



Configuring Cisco Mainframe Channel Connection Adapters

This chapter provides an introduction to the Cisco Mainframe Channel Connection Adapters (CMCCs) and provides information about the basic tasks required to configure any CMCC adapter on a Cisco router. This information is described in the following sections:

- [Overview of the CMCC Adapters, page 1](#)
- [Preparing to Configure a CMCC Adapter, page 6](#)
- [CMCC Adapter Configuration Task List, page 16](#)
- [Monitoring and Maintaining a CMCC Adapter, page 23](#)
- [CPA Microcode Load Configuration Examples, page 29](#)

Details about configuring the Cisco IOS features that are supported by the CMCCs are described in the related chapters of this publication. For more information about the functions supported on a CMCC, see the [“Supported Environments” section on page 5](#).

For hardware technical descriptions and information about installing the router interfaces, refer to the hardware installation and maintenance publication for your product. For a complete description of the CMCC adapter commands in this chapter, refer to the *Cisco IOS Bridging and IBM Networking Command Reference* (Volume 2 of 2). To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

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

Overview of the CMCC Adapters

A CMCC adapter is installed in a Cisco router to provide IBM channel attachment from the router to a mainframe host. The Cisco family of CMCC adapters consists of two basic types of adapters:

- [Channel Interface Processor \(CIP\)](#)—Installed on Cisco 7000 with RSP7000 and Cisco 7500 series routers
- [Channel Port Adapter \(CPA\)](#)—Installed on Cisco 7200 series routers



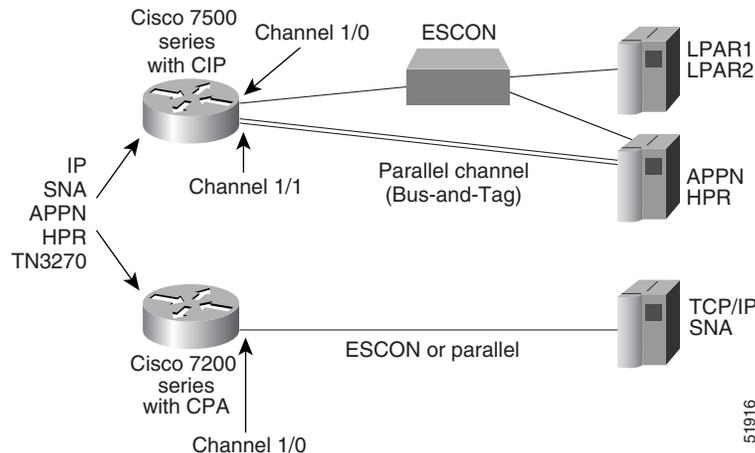
Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Each type of adapter (CIP or CPA) supports both ESCON and parallel channel attachment to the host and can eliminate the need for a separate front-end processor (FEP).

All CMCC adapters support the full range of channel software applications available in the Cisco IOS software including support for the Common Link Access to Workstation (CLAW) protocol, TCP/IP offload, IP host backup, Cisco SNA (CSNA), Cisco Multipath Channel (CMPC), Cisco Multipath Channel+ (CMPC+), and the TN3270 server.

Figure 1 shows the type of channel connections and environments supported by the CMCC adapters.

Figure 1 Cisco Mainframe Channel Connection Adapters



The following topics in this section provide additional overview information about the CMCC adapters:

- [Channel Interface Processor, page 2](#)
- [Channel Port Adapter, page 3](#)
- [Differences between the CIP and CPA, page 4](#)
- [Supported Environments, page 5](#)

Channel Interface Processor

The CIP for the Cisco 7000 with RSP7000 and Cisco 7500 series routers is designed for high-end network environments that demand high-performance, high-port density, and high-capacity solutions.

The CIP provides support for IBM ESCON and bus-and-tag parallel channel attachment using the following types of interfaces:

- ESCON Channel Adapter (ECA)
- Parallel Channel Adapter (PCA)

A single CIP can support up to two physical channel interfaces in any combination of either PCA or ECA. Each CIP is pre-configured with the appropriate channel adapters at manufacturing time.

The Cisco 7000 with RSP7000 and Cisco 7500 series routers support online insertion and removal (OIR), which allows you to install or remove CIPs while the system is operating.

Benefits of the CIP

The CIP provides the following primary benefits:

- **Maximum throughput for every application**—For the individual applications supported on the CIP, the CIP configured with 128 MB of memory offers maximum throughput. For example, the number of users supported for TCP/IP offload is 10,000 and the number of LLC2 session supported is 6000.
- **Scalability**—The CIP supports up to 22 channel connections on Cisco 7000 with RSP7000 and Cisco 7500 series routers.
- **Multiple interface support**—The CIP supports multiple ESCON and bus-and-tag channel interfaces.
- **Higher memory capacity**—The CIP offers a high memory capacity of 128 MB that can be useful for software applications, such as the TN3270 server, that have a large number of sessions.
- **Port density**—The CIP contains two channel interfaces in contrast to the CPA's single channel interface.

Channel Port Adapter

The CPA is available for the Cisco 7200 series routers. The CPA expands the value of Cisco's IBM channel solution by providing channel connectivity to mid-range mainframe configurations.

The CPA is a standard, single-width port adapter that provides support for IBM ESCON and bus-and-tag parallel channel attachment using the following types of interfaces:

- [ESCON Channel Port Adapter \(ECPA\)](#)
- [Parallel Channel Port Adapter \(PCPA\)](#)

Each CPA provides a single channel interface (with a single I/O connector) for Cisco 7200 series routers. In some situations, this eliminates the need for a separate FEP.

The only differences between CMCC software applications running on the CIP and a CPA are performance and capacity. The performance difference is based upon differences in the internal bus architecture of a CIP and a CPA, and the capacity difference is based on the difference in maximum memory configurations (128 MB for CIP and 32 MB for CPA). For more information about differences between the CIP and CPA, see the [“Differences between the CIP and CPA” section on page 4](#).

The Cisco 7200 series router supports online insertion and removal (OIR), which allows you to install or remove port adapters while the system is operating.



Note

In this chapter, references to CPA correspond to both the ECPA and the PCPA.

Benefits of the CPA

The CPA provides the following primary benefits:

- **Cost-effective**—A CPA in a Cisco 7200 series router provides industry-leading price performance.
- **Simplified migration path**—The CPA and CIP microcode support the same features and applications, enabling seamless migration for network expansion.
- **Flexibility**—The Cisco 7200 series router platform provides a great number of features and capabilities that can be used in conjunction with a CPA.

ESCON Channel Port Adapter

An ECPA is classified as a high-speed port adapter providing a single ESCON physical channel interface. Current Cisco 7200 configuration guidelines recommend using no more than three high-speed port adapters in a single Cisco 7200 router.

Refer to the *Cisco 7200 Series Port Adapter Hardware Configuration Guidelines* publication for more details.

Parallel Channel Port Adapter

A Parallel Channel Port Adapter (PCPA) provides a single parallel channel physical interface supporting 3.0 or 4.5 Mbps data transfer rates.

Differences between the CIP and CPA

Table 1 illustrates the differences between the CMCC adapters.

Table 1 Differences Between the CIP and the CPA

Product Differences	CIP	ECPA	PCPA
Router platform	Cisco 7500 Cisco 7000 with RSP7000	Cisco 7200	Cisco 7200
Channel interfaces	ESCON Parallel	ESCON	Parallel
Maximum number of interfaces	2	1	1
Maximum memory	128 MB	32 MB	32 MB
Cisco IOS release support	Cisco IOS Release 10.2 and later	Cisco IOS Release 11.3(3)T and later	Cisco IOS Release 11.3(3)T and later
Virtual port number	2	0	0
Channel interface state tracking (HSRP, SNMP alerts)	Yes	Disabled—Use the state-tracks-signal command to enable	Disabled—Use the state-tracks-signal command to enable

Supported Environments

The CMCC adapters provide support for the following environments:

- TCP/IP environments using CLAW—The Cisco IOS software implements the CLAW channel protocol to transport data between the mainframe and a CMCC adapter in TCP/IP environments.

For more information about configuring a CMCC adapter for CLAW, see the “Configuring CLAW and TCP/IP Offload Support” chapter in this publication.

- TCP/IP offload environments—TCP/IP offload support on a CMCC adapter provides the capability to significantly reduce the amount of overhead processing that an IBM mainframe (running the Multiple Virtual Storage (MVS), Virtual Machine (VM), or Transaction Processing Facility (TPF) operating system) must execute for handling of TCP/IP packets.

For more information about configuring a CMCC adapter to support TCP/IP offload, see the “Configuring CLAW and TCP/IP Offload Support” chapter in this publication.

- IP host backup environments—IP host backup support on a CMCC adapter allows the mainframe operating system to be moved from one mainframe to another without requiring a change to the router configuration at the time of the move.

For more information about configuring a CMCC adapter for IP host backup support, see the “Configuring CLAW and TCP/IP Offload Support” chapter in this publication.

- CSNA environments—The CSNA feature on a CMCC adapter provides support for Systems Network Architecture (SNA) protocols to the IBM mainframe.

For more information about configuring a CMCC adapter for CSNA, see the “Configuring CSNA and CMPC” chapter in this publication.

- Cisco Multipath Channel (CMPC) environments—CMPC is Cisco System’s implementation of IBM’s MultiPath Channel (MPC) feature on a CMCC adapter. CMPC allows VTAM to establish Advanced-Peer-to-Peer Networking (APPN) connections using both High Performance Routing (HPR) and Intermediate Session Routing (ISR) through channel-attached router platforms.

For more information about configuring a CMCC adapter for CMPC, see the “Configuring CSNA and CMPC” chapter in this publication.

- Cisco Multipath Channel+ (CMPC+) environments—CMPC+ is Cisco System’s implementation of IBM’s Multipath Channel+ feature on a CMCC adapter. CMPC+ supports the MPC+ features and protocols necessary to support IP and enables High Performance Data Transfer (HPDT). It allows TCP/IP connections to the host through a CMCC adapter, using either the TCP/IP stack or the High Speed Access Services (HSAS) IP stack.

For more information about configuring a CMCC adapter for CMPC+, see the “Configuring CMPC+” chapter in this publication.

- TN3270 server environments—The TN3270 server feature on a CMCC adapter provides a mapping between an SNA 3270 host and a TN3270 client connected to a TCP/IP network. From the perspective of an SNA 3270 host connected to the CMCC adapter, the TN3270 server is an SNA device that supports multiple PUs, with each PU supporting up to 255 logical units (LUs). From the perspective of a TN3270 client, the TN3270 server is a high-performance Telnet server that supports Telnet connections, negotiation and data format.

For more information about configuring a CMCC adapter to support the TN3270 server, see the “Configuring the TN3270 Server” chapter in this publication.

Preparing to Configure a CMCC Adapter

This section provides guidelines to consider when preparing to configure a CMCC adapter. It includes limitations on the number of entities that you can configure on a CMCC adapter and provides information about correlating host configuration elements with your router configuration.

These guidelines are provided in the following subsections:

- [CMCC Configuration Guidelines, page 6](#)
- [SAP Configuration Guidelines, page 6](#)
- [Mainframe Host Configuration Considerations, page 9](#)

CMCC Configuration Guidelines

Each CMCC adapter can support the following number of configuration entities:

- A CMCC adapter can have multiple internal LANs, up to a maximum of 18.



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

- A CMCC adapter can have multiple internal adapters, up to a maximum of 18.
- Up to 127 Service Access Points (SAPs) per internal adapter, with the Null Link Layer Service Access Point (LSAP) 0x00 reserved for the underlying MAC service access point (which is usually being used for the exchange of test frames during station discovery).



Note Several SAP values are reserved for particular protocols by the IEEE, which effectively reduces the number of SAPs available outside the router to a total of 64. This is important to remember for SAP values that you configure on the CMCC adapter for communication with network entities external to the router, so that you avoid SAP conflicts. For communication outside the router, SAP values in the range of hexadecimal 04 to 9E are recommended in increments of 4. For additional guidelines on configuring SAPs, see the [“SAP Configuration Guidelines” section on page 6](#).

SAP Configuration Guidelines

Configuring Cisco IOS software application features on a CMCC adapter for communication with the mainframe host requires the configuration of SAPs. SAPs are used by the CMCC adapter to establish communication with the Virtual Telecommunications Access Method (VTAM) on the mainframe and to identify Logical Link Control (LLC) sessions on a CMCC’s internal adapter.

To uniquely identify an LLC session, a combination of the following four entities are used in a CMCC adapter. This combination of values is sometimes referred to as the *MAC/SAP quadruple*:

- Source MAC address
- Destination MAC address
- Source SAP value
- Destination SAP value

When you are configuring SAPs on a CMCC, it is important to remember how the SAP is used in combination with these other entities to establish a unique LLC session. In order for the LLC session to be unique, there cannot be an LLC session that duplicates all four values of the MAC/SAP quadruple. In fact, only one of the values needs to be unique to qualify the particular session. Understanding this requirement is a key factor in successfully configuring a CMCC adapter to support multiple entities.

To establish the LLC sessions between external network traffic and a feature such as CSNA on a CMCC adapter in the router, an internal LAN along with an internal adapter is defined. MAC addresses are established for the internal adapters that are defined on the internal LAN in the CMCC. An internal LAN can have multiple internal adapters, and therefore, multiple MAC addresses associated with it. When LLC sessions on the CMCC are established using the same internal adapter (and therefore, the same MAC address) and are destined for the same SAP and MAC address, the source SAP must uniquely identify the session.

Consider the following guidelines when configuring SAPs on a CMCC adapter:

- If the SAP is going to be used for communication external to the router, use the following guidelines when specifying the SAP value:
 - Avoid SAPs reserved for well-known protocols.
 - Avoid a SAP of 00, which is reserved for the MAC SAP often used in the exchange of a test frame.
 - Specify SAP values in multiples of 4.

**Note**

Some of the well-known SAP values for protocols are hexadecimal AA for SNAP, E0 for IPX, F0 for NetBIOS. For more information about some of these reserved SAP values, see [Table 2](#) and [Table 3](#).

- If the SAP is going to be used for communication within the router, you can maximize the number of available SAPs on an internal adapter by using multiples of 2 up to a total of 128. The CMCC adapter does not enforce the well-known values reserved for protocols and accepts any even SAP value.
- SAP 4 is commonly used as the SAP for SNA.
- CSNA can activate a maximum of 128 SAPs on the CMCC at any given time. If you are configuring the TN3270 server using a CSNA connection, the total number of SAPs open on the host plus the number of SAPs defined for PUs on the TN3270 server must be less than or equal to 128.

Reference for IEEE and Manufacturer Administered SAPs

The information in [Table 2](#) and [Table 3](#) is useful as a reference for understanding some of the administered LSAPs that might be encountered on the network external to the router. Remember that these are not values that the CMCC adapter enforces, and they do not specifically pertain to limitations in configuring the CMCCs.

Table 2 *LSAPs Administered by IEEE*

LSAP	Description
00	Null
02	Individual LLC Sublayer Management function
03	Group LLC Sublayer Management function
06	ARPANET IP
0E	Proway Network Management and Initialization
42	IEEE 802.1 Bridge Spanning-Tree Protocol
4E	EIA RS-511 Manufacturing Message Service
7E	Cisco IOS 8208 (X.25 over IEEE 802.2)
8E	Proway Active Station List
AA	Subnetwork Access Protocol (SNAP)
FE	Cisco IOS Network Layer Protocol
FF	Global LSAP

Table 3 *LSAPs Implemented by Manufacturer*

LSAP	Description
04	IBM SNA Path control (individual)
05	IBM SNA Path control (group)
18	Texas Instruments
80	XNS
86	Nestar
98	ARPANET (ARP)
BC	Banyan Vines
E0	Novell
F0	IBM NetBIOS
F4	IBM LAN Management (individual)
F5	IBM LAN Management (group)
F8	IBM Remote Program Load (RPL)
FA	Ungermann-Bass

Mainframe Host Configuration Considerations

Configuring a CMCC adapter and its associated features requires that you perform tasks for configuration of the mainframe and the router sides of the network environment.

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

This section contains information for both the network engineer and the MVS systems programmer to properly configure the channel subsystem for the router and includes the following topics:

- [Defining the Channel Subsystem for the Router, page 9](#)
- [Correlating Channel Configuration Parameters, page 10](#)

Other chapters in this publication that discuss configuration of supported features on a CMCC adapter provide additional information about host-related and router-related configuration tasks associated with that feature.

Defining the Channel Subsystem for the Router

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

The following sample configuration shows the CHPID, CNTLUNIT, and IODEVICE statements that might be defined in an IOCP file for parallel channels and ESCON channels on the CIP or CPA. The parameters in bold indicate values that might vary by the type of channel being defined.

```
*****
* Parallel channel--CIP or CPA may be subchannel addresses 580-58F
*****
CHPID    PATH=( (21) ), TYPE=BL
CNTLUNIT CUNUMBER=0580, PATH=(21), UNIT=3088, UNITADD=( (80,16) ), SHARED=N, PROTOCOL=S4
IODEVICE ADDRESS=(580,16), CUNUMBER=(0580), UNIT=CTC
*****
* ESCON channel--CIP or CPA may be subchannel addresses D00-D0F
*****
CHPID    PATH=( (1F) ), TYPE=CNC
CNTLUNIT CUNUMBER=0D00, PATH=(1F), UNIT=3172, UNITADD=( (00,16) )
IODEVICE ADDRESS=(D00,16), CUNUMBER=(0D00), UNIT=SCTC
*****
* ESCON channel with ESCON director--CIP or CPA may be subchannel addresses 700-70F
*****
CHPID    PATH=( (1C) ), TYPE=CNC, SWITCH=01
CNTLUNIT CUNUMBER=0700, PATH=(1C), UNIT=3172, UNITADD=( (00,16) ), LINK=(C4)
IODEVICE ADDRESS=(700,16), CUNUMBER=(0700), UNIT=SCTC
```

The subchannel parameters differ by the type of channel that you are defining. For example, to support a CMCC parallel channel always use the channel type BL for block multiplexor, data streaming mode. ESCON channels use a channel type of CNC for Native ESCON (or type CVC might be used if an ESCON Converter is in use).

In addition, the UNIT types specified in the CNTLUNIT and IODEVICE statements differ for parallel and ESCON channels. The ESCON director also implements the additional parameters for SWITCH and LINK to identify a number for the ESCON director and specify the port in the ESCON director to which the router is connected.

**Note**

In the format of a real IOCP file, all of the CHPID, CNTLUNIT, and IODEVICE statements are organized into separate groups, and are not listed one after the other as shown. You can correlate the statements in a real IOCP file by using the PATH parameter to associate the CHPID definition with a corresponding CNTLUNIT statement, and using the CUNUMBER parameter to correlate the IODEVICE and the CNTLUNIT statements.

Correlating Channel Configuration Parameters

This section provides detailed information about correlating values found in the VM and MVS system I/O configuration files with the arguments required in the **claw**, **csna**, **cmpe**, and **offload** interface configuration commands on the CMCC adapter.

To properly configure the channel subsystem on the router side you need to know the following information:

- Channel path, including any of the following values when applicable:
 - ESCON director output port to the mainframe
 - LPAR number
 - CUADD value
- Unit address

This information is defined on the host in the IOCP. In versions of MVS 5.2 and later, an HCD might be used as an alternative method to define this information. To locate this information or to configure it on the mainframe host, contact your site's systems programmer.

Determining the Path Argument

When you define CLAW, CSNA, CMPC or CMPC+, and Offload parameters on a CMCC adapter, 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 using bus and tag cables, or more complex when the path includes an ESCON director switch or multiple image facility (EMIF) support.

This example shows the syntax for the CMCC adapter commands that require subchannel information, which is configured in the *path* and *device* arguments of the following commands:

```
claw path device ip-address host-name device-name host-app device-app [broadcast]
```

```
csna path device [maxpiu value] [time-delay value] [length-delay value]
```

```
cmpe path device tg-name {read | write}
```

```
offload path device ip-address host-name device-name host-ip-link device-ip-link  
host-api-link device-api-link [broadcast] [backup]
```

The *path* argument in each of the commands is a four-digit hexadecimal value that concatenates the path value (2 digits), EMIF partition number (1 digit), and control unit logical address (1 digit) as described in [Table 4](#).

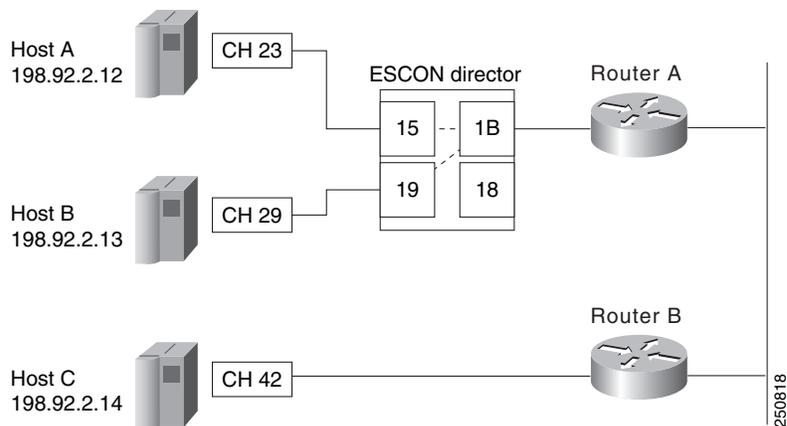
For bus and tag channel connections, the *path* value is always 0100. You do not need the information in [Table 4](#) to determine the *path* value.

Table 4 Breakdown of Path Argument Values

Path Argument Breakdown	Values	Description
Path digits	01–FF	For a directly attached ESCON channel or any Parallel channel this value is 01, <i>unless</i> a systems programmer has configured another value. For a channel attached through an ESCON director switch, specify the outbound port number in the first two digits of the <i>path</i> argument. This is the port which, from the router point of view, exits the switch and attaches to the host.
EMIF partition number digit	0–F	For a Parallel channel, this value is 0. For a directly attached ESCON channel, the value might be non-zero. If the host is running in Logical Partition (LPAR) mode and the CHPID is defined as shared, specify the partition number in this digit of the <i>path</i> argument.
Control unit logical address digit	0–F	For a Parallel channel, this value is 0. For a directly attached ESCON channel, the value might be non-zero. If the CUADD value is specified in the IOCP CNTLUNIT statement, specify that value in this digit of the <i>path</i> argument.

Consider the network configuration in [Figure 2](#), where 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. Note that the path between Host A and Host B is dynamically switched within the ESCON director. Host C is attached directly to Router B through path 42.

Figure 2 System with an ESCON Director Switch and a Directly Attached Channel



The IOCP control unit statements to configure the channel paths shown in [Figure 2](#) might look similar to the following sample configuration statements:

Sample IOCP Control Unit Statements for Host A

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

Sample IOCP Control Unit Statements for Host B

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

Sample IOCP Control Unit Statements for Host C

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



Note

A mainframe systems programmer can provide you with the actual IOCP values for your site's configuration.

Using the above IOCP values as an example and following the guidelines provided in [Table 4](#), the following *path* argument is used as shown in the example **csna** or **cmpc** commands for the two channel attachments to Router A:

```
csna 150F
csna 190A
```

```
cmpc 150F
cmpc 190A
```

In [Figure 2](#) the ESCON director ports 15 and 19 are the channel attachments from the ESCON director to each host. Note that the outbound ports from the ESCON director to the host are the values used in the first 2 digits of the *path* argument.

The following *path* argument is used for the directly attached channel to Router B, as shown in the example **csna** or **cmpc** commands:

```
csna 0100
```

```
cmpc 0100
```

Determining the Device Argument

When you define CLAW, CSNA, CMPC or CMPC+, and Offload parameters on a CMCC adapter, you must supply path information and device address information to support routing on an IBM channel. To determine the value for the *device* argument in the **claw**, **csna**, **cmpc**, or **offload** interface configuration commands on the CMCC adapter, find the UNITADD parameter in the host IOCP definition.

The UNITADD parameter in the CNTLUNIT macro of the IOCP file defines the valid range for device addresses. For example, a UNITADD parameter of (00,64) means that the first valid device address is 00 and the number of devices is 64. In the hexadecimal notation used by channel configuration commands this translates to a range of 00 to 3F.

Using that unit address information, the example **csna** and **cmpc** commands now add values for the *device* arguments to the two channel attachments to Router A:

```
csna 150F 00
csna 190A 01
```

```
cmpc 150F 02
cmpc 150F 03
```

```
cmpc 190A 03
```

```
cmpc 190A 04
```

The following example **csna** and **cmpc** commands show the *path* and *device* arguments for the directly attached channel to Router B:

```
csna 0100 00
```

```
cmpc 0100 01
cmpc 0100 02
```



Note

In this example, if you configure CSNA and CMPC on the same CMCC port then you must use unique unit addresses. Also, CMPC requires two unit addresses for the *device* argument. One unit address is used in a **cmpc** command to define the read subchannel, and one is used in a second **cmpc** command to define the write subchannel. The device addresses do not need to be consecutive.

Determining the Device Argument from an IODEVICE Address

When you have a directly attached channel, the mainframe systems programmer might provide you with a system IODEVICE ADDRESS that you can use to determine the required subchannel information. In this case, you must work backwards through the IOCP file to locate the proper *device* argument value for the CMCC adapter interface commands.

Example 1

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

```
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))
**** A valid value for the device argument is the UNITADD value of 00
```

From this example, the **csna** command would be similar to the following:

```
csna 0100 00
```

Example 2

In this example the mainframe systems programmer provides an available IODEVICE ADDRESS of 350, which does not directly correspond to a value in the IOCP file, but is within a range of 64 addresses beginning at device address 340 (as shown in the IODEVICE ADDRESS=(340,64) statement). The value 350 is at an offset of 10 from the beginning value of 340 in this statement:

```
IODEVICE ADDRESS=(0340,64),CUNUMBR=(0008),UNIT=SCTC
IODEVICE ADDRESS=(0380,64),CUNUMBR=(0009),UNIT=SCTC
**** Address 350 is in the range of 64 addresses beginning at address 340 corresponding
**** to CUNUMBR 0008

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

To determine the unit address for the *device* argument value in the **claw**, **csna**, **cmpc** or **offload** commands, you must use the same offset that you determined for the IODEVICE ADDRESS and calculate the UNITADD parameter from the corresponding CNTLUNIT statement. In this example, CUNUMBR=0008 is the corresponding CNTLUNIT statement for IODEVICE ADDRESS 350. The first

unit address in that CNTLUNIT statement is 40 (in parameter UNITADD), which correlates to the first IODEVICE ADDRESS of 340. To determine the corresponding unit address for IODEVICE ADDRESS 350, determine the value at offset 10 from 40, which is 50.

In this example, the **csna** command would be similar to the following:

```
csna 0100 50
```

**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.

**Tip**

You can prevent configuration problems and more readily correlate configuration between the router and the host if you follow the convention of using the last two digits of the starting IODEVICE ADDRESS as the starting value for the range of unit addresses in the UNITADD parameter of the CNTLUNIT statement. For example, if you use IODEVICE ADDRESS=(410,8) then use “10” as the beginning value of the unit address as in UNITADD=((10,8)). To avoid confusion and potential configuration errors, do not specify IODEVICE ADDRESS=(410,8) and then begin the unit addresses at value 00.

Disabling the Missing Interrupt Handler

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

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

This section includes the following topics:

- [Disabling the MIH on Mainframes Running MVS, page 14](#)
- [Disabling the MIH on Mainframes Running VM, page 15](#)

For additional information about disabling the MIH, 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).

Disabling the MIH on Mainframes Running MVS

To disable the MIH on an MVS host, you need to configure a statement in the IECIOS_{xx} member of the SYS1.PARMLIB partitioned dataset. To properly identify the IECIOS_{xx} member to use, there must be a corresponding statement IOS=_{xx} in the member IEASYS00 (where 00 is the default suffix).

**Note**

The statement IOS=_{xx} specifies that _{xx} is the suffix of the IECIOS member that contains the configuration. For example, the statement IOS=01 points to the IECIOS01 member. If this statement is not included in the IEASYS file, you can specify it dynamically using the **/SET IOS=_{xx}** command on the command line. For more information, see your site’s systems programmer.

To disable the MIH on an MVS host, perform the following steps:

- Step 1** Type the following statement in the IECIOS.*xx* member of SYS1.PARMLIB, where *yyy-yyy* specifies the range of unit addresses for which you want to disable the MIH:

```
MIH TIME=00:00:00, DEV=(yyy-yyy)
```

This configures the MVS host to disable the MIH every time that MVS is restarted (an Initial Program Load (IPL) is performed).

- Step 2** To dynamically change the MIH value for the currently active MVS operating system, issue the following command at the command line:

```
/SETIOS MIH DEV=xxx, TIME=00:00
```

- Step 3** To display the currently enabled MIH value, issue the following command at the command line:

```
/D IOS,MIH
```

**Note**

If you are using Dynamic Reconfiguration Management (DRM), type DYNAMIC=NO in the device statement. This value can be YES for IBM TCP/IP version 3.2.

Disabling the MIH on Mainframes Running VM

To disable the MIH on a VM host, you need to configure a statement in the PROFILE EXEC for the AUTOLOG1 userid (or equivalent userid for your site).

To disable the MIH on a VM host, perform the following steps:

- Step 1** Type the following statement in the PROFILE EXEC of the AUTOLOG1 (or equivalent) userid, where *yyy-yyy* specifies the range of unit addresses for which you want to disable the MIH:

```
SET MITIME yyy-yyy 00:00
```

or

```
SET MITIME yyy-yyy OFF
```

This configures the VM host to disable the MIH every time that VM is restarted (an Initial Program Load (IPL) is performed).

- Step 2** To dynamically change the MIH value for the currently active VM operating system, issue either of the commands shown in Step 1 at the command line.

- Step 3** To display the currently enabled MIH value, issue the following command at the command line:

```
Q MITIME
```

**Note**

For VM or MVS Guests under VM, code V=R (Real mode) for the Guest so that the CLAW channel programs build properly. For more information, see your site's systems programmer.

CMCC Adapter Configuration Task List

This section describes some of the global tasks that apply to configuring any CMCC adapter. Information about configuring features on a CMCC adapter are described in the related chapters of this guide.

This section includes the following configuration tasks:

- [Loading the CMCC Adapter Microcode Image, page 16](#)
- [Selecting the Interface, page 21](#)
- [Selecting a Data Rate for the Parallel Channel Interfaces, page 22](#)
- [Configuring Channel Interface Tracking for HSRP or SNMP Alerts, page 23](#)

See the “CPA Microcode Load Configuration Examples” section on page 29 for examples.

Loading the CMCC Adapter Microcode Image

This section provides information on loading, upgrading and verifying the microcode images for the CIP and CPA in the following topics:

- [Loading the CIP Microcode Image for All Adapters in the Router, page 16](#)
- [Upgrading the CIP Microcode Image, page 18](#)
- [Upgrading the CPA Microcode Image for All Adapters in the Router, page 19](#)
- [Upgrading the CPA Microcode Image for a Particular Adapter, page 20](#)
- [Verifying the CIP and CPA Microcode Image, page 20](#)

Loading the CIP Microcode Image for All Adapters in the Router

Beginning with Cisco IOS 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 Switch Processor (RSP) card to use the IBM channel-attachment features in Cisco IOS 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 Release 11.1 and later.

Use the commands in this section if you are loading the CIP microcode image for the first time, or for all adapters in your router.



Caution

Using the **microcode reload** command as shown in step 5 forces a microcode reload on all adapters in the router and shuts down the router. Do not use this command if you are on a production network and are not prepared for a router outage.

To prepare the CIP, use the following commands beginning in privileged EXEC command mode:

	Command	Purpose
Step 1	Router> enable	Enters the privileged EXEC mode command interpreter.
Step 2	Router# copy tftp:filename [bootflash: slot0: slot1:] filename	<p>Copies the CIP microcode image from a server to either of the Flash memory cards. The source of the file is tftp:filename.</p> <p>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.</p>
Step 3	Router# configure terminal	From privileged EXEC command mode, enters global configuration mode and specifies that the console terminal is the source of the configuration subcommands.
Step 4	Router(config)# microcode cip flash slotn:cipxx-yy or Router(config)# microcode cip flash bootflash:cipxx-yy	<p>Configures the router to load the Flash image to the CIP:</p> <ul style="list-style-type: none"> • Enters global configuration mode and specifies that the CIP microcode loads from a Flash card in router slot <i>n</i> or from embedded Flash. • Loads the image from Flash to the CIP card.
Step 5	Router(config)# microcode reload	<p>Forces a microcode reload for all adapters in the router.</p> <p>Note This command shuts down the router if you are on a live network.</p>
Step 6	Router(config)# end	Exits global configuration mode.
Step 7	Router# copy running-config startup-config	Saves the running configuration as the new startup configuration in NVRAM.

Upgrading the CIP Microcode Image

Beginning with Cisco IOS 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 RSP card to use the IBM channel-attachment features in Cisco IOS 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 Release 11.1 and later.

Use the commands in this section if you are upgrading the CIP image in your router.

To upgrade the CIP microcode, use the following commands beginning in privileged EXEC command mode:

	Command	Purpose
Step 1	Router> enable	Enters the privileged EXEC mode command interpreter.
Step 2	Router# copy tftp:filename [bootflash: slot0: slot1:] filename	Copies the CIP microcode image from a server to either of the Flash memory cards. The source of the file is tftp:filename . 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.
Step 3	Router# configure terminal	From privileged EXEC command mode, enters global configuration mode and specifies that the console terminal is the source of the configuration subcommands.
Step 4	Router(config)# microcode cip flash slotn:cipxx-yy or Router(config)# microcode cip flash bootflash:cipxx-yy	Configures the router to load the Flash image to the CIP: <ul style="list-style-type: none"> Enters global configuration mode and specifies that the CIP microcode loads from a Flash card in router slot <i>n</i> or from embedded Flash. Loads the image from Flash to the CIP card.
Step 5	Router(config)# end	Exits global configuration mode.
Step 6	Router# copy running-config startup-config	Saves the running configuration as the new startup configuration in NVRAM.

Upgrading the CPA Microcode Image for All Adapters in the Router

The CPA microcode image is preloaded on Flash memory cards for Cisco 7200 series routers for Cisco IOS Release 11.3(3)T and later. You may be required to copy a new image to Flash memory when a new microcode image becomes available. Use the commands in this section if you are upgrading or loading a microcode image other than the default image for all adapters in the router.



Caution

Using the **microcode reload** command as shown in Step 5 forces a microcode reload on all interfaces in the router and shuts down the router. Do not use this command if you are on a production network and are not prepared for a router outage.

To prepare the CPA, use the following commands beginning in privileged EXEC command mode:

	Command	Purpose
Step 1	Router> enable	Enters the privileged EXEC mode command interpreter.
Step 2	Router# copy tftp:filename [bootflash: slot0: slot1:] <i>filename</i>	Copies the CPA microcode image from a server to either of the Flash memory cards. The source of the file is tftp:filename . 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.
Step 3	Router# configure terminal	From privileged EXEC command mode, enters global configuration mode and specifies that the console terminal is the source of the configuration subcommands.
Step 4	Router(config)# microcode { ecpa pcpa } slotn:xcpaxx-yy	Loads the microcode from an individual microcode image that is stored as a file on a Flash memory card on a CPA adapter. The slot argument of the command specifies the slot location and filename of the microcode image, such as slot0:xcpa26-1 .
Step 5	Router(config)# microcode reload or Router# microcode reload all	From global configuration mode, loads the CPA microcode image for all of the adapters in the router. or From privileged EXEC mode, forces a microcode reload for all CPA adapters. Note These commands shut down the router if you are on a live network.
Step 6	Router(config)# end	Exits global configuration mode.
Step 7	Router# copy running-config startup-config	Saves the running configuration as the new startup configuration in NVRAM.

Upgrading the CPA Microcode Image for a Particular Adapter

The CPA microcode image is preloaded on Flash memory cards for Cisco 7200 series routers for Cisco IOS Release 11.3(3)T and later. You may be required to copy a new image to Flash memory when a new microcode image becomes available. Use the commands in this section if you are upgrading or loading a microcode image other than the default image for a particular CPA adapter.

To prepare the CPA, use the following commands beginning in privileged EXEC command mode:

	Command	Purpose
Step 1	Router> enable	Enters the privileged EXEC mode command interpreter.
Step 2	Router# copy tftp:filename [bootflash: slot0: slot1:]filename	Copies the CPA microcode image from a server to either of the Flash memory cards. The source of the file is tftp:filename . 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.
Step 3	Router# configure terminal	From privileged EXEC command mode, enters global configuration mode and specifies that the console terminal is the source of the configuration subcommands.
Step 4	Router(config)# microcode {ecpa pcpa} slotn:xcpaxx-yy	Loads the microcode from an individual microcode image that is stored as a file on a Flash memory card on a CPA adapter. The slot argument of the command specifies the slot location and filename of the microcode image, such as slot0:xcpa26-1.
Step 5	Router# microcode reload {all {{ecpa pcpa} [slot number]}}	From privileged EXEC mode, forces a microcode reload for a specific interface in a particular slot in a CPA adapter. This command allows you to reset a particular card without resetting every card in the router. Note The all keyword reloads all adapters in the router.
Step 6	Router(config)# end	Exits global configuration mode.
Step 7	Router# copy running-config startup-config	Saves the running configuration as the new startup configuration in NVRAM.

Verifying the CIP and CPA Microcode Image

When a router is starting and the bootflash is loading, the router searches for the default CIP or CPA microcode associated with the current bootflash image. This microcode image might not be the current image that you have loaded. This produces some messages that seem to indicate that the microcode is not loading properly. However, these messages (as shown in the following example for the CIP) are part of the normal loading process:

```
*Oct 1 13:37:28.078: %SYS-5-RELOAD: Reload requested
System Bootstrap, Version 11.1(2) [nitin 2], RELEASE SOFTWARE (fc1)
```


Command	Purpose
Router(config)# interface channel slot/port	<p>Selects the interface and enters interface configuration mode. The <i>port</i> value differs by the type of CMCC adapter:</p> <ul style="list-style-type: none"> • CIP—<i>Port</i> value corresponds to 0 or 1 for the physical interface, and 2 for the virtual interface. • CPA—<i>Port</i> value corresponds to port 0.

Use the **show extended channel EXEC** commands to display current CMCC adapter status. This command provides a report for each interface configured to support IBM channel attachment.

Selecting a Data Rate for the Parallel Channel Interfaces

When you configure a parallel channel-attached interface (such as a PCA on a CIP or a PCPA on a CPA) that uses bus-and-tag connections, you can specify a data rate of either 3 MBps or 4.5 MBps.

Note that the unit of measure for this command is *megabytes* per second (MBps). When you use the **show interface channel** command, the data rate is shown in the **BW** field (for bandwidth) in *kilobits* per second (kbps). For example, a channel data rate of 3 MBps is shown as 36864 kbps in the output for the **show interface channel** command.

To configure the parallel data rate on the router, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# channel-protocol [s s4]	<p>(Optional) Defines the data transfer rate for parallel channel interfaces. The available options for this command are:</p> <ul style="list-style-type: none"> • s—Specifies that the parallel channel interface operates at a rate of 3 MBps, or 36864 kbps. This is the default. • s4—Specifies that the parallel channel interface operates at a rate of 4.5 MBps.

Mainframe Configuration Tip

The **channel-protocol** command has a corollary parameter called **PROTOCOL** in the **CNTLUNIT** statement of the mainframe IOCP definition. The **PROTOCOL** parameter in the IOCP definition specifies the maximum speed of a bus-and-tag channel connection for the corresponding CSNA device in the router. Note that even if the **CNTLUNIT** statement in the IOCP specifies a value of **PROTOCOL=S4** (4.5 MBps), the channel interface will operate at 3 MBps if at the router you use the default value or specify **s** in the **channel-protocol** command. Therefore, if you want to configure a channel speed of 4.5 MBps, be sure to specify a value of **s4** for both the **PROTOCOL** parameter in the IOCP and the **channel-protocol** command in the router.

Configuring Channel Interface Tracking for HSRP or SNMP Alerts

If you want to use Hot Standby Router Protocol (HSRP) or SNMP alerts to monitor channel interface status for an ECPA or PCPA channel interface, use the following command in interface configuration mode to enable physical interface signal tracking:

Command	Purpose
Router(config-if)# state-tracks-signal	Enables tracking of the physical interface signal for an ECPA or PCPA channel interface.

The **state-tracks-signal** command is valid only on channel interfaces which combine the functions of both a physical and virtual interface. The ECPA and PCPA are examples of this type of channel interface. The command is not valid for the CIP, which has a separate channel interface for the virtual channel functions.

Monitoring and Maintaining a CMCC Adapter

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

- [Monitoring Interface Status, page 23](#)
- [Clearing and Resetting an Interface, page 26](#)
- [Monitoring the Physical Channel Interface on the CPA, page 27](#)
- [Shutting Down and Restarting an Interface, page 27](#)
- [Running CMCC Adapter Interface Loopback Diagnostics, page 28](#)
- [Configuring a CMCC Adapter Core Dump, page 28](#)

Monitoring Interface Status

To display information about the interface, including the version of the software and the hardware, the controller status, and statistics about the interfaces, you can use the show commands listed in the following table. To see the full list of **show** commands supported, enter **show ?** at the EXEC prompt.

Perform the following commands in EXEC mode to display information associated with each command. All commands are applicable to all CMCC adapter interfaces (CIP and CPA), unless it is mentioned that they are specific to a particular CMCC adapter. Commands are listed in alphabetic order.

Command	Purpose
Router# show controllers cbus	Displays the cbus internal state for the Cisco 7000 with RSP7000 and Cisco 7500 series routers. Also included in the display is CIP-specific information such as the currently loaded microcode, currently loaded microcode application segments, and load metrics (such as CPU and memory statistics).
Router# show controllers channel <i>[slot/port]</i>	Displays CPA-specific information, including the currently loaded microcode.
Router# show extended channel <i>slot/port backup</i> <i>[ip-address]</i>	Displays information about CLAW and offload commands for each backup group.
Router# show extended channel <i>slot/port cmgr</i> <i>[tg-name]</i>	Displays information about the MPC+ TG connection manager.
Router# show extended channel <i>slot/port cmpc</i> <i>[path [device]]</i>	Displays information about each CMPC or CMPC+ subchannel configured on the specified CMCC adapter interface.
Router# show extended channel <i>slot/port connection-map llc2</i>	Displays the number of active LLC2 connections for each SAP and the mapping of the internal MAC adapter and the SAP to the resource that activated the SAP.
Router# show extended channel <i>slot/port csna</i> <i>[admin oper stats]</i> <i>[path [device]]</i>	Displays information about the CSNA subchannels configured on the specified CMCC adapter interface.
Router# show extended channel <i>slot/port llc2</i> <i>[admin oper stats]</i> <i>[lmac [lsap [rmac [rsap]]]]</i>	Displays information about the LLC2 sessions running on the CMCC adapter interfaces.
Router# show extended channel <i>slot/port max-llc2-sessions</i>	Displays information about the number of LLC2 sessions supported on the CMCC adapter.
Router# show extended channel <i>slot/port icmp-stack</i> <i>[ip-address]</i>	Displays information about the ICMP stack running on the CMCC adapter interfaces.
Router# show extended channel <i>slot/port ip-stack</i> <i>[ip-address]</i>	Displays information about the IP stack running on the CMCC adapter interfaces.
Router# show extended channel <i>slot/port llc2</i> <i>[admin oper stats]</i> <i>[lmac [lsap [rmac [rsap]]]]</i>	Displays information about the LCC2 sessions running on the CMCC adapter interfaces.
Router# show extended channel <i>slot/port packing names</i> <i>[path [device]]</i>	Displays CLAW packing names and their connection state.
Router# show extended channel <i>slot/port packing stats</i> <i>[path[device]]</i>	Displays CLAW packing statistics.
Router# show extended channel <i>slot/port statistics</i> <i>[path [device]]</i> <i>[connected]</i>	Displays information about CMCC adapter interfaces for diagnostic purposes.
Router# show extended channel <i>slot/port subchannel</i> <i>[connected]</i>	Displays information about the CMCC adapter interfaces.

Command	Purpose
Router# show extended channel slot/port tcp-connections [[<i>loc-ip-addr</i> [<i>loc-port</i> [<i>rem-ip-addr</i> [<i>rem-port</i>]]] [detail summary]	Displays information about the TCP sockets on a channel interface.
Router# show extended channel slot/port tcp-stack [<i>ip-address</i>]	Displays information about the TCP stack running on the CMCC adapter interfaces.
Router# show extended channel slot/port tg [oper stats] [detailed] [<i>tg-name</i>]	Displays configuration, operational, and statistics information for CMPC and CMPC+ transmission groups configured on a specified CMCC adapter internal LAN interface.
Router# show extended channel slot/port tn3270-server	Displays current configuration parameters and the status of the PUs defined in each TN3270 server.
Router# show extended channel slot/port tn3270-server client-ip-address ip-address [disconnected in-session pending]	Displays information about all clients at a specific IP address.
Router# show extended channel slot/port tn3270-server dlur	Displays information about the SNA session switch.
Router# show extended channel slot/port tn3270-server dlurlink name	Displays information about the DLUR components.
Router# show extended channel slot/port tn3270-server nailed-ip ip-address	Displays mappings between a nailed client IP address and nailed LUs.
Router# show extended channel slot/virtual channel tn3270-server pu pu-name [cluster]	Displays information about the client LUs associated with a specified PU including the cluster layout and pool name.
Router# show extended channel slot/port tn3270-server pu pu-name lu locaddr [history]	Displays information about the TN3270 server LUs running on CMCC adapter interfaces.
Router# show extended channel slot/port udp-listeners [<i>ip-address</i>]	Displays information about the UDP listener sockets on the CMCC adapter interfaces.
Router# show extended channel slot/virtual channel tn3270-server response-time application [<i>appl-name</i> [detail]]	Displays information about each client group application for the specified VTAM appl name. List each member of the client group with its individual response-time statistics.
Router# show extended channel slot/virtual channel tn3270-server response-time global	Displays information about the global client groups.
Router# show extended channel slot/virtual/channel tn3270-server response-time link [<i>link-name</i>]	Displays information about the specified per-host-link client group.
Router# show extended channel slot/virtual channel tn3270-server response-time listen-point	Displays information about listen-point type client groups.
Router# show extended channel slot/virtual channel tn3270-server response-time subnet [<i>ip-mask</i> [detail]]	Displays information about the specified client group.
Router# show extended channel slot/port udp-stack [<i>ip-address</i>]	Displays information about the UDP stack running on the CMCC adapter interfaces.

Command	Purpose
Router# show interfaces channel slot/port accounting	Displays the number of packets for each protocol type that has been sent through the channel interface.
Router# show version	Displays the hardware configuration, software version, names and sources of configuration files, and boot images.

Clearing and Resetting an Interface

There are several commands that you can use on a CMCC adapter to clear statistics counters by interface or by feature, or to reset the hardware logic on an interface.

Clearing Interface Statistics Counters

To clear the statistics counters that are displayed in the output of the **show interfaces** command, use the following command in EXEC mode:

Command	Purpose
Router# clear counters [<i>type slot/port</i>]	Clears interface counters on the router.



Note

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

Clearing Feature-Specific Statistics Counters

You can reset the statistics counters that are displayed in the output of the **show extended channel** commands by a particular feature on the interface.

To clear the counters associated with application features configured on the CMCC adapters, use the following command in EXEC mode:

Command	Purpose
Router# clear extended counters channel slot/port [<i>csna icmp-stack ip-stack llc2 statistics tcp-connections tcp-stack tg tn3270-server udp-stack</i>]	Clears counters for application features configured on CMCC adapters.



Note

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

Clearing the Hardware Logic on an Interface

Under normal circumstances, you do not need to clear the hardware logic on interfaces. However, if it is necessary to clear the hardware logic on an interface, use the following command in EXEC mode:

Command	Purpose
Router# clear interface [<i>type slot/port</i>]	Resets the hardware logic on an interface.

Monitoring the Physical Channel Interface on the CPA

Unlike the CIP, which has a separate channel interface for the virtual channel functions, the ECPA and PCPA have a single interface that combines the functions of both a physical and virtual channel interface. For this reason, monitoring the physical channel interface on a CPA requires other considerations in its implementation.

In Cisco IOS releases prior to 12.0(4.1), you could not configure how the state of the physical interface on a CPA was tracked, particularly when the interface was configured for **no shutdown**. In those previous Cisco IOS releases when the CPA channel interface was configured for **no shutdown**, the channel interface status was always reported as UP/UP, even when no signal was present on the physical connection.

In Cisco IOS Release 12.0(4.1) and later, you can use the **state-tracks-signal** configuration command to control how you want the state of the CPA's channel interface to be reported. The **state-tracks-signal** command is useful in environments where you are using HSRP or SNMP alerts to monitor channel interface status.

To enable physical interface signal tracking, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# state-tracks-signal	Enables tracking of the physical interface signal for an ECPA or PCPA channel interface.

When the **state-tracks-signal** command is used on an interface that is configured for **no shutdown**, then the state of the channel interface is reported according to the status of the physical channel interface signal. If the physical channel interface signal is not present, then the channel interface status is DOWN/DOWN.

When the channel interface is configured for **no state-tracks-signal** (the default) and **no shutdown**, the channel interface status is always reported as UP/UP, even when there is no signal present on the physical connection. This configuration is useful for TN3270 server environments that are operating in a mode without any physical channel interface connections.

Shutting Down and Restarting an Interface

You can disable an interface on a CMCC adapter. Disabling an interface disables all of the 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 a CMCC adapter with an ESCON interface,

a command is sent to the host to inform it of the impending shutdown. On the CMCC adapter's Parallel interface, the **shutdown** command disables the adapter card's transceivers and the interface stops responding to all commands.

It is recommended that you shut down a channel interface for some of the following reasons:

- For a CMCC adapter's ESCON interface, 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 and then reenables it after changing the interface. Refer to your hardware documentation for more details.
- If you want to reload the router
- If, prior to reloading the microcode, you want to shut down the interface
- If you want to power off the router
- If it is recommended that a channel interface be shut down

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

	Command	Purpose
Step 1	Router(config-if)# shutdown	Shuts down an interface.
Step 2	Router(config-if)# no shutdown	Enables an interface.

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.

Running CMCC Adapter Interface Loopback Diagnostics

The CMCC adapter does not provide software loopback support. You can use special loopback wrap plugs to perform hardware loopback with the ESCON and Parallel channel interfaces. Hardware loopback information is included in the hardware installation notes for the CMCC adapters.

Configuring a CMCC Adapter Core Dump

To obtain the output of a CMCC adapter core dump, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ip domain-name <i>name</i> Router(config)# ip name-server <i>address</i> Router(config)# ip ftp username <i>name</i> Router(config)# ip ftp password <i>password</i>	Configures the router FTP services.
Step 2	Router(config)# exception slot [<i>slot</i>] <i>protocol</i> :: <i>host</i> / <i>filename</i>	Configures the CMCC adapter core dump feature.



Note

The exception slot command is only supported on the Cisco 7000 with RSP7000 and Cisco 7500 series routers. On the Cisco 7200 series routers, only FTP is supported.

While the router is running, you can use the **write EXEC** command to write the contents of a CMCC adapter that is not halted:

Command	Purpose
Router# write	Writes the contents of a CMCC adapter.



Note The output obtained by the **exception slot** command can be interpreted by a qualified Cisco technical support person.

CPA Microcode Load Configuration Examples

The following example shows output from running the **copy tftp** command to copy a new image to Flash memory:

```
Router#copy tftp:xcpa26-2 slot0:xcpa26-2

Address or name of remote host []? neptune
Translating "neptune"...domain server (10.20.30.10) [OK]
Destination filename [xcpa26-2]?
Accessing tftp://neptune/xcpa26-2...
Loading motto/xcpa26-2 from 10.20.30.10 (via Fast Ethernet0/0): !
  Expanding slot0:xcpa26-2_kernel_xcpa (343148 bytes):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  Expanding slot0:xcpa26-2_seg_802 (237848 bytes):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  Expanding slot0:xcpa26-2_seg_cmpc (319960 bytes):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  Expanding slot0:xcpa26-2_seg_csna (89856 bytes): !!!!!!!!!!!!!!!!!!!!!!!
  Expanding slot0:xcpa26-2_seg_eca (461424 bytes):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  Expanding slot0:xcpa26-2_seg_offload (80344 bytes): !!!!!!!!!!!!!!!!!!!!!
  Expanding slot0:xcpa26-2_seg_pca (69376 bytes): !!!!!!!!!!!!!!!!!!!!!
  Expanding slot0:xcpa26-2_pseg_push (15936 bytes): !!!
  Expanding slot0:xcpa26-2_seg_tcpip (158896 bytes): !!!!!!!!!!!!!!!!!!!!!!!
  Expanding slot0:xcpa26-2_seg_tn3270 (601784 bytes):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 2387456/4774912 bytes]
2387456 bytes copied in 110.588 secs (21704 bytes/sec)
router#
```

After copying a CMCC ucode image to flash memory, a directory command of the flash device displays the following:

```
Router#dir slot0:

Directory of slot0:/
 1 -rw-      1   Aug 18 1998 12:29:12  xcpa26-2
 2 -rw-    344438   Aug 18 1998 12:29:12  xcpa26-2.kernel_xcpa
 3 -rw-    237848   Aug 18 1998 12:29:37  xcpa26-2.seg_802
 4 -rw-    319960   Aug 18 1998 12:29:56  xcpa26-2.seg_cmpc
 5 -rw-     89856   Aug 18 1998 12:30:15  xcpa26-2.seg_csna
 6 -rw-    461424   Aug 18 1998 12:30:20  xcpa26-2.seg_eca
 7 -rw-     80344   Aug 18 1998 12:31:03  xcpa26-2.seg_offload
 8 -rw-     69376   Aug 18 1998 12:31:07  xcpa26-2.seg_pca
 9 -rw-     15936   Aug 18 1998 12:31:11  xcpa26-2.seg_push
```

```
10 -rw-      158896   Aug 18 1998 12:31:12  xcpa26-2.seg_tcpip
11 -rw-      601784   Aug 18 1998 12:31:32  xcpa26-2.seg_tn3270
7995392 bytes total (5614116 bytes free)
```

The following example loads the microcode from an individual microcode image that is stored as a file in the PCMCIA card in slot 0:

```
Router(config)# microcode ecpa slot0:xcpa26-2
Router(config)# microcode reload
```

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

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

© 2008 Cisco Systems, Inc. All rights reserved.