

I Commands

The commands shown in this chapter apply to the Catalyst 8540 MSR, Catalyst 8510 MSR, and LightStream 1010 ATM switch routers. Where an entire command or certain attributes of a command have values specific to a particular switch or switch router, an exception is indicated by the following callouts:

- Catalyst 8540 MSR
- Catalyst 8510 MSR and LightStream 1010



Note

Commands that are identical to those documented in the Cisco IOS software documentation have been removed from this chapter.



Note

Commands that no longer function as expected in ATM environments have also been removed from this chapter.

Refer to Appendix D of this command reference for a detailed list of commands that have been removed, changed or replaced.

ima active-links-minimum

To configure the minimum active links for an IMA group to function, use the **ima active-links-minimum** interface configuration command. To restore the default value, use the **no** form of this command.

ima active-links-minimum *number*

no ima active-links-minimum

Syntax Description	<i>number</i> Configures the minimum number (1 to 8) of active links for an IMA group to function.
---------------------------	--

Defaults	1
-----------------	---

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.0(4a)W5(11a)	New command

Usage Guidelines	An IMA group might be configured to require a minimum amount of bandwidth or active links to function correctly. However, if you reduce the minimum number of active links to below the minimum active links configured, the far-end connection receives an ICP cell with a failure error, and the interface changes to the down state.
-------------------------	---



Note

This command is only supported on systems equipped with FC-PFQ.

Examples	The following example uses the ima active-links-minimum command to configure the minimum number of active links that must be active for the IMA group to function correctly.
-----------------	---

```
Switch(config)# interface atm 0/0/ima1
Switch(config-if)# ima active-links-minimum 2
```

Related Commands	Command	Description
	show ima interface	Displays the IMA interface, IMA group, and ATM layer hardware configuration.

ima clock-mode

To configure the clocking mode for the IMA group, use the **ima clock-mode** interface configuration command. To restore the default value, use the **no** form of this command.

ima clock-mode { common | independent }

no ima clock-mode

Syntax Description	common	Configures the clocking as CTC, where the same clocking is used for all interfaces.
	independent	Configures the clocking as ITC, where each interface derives its clocking from a different clock source.

Defaults	common
----------	---------------

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	12.0(4a)W5(11a)	New command

Usage Guidelines The transmit clock of members of an IMA group can be derived from one single clock source or driven individually from different sources.

The term ITC is used when the transmit clock on each link is independently derived from a clock source. The transmit clock source for each member interface is configured using the **clock source (Catalyst 8540 MSR)** command at interface configuration.

The term CTC applies when the same clock is used for all links. In CTC mode, the network clock as configured by the **network-clock-select** command is the source that drives the transmit clock of all the members of an IMA group.



Note

This command is only supported on systems equipped with FC-PFQ.

Examples

The following example uses the **ima clock-mode** command to configure the IMA group clocking mode as independent.

```
SwitchA(config)# interface atm 0/0/ima1
SwitchA(config-if)# ima clock-mode independent
```

The following example uses the **ima clock-mode** command to configure the IMA group clocking mode as common with network clock from interface ATM 0/0/6.

```
Switch(config)# network 1 atm 0/0/6
Switch(config)# interface atm 0/0/ima1
Switch(config-if)# ima clock-mode common
```

Related Commands

Command	Description
clock source (interface) (Catalyst 8510 MSR and LightStream 1010)	Used to select a transmit clock source for a physical device, such as a port.
network-clock-select	Enables the recovered clock to specify a particular port to provide network clocking.
show ima interface	Displays the IMA interface, IMA group, and ATM layer hardware configuration.

ima differential-delay-maximum

To configure the maximum differential delay used to align the transmission of IMA frames on all links, use the **ima differential-delay-maximum** interface configuration command. To restore the default value, use the **no** form of this command.

ima differential-delay-maximum *msecs*

no ima differential-delay-maximum

Syntax Description

msecs Configures the maximum differential delay in milliseconds as follows:

- For T1 the range is 25 to 250 milliseconds.
- For E1 the range is 25 to 190 milliseconds.

Defaults

25 milliseconds

Command Modes

Interface configuration

Command History

Release	Modification
12.0(4a)W5(11a)	New command

Usage Guidelines

The transmitter on the T1/E1 IMA port adapter must align the transmission of IMA frames on all interfaces that are members of the IMA group. This allows the receiver to adjust for differential link delays among the interfaces that are members of the IMA group. Based on this required behavior, the receiver can detect the differential delays by measuring the arrival times of the IMA frames on each link.

At the transmitting end, the cells are transmitted continuously. If no ATM layer cells need to be sent between ICP cells within an IMA frame, then the transmit IMA sends filler cells to maintain a continuous stream of cells at the physical layer.



Note

This command is only supported on systems equipped with FC-PFQ.

Examples

The following example configures the maximum allowable differential delay to 100 milliseconds for all interfaces assigned to the IMA group.

```
Switch(config)# interface atm 0/0/ima1
Switch(config-if)# ima differential-delay-maximum 100
```


Related Commands	Command	Description
	show ima interface	Displays the IMA interface, IMA group, and ATM layer hardware configuration.

ima frame-length

To configure the IMA interface frame length (number of cells per frame), use the **ima frame-length** interface configuration command. To restore the default value, use the **no** form of this command.

ima frame-length { 128 | 256 | 32 | 64 }

no ima frame-length

Syntax Description	128	Configures IMA frame length to 128 cells (default).
	256	Configures IMA frame length to 256 cells.
	32	Configures IMA frame length to 32 cells.
	64	Configures IMA frame length to 64 cells.
Defaults	128	
Command Modes	Interface configuration	
Command History	Release	Modification
	12.0(4a)W5(11a)	New command
Usage Guidelines	An IMA group uses the frame length parameter to set the insertion of the ICP cells at the beginning of frames in the transmit direction.	
 Note	This command is only supported on systems equipped with FC-PFQ.	
Examples	The following example uses the ima frame-length command to configure the frame length transmitted as 256 cells for the IMA group: <pre>Switch(config)# interface atm 0/0/ima1 Switch(config-if)# ima frame-length 256</pre>	
Related Commands	Command	Description
	show ima interface	Displays the IMA interface, IMA group, and ATM layer hardware configuration.

ima-group

To assign an interface as a member of an IMA group, use the **ima-group** interface configuration command. To remove an interface from an IMA group, use the **no** form of this command.

ima-group *number*

no ima-group

Syntax Description	<i>number</i> Specifies the IMA group number (0 to 3).
---------------------------	--

Defaults	Disabled
-----------------	----------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.0(4a)W5(11a)	New command

Usage Guidelines	<p>Use the ima-group interface command to configure a T1/E1 IMA port adapter interface as part of an IMA group. IMA allows you to aggregate multiple low-speed links into one larger virtual trunk or IMA group which appears to your ATM switch router as one logical pipe. This IMA group provides modular bandwidth for user access to ATM networks for connections between ATM network elements at rates between the traditional order of multiplex levels, such as between T1 or E1, and T3 or E3.</p>
-------------------------	--

IMA requires inverse multiplexing and demultiplexing of ATM cells in a cyclical fashion among links grouped to form a higher bandwidth logical group with a rate approximately the sum of the link rates. This grouping is called an IMA group.



Note	This command is only supported on systems equipped with FC-PFQ.
-------------	---



Note	To configure a T1/E1 IMA port adapter interface as a member of an IMA group, you must shut down the interface before using the ima-group command when no shutdown has been previously configured .
-------------	---

Examples	<p>The following example uses the ima-group command to assign ATM interface 0/0/0 as part of IMA group 1.</p>
-----------------	--

```
Switch(config)# interface atm 0/0/0
Switch(config-if)# shutdown
Switch(config-if)# ima-group 1
Switch(config-if)# no shutdown
```


Related Commands	Command	Description
	show ima interface	Displays the IMA interface, IMA group, and ATM layer hardware configuration.
	show interfaces	Displays the interface configuration, status, and statistics.

ima test

To configure an IMA group test pattern transmitted in the ICP cells, use the **ima test** interface configuration command. To restore the default value, use the **no** form of this command.

```
ima test [link link-value] [pattern pattern-value]
```

```
no ima test
```

Syntax Description

link	Configures the link transmitting the test pattern.
<i>link-value</i>	Specifies which IMA group member link is transmitting the test pattern.
pattern	Configures the test pattern.
<i>pattern-value</i>	Specifies the test pattern transmitted in the ICP cells.

Defaults

The link-value: First link in the IMA group
The pattern-value: Default is the link-value

For example, suppose an IMA group includes ATM interfaces 0/0/3, 0/0/4 and 0/0/6. If the link or pattern value is not specified in the **ima test** command, then interface 0/0/3 (default) is chosen as test-link, and the pattern value used is 03 (default).

Command Modes

Interface configuration

Command History

Release	Modification
12.0(4a)W5(11a)	New command

Usage Guidelines

The test pattern procedure verifies the connectivity of a link within an IMA group. The procedure uses a test pattern sent over one link to verify the connectivity to the other links in the IMA group. The test pattern should be looped over all the other links in the group at the far end of the connection. All of the IMA test pattern procedures are performed over the ICP cells exchanged between both ends of the IMA virtual links. After the test is configured on the IMA group, the test continues until explicitly configured to the default.



Note

This command is only supported on systems equipped with FC-PFQ.

Examples

The following example uses the **ima test** command to configure the test pattern 0x010 (octal 8) to transmit over ATM interface 0/0/3 of IMA group 1.

```
Switch(config)# interface atm 0/0/ima1  
Switch(config-if)# ima test link 3 pattern 010
```

Related Commands	Command	Description
	show ima interface	Displays the IMA interface, IMA group, and ATM layer hardware configuration.

incoming-port

To filter ATM signalling call failures based on the incoming interface of the call, use the **incoming-port** ATM signalling diagnostics configuration command. To return the incoming port to the default, use the **no** form of this command.

incoming-port atm *card/subcard/port*

no incoming-port atm *card/subcard/port*

Syntax Description

card/subcard/port Specifies the card, subcard, and port number of the ATM interface. The card number is displayed using the **show interfaces** command. The subcard number can be either 0 or 1.

Defaults

0

Command Modes

ATM signalling diagnostics configuration

Command History

Release	Modification
11.2(8.0.1)	New command

Usage Guidelines

The default 0 means the incoming interface is not considered during filtering.

Examples

The following example configures ATM 0/1/1 so all previous records collected on the incoming port are purged.

```
Switch# configure terminal
Switch(config)# controller atm 0/0/0
Switch(config-if)# atm signalling diagnostics 1
Switch(cfg-atmsig-diag)# incoming-port atm 0/1/1
```

interface

To configure an interface type and enter interface configuration mode, use the **interface** global configuration command.

```
interface type card/subcard/port
interface atm card/subcard/imagroup
interface type number
```

To configure a subinterface, use the **interface** global configuration command.

```
interface type card/subcard/port.vpt#
interface type card/subcard/port.subinterface# [multipoint | point-to-point]
```

Syntax Description	type	Specifies the type of interface to be configured. Refer to Table 9-1 for a list of keywords.
	card	Specifies the interface card number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the show interfaces command.
	subcard	Specifies the backplane slot number. The value is either 0 or 1. The slots are numbered from left to right.
	port	Specifies the port number of the interface.
	ima group	Specifies the IMA group number (0 to 3).
	number	Specifies the integer used to identify the interface.
	.vpt#	Specifies the virtual path tunnel number for the subinterface on physical ATM ports.
	.subinterface#	Specifies the subinterface number in the range of 1 to 4294967293. The number that precedes the periods (.) must match the number where this subinterface belongs.
	multipoint	Specifies a multipoint subinterface. This option only applies to the route processor interface ATM 0.
	point-to-point	Specifies a point-to-point subinterface. The default is multipoint . This option only applies to the route processor interface ATM 0.

Command Modes Global configuration

Command History	Release	Modification
	11.2(5)	New command

Usage Guidelines Multiple subinterfaces can be configured on a single route processor interface. The route processor and Ethernet interface address is 0 in the ATM switch router environment.

Multiple subinterfaces for VP tunneling can be configured on a single ATM interface (not on a route processor interface). VP tunnels are useful when you want to run signalling, ILMI, and possibly PNNI routing between two switches that are not directly connected to each other. Before configuring the subinterface, a permanent virtual path must be configured on the ATM interface using the **atm pvp** command. The subinterface for the VP tunnel is created by specifying the VPI used to define the permanent virtual path as the subinterface number.

Table 9-1 lists typical interface keywords.

Table 9-1 Interface Type Keywords

Keyword	Interface Type
atm	ATM interface.
async	Auxiliary port line used as an asynchronous interface.
bvi	Bridge-group virtual interface.
cbr	CBR interface.
cable	CMTS interface.
dialer	Dialer interface.
ethernet	Ethernet IEEE 802.3 interface.
group-async	Master asynchronous interface.
lex	Lex interface.
loopback	Software-only loopback interface that emulates a continually running interface. All platforms support this virtual interface. The interface <i>number</i> (0 to 2147483647) is the number of the loopback interfaces you want to create or configure.
null	Null interface.
Port-channel	Ethernet channel of interfaces.
serial	Serial interface.
tunnel	Tunnel interface, used to declare a TSP tunnel interface. The tunnel interface <i>number</i> is in the range of 0 to 2147483647.
virtual-template	Virtual template interface.
virtual-tokenring	Virtual Token Ring interface.
vlan	Catalyst 5000 VLAN interface.

Examples

The following example shows how to begin configuration of the ATM interface on card 0, subcard 0, and port 1 using the **interface** global configuration command.

```
Switch(config)# interface atm 0/0/1
Switch(config-if)#
```

The following example shows how to create a VP tunnel with VPI 50 on card 0, subcard 0, and port 1, and enter the subinterface configuration mode for the VP tunnel using the **interface** global configuration command.

```
Switch(config)# interface atm 0/0/1
Switch(config-if)# atm pvp 50
Switch(config-if)# interface atm 0/0/1.50
Switch(config-subif)#
```

The following example shows how to begin configuration of the route processor interface using the **interface** global configuration command.

```
Switch(config)# interface atm 0
Switch(config-if)#
```

The following example shows how to create a point-to-point subinterface on the SAP port and enter the subinterface configuration mode, using the **interface** global configuration command.

```
Switch(config)# interface atm 0.1 point-to-point
Switch(config-subif)#
```

The following example shows how to begin configuration of the Ethernet interface on the ATM switch router using the **interface** global configuration command.

```
Switch(config)# interface ethernet 0
Switch(config-if)#
```

The following example shows how to begin configuration of a CBR interface using the **interface** global configuration command.

```
Switch(config)# interface cbr 1/1/1
Switch(config-if)#
```

The following example shows how to use the **interface tunnel** command to declare a TSP tunnel interface with interface number 2100.

```
Switch(config)# interface tunnel 2100
Switch(config-if)#
```

The following example shows how to begin configuration of an IMA group interface using the **interface** global configuration command.

```
Switch(config)# interface atm 0/0/ima1
Switch(config-if)#
```

Related Commands

Command	Description
show interfaces	Displays the interface configuration, status, and statistics.
show ima interface	Displays the IMA interface, IMA group, and ATM layer hardware configuration.

ip address

To set a primary or secondary IP address for an interface, use the **ip address** interface configuration command. To remove an IP address or disable IP processing, use the **no** form of this command.

ip address *ip-address mask* [**secondary**]

no ip address *ip-address mask* [**secondary**]

Syntax Description

<i>ip-address</i>	IP address.
<i>mask</i>	Mask for the associated IP subnet.
secondary	Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

Defaults

No IP address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
11.1(4)	New command

Usage Guidelines

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the switch always use the primary IP address. Therefore, all switch routers on a segment should share the same primary network number.

Hosts can determine subnet masks using the ICMP Mask Request message. Switch routers respond to this request with an ICMP Mask Reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the switch router detects another host using one of its IP addresses, it prints an error message on the console.

The optional keyword **secondary** allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and ARP requests are processed properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There might 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 switch routers allows you to have two logical subnets using one physical subnet.
- 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 by using secondary addresses.



Note

If any switch router on a network segment uses a secondary address, all other switch routers 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 cause routing loops to occur very quickly.

Examples

In the following example, 131.108.1.27 is the primary address and 192.31.7.17 and 192.31.8.17 are secondary addresses for main Ethernet 0 interface.

```
Switch# configure terminal
Switch(config)# interface ethernet 0
Switch(config-if)# ip address 131.108.1.27 255.255.255.0
Switch(config-if)# ip address 192.31.7.17 255.255.255.0 secondary
Switch(config-if)# ip address 192.31.8.17 255.255.255.0 secondary
```

Related Commands

Command	Description
show ima interface	Displays the IMA interface, IMA group, and ATM layer hardware configuration.

ip broadcast-address

To define a broadcast address for an interface, use the **ip broadcast-address** interface configuration command. To restore the default IP broadcast address, use the **no** form of this command.

ip broadcast-address [*ip-address*]

no ip broadcast-address [*ip-address*]

Syntax Description	<i>ip-address</i> IP broadcast address for a network.
---------------------------	---

Defaults	Default address is 255.255.255.255 (all ones).
-----------------	--

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	11.1(4)	New command

Usage Guidelines	This command sets the broadcast address of an interface.
-------------------------	--

Examples	The following example specifies an IP broadcast address of 172.10.50.4.
-----------------	---

```
Switch# configure terminal
Switch(config)# ip broadcast-address 172.10.50.4
```

Related Commands	Command	Description
	show ima interface	Displays the IMA interface, IMA group, and ATM layer hardware configuration.

ip directed-broadcast

To enable the translation of directed broadcasts to physical broadcasts, use the **ip directed-broadcast** interface configuration command. To return the directed broadcast to the default, use the **no** form of this command.

ip directed-broadcast [*access-list-number*]

no ip directed-broadcast [*access-list-number*]

Syntax Description	<i>access-list-number</i> Number of the access list. If specified, a broadcast must pass the access list to be forwarded. If not specified, all broadcasts are forwarded.				
Defaults	Enabled with no list specified				
Command Modes	Interface configuration				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Release</th> <th style="text-align: left;">Modification</th> </tr> </thead> <tbody> <tr> <td>11.1(4)</td> <td>New command</td> </tr> </tbody> </table>	Release	Modification	11.1(4)	New command
Release	Modification				
11.1(4)	New command				
Usage Guidelines	This feature is enabled only for those protocols configured using the ip forward-protocol global configuration command. An access list might be specified to control which broadcasts are forwarded. When an access list is specified, only those IP packets permitted by the access list are eligible to be translated from directed broadcasts to physical broadcasts.				
Examples	<p>The following example enables forwarding of IP directed broadcasts on the main Ethernet 0 interface.</p> <pre>Switch# configure terminal Switch(config)# interface ethernet 0 Switch(config-if)# ip directed-broadcast</pre>				
Related Commands	None				

ip mtu

To set the MTU size of IP packets sent on an interface, use the **ip mtu** interface configuration command. To restore the default MTU size, use the **no** form of this command.

ip mtu *bytes*

no ip mtu

Syntax Description	<i>bytes</i> MTU in bytes.
---------------------------	----------------------------

Defaults	Minimum: 128 bytes Maximum: Depends on the interface medium
-----------------	--

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	11.1(4)	New command

Usage Guidelines	If an IP packet exceeds the MTU set for the interface of the switch router, the switch router fragments the packet.
-------------------------	---

All devices on a physical medium must have the same protocol MTU in order to operate.



Note

Changing the MTU value (with the **mtu** interface configuration command) can affect the IP MTU value. If the current IP MTU value is the same as the MTU value and you change the MTU value, the IP MTU value is modified automatically to match the new MTU. However, the reverse is not true; changing the IP MTU value has no effect on the value for the **mtu** command.

Examples	The following example sets the maximum IP packet size for the first interface to 300 bytes.
-----------------	---

```
Switch# configure terminal
Switch(config)# interface ethernet 0
Switch(config-if)# ip mtu 300
```

Related Commands	Command	Description
	mtu	Used to adjust the maximum packet size or MTU size.

ip proxy-arp

To enable proxy ARP on an interface, use the **ip proxy-arp** interface configuration command. To disable proxy ARP on the interface, use the **no** form of this command.

ip proxy-arp

no ip proxy-arp

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Interface configuration

Command History	Release	Modification
	11.1(4)	New command

Usage Guidelines Used to enable proxy ARP.

Examples The following example enables proxy ARP on Ethernet interface 0.

```
Switch# configure terminal
Switch(config)# interface ethernet 0
Switch(config-if)# ip proxy-arp
```

ip rarp-server

Use the **ip rarp-server** interface configuration command to allow the switch router to act as a RARP server. To return the RARP server to the default, use the **no** form of this command.

ip rarp-server *ip-address*

no ip rarp-server *ip-address*

Syntax Description

ip-address IP address that is to be provided in the source protocol address field of the RARP response packet. Normally, this is set to whatever address you configure as the primary address for the interface.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.1(4)	New command

Usage Guidelines

This feature makes diskless booting of clients possible between network subnets where the client and server are on separate subnets.

RARP server support can be configured on a per-interface basis so the switch router does not interfere with RARP traffic on subnets that do not need RARP assistance from the switch router.

The switch router answers incoming RARP requests only if both of the following two conditions are met:

- The **ip rarp-server** command has been configured for the interface on which the request was received.
- There is a static entry found in the IP ARP table that maps the MAC address contained in the RARP request to an IP address.

Use the **show ip arp EXEC** command to display the contents of the IP ARP cache.

Sun Microsystems makes use of RARP-based and UDP-based network services to facilitate network-based booting of SunOS on their workstations. By bridging RARP packets and using both the **ip mtu** interface configuration command and the **ip forward-protocol** global configuration command, the switch should be able to perform the necessary packet switching to enable booting of Sun workstations across subnets. However, some Sun workstations assume that the sender of the RARP response, in this case the switch router, is the host that the client can contact to TFTP-load the bootstrap image. This causes the workstations to fail to boot.

By using the **ip rarp-server** feature, the switch router can be configured to answer these RARP requests, and the client machine should be able to reach its server by having its TFTP requests forwarded through the switch router that acts as the RARP server.

ip route

To establish static routes, use the **ip route** global configuration command. To remove static routes, use the **no** form of this command.

```
ip route destination-prefix destination-prefix-mask [interface-type card/subcard/port]
forward-addr [metric | permanent | tag tag-value]
```

```
no ip route destination-prefix destination-prefix-mask [interface-type card/subcard/port]
forward-addr [metric | permanent | tag tag-value]
```

Syntax Description		
<i>destination-prefix</i>	IP address of the target network or subnet.	
<i>destination-prefix-mask</i>	Address mask for the destination address.	
<i>interface-type</i>	Interface type, specified as atm , atm-p , cbr , ethernet , or null .	
<i>card/subcard/port</i>	Identifier of the interface specified by <i>interface-type</i> .	
<i>forward-addr</i>	Forwarding router's IP address.	
<i>metric</i>	Distance metric for this route, in the range of 1 to 255.	
permanent	Specifies this route as a permanent route.	
<i>tag-value</i>	Sets the tag value for this route, in the range of 1 to 4294967295.	

Defaults No IP route is specified.

Command Modes Global configuration

Command History	Release	Modification
	11.1(4)	New command

Usage Guidelines This command does not apply to the route processor interface main ATM 0.

Examples In the following example, an administrative distance of 110 was chosen. In this case, packets for network 10.0.0.0 are routed to the switch at 131.108.3.4 if dynamic information with an administrative distance less than 110 is not available.

```
Switch# configure terminal
Switch(config)# ip route 10.0.0.0 255.0.0.0 131.108.3.4 110
```

In the following example, packets for network 131.108.0.0 are routed to the switch at 131.108.6.6.

```
Switch(config)# ip route 131.108.0.0 255.255.0.0 131.108.6.6
```

ip security add

To add a basic security option to all outgoing packets, use the **ip security add** interface configuration command. To disable the adding of a basic security option to all outgoing packets, use the **no** form of this command.

ip security add

no ip security add

Syntax Description This command has no arguments or keywords.

Defaults Disabled when the security level of the interface is “Unclassified Genser” (or unconfigured). Otherwise, the default is enabled.

Command Modes Interface configuration

Command History	Release	Modification
	11.1(4)	New command

Usage Guidelines If an outgoing packet does not have a security option present, this interface configuration command adds one as the first IP option. The security label added to the option field is the label that was computed for this packet when it first entered the switch. Because this action is performed after all the security tests have been passed, this label is either the same as or is in the range of the interface.

Examples The following example adds a basic security option to each packet leaving main Ethernet interface 0.

```
Switch# configure terminal
Switch(config)# interface ethernet 0
Switch(config-if)# ip security add
```

Related Commands	Command	Description
	ip security dedicated	Sets the level of classification and authority on the interface.

ip security aeso

To attach AESOs to an interface, use the **ip security aeso** interface configuration command. To disable AESOs on an interface, use the **no** form of this command.

ip security aeso *source compartment-bits*

no ip security aeso [*source compartment-bits*]

Syntax Description	<i>source</i>	AESO source. This can be an integer from 0 through 255.
	<i>compartment-bits</i>	Compartment bits, in hexadecimal.
Defaults	Disabled	
Command Modes	Interface configuration	
Command History	Release	Modification
	11.1(4)	New command
Usage Guidelines	<p>Compartment bits are specified only if this AESO is to be inserted in a packet. On every incoming packet at this level on this interface, these AESOs should be present.</p> <p>Beyond being recognized, no further processing of AESO information is performed. AESO contents are not checked and are assumed to be valid if the source is listed in the configurable AESO table.</p> <p>Configuring any per-interface extended IPSO information automatically enables ip security extended-allowed (disabled by default).</p>	
Examples	<p>In the following example, the extended security option source is defined as 5, and the compartment bits are set to 5.</p> <pre>Switch# configure terminal Switch(config)# interface ethernet 0 Switch(config-if)# ip security aeso 5 5</pre>	
Related Commands	Command	Description
	ip security eso-info	Cisco IOS command removed from this manual.
	ip security eso-max	Specifies the maximum sensitivity level for an interface.

ip security dedicated

To set the level of classification and authority on the interface, use the **ip security dedicated** interface configuration command. To reset the interface to default (disabled), use the **no** form of this command.

ip security dedicated *level authority [authority...]*

no ip security dedicated [*level authority [authority...]*]

Syntax Description	<i>level</i>	Degree of sensitivity of information. The <i>level</i> keywords are listed in Table 9-2.
	<i>authority</i>	Organization that defines the set of security levels that is used in a network. The <i>authority</i> keywords are listed in Table 9-3.

Defaults	Disabled
----------	----------

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	11.1(4)	New command

Usage Guidelines All traffic entering the system on this interface must have a security option that exactly matches this label. Any traffic leaving through this interface has this label attached.

The following definitions apply to the descriptions of the IPSO in this section:

- **level**—The degree of sensitivity of information. For example, data marked TOPSECRET is more sensitive than data marked SECRET. The level keywords and their corresponding bit patterns are shown in Table 9-2.

Table 9-2 PSO Level Keywords and Bit Patterns

Level Keyword	Bit Pattern
Reserved4	0000 0001
TopSecret	0011 1101
Secret	0101 1010
Confidential	1001 0110
Reserved3	0110 0110
Reserved2	1100 1100
Unclassified	1010 1011
Reserved1	1111 0001

- **authority**—An organization that defines the set of security levels used in a network. For example, the Genser authority consists of level names defined by the DCA. The authority keywords and their corresponding bit patterns are shown in Table 9-3.

Table 9-3 PSO Authority Keywords and Bit Patterns

Authority Keyword	Bit Pattern
Genser	1000 0000
Siop-Esi	0100 0000
DIA	0010 0000
NSA	0001 0000
DOE	0000 1000

- **label**—A combination of a security level and an authority or authorities.

Examples

The following example sets a confidential level with Genser authority.

```
Switch# configure terminal
Switch(config)# ip security dedicated confidential Genser
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.

ip security eso-max

To specify the maximum sensitivity level for an interface, use the **ip security eso-max** interface configuration command. To return to the default, use the **no** form of this command.

ip security eso-max *source compartment-bits*

no ip security eso-max *source* [*compartment-bits*]

Syntax Description

<i>source</i>	ESO source. This is an integer from 1 through 255.
<i>compartment-bits</i>	Compartment bits, in hexadecimal.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.1(4)	New command

Usage Guidelines

This command is used to specify the minimum sensitivity level for a particular interface. Before the per interface compartment information for a particular NLESO source can be configured, the **ip security eso-info** global configuration command must be used to specify the default information.

On every incoming packet on the interface, these extended security options should be resent at the minimum level and should match the configured compartment bits. Every outgoing packet must have these ESOs.

On every packet transmitted or received on this interface, any NLESO sources present in the IP header should be limited by the minimum sensitivity level and by the maximum sensitivity level configured for the interface.

When transmitting locally generated traffic out this interface or adding security information (with the **ip security add** command), the maximum compartment bit information can be used to construct the NLESO sources placed in the IP header.

A maximum of 16 NLESO sources can be configured per interface. Due to IP header length restrictions, a maximum of nine of these NLESO sources appear in the IP header of a packet.

Examples

In the following example, the specified ESO source is 240, and the compartment bits are specified as 500.

```
Switch# configure terminal
Switch(config)# interface ethernet 0
Switch(config-if)# ip security eso-max 240 500
```

Related Commands	Command	Description
	ip security eso-info	Cisco IOS command removed from this manual.
	ip security add	Adds a basic security option to all outgoing packets.

ip tcp chunk-size

To alter the TCP maximum read size for Telnet or rlogin, use the **ip tcp chunk-size** global configuration command. To restore the default value, use the **no** form of this command.

ip tcp chunk-size *characters*

no ip tcp chunk-size

Syntax Description	<i>characters</i>	Maximum number of characters that Telnet or rlogin can read in one read instruction.
---------------------------	-------------------	--

Defaults	0, which Telnet and rlogin interpret as the largest possible 32-bit positive number.
-----------------	--

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.2(5)	New command

Usage Guidelines	Do not use this command unless you understand why you need to change the default value.
-------------------------	---

Examples	The following example sets the maximum TCP read size to 64000 bytes.
-----------------	--

```
Switch# configure terminal
Switch(config)# ip tcp chunk-size 64000
```

ip tcp queuemax

To alter the maximum TCP outgoing queue per connection, use the **ip tcp queuemax** global configuration command. To restore the default value, use the **no** form of this command.

ip tcp queuemax *packets*

no ip tcp queuemax

Syntax Description	<i>packets</i> Outgoing queue size of TCP packets.				
Defaults	The default value is 5 segments if the connection has a TTY associated with it. If there is no TTY associated with it, the default value is 20 segments.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>11.2(5)</td> <td>New command</td> </tr> </tbody> </table>	Release	Modification	11.2(5)	New command
Release	Modification				
11.2(5)	New command				
Usage Guidelines	Changing the default value only changes the queue that has a TTY associated with the connection.				
Examples	<p>The following example sets the maximum TCP outgoing queue to 10 packets.</p> <pre>Switch(config)# ip tcp queuemax 10</pre>				

ip tcp synwait-time

To set a period of time the switch router waits while attempting to establish a TCP connection before it times out, use the **ip tcp synwait-time** global configuration command. To restore the default time, use the **no** form of this command.

ip tcp synwait-time *seconds*

no ip tcp synwait-time *seconds*

Syntax Description	<i>seconds</i> Time in seconds the switch router waits while attempting to establish a TCP connection. It can be an integer from 5 to 300 seconds. The default is 30 seconds.
---------------------------	---

Defaults	30 seconds
-----------------	------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.1(4)	New command

Usage Guidelines	<p>If your network contains PSTN DDR, it is possible that the call setup time exceeds 30 seconds. This amount of time is not sufficient in networks that have dialup asynchronous connections because it affects your ability to Telnet over the interface (from the switch router) if the interface must be brought up. If you have this type of network, you might want to set this value to the UNIX value of 75.</p>
-------------------------	--

Because this is a host parameter, it does not pertain to traffic going *through* the switch, just for traffic originating *at* the switch. Because UNIX has a fixed 75-second timeout, hosts are unlikely to see this problem.

Examples	The following example configures the switch router to continue attempting to establish a TCP connection for 180 seconds.
-----------------	--

```
Switch(config)# ip tcp synwait-time 180
```