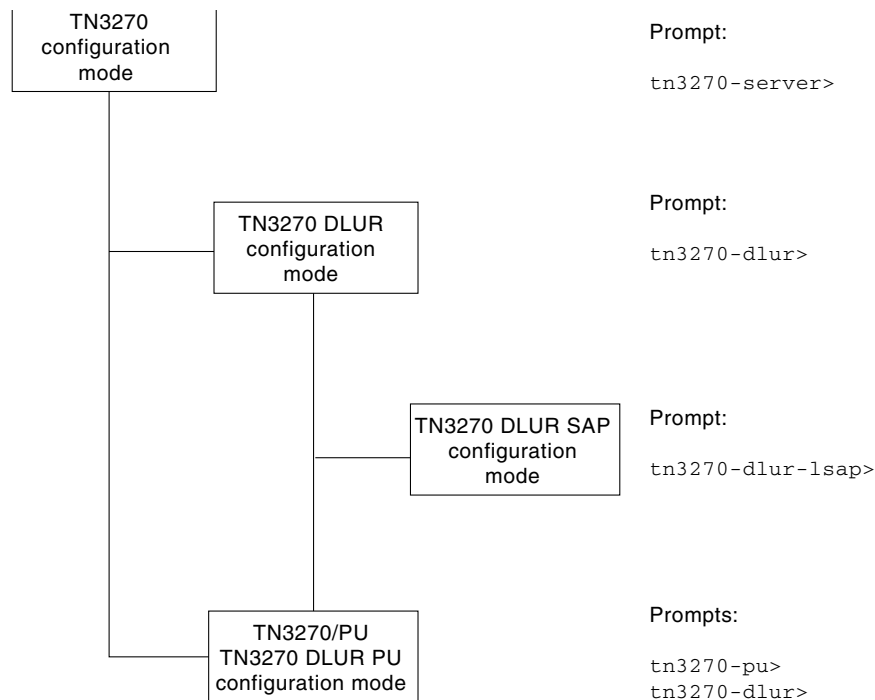
To remove an entity, the same identification parameters are needed. Perform the following task beginning in TN3270 DLUR configuration mode:

Task	Command
Remove a previously defined DLUR LSAP entity.	no lsap token-adapter 1

TN3270 configuration modes described in this section include the following:

- TN3270 Server Configuration Mode
- DLUR Configuration Mode
- DLUR SAP Configuration Mode
- PU Configuration Mode
- Commands Allowed in Multiple Modes

Figure 149 TN3270 Configuration Modes



Prompt:
tn3270-server>

Prompt:
tn3270-dlur>

Prompt:
tn3270-dlur-lsap>

Prompts:
tn3270-pu>
tn3270-dlur>

Use TN3270 PU configuration mode when the TN3270 server is attached to a non-APPN host.

Use TN3270 DLUR PU configuration mode when the TN3270 server is attached to an APPN host.

S4736

TN3270 Server Configuration Mode

From interface configuration mode, **tn3270-server** command puts you in TN3270 server configuration mode.

The following prompt appears:

```
tn3270-server>
```

DLUR Configuration Mode

From TN3270 server configuration mode, the **dlur** command puts you in DLUR configuration mode.

The following prompt appears:

```
tn3270-dlur>
```

DLUR SAP Configuration Mode

From DLUR server configuration mode, **lsap** command puts you in DLUR SAP configuration mode.

The following prompt appears:

```
tn3270-dlur-lsap>
```

PU Configuration Mode

There are two paths to PU configuration mode: from the TN3270 server configuration mode, or from the DLUR configuration mode. In either mode, the **pu** command puts you in PU configuration mode.

From TN3270 configuration mode, the **pu** command to create a new PU is:

```
pu pu-name idblk-idnum ip-address type adapno lsap [rmac rmac] [rsap rsap] [lu-seed  
lu-name-stem]
```

From DLUR configuration mode, the **pu** command to create a new PU is:

```
pu pu-name idblk-idnum ip-address
```

From either mode, to return to PU configuration mode on PU *pu-name* the command is:

```
pu pu-name
```

The following prompts appear, depending on which mode you are in:

```
tn3270-pu>  
tn3270-dlur-pu>
```

Commands Allowed in Multiple Modes

The following commands are valid in TN3270 configuration mode, or in either variation of PU configuration mode:

- **generic-pool** {**permit** | **deny**}
- **idle-time** *seconds*
- **ip precedence** {**screen** | **printer**} *value*
- **ip tos** {**screen** | **printer**} *value*
- **keepalive** *seconds*
- **shutdown**
- **tcp-port** *port-number*
- **unbind-action** {**keep** | **disconnect**}

Values entered in PU configuration mode override settings made in TN3270 configuration mode. In addition, the **no** form of these commands entered in PU configuration mode will restore the command value entered in TN3270 command mode.

TN3270 Configuration Task List

The following sections describe how to configure TN3270 server support on the CIP. Not all tasks are required. Refer to “TN3270 Configuration Example” for configuration examples.

Note The TN3270 server is configured on an internal LAN interface in the CIP, which is port 2 of a CIP. Port 0 and port 1 represent physical interface ports; port 2 is a “virtual” port and always reserved for the internal LAN interface.

Task List for Multiple APPN Hosts

When the host site uses APPN and the TN3270 server can reach multiple hosts, we recommend you use DLUR and configure your PUs under DLUR. In this instance, perform the following tasks:

- Configure SNA Support
- Configure TN3270 Server
- Configure IP Precedence
- Configure IP TOS
- Configure DLUR
- Configure SAPs under DLUR
- Configure PUs under DLUR
- Configure LU Nailing
- Monitor the TN3270 Server

Note You can also use DLUR to reach a mix of APPN and non-APPN hosts. The host owning the PUs must be an APPN network node that also supports the subarea (that is, an interchange node). When an SLU starts a session with any of the APPN hosts, it can use session switching to reach that host directly. When it starts a session with a non-APPN host, the traffic will be routed through the owning host.

Task List for non-APPN Hosts

When the host site does not use APPN, you configure your PU parameters for a directly-connected host. In this instance, perform the following tasks:

- Configure SNA Support
- Configure TN3270 Server
- Configure IP Precedence
- Configure IP TOS
- Configure PU Parameters on the TN3270 Server
- Configure LU Nailing
- Monitor the TN3270 Server

Configure SNA Support

CIP SNA support (CSNA) must be configured prior to configuring TN3270 support. Refer to the section “Configure IBM Channel Attach for CSNA Support,” earlier in this chapter.

After you have configured CSNA support, you proceed with TN3270 configuration.

Configure TN3270 Server

This task is required. To establish a TN3270 server on the internal LAN interface on the CIP, perform the following tasks beginning in global configuration mode:

Task	Command
Select the channel attach internal LAN interface and enter interface configuration mode.	interface channel <i>slot/2</i>
Specify a TN3270 server on the internal LAN interface and enter TN3270 configuration mode.	tn3270-server
(Optional) Configure maximum number of LUs allowed.	maximum-lus <i>max-number-of-lu-allocated</i>
(Optional) Configure LU session limits for each client IP address or IP subnetwork address.	client [<i>ip [ip-mask]</i>] lu maximum number
(Optional) Configure transmission of a WILL TIMING-MARK.	timing-mark
(Optional) Assign a TCP port other than the default of 23. This command is also available in PU configuration mode.	tcp-port <i>port-nbr</i>
(Optional) Specify the idle time for server disconnect. This command is also available in PU configuration mode.	idle-time <i>num-of-seconds</i>
(Optional) Specify the maximum time allowed between keepalive marks before the server disconnects. This command is also available in PU configuration mode. Note: To enable sending of power-off Reply product set identification (PSID) network management vector transport (NMVT) to the host, the value should be set to 50000 more than the desired value. If the configured value is greater than 50000, the value used for the keepalive function will be 50000 less than the configured value.	keepalive <i>num-of-seconds</i>
(Optional) Specify whether the TN3270 session will disconnect when an UNBIND command is received. This command is also available in PU configuration mode.	unbind-action { keep disconnect }
(Optional) Select whether “left-over” LUs can be used from a generic LU pool. This command is also available in PU configuration mode.	generic-pool { permit deny }

When you use the **tn3270-server** command, you enter TN3270 configuration mode and can use all other commands in the task list. You can later override many configuration values you enter in TN3270 configuration mode from PU configuration mode. On IBM host systems, these types of commands are often referred to as “sift down” commands because their values can sift down through several levels of configuration and can be optionally altered at each configuration level.

Configure IP Precedence

To configure IP precedence, perform the following task in TN3270 server or TN3270 PU configuration mode:

Task	Command
Configure the IP level.	ip precedence { screen printer } <i>value</i>

Use the **no ip precedence screen** or the **no ip precedence printer** commands to return the precedence value to a default of 0.

Configure IP TOS

To configure IP TOS, perform the following task in TN3270 server or TN3270 PU configuration mode:

Task	Command
Configure the IP TOS delay level.	ip tos { screen printer } <i>value</i>

Use the **no ip tos screen** or the **no ip tos printer** commands to return the precedence value to a default of 0.

Configure PU Parameters on the TN3270 Server

This task is required when configuring PUs that do not use DLUR. To configure PU parameters for the TN3270 server, perform the following tasks beginning in TN3270 configuration mode:

Task	Command
Enter PU configuration mode and create or delete PUs with direct host links.	pu <i>pu-name idblk-idnum ip-address type adapno lsap</i> [rmac <i>rmac</i>] [rsap <i>rsap</i>] [lu-seed <i>lu-name-stem</i>]
(Optional) Assign a TCP port other than the default of 23. This command is also available in TN3270 configuration mode.	tcp-port <i>port-nbr</i>
(Optional) Specify the idle time for server disconnect. This command is also available in TN3270 configuration mode.	idle-time <i>num-of-seconds</i>
(Optional) Specify the maximum time allowed between keepalive marks before the server disconnects. This command is also available in TN3270 configuration mode.	keepalive <i>num-of-seconds</i>
(Optional) Specify whether the TN3270 session will disconnect when an UNBIND command is received. This command is also available in TN3270 configuration mode.	unbind-action { keep disconnect }
(Optional) Select whether “left-over” LUs can be used from a generic LU pool. This command is also available in TN3270 configuration mode.	generic-pool { permit deny }

When you use the **pu** command, you enter PU configuration mode and can use all other commands in this task list. Configuration values you enter in PU configuration mode will override other values entered while in TN3270 configuration mode. In addition, you can enter PU configuration mode from DLUR configuration mode when configuring PUs that are connected by means of DLUR.

If you are configuring PUs for directly connected hosts, you need not perform any additional configuration tasks.

Configure DLUR

This task is required when configuring DLUR connected hosts. To configure DLUR parameters for the TN3270 server, perform the following tasks beginning in TN3270 configuration mode:

Task	Command
Create a DLUR function in the TN3270 server and enter DLUR configuration mode.	dlur <i>fq-cpname fq-dlusname</i>
(Optional) Specify the fallback choice for the DLUR DLUS.	dlus-backup <i>dlusname2</i>
(Optional) Specify the preferred network node (NN) server.	preferred-nnserver <i>NNserver</i>

Configure SAPs under DLUR

To configure SAPs under the DLUR function, perform the following tasks beginning in DLUR configuration mode:

Task	Command
Create a SAP function under DLUR and enter DLUR SAP configuration mode.	lsap <i>type adapno [lsap]</i>
(Optional) Identify an APPN virtual routing node (VRN).	vrn <i>vrn-name</i>
(Optional) Create named links to hosts. A link should be configured to each potential NN server. (The alternative is to configure the NN servers to connect to DLUR.) If VRN is used it is not necessary to configure links to other hosts. Do not configure multiple links to the same host.	link <i>name [rmac rmac] [rsap rsap]</i>

Configure PUs under DLUR

This task is required when configuring DLUR connected hosts. To configure PUs under the DLUR function, perform the following tasks beginning in DLUR configuration mode:

Task	Command
Create a PU function under DLUR and enter PU configuration mode.	pu <i>pu-name idblk-idnum ip-address</i>
Assign a TCP port other than the default of 23.	tcp-port <i>port-nbr</i>
Specify the idle time for server disconnect.	idle-time <i>num-of-seconds</i>
Specify the maximum time allowed between keepalive marks before the server disconnects.	keepalive <i>num-of-seconds</i>

Task	Command
Specify whether the TN3270 session will disconnect when an UNBIND command is received.	unbind-action { keep disconnect }
Select whether “left-over” LUs can be used from a generic LU pool.	generic-pool { permit deny }

The **pu** command entered in DLUR configuration mode has different parameters than when it is entered from TN3270 configuration mode.

Configure LU Nailing

To configure LU nailing, perform the following task in TN3270 PU configuration mode:

Task	Command
Configure the IP address and nail type and specify the locaddr range.	client [printer] ip <i>ip-address</i> [<i>mask</i>] lu <i>first-locaddr</i> [<i>last-locaddr</i>]

The **client** command allows a client with multiple TN3270 connections from the same IP address to nail their screen connections to LUs that are configured as screen LUs at the host and to nail printer connections to LUs that are configured as printers at the host. When the connection is made, a device type of “328*” is matched to a printer definition, and any other device type is matched to a screen definition.

Monitor the TN3270 Server

The following table lists some of the monitoring tasks specific to the TN3270 server. To display the full list of **show** commands, enter **show ?** at the EXEC prompt.

Use the following commands in privileged EXEC mode:

Task	Command
Display the current server configuration parameters and the status of the PUs defined in each server.	show extended channel tn3270-server
Display the PU configuration parameters, statistics and all the LUs currently attached to the PU.	show extended channel tn3270-server <i>pu-name</i>
Display mappings between a nailed client IP address and nailed LUs	show extended channel tn3270-server nailed-ip <i>ip-address</i>
Display the status of the LU.	show extended channel tn3270-server <i>pu-name</i> lu <i>lu-number</i> [history]
Display information about LUs at a specific IP address with a particular status.	show extended channel tn3270-server client-ip-address <i>ip-address</i> [disconnected in-session pending]
Display information about the DLUR components.	show extended channel tn3270-server dlur

Cisco MultiPath Channel

Cisco MultiPath Channel (CMPC) is Cisco System's implementation of IBM's MultiPath Channel (MPC) feature. CMPC allows the virtual telecommunications access method (VTAM) to establish Advanced-Peer-to-Peer Networking (APPN) connections using both High Performance Routing (HPR) and Intermediate Session Routing (ISR) through a channel-attached Cisco 7000 with RSP7000 and Cisco 7500 series router using the MPC protocols.

An APPN ISR channel connection to a Cisco router also can be established with CSNA. However, an APPN HPR channel connection to a Cisco router is possible only through the use of CMPC.

With CMPC, Cisco 7000 with RSP7000 and Cisco 7500 series routers can be deployed in parallel MVS systems complex (sysplex) configurations.

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

- Another VTAM channel-attached to the same CIP.
- Another VTAM channel-attached to a different CIP in the same router.
- TN3270 server DLUR in the same CIP.
- APPN network node (NN) in the CIP router.
- Other APPN nodes external to the CIP and CIP router: CS/2, AS/400, other LAN or WAN attached VTAM hosts.

One read subchannel and one write subchannel are supported for each MPC transmission group. The read subchannel and write subchannel may be split over two physical channel connections.

CMPC insulates VTAM from the actual network topology. The MPC protocols are terminated on the CIP and converted to LLC protocols. Once 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 coexists on a CIP with the TCP/IP Offload, IP Datagram, TN3270, and CSNA features.

Requirements

The following are minimum router requirements to support CMPC:

- CIP version 4.4 (CIP1) with a minimum of 32 MB DRAM
- CIP microcode version cip25-0 or later
- Cisco IOS Release 11.3 or later

The following are minimum host system requirements to support CMPC:

- VTAM V4.2+, for MPC APPN ISR connections
- VTAM V4.3+, for MPC APPN HPR connections

Configuration Overview

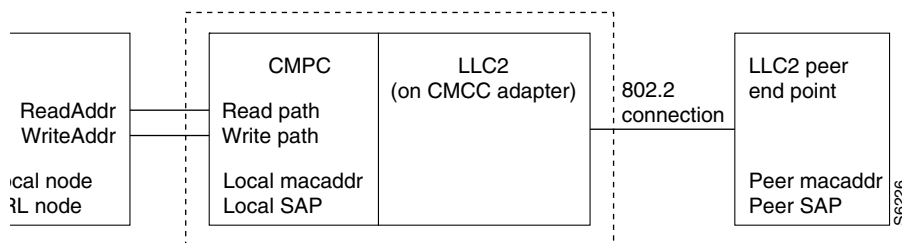
To configure the CMPC feature, you must configure the host VTAM parameters and the CIP card in the Cisco 7000 with RSP7000 or Cisco 7500 series router. The CMPC Configuration Examples show the VTAM configuration parameters and the router configuration commands for each example.

The following guidelines will help you prepare for CMPC configuration:

- A CMPC link uses two subchannels: one read and one write. Some IBM implementations of MPC allow multiple read and multiple write subchannels. CMPC will 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 transmission group.
- Multiple CMPC links can be configured between the host and the CIP in the Cisco 7500 series router.
- The two subchannels in a CMPC link need not be adjacent devices. Either channel may be the read subchannel and either channel may be the write subchannel. The two subchannels can be on separate channel process IDs in the host.
- The two subchannels must be connected to the same CIP, however they do not have to be connected to the same CIP port adapter. In other words, it is possible to connect a read subchannel to the CIP's port adapter 0 while the write subchannel is connected to the same CIP's port adapter 1.
- Only APPN connections will be supported across CMPC. For this reason when TN3270 server is configured with CMPC, it must be configured as an APPN end node with DLUR.
- You must know what device addresses you will be using and the associated channel path statements.
- You must know whether or not you will use HPR.
- To configure the LLC2 interface for the CIP, you will need to choose a local MAC address and a local SAP address.
- You must know the remote MAC address and remote SAP of the LLC2 peer with which the CMPC communicates.
- You must understand how to configure source-bridge ring groups on the CIP and RSP or RP.
- On the router, the combination of one read subchannel definition, one write subchannel definition, and a transmission group definition, associated by a unique *tg-name*, makes up a CMPC transmission group specification.

To help clarify the configuration process, refer to Figure 150, which shows the CMPC link between the VTAM host, the router, and CIP card, and the communication to the LLC2 end point. 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 end point of the connection by means of the IEEE 802.2 link.

Figure 150 Logical View of CMPC Link



Configuration Tasks

This section describes the following configuration tasks associated with the CMPC feature. The first two tasks are performed on the VTAM host. The remaining tasks are performed on the router. All tasks are required.

- Configure the VTAM Transport Resource List Major Node
- Configure the VTAM Local SNA Major Node
- Configure the CMPC Subchannels
- Configure the CMPC Transmission Groups
- Configure the CIP Internal LAN for CMPC

Configure the VTAM Transport Resource List Major Node

To configure MPC on the host, define the Transport Resource List (TRL) major node. See the following IBM documents for details on how to configure the TRL major node:

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

The following is an example of a typical configuration:

```

LAGTRLA  VBUILD  TYPE=TRL
LAGTRLEA  TRLE  LNCTL=MPC,MAXBFRTU=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. The command to activate the TRL should be issued before activating the Local node. If your TRL data set was named LAGTRLA, the activate command would be as follows:

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

where the ID parameter refers to the name of the data set containing the TRL definition.

Note that “update=add” is preferred. 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 data set and wish 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,trl=trl_name
```

Configure 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 refers to the label on the TRLE statement from the TRL major node LAGTRLA. Also, if you do not want to run HPR set the HPR parameter to “NO.” The local SNA major node must be activated after the TRL node has been activated. If your local node data set was named LAGLNA, the activate command is as follows:

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

Configure the CMPC Subchannels

To define a CMPC read subchannel and CMPC write subchannel, perform the following tasks in interface configuration mode on a CIP physical interface:

Task	Command
Configure the CMPC read subchannel.	cmnpc path device tg-name {read write}
Configure the CMPC write subchannel.	cmnpc path device tg-name {read write}

These statements define the subchannel addresses that CMPC will use to connect to the host, and correspond to the definitions in the TRL major network node on the host.

Use the **no cmnpc path** command to remove the definition of a subchannel and to deactivate the CMPC transmission group.

Configure the CMPC Transmission Groups

To define a CMPC transmission group by name and specify its connection to the LLC2 stack, perform the following task in interface configuration mode on a CIP virtual interface:

Task	Command
Define the CMPC transmission group name.	tg tg-name llc type adaptno lsap [rmac rmac] [rsap rsap]

The **tg** command defines an LLC connection with a complete addressing 4-tuple. The *lsap*, *rmac*, and *rsap* are specified explicitly by parameters. The *lmac* is the LMAC of the adapter referred to by the *type* and *adaptno* parameters.

The *tg-name* must match the name given in the **cmpc** command issued in the physical interface(s) on the same CIP.

Use the **no tg** command to remove a CMPC transmission group from the configuration, which will deactivate the named CMPC transmission group.

To change any parameter of the **tg** statement, the statement must be removed by using the **no tg tg-name** command.

Configure the CIP Internal LAN for CMPC

Configuring CMPC support on the CIP internal LAN is similar to configuring CSNA support. Many of the configuration tasks are the same. To configure the internal LAN adapter on the CIP to support CMPC, perform the following tasks:

- Configure the CIP Internal LANs
- Configure Source-Route Bridging
- Configure the Internal Adapter and Its Link Characteristics
- Name the Internal Adapter

Configure the CIP Internal LANs

To select a CIP internal LAN interface, perform the following tasks beginning in global configuration mode:

Task	Command
Step 1 Select the channel attach interface and enter interface configuration mode.	interface channel <i>slot/2</i>
Step 2 Select the maximum number of concurrent LLC2 sessions.	max-llc2-sessions <i>number</i>
Step 3 Select the LAN interface and enter internal LAN configuration mode.	lan type <i>lan-id</i>

Use the **no lan** command to disconnect all LLC2 sessions established through all internal LAN interfaces configured on a particular internal LAN.

Up to 18 internal adapters can be configured on an internal LAN.

Configure Source-Route Bridging

Select the bridging characteristics for Token Ring and FDDI or for Ethernet. Perform either of the following tasks in internal LAN configuration mode:

Task	Command
Select source-route bridging for Token Ring or FDDI.	source-bridge <i>local-ring bridge-number target-ring</i>
Select transparent bridging for Ethernet.	bridge-group <i>bridge-group</i>

Configure the Internal Adapter and Its Link Characteristics

To configure the link characteristics of the internal LAN adapter, perform the following tasks in internal LAN configuration mode:

Task	Command
Step 1 Enter internal adapter configuration mode and configure the adapter.	adapter <i>adapter-number mac-address</i>
Step 2 Configure the link parameters.	llc2 ack-delay time <i>milliseconds</i> llc2 ack-max <i>packet-count</i> llc2 idle-time <i>milliseconds</i> llc2 local-window <i>packet-count</i> llc2 n2 <i>retry-count</i> llc2 t1-time <i>milliseconds</i> llc2 tbusy-time <i>milliseconds</i> llc2 tpf-time <i>milliseconds</i> llc2 trej-time <i>milliseconds</i> llc2 xid-neg-val-time <i>milliseconds</i> llc2 xid-retry-time <i>milliseconds</i>

Configuring LLC parameters is optional. Default values are used when no parameters are configured.

Name the Internal Adapter

To select a name for the internal adapter, perform the following task in internal adapter configuration mode:

Task	Command
Select a name for the internal adapter.	name <i>name</i>

Naming an internal adapter is optional.

IBM Channel Attach Interface Configuration Examples

The following sections include examples to help you understand some aspects of interface configuration:

- Routing Process Configuration Example
- IP Address and Network Mask Configuration Example
- CLAW Configuration Example
- Offload Configuration Example
- CSNA Configuration Example
- Interface Shutdown and Startup Example
- TN3270 Configuration Example
- Configure Static and Dynamic LUs with LU Nailing Example
- Remove LU Nailing Definitions Example

- Configuring Different Values for Precedence and TOS Example
- Overriding Configured Values Example

Routing Process Configuration Example

The following example configures an Enhanced IGRP routing process in autonomous system 127 and defines two networks to be advertised as originating within that autonomous system:

```
router eigrp 127
 network 197.91.2.0
 network 197.91.0.0
```

IP Address and Network Mask Configuration Example

The following example assigns an IP address and network mask to the IBM channel attach interface on the router:

```
ip address 197.91.2.5 255.255.255.0
```

CLAW Configuration Example

The following example configures the IBM channel attach interface to support a directly connected device:

```
claw 0100 00 197.91.0.21 VMSYSTEM C7000 TCPIP TCPIP
```

Offload Configuration Example

The following example consists of the mainframe host profile statements, buffer poolsize recommendations, and router configuration statements for the network shown in Figure 151.

Host Profile Statements

```
; Device statement
DEVICE OFF CLAW 762 CISCOVM CIP1 NONE 20 20 4096 4096
!
; Link Statements (both needed)
LINK OFFL OFFLOADLINK1 1 OFF
LINK MEMD OFFLOADAPIBROAD 162.18.4.59 OFF OFFL
!
; Home Statement
; (No additional home statements are added for offload)
!
!
; Routing information (if you are not using the ROUTED SERVER)
GATEWAY
; NETWORK FIRST HOP DRIVER PCKT_SZ SUBN_MSK SUBN_VALUE
162.18 = MEMD 4096 0.0.255.248 0.0.4.56
DEFAULTNET = MEMD 1500 0
!
;START statements
START OFF
!
```

Buffer Poolsize Recommendations

See the IBM *TCP/IP Performance Tuning Guide* (SC31-7188-00) for buffer size adjustments.

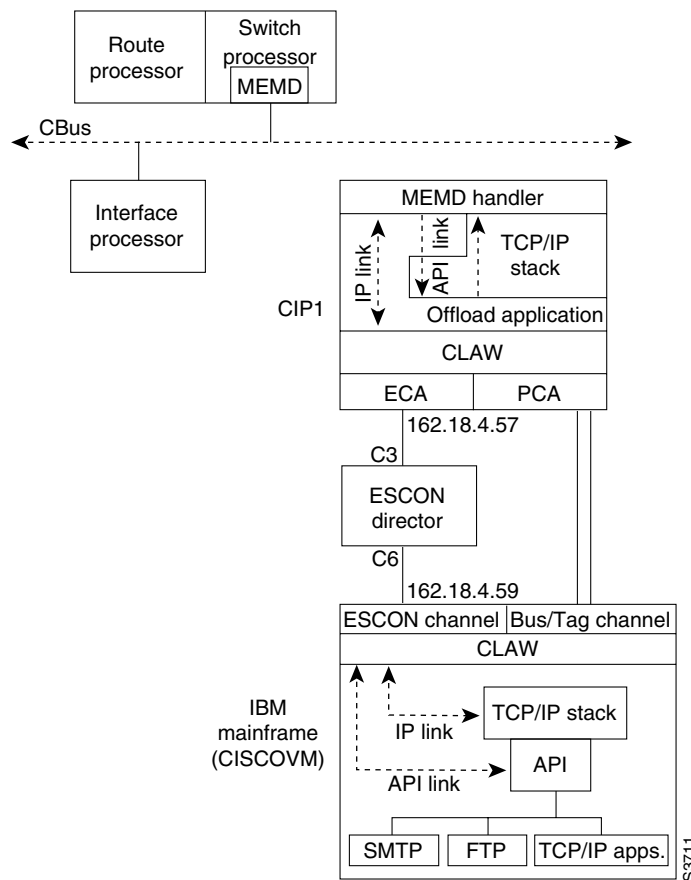
Router Configuration Statements

The following statements configure the offload feature in the router. When you configure an host-to-host communication through the same ECA adapter, include the **no ip redirects** and **ip route-cache same-interface** commands:

```

!
interface Channel0/0
 ip address 162.18.4.57 255.255.255.248
 no ip redirects
 ip route-cache same-interface
 ip route-cache cbus
 no keepalive
 offload C300 62 162.18.4.59 CISCOVM CIP1 TCPIP TCPIP TCPIP API
!
    
```

Figure 151 Offload Network Configuration Block Diagram



CSNA Configuration Example

The following configuration shows how to configure CSNA in a Cisco 7000 with RSP7000 and Cisco 7500 channel-attached router. This configuration example accommodates the router configuration illustrated in Figure 152.

```

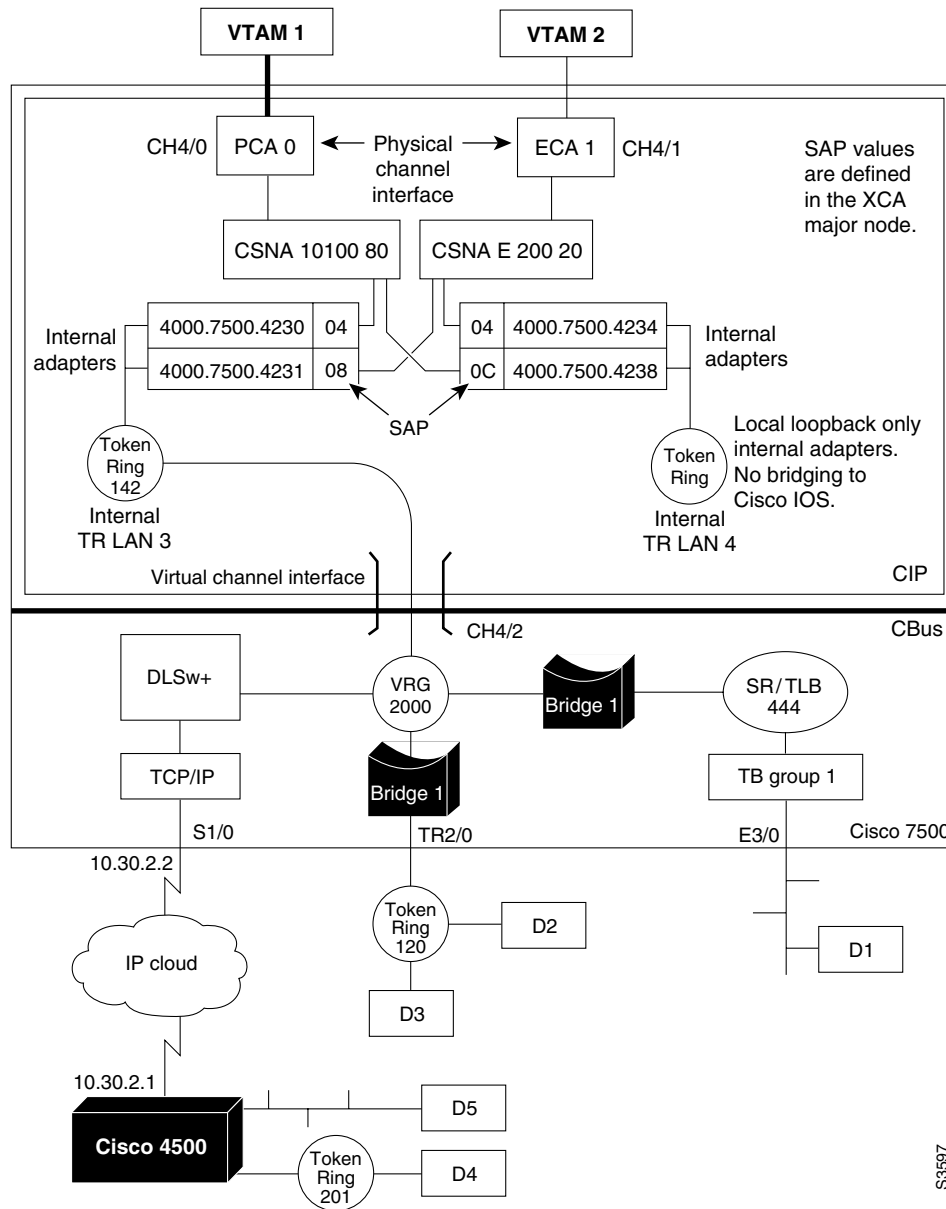
source-bridge ring-group 2
source-bridge remote-peer tcp 198.92.0.122
    
```

```

source-bridge remote-peer tcp 198.92.0.123
!
interface serial 1/0
 ip address 198.92.0.122 255.255.255.0
 clockrate 56000
!
interface tokenring 2/0
 mac-address 400070000411
 no ip address
 ring-speed 16
 source-bridge active 101 1 2
 source-bridge spanning
!
interface ethernet 3/0
 mac-address 020070000412
 no ip address
 bridge-group 1
!
interface fddi 4/0
 mac-address 400070000413
 no ip address
 source-bridge 102 1 2
!
interface channel 0/0
 csna 0100 80
 csna 0100 81
!
interface channel 0/1
 csna 0100 40
 csna 0100 41 time-delay 30 length-delay 4096
!
interface channel 0/2
!
max-llc2-sessions 2048
!
lan tokenring 0
 source-bridge 1000 1 2
 adapter 0 4000.0000.0401
 adapter 1 4000.0000.0402
 llc2 N2 3
 llc2 t1-time 2000
!
lan tokenring 1
 source-bridge 1001 1 2
 adapter 2 4000.0000.0401
 adapter 3 4000.0000.0403
 llc2 N2 3
 llc2 t1-time 2000
!
lan ethernet 0
 bridge-group 1
 adapter 0 4000.0000.0C01
!
lan fddi 0
 source-bridge 1002 1 2
 adapter 0 4000.0000.0D01
!
bridge 1 protocol ieee

```

Figure 152 CSNA Internal LAN Network Diagram



Interface Shutdown and Startup Example

The following example turns off the CIP interface in slot 2 at port 0:

```
interface channel 2/0
shutdown
```

The following example enables the CIP interface in slot 3 at port 0 that had been previously shut down:

```
interface channel 3/0
no shutdown
```

TN3270 Configuration Example

The following configuration has three PUs using DLUR and two more with direct connections.

The initial CIP configuration is as follows:

```
interface Channel2/2
 ip address 10.10.20.126 255.255.255.128
 no ip redirects
 no ip directed-broadcast
 ip pim query-interval 0
 ip igmp query-interval 0
 no ip route-cache
 no keepalive
 no clns checksum
 clns congestion-threshold 0
 clns erpdu-interval 0
 clns rdpdu-interval 0
 no clns route-cache
 no clns send-erpdu
 no clns send-rdpdu
 lan TokenRing 0
 source-bridge 223 1 2099
 adapter 0 4100.cafe.0001
 11c2 N1 2057
 adapter 1 4100.cafe.0002
 11c2 N1 2057
```

Configuration dialog to configure the TN3270 function follows:

```
! HOSTA is channel-attached and will open SAP 8 on adapter 0.
! HOSTB is reached via token-ring
! HOSTC is channel-attached non-APPN and will open SAP 4 on adapter 0.

! enter interface configuration mode for the virtual interface in slot 2
router(config)#int channel 2/2

! create TN3270 Server entity
router(config-if)#tn3270-server

! set server-wide defaults for PU parameters
router(cfg-tn3270)#keepalive 0
router(cfg-tn3270)#unbind-action disconnect
router(cfg-tn3270)#generic-pool permit

! define DLUR parameters and enter DLUR configuration mode
router(cfg-tn3270)#dlur SYD.TN3020 SYD.VMG

! create PUs under DLUR
! Note that the first two share an IP address
router(tn3270-dlur)#pu pu0 05d99001 10.10.20.1
router(tn3270-dlur-pu)#pu pu1 05d99002 10.10.20.1
router(tn3270-dlur-pu)#pu pu2 05d99003 10.10.20.2

! create a DLUR LSAP and enter DLUR LSAP configuration mode
router(tn3270-dlur-pu)#lsap token-adapter 1

! specify the VRN name of the network containing this lsap
router(tn3270-dlur-lsap)#vrn syd.lan4

! create a link from this lsap
router(tn3270-dlur-lsap)#link hosta rmac 4100.cafe.0001 rsap 8
router(tn3270-dlur-lsap)#link hostb rmac 4000.7470.0009 rsap 4
router(tn3270-dlur-lsap)#exit
router(tn3270-dlur)#exit
```

```
! create direct pus for the non-APPN Host
! note that they must use different lsaps because they go to the same Host
router(cfg-tn3270)#pu pu3 05d00001 10.10.20.5 tok 1 24 rmac 4100.cafe.0001 lu-seed pu3###
router(tn3270-pu)#pu pu4 05d00002 10.10.20.5 tok 1 28 rmac 4100.cafe.0001 lu-seed pu4###
router(tn3270-pu)#end
```

The resulting configuration from the initial configuration and the configuration dialog follows:

```
interface Channel2/2
 ip address 10.10.20.126 255.255.255.128
 no ip redirects
 no ip directed-broadcast
 ip pim query-interval 0
 ip igmp query-interval 0
 no ip route-cache
 no keepalive
 no clns checksum
 clns congestion-threshold 0
 clns erpdu-interval 0
 clns rdpdu-interval 0
 no clns route-cache
 no clns send-erpdu
 no clns send-rdpdu
 lan TokenRing 0
 source-bridge 223 1 2099
 adapter 0 4100.cafe.0001
 llc2 N1 2057
 adapter 1 4100.cafe.0002
 llc2 N1 2057
tn3270-server
 pu PU3      05D00001 10.10.20.5   token-adapter 1 24 rmac 4100.cafe.0001 lu-seed PU3###
 pu PU4      05D00002 10.10.20.5   token-adapter 1 28 rmac 4100.cafe.0001 lu-seed PU4###
 dlur SYD.TN3020 SYD.VMG
   lsap token-adapter 1
     vrn SYD.LAN4
     link HOSTB      rmac 4000.7470.0009
     link HOSTA      rmac 4100.cafe.0001 rsap 08
 pu PU0      05D99001 10.10.20.1
 pu PU1      05D99002 10.10.20.1
 pu PU2      05D99003 10.10.20.2
```

Configure Static and Dynamic LUs with LU Nailing Example

The following example shows a direct PU and a DLUR PU configured with the same listening point. The PUs are configured with the same nailed client IP address.

```
tn3270-server
 pu PU1 05D18081 172.28.1.82 ...
 client ip 192.195.80.40 lu 1 10
 dlur
 pu PU2 05D190B3 172.28.1.82
 client ip 192.195.80.40 lu 1 10
```

Assuming each PU has three static LUs, which are ACTLU enabled and not connected, then these LUs will be the first to be nailed. That is, the first six connections from client IP address 192.195.80.40 will use the static LUs and subsequent connections will use the remaining dynamic LUs.

Remove LU Nailing Definitions Example

In the following example, locaddrs 1 to 50 are reserved for all remote screen devices in the 171.69.176.0 subnet.

```
interface channel 2/2
  tn3270-server
  pu BAGE4
  client ip 171.69.176.28 255.255.255.0 lu 1 50
```

To remove a nailing definition, the complete range of locaddrs must be specified as configured. So for the example above, the following command would remove the LU nailing definition.

```
no client ip 171.69.176.28 255.255.255.0 lu 1 50
```

If an attempt is made to remove a subset of the range of configured locaddrs then the command is rejected.

```
no client ip 171.69.176.28 255.255.255.0 lu 1 20
% client ip 171.69.176.28 lu not matched with configured lu 1 50
```

Configuring Different Values for Precedence and TOS Example

The following example changes IP precedence and IP TOS to different values under the TN3270 server for both the screen and printer. Note that any PUs defined under this configuration will inherit these values unless the corresponding parameter is specifically changed for that PU.

```
interface channel 3/2
  tn3270-server
  ip precedence screen 6
  ip precedence printer 3
  ip tos screen 8
  ip tos printer 4
```

Overriding Configured Values Example

In the following example, the PU PUS1 uses the IP TOS precedence screen and printer values from the values provided in TN3270 server configuration mode. PUS2 uses the IP TOS screen and printer values defined in TN3270 server configuration mode. However, different values for IP precedence are provided for PUS2 under PU configuration mode.

```
interface channel 3/2
  tn3270-server
  ip precedence screen 6
  ip precedence printer 3
  ip tos screen 8
  ip tos printer 4
  pu PUS1      05D18009 172.28.1.101  token-adapter 0 AC rsap 08
  pu PUS2      05D18071 172.28.1.99   token-adapter 0 A4 rmac 4000.7470.00e7
  ip precedence screen 7
  ip precedence printer 0
```

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.

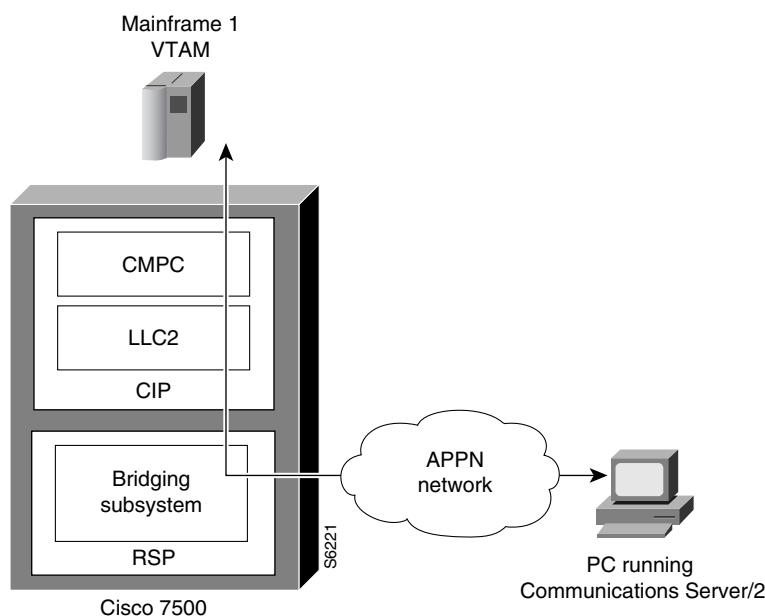
Refer to the following configuration examples to see how different networked systems can be configured:

- Connecting VTAM to a Remote PC with Communications Server/2 Example
- Connecting VTAM to the APPN NN on the CIP Example
- Connecting Two VTAM Nodes Using Two CIPs in the Same Router Example
- Connecting VTAM to the APPN NN on a Remote Router with DLUR Example
- TN3270 Server DLUR Running on the Same CIP Example

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

Figure 153 shows the physical components for this example. Figure 154 shows the various parameters for each component in the configuration example.

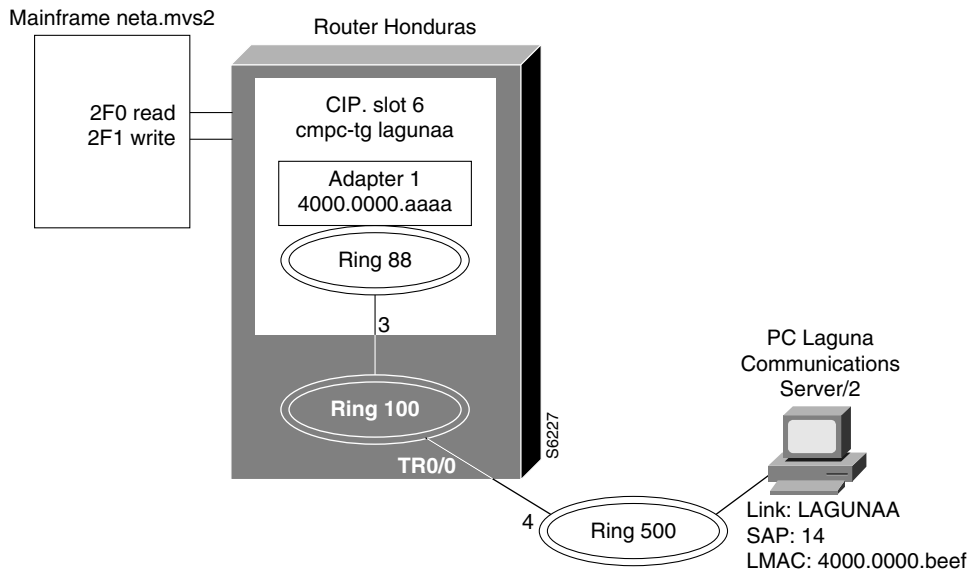
Figure 153 Topology for VTAM-to-Remote PC with Communications Server/2



In Figure 153, 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 154 Parameters for VTAM-to-Remote PC with Communications Server/2



The example in Figure 154 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.

Configuration for TRL Node LAGTRLA on MVS2

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

Configuration for Local Node LAGLNA on MVS2

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

Configuration for Honduras Router

```
microcode CIP flash slot0:johnchap/cip209-157.mpc
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 Channel6/2
  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
  
```

Activate the Configuration

To activate the configuration, issue the following commands from MVS2:

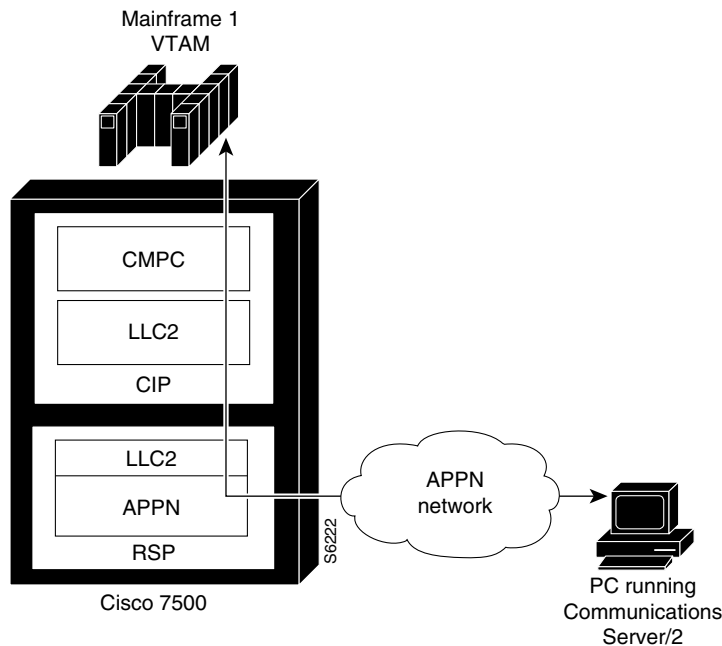
```

v net,act,id=lagtr1a,update=add
v net,act,id=lag1na
  
```

Connecting VTAM to the APPN NN on the CIP Example

Figure 155 shows the physical components for this example. Figure 156 shows the various parameters for each component in the configuration example.

Figure 155 Topology for VTAM-to-APPN NN Connection on the CIP



In Figure 156, 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.

Configuration for Local SNA Major Node LAGLNB

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

X
X

Configuration for Honduras Router

```
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 llc token-adapter 2 20 rmac 4000.0000.bbbb rsap 24
!
!
appn control-point NETA.HONDURAS
complete
!
appn port RSRBPORT rsrb
local-sap 24
desired-max-send-btu-size 4096
max-rcv-btu-size 4096
rsrb-virtual-station 4000.0000.bbbb 61 2 100
complete
!
appn link-station LAGUNAB
port RSRBPORT
lan-dest-address 4000.0000.beef 14
complete
router eigrp 109
network 172.18.0.0
```

Activate the Configuration

After all configurations are in place, the following commands can be used to start up the links. On the MVS system, enter the following commands:

```
v net,act,id=lagtrlb,update=add
v net,act,id=laglnb
```

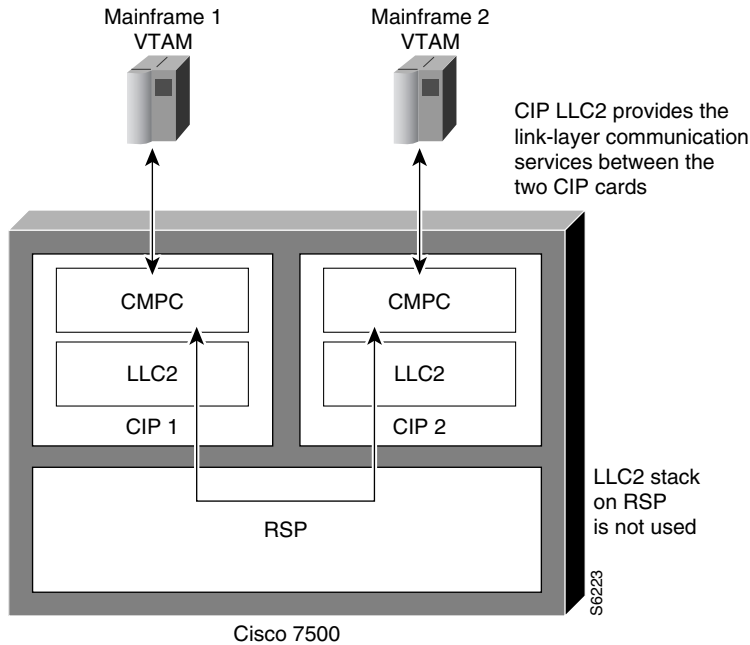
On the router, enter the following command from the global configuration mode:

```
appn start
```

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

Figure 157 shows the physical components for this example. Figure 158 shows the various parameters for each component in the configuration example.

Figure 157 Topology for VTAM-to-VTAM Connection

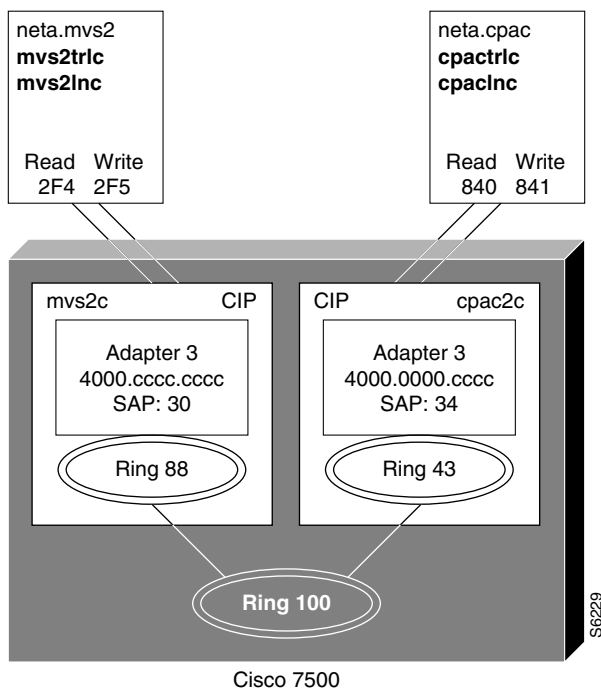


In Figure 157, the following activity occurs:

- 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 158 Parameters for VTAM-to-VTAM Connection



Differing solutions can be configured for the example shown in Figure 158. 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.

Configuration for mvs2trlc

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

Configuration for mvs2lnc

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

Configuration for cpactrlc

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

Configuration for cpac1nc

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

Configuration for the Router

```
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 1lc 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 1lc token-adapter 3 30 rmac 4000.0000.cccc rsap 34
```

Activate the Configuration

On the MVS system MVS2, enter the following commands to activate the configuration:

```
v net,act,id=mvs2trlc,update=add
v net,act,id=mvs2lnc
```

On the MVS system CPAC, enter the following commands to activate the configuration:

```
v net,act,id=cpactrlc,update=add
v net,act,id=cpac1nc
```

Connecting VTAM to the APPN NN on a Remote Router with DLUR Example

Figure 159 shows the physical components for the DLUS-to-DLUR configuration. Figure 160 shows the various parameters for each component in the configuration example.

Figure 159 Topology for VTAM-to-APPN NN on a Remote Router with DLUR Connection

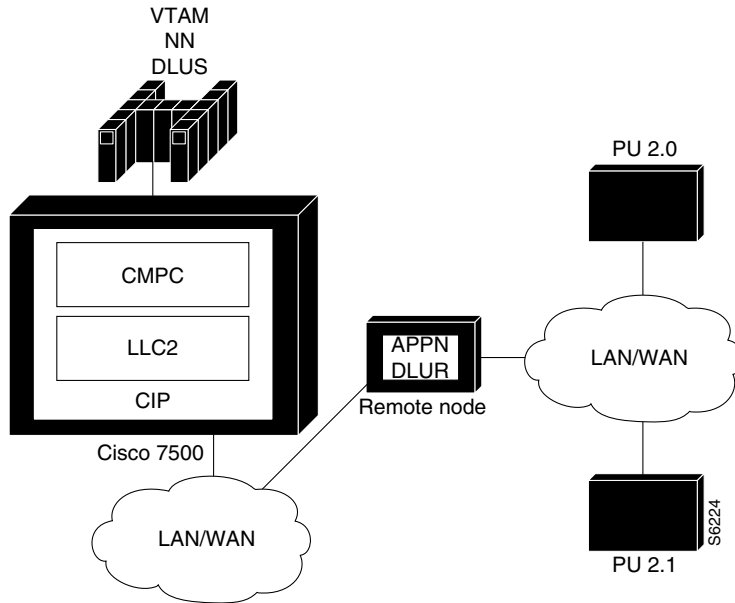
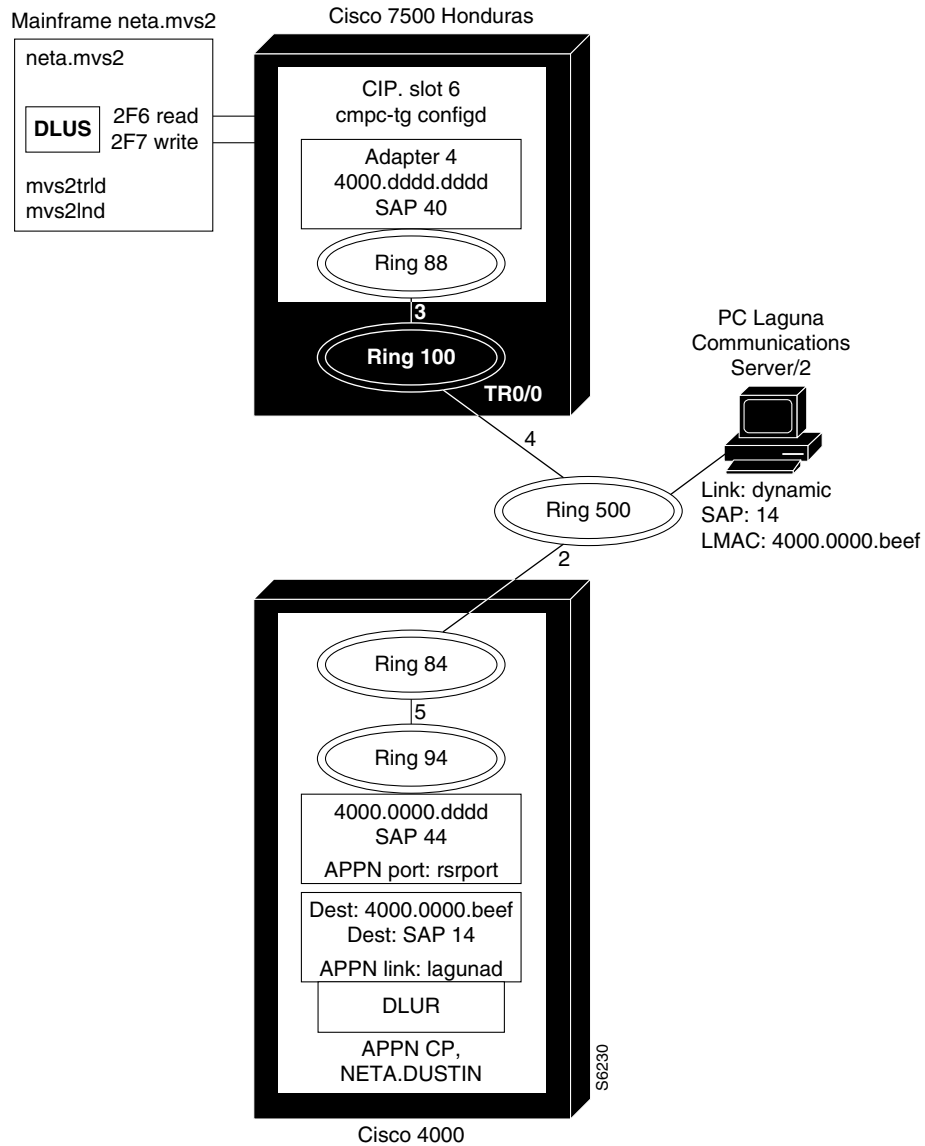


Figure 160 Parameters for VTAM-to-APPN NN on a Remote Router with DLUR Connection



In the example shown in Figure 160, 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.

Configuration for mvs2trld

```

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

Configuration for mvs2lnd

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

X
X

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
```

Configuration for 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
!
appn control-point NETA.DUSTIN
  dlus NETA.MVS2
  dlur
  complete
!
appn port RSRBPORT rsrp
  local-sap 44
  desired-max-send-btu-size 4096
  max-rcv-btu-size 4096
  rsrp-virtual-station 4000.0000.dddd 94 5 84
  complete
!
appn link-station LAGUNAD
  port RSRBPORT
  lan-dest-address 4000.0000.beef 14
  complete
!
appn link-station MVS2D
  port RSRBPORT
  lan-dest-address 4000.dddd.dddd 40
  complete
```

Activate the Configuration

On the MVS2 system, enter the following commands to activate the configuration:

```
v net,act,id=mvs2trld,update=add
v net,act,id=mvs2lnd
```

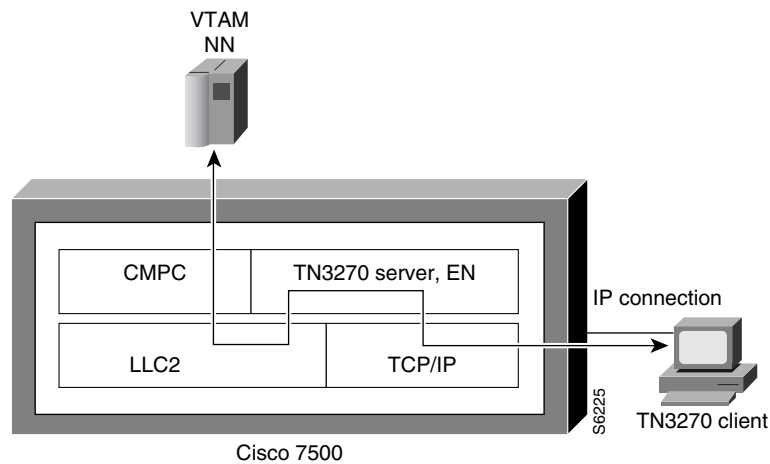
On the router Dustin, enter the following command from the global configuration mode:

```
appn start
```

TN3270 Server DLUR Running on the Same CIP Example

Figure 161 shows the physical components for this example. Figure 162 shows the various parameters for each component in the configuration example.

Figure 161 Topology for VTAM-to-TN3270 Server DLUR Running on the Same CIP Connection

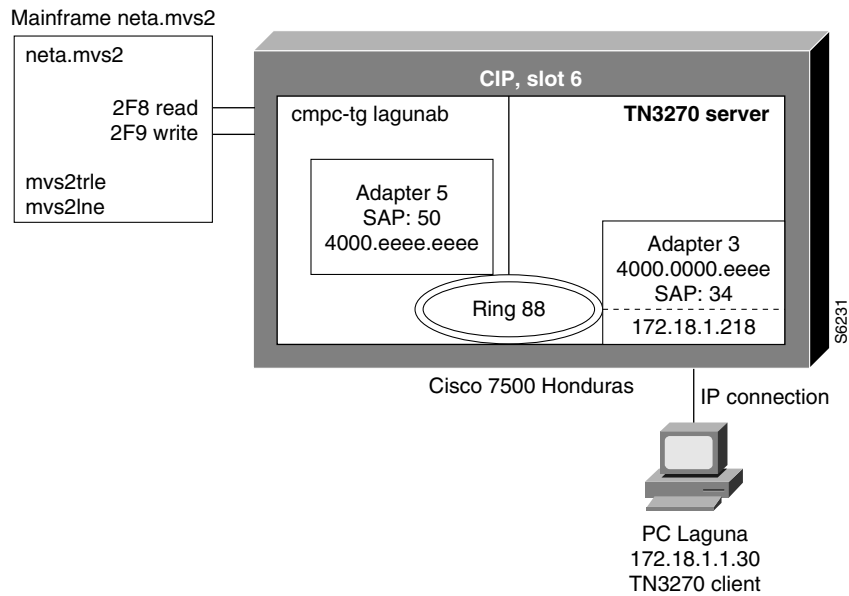


In Figure 161, the following activity occurs:

- The TN3270 server on the CIP takes on the role of an APPN EN running DLUR.
- The APPN NN in VTAM communicates with the CMPC driver over the channel.
- The CMPC driver on the CIP passes the data to the LLC2 stack on the CIP via a fast-path loopback driver to the TN3270 server on the CIP.
- The TN3270 server converts the 3270 data stream to a TN3270 data stream and forwards the packets to the IP TN3270 clients in the IP network.

The TN3270 server does not have to be in the same CIP as the CMPC driver.

Figure 162 Parameters for VTAM-to-TN3270 DLUR Running on the Same CIP Connection



The following configurations apply to the example shown in Figure 162.

Configuration for mvs2trle

```
MVS2TRE  VBUILD TYPE=TRL
MVS2TRLE TRLE LNCTL=MPC,MAXBFRU=8,REPLYTO=3.0,
           READ=(2F8),
           WRITE=(2F9)
```

Configuration for mvs2lne

```
MVS2NNE  VBUILD TYPE=LOCAL
MVS2PUE  PU     TRLE=MVS2TRLE,
           ISTATUS=ACTIVE,
           XID=YES,CONNTYPE=APPN,CPCP=YES
```

Configuration for swlagtn

```
SWLAGTN  VBUILD TYPE=SWNET,MAXGRP=10,MAXNO=10,MAXDLUR=10
LAGTNPU  PU     ADDR=01,                                     X
           MAXPATH=1,                                       X
           IDBLK=017,IDNUM=EFEED,                           X
           PUTYPE=2,                                         X
           MAXDATA=4096,                                     X
           LUGROUP=TNGRP1,LUSEED=LAGLU##
```

Configuration for tngrp1

```

TNGRP1E  VBUILD TYPE=LUGROUP
TNGRP1   LUGROUP
DYNAMIC  LU    DLOGMOD=D4C32XX3,                                X
           MODETAB=ISTINCLM, USSTAB=USSTCPIP, SSCPFM=USS3270
@        LU    DLOGMOD=D4C32784,                                X
           MODETAB=ISTINCLM, USSTAB=USSTCPIP, SSCPFM=USS3270

```

Additional Router Configuration for Router Honduras

```

interface Channel6/1
  cmpc C020 F8 CONFIGE READ
  cmpc C020 F9 CONFIGE WRITE
!
interface Channel6/2
  lan TokenRing 0
  source-bridge 88 3 100
  adapter 5 4000.eeee.eeee
  adapter 6 4000.0000.eeee
tn3270-server
dlur NETA.HOND327S NETA.MVS2
  lsap token-adapter 6 54
  link MVS2TN rmac 4000.eeee.eeee rsap 50
  pu TNPU 017EFEED 172.18.1.218
tg CONFIGE 11c token-adapter 5 50 rmac 4000.eeee.eeee rsap 54

```

Activate the Configuration

On the MVS system, enter the following commands to activate the configuration:

```

v net,act,id=mvstrle,update=add
v net,act,id=mvslne
v net,act,id=swhondpu
v net,act,id=swlagtn
v net,act,id=swhondcp
v net,act,id=tngrp1

```

On the router Honduras, enter the following command from TN3270 configuration mode:

```
no shutdown
```

