



## Interface Common Attributes Configuration Application

---

The Interface Common Attributes Configuration Application contains the following tabs and subtabs:

- [General Tab, page 7-2](#)
  - [IPv4 Configuration Subtab, page 7-3](#)
  - [Dampening Subtab, page 7-5](#)
- [Operation Tab, page 7-7](#)

The Interface Common Attributes Configuration application allows you to configure interface attributes that are common across all interfaces, including Ethernet and Packet-over-SONET POS. Configuration of common attributes prevents the need to enter the same data numerous times across various interfaces.

When a common attribute is configured in the Ethernet or POS application, the changes can be displayed and edited in the Interface Common Attributes Configuration application.

See [Figure 7-1](#) for an example of the Interface Common Attributes Configuration application.

Refer to the *Cisco CRS-1 Series Carrier Routing System Craft Works Interface User Interface Guide* for information on the common window elements and common activities procedures in the Interface Common Attributes Configuration application.

Figure 7-1 Interface Common Attributes Configuration Application

The screenshot displays the 'Interface Common Attributes Configuration - [17]' window. It features a toolbar with icons for file operations and navigation. Below the toolbar are two tabs: 'General' (selected) and 'Operation'. The 'General' tab contains a table listing interface configurations and a detailed configuration panel below it.

Interface Name	Description	IP Address	Mask	MTU Layer 2 (bytes)	CDP	Enable IPv4
MgmtEth0/0/CPU0/0		172.16.23.69	255.255.0.0			true
POS0/1/0/0						false
POS0/1/0/1						false
POS0/1/0/2						false
POS0/1/0/3						false

The configuration panel below the table includes the following fields and sections:

- Description:** A text input field.
- MTU Layer 2 (bytes):** A text input field.
- CDP:** A dropdown menu.
- IPv4 Configuration:** A sub-tabbed section containing:
  - IPv4 Processing:**
    - Enable IPv4 Processing
    - Unnumbered
    - IP Address: 172.16.23.69
    - Mask: 255.255.0.0
  - Secondary Addresses:** A table with columns for IP Address and Mask, and 'Add' and 'Remove' buttons.
  - General:**
    - MTU Layer 3 (bytes): A text input field.
    - ICMP Mask Reply
  - Helper Addresses:** A text input field for the Helper IP Address, with 'Add' and 'Remove' buttons.

At the bottom of the window are 'OK', 'Cancel', and 'Apply' buttons. A status bar at the very bottom indicates '5 record entries' and the number '98490'.

## General Tab

The General tab contains two subtabs: IPv4 Configuration and Dampening. The IPv4 Configuration subtab is displayed by default when the General tab is clicked.

The General tab allows you to perform the following tasks:

- Provide a description of the interface.
- Specify the maximum transmission unit (MTU) Layer 2 value.
- Choose to enable or disable the Cisco Discovery Protocol (CDP).

See [Figure 7-1](#) for an example of the General tab. [Table 7-1](#) describes the General tab fields.

Table 7-1 General Tab Description

Field	Description
Description field	Allows you to enter a description of the interface.
MTU Layer 2 (bytes) field	<p>Allows you to enter a MTU Layer 2 value in bytes for the interface. This value is the maximum packet size or MTU size.</p> <p>The following are the default MTUs according to media type:</p> <ul style="list-style-type: none"> <li>• Ethernet—1514 bytes</li> <li>• POS—4474 bytes</li> <li>• Tunnel—1500 bytes</li> <li>• Loopback—1514 bytes</li> </ul> <p>Each interface has a default maximum packet size or MTU size. This number generally defaults to the largest size possible for that interface type.</p>
CDP list	<p>Allows you to enable or disable CDP on the interface.</p> <p>CDP is disabled by default at the global level. CDP is supported on all interfaces except for Spatial Reuse Protocol (SRP) interfaces. To start sending and receiving CDP information on the interface choose enable. Choose disable to stop sending and receiving CDP information on the interface.</p> <p>CDP allows Cisco routers to discover each other in a protocol/media independent way. It allows a device to advertise its existence to devices, and also to detect all other devices on the same LAN (or on the other side of a WAN). CDP is a hello-based protocol, and all devices running CDP will periodically advertise their attributes to their neighbors.</p>

## IPv4 Configuration Subtab

The IPv4 Configuration subtab allows you to perform the following tasks:

- Specify the IPv4 address and mask.
- Specify secondary addresses for the interface.
- Specify the IPv4 MTU for the interface.
- Configure the software response to Internet Control Message Protocol (ICMP) mask requests.
- Specify helper addresses for the interface.

See [Figure 7-1](#) for an example of the IPv4 Configuration subtab. [Table 7-2](#) describes the IPv4 Configuration subtab fields.



### Note

If any networking device on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can quickly cause routing loops.

Table 7-2 IPv4 Configuration Subtab Description

Field	Description
<b>IPv4 Configuration Area</b>	
Enable IPv4 Processing check box	<p>Enables IPv4 processing, which allows you to either set primary and secondary IP Version 4 addresses for an interface or set an unnumbered interface to make this interface use the unnumbered interface IP address.</p> <p>An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the software always use the primary IP address. Therefore, all networking devices on a segment should share the same primary network number.</p>
Unnumbered	Allows you to enable IPv4 processing without an explicit address.
Unnumbered radio button	Allows you to enable IP v4 processing.
Unnumbered field	Allows you to view the chosen interface name.
Unnumbered ellipsis button	Allows you to choose an interface from the Select Interfaces dialog box. The Unnumbered radio button must be chosen to enable the Unnumbered field. (See <a href="#">Unnumbered radio button</a> .)
IP Address	Allows you to enter a valid IPv4 address for the interface.
IP Address radio button	Allows you to configure the IPv4 address.
IP Address field	Allows you to enter a valid IP address. The IP Address radio button must be chosen to enable the IP Address field. (See <a href="#">IP Address radio button</a> .)
Mask field	Allows you to enter a valid mask for the IP address of the interface.
Secondary Addresses table	<p>Allows you to specify secondary IP addresses for the interface. Click the Add button to add a secondary address. Choose an address in the table and click Remove to delete a secondary address from the interface.</p> <p>Double-click a cell in the IP Address column to activate it and enter the IP address for the secondary address. Double-click a cell in the Mask column to activate it and enter the mask for the secondary address.</p> <p>There can be more than one secondary address specified. Secondary addresses are treated like primary addresses, except that the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.</p> <p>Secondary IP addresses can be used in a variety of situations. The following are the most common applications:</p> <ul style="list-style-type: none"> <li>• There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need to have 300 host addresses. Using secondary IP addresses on the networking devices allows you to have two logical subnets using one physical subnet.</li> <li>• Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can be easily made aware that there are many subnets on that segment.</li> <li>• Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is extended, or layered on top of the second network using secondary addresses.</li> </ul>

Table 7-2 IPv4 Configuration Subtab Description (continued)

Field	Description
<b>General Area</b>	
MTU Layer 3 (bytes) field	Allows you to enter a valid MTU Layer 3 size in bytes. The MTU Layer 3 field contains the maximum MTU available for IP traffic.
ICMP Mask Reply check box	Allows you to configure the software to respond to ICMP mask requests by sending ICMP mask reply messages to the interface.  Hosts can determine subnet masks using the ICMP mask request message. Networking devices respond to this request with an ICMP mask reply message.
Helper Addresses table	Allows you to specify helper addresses for the interface. Helper addresses are the addresses to which the software forwards User Datagram Protocol (UDP) broadcasts/packets, including BOOTP, received on an interface.  Click the Add button to add a helper address. Choose an address in the table and click Remove to delete a helper address from the interface. There can be more than one helper address for an interface.  Double-click a cell in the Helper IP Address column to activate it and enter the IP address for the helper address.  One common application that requires helper addresses is Dynamic Host Configuration Protocol (DHCP), which is defined in RFC 1531. DHCP protocol information is carried inside of BOOTP packets. To enable BOOTP broadcast forwarding for a set of clients, configure a helper address on the networking device interface closest to the client. The helper address should specify the address of the DHCP server. If you have multiple servers, you can configure one helper address for each server. Because BOOTP packets are forwarded by default, DHCP information can now be forwarded by the networking device. The DHCP server now receives broadcasts from the DHCP clients.

## Dampening Subtab

Currently, a router with an unstable data link (also known as a link flap) may remove itself from service and return to service several times in a matter of seconds, requiring all other routers to rebuild their routing tables with each event. Dampening enables a router experiencing link flap to remove itself from network routing tables until return to data-link stability is ensured. Once the link is stable, an up event is sent and the route is added back to the routing table.

With interface state dampening, the interface will immediately remove itself from the routing table on the down event (link flap). If there are multiple link flaps in a short period of time, the interface will ignore the next up event. The interface will remain down until the data link has stabilized based on the dampening configuration parameters. Dampening can ignore up events based but cannot ignore down events unless the interface is already down.

Dampening delivers resiliency improvements that include the following:

- Faster convergence. Routers that are not experiencing link flap reach convergence sooner, because routing tables are not rebuilt each time the offending router leaves and enters service. Faster convergence provides a more stable network because a router remains out of service until it is ready to enter service, ensuring fewer transitions.
- Increased network stability. A router with data-link problems removes itself from service until the data link is consistently stable. Other routers simply redirect traffic around the affected router until data-link issues are resolved, thus ensuring that the router loses no data packets.

The Dampening subtab allows you to perform the following tasks:

- Enable dampening for the interface.
- Configure the half-life, suppress, reuse, and maximum suppress values.

See [Figure 7-2](#) for an example of the Dampening subtab. [Table 7-3](#) describes the Dampening subtab fields.

**Figure 7-2 Dampening Subtab**

**Table 7-3 Dampening Subtab Description**

Field	Description
<b>IPv4 Configuration Area</b>	
Dampening check box	Allows you to enable state dampening for the interface.
HalfLife (min) field	Allows you to enter a time after which a penalty is decreased (decay half life). Once the interface has been assigned a penalty, the penalty is decreased by half after the half life period.
Suppress field	Allows you to set a suppress threshold. An interface state is suppressed down when its penalty (increased by state flaps) exceeds the suppress threshold.

Table 7-3 Dampening Subtab Description (continued)

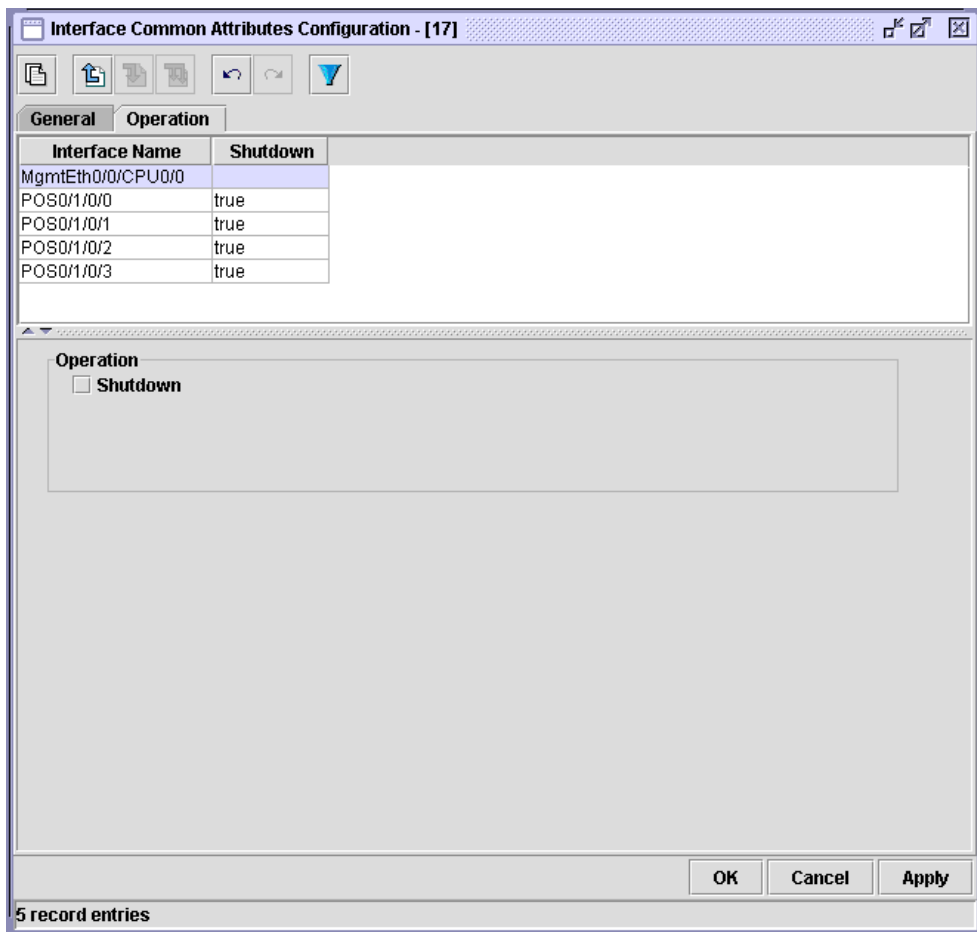
Field	Description
Reuse field	Allows you to set the reuse threshold. An interface state is unsuppressed if the penalty for an interface decreases enough to fall below the reuse threshold.
Max Suppress (min) field	Allows you to set the maximum time (in minutes) an interface state can be suppressed down. A reasonable rule is to configure the maximum suppress to approximately four times the half life value.

## Operation Tab

The Operation tab allows you to manually shut down the interface.

See [Figure 7-3](#) for an example of the Operation tab. [Table 7-4](#) describes the Operation tab fields.

Figure 7-3 Operation Tab



**Table 7-4** *Operation Tab Description*

Field	Description
Shutdown check box	Allows you to shut down the interface. Shutdown administratively brings down an interface.