

CLI Command Reference

Revised: November 21, 2013, OL-26031-06

This chapter contains an alphabetical listing of commands for the Cisco ASR 901 Series Aggregation Services Router.

Note

For a general reference for Cisco IOS, see the documentation for Cisco IOS Software Releases 15.1S. The Cisco ASR 901 does not necessarily support all of the commands listed in the 15.1S documentation.

- asr901-ecmp-hash-config global-type
- asr901-ecmp-hash-config ipv4-type
- asr901-ecmp-hash-config ipv6-type
- asr901-ecmp-hash-config mpls-to-ip
- asr901-multicast source
- asr901-platf-frr enable
- asr901-platf-multicast enable
- asr901-platf-multi-nni-cfm
- bfd all-interfaces
- bfd interval
- channel-group (interface)
- channel-protocol (interface)
- class (policy-map)
- class cem
- clear platform ptp stats
- clock-port
- clock-destination
- clock source (interface)
- controller
- cpu traffic ppp set ip dscp cs
- cpu traffic ppp set mpls experimental topmost
- debug platform tcam error

Γ

- debug platform tcam info
- dejitter-buffer
- dmm responder hardware timestamp
- duplex
- encapsulation dot1q (service instance)
- encapsulation dot1ad
- esmc mode
- ethernet loopback
- idle-pattern
- interface vlan
- interface atm ima
- interface port-channel
- interface range
- ip tos
- 13-over-12 flush buffers
- load-interval
- mac-flap-ctrl
- match ip dscp
- match vlan
- mtu
- name
- negotiation
- network-clock clear switch
- network-clock eec
- network-clock external hold-off
- network-clock hold-off global
- network-clock hold-off
- network-clock input-source
- network-clock input-source controller
- network-clock output-source system
- network-clock quality-level
- network-clock revertive
- network-clock wait-to-restore
- network-clock wait-to-restore global
- network-clock set lockout
- network-clock switch force
- network-clock switch manual
- network-clock synchronization automatic

- network-clock synchronization ssm option
- payload-size
- police (percent)
- police (two rates)
- policy-map
- protocol (ATM)
- pseudowire-class
- ptp profile telecom
- ptp profile telecom
- ql-enabled rep segment
- rep block port
- rep platform vlb segment
- rep segment
- router isis
- service instance
- service-policy (policy-map class)
- set cos
- set dscp
- set ip dscp
- set ip precedence (policy-map)
- set ip precedence (route-map)
- set ip precedence tunnel
- set ip tos (route-map)
- set network-clocks
- set precedence
- shape (percent)
- shape (policy-map class)
- show asr901 multicast-support
- show atm cell-packing
- show cem circuit
- show cem platform
- show etherchannel
- show ethernet loopback
- show interface port-channel
- show interfaces rep
- show ip vrf
- show mac-address-table
- show network-clock synchronization

- show platform hardware
- show platform ptp state
- show platform ptp stats
- show platform ptp stats detailed
- show platform tcam detailed
- show platform tcam summary
- show policy-map
- show policy-map interface
- show ptp port running detail
- show rep topology
- show table-map
- show xconnect
- snmp mib rep trap-rate
- speed
- synce state master
- synce state slave
- synchronous mode
- table-map
- termination
- transport ipv4
- tune-buffer port
- xconnect logging redundancy

asr901-ecmp-hash-config global-type

To specify the equal-cost multi-path routing (ECMP) hashing algorithm at the global level, use the **asr901-ecmp-hash-config global-type** command in global configuration mode. To remove this configuration, use the **no** form of this command.

asr901-ecmp-hash-config global-type {hash-crc16-mode | hash-seed seed-value | hash-xor1-mode | hash-xor2-mode | hash-xor4-mode | hash-xor8-mode | tunnel-mode} add

no asr901-ecmp-hash-config global-type {hash-crc16-mode | hash-seed seed-value | hash-xor1-mode | hash-xor2-mode | hash-xor4-mode | hash-xor8-mode | tunnel-mode} add

Syntax Description		
	hash-crc16-mode	Enables hash CRC-16 modes.
	hash-seed	Enables hash seed value for hash computation.
	seed-value	Hash seed value.
	hash-xor1-mode	Enables hash XOR1 mode.
	hash-xor2-mode	Enables hash XOR2 mode.
	hash-xor4-mode	Enables hash XOR4 mode.
	hash-xor8-mode	Enables hash XOR8 mode.
	tunnel-mode	Enables tunnel mode to look into the inner header for tunneled packets.
	add	Adds hash mode.
Command Modes	Global configuration (config)#
Command History	Release	Modification
	15.3(2)S	This command was introduced on the Cisco ASR 901 Series Aggregation Services Routers.
	This command is used to configure the ECMP hash configurations for improved load distribution of traffic. The hash-crc16-mode algorithm is enabled by default for ECMP.	
Usage Guidelines		• • •
Usage Guidelines Examples	traffic. The hash-crc1	• • •

Related Commands	Command	Description
	asr901-ecmp-hash-con fig ipv4-type	Enables the ipv4-type of ECMP hash configurations.
	asr901-ecmp-hash-con fig ipv6-type	Enables the ipv6-type of ECMP hash configurations.
	asr901-ecmp-hash-con fig mpls-to-ip	Enables the mpls-to-ip type of ECMP hash configurations.

asr901-ecmp-hash-config ipv4-type

To specify equal-cost multi-path routing (ECMP) hashing algorithm for IPv4 configuration, use the **asr901-ecmp-hash-config ipv4-type** command in global configuration mode. To remove this configuration, use the **no** form of this command.

```
asr901-ecmp-hash-config ipv4-type {dest-addrs | dest-l4-port | l3-proto-id | outer-vlan |
src-addrs | src-intf | src-l4-port } add
```

no asr901-ecmp-hash-config ipv4-type {dest-addrs | dest-l4-port | l3-proto-id | outer-vlan | src-addrs | src-intf | src-l4-port } add

ntax Description	dest-addrs	Specifies the destination IPv4 address.
	dest-l4-port	Specifies the destination Layer 4 port.
	13-proto-id	Specifies the Layer 3 protocol identifier.
	outer-vlan	Specifies the outer virtual local area network (VLAN).
	src-addrs	Specifies the source IPv4 address.
	src-intf	Specifies the source or the incoming interface.
	src-l4-port	Specifies the source Layer 4 port.
	add	Adds IPv4 ECMP hash configuration.
ommand Modes	Global configuratio	on (config)#
ommand Modes ommand History	Global configuratio	on (config)# Modification
	Release 15.3(2)S This command is us of IP traffic. All the	Modification This command was introduced on the Cisco ASR 901 Series Aggregation

Related Commands	Command	Description
	asr901-ecmp-hash-con fig global-type	Enables the global-type of ECMP hash configurations.
	asr901-ecmp-hash-con fig ipv6-type	Enables the ipv6-type of ECMP hash configurations.
	asr901-ecmp-hash-con fig mpls-to-ip	Enables the mpls-to-ip type of ECMP hash configurations.

asr901-ecmp-hash-config ipv6-type

To specify equal-cost multi-path routing (ECMP) hashing algorithm for IPv6 configuration, use the **asr901-ecmp-hash-config ipv6-type** command in global configuration mode. To remove this configuration, use the **no** form of this command.

asr901-ecmp-hash-config ipv4-type {dest-addrs | dest-l4-port | ipv6-next-header | outer-vlan | src-addrs | src-intf | src-l4-port } add

no asr901-ecmp-hash-config ipv4-type {dest-addrs | dest-l4-port | ipv6-next-header | outer-vlan | src-addrs | src-intf | src-l4-port } add

Syntax Description		
	dest-addrs	Specifies the destination IPv6 address.
	dest-l4-port	Specifies the destination Layer 4 port.
	ipv6-next-header	Specifies the source or the incoming interface.
	outer-vlan	Specifies the outer virtual local area network (VLAN).
	src-addrs	Specifies the source IPv4 address.
	src-intf	Specifies the source or the incoming interface.
	src-l4-port	Specifies the source Layer 4 port.
	add	Adds IPv6 ECMP hash configuration.
Command Default	The ECIVIF paralleter	s, such as dest-l4-port , src-intf , and src-l4-port , are disabled by default.
Command Modes	Global configuration ((config)#
Command History	Release	Modification
Command History	Release 15.3(2)S	Modification This command was introduced on the Cisco ASR 901 Series Aggregation Services Routers.
	This command is used of IP traffic. All the E	This command was introduced on the Cisco ASR 901 Series Aggregation
Command History Usage Guidelines Examples	This command is used of IP traffic. All the E src-14-port . You shou	This command was introduced on the Cisco ASR 901 Series Aggregation Services Routers.

Related Commands	Command	Description
	asr901-ecmp-hash-con fig global-type	Enables the global-type of ECMP hash configurations.
	asr901-ecmp-hash-con fig ipv4-type	Enables the IPv4-type of ECMP hash configurations.
	asr901-ecmp-hash-con fig mpls-to-ip	Enables the mpls-to-ip type of ECMP hash configurations.

OL-26031-06

asr901-ecmp-hash-config mpls-to-ip

To specify equal-cost multi-path routing (ECMP) hashing algorithm for Multiprotocol Label Switching (MPLS) to IP configuration, use the **asr901-ecmp-hash-config mpls-to-ip** command in global configuration mode. To remove this configuration, use the **no** form of this command.

asr901-ecmp-hash-config mpls-to-ip {dest-addrs | dest-l4-port | l3-proto-id | outer-vlan | src-addrs | src-intf | src-l4-port } add

no asr901-ecmp-hash-config mpls-to-ip {dest-addrs | dest-l4-port | l3-proto-id | outer-vlan | src-addrs | src-intf | src-l4-port } add

Syntax Description		
	dest-addrs	Specifies the destination IPv4 address.
	dest-l4-port	Specifies the destination Layer 4 port.
	13-proto-id	Specifies the Layer 3 protocol ID.
	outer-vlan	Specifies the outer virtual local area network (VLAN).
	src-addrs	Specifies the source IPv4 address.
	src-intf	Specifies the source or the incoming interface.
	src-l4-port	Specifies the source Layer 4 port.
	add	Adds ECMP hash configuration.
Command Modes	Global configuratio	n (config)#
Command History	Release	
	nonouoo	Modification
	15.3(2)S	Modification This command was introduced on the Cisco ASR 901 Series Aggregation Services Routers.
Usage Guidelines	This command is us parameters are enabled	This command was introduced on the Cisco ASR 901 Series Aggregation
Usage Guidelines Examples	This command is us parameters are enab the asr901-ecmp-h	This command was introduced on the Cisco ASR 901 Series Aggregation Services Routers. Seed to configure MPLS to IP-type ECMP hash configurations. All the ECMP oled by default except dest-14-port , src-intf , and src-14-port . You should configure ash-config mpls-to-ip command to enable them.

Related Commands	Command	Description
	asr901-ecmp-hash-con fig global-type	Enables the global-type of ECMP hash configurations.
	asr901-ecmp-hash-con fig ipv4-type	Enables the IPv4-type of ECMP hash configurations.
	asr901-ecmp-hash-con fig ipv6-type	Enables the IPv6-type of ECMP hash configurations.

asr901-multicast source

To send the multicast packets to the CPU enabling it to transmit register packets to Rendezvous Point (RP), use the **asr901-multicast source** command on the interface configuration mode. Use the **no** form of the command to disable transmission of multicast packets.

asr901-multicast source

no asr901-multicast source

Syntax Description	This command has no	o arguments or keywords.
--------------------	---------------------	--------------------------

Command Default This command is enabled by default.

Command Modes Interface configuration (config-if)#

Command History	Release	Modification
	15.4(1)S	This command was introduced on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines This command should be enabled on the SVI interface that is connected to the traffic source. After the configuration, normal Protocol Independent Multicast sparse mode (PIM-SM) register process begins.

Examples This example shows how to enable multicast on a Cisco ASR 901 series router:

Router# configure terminal Router(config)# interface type number Router(config-if)# asr901-multicast source

asr901-platf-frr enable

To enable traffic engineering (TE) Fast Reroute (FRR) link protection on the Cisco ASR 901 router, use the **asr901-platf-frr** command in global configuration mode. To delete this configuration, use the **no** form of this command.

asr901-platf-frr enable

no asr901-platf-frr enable

Syntax Description	This command has no arguments or keywords.
--------------------	--

Command Default The TE-FRR functionality is not enabled.

Command Modes Global configuration (config)

Command History	Release	Modification
	15.2(2)SNG	This command was introduced.

Examples The following example shows how to enable TE-FRR on the Cisco ASR 901 router:

Router# configure terminal Router#(config) asr901-platf-frr enable

asr901-platf-multicast enable

To enable multicast on the Cisco ASR 901 series routers, use the **asr901-platf-multicast enable** command. Use the **no** form of the command to disable multicast.

asr901-platf-multicast enable

no asr901-platf-multicast enable

Syntax Description	This command	has no arguments	or keywords.
--------------------	--------------	------------------	--------------

Command Default This command is enabled by default.

Command Modes Global configuration (config)#

 Command History
 Release
 Modification

 15.4(1)S
 This command was introduced on the Cisco ASR 901 Series Aggregation

Usage Guidelines This command is used to enable platform multicast on a Cisco ASR 901 series router.

Services Routers.

Examples This example shows how to enable multicast on a Cisco ASR 901 series router: Router# configure terminal Router(config)# ip multicast-routing Router(config)# asr901-platf-multicast enable

Related Commands	nands Command Description	
	show asr901	Displays the platform support for IPv4 or IPv6 multicast on the Cisco ASR
	multicast-support	901 series routers.

asr901-platf-multi-nni-cfm

To enable the multi-Network-to-Network Interface Connectivity Fault Management (multi-NNI CFM) configuration, use the **asr901-platf-multi-nni-cfm** command. Use the **no** form of the command to enable the Synthetic Loss Measurement (SLM) over cross connect EVC configuration.

asr901-platf-multi-nni-cfm

no asr901-platf-multi-nni-cfm

Syntax Description	This command has no arguments of	or keywords.
--------------------	----------------------------------	--------------

- **Command Default** This command is enabled by default.
- **Command Modes** Global configuration (config)#

Command History	Release	Modification
	15.3(3)S	This command was introduced on the Cisco ASR 901 Series Aggregation
		Services Routers.

Usage GuidelinesThis command is used to enable multi-NNI CFM configuration or SLM over cross connect EVC
configuration on a Cisco ASR 901 router. You can configure by enabling or disabling the command. By
default, the multi-NNI CFM configuration is enabled. When you run the required command, a syslog is
generated so that you can save the configuration and reload the router. You should reload the router after
using the asr901-multi-nni-cfm command or no form of the command.

Examples

This example shows how to enable multi-NNI CFM over cross connect EVC configuration on a Cisco ASR 901 router:

Router# configure terminal Router(config)# asr901-platf-multi-nni-cfm

This example shows how to enable SLM over cross connect EVC configuration on a Cisco ASR 901 router:

Router# configure terminal Router(config)# no asr901-platf-multi-nni-cfm

bfd all-interfaces

To enable Bidirectional Forwarding Detection (BFD) for all interfaces participating in the routing process, use the **bfd all-interfaces** command in router configuration mode. To disable BFD for all interfaces, use the **no** form of this command.

bfd all-interfaces

no bfd all-interfaces

Syntax Description	This command	has no arguments	or keywords.
--------------------	--------------	------------------	--------------

Command Default BFD is not enabled on the interfaces participating in the routing process.

Command Modes Router configuration

Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.

Usage Guidelines There are two methods to configure routing protocols to use BFD for failure detection. To enable BFD for all neighbors of a routing protocol, enter the **bfd all-interfaces** command in router configuration mode. If you do not want to enable BFD on all interfaces, enter the **bfd interface** command in router configuration mode.

Examples The following example shows BFD enabled for all Intermediate System-to-Intermediate System (IS-IS) neighbors:

Router> enable
Router# configure terminal
Router(config)# router isis tag1
Router(config-router)# bfd all-interfaces
Router(config-router)# end

The following example shows BFD enabled for all Open Shortest Path First (OSPF) neighbors:

Router> enable
Router# configure terminal
Router(config)# router ospf 123
Router(config-router)# bfd all-interfaces
Router(config-router)# end

Related Commands	Command	Description
	bfd	Sets the baseline BFD session parameters on an interface.
	bfd interface	Enables BFD on a per-interface basis for a BFD peer.

bfd interval

To set the baseline Bidirectional Forwarding Detection (BFD) session parameters on an interface, use the **bfd** command in interface configuration mode. To remove the baseline BFD session parameters, use the **no** form of this command.

bfd interval milliseconds min_rx milliseconds multiplier multiplier-value

no bfd interval milliseconds min_rx milliseconds multiplier multiplier-value

Syntax Description	interval milliseconds	Specifies the rate at which BFD control packets will be sent to BFD peers. The configurable time period for the <i>milliseconds</i> argument is from 50 to 999 milliseconds (ms).	
	min_rx <i>milliseconds</i>	Specifies the rate at which BFD control packets will be expected to be received from BFD peers. The configurable time period for the <i>milliseconds</i> argument is from 1 to 999 milliseconds (ms).	
	multiplier multiplier-value	Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The configurable value range for the <i>multiplier-value</i> argument is from 3 to 50.	
Command Default	No baseline BFD sessio	n parameters are set.	
Command Modes	Interface configuration (config-if)		
Command History	Release	Modification	
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
Examples	The following example shows the BFD session parameters set for Fast Ethernet interface 3/0:		
	Router configure terminal Router(config)# interface vlan1 Router(config-if)# bfd interval 50 min_rx 3 multiplier 3 Router(config-if)# end		
Related Commands	Command	Description	
	bfd all-interfaces	Enables BFD for all interfaces for a BFD peer.	
	bfd interface	Enables BFD on a per-interface basis for a BFD peer.	
	ip ospf bfd	Enables BFD on a specific interface configured for OSPF.	

channel-group (interface)

To assign and configure an EtherChannel interface to an EtherChannel group, use the channel-group command in interface configuration mode. To remove the channel-group configuration from the interface, use the no form of this command.

channel-group number mode {active | on | passive}

no channel-group number

Syntax Description	number	Integer that identifies the channel-group. Valid values are from 1 to 256; the maximum number of integers that can be used is 64.		
		For Fast EtherChannel groups, the number is an integer from 1 to 4. This number is the one previously assigned to the port-channel interface.		
	mode	Specifies the EtherChannel mode of the interface.		
	active	Enables Link Aggregation Control Protocol (LACP) unconditionally.		
	on	Enables EtherChannel only.		
	passive	Enables LACP only when an LACP device is detected. This is the default state.		
Command Default	No channel groups	s are assigned.		
Command Modes	Interface configura	ation		
Command History	Release	Modification		
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.		
Usage Guidelines	The on Keyword			
	When you use the on keyword, a usable EtherChannel exists only when a port group in on mode is connected to another port group in the on mode.			
	You can change the channel group.	e mode for an interface only if it is the only interface that is designated to the specified		
	The on keyword forces the bundling of the interface on the channel without any negotiation.			
	With the on mode, a usable EtherChannel exists only when a port group in on mode is connected to another port group in on mode.			
		annel-group command on an interface that is added to a channel with a different protocol you are entering, the command is rejected.		
	If the interface belongs to a channel, the no form of this command is rejected.			
	All ports in the sar channel group.	All ports in the same channel group must use the same protocol; you cannot run two protocols on one channel group.		

You can change the protocol at any time, but this change causes all existing EtherChannels to reset to the default channel mode for the new protocol.

Configure all ports in an EtherChannel to operate at the same speed and duplex mode (full duplex only for LACP mode).

All ports in a channel must be on the same DFC-equipped module. You cannot configure any of the ports to be on other modules.

On systems that are configured with nonfabric-enabled modules and fabric-enabled modules, you can bundle ports across all modules, but those bundles cannot include a DFC-equipped module port.

You do not have to create a port-channel interface before assigning a physical interface to a channel group. A port-channel interface is created automatically when the channel group gets its first physical interface, if it is not already created.

You do not have to disable the IP address that is assigned to a physical interface that is part of a channel group, but it is highly recommended.

You can create both Layer 2 and Layer 3 port channels by entering the interface port-channel command or when the channel group gets its first physical interface assignment. The port channels are not created at runtime or dynamically.

Any configuration or attribute changes that you make to the port-channel interface are propagated to all interfaces within the same channel group as the port channel (for example, configuration changes are also propagated to the physical interfaces that are not part of the port channel but are part of the channel group).

When configuring Layer 2 EtherChannels, you cannot put Layer 2 LAN ports into manually created port-channel logical interfaces.



Caution Do not enable Layer 3 addresses on the physical EtherChannel interfaces. Assigning bridge groups on the physical EtherChannel interfaces causes loops in your network.

Examples

This example shows how to add EtherChannel interface 1/0 to the EtherChannel group that is specified by port-channel 1:

Router(config-if)# channel-group 1 mode on Router(config-if)#

Related Commands

Command	Description	
interface	Creates a port-channel virtual interface and puts the CLI in interface configuration mode when the port-channel keyword is used.	
ip address	Sets a primary or secondary IP address on an interface.	
show etherchannel	Displays the EtherChannel information for a channel.	
show interfaces port-channel	Displays traffic that is seen by a specific port channel.	

channel-protocol (interface)

To enable Link Aggregation Control Protocol (LACP) on an interface to manage channeling, use the **channel-protocol** command in interface configuration mode. Use the **no** form of this command to deselect the protocol.

channel-protocol {lacp}

no channel-protocol

Syntax Description	lacp	Specifies LACP to manage channeling.	
Command Modes	Interface configuratio	n	
Command History	Release	Modification	
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
Usage Guidelines	This command is valid	d on multiple interfaces (for example, Fast Ethernet) and routers and switches.	
Examples	The following exampl	le shows how to set the lacp.	
	(config-if)# channel-protocol lacp		

class (policy-map)

To specify the name of the class whose policy you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy, use the **class** command in policy-map configuration mode. To remove a class from the policy map, use the **no** form of this command.

class {class-name | class-default}

no class {*class-name* | **class-default**}

Syntax Description	class-name	Name of the class to be configured or whose policy is to be modified. The class name is used for both the class map and to configure a policy for the class in the policy map.	
	class-default	Specifies the default class so that you can configure or modify its policy.	
Command Default	No class is specifie	d.	
Command Modes	Policy-map configu	uration (config-pmap)	
Command History	Release	Modification	
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
Usage Guidelines	Policy Map Configuration Mode Within a policy map, the class (policy-map) command can be used to specify the name of the class whose policy you want to create or change. First, the policy map must be identified.		
Usage Guidelines	Within a policy map, the class (policy-map) command can be used to specify the name of the class whose		
	command before yo	cy map (and enter the required policy-map configuration mode), use the policy-map ou use the class (policy-map) command. After you specify a policy map, you can r new classes or modify the policy for any existing classes in that policy map.	
	Class Characteristics	3	
		t you specify in the policy map ties the characteristics for that class—that is, its s map and its match criteria, as configured using the class-map command.	
	interface, class-base	e policy for a class and specify its bandwidth and attach the policy map to an ed weighted fair queueing (CBWFQ) determines if the bandwidth requirement of the ed. If so, CBWFQ allocates a queue for the bandwidth requirement.	
		noved, available bandwidth for the interface is incremented by the amount previously	
	allocated to the clas	SS.	

Predefined Default Class

The **class-default** keyword is used to specify the predefined default class called class-default. The class-default class is the class to which traffic is directed if that traffic does not match any of the match criteria in the configured class maps.

```
      Examples
      The following example configures a class policy included in the policy map called policy1. Class2 specifies policy for traffic with a CoS value of 2.

      ! The following commands create class-maps class1 and class2

      ! and define their match criteria:

      class-map class2

      match cos 2

      ! The following commands create the policy map, which is defined to contain policy

      ! specification for class2:

      policy-map policy1

      Router(config-pmap)# class class2

      Router(config-pmap)# class class2
```

Router(config-pmap-c)# random-detect

Router(config-pmap-c)#

Related Commands	Command	Description
	bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
	class-map	Creates a class map to be used for matching packets to a specified class.
	fair-queue (class-default)	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
	policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
	queue-limit	Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
	random-detect (interface)	Enables WRED or DWRED.
	random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
	random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.

class cem

To configure CEM interface parameters in a class that is applied to CEM interfaces together, use the **class cem** command in global configuration mode. This command works in the same manner for CEM interfaces as the **pseudowire-class** command does for xconnect.

class cem class-name

Syntax Description	class-name	The name of a CEM interface parameters class.	
Command Modes	Global configura	ation	
Command History	Release	Modification	
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
Usage Guidelines		ommand allows you to configure CEM interface parameters in a class that is applied to to together. A class cem command includes the following configuration settings:	
	• dejitter-buf	f fer dejitter-in-ms	
	• idle-pattern 8-bit-idle-pattern		
	 payload-siz 	e payload-size-in-ms	
Note	-	e the performance of packet reordering on TDM/PWE connections by using the ze of the dejitter buffer using the dejitter-buffer parameter.	
Examples	The following ex Router# config Router (config) Router (config) Router (config) Router (config) Router (config) Router (config) Router (config)	<pre>xample shows how to configure CEM interface parameters: t # class cem mycemclass cem-class)# dejitter-buffer 10 cem-class)# exit # interface cem 0/0 if)# no ip address if)# cem 0 if-cem)# xconnect 10.10.10 200 encapsulation mpls if-cem.y# xconnect 10.10.10.10 200 encapsulation mpls if-cem.y# exit if-cem.y# exit</pre>	

Related Commands	Command	Description
	dejitter-buffer	Specifies the size of the dejitter buffer used for network jitter in CEM configuration mode.
	idle-pattern	Specifies the data pattern to transmit on the T1/E1 line when missing packets are detected on the PWE3 circuit in CEM configuration mode.
	cem	Enters circuit emulation configuration mode.

clear platform ptp stats

To clear the statistics of ptp protocol on the Cisco ASR 901 router, use the **clear platform ptp stats** command.

clear platform ptp stats

Syntax Description	This command has no arguments.		
Command Modes	Privileged EXEC		
Command History	Release	Modification	
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
Examples	The following example shows sample output for clear platform ptp stats command: Router# clear platform ptp stats PTP counters cleared		
Related Commands	Command show platform ptp sta	Description Its Displays statistics about the ptp protocol on the Cisco ASR 901	
		router.	

clock-port

Specifies the mode of a PTP clock port.

clock-port port-name port-role

no clock-port *port-name port-role*

Syntax Description	name	Specifies a name for the clock port.
,	port-role	Specifies the role of the clock port, which can be slave or master.
	pontrole	 slave—Sets the clock port to PTP slave mode; the port exchanges timing packets with a PTP master device.
		• master—Sets the clock port to PTP master mode; the port exchanges timing packets with PTP slave devices.
Defaults	This command i	s disabled by default.
command Modes	PTP clock config	guration mode
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
	13.1(2)51(0	Support for this command was introduced on the Cisco ASK 901 fouter.
xamples		support for this command was introduced on the Cisco ASK 901 fouter.
Examples	The following ex Router# config Router(config) Router(config) Router(config)	cample shows how to configure a PTP clock port.
Examples Related Commands	The following ex Router# config Router(config) Router(config) Router(config)	<pre>kample shows how to configure a PTP clock port. terminal # ptp clock ordinary domain 0 ptp-clk)# clock-port SLAVE slave ptp-port)# transport ipv4 unicast interface loopback</pre>

I

clock-destination

Specifies the IP address of a clock destination. This command applies only when the router is in PTP master unicast mode.

ptp clock-destination clock-ip-address

no ptp clock-destination clock-ip-address

Syntax Description	<i>clock-ip-address</i> The IP address of the clock destination.	
Defaults	There is no default s	etting.
Command Modes	Interface configurati	on
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Examples	The following exam	ple shows how to configure a PTP announcement:
Examples	Router(config-ptp-clk)# clock-port MASTER Master Router(config-ptp-port)# transport ipv4 unicast interface loopback Router(config-ptp-port)#clock destination 8.8.8.2	
	Router(config-if)# Router(config)# ex	
Related Commands	Command	Description
	ptp enable	Enables PTP mode on an interface.
	ptp enable ptp master	Enables PTP mode on an interface. Sets an interface in master clock mode for PTP clocking

clock source (interface)

To set the clock source on the interface, use the **clock source** command in interface configuration mode. To restore the default clock source, use the **no** form of this command.

clock source clock-ip-address

no clock source clock-ip-address

Syntax Description	clock-ip-address T	The IP address of the clock source.
Defaults	There is no default sett	ing.
Command Modes	Interface configuration mode.	
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Examples	The following example	instructs the controller to use an internal clock source:
Examples		k) # clock-port SLAVE slave
	Router(config-ptp-po:	rt)# transport ipv4 unicast interface loopback 0
	Router(config-ptp-port)# clock source 2.2.2.2 Router(config-if)# exit Router(config)# exit	
Related Commands	Command	Description
	ptp slave	Sets an interface in slave clock mode for PTP clocking
	ptp mode	Specifies the PTP mode.
	ptp clock-destination	Specifies a PTP clock destination.

controller

To configure a T1 or E1 controller and enter controller configuration mode, use the **controller** command in global configuration mode.

controller {t1 | e1 } slot/port/subslot number/port number

Syntax Description	t1 T1	1 controller.			
		E1 controller.			
	slot/port Ba				
	<i>subslot</i> Defines the subslot on the router in which the HWIC is installed. <i>number</i>				
	1	portPort number of the controller. Valid numbers are 0 and 1. The slash mark (/) isrequired between the <i>slot</i> argument and the <i>port</i> argument.			
Defaults Command Modes	No T1 or E1 controller is configured. Global configuration				
Command History	Release	Modification			
Command History		Modification Support for this command was introduced on the Cisco ASR 901 router.			
Command History Related Commands	Release				
	Release 15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router. Description			

cpu traffic ppp set ip dscp cs

To re-mark the CPU generated traffic from default value (DSCP CS6) to the desired differentiated service code point (DSCP) value for QoS treatment, use the **cpu traffic ppp set ip dscp cs** command on the global configuration mode. Use the **no** form of the command to reset matching of packets with DSCP Certificate Server (CS).

cpu traffic ppp set ip dscp cs

no cpu traffic ppp set ip dscp cs

Syntax Description	This command has no arguments or keywords.	
Command Default	None	
Command Modes	Global configuration (c	config)#
Command History	Release	Modification
	15.4(1)S	This command was introduced on the Cisco ASR 901 Series Aggregation Services Routers.
Usage Guidelines		to mark the CPU generated traffic transmitted through MLPPP Interface. It vide desired QoS treatment to CPU generated traffic. The valid values are from
Examples	value for QoS treatmen Router# configure ter	w to re-mark the CPU generated traffic from default value to the desired DSCP t on a Cisco ASR 901 series router: rminal traffic ppp set ip dscp cs5

cpu traffic ppp set mpls experimental topmost

To re-mark the CPU generated traffic from default value (MPLS EXP 6) to the desired EXP value for QoS treatment, use the **cpu traffic ppp set mpls experimental topmost** command on the global configuration mode. Use the **no** form of the command to revert to the default values.

cpu traffic ppp set mpls experimental topmost value

no cpu traffic ppp set mpls experimental topmost value

Syntax Description	value	Multiprotocol Label Switching (MPLS) EXP field in the topmost label header. Valid values are 0 to 7.
Command Default	None	
Command Modes	Global configura	tion (config)#
Command History	Release	Modification
	15.4(1)S	This command was introduced on the Cisco ASR 901 Series Aggregation Services Routers.
Usage Guidelines		s used to mark the CPU generated traffic transmitted through MLPPP Interface. It to provide desired QoS treatment to CPU generated traffic. The valid values are from 0
Examples	-	ows how to re-mark the CPU generated traffic from default value to the desired MPLS oS treatment on a Cisco ASR 901 series router:
	Router# config Router(config)#	re terminal cpu traffic ppp set mpls experimental topmost 6

debug platform tcam error

To enable Ternary Content Addressable Memory (TCAM) error printing, use the **debug platform tcam error** command in the privileged EXEC mode. To disable TCAM error printing, use the **no debug platform tcam error** command.

debug platform tcam error

no debug platform tcam error

Syntax Description	This command has n	o arguments or	keywords.
--------------------	--------------------	----------------	-----------

Command ModesPrivileged EXEC (#)

Command History	Release	Modification
	15.3(2)S	This command was introduced on the Cisco ASR 901 Series Aggregation Services Routers.

Examples

The following is sample output from the **debug platform tcam error** command:

Router# **debug platform tcam error** TCAM Error printing turned ON

debug platform tcam info

To enable TCAM info printing, use the **debug platform tcam info** command in the privileged EXEC mode. To disable TCAM info printing, use the **no debug platform tcam info** command.

debug platform tcam info

no debug platform tcam info

Command Modes Privileged EXEC (#)

Command History	Release	Modification	
	15.3(2)S	This command was introduced on the Cisco ASR 901 Series Aggregation Services Routers.	

Examples

The following is sample output from the **debug platform tcam info** command:

Router# **debug platform tcam info** TCAM Info printing turned ON

dejitter-buffer

To configure the size of the dejitter buffer, use the **dejitter-buffer** command in CEM configuration mode. To restore the dejitter buffer to its default size, use the **no** form of this command.

dejitter-buffer size

no dejitter-buffer

Syntax Description	size	Specifies the size of the dejitter buffer in milliseconds. The range is 4 to 500 ms; the default is 4 ms.	
Defaults	The default dejitter-buffer size is 4 milliseconds.		
Command Modes	CEM configuration		
Command History	Release	Modification	
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
Examples	The following example shows how to specify the size of the dejitter buffer: Router# config t Router(config)# interface cem 0/0 Router(config-if)# no ip address Router(config-if)# cem 0 Router(config-if-cem)# dejitter-buffer 10 Router(config-if-cem)# xconnect 10.10.10 200 encapsulation mpls Router(config-if-cem)# exit Router(config-if-cem)# exit Router(config-if)# exit Router(config-if)# exit		
Related Commands	Command	Description	
	cem	Enters circuit emulation configuration mode.	
	cem class	Applies the CEM interface parameters defined in the given CEM class name to the circuit.	
	class cem	Configures CEM interface parameters in a class that's applied to CEM interfaces together in global configuration mode.	

dmm responder hardware timestamp

To configure hardware-based timestamping, use the **dmm responder hardware timestamp** command in Maintenance End Point (MEP) configuration mode. To disable hardware-based time stamping, use the **no** form of this command.

dmm responder hardware timestamp

no dmm responder hardware timestamp

Syntax Description	This command has no	arguments or keywords.
--------------------	---------------------	------------------------

Command Default Hardware-based timestamping is disabled on the receiver MEP.

Command Modes MEP configuration (config-if-srv-ecfm-mep)

Command History	Release	Modification
	15.3(2)\$	This command was introduced on the Cisco ASR 901 Series Aggregation Services Router.

```
Examples
```

The following example shows how to configure hardware-based timestamping on the receiver MEP:

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0
Router(config-if)# service instance 1310 ethernet ssvc1310
Router(config-if-srv)# encapsulation dot1q 1310
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 1310
Router(config-if-srv)# cfm mep domain sdmm mpid 1310
Router(config-if-srv-ecfm-mep)# dmm responder hardware timestamp
```

Related Commands	Command	Description	
	bridge-domain (service instance)	Binds a service instance or a MAC tunnel to a bridge domain instance.	
	cfm mep domain	Configures MEP for a domain.	
	encapsulation dot1q (service instance)	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance	
	rewrite ingress tag	Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance.	
	service instance ethernet	Configures an Ethernet service instance on an interface.	

duplex

To configure duplex operation on an interface, use the **duplex** command in interface configuration mode. Use the **no** form of this command to return to the default value.

duplex [full | half]

no duplex

Syntax Description	full Spe	ecifies full-duplex operation.
	half Spe	cifies half-duplex operation.
Defaults	Full-duplex mode	
Command Modes	Interface configu	ration
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.

Usage Guidelines Duplex Options and Interfaces

Table 2-1 lists the supported command options by interface.

Table 2-1Supported duplex Command Options

Interface Type	Supported Syntax	Default Setting	Usage Guidelines
Gigabit Ethernet Interfaces	duplex full	full	
10-Mbps ports	duplex [half full]	half	
100-Mbps ports	duplex [half full]	half	

If the transmission speed on a 16-port RJ-45 Gigabit Ethernet port is set to 1000, the duplex mode is set to full. If the transmission speed is changed to 10 or 100, the duplex mode stays at half duplex. You must configure the correct duplex mode when the transmission speed is changed to 10 or 100 from 1000.

Gigabit Ethernet is full duplex only. You cannot change the duplex mode on Gigabit Ethernet ports or on a 10/100/1000-Mbps port that is configured for Gigabit Ethernet.

When manually configuring the interface speed to either 10 or 100 Mbps, you should also configure the duplex mode on the interface.



Changing the interface speed and duplex mode configuration might shut down and reenable the interface during the reconfiguration.

Table 2-2 describes the interface behavior for different combinations of the **duplex** and **speed** command settings. The specified **duplex** command configured with the specified **speed** command produces the resulting system action.



If you need to force an interface port to operate with certain settings and therefore disable autonegotiation, you must be sure that the remote link is configured with compatible link settings for proper transmission. This includes support of flow control on the link.

duplex Command	speed Command	Resulting System Action
duplex half	speed 10	Forces 10-Mbps and half-duplex operation, and disables autonegotiation on the interface.
duplex full	speed 10	Forces 10-Mbps and full-duplex operation, and disables autonegotiation on the interface.
duplex half	speed 100	Forces 100-Mbps and half-duplex operation, and disables autonegotiation on the interface.
duplex full	speed 100	Forces 100-Mbps and full-duplex operation, and disables autonegotiation on the interface.
duplex full	speed 1000	Forces 1000-Mbps and full-duplex operation, and disables autonegotiation on the interface (Gigabit Ethernet only).

Table 2-2 Relationship Between duplex and speed Commands

Examples

The following example shows how to configure duplex half operation:

Router(config)# interface gigabitethernet0/0
Router(config-if)# duplex half

Related Commands

Command	Description
interface	Selects an interface to configure and enters interface configuration mode.
interface gigabitethernet	Selects a particular Gigabit Ethernet interface for configuration.
show controllers	Displays information that is specific to the hardware on a module.
show controllers gigabitethernet	Displays Gigabit Ethernet interface information, transmission statistics and errors, and applicable MAC destination address and VLAN filtering tables.
show interfaces	Displays traffic that is seen by a specific interface.
show interfaces gigabitethernet	Displays information about the Gigabit Ethernet interfaces.
speed	Sets the port speed for a Fast Ethernet interface.

encapsulation dot1q (service instance)

To define the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance, use the **encapsulation dot1q** command in the service instance mode. To delete the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance, use the **no** form of this command.

encapsulation dot1q vlan-id[,vlan-id[-vlain-id]] [native]

no encapsulation dot1q *vlan-id*[*,vlan-id*[*-vlain-id*]] [**native**]

Syntax Description	vlan-idVLAN ID, integer in the range 1 to 4094. Hyphen must be entered to separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs. Optional) Comma must be entered to separate each VLAN ID range from the next range.		
	native	(Optional) Sets the VLAN ID value of the port to the value specified by the <i>vlan-id</i> argument.	
Command Default	No matching c	criteria are defined.	
Command Modes	Service instand	ce	
Command History	Release	Modification	
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
Usage Guidelines	The criteria fo	r this command are: single VLAN, range of VLANs, and lists of the previous two.	
	U U	Q service instance, allows one VLAN, multiple VLANs, or a range of VLANs. The native only be set if a single VLAN tag has been specified.	
	Only a single s	service instance per port is allowed to have the native keyword.	
	Only one enca	psulation command may be configured per service instance.	
Examples	The following service instance	example shows how to map 802.1Q frames ingress on an interface to the appropriate ce:	
	Router (config	g-if-srv)# encapsulation dot1g 10	

Related	Commands
---------	----------

ommands	Command	Description
	encapsulation dot1q second-dot1q	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
	encapsulation untagged	Defines the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance.

encapsulation dot1ad

To define the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance, use the encapsulation dot1ad command in the service instance mode. To delete the matching criteria to map 802.1ad frames ingress on an interface to the appropriate service instance, use the no form of this command.

encapsulation dot1ad {vlan-id[,vlan-id[-vlain-id]] | any}

no encapsulation dot1ad

Syntax Description	vlan-id	 VLAN ID, integer in the range 1 to 4094. Hyphen must be entered to separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs. (Optional) Comma must be entered to separate each VLAN ID range from the next range. Matches any packet with one or more VLANs.
	any	Matches any packet with one of more vLANS.
Command Default	No matching criteria are	e defined.
Command Modes	Service instance	
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines	-	osulation dot1ad causes the router to categorize the interface as an 802.1ad pecial processing for certain protocols and other features:
	• MSTP uses the IEE	EE 802.1ad MAC STP address instead of the STP MAC address.
	Certain QoS function	ons may use the Drop Eligibility (DE) bit of the IEEE 802.1ad tag.
	The encapsulation dot interface) port.	1ad command requires the interface to be of dot1ad nni (network-network
Related Commands	Command	Description
	encapsulation dot1q	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.

Command	Description
encapsulation dot1q second dot1q	Double-tagged 802.1Q encapsulation. Matching criteria to be used to map QinQ frames ingress on an interface to the appropriate EFP. The outer tag is unique and the inner tag can be a single VLAN, a range of VLANs or lists of VLANs or VLAN ranges.
encapsulation untagged	Matching criteria to be used to map untagged (native) Ethernet frames entering an interface to the appropriate EFP.

esmc mode

To enable or disable ESMC process on the interface, use the **esmc mode** command in interface configuration mode. Use the **no** form of this command to disable the configuration

esmc mode <*tx* | *rx* >

no esmc mode

SyntaDescription	tx Tr	ansmission mode
	rx Re	eceiving mode
Command Default	Enabled for synchronous mo	de and disabled for asynchronous mode.
Command Modes	Interface configuration (conf	äg-if)
Command History	Release Mo	odification
	15.1(2)SNG Su	pport for this command was introduced on the Cisco ASR 901 router.
		is removed from selectable clock source list. By default this is enabled for
	synchronous mode and disab	oled for asynchronous mode.
Note	This command is not suppor	ted for non-synchronous ethernet interfaces.
Note	This command is not support The following example show	ted for non-synchronous ethernet interfaces.
	This command is not suppor	ted for non-synchronous ethernet interfaces.
	This command is not support The following example show	ted for non-synchronous ethernet interfaces.
Examples	This command is not support The following example show Router(config-if)#esmc mo	ted for asynchronous mode. ted for non-synchronous ethernet interfaces. //s how to enable ESMC process: de tx
Examples	This command is not support The following example show Router(config-if)#esmc mo Command	ted for asynchronous mode. ted for non-synchronous ethernet interfaces. s how to enable ESMC process: de tx Description

ethernet loopback

To start or stop an ethernet loopback function on an interface, use the **ethernet loopback** privileged EXEC command.

ethernet loopback start local interface type number [service instance instance-number] {external | internal} source mac-address source-address [destination mac-address destination-address] timeout {time-in-seconds | none}

or

ethernet loopback stop local interface type number id session id

Syntax Description	start	Starts the Ethernet loopback operation configured on the interface.
	stop	Stops the Ethernet loopback operation configured on the interface.
	local interface <i>type number</i>	Specifies the interface on which to start or stop the loopback operation.
	service-instance instance-number	Specifies the service instance ID. This is an optional field.
	external internal source mac-address source-address	Specifies the external or internal source MAC address for the loopback operation.
	destination mac-address destination-address	Specifies the destination MAC address for the loopback operation. This is an optional field.
	timeout { <i>time-in-seconds</i>	Specifies the timeout interval in seconds. The range is from 0 to 90000 seconds. The default is 300 seconds.
	none}	Specify timeout none to set the loopback to no time out.
	id session id	Specifies the data plane loopback session ID. The range is from 1 to 3.
	all	Stop all Ethernet loopback operations on the switch. This keyword is available only after the stop keyword.
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	15.2(2)SNG	This command was introduced on the Cisco ASR 901 router.
Usage Guidelines		al loopback. You can configure ethernet loopback and use the ethernet loopback back stop command only for physical ports and not for VLANs.

Examples	The following example shows how to start a facility port loopback process, verify it, and then to stop it:
	Router(config)# interface gigabitEthernet0/1
	Router(config-if)# service instance 10 ethernet
	Router(config-if-srv)# encapsulation dotlq 10
	Router(config-if-srv)# rewrite ingress tag pop1
	Router(config-if-srv)# bridge domain 10
	Router(config-if-srv)# end
	Router# ethernet loopback start local interface gigabitEthernet 0/1 service instance 10
	internal source mac-address 0123.4567.89ab destination mac-address 255.255.255 timeout
	9000
	Router# ethernet loopback stop local interface gigabitEthernet 0/1 id 3

Related Commands	Command	Description
	show ethernet loopback	Shows information about the per port Ethernet loopbacks configured on a router or an interface.
		on a router of an interface.

ethernet oam remote-failure action

To enable Ethernet Operations, Administration, and Maintenance (OAM) remote failure actions, use the **ethernet oam remote-failure action** command in interface configuration mode. To turn off remote failure actions, use the **no** form of this command.

ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action error-disable-interface

no ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action

Syntax Description	critical-event	Specifies remote critical event failures.
	dying-gasp	Specifies remote dying-gasp failures.
	link-fault	Specifies remote link-fault failures.
	error-disable-interface	Disables the interface when an error occurs.
Command Default	Actions in response to Et	hernet OAM remote failures do not occur.
Command Modes	Interface configuration (c	config-if)
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines	events occur.	figure an interface to take specific actions when Ethernet OAM remote-failure s not support sending critical-event messages but can receive all three message
Examples	The following example sh critical event occurs:	nows how to configure the action that the Ethernet 1/1 interface takes when a

idle-pattern

To specify the data pattern transmitted on the T1/E1 line when missing packets are detected on the PWE3 circuit, use the **idle-pattern** command in CEM configuration mode. To stop sending idle pattern data, use the **no** form of this command.

idle-pattern [pattern]

no idle-pattern

Syntax Description	pattern	(Optional) An 8-bit hexadecimal number that is transmitted as the idle pattern. T1 and E1 channels require only this argument.
Defaults	For T1 or E1 chanr	nels, the default idle pattern is 0xFF.
Command Modes	CEM circuit configuration	
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines	The idle-pattern da	ta is sent to replace the data from missing packets.
xamples	The following exar	nple shows how to specify a data pattern:
	Router# config t Router(config)# interface cem 0/0	
	Router(config-if)# no ip address Router(config-if)# cem 0	
	Router(config-if-cem)# idle-pattern 0x55	
	Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls Router(config-if-cem-xconn)# exit	
	Router(config-if-cem)# exit Router(config-if)# exit Router(config)# exit	
Related Commands	Command	Description
	cem	Enters circuit emulation configuration mode.
	cem class	Applies the CEM interface parameters defined in the given CEM class name to the circuit.
	class cem	Configures CEM interface parameters in a class that's applied to CEM interfaces together in global configuration mode.

interface vlan

To create a dynamic Switch Virtual Interface (SVI), use the **interface vlan** command in global configuration mode.

interface vlan vlanid

no interface vlan vlanid

Syntax Description	vlanid	Unique VLAN ID number (1 to 4094) used to create or access a VLAN.
Command Default	None	
Command Modes	Global configuration	on
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines	The vlanid value co Link (ISL), the 802	e first time that you enter the interface vlan <i>vlanid</i> command for a particular VLAN. presponds to the VLAN tag that is associated with the data frames on an Inter-Switch 2.1Q-encapsulated trunk, or the VLAN ID that is configured for an access port. A whenever you create a new VLAN interface, so that you can check if you entered the aber.
	part (IDP) pair is fo	I by entering the no interface vlan <i>vlanid</i> command, the associated initial domain orced into an administrative down state and is marked as deleted. The deleted interface in the show interface command.
		deleted SVI by entering the interface vlan <i>vlanid</i> command for the deleted interface. es back up, but much of the previous configuration is gone.
Examples	The following exar VLAN number:	nple shows the output when you enter the interface vlan vlanid command for a new
	Router(config)# i % Creating new VI	

interface atm ima

To configure an ATM IMA group and enter interface configuration mode, use the **interface atm ima** global configuration command. If the group does not exist when the command is issued, the command automatically creates the group.

interface atm slot/imagroup-number

Syntax Description	slot	Specifies the slot location of the ATM IMA port adapter.
	group-number	Specifies an IMA group number from 0 to 3. You can create up to four groups.
Defaults	The interface includes in	ndividual ATM links, but no IMA groups.
Command Modes	Global configuration	
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines	Specifying ATM links a	ed for IMA functionality, it no longer operates as an individual ATM link. s members of a group using the ima-group interface command does not enable the interface atm <i>slot/</i> ima <i>group-number</i> command to create the group.
	Specifying ATM links a the group. You must use	s members of a group using the ima-group interface command does not enable
	Specifying ATM links a the group. You must use	s members of a group using the ima-group interface command does not enable the interface atm <i>slot/imagroup-number</i> command to create the group. shows the how to create the IMA group: face ATM0/IMA0
Examples	Specifying ATM links a the group. You must use The following example Router(config)# inter	s members of a group using the ima-group interface command does not enable the interface atm <i>slot/imagroup-number</i> command to create the group. shows the how to create the IMA group: face ATM0/IMA0
Examples	Specifying ATM links a the group. You must use The following example Router(config)# inter Router(config-if)# no	s members of a group using the ima-group interface command does not enable the interface atm <i>slot/imagroup-number</i> command to create the group. shows the how to create the IMA group: face ATM0/IMA0 o ip address
Examples	Specifying ATM links a the group. You must use The following example Router(config)# inter Router(config-if)# no	s members of a group using the ima-group interface command does not enable the interface atm <i>slot/imagroup-number</i> command to create the group. shows the how to create the IMA group: face ATMO/IMA0 o ip address Description Configures the physical links as IMA group members; execute this interface configuration command for each physical link that you
Usage Guidelines Examples Related Commands	Specifying ATM links a the group. You must use The following example Router(config)# inter Router(config-if)# no Command ima-group	s members of a group using the ima-group interface command does not enable the interface atm <i>slot/imagroup-number</i> command to create the group. shows the how to create the IMA group: face ATMO/IMA0 o ip address Description Configures the physical links as IMA group members; execute this interface configuration command for each physical link that you include in an IMA group. Enables the user to configure the IMA Group ID for the IMA

interface port-channel

To create an EtherChannel interface, use the **interface port-channel** command in global configuration mode. To remove this EtherChannel port from the Cisco CMTS, use the **no** form of this command.

interface port-channel number

no interface port-channel number

Syntax Description	number	Identifying port channel number for this interface (EtherChannel port). The range is 1 to 8.
Command Default	By default, EtherCl	hannel groups and ports are not defined, and they are disabled (off mode) configured.
Command Modes	Global configuration	on
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
	The first EtherChannel interface configured becomes the bundle master for all EtherChannel interfaces in the group. That is, the MAC address of the first EtherChannel interface is the MAC address for all EtherChannel interfaces in the group. If the first EtherChannel interface is later removed, the second EtherChannel interface to be configured becomes the bundled master by default. Repeat this configuration on every EtherChannel port to be bundled into a FastEtherChannel (FEC) or GigabitEtherChannel (GEC) group. This configuration must be present on all EtherChannel interfaces	
	•	annel group can be configured.
Examples		nple configures the port to have an EtherChannel port number of 1 within its p. The EtherChannel group is defined with the channel-group command.
	Router(config)# i	interface port-channel 1
Related Commands	Command	Description

channel-group	Assigns an EtherChannel port to an EtherChannel group.
show interface port-channel	Displays the EtherChannel interfaces and channel identifiers, with their mode and operational status.

interface range

To execute commands on multiple subinterfaces at the same time, use the **interface range** command in global configuration mode.

interface range {type number [- interface-number] [,] . . .type number | macro word}

no interface range type number

Syntax Description	type number	Interface type and interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.	
		• You can enter any number of interface type and numbers.	
	- interface-number	(Optional) Ending interface number.	
	,	Allows you to configure more interface types.	
	macro	Specifies a macro keyword.	
	word	Previously defined keyword, up to 32 characters long.	
Command Default	No interface range is s	set.	
Command Modes	Global configuration (Global configuration (config)	
Command History	Release	Modification	
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
Usage Guidelines	Configuration Changes		
	•	nges made to a range of subinterfaces are saved to NVRAM, but the range itself NVRAM. Use the define interface range command to create and save a range.	
	You can enter the rang	ge in two ways:	
	• Specifying up to f	five interface ranges	
	• Specifying a prev	iously defined macro	
	- ·	the interfaces or the name of a range macro. A range must consist of the same interfaces within a range cannot span slots.	
	a macro, the command	th the interface range and macro keywords in the same command. After creatin d does not allow you to enter additional ranges. Likewise, if you have already range, the command does not allow you to enter a macro.	
	VLANs		
		AN, valid values are from 1 to 4094. The last VLAN number cannot exceed 4094	
	•		

	You cannot use the interface range command to create switch virtual interfaces (SVIs) in that particular range. You can use the interface range command only to configure existing VLAN SVIs within the range. To display VLAN SVIs, enter the show running-config command. VLANs not displayed cannot be used in the interface range command.
	The commands entered under the interface range command are applied to all existing VLAN SVIs within the range.
	You can enter the command interface range create vlan $x - y$ to create all VLANs in the specified range that do not already exist. If you are using discontiguous VLANs, you can use the interface range vlan command to configure multiple SVIs without creating unneeded SVIs and wasting interface descriptor blocks (IDBs).
	After specifying a VLAN range, you can continue using the interface range command to specify another interface (ATM, Fast Ethernet, Gigabit Ethernet, loopback, port-channel, or tunnel).
Note	VLANs 4093, 4094, and 4095 are reserved and cannot be configured by the user.
Examples	interface range Gigabit Ethernet Example The following example shows how to set a Gigabit Ethernet range: Router (config) # interface range gigabitethernet 0/1 - 3
Related Commands	Command Description
neialeu commalius	define interface range Defines an interface range macro.

Applies a unique VLAN ID to each subinterface within the range.

encapsulation dot1q

To configure the Type of Service (ToS) level for IP traffic, use the ip tos command in pseudowire class configuration mode. To disable a configured ToS value, use the **no** form of this command.

ip tos value *value_number*

no ip tos value value_number

Syntax Description	value <i>value_number</i>	Specifies the type of service (ToS) level for IP traffic in the pseudowire.
Defaults	The default ToS value i	s 0.
Command Modes	Pseudowire class config	guration
Command History	Release	Modification
	15.1(2)SNI	Support for this command was introduced on the Cisco ASR 901 router.
Examples	Router(config) # pser Router(config-pw)# ij	udowire-class ether-pw p tos value 1
Related Commands	Command	Description
	pseudowire-class	Specifies the name of a Layer 2 pseudowire-class and enters pseudowire-class configuration mode.

I3-over-I2 flush buffers

To enable 13-over-12 flush buffers for layer 3 over layer 2 deployments, use the **13-over-12 flush buffers** command in global configuration mode. To remove this configuration, use the **no** form of this command.

13-over-12 flush buffers

no l3-over-l2 flush buffers

Syntax Description	flush	Configures flushing of layer 3 buffers.
	buffers	Enables flushing of layer 3 buffers for layer 3 over layer 2 support.
Command Default	This command is e	enabled by default.
Command Modes	Global configuration	on (config)#
Command History	Release	Modification
	15.2(2)SNG	This command was introduced on the Cisco ASR 901 Series Aggregation Services Routers.
Usage Guidelines	ARP flushing is do	required only when layer 3 is deployed over layer 2. When this command is enabled, one whenever there is a MAC table flush. e no form of this command before configuring Layer 3 FRR features.
Examples	The following exar on a Cisco ASR 90	nple shows how to enable 13-over-12 flush buffers for layer 3 over layer 2 deployments)1 router:

I2proto-forward

To configure the forwarding of tagged Layer 2 Control Packets and dropping of untagged layer 2 control packets, use the **l2proto-forward** command in interface configuration mode. To delete this configuration, use the **no** form of this command.

l2proto-forward tagged {cdp | dtp | lacp | lldp | stp | udld | vtp}

no l2proto-forward tagged {cdp | dtp | lacp | lldp | stp | udld | vtp}

cdp	
cup	Enables Cisco Discovery Protocol (CDP) tunneling.
dtp	Enables Dynamic Trunking Protocol (DTP) tunneling.
lacp	Enables Link Aggregration Control Protocol (LACP) tunneling.
lldp	Enables Link Layer Discovery Protocol (LLDP) tunneling.
stp	Enables Spanning Tree Protocol tunneling (STP).
udld	Enables UniDirectional Link Detection (UDLD) protocol tunneling.
vtp	Enables Vlan Trunking Protocol (VTP) tunneling.
packets.	or is to peer the untagged layer 2 control packets and drop tagged layer 2 control
Interface configurat	tion (config-if)
Release	Modification
Release 15.2(2)SNG	Modification This command was introduced.
15.2(2)SNG Use this command The following exan	This command was introduced. to forward tagged and drop untagged layer 2 control protocol packets. nple shows how to configure the forwarding of tagged Layer 2 Control Packets and
15.2(2)SNG Use this command The following exan	This command was introduced. to forward tagged and drop untagged layer 2 control protocol packets. nple shows how to configure the forwarding of tagged Layer 2 Control Packets and ed layer 2 control packets using the l2proto-forward command.
	lacp lldp stp udld vtp The default behavior packets.

load-interval

To change the length of time for which data is used to compute load statistics, use the **load-interval** interface configuration command. Use the **no** form of this command to revert to the default setting.

load-interval seconds

no load-interval seconds

Syntax Description	seconds	Length of time for which data is used to compute load statistics. Specify a value that is a multiple of 30, from 30 to 600 (30, 60, 90, 120, and so forth).
Defaults	The default is 300	seconds (5 minutes).
Command Modes	Interface configura	ation
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines	•	omputations to be more reactive to short bursts of traffic, rather than averaged over you can shorten the length of time over which load averages are computed.
	This data is used to	is set to 30 seconds, new data is used for load calculations over a 30-second period. o compute load statistics, including input rate in bits and packets per second, output exters per second, load, and reliability.
	more-recent load d	red every 5 seconds. This data is used for a weighted average calculation in which ata has more weight in the computation than older load data. If the load interval is set average is computed for the last 30 seconds of load data.
	period of time. if y displayed when yo	command allows you to change the default interval of 5 minutes to a shorter or longer you change it to a shorter period of time, the input and output statistics that are bu use the show interface command will be more current, and based on more , rather than reflecting a more average load over a longer period of time.
		ften used for dial backup purposes, to increase or decrease the likelihood of a backup plemented, but it can be used on any interface.
Examples	In the following ex	cample, the default 5-minute average is set to a 30-second average.
		interface GigabitEthernet0/7)# load-interval 30

Related Commands	Command	Description
	show interfaces	Displays ALC information.

mac-flap-ctrl

To identify MAC flaps occurring in the router and to take preventive action, use the **mac-flap-ctrl on per-mac** command. To remove MAC flap control, use the **no** form of the command.

mac-flap-ctrl on per-mac <mac-movement> <time-interval>

no mac-flap-ctrl on per-mac <*mac-movement>* <*time-interval>*

time. time-interval Time interval that can elapse before the MAC movements are tagged as flapping. Command Default The default values for the counters are five and ten; that is five movements in ten seconds. Command Modes Global configuration Command History Release Modification 15.1(2)SN1 Support for this command was introduced on the Cisco ASR 901 router. Usage Guidelines Configure the maximum number of MAC movements that are allowed in a specified time interval, beyond which the MAC movement is termed as flapping. As preventive action, err-disabling is done i one of the ports that has MAC flapping. Once the port is err-disabled, it can be administratively brought up using the shut and no shut commands. Examples The following example sets the maximum number of mac movements to 20 in 10 seconds, before a MAC flap is detected in the router. Router (config) # mac-flap-ctrl on per-mac 20 10 None	Syntax Description	mac-movement	Maximum number of MAC movements that are allowed in the specified
flapping. Command Default The default values for the counters are five and ten; that is five movements in ten seconds. Command Modes Global configuration Command History Release Modification 15.1(2)SNI Support for this command was introduced on the Cisco ASR 901 router. Usage Guidelines Configure the maximum number of MAC movements that are allowed in a specified time interval, beyond which the MAC movement is termed as flapping. As preventive action, err-disabling is done i one of the ports that has MAC flapping. Once the port is err-disabled, it can be administratively brought up using the shut and no shut commands. Examples The following example sets the maximum number of mac movements to 20 in 10 seconds, before a MAC flap is detected in the router. Router (config) # mac-flap-ctrl on per-mac 20 10 10			
Command Modes Global configuration Command History Release Modification 15.1(2)SNI Support for this command was introduced on the Cisco ASR 901 router. Usage Guidelines Configure the maximum number of MAC movements that are allowed in a specified time interval, beyond which the MAC movement is termed as flapping. As preventive action, err-disabling is done is one of the ports that has MAC flapping. Once the port is err-disabled, it can be administratively brought up using the shut and no shut commands. Examples The following example sets the maximum number of mac movements to 20 in 10 seconds, before a MAC flap is detected in the router. Router(config)# mac-flap-ctrl on per-mac 20 10 Related Commands Command		time-interval	
Command History Release Modification 15.1(2)SNI Support for this command was introduced on the Cisco ASR 901 router. Usage Guidelines Configure the maximum number of MAC movements that are allowed in a specified time interval, beyond which the MAC movement is termed as flapping. As preventive action, err-disabling is done is one of the ports that has MAC flapping. Once the port is err-disabled, it can be administratively brought up using the shut and no shut commands. Examples The following example sets the maximum number of mac movements to 20 in 10 seconds, before a MAC flap is detected in the router. Router (config) # mac-flap-ctrl on per-mac 20 10 Related Commands Command	Command Default	The default values f	or the counters are five and ten; that is five movements in ten seconds.
15.1(2)SNI Support for this command was introduced on the Cisco ASR 901 router. Usage Guidelines Configure the maximum number of MAC movements that are allowed in a specified time interval, beyond which the MAC movement is termed as flapping. As preventive action, err-disabling is done is one of the ports that has MAC flapping. Once the port is err-disabled, it can be administratively brought up using the shut and no shut commands. Examples The following example sets the maximum number of mac movements to 20 in 10 seconds, before a MAC flap is detected in the router. Router (config) # mac-flap-ctrl on per-mac 20 10 Related Commands Command	Command Modes	Global configuratio	n
Usage Guidelines Configure the maximum number of MAC movements that are allowed in a specified time interval, beyond which the MAC movement is termed as flapping. As preventive action, err-disabling is done is one of the ports that has MAC flapping. Once the port is err-disabled, it can be administratively brought up using the shut and no shut commands. Examples The following example sets the maximum number of mac movements to 20 in 10 seconds, before a MAC flap is detected in the router. Router (config)# mac-flap-ctrl on per-mac 20 10 Related Commands	Command History	Release	Modification
beyond which the MAC movement is termed as flapping. As preventive action, err-disabling is done is one of the ports that has MAC flapping. Once the port is err-disabled, it can be administratively brought up using the shut and no shut commands. Examples The following example sets the maximum number of mac movements to 20 in 10 seconds, before a MAC flap is detected in the router. Router (config) # mac-flap-ctrl on per-mac 20 10 Related Commands		15.1(2)SNI	Support for this command was introduced on the Cisco ASR 901 router.
Image: The control of the port is err-disabled, it can be administratively brought up using the shut and no shut commands. Examples The following example sets the maximum number of mac movements to 20 in 10 seconds, before a MAG flap is detected in the router. Router (config) # mac-flap-ctrl on per-mac 20 10 Related Commands Command Description	Usage Guidelines	beyond which the M	IAC movement is termed as flapping. As preventive action, err-disabling is done in
flap is detected in the router. Router(config)# mac-flap-ctrl on per-mac 20 10 Related Commands Command Description		Once the port is err-	
Related Commands Command Description	Examples	-	•
		Router(config)# m	ac-flap-ctrl on per-mac 20 10
	Related Commands	Command	Description
i tone		None	None

match ip dscp

To identify a specific IP differentiated service code point (DSCP) value as a match criterion, use the **match ip dscp** class-map configuration command. To remove a specific IP DSCP value from a class map, use the **no** form of this command.

match ip dscp *ip-dscp-value* [*ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value*]

no match ip dscp *ip-dscp-value* [*ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value*]

Syntax Description	ip-dscp-value	Specifies the exact value from 0 to 63 used to identify an IP DSCP value.
Command Modes	Class-map configura	tion
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines	DSCP values of 0, 1	P values can be matched in one match statement. For example, if you wanted the IP, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values must be a successful all of the specified IP DSCP values), enter the match ip dscp 0 1 2 3 4 5 6 7
	<i>ip-dscp-value</i> argum significance. For inst packet marked with	ed by the class map to identify a specific IP DSCP value marking on a packet. The ents are used as markings only. The IP DSCP values have no mathematical tance, the <i>ip-dscp-value</i> of 2 is not greater than 1. The value simply indicates that a an <i>ip-dscp-value</i> of 2 is different from a packet marked with an <i>ip-dscp-value</i> of 1. se marked packets is defined by the user through the setting of QoS policies in nfiguration mode.

Examples

The following example shows how to configure the service policy called priority55 and attach service policy priority55 to an interface. In this example, the class map called ipdscp15 evaluates all packets entering interface Fast Ethernet 0/0 for an IP DSCP value of 15. If the incoming packet has been marked with the IP DSCP value of 15, the packet is treated with a priority level of 55.

```
Router(config)# class-map ip dscp15
Router(config-cmap)# match ip dscp 15
Router(config-cmap)# exit
Router(config)# policy-map priority55
Router(config-pmap)# class ip dscp 15
Router(config-pmap-c)# priority55
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitethernet0/0
Router(config-if)# service-policy input priority55
```

Related Commands	Command	Description
	class-map	Creates a class map to be used for matching packets to a specified class.
	policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
	service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
	set ip dscp	Marks the IP DSCP value for packets within a traffic class.
	show class-map	Displays all class maps and their matching criteria.

match vlan

To match and classify traffic on the basis of the virtual local-area network (VLAN) identification number, use the **match vlan** command in class-map configuration mode. To remove a previously specified VLAN identification number as a match criterion, use the **no** form of this command.

match vlan vlan-id-number

no match vlan vlan-id-number

Syntax Description	vlan-id-number	VLAN identification number, numbers, or range of numbers. Valid VLAN identification numbers must be in the range of 1 to 4095.
Command Default	Traffic is not matche	ed on the basis of the VLAN identification number.
Command Modes	Class-map configura	tion
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines		tification Numbers agle VLAN identification number, multiple VLAN identification numbers separated ple, 2 5 7), or a range of VLAN identification numbers separated by a hyphen (for
	••	ctions apply to the match vlan command:
	• The match vlan encapsulations of	a command is supported for IEEE 802.1q and Inter-Switch Link (ISL) VLAN only.
Examples	on the basis of a ran	ple configuration, the match vlan command is enabled to classify and match traffic ge of VLAN identification numbers. Packets with VLAN identification numbers in) are placed in the class called class1.
	Router> enable Router# configure Router(config)# cl Router(config-cmap Router(config-cmap	ass-map class1)# match vlan 25-50

Related Commands

Commands	Command	Description
	bandwidth	Specify or modifies the bandwidth allocated for a class belonging to a policy
	(policy-map class)	map.
	class-map	Creates a class map to be used for matching packets to a specified class.
	policy-map	Creates or modifies a policy map that can be attached to one or more interfaces.
	service-policy	Attached a policy map to an interface.

mtu

To adjust the maximum packet size or maximum transmission unit (MTU) size, use the **mtu** command in interface configuration mode, connect configuration mode, or xconnect subinterface configuration mode. To restore the MTU value to its original default value, use the **no** form of this command.

mtu bytes

no mtu

Syntax Description	bytes	MTU size, in bytes.

Command Default Table 2-3 lists default MTU values according to media type.

Table 2-3 Default Media MTU Values

Media Type	Default MTU (Bytes)
Ethernet	1500
Serial	1500
Token Ring	4464
ATM	4470
FDDI	4470
HSSI (HSA)	4470

Command Modes

Interface configuration (config-if) Connect configuration (xconnect-conn-config) xconnect subinterface configuration (config-if-xconn)

Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.

Usage Guidelines

Each interface has a default maximum packet size or MTU size. This number generally defaults to the largest size possible for that interface type.

Note

The connect configuration mode is used only for Frame Relay Layer 2 interworking.

Changing the MTU Size

Changing the MTU size is not supported on a loopback interface.

mtu

Protocol-Specific Versions of the mtu Command

Changing the MTU value with the **mtu** interface configuration command can affect values for the protocol-specific versions of the command (the **ip mtu** command, for example). If the value specified with the **ip mtu** interface configuration command is the same as the value specified with the **mtu** interface configuration command, and you change the value for the **mtu** interface configuration command value. However, changing the values for the **ip mtu** configuration commands has no effect on the value for the **mtu** interface configuration command.

Examples

mtu

The following example shows how to specify an MTU of 1000 bytes:

Router# configure terminal Router(config)# vlan 20 Router(config-vlan)# name test20 Router(config-if)# mtu 1000

Related Commands	Command	Description
	ip mtu	Sets the MTU size of IP packets sent on an interface.

name

To specify the name of a iSCSI target in the target profile on the GGSN, use the **name** command in iSCSI interface configuration mode. To remove the IP address configuration, use the **no** form of the command.

name target_name

no name *target_name*

Contra Deservitation		
Syntax Description	target_name	Name of the SCSI target.
Command Default	No default behavior	r or values.
Command Modes	iSCSI interface con	figuration
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines	Use the name com	mand to specify the name of the SCSI target in an iSCSI target interface profile on
	the GGSN.	
Examples		s how to create Ethernet VLAN 20, name it test20, and add it to the VLAN database
Examples		e terminal rlan 20 m) # name test20
	This example shows Router# configure Router(config)# v Router(config-vla Router(config-vla	e terminal Plan 20 n) # name test20 n) # end
	This example shows Router# configure Router(config)# v Router(config-vla	e terminal rlan 20 m) # name test20
	This example shows Router# configure Router(config)# v Router(config-vla Router(config-vla Command	e terminal rlan 20 n) # name test20 n) # end Description Configures the GGSN to use the specified iSCSI profile for
Examples Related Commands	This example shows Router# configure Router(config)# v Router(config-vla Router(config-vla Command gprs iscsi	Plan 20 In) # name test20 In) # end End Description Configures the GGSN to use the specified iSCSI profile for record storage. Specifies the IP address of the target on the SAN.

negotiation

To enable advertisement of speed, duplex mode, and flow control on a Gigabit Ethernet interface, use the **negotiation** command in interface configuration mode. To disable automatic negotiation, use the **no negotiation** auto command.

negotiation {auto}

no negotiation auto

Syntax Description	auto	Enables the autonegotiation protocol to configure the speed, duplex, and automatic flow control of the Gigabit Ethernet interface. This is the default.	
Command Default	Autonegotiation is enable	zd.	
Command Modes	Interface configuration (c	config-if)	
Command History	Release	Modification	
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
Usage Guidelines	The negotiation auto command is used instead of the duplex and speed commands (which are used on Ethernet to automatically configure the duplex and speed settings of the interfaces.		
	The no negotiation auto command is used to disable the autonegotiation. If the speed is set to 1000 Mbps and full-duplex is set for the Gigabit Ethernet interface in small form-factor pluggable (SFP) mode, then the autonegotiation is disabled (forced mode) using the no negotiation auto command.		
Related Commands	Command	Description	

network-clock clear switch

Clears the forced switch and manual switch commands.

network-clock clear switch {*t0* | **external** <*slot/card/port>* | **10m** }

Syntax Description	slot/card/port	Specifies the slot/card/port.
Command Modes	Global configuration.	
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Examples	This example clears the Router (config) # netwo	e switch command. rk-clock clear switch t0

I

network-clock eec

To configure the clocking system hardware with the desired parameters, use the **network-clock eec** command. Use the **no** form of the command to disable the clocking system hardware.

network-clock eec {1 | 2}

no network-clock eec {1 | 2}

Syntax Description	1	For option 1, the default value is EEC-Option 1 (2048).
	2	For option 2, the default value is EEC-Option 2 (1544).
Command Modes	Global configuration	
Command History	Release	Modification
	15.1(2)SNG	This command was introduced.
Usage Guidelines Examples		command configures the clocking system hardware with the desired parameters. configures the clocking system hardware with EEC option 1:
	Router(config)# netwo	ork-clock eec 1
Related Commands	Command	Description
	network-clock	Configures the router to work in a synchronized network mode as described

network-clock external hold-off

To override hold-off timer value for external interface, use the **network-clock external hold-off** command. Use the **no** form of the command to disable the configuration.

network-clock external <*slot/card/port>* **hold-off** {0 | <*50-10000>*}

no network-clock external <*slot/card/port>* **hold-off** {0 | <*50-10000>*}

Syntax Description	slot/port/card	Specifies the slot, card, or port of the interface used for timing.
	hold-off	Specifies the hold-off timer value.
Command Modes	Global configuration	n
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Examples	clock to go into the This example specif	ies the hold-off timer value for the external interface.
	Router(config)# net	twork-clock external 3/1/1 hold-off 300
Related Commands	Command	Description
	network-clock hold-off	Configures general hold-off timer in milliseconds.

network-clock hold-off global

To configure general hold-off timer in milliseconds, use the **network-clock hold-off** command. Use the **no** form of the command to remove the configuration.

network-clock hold-off {0 | <50-10000>} global

no network-clock hold-off {0 | <50-10000>} global

SyntaDescription	global	Configures the hold-off timer globally.
Command Default	The default value is 300	0 milliseconds.
Command Modes	Interface configuration	
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines Examples		ssage for values below 300 ms and above 1800 ms.
Examples	This example configure	twork-clock hold-off 75 global
	Notice (config fi) #Met	twork-crock hold-off /5 global
Related Commands	Command	Description
	network-clock synchronization ssm option	Configures the router to work in a synchronized network mode as described in G.781.

network-clock hold-off

To configure general hold-off timer in milliseconds, use the **network-clock hold-off** command in the interface configuration mode. Use the **no** form of the command to remove the configuration.

network-clock hold-off {0 | <50-10000>}

no network-clock hold-off {0 | <50-10000>}

SyntaDescription	<50-10000>	Sets the hold-off timer. The default value is 300 milliseconds.
Command Default	The default value is 300) milliseconds.
Command Modes	Interface configuration	
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines	Displays a warning mes	ssage for values below 300 ms and above 1800 ms.
Examples	This example configure	s the hold-off timer:
	Router(config-if)# network-clock hold-off 1000	
Related Commands	Command	Description
	network-clock synchronization ssm option	Configures the router to work in a synchronized network mode as described in G.781.

network-clock input-source

To configure a clock source line interface, an external timing input interface, a GPS interface, or a packet-based timing recovered clock as the input clock for the system, use the **network-clock input-source** command. Use the **no** form of the command to disable the configuration.

network-clock input-source <priority> {interface <interface_name> <slot/port> | top
 <slot/port/> | {external <slot/card/port> [t1 {sf | efs | d4} | e1 [crc4| fas| cas [crc4] | 2m |
 10m]}}

no network-clock input-source

Syntax Description	priority	Selection priority for the clock source (1 is the highest priority). When the higher-priority clock source fails, the next-higher-priority clock source is selected. Priority is a number between 1 and 250.			
	interface-name	Specifies the interface name.			
	slot/port	Specifies the slot/port name.			
	external	 Refers to the external slot/card/port. This command also configures the type of signal for an external timing input interface. These signals are: T1 with Standard Frame format or Extended Standard Frame format. E1 with or without CRC4 2 MHz signal Default for Europe or Option I is e1 crc4 if the signal type is not specified. Default for North America or Option II is t1 esf if signal type is not specified. 			
			Command Modes	Global configuration	1
			Command History	Release	Modification
				15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines	The no version of the command reverses the command configuration, implying that the priority has changed to undefined and the state machine is informed.				
Examples	1 0	ures the priority of the interface to 23. etwork-clock input-source 23 interface top 0/12			

Related Commands	Command	Description
	network-clock wait-to-restore	Sets the value for the wait-to-restore timer globally.

network-clock input-source controller

To add the clock recovered from the serial interfaces as one of the nominated sources, for network-clock selection, use the **network-clock input-source controller** command. Use the **no** form of the command to disable the configuration.

network-clock input-source <*priority*> **controller** [*t1* | *e1*] <*slot/port*>

no network-clock input-source controller

Syntax Description	priority	Selection priority for the clock source (1 is the highest priority). When the higher-priority clock source fails, the next-higher-priority clock source is selected. Priority is a number between 1 and 250.
	controller	Specifies T1 or E1 interface.
Command Modes	Global configuration	n
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Examples	This example config	gures a clock as one of the nominated sources:
	Router(config)# ne	etwork-clock input-source 10 controller e1 0/12
Related Commands	Command	Description
	network-clock wait-to-restore	Sets the value for the wait-to-restore timer globally.

network-clock output-source system

To allow transmitting the system clock to external timing output interfaces, use the **network-clock output-source system** command. Use the **no** form of the command to disable the configuration.

network-clock output-source system <priority> {external <slot/card/port> [t1 {sf | efs | d4} | e1 [crc4| fas| cas [crc4] | 2m | 10m] }

no network-clock output-source system

Syntax Description	priority	Selection priority for the clock source (1 is the highest priority). When the higher-priority clock source fails, the next-higher-priority clock source is selected.
	external	Specifies the external interface.
Command Modes	Global configuration	1
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines	This command provi	the system clock to external timing output interfaces. ides station clock output as per G.781. It is recommend that you use the interface ead of global commands. Global command should preferably be used for interfaces interface sub mode.
Examples	Ĩ	e output-source to external interface 3/0/1: work-clock output-source system 55 external 3/0/1 t1 efs
Related Commands	Command	Description
	network-clock	Specifies the QL value for line or external timing input or output.

quality-level

network-clock quality-level

To specify the QL value for line or external timing input or output, use the **network-clock quality-level** command. Use the **no** form of the command to remove the configuration.

network-clock quality-level {*tx* | *rx*} <*value*> {**interface** *cinterface name*> <*slot/port*> | **external** <*slot/card/port*> | **controller** *cilot/card/port*> }

no network-clock quality-level

interface-name	Specifies the interface.	
external	Specifies an external slot/port/card.	
controller	Specifies the controller slot/port/card.	
value	Value is based on options specified in usage guidelines section.	
Interface configurati	ion	
Release	Modification	
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
 output. The value is based on a global interworking Option. If Option 1 is configured, the available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and OL-DNU 		
 QL-DNU. If Option 2 is configured with GEN 2, the available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4 and QL-DUS. 		
• If option 2 is configured with GEN1, the available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4 and QL-DUS		
This command is no	t supported for synchronous ethernet interfaces.	
This example specif	ies the QL value for external timing input:	
	external controller value Interface configuration Release 15.1(2)SNG The network-clock output. The value is • If Option 1 is congle-DNU. • If Option 2 is congle-TNC, QL-S • If option 2 is congle-ST4 and QL	

network-clock revertive

To configure the clock-source as revertive, use the **network-clock revertive** command. Use the **no** form of the command to remove the configuration.

network-clock revertive

no network-clock revertive

- **Command Default** The default value is non-revertive.
- **Command Modes** Global configuration

Command History	Release	Modification
	15.1(2)SNG	This command was introduced.

Usage Guidelines T he **network-clock revertive** command specifies whether or not the clock source is revertive. Clock sources with the same priority are always non-revertive. The default value is non-revertive.

In non-revertive switching, a switch to an alternate reference is maintained even after the original reference recovers from the failure that caused the switch. In revertive switching, the clock switches back to the original reference after that reference recovers from the failure, independent of the condition of the alternate reference.

ExamplesThis example shows how to make the clock-source revertive:
Router(config)#[no] network-clock revertive

Related Commands	Command	Description
	network-clock input-source	Configures a clock source line interface, an external timing input interface, GPS interface, or a packet-based timing recovered clock as the input clock for the system.

network-clock wait-to-restore

Specifies the amount of time in seconds that the Cisco ASR 901 waits before considering a new clock source. Specify the **network-clock wait-to-restore-timeout** command in the interface configuration mode.

network-clock wait-to-restore <0-86400>

no network-clock wait-to-restore <0-86400>

<0-86400>	The wait to restore time is configurable in the range of 0 to 86400 seconds. The default value is 300 seconds.
The default setting is r	network-clock-select wait-to-restore 300.
Interface configuration	n mode.
Release	Modification
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
The wait to restore tim seconds.	ne is configurable in the range of 0 to 86400 seconds. The default value is 300
Ensure that you set the	e wait-to-restore values above 50 seconds to avoid a timing flap.
Router# config t	e shows how to use the network-clock wait-to-restore command: network-clock wait-to-restore 1000 global exit
Command	Description
set network-clocks force-reselect	Forces the router to re-select the network clock.
	The default setting is a Interface configuration Release 15.1(2)SNG The wait to restore tim seconds. Ensure that you set the The following example Router# config t Router# config t Router(config-if)# r Router(config-if)# c Command set network-clocks

network-clock wait-to-restore global

Specifies the amount of time in seconds that the Cisco ASR 901 waits before considering a new clock source.

network-clock wait-to-restore <0-86400> global

no network-clock wait-to-restore <0-86400> **global**

Syntax Description	<0-86400>	The wait to restore time is configurable in the range of 0 to 86400 seconds. The default value is 300 seconds.
	global	Sets the value for the wait-to-restore timer globally.
Defaults	The default setting is r	network-clock-select wait-to-restore 300.
ommand Modes	Global configuration	
Command History	Release	Modification
Jsage Guidelines	15.1(2)SNG The wait to restore tim seconds.	Support for this command was introduced on the Cisco ASR 901 router. The is configurable in the range of 0 to 86400 seconds. The default value is 300
Usage Guidelines	The wait to restore tim	
Jsage Guidelines <u>^</u> Caution	The wait to restore tim seconds.	
 Caution	The wait to restore tim seconds. Ensure that you set the	te is configurable in the range of 0 to 86400 seconds. The default value is 300
Usage Guidelines <u> </u>	The wait to restore tim seconds. Ensure that you set the The following example Router# config t	the is configurable in the range of 0 to 86400 seconds. The default value is 300 wait-to-restore values above 50 seconds to avoid a timing flap.
<u>Caution</u>	The wait to restore time seconds. Ensure that you set the The following example Router# config t Router(config)# netw	the is configurable in the range of 0 to 86400 seconds. The default value is 300 wait-to-restore values above 50 seconds to avoid a timing flap.

network-clock set lockout

To lock out a clock source, use the **network-clock set lockout** command. Use the **network-clock clear lockout** form of the command to remove the lockout.

network-clock set lockout {interface interface_name slot/port | external slot/card/port}

network-clock clear lockout

Syntax Description	interface_name	Specifies the interface name.
	external	specifies the external interface name.
Command Modes	Global configuratior	1
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines	The network-clock is not selected for Sy	set lockout command locks out a clock source. A clock source flagged as lock-out yncE.
	To clear the lock-out on a source, use network-clock clear lockout { interface <i>interface_name</i> external <i>slot/card/port</i> } command.	
Note	Lockout takes prece	dence over force switch and force switch overrides the manual switch.
Examples	This example shows	how to lockout the clock source.
	Router(config)# net	work-clock set lockout interface GigabitEthernet 0/1

network-clock switch force

To forcefully select a synchronization source irrespective of whether the source is available and is within the range, use the **network-clock switch force** command. Use the **network-clock clear switch** command to remove the forced switch command.

network-clock switch force {interface *interface_name slot/port* | **external** *slot/card/port*}

Syntax Description	interface_name	Specifies the interface name.
	slot/card/port	Specifies the external slot/card/port name.
Command Modes	Global configuration.	
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.

Router(config)#network-clock switch force interface GigabitEthernet 0/1 t1

network-clock switch manual

To manually select a synchronization source, provided the source is available and is within the range, use the **network-clock switch manual** command.

network-clock switch manual {interface *interface_name slot/port* | **external** *slot/card/port*}

Syntax Description	interface_name	Specifies the interface name.
	slot/card/port	Specifies the external slot/card/port.
Command Modes	Global configuration	
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Examples	This example manua	lly sets the synchronization source.
	Router(config)# net	work-clock switch manual interface GigabitEthernet 0/1 t1

network-clock synchronization automatic

To enable G.781 based automatic clock selection process, use the **network-clock synchronization automatic** command. Use the **no** form of the command to disable the G.781 based automatic clock selection process.

network-clock synchronization automatic

no network-clock synchronization automatic

Command Modes	Global configuration	
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines	-	Achronization automatic command enables the G.781 based automatic clock 1 is the ITU-T Recommendation that specifies the synchronization layer
Examples	The following example shows how to enable the G.781 based automatic clock selection proce Router(config)# network-clock synchronization automatic	
Related Commands	Command	Description
	network-clock eec	Configures the clocking system hardware with the desired parameters
	network-clock synchronization ssm option	Configures the router to work in a synchronized network mode as described in G.781

network-clock synchronization ssm option

To configure the router to work in a synchronized network mode as described in G.781, use the **network-clock synchronization ssm option** command. Use the **no** form of the command to remove the configuration.

network-clock synchronization ssm option {*1*| 2 {*GEN1* | *GEN2*}}

no network-clock synchronization ssm option

	network-clock eec	Configures the clocking system hardware with the desired parameters
Related Commands	Command	Description
	Router(config)# netw	ork-clock synchronization ssm option 2 GEN1
Examples	This example show how to configure the router to work in a synchronized network mode:	
	-	and while choosing option 2, you need to specify the second generation message ation message (GEN1).
Usage Guidelines	-	urations that are not common between options need to be configured again.
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Command History	Release	Modification
Command Modes	Global configuration	
Command Default	Option 1	
	GEN2	Specifies the second generation message.
	GEN1	Specifies the first generation message.
	2	Refers to synchronization networks designed for the US (T1 framings are compatible with this option).
Syntax Description	1	(Default) Refers to synchronization networks designed for Europe (E1 framings are compatible with this option)

payload-size

Specifies the size of the payload for packets on a structured CEM channel.

payload-size [payload-size]

Syntax Description	payload-size	Specifies the size of the payload for packets on a structured CEM channel. Valid values are 32–512. The default payload size for a T1 is 192 bytes; the default size for an E1 is 256 bytes.
		Note The payload size must be a multiple of the number of timeslots for the CEM channel.
		The default payload size is calculated as follows:
		8 x number of timeslots x 1 ms packetization delay
Defaults	1.	d size for a structured CEM channel depends on the number of timeslots that nel. The default payload size for a T1 is 192 bytes; the default size for an E1 is 256
Command Modes	CEM circuit config	uration
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Examples	The following exan	nple shows how to specify a sample rate:
		<pre># no ip address # cem 0 ccem)# payload-size 256 ccem)# xconnect 10.10.10.10 200 encapsulation mpls ccem-xconn)# exit ccem)# exit # exit</pre>

Related Commands	Command	Description
	dejitter-buffer	Configures the size of the dejitter buffer on a CEM channel.
	idle-pattern	Specifies the data pattern transmitted on the T1/E1 line when missing packets are detected on the PWE3 circuit.

police (percent)

To configure traffic policing on the basis of a percentage of bandwidth available on an interface, use the **police** command in policy-map class configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

- police cir percent percentage [burst-in-msec] [bc conform-burst-in-msec ms]
 [be peak-burst-in-msec ms] [pir percent percentage] [conform-action action [exceed-action
 - action [violate-action action]]]
- **no police cir percent** percentage [burst-in-msec] [bc conform-burst-in-msec ms] [be peak-burst-in-msec ms] [pir percent percentage] [conform-action action [exceed-action action [violate-action action]]]

Syntax Description	cir	Committed information rate. Indicates that the CIR will be used for policing traffic.
	percent	Specifies that a percentage of bandwidth will be used for calculating the CIR.
	percentage	Specifies the bandwidth percentage. Valid range is a number from 1 to 100.
	burst-in-msec	(Optional) Burst in milliseconds. Valid range is a number from 1 to 2000.
	bc	(Optional) Conform burst (bc) size used by the first token bucket for policing traffic.
	conform-burst-in-msec	(Optional) Specifies the bc value in milliseconds. Valid range is a number from 1 to 2000.
	ms	(Optional) Indicates that the burst value is specified in milliseconds.
	be	(Optional) Peak burst (be) size used by the second token bucket for policing traffic.
	peak-burst-in-msec	(Optional) Specifies the be size in milliseconds. Valid range is a number from 1 to 2000.
	pir	(Optional) Peak information rate. Indicates that the PIR will be used for policing traffic.
	percent	(Optional) Specifies that a percentage of bandwidth will be used for calculating the PIR.
	conform-action	(Optional) Action to take on packets whose rate is less than the conform burst. You must specify a value for peak-burst-in-msec before you specify the conform-action .
	exceed-action	(Optional) Action to take on packets whose rate is within the conform and conform plus exceed burst.
	violate-action	(Optional) Action to take on packets whose rate exceeds the conform plus exceed burst. You must specify the exceed-action before you specify the violate-action .

action	(Optional) Action to take on packets. Specify one of the following keywords:
	All Supported Platforms
	• drop —Drops the packet.
	• set-clp-transmit —Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and sends the packet with the ATM CLP bit set to 1.
	• set-dscp-transmit <i>new-dscp</i> —Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting.
	• set-frde-transmit —Sets the Frame Relay discard eligible (DE) bit from 0 to 1 on the Frame Relay frame and sends the packet with the DE bit set to 1.
	• set-prec-transmit <i>new-prec</i> —Sets the IP precedence and sends the packet with the new IP precedence value setting.
	• transmit —Sends the packet with no alteration.
	• policed-dscp-transmit —(Exceed and violate action only). Changes the DSCP value per the policed DSCP map and sends the packet.
	• set-cos-inner-transmit <i>value</i> —Sets the inner class of service field as a policing action for a bridged frame on the Enhanced FlexWAN module, and when using bridging features on SPAs.
	• set-cos-transmit value—Sets the packet cost of service (CoS) value and sends the packet.
	• set-mpls-exposition-transmit —Sets the Multiprotocol Label Switching (MPLS) experimental bits from 0 to 7 and sends the packet with the new MPLS experimental bit value setting.
	• set-mpls-topmost-transmit —Sets the MPLS experimental bits on the topmost label and sends the packet.
nd Default All Supported	topmost label and sends the packet.

The default bc and be values are 4 ms.

Command Modes Policy-map class configuration (config-pmap-c)

Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.

Usage Guidelines

This command calculates the cir and pir on the basis of a percentage of the maximum amount of bandwidth available on the interface. When a policy map is attached to the interface, the equivalent cir and pir values in bits per second (bps) are calculated on the basis of the interface bandwidth and the percent value entered with this command. The **show policy-map interface** command can then be used to verify the bps rate calculated.

The calculated cir and pir bps rates must be in the range of 8000 and 200000000 bps. If the rates are outside this range, the associated policy map cannot be attached to the interface. If the interface bandwidth changes (for example, more is added), the bps values of the cir and the pir are recalculated on the basis of the revised amount of bandwidth. If the cir and pir percentages are changed after the policy map is attached to the interface, the bps values of the cir and pir are recalculated.

Conform Burst and Peak Burst Sizes in Milliseconds

This command also allows you to specify the values for the conform burst size and the peak burst size in milliseconds. If you want bandwidth to be calculated as a percentage, the conform burst size and the peak burst size must be specified in milliseconds (ms).

Hierarchical Policy Maps

Policy maps can be configured in two-level (nested) hierarchies; a top (or "parent") level and a secondary (or "child") level. The **police** (percent) command can be configured for use in either a parent or child policy map.

Bandwidth and Hierarchical Policy Maps

The **police** (percent) command uses the maximum rate of bandwidth available as the reference point for calculating the bandwidth percentage. When the **police** (percent) command is configured in a child policy map, the **police** (percent) command uses the bandwidth amount specified in the next higher-level policy (in this case, the parent policy map). If the parent policy map does not specify the maximum bandwidth rate available, the **police** (percent) command uses the maximum bandwidth rate available, the **police** (percent) command uses the maximum bandwidth rate available on the next higher level (in this case, the physical interface, the highest point in the hierarchy) as the reference point. The **police** (percent) command always looks to the next higher level for the bandwidth reference point. The following sample configuration illustrates this point:

```
Policymap parent_policy
class parent
shape average 512000
service-policy child_policy
Policymap child_policy
class normal_type
police cir percent 30
```

In this sample configuration, there are two hierarchical policies: one called parent_policy and one called child_policy. In the policy map called child_policy, the police command has been configured in the class called normal_type. In this class, the percentage specified by for the **police** (percent) command is 30 percent. The command will use 512 kbps, the peak rate, as the bandwidth reference point for class parent in the parent_policy. The **police** (percent) command will use 512 kbps as the basis for calculating the cir rate (512 kbps * 30 percent).

```
interface serial 4/0
service-policy output parent_policy
Policymap parent_policy
class parent
  bandwidth 512
  service-policy child_policy
```

In the above example, there is one policy map called parent_policy. In this policy map, a peak rate has not been specified. The **bandwidth** command has been used, but this command does not represent the maximum rate of bandwidth available. Therefore, the **police** (percent) command will look to the next higher level (in this case serial interface 4/0) to get the bandwidth reference point. Assuming the bandwidth of serial interface 4/0 is 1.5 Mbps, the **police** (percent) command will use 1.5 Mbps as the basis for calculating the cir rate (1500000 * 30 percent).

How Bandwidth Is Calculated

The **police** (percent) command is often used in conjunction with the **bandwidth** and **priority** commands. The **bandwidth** and **priority** commands can be used to calculate the total amount of bandwidth available on an entity (for example, a physical interface). When the **bandwidth** and **priority** commands calculate the total amount of bandwidth available on an entity, the following guidelines are invoked:

- If the entity is a physical interface, the total bandwidth is the bandwidth on the physical interface.
- If the entity is a shaped ATM permanent virtual circuit (PVC), the total bandwidth is calculated as follows:
 - For a variable bit rate (VBR) virtual circuit (VC), the sustained cell rate (SCR) is used in the calculation.
 - For an available bit rate (ABR) VC, the minimum cell rate (MCR) is used in the calculation.

For more information on bandwidth allocation, refer to the "Congestion Management Overview" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

The following example shows how to configure traffic policing using a CIR and a PIR on the basis of a percentage of bandwidth. In this example, a CIR of 20 percent and a PIR of 40 percent have been specified. Additionally, an optional bc value and be value (300 ms and 400 ms, respectively) have been specified.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# police cir percent 20 bc 300 ms be 400 ms pir percent 40
Router(config-pmap-c-police)# exit
```

After the policy map and class maps are configured, the policy map is attached to an interface as shown in the following example:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet0/1
Router(config-if)# service-policy input policy1
Router(config-if)# exit
```

Related Commands	Command	Description
	bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
	bridge-domain	Enables RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged VLAN to an ATM PVC or Frame Relay DLCI.
	policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

Command	Description		
priority	Gives priority to a traffic class in a policy map.		
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.		
shape (percent)	Specifies average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface.		
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.		
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.		

police (two rates)

To configure traffic policing using two rates, the committed information rate (CIR) and the peak information rate (PIR), use the **police** command in policy-map class configuration mode. To remove two-rate traffic policing from the configuration, use the **no** form of this command.

police cir cir [**bc** conform-burst] [**pir** pir] [**be** peak-burst] [**conform-action** action [**exceed-action** action]]]

no police cir

Syntax Description	cir	Committed information rate (CIR) at which the first token bucket is updated.
	cir	Specifies the CIR value in bits per second. The value is a number from 8000 to 200000000.
	bc	(Optional) Conform burst (bc) size used by the first token bucket for policing.
	conform-burst	(Optional) Specifies the bc value in bytes. The value is a number from 1000 to 51200000.
	pir	(Optional) Peak information rate (PIR) at which the second token bucket is updated.
	pir	(Optional) Specifies the PIR value in bits per second. The value is a number from 8000 to 200000000.
	be	(Optional) Peak burst (be) size used by the second token bucket for policing.
	peak-burst	(Optional) Specifies the peak burst (be) size in bytes. The size varies according to the interface and platform in use.
	conform-action	(Optional) Action to take on packets that conform to the CIR and PIR.
	exceed-action	(Optional) Action to take on packets that conform to the PIR but not the CIR.

	violate-action	(Optional) Action to take on packets exceed the PIR.
	action	(Optional) Action to take on packets. Specify one of the following keywords:
		• drop —Drops the packet.
		• set-clp-transmit —Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and sends the packet with the ATM CLP bit set to 1.
		• set-dscp-transmit <i>new-dscp</i> —Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting.
		• set-dscp-tunnel-transmit <i>value</i> —Sets the DSCP value (0 to 63) in the tunnel header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) or Generic Routing Encapsulation (GRE) tunneled packet for tunnel marking and transmits the packet with the new value.
		• set-frde-transmit —Sets the Frame Relay discard eligible (DE) bit from 0 to 1 on the Frame Relay frame and sends the packet with the DE bit set to 1.
		• set-mpls-exp-transmit—Sets the Multiprotocol Label Switching (MPLS) experimental bits from 0 to 7 and sends the packet with the new MPLS experimental bit value setting.
		• set-prec-transmit <i>new-prec</i> —Sets the IP precedence and sends the packet with the new IP precedence value setting.
		• set-prec-tunnel-transmit <i>value</i> —Sets the precedence value (0 to 7) in the tunnel header of an L2TPv3 or GRE tunneled packet for tunnel marking and transmits the packet with the new value.
		• set-qos-transmit <i>new-qos</i> —Sets the quality of service (QoS) group value and sends the packet with the new QoS group value setting.
		• transmit —Sends the packet with no alteration.
Command Default	Traffic policing usi	ng two rates is disabled.
Command Modes	Policy-map class co	onfiguration (config-pmap-c)
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines	Configuring Priority v	with an Explicit Policing Rate
	regardless of conge	re a priority class with an explicit policing rate, traffic is limited to the policer rate estion conditions. In other words, even if bandwidth is available, the priority traffic rate specified with the explicit policer.

Token Buckets

Two-rate traffic policing uses two token buckets—Tc and Tp—for policing traffic at two independent rates. Note the following points about the two token buckets:

- The Tc token bucket is updated at the CIR value each time a packet arrives at the two-rate policer. The Tc token bucket can contain up to the confirm burst (Bc) value.
- The Tp token bucket is updated at the PIR value each time a packet arrives at the two-rate policer. The Tp token bucket can contain up to the peak burst (Be) value.

Updating Token Buckets

The following scenario illustrates how the token buckets are updated:

A packet of B bytes arrives at time t. The last packet arrived at time t1. The CIR and the PIR token buckets at time t are represented by Tc(t) and Tp(t), respectively. Using these values and in this scenario, the token buckets are updated as follows:

Tc(t) = min(CIR * (t-t1) + Tc(t1), Bc)Tp(t) = min(PIR * (t-t1) + Tp(t1), Be)

Marking Traffic

The two-rate policer marks packets as either conforming, exceeding, or violating a specified rate. The following points (using a packet of B bytes) illustrate how a packet is marked:

- If B > Tp(t), the packet is marked as violating the specified rate.
- If B > Tc(t), the packet is marked as exceeding the specified rate, and the Tp(t) token bucket is updated as Tp(t) = Tp(t) B.

Otherwise, the packet is marked as conforming to the specified rate, and both token buckets—Tc(t) and Tp(t)—are updated as follows:

Tp(t) = Tp(t) - B

Tc(t) = Tc(t) - B

For example, if the CIR is 100 kbps, the PIR is 200 kbps, and a data stream with a rate of 250 kbps arrives at the two-rate policer, the packet would be marked as follows:

- 100 kbps would be marked as conforming to the rate.
- 100 kbps would be marked as exceeding the rate.
- 50 kbps would be marked as violating the rate.

Marking Packets and Assigning Actions Flowchart

The flowchart in Figure 2-1 illustrates how the two-rate policer marks packets and assigns a corresponding action (that is, violate, exceed, or conform) to the packet.

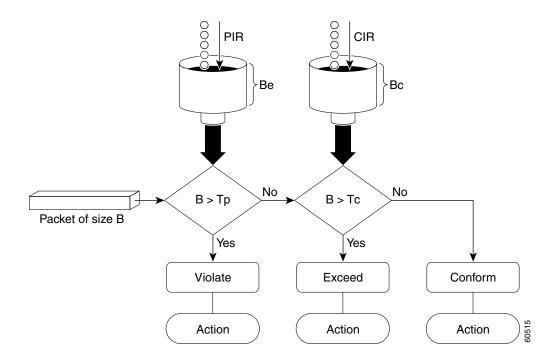


Figure 2-1 Marking Packets and Assigning Actions with the Two-Rate Policer

Examples

Setting Priority with an Explicit Policing Rate

In the following example, priority traffic is limited to a committed rate of 1000 kbps regardless of congestion conditions in the network:

```
Router(config)# policy-map p1
Router(config-pmap)# class c1
Router(config-pmap-c)# police cir 1000000 conform-action transmit exceed-action drop
```

Two-Rate Policing

In the following example, two-rate traffic policing is configured on a class to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps:

```
Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitethernet0/1
Router(config-if)# service-policy output policy1
Router(config-if)# end
Router# show policy-map policy1
Policy Map policy1
Class police
```

```
police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action transmit exceed-action set-prec-transmit 2 violate-action drop
```

Γ

Traffic marked as conforming to the average committed rate (500 kbps) will be sent as is. Traffic marked as exceeding 500 kbps, but not exceeding 1 Mbps, will be marked with IP Precedence 2 and then sent. All traffic marked as exceeding 1 Mbps will be dropped. The burst parameters are set to 10000 bytes.

Command	Description		
police	Configures traffic policing.		
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.		
service-policy	Attaches a policy map to an input interface or an output interface to be used as the service policy for that interface.		
show policy-map	Displays the configuration of all classes for a specified service policy ma or all classes for all existing policy maps.		
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.		

policy-map

To enter policy-map configuration mode and create or modify a policy map that can be attached to one or more interfaces to specify a service policy, use the **policy-map** command in global configuration mode. To delete a policy map, use the **no** form of this command.

policy-map [type {control | service}] policy-map-name

no policy-map [**type** {**control** | **traffic**}] *policy-map-name*

	type	Specifies the policy-map type.
	control	(Optional) Creates a control policy map.
	service	(Optional) Creates a service policy map.
	policy-map-name	Name of the policy map. The name can be a maximum of 40 alphanumeric characters.
Command Default	The policy map is n	ot configured.
Command Modes	Global configuration (config)	
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines		command to specify the name of the policy map to be created, added to, or modified
Usage Guidelines	before you configure policy-map comman	e policies for classes whose match criteria are defined in a class map. The nd enters policy-map configuration mode, in which you can configure or modify the
Usage Guidelines	before you configure policy-map comman class policies for a p You can configure cl Use the class-map a	e policies for classes whose match criteria are defined in a class map. The nd enters policy-map configuration mode, in which you can configure or modify the policy map. ass policies in a policy map only if the classes have match criteria defined for them. and match commands to configure the match criteria for a class. Because you can
Usage Guidelines	before you configure policy-map comman class policies for a p You can configure cl Use the class-map a	e policies for classes whose match criteria are defined in a class map. The nd enters policy-map configuration mode, in which you can configure or modify the policy map. ass policies in a policy map only if the classes have match criteria defined for them.
Usage Guidelines	before you configure policy-map comman class policies for a p You can configure cl Use the class-map a configure a maximu A single policy map attempt to attach a p interface cannot acc	e policies for classes whose match criteria are defined in a class map. The nd enters policy-map configuration mode, in which you can configure or modify the policy map. ass policies in a policy map only if the classes have match criteria defined for them. and match commands to configure the match criteria for a class. Because you can
Usage Guidelines	before you configure policy-map comman class policies for a p You can configure cl Use the class-map a configure a maximu A single policy map attempt to attach a p interface cannot acc map. In this case, if Whenever you modi	e policies for classes whose match criteria are defined in a class map. The nd enters policy-map configuration mode, in which you can configure or modify the policy map. ass policies in a policy map only if the classes have match criteria defined for them. and match commands to configure the match criteria for a class. Because you can m of 64 class maps, a policy map cannot contain more than 64 class policies. can be attached to more than one interface concurrently. Except as noted, when you olicy map to an interface, the attempt is denied if the available bandwidth on the ommodate the total bandwidth requested by class policies that make up the policy
Usage Guidelines	before you configure policy-map comman class policies for a p You can configure cl Use the class-map a configure a maximu A single policy map attempt to attach a p interface cannot acc map. In this case, if Whenever you modi	e policies for classes whose match criteria are defined in a class map. The nd enters policy-map configuration mode, in which you can configure or modify the policy map. ass policies in a policy map only if the classes have match criteria defined for them. and match commands to configure the match criteria for a class. Because you can m of 64 class maps, a policy map cannot contain more than 64 class policies. can be attached to more than one interface concurrently. Except as noted, when you olicy map to an interface, the attempt is denied if the available bandwidth on the ommodate the total bandwidth requested by class policies that make up the policy the policy map is already attached to other interfaces, it is removed from them. fy class policy in an attached policy map, class-based weighted fair queueing

Examples

The following example creates a policy map called "in-gold-policy":

Router(config)# policy-map in-gold-policy
Router(config-pmap)# class in-class1

protocol (ATM)

To configure a static map for an ATM permanent virtual circuit (PVC), switched virtual circuit (SVC), or virtual circuit (VC) class or to enable Inverse Address Resolution Protocol (ARP) or Inverse ARP broadcasts on an ATM PVC, use the **protocol** command in the appropriate mode. To remove a static map or disable Inverse ARP, use the **no** form of this command.

protocol protocol {protocol-address [virtual-template] | inarp } [[no] broadcast | disable-check-subnet | [no] enable-check-subnet]

no protocol *protocol* {*protocol-address* [**virtual-template**] | **inarp**} [[**no**] **broadcast disable-check-subnet** | [**no**] **enable-check-subnet**]

Syntax Description

protocol	Choose one of the following values:
	• arp —IP ARP
	• bridge —bridging
	• cdp—Cisco Discovery Protocol
	• clns—ISO Connectionless Network Service (CLNS)
	• clns_es—ISO CLNS end system
	clns_is—ISO CLNS intermediate system
	• cmns—ISO CMNS
	compressedtcp—Compressed TCP
	• ip —IP
	• llc2 —llc2
	• pad —packet assembler/disassembler (PAD) links
	• ppp —Point-to-Point Protocol carried on the VC
	• pppoe —PPP over Ethernet
	• pppovlan —PPPoE over vlan
	• rsrb —remote source-route bridging
_	snapshot—snapshot routing support
protocol-address	Destination address that is being mapped to a PVC.
virtual-template	(Optional) Specifies parameters that the point-to-point protocol ove ATM (PPPoA) sessions will use.
	Note This keyword is valid only for the PPP protocol.

	inarp	Enables Inverse ARP on an ATM PVC. If you specify a protocol address instead of inarp , Inverse ARP is automatically disabled for that protocol.
	[no] broadcast	(Optional) Indicates that this map entry is used when the corresponding protocol sends broadcast packets to the interface. Pseudobroadcasting is supported. The broadcast keyword of the protocol command takes precedence if you previously configured the broadcast command on the ATM PVC or SVC.
	disable-check-subn	et (Optional) Disables subnet checking for InARP.
	enable-check-subne	et (Optional) Enables subnet checking for InARP.
		ed for IP if the protocol is running on the interface and no static map is configured InARP is disabled by default.
Command Modes	PVC-in-range config	configuration (for an ATM PVC or SVC) guration (for an individual PVC within a PVC range) ation (for an ATM PVC range) on (for a VC class)
Command History	Release	Modification
Command History	Release 15.1(2)SNG	Modification Support for this command was introduced on the Cisco ASR 901 router.
Command History Usage Guidelines	15.1(2)SNG Command Application	Support for this command was introduced on the Cisco ASR 901 router.
	15.1(2)SNG Command Application Use this command to	Support for this command was introduced on the Cisco ASR 901 router.
	 15.1(2)SNG Command Application Use this command to Configure a stati Enable Inverse A 	Support for this command was introduced on the Cisco ASR 901 router. o perform either of the following tasks: ic map for an ATM PVC, SVC, or VC class. ARP or Inverse ARP broadcasts on an ATM PVC or PVC range by configuring
	 15.1(2)SNG Command Application Use this command to Configure a stati Enable Inverse A Inverse ARP dire Enable the router 	Support for this command was introduced on the Cisco ASR 901 router. o perform either of the following tasks: ic map for an ATM PVC, SVC, or VC class. ARP or Inverse ARP broadcasts on an ATM PVC or PVC range by configuring
	 15.1(2)SNG Command Application Use this command to Configure a stati Enable Inverse A Inverse ARP dire Enable the router request is not in Enable the router 	Support for this command was introduced on the Cisco ASR 901 router. o perform either of the following tasks: the map for an ATM PVC, SVC, or VC class. ARP or Inverse ARP broadcasts on an ATM PVC or PVC range by configuring ectly on the PVC, in the PVC range, or in a VC class (applies to IP protocol only) r to respond to an InARP request when the source IP address contained in the the subnet as the receiving sub-interface on which PVC is configured.
	 15.1(2)SNG Command Application Use this command to Configure a stati Enable Inverse A Inverse ARP dire Enable the router request is not in Enable the router as the receiving state 	Support for this command was introduced on the Cisco ASR 901 router. o perform either of the following tasks: ic map for an ATM PVC, SVC, or VC class. ARP or Inverse ARP broadcasts on an ATM PVC or PVC range by configuring ectly on the PVC, in the PVC range, or in a VC class (applies to IP protocol only) r to respond to an InARP request when the source IP address contained in the the subnet as the receiving sub-interface on which PVC is configured. r to accept InARP reply when the peer router's IP address is not in the same subne
	 15.1(2)SNG Command Application Use this command to Configure a stati Enable Inverse A Inverse ARP dire Enable the router request is not in Enable the router as the receiving s Does not provide 	Support for this command was introduced on the Cisco ASR 901 router. o perform either of the following tasks: ac map for an ATM PVC, SVC, or VC class. ARP or Inverse ARP broadcasts on an ATM PVC or PVC range by configuring ectly on the PVC, in the PVC range, or in a VC class (applies to IP protocol only) r to respond to an InARP request when the source IP address contained in the the subnet as the receiving sub-interface on which PVC is configured. r to accept InARP reply when the peer router's IP address is not in the same subne sub-interface on which the PVC is configured.
	 15.1(2)SNG Command Application Use this command to Configure a stati Enable Inverse A Inverse ARP dire Enable the router request is not in Enable the router as the receiving s Does not provide PVC range and PVC- In the following examples of the state of the state	Support for this command was introduced on the Cisco ASR 901 router. o perform either of the following tasks: ic map for an ATM PVC, SVC, or VC class. ARP or Inverse ARP broadcasts on an ATM PVC or PVC range by configuring ectly on the PVC, in the PVC range, or in a VC class (applies to IP protocol only) r to respond to an InARP request when the source IP address contained in the the subnet as the receiving sub-interface on which PVC is configured. r to accept InARP reply when the peer router's IP address is not in the same subne sub-interface on which the PVC is configured. e support for SVC, PVC, and SVC bundles.
Usage Guidelines	 15.1(2)SNG Command Application Use this command to Configure a stati Enable Inverse A Inverse ARP dire Enable the router request is not in Enable the router as the receiving s Does not provide PVC range and PVC- In the following examples of the state of the state	Support for this command was introduced on the Cisco ASR 901 router. o perform either of the following tasks: ic map for an ATM PVC, SVC, or VC class. ARP or Inverse ARP broadcasts on an ATM PVC or PVC range by configuring ectly on the PVC, in the PVC range, or in a VC class (applies to IP protocol only) r to respond to an InARP request when the source IP address contained in the the subnet as the receiving sub-interface on which PVC is configured. r to accept InARP reply when the peer router's IP address is not in the same subne sub-interface on which the PVC is configured. e support for SVC, PVC, and SVC bundles. -in-range configuration modes support only IP. nple, the router creates a static map on a VC, indicates that 10.68.34.237 is c, and sends ATM pseudobroadcasts:
Usage Guidelines	 15.1(2)SNG Command Application Use this command to Configure a stati Enable Inverse A Inverse ARP dire Enable the router request is not in Enable the router as the receiving s Does not provide PVC range and PVC- In the following examples of the second second	Support for this command was introduced on the Cisco ASR 901 router. o perform either of the following tasks: ic map for an ATM PVC, SVC, or VC class. ARP or Inverse ARP broadcasts on an ATM PVC or PVC range by configuring ectly on the PVC, in the PVC range, or in a VC class (applies to IP protocol only) r to respond to an InARP request when the source IP address contained in the the subnet as the receiving sub-interface on which PVC is configured. r to accept InARP reply when the peer router's IP address is not in the same subner sub-interface on which the PVC is configured. e support for SVC, PVC, and SVC bundles. -in-range configuration modes support only IP. nple, the router creates a static map on a VC, indicates that 10.68.34.237 is c, and sends ATM pseudobroadcasts:

In the following example, the VC carries PPP traffic and its associated parameters:

protocol ppp 10.68.34.237 virtual-template

pseudowire-class

To specify the name of a Layer 2 pseudowire-class and enter pseudowire-class configuration mode, use the **pseudowire-class** command in global configuration mode. To remove a pseudowire class configuration, use the **no** form of this command.

pseudowire-class *pw-class-name*

no pseudowire-class pw-class-name

Syntax Description	pw-class-name	The name of a Layer 2 pseudowire-class. If you want to configure more than one pseudowire class, define a class name using the <i>pw-class-name</i> parameter.	
Defaults	No pseudowire-class	s is defined.	
Command Modes	Global configuration	n	
Command History	Release	Modification	
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
Usage Guidelines	The pseudowire-class command configures a pseudowire-class template that consists of configuration settings used by all attachment circuits bound to the class. A pseudowire-class includes the following configuration settings:		
	• Data encapsulat	ion type	
	Control protoco	-l	
		e local Layer 2 interface	
		(ToS) value in IP headers	
	The local interface r same or different.	name for each pseudowire class configured between a pair of PE routers can be the	
		seudowire-class command, the router switches to pseudowire-class configuration tings can be configured.	
Examples	configuration templa Router# config t Router(config)# ps	ple shows how to enter pseudowire-class configuration mode to configure a PW ate named "ether-pw": seudowire-class mpls class)# encapsulation mpls	
	Router(config-pw-c Router(config)# ex	class)# exit	

Related Commands	Command	Description
	pseudowire	Binds an attachment circuit to a Layer 2 PW for an xconnect service.
	xconnect	Binds an attachment circuit to an Layer 2 PW for an xconnect service and then enters xconnect configuration mode.

ptp profile telecom

To enable the PTP telecom profile on the router, use **ptp profile telecom** in the clock configuration mode. To disable PTP telecom profile, use the **no** form of the command.

ptp profile telecom

no ptp profile telecom

- **Syntax Description** This command has no arguments.
- Command Modes Clock configuration
- Command HistoryReleaseModification15.1(2)SNISupport for this command was introduced on the Cisco ASR 901 router.
- **Usage Guidelines** This command enables the PTP telecom profile on the router.
- **Examples** The following example shows how to configure a PTP clock and enter clock configuration mode:

Router# **configure terminal** Router(config)# **ptp clock ordinary domain 0** Router(config-ptp-clk)# **ptp profile telecom**

Related Commands	Command	Description
	ptp clock	Creates a PTP clock instance.

ql-enabled rep segment

Specifies the REP segment used for synchronous Ethernet clock selection.

ql-enabled rep segment segment-id

no ql-enabled rep segment segment-id

Syntax Description	segment	Specifies a REP segment.	
	segment-id	The REP segment ID of the REP segment	
Defaults	There is no default	setting.	
Command Modes	Global configuration	n	
Command History	Release	Modification	
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
Usage Guidelines	This command requ	aires that you specify a synchronous Ethernet clock source.	
Examples	The following example shows how to use the ql-enabled command: Router# config t Router(config)# ql-enabled rep segment 5 Router(config)# exit		
Related Commands	Command	Description	
	rep segment	Enables Resilient Ethernet Protocol (REP) on an interface assigns a segment ID.	

rep block port

Use the **rep block port** interface configuration command on the REP primary edge port to configure Resilient Ethernet Protocol (REP) VLAN load balancing. Use the **no** form of this command to return to the default configuration.

rep block port {id *port-id* | *neighbor_offset* | **preferred**} **vlan** {*vlan-list* | **all**}

no rep block port {**id** *port-id* | *neighbor_offset* | **preferred**}

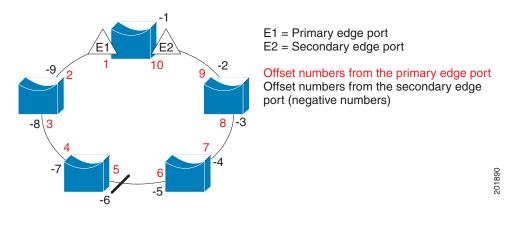
Syntax Description	id port-id	Identify the VLAN blocking alternate port by entering the unique port ID that is automatically generated when REP is enabled. The REP port ID is a 16-character hexadecimal value. You can view the port ID for an interface by entering the show interface <i>interface-id</i> rep detail command.
	neighbor_offset	Identify the VLAN blocking alternate port by entering the offset number of a neighbor. The range is -256 to +256; a value of 0 is invalid. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors.
		NoteBecause you enter this command at the primary edge port (offset number 1), you would never enter an offset value of 1 to identify an alternate port.
	preferred	Identify the VLAN blocking alternate port as the segment port on which you entered the rep segment <i>segment-id</i> preferred interface configuration command.
		Note Entering the preferred keyword does not ensure that the preferred port is the alternate port; it gives it preference over other similar ports.
	vlan	Identify the VLANs to be blocked.
	vlan-list	Enter a VLAN ID from 1 to 4094 or a range or sequence of VLANs (such as 1-3, 22, 41-44) of VLANs to be blocked.
	all	Enter to block all VLANs.
Defaults		or after you enter the rep preempt segment privileged EXEC command (for manual lock all VLANs at the primary edge port. This behavior remains until you configure command.
		port cannot determine which port is to be the alternate port, the default action is no VLAN load balancing.
Command Modes	Interface configur	tion
Command History	Release	Modification
-	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.

Usage Guidelines

You must enter this command on the REP primary edge port.

When you select an alternate port by entering an offset number, this number identifies the downstream neighbor port of an edge port. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors. See Neighbor Offset Numbers in a REP SegmentFigure 2-2.







You would never enter an offset value of 1 because that is the offset number of the primary edge port itself.

If you have configured a preempt delay time by entering the **rep preempt delay** *seconds* interface configuration command and a link failure and recovery occurs, VLAN load balancing begins after the configured preemption time period elapses without another link failure. The alternate port specified in the load-balancing configuration blocks the configured VLANs and unblocks all other segment ports. If the primary edge port cannot determine the alternate port for VLAN balancing, the default action is no preemption.

Each port in a segment has a unique port ID. The port ID format is similar to the one used by the spanning tree algorithm: a port number (unique on the bridge) associated to a MAC address (unique in the network). To determine the port ID of a port, enter the **show interface** *interface-id* **rep detail** privileged EXEC command.

Examples

This example shows how to configure REP VLAN load balancing on the Switch B primary edge port (Gigabit Ethernet port 0/1) and to configure Gigabit Ethernet port 0/2 of Switch A as the alternate port to block VLANs 1 to 100. The alternate port is identified by its port ID, shown in bold in the output of the **show interface rep detail** command for the Switch A port.

```
Switch A# show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB17800EEE
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 1
```

```
Preempt Delay Timer: 35 sec
Load-balancing block port: none
Load-balancing block vlan: none
STCN Propagate to:
PDU/TLV statistics:
LSL PDU rx: 107122, tx: 192493
Router# config t
Router (config)# interface gigabitethernet0/1
Router (config-if)# rep block port id 0080001647FB1780 vlan 1-100
Router (config-if)# exit
```

This example shows how to configure VLAN load balancing by using a neighbor offset number and how to verify the configuration by entering the **show interfaces rep detail** privileged EXEC command:

```
Router# config t
Router (config)# interface gigabitethernet0/2
Router (config-if) # rep block port 6 vlan 1-110
Router (config-if)# end
Router# show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB178009C3
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 3
Preempt Delay Timer: 35 sec
Load-balancing block port: 6
Load-balancing block vlan: 1-110
STCN Propagate to: none
LSL PDU rx: 1466780, tx: 3056637
HFL PDU rx: 2, tx: 0
BPA TLV rx: 1, tx: 2119695
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 757406, tx: 757400
EPA-COMMAND TLV rx: 1, tx: 1
EPA-INFO TLV rx: 178326, tx: 178323
```

Related Commands	Command	Description
	rep preemt delay	Configures a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.
	rep preempt segment	Manually starts REP VLAN load balancing on a segment.
	show interface rep detail	Displays REP detailed configuration and status for all interfaces or the specified interface, including the administrative VLAN.

rep platform vlb segment

To configure the VLAN list which forms VLAN load balancing group use the **rep platform vlb segment** command. For more information on VLAN Load Balancing, see the Cisco ASR 901 Configuration Guide.

rep platform vlb segment segment-id vlan {vlan-list | all}

no rep platform vlb

Syntax Description	segment-id	ID of the REP segment. The range is from 1 to 1024.
	vlan vlan-list	Enter vlan vlan-list to block a single VLAN or a range of VLANs,
	all	Enter vlan all to block all VLANs. This is the default configuration.
Command Modes	Global Configuration	on
Command History	Release	Modification
	15.1(2)SNG	This command was introduced.
Usage Guidelines	in VLB for a particu	VIb segment command should be issued on all Cisco ASR 901 routers participating alar segment and should have a matching VLAN list. This vlan list should also match command issued on primary edge port
-	in VLB for a particu with the rep block	Ilar segment and should have a matching VLAN list. This vlan list should also match command issued on primary edge port.
Usage Guidelines Examples	in VLB for a particu with the rep block The example shows	alar segment and should have a matching VLAN list. This vlan list should also match command issued on primary edge port.
	in VLB for a particu with the rep block The example shows	Ilar segment and should have a matching VLAN list. This vlan list should also match command issued on primary edge port.
	in VLB for a particu with the rep block The example shows	alar segment and should have a matching VLAN list. This vlan list should also match command issued on primary edge port.

rep segment

Use the **rep segment** interface configuration command to enable Resilient Ethernet Protocol (REP) on the interface and to assign a segment ID to it. Use the **no** form of this command to disable REP on the interface.

rep segment segment-id [edge [no-neighbor] [primary]] [preferred]

no rep segment

When I	(Opt keyv port Note ghbor (Opt an e then y (Opt has prim then port red (Opt	 You must configure two edge ports, including one primary edge port for each segment. and to be the port of the port of the port of the port is all properties of edge ports, and you can configure in the same as any edge port. The port inherits all properties of edge ports, and you can configure in the same as any edge port. A segment only one primary edge port. If you configure two ports in a segment as the mary edge port, for example ports on different switches, the REP selects one of in to serve as the segment primary edge port. You can identify the primary edge t for a segment by entering the show rep topology privileged EXEC command. A be port of the port is the preferred alternate port or the preferred port VLAN load balancing. 		
no-nei prima prefer Defaults REP is When I Command Modes Interface	keyv port Note ghbor (Opt an e then 'y (Opt has prim then port red (Opt for '	 word without the primary keyword configures the port as the secondary edge t. Each segment has only two edge ports. You must configure two edge ports, including one primary edge port for each segment. betional) Enter no-neighbor to configure a port with no external REP neighbors as edge port. The port inherits all properties of edge ports, and you can configure m the same as any edge port. betional) On an edge port, specify that the port is the primary edge port. A segment only one primary edge port. If you configure two ports in a segment as the mary edge port, for example ports on different switches, the REP selects one of m to serve as the segment primary edge port. You can identify the primary edge t for a segment by entering the show rep topology privileged EXEC command. betional) Specify that the port is the preferred alternate port or the preferred port VLAN load balancing. Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The 		
prima prefer Defaults REP is When I Command Modes Interface	ghbor (Opt an e then y (Opt has prim then port red (Opt for v	 t. Each segment has only two edge ports. You must configure two edge ports, including one primary edge port for each segment. potional) Enter no-neighbor to configure a port with no external REP neighbors as edge port. The port inherits all properties of edge ports, and you can configure m the same as any edge port. potional) On an edge port, specify that the port is the primary edge port. A segment only one primary edge port. If you configure two ports in a segment as the mary edge port, for example ports on different switches, the REP selects one of m to serve as the segment primary edge port. You can identify the primary edge t for a segment by entering the show rep topology privileged EXEC command. potional) Specify that the port is the preferred alternate port or the preferred port VLAN load balancing. e Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The 		
prima prefer Defaults REP is When I Command Modes Interface	ghbor (Opt an e then y (Opt has prim then port red (Opt	 You must configure two edge ports, including one primary edge port for each segment. Potional) Enter no-neighbor to configure a port with no external REP neighbors as edge port. The port inherits all properties of edge ports, and you can configure m the same as any edge port. Potional) On an edge port, specify that the port is the primary edge port. A segment only one primary edge port. If you configure two ports in a segment as the mary edge port, for example ports on different switches, the REP selects one of m to serve as the segment primary edge port. You can identify the primary edge t for a segment by entering the show rep topology privileged EXEC command. Potional) Specify that the port is the preferred alternate port or the preferred port VLAN load balancing. Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The 		
prima prefer Defaults REP is When I Command Modes Interface	ghbor (Opt an e then y (Opt has prim then port red (Opt for V	 You must configure two edge ports, including one primary edge port for each segment. bitional) Enter no-neighbor to configure a port with no external REP neighbors as edge port. The port inherits all properties of edge ports, and you can configure m the same as any edge port. bitional) On an edge port, specify that the port is the primary edge port. A segment only one primary edge port. If you configure two ports in a segment as the mary edge port, for example ports on different switches, the REP selects one of m to serve as the segment primary edge port. You can identify the primary edge t for a segment by entering the show rep topology privileged EXEC command. bitional) Specify that the port is the preferred alternate port or the preferred port VLAN load balancing. configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The 		
prima prefer Defaults REP is When I Command Modes Interface	an e then y (Opt has prin then port red (Opt for y	 edge port. The port inherits all properties of edge ports, and you can configure m the same as any edge port. botional) On an edge port, specify that the port is the primary edge port. A segment only one primary edge port. If you configure two ports in a segment as the mary edge port, for example ports on different switches, the REP selects one of m to serve as the segment primary edge port. You can identify the primary edge t for a segment by entering the show rep topology privileged EXEC command. botional) Specify that the port is the preferred alternate port or the preferred port VLAN load balancing. e Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The 		
Defaults REP is When I Command Modes Interface	has prim then port red (Opi for V	 only one primary edge port. If you configure two ports in a segment as the mary edge port, for example ports on different switches, the REP selects one of m to serve as the segment primary edge port. You can identify the primary edge t for a segment by entering the show rep topology privileged EXEC command. btional) Specify that the port is the preferred alternate port or the preferred port VLAN load balancing. e Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The 		
Defaults REP is When I Command Modes Interfac	for	VLAN load balancing.configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The		
When I Command Modes Interfac	Note	alternate port; it merely gives it a slight edge among equal contenders. The		
When I Command Modes Interfac				
Command Modes Interfac	REP is disabled on the interface.			
	EP is enabled of	on an interface, the default is for the port to be a regular segment port.		
Command History Releas	e configuration	1		
	9	Modification		
15.1(2	SNG	Support for this command was introduced on the Cisco ASR 901 router.		
Usage Guidelines REP po				
A non-	rts must be Lay	yer 2 trunk ports.		

REP ports should not be configured as one of these port types:

- SPAN destination port
- Private VLAN port
- Tunnel port
- Access port
- REP ports must be network node interfaces (NNIs). REP ports cannot be user-network interfaces (UNIs) or enhanced network interfaces (ENIs).

You must configure two edge ports on each REP segment, a primary edge port and a port to act as a secondary edge port. If you configure two ports in a segment as the primary edge port, for example ports on different switches, the configuration is allowed, but the REP selects one of them to serve as the segment primary edge port.

- REP ports follow these rules:
 - There is no limit to the number of REP ports on a switch; however, only two ports on a switch can belong to the same REP segment.
 - If only one port on a switch is configured in a segment, the port should be an edge port.
 - If two ports on a switch belong to the same segment, they must be both edge ports, both regular segment ports, or one regular port and one edge no-neighbor port. An edge port and regular segment port on a switch cannot belong to the same segment.



Release 12.2(33)MRA does not support the **no-neighbor** keyword.

- If two ports on a switch belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.

If you configure two ports in a segment as the primary edge port, for example ports on different switches, the REP selects one of them to serve as the segment primary edge port. Enter the **show rep topology** privileged EXEC command on a port in the segment to verify which port is the segment primary edge port.

REP interfaces come up in a blocked state and remain in a blocked state until notified that it is safe to unblock. You need to be aware of this to avoid sudden connection losses.

You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

ExamplesThis example shows how to enable REP on a regular (nonedge) segment port:
Router (config)# interface gigabitethernet 0/1
Router (config-if)# rep segment 100This example shows how to enable REP on a port and to identify the port as the REP primary edge port:
Router (config)# interface gigabitethernet 0/2
Router (config-if)# rep segment 100 edge primaryThis example shows how to enable REP on a port and to identify the port as the REP primary edge port:
Router (config-if)# rep segment 100 edge primary

Router (config)# interface gigabitethernet 0/2 Router (config-if)# rep segment 100 edge You can verify your settings by entering the **show interfaces rep** privileged EXEC command. To verify which port in the segment is the primary edge port, enter the **show rep topology** privileged EXEC command.

Related Commands

ds	Command	Description
	show interfaces rep [detail]	Displays REP configuration and status for all interfaces or the specified interface.
	show rep topology [detail]	Displays information about all ports in the segment, including which one was configured and selected as the primary edge port.

router isis

To enable the Intermediate System-to-Intermediate System (IS-IS) routing protocol and to specify an IS-IS process, use the **router isis** command in global configuration mode. To disable IS-IS routing, use the **no** form of this command.

router isis area-tag

no router isis *area-tag*

Syntax Description	area-tag	Meaningful name for a routing process. If it is not specified, a null tag is assumed and the process is referenced with a null tag. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router.		
		Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration.		
Defaults	This command is d	isabled by default.		
Command Modes	Global configuration)n		
Command History	Release	Modification		
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.		
Usage Guidelines	configured to speci	sed to enable routing for an area. An appropriate network entity title (NET) must be fy the area address of the area and system ID of the router. Routing must be enabled erfaces before adjacencies may be established and dynamic routing is possible.		
	If you have IS-IS running and at least one International Standards Organization Interior Gateway Routing Protocol (ISO-IGRP) process, the IS-IS process and the ISO-IGRP process cannot both be configured without an area tag. The null tag can be used by only one process. If you run ISO-IGRP and IS-IS, a null tag can be used for IS-IS, but not for ISO-IGRP at the same time. However, each area in an IS-IS multiarea configuration should have a nonnull area tag to facilitate identification of the area.			
	You can configure only one IS-IS routing process to perform Level 2 (interarea) routing. You can configure this process to perform Level 1 (intra-area) routing at the same time. You can configure up to 29 additional processes as Level 1-only processes. If Level 2 routing is configured on any process, all additional processes are automatically configured as Level 1.			
	An interface cannot be part of more than one area, except in the case where the associated routing process is performing both Level 1 and Level 2 routing. On media such as WAN media where subinterfaces are supported, different subinterfaces could be configured for different areas.			
	If Level 2 routing is not desired for a given area, use the is-type command to remove Level 2. Level 2 routing can then be enabled on some other router instance.			

Explicit redistribution between IS-IS instances is prohibited (prevented by the parser). In other words, you cannot issue a **redistribute isis** *area-tag* command in the context of another IS-IS router instance (**router isis** *area-tag*). Redistribution from any other routing protocol into a particular area is possible, and is configured per router instance, as in Cisco IOS software Release 12.0, using the **redistribute** and **route map** commands. By default, redistribution is into Level 2.

If multiple Level 1 areas are defined, the Target Address Resolution Protocol (TARP) behaves in the following way:

- The locally assigned target identifier gets the network service access point (NSAP) of the Level 2 area, if present.
- If only Level 1 areas are configured, the router uses the NSAP of the first active Level 1 area as shown in the configuration at the time of TARP configuration ("tarp run"). (Level 1 areas are sorted alphanumerically by tag name, with capital letters coming before lowercase letters. For example, AREA-1 precedes AREA-2, which precedes area-1.) Note that the target identifier NSAP could change following a reload if a new Level 1 area is added to the configuration after TARP is running.
- The router continues to process all Type 1 and 2 protocol data units (PDUs) that are for this router. Type 1 PDUs are processed locally if the specified target identifier is in the local target identifier cache. If not, they are "propagated" (routed) to all interfaces in the *same* Level 1 area. (The same area is defined as the area configured on the input interface.)
- Type 2 PDUs are processed locally if the specified target identifier is in the local target identifier cache. If not, they are propagated via all interfaces (all Level 1 or Level 2 areas) with TARP enabled. If the source of the PDU is from a different area, the information is also added to the local target identifier cache. Type 2 PDUs are propagated via all static adjacencies.
- Type 4 PDUs (for changes originated locally) are propagated to all Level 1 and Level 2 areas (because internally they are treated as "Level 1-2").
- Type 3 and 5 PDUs continue to be routed.
- Type 1 PDUs are propagated only via Level 1 static adjacencies if the static NSAP is in one of the Level 1 areas in this router.

After you enter the **router isis** command, you can enter the maximum number of paths. There can be from 1 to 32 paths.

Examples

The following example starts IS-IS routing with the optional *area-tag* argument, where CISCO is the value for the *area-tag* argument:

router isis CISCO

The following example specifies IS-IS as an IP routing protocol for a process named Finance, and specifies that the Finance process will be routed on Ethernet interface 0 and serial interface 0:

```
router isis Finance
net 49.0001.aaaa.aaaa.aoaa.00
interface Ethernet 0
ip router isis Finance
interface serial 0
ip router isis Finance
```

The following example shows usage of the maximum-paths option:

router isis maximum-paths? 20

Related Commands	Command	Description
	clns router isis	Enables IS-IS routing for ISO CLNS on an interface and attaches an area designator to the routing process.
	ip router isis	Configures an IS-IS routing process for IP on an interface and attaches an area designator to the routing process.
	net	Configures an IS-IS NET for the routing process.
	redistribute (IP)	Redistribute routes from one routing domain into another routing domain.
	route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.

service instance

To configure an Ethernet service instance, use the service instance command in Layer 2 VPN configuration mode. To disable this configuration, use the no form of this command.

service instance *id service-type*

no service instance id service-type

Syntax Description	id	Service instance ID. Integer from 1 to 4294967295.
	service-type	Service type for the instance.
Command Default	None	
Command Modes	Layer 2 VPN confi	guration (config-l2vpn)
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Usage Guidelines	-	a Multiprotocol Label Switching (MPLS) pseudowire before configuring an Ethernet Layer 2 VPN configuration mode.
Examples	The following exar router:	nple shows how to configure an Ethernet service instance on a Cisco uBR10012
	Router(config-12	upn) # service instance 4095 ethernet

service-policy (policy-map class)

To use a service policy as a QoS policy within a policy map (called a hierarchical service policy), use the **service-policy** command in policy-map class configuration mode. To disable a particular service policy as a QoS policy within a policy map, use the **no** form of this command.

service-policy policy-map-name

no service-policy policy-map-name

 This command is different from the service-policy [input output] policy-map-name command used i interface configuration mode. The purpose of the service-policy [input output] policy-map-name is a attach service policies to interfaces. The child policy is the previously defined service policy that is being associated with the new service policy through the use of the service-policy command. The new service policy using the preexisting service policy is the parent policy. This command has the following restrictions: The set command is not supported on the child policy. The priority command can be used in either the parent or the child policy, but not both policies simultaneously. The shape command can be used in either the parent or the child policy, but not both polices simultaneously on a subinterface. The fair-queue command cannot be defined in the parent policy. 	Syntax Description	policy-map-name	Specifies the name of the predefined policy map to be used as a QoS policy. The name can be a maximum of 40 alphanumeric characters.	
Command History Release Modification 15.1(2)SNG Support for this command was introduced on the Cisco ASR 901 router. Usage Guidelines This command is used to create hierarchical service policies in policy-map class configuration mode. This command is different from the service-policy [input output] policy-map-name command used i interface configuration mode. The purpose of the service-policy [input output] policy-map-name is to attach service policies to interfaces. The child policy is the previously defined service policy that is being associated with the new service policy through the use of the service-policy command. The new service policy using the preexisting service policy is the parent policy. This command has the following restrictions: • The set command is not supported on the child policy. • The shape command can be used in either the parent or the child policy, but not both policies simultaneously. • The shape command can be used in either the parent or the child policy, but not both polices simultaneously on a subinterface. • The fair-queue command cannot be defined in the parent policy. • If the bandwidth command is used in either the child policy.	Command Default	No service policies ar	e used.	
15.1(2)SNG Support for this command was introduced on the Cisco ASR 901 router. Usage Guidelines This command is used to create hierarchical service policies in policy-map class configuration mode. This command is different from the service-policy [input output] policy-map-name command used interface configuration mode. The purpose of the service-policy [input output] policy-map-name command used interface being associated with the new service policy through the use of the service-policy command. The new service policy using the preexisting service policy is the parent policy. This command has the following restrictions: • The set command is not supported on the child policy. • The shape command can be used in either the parent or the child policy, but not both polices simultaneously. • The shape command can be used in either the parent or the child policy, but not both polices simultaneously on a subinterface. • The fair-queue command cannot be defined in the parent policy. • If the bandwidth command is used in the child policy, the bandwidth command must also be used	Command Modes	Policy-map class conf	iguration (config-pmap-c)	
Usage Guidelines This command is used to create hierarchical service policies in policy-map class configuration mode. This command is different from the service-policy [input output] policy-map-name command used is interface configuration mode. The purpose of the service-policy [input output] policy-map-name is that attach service policies to interfaces. The child policy is the previously defined service policy that is being associated with the new service policy through the use of the service-policy command. The new service policy using the preexisting service policy is the parent policy. This command has the following restrictions: • The set command is not supported on the child policy. • The shape command can be used in either the parent or the child policy, but not both polices simultaneously. • The shape command can be used in either the parent or the child policy, but not both polices using the police simultaneously on a subinterface. • The fair-queue command cannot be defined in the parent policy. • If the bandwidth command is used in either the ploicy, the bandwidth command must also be used	Command History	Release	Modification	
 This command is different from the service-policy [input output] policy-map-name command used i interface configuration mode. The purpose of the service-policy [input output] policy-map-name is to attach service policies to interfaces. The child policy is the previously defined service policy that is being associated with the new service policy through the use of the service-policy command. The new service policy using the preexisting service policy is the parent policy. This command has the following restrictions: The set command is not supported on the child policy. The priority command can be used in either the parent or the child policy, but not both policies simultaneously. The shape command can be used in either the parent or the child policy, but not both polices simultaneously on a subinterface. The fair-queue command cannot be defined in the parent policy. 		15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
 policy through the use of the service-policy command. The new service policy using the preexisting service policy is the parent policy. This command has the following restrictions: The set command is not supported on the child policy. The priority command can be used in either the parent or the child policy, but not <i>both</i> policies simultaneously. The shape command can be used in either the parent or the child policy, but not <i>both</i> polices simultaneously on a subinterface. The fair-queue command cannot be defined in the parent policy. 	Usage Guidelines	This command is used to create hierarchical service policies in policy-map class configuration mode. This command is different from the service-policy [input output] <i>policy-map-name</i> command used in interface configuration mode. The purpose of the service-policy [input output] <i>policy-map-name</i> is to		
 The set command is not supported on the child policy. The priority command can be used in either the parent or the child policy, but not <i>both</i> policies simultaneously. The shape command can be used in either the parent or the child policy, but not <i>both</i> polices simultaneously on a subinterface. The fair-queue command cannot be defined in the parent policy. If the bandwidth command is used in the child policy, the bandwidth command must also be used 				
 The priority command can be used in either the parent or the child policy, but not <i>both</i> policies simultaneously. The shape command can be used in either the parent or the child policy, but not <i>both</i> polices simultaneously on a subinterface. The fair-queue command cannot be defined in the parent policy. If the bandwidth command is used in the child policy, the bandwidth command must also be used 		This command has the following restrictions:		
 simultaneously. The shape command can be used in either the parent or the child policy, but not <i>both</i> polices simultaneously on a subinterface. The fair-queue command cannot be defined in the parent policy. If the bandwidth command is used in the child policy, the bandwidth command must also be use 		• The set command is not supported on the child policy.		
 simultaneously on a subinterface. The fair-queue command cannot be defined in the parent policy. If the bandwidth command is used in the child policy, the bandwidth command must also be use 				
• If the bandwidth command is used in the child policy, the bandwidth command must also be use				
		• The fair-queue command cannot be defined in the parent policy.		
		\mathbf{F}		

Examples

The following example creates a hierarchical service policy in the service policy called parent:

Router(config)# policy-map child Router(config-pmap)# class voice Router(config-pmap-c)# priority 500 Router(config-pmap-c)# exit Router(config-pmap)# exit Router(config)# policy-map parent Router(config-pmap)# class class-default Router(config-pmap-c)# shape average 10000000 Router(config-pmap-c)# service-policy child

Related Commands	Command	Description
	bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
	fair-queue	Specifies the number of queues to be reserved for use by a traffic class.
	policy-map	Specifies the name of the service policy to configure.
	priority	Gives priority to a class of traffic belonging to a policy map.
	service-policy	Specifies the name of the service policy to be attached to the interface.
	shape	Specifies average or peak rate traffic shaping.
	show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
	show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

set cos

To set the Layer 2 class of service (CoS) value of an outgoing packet, use the **set cos** command in policy-map class configuration mode. To remove a specific CoS value setting, use the **no** form of this command.

set cos {cos-value}

no set cos {cos-value}

Syntax Description	cos-value	Specific IEEE 802.1Q CoS value from 0 to 7.	
Command Default	No CoS value is se	et for the outgoing packet.	
Command Modes	d Modes Policy-map class configuration		
Command History	Release	Modification	
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
Usage Guidelines	CoS packet markin	ng is supported only in the Cisco Express Forwarding switching path.	
		and should be used by a router if a user wants to mark a packet that is being sent to a an leverage Layer 2 header information, including a CoS value marking.	
	The set cos command can be used only in service policies that are attached in the output of interface. Packets entering an interface cannot be set with a CoS value.		
	The match cos and set cos commands can be used together to allow routers and switches to interoperate and provide quality of service (QoS) based on the CoS markings.		
	Layer 2 to Layer 3 mapping can be configured by matching on the CoS value because switches already can match and set CoS values. If a packet that needs to be marked to differentiate user-defined QoS services is leaving a router and entering a switch, the router should set the CoS value of the packet because the switch can process the Layer 2 header.		
	Using This Command with the Enhanced Packet Marking Feature		
	You can use this command as part of the Enhanced Packet Marking feature-to specify the "from-field" packet-marking category to be used for mapping and setting the CoS value. The "from-field" packet-marking categories are as follows:		
	• Precedence		
	• Differentiated services code point (DSCP)		
	<i>table-map-name</i> ar category as the Co	rom-field" category but do not specify the table keyword and the applicable gument, the default action will be to copy the value associated with the "from-field" S value. For instance, if you configure the set cos precedence command, the will be copied and used as the CoS value.	

You can do the same for the DSCP marking category. That is, you can configure the **set cos dscp** command, and the DSCP value will be copied and used as the CoS value.

<u>Note</u>

If you configure the **set cos dscp** command, only the *first three bits* (the class selector bits) of the DSCP field are used.

Examples

In the following example, the policy map called "cos-set" is created to assign different CoS values for different types of traffic. This example assumes that the class maps called "voice" and "video-data" have already been created.

```
Router(config)# policy-map cos-set
Router(config-pmap)# class voice
Router(config-pmap-c)# set cos 1
Router(config-pmap-c)# exit
Router(config-pmap)# class video-data
Router(config-pmap-c)# set cos 2
Router(config-pmap-c)# end
```

Enhanced Packet Marking Example

In the following example, the policy map called "policy-cos" is created to use the values defined in a table map called "table-map1". The table map called "table-map1" was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page.

In this example, the setting of the CoS value is based on the precedence value defined in "table-map1":

```
Router(config)# policy-map policy-cos
Router(config-pmap)# class class-default
Router(config-pmap-c)# set cos precedence table table-map1
Router(config-pmap-c)# end
```

Related Commands	Command	Description
	match cos	Matches a packet on the basis of Layer 2 CoS marking.
	policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
	service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
	set dscp	Marks a packet by setting the Layer 3 DSCP value in the ToS byte.
	set precedence	Sets the precedence value in the packet header.
	show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
	show policy-map class	Displays the configuration for the specified class of the specified policy map.
	show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

set dscp

To mark a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte, use the **set dscp** command in policy-map class configuration mode. To remove a previously set DSCP value, use the **no** form of this command.

set [ip] dscp {dscp-value}

no set [ip] dscp {dscp-value}

Syntax Description	ip	(Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets.
	dscp-value	A number from 0 to 63 that sets the DSCP value. The following reserved keywords can be specified instead of numeric values:
		• EF (expedited forwarding)
		• AF11 (assured forwarding class AF11)
		• AF12 (assured forwarding class AF12)
Command Default	Disabled	
Command Modes	Policy-map class c	onfiguration
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.

Usage Guidelines Once the DSCP bit is set, other quality of service (QoS) features can then operate on the bit settings.

DSCP and Precedence Values Are Mutually Exclusive

The **set dscp** command cannot be used with the **set precedence** command to mark the *same* packet. The two values, DSCP and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

Precedence Value and Queueing

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the precedence. Weighted fair queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Use of the "from-field" Packet-marking Category

If you are using this command as part of the Enhanced Packet Marking feature, you can use this command to specify the "from-field" packet-marking category to be used for mapping and setting the DSCP value. The "from-field" packet-marking categories are as follows:

- Class of service (CoS)
- QoS group

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the "from-field" category as the DSCP value. For instance, if you configure the **set dscp cos** command, the CoS value will be copied and used as the DSCP value.



The CoS field is a three-bit field, and the DSCP field is a six-bit field. If you configure the **set dscp cos** command, only the three bits of the CoS field will be used.

If you configure the **set dscp qos-group** command, the QoS group value will be copied and used as the DSCP value.

The valid value range for the DSCP is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **set dscp qos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value will be copied and the packets will be marked.
- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value will not be copied and the packet will not be marked. No action is taken.

Set DSCP Values in IPv6 Environments

When this command is used in IPv6 environments, the default match occurs on both IP and IPv6 packets. However, the actual packets set by this function are only those which meet the match criteria of the class-map containing this function.

Set DSCP Values for IPv6 Packets Only

To set DSCP values for IPv6 values only, the **match protocol ipv6** command must also be used. Without that command, the precedence match defaults to match both IPv4 and IPv6 packets.

Set DSCP Values for IPv4 Packets Only

To set DSCP values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword, the match occurs on both IPv4 and IPv6 packets.

Examples

Packet-marking Values and Table Map

In the following example, the policy map called "policy1" is created to use the packet-marking values defined in a table map called "table-map1". The table map was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the table-map (value mapping) command page.

In this example, the DSCP value will be set according to the CoS value defined in the table map called "table-map1".

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set dscp cos table table-map1
Router(config-pmap-c)# end
```

The **set dscp** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface. For information on attaching a service policy to an interface, refer to the "Modular Quality of Service Command-Line Interface" section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Related Commands	Command	Description
	match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
	policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
	service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
	set cos	Sets the Layer 2 CoS value of an outgoing packet.
	set precedence	Sets the precedence value in the packet header.
	show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
	show policy-map class	Displays the configuration for the specified class of the specified policy map.
	show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.
	show table-map	Displays the configuration of a specified table map or all table maps.
	table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

set ip dscp

The **set ip dscp** command is replaced by the set dscp command. See the set dscp command for more information.

set ip precedence (policy-map)

The **set ip precedence** (policy-map) command is replaced by the **set precedence** command. See the set precedence command for more information.

set ip precedence (route-map)

To set the precedence value (and an optional IP number or IP name) in the IP header, use the **set ip precedence** command in route-map configuration mode. To leave the precedence value unchanged, use the **no** form of this command.

set ip precedence [number | name]

no set ip precedence

Syntax Description	number name	(Optional) A number or name that sets the precedence bits in the IP header. The values for the <i>number</i> argument and the corresponding <i>name</i> argument are listed in Table 2-4 from least to most important.
Command Default	Disabled	
Command Modes	Route-map configurat	ion
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.

Usage Guidelines Table 2-4 lists the values for the *number* argument and the corresponding *name* argument for precedence values in the IP header. They are listed from least to most important.

Table 2-4	Number and Name Values for IP Precedence
-----------	--

Number	Name
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

You can set the precedence using either a number or the corresponding name. Once the IP Precedence bits are set, other QoS services such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) then operate on the bit settings.

The network gives priority (or some type of expedited handling) to marked traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set IP Precedence at the edge of the network (or administrative domain); data then is queued based on the precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during times of congestion.

The mapping from arguments such as **routine** and **priority** to a precedence value is useful only in some instances. That is, the use of the precedence bit is evolving. You can define the meaning of a precedence value by enabling other features that use the value. In the case of the high-end Internet QoS available from Cisco, IP Precedences can be used to establish classes of service that do not necessarily correspond numerically to better or worse handling in the network.

Use the **route-map** (IP) global configuration command with the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another, or for policy routing. Each **route-map** command has an associated list of **match** and **set** commands. The **match** commands specify the match criteria—the conditions under which redistribution or policy routing is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution or policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution set actions to be performed when all of the match criteria of a route map are met.

Examples

The following example sets the IP Precedence to 5 (critical) for packets that pass the route map match:

interface gigabitethernet0/1
 ip policy route-map texas

route-map texas match length 68 128 set ip precedence 5

Related Commands	Command	Description
	random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.

L

set ip precedence tunnel

To set the precedence value in the header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) or Generic Routing Encapsulation (GRE) tunneled packet for tunnel marking, use the **set ip precedence tunnel** command in policy-map class configuration mode. To disable this functionality, use the **no** form of this command.

set ip precedence tunnel precedence-value

no set ip precedence tunnel precedence-value

Syntax Description	precedence-value	Number from 0 to 7 that identifies the precedence value of the tunnel header.			
Command Default	The precedence value	is not set.			
Command Modes	Policy-map class conf	iguration (config-pmap-c)			
Command History	Release	Modification			
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.			
Usage Guidelines	It is possible to configure L2TPv3 (or GRE) tunnel marking and the ip tos command at the same time. However, Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) (L2TPv3 or GRE) tunnel marking has higher priority over ip tos commands, meaning that tunnel marking always rewrites the IP header of the tunnel packet and overwrites the values set by ip tos commands. The order of enforcement is as follows when these commands are used simultaneously:				
	1. set ip dscp tunnel or set ip precedence tunnel (L2TPv3 or GRE tunnel marking)				
	2. ip tos reflect				
	3. ip tos tos-value				
•	This is the designed behavior. We recommend that you configure only L2TPv3 (or GRE) tunnel marking and reconfigure any peers configured with the ip tos command to use L2TPv3 (or GRE) tunnel marking.				
Note	For Cisco IOS Release 12.4(15)T2, marking GRE-tunneled packets is supported only on platforms equipped with a Cisco RPM-XF.				
Examples	The following example shows the set ip precedence tunnel command used in a tunnel marking configuration. In this example, a class map called "MATCH_FRDE" has been configured to match traffic on the basis of the Frame Relay discard eligible (DE) bit setting. Also, a policy map called "policy1" has been created within which the set ip precedence tunnel command has been configured.				
	Router> enable Router# configure t (erminal			

Cisco ASR 901 Aggregation Services Router Command Reference Guide

```
Router(config)# class-map MATCH_FRDE
Router(config-cmap)# match fr-de
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class tunnel
Router(config-pmap-c)# set ip precedence tunnel 7
Router(config-pmap-c)# end
```

Related	Commands
---------	----------

	Command	Description			
-	ip tos	Specifies the ToS level for IP traffic in the TN3270 server.			
	set ip dscp tunnel	Sets the DSCP value in the header of an L2TPv3 tunneled packet.			

I

set ip tos (route-map)

To set the type of service (ToS) bits in the header of an IP packet, use the **set ip tos** command in route-map configuration mode. To leave the ToS bits unchanged, use the **no** form of this command.

set ip tos [tos-bit-value | max-reliability | max-throughput | min-delay | min-monetary-cost |
normal]

no set ip tos

Syntax Description	tos-bi	it-value			(Optional) A value (number) from 0 to 15 that sets the ToS bits in the IP header. See Table 2-5 for more information.			
	max-	reliabilit	y	(Optio	(Optional) Sets the maximum reliability ToS bits to 2.			
	max-	throughp	out	(Optio	onal) Sets the maximum throughput ToS bits to 4.			
	min-o	delay		(Optio	onal) Sets the minimum delay ToS bits to 8.			
	min-ı	monetary	-cost	(Optio	onal) Sets the minimum monetary cost ToS bits to 1.			
	norm	al		(Optio	onal) Sets the normal ToS bits to 0.			
Command Default	Disab	led						
Command Modes	Route	-map con	figurati	on				
Command History	Relea	se		Modifi	ication			
	15.1(2)SNG			Suppor	rt for this command was introduced on the Cisco ASR 901 router.			
Usage Guidelines		binary fo	orm.	you to set n d Descrip	four bits in the ToS byte header. Table 2-5 shows the format of the four			
	Т3	T2	T1	TO	Description			
	0	0	0	0	0 normal forwarding			
	0	0	0	1	1 minimum monetary cost			
					•			
	0	0	1	0	2 maximum reliability			
	$\frac{0}{0}$	0	1	0	2 maximum reliability 4 maximum throughput			

The T3 bit sets the delay. Setting T3 to 0 equals normal delay, and setting it to 1 equals low delay.

8 minimum delay

0

0

1

The T2 bit sets the throughput. Setting this bit to 0 equals normal throughput, and setting it to 1 equals maximum throughput. Similarly, the T1 and T0 bits set reliability and cost, respectively. Therefore, as an example, if you want to set a packet with the following requirements:

- minimum delay T3 = 1
- normal throughput T2 = 0
- normal reliability T1 = 0
- minimum monetary cost T0 = 1

You would set the ToS to 9, which is 1001 in binary format.

Use the **route-map** (IP) global configuration command with the **match** and **set** (route-map) configuration commands to define the conditions for redistributing routes from one routing protocol into another, or for policy routing. Each **route-map** command has an associated list of **match** and **set** commands. The **match** commands specify the match criteria—the conditions under which redistribution or policy routing is allowed for the current route-map command. The **set** commands specify the set actions—the particular redistribution or policy routing actions to perform if the criteria enforced by the match commands are met. The **no route-map** command deletes the route map.

The **set** (route-map) commands specify the redistribution set actions to be performed when all of the match criteria of a route map are met.

Examples	The following example sets the IP ToS bits to 8 (minimum delay as shown in Table 2-5) for packets that pass the route-map match:
	Router(config)# interface gigabitethernet0/1 Router(config-if)# ip policy route-map texas !
	Router(config-if)# route-map texas Router(config-route-map)# match length 68 128 Router(config-route-map)# set ip tos 8 !
Polated Common	de Command Description

Related Commands	Command	Description
	ip policy route-map	Identifies a route map to use for policy routing on an interface.
	route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

set network-clocks

This command causes the router to reselect a network clock; the router selects a new clock based on clock priority.

set network-clocks [force-reselect | next-select]

force-reselect	Forces the router to select a new network clock.	
next-select	Forces the router to select the next available network clock.	
Privileged EXEC		
Release	Modification	
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
The following example shows how to use the set network-clocks force-reselect command: Router# set network-clocks force-reselect		
Command	Description	
	next-select Privileged EXEC Release 15.1(2)SNG The following example Router# set network-o	

set precedence

To set the precedence value in the packet header, use the **set precedence** command in policy-map class configuration mode. To remove the precedence value, use the **no** form of this command.

set precedence {precedence-value}

no set precedence {*precedence-value*}

Syntax Description	precedence-value	A number from 0 to 7 that sets the precedence bit in the packet header.			
Command Default	Disabled				
Command Modes	Policy-map class configuration				
Command History	Release	Modification			
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.			
	contained an old configuration, the set ip precedence command is still recognized. However, the set precedence command will be used in place of the set ip precedence command. The set precedence command cannot be used with the set dscp command to mark the <i>same</i> packet. The two values, DSCP and precedence, are mutually exclusive. A packet can be one value or the other, but not both.				
	Bit Settings Once the precedence bits are set, other quality of service (QoS) features such as weighted fair queueing				
	(WFQ) and Weighted Random Early Detection (WRED) then operate on the bit settings.				
	Precedence Value				
	The network gives priority (or some type of expedited handling) to marked traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the specified precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during times of congestion.				
	The set precedence command cannot be used with the set dscp command to mark the <i>same</i> packet. The two values, differentiated services code point (DSCP) and precedence, are mutually exclusive. A packet				

two values, differentiated services code point (DSCP) and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

Using This Command with the Enhanced Packet Marking Feature

If you are using this command as part of the Enhanced Packet Marking feature, you can use this command to specify the "from-field" packet-marking category to be used for mapping and setting the precedence value. The "from-field" packet-marking categories are as follows:

- CoS
- QoS group

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the "from-field" category as the precedence value. For instance, if you configure the **set precedence cos** command, the CoS value will be copied and used as the precedence value.

You can do the same for the QoS group-marking category. That is, you can configure the **set precedence qos-group** command, and the QoS group value will be copied and used as the precedence value.

The valid value range for the precedence value is a number from 0 to 7. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **set precedence qos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 6), the packet-marking value will be copied and the packets will be marked.
- If QoS group value exceeds the precedence range (for example, 10), the packet-marking value will not be copied, and the packet will not be marked. No action is taken.

Setting Precedence Values for IPv4 Packets Only

To set the precedence values for IPv4 packets only, use a command involving the **ip** keyword like the **match ip precedence** or **match ip dscp** command or include the **match protocol ip** command along with the others in the class map. Without the additional **ip** keyword, the class-map may match both IPv6 and IPv4 packets (depending on the other match criteria) and the **set precedence** or **set dscp** command may act upon both types of packets.

```
Examples
```

The following example shows how to use the set precedence command.

```
Router(config)# policy-map policy-cos
Router(config-pmap)# class class-default
Router(config-pmap-c)# set precedence 4
Router(config-pmap-c)# end
```

The **set precedence** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface or to an ATM virtual circuit. For information on attaching a service policy to an interface, refer to the "Modular Quality of Service Command-Line Interface Overview" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Related Commands	Command	ommand Description				
	match dscp	Identifies a specific IP DSCP value as a match criterion.				
	match precedence	Identifies IP precedence values as match criteria.				
	match protocol	Configures the match criteria for a class map on the basis of the specified protocol.				
	policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.				

Command	Description
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set cos	Sets the Layer 2 CoS value of an outgoing packet.
set dscp	Marks a packet by setting the Layer 3 DSCP value in the ToS byte.
set qos-group	Sets a group ID that can be used later to classify packets.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration for all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.
show table-map	Displays the configuration of a specified table map or all table maps.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

shape (percent)

To specify average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface, use the **shape** command in policy-map class configuration mode. To remove traffic shaping, use the **no** form of this command.

shape {average} percent percentage [sustained-burst-in-msec ms] [be excess-burst-in-msec ms]
[bc committed-burst-in-msec ms]

no shape {average} percent percentage [sustained-burst-in-msec ms] [be excess-burst-in-msec ms] [bc committed-burst-in-msec ms]

percentSpecifies that a percent of bandwidth will be used for either th rate traffic shaping or peak rate traffic shaping.percentageSpecifies the bandwidth percentage. Valid range is a number fr to 100.sustained-burst-in-msec(Optional) Sustained burst size used by the first token bucket for traffic. Valid range is a number from 4 to 200.ms(Optional) Indicates that the burst value is specified in millised be policing traffic.excess-burst-in-msec(Optional) Specifies the be size in milliseconds. Valid range is from 0 to 200.bc(Optional) Specifies the be size used by the first token bucket for policing traffic.excess-burst-in-msec(Optional) Specifies the be size in milliseconds. Valid range is from 0 to 200.bc(Optional) Specifies the be value in milliseconds. Valid range i from 1 to 2000.Command DefaultThe default bc and be is 4 ms.Command ModesPolicy-map class configuration (config-pmap-c)					
percentage Specifies the bandwidth percentage. Valid range is a number from 100. sustained-burst-in-msec (Optional) Sustained burst size used by the first token bucket for traffic. Valid range is a number from 4 to 200. ms (Optional) Indicates that the burst value is specified in millised be be (Optional) Excess burst (be) size used by the second token bucket form 0 to 200. bc (Optional) Specifies the be size in milliseconds. Valid range is from 0 to 200. bc (Optional) Committed burst (bc) size used by the first token burst policing traffic. committed-burst-in-msec (Optional) Specifies the be value in milliseconds. Valid range is from 0 to 200. bc (Optional) Specifies the bc value in milliseconds. Valid range i from 1 to 2000. Command Default The default bc and be is 4 ms.	e average				
to 100. sustained-burst-in-msec (Optional) Sustained burst size used by the first token bucket for traffic. Valid range is a number from 4 to 200. ms (Optional) Indicates that the burst value is specified in millised be be (Optional) Excess burst (be) size used by the second token bucket for policing traffic. excess-burst-in-msec (Optional) Specifies the be size in milliseconds. Valid range is from 0 to 200. bc (Optional) Committed burst (bc) size used by the first token burpolicing traffic. committed-burst-in-msec (Optional) Specifies the bc value in milliseconds. Valid range is from 1 to 2000. Command Default The default bc and be is 4 ms.					
traffic. Valid range is a number from 4 to 200. ms (Optional) Indicates that the burst value is specified in millised be (Optional) Excess burst (be) size used by the second token bud policing traffic. excess-burst-in-msec (Optional) Specifies the be size in milliseconds. Valid range is from 0 to 200. bc (Optional) Committed burst (bc) size used by the first token bur policing traffic. committed-burst-in-msec (Optional) Specifies the bc value in milliseconds. Valid range i from 1 to 2000. Command Default The default bc and be is 4 ms.	om 1				
be (Optional) Excess burst (be) size used by the second token bud policing traffic. excess-burst-in-msec (Optional) Specifies the be size in milliseconds. Valid range is from 0 to 200. bc (Optional) Committed burst (bc) size used by the first token bu policing traffic. committed-burst-in-msec (Optional) Specifies the bc value in milliseconds. Valid range i from 1 to 2000. Command Default The default bc and be is 4 ms.	r policing				
policing traffic. excess-burst-in-msec (Optional) Specifies the be size in milliseconds. Valid range is from 0 to 200. bc (Optional) Committed burst (bc) size used by the first token bu policing traffic. committed-burst-in-msec (Optional) Specifies the bc value in milliseconds. Valid range i from 1 to 2000. Command Default The default bc and be is 4 ms.	(Optional) Indicates that the burst value is specified in milliseconds (ms).				
from 0 to 200. bc (Optional) Committed burst (bc) size used by the first token by policing traffic. committed-burst-in-msec (Optional) Specifies the bc value in milliseconds. Valid range i from 1 to 2000. Command Default The default bc and be is 4 ms.	ket for				
policing traffic. committed-burst-in-msec (Optional) Specifies the bc value in milliseconds. Valid range i from 1 to 2000. Command Default The default bc and be is 4 ms.	a number				
from 1 to 2000. Command Default The default bc and be is 4 ms.	cket for				
	a number				
Command Modes Policy-map class configuration (config-pmap-c)					
Command History Release Modification					
15.1(2)SNGSupport for this command was introduced on the Cisco ASR 901	router.				
Usage Guidelines Committed Information Rate					
This command calculates the committed information rate (CIR) on the basis of a percentag available bandwidth on the interface. Once a policy map is attached to the interface, the equ value in bits per second (bps) is calculated on the basis of the interface bandwidth and the p entered with this command. The show policy-map interface command can then be used to CIR bps value calculated.	ivalent CIR ercent value				

The calculated CIR bps rate must be in the range of 8000 and 154,400,000 bps. If the rate is less than 8000 bps, the associated policy map cannot be attached to the interface. If the interface bandwidth changes (for example, more is added), the CIR bps values are recalculated on the basis of the revised amount of bandwidth. If the CIR percentage is changed after the policy map is attached to the interface, the bps value of the CIR is recalculated.

Conform Burst and Peak Burst Sizes in Milliseconds

This command also allows you to specify the values for the conform burst size and the peak burst size in milliseconds. If you want bandwidth to be calculated as a percentage, the conform burst size and the peak burst size must be specified in milliseconds (ms).

The traffic shape converge rate depends on the traffic pattern and the time slice (Tc) parameter, which is directly affected by the bc that you configured. The Tc and the average rate configured are used to calculate bits per interval sustained. Therefore, to ensure that the shape rate is enforced, use a bc that results in a Tc greater than 10 ms.

How Bandwidth Is Calculated

The **shape** (percent) command is often used in conjunction with the **bandwidth** and **priority** commands. The **bandwidth** and **priority** commands can be used to calculate the total amount of bandwidth available on an entity (for example, a physical interface). When the **bandwidth** and **priority** commands calculate the total amount of bandwidth available on an entity, the following guidelines are invoked:

- If the entity is a physical interface, the total bandwidth is the bandwidth on the physical interface.
- If the entity is a shaped ATM permanent virtual circuit (PVC), the total bandwidth is calculated as follows:
 - For a variable bit rate (VBR) virtual circuit (VC), the sustained cell rate (SCR) is used in the calculation.
 - For an available bit rate (ABR) VC, the minimum cell rate (MCR) is used in the calculation.

For more information on bandwidth allocation, see the "Congestion Management Overview" chapter in the Cisco IOS Quality of Service Solutions Configuration Guide.

Examples

The following example configures traffic shaping using an average shaping rate on the basis of a percentage of bandwidth. In this example, 25 percent of the bandwidth has been specified. Additionally, an optional be value and bc value (100 ms and 400 ms, respectively) have been specified.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class-map class1
Router(config-pmap-c)# shape average percent 25 20 ms be 100 ms bc 400 ms
Router(config-pmap-c)# end
```

After the policy map and class maps are configured, the policy map is attached to interface as shown in the following example.

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet0/1
Router(config-if)# service-policy input policy1
Router(config-if)# end
```

Related Commands

Command	Description
bandwidth	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
class (policy-map)	Specifies the name of the class whose policy you want to create or change and the default class (commonly known as the class-default class) before you configure its policy.
police (percent)	Configures traffic policing on the basis of a percentage of bandwidth available on an interface.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
priority	Gives priority to a class of traffic belonging to a policy map.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
shape max-buffers	Specifies the maximum number of buffers allowed on shaping queues.
show policy-map interface	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

shape (policy-map class)

To shape traffic to the indicated bit rate according to the algorithm specified, or to enable ATM overhead accounting, use the **shape** command in policy-map class configuration mode. To remove shaping and leave the traffic unshaped, use the **no** form of this command.

shape [average | peak] mean-rate [burst-size] [excess-burst-size]

no shape [average | peak]

Syntax Description	average	(Optional) Committed Burst (Bc) is the maximum number of bits sent				
Cynaw 2000rprom	average	out in each interval.				
	peak	(Optional) Bc + Excess Burst (Be) is the maximum number of bits sent out in each interval.				
	mean-rate	(Optional) Also called committed information rate (CIR). Indicates the bit rate used to shape the traffic, in bits per second. When this command is used with backward explicit congestion notification (BECN) approximation, the bit rate is the upper bound of the range of bit rates that will be permitted.				
		For a committed (average) burst rate, valid values are 30,000–10,000,000,000. For an excess (peak) burst rate, valid values are 8,000-10,000,000,000.				
	burst-size	(Optional) The number of bits in a measurement interval (Bc).				
	excess-burst-size	(Optional) The acceptable number of bits permitted to go over the Be.				
	account	(Optional) Enables ATM overhead accounting.				
		Note This keyword is required if you configure ATM overhead accounting.				
	qinq	Specifies queue-in-queue (qinq) encapsulation as the broadband aggregation system (BRAS) to digital subscriber line access multiplexer (DSLAM) encapsulation type for ATM overhead accounting.				
	dot1q	Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type for ATM overhead accounting.				
	aal5	Specifies the ATM Adaptation Layer 5 service for ATM overhead accounting. AAL5 supports connection-oriented variable bit rate (VBR) services.				

Command Default When the excess burst size (Be) is not configured, the default Be value is equal to the committed burst size (Bc). For more information about burst size defaults, see the *Usage Guidelines* section.

Traffic shaping overhead accounting for ATM is disabled.

Command Modes Policy-map class configuration (config-pmap-c)

Command History	Release Modification					
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.				
Usage Guidelines	The measurement interval is the committed burst size (Bc) divided by committed information rate (CIR). Bc cannot be set to 0. If the measurement interval is too large (greater than 128 milliseconds), the system subdivides it into smaller intervals.					
		fy the committed burst size (Bc) and the excess burst size (Be), the algorithm decides for the shape entity. The algorithm uses a 4 milliseconds measurement interval, so Bc				
	Burst sizes larger than the default committed burst size (Bc) need to be explicitly specified. The larger the Bc, the longer the measurement interval. A long measurement interval may affect voice traffic latency, if applicable.					
	When the excess be (Bc).	urst size (Be) is not configured, the default value is equal to the committed burst size				
Examples		mple configures a shape entity with a CIR of 1 Mbps and attaches the policy map e-all-action to interface pos1/0/0:				
	policy-map dts-interface-all-action class class-interface-all shape average 1000000					
	interface pos1/0, service-policy o	/0 output dts-interface-all-action				
	Traffic Shaping Over	rhead Accounting for ATM				
	When a parent policy has ATM overhead accounting enabled for shaping, you are not required to enable accounting at the child level using the police command. In the following configuration example, ATM overhead accounting is enabled for bandwidth on the gaming and class-default class of the child policy map named subscriber_classes and on the class-default class of the parent policy map named subscriber_line. The voip and video classes do not have ATM overhead accounting explicitly enabled. These priority classes have ATM overhead accounting implicitly enabled because the parent policy has ATM overhead accounting enabled. Notice that the features in the parent and child policies use the same encapsulation type.					
	class class-defa	1 2 ining percent 80 account aal5 snap-rbe-dot1q				

bandwidth remaining percent 20 account aal5 snap-rbe-dot1q
policy-map subscriber_line
class class-default
bandwidth remaining ratio 10 account aal5 snap-rbe-dot1q
shape average 512 account aal5 snap-rbe-dot1q
service policy subscriber_classes

Related Commands	Command	Description				
	bandwidth	Specifies or modifies the bandwidth allocated for a class belonging to a policy map, and enables ATM overhead accounting.				
	show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. If configured, the command output includes information about ATM overhead accounting.				
	show running-config	Displays the current configuration of the router. If configured, the command output includes information about ATM overhead accounting.				

show asr901 multicast-support

To display the platform support for IPv4 or IPv6 multicast, use the **show asr901 multicast-support** command.

show asr901 multicast-support

Syntax Description	This command has no arguments or keywords.				
Command Modes	Privileged EXEC (#)				
Command History	Release	Modification			
	15.4(1)S	This command was introduced on the Cisco ASR 901 Series Aggregation Services Routers.			
Usage Guidelines Examples	This example shows the	the platform support for IPv4 or IPv6 multicast. output from show asr901 multicast-support command on a			
	Cisco ASR 901 series ro Router# show asr901 mm				
		IPv4(v6) Multicast: ENABLED			
	<u> </u>				
Related Commands	Command	Description			
	asr901-platf-multicast	Enables platform multicast.			

enable

show atm cell-packing

To display cell packing information for the Layer 2 attachment circuits (ACs) configured on your system, use the show atm cell-packing command in privileged EXEC mode.

show atm cell-packing

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.

Examples

The following example shows output from the show atm cell-packing command:

Router# show atm cell-packing

		a	vg #	avg	s #	
Circuit Type		local MNCP	cells/pkt rcvd	negotiated MNCP	cells/pkt sent	MCPT (us)
ATM0/2/0/1.200	vc 1/200	1	0	1	0	50
ATM0/2/0/1.300	vc 1/300	1	0	1	0	50

Related Commands	Command	Description		
	cell-packing	Packs multiple ATM cells into each MPLS or L2TPv3 packet.		
	atm cell-packing	Packs multiple ATM cells into each MPLS or L2TPv3 packet.		

show cem circuit

To display a summary of CEM circuits, use the show cem circuit command in privileged EXEC mode.

show cem circuit [cem-id]

Syntax Description	<i>cem-id</i> (Optional) Identifies the circuit configured					red with the cem-group command.		
Command Modes	Privileged EXEC	Privileged EXEC						
Command History	Release		Modif	fication				
	15.1(2)SNG		Suppo	ort for this	command was introduc	ed on the Cisco ASR 901 router.		
Examples	The following ex	amp	oles show t	he output g	generated by this comm	and;		
	Router# show ce	m c:	ircuit					
		ID	Ctrlr	Admin	Circuit A	.C		
	 CEM0/0	0	UP	 UP	Enabled U	 IP		
		1	UP	UP		IP		
		2	UP	UP		- IP		
		3	UP	UP		P		
	CEM0/4	4	UP	UP	Enabled U	P		
	CEM0/5	5	UP	UP	Enabled U	P		
	Router# show ce	Router# show cem circuit 5						
	CEM0/5, ID: 5, Line: UP, Admin: UP, Ckt: Enabled							
	Controller stat							
		Idle Pattern: 0xFF, Idle cas: 0x8						
	Dejitter: 4, Sa	Dejitter: 4, Sample Rate: 1, Payload Size: 192						
	Framing: Framed, (DS0 channels: 1-24)							
	CEM Defects Set							
	None							
	Signalling: No RTP: No RTP	CAS						
	Ingress Pkts:	53	27521938		Dropped:	0		
	Egress Pkts:		27521938		Dropped:	0		
	CEM Counter Det	ail	a					
	Input Errors:	.a.ı.; 0	5		Output Errors:	0		
	Pkts Missing:	0			Pkts Reordered:	0		
	Misorder Drops:				JitterBuf Underrun:			
	Error Sec:	0			Severly Errored Sec			
					-			
	Unavailable Sec	• ()			Failure Counts:	0		

Related Commands

Command	Description		
show cem circuit detail	Displays detailed information about all CEM circuits.		
show cem platform	Displays platform-specific error counters for all CEM circuits.		
show cem platform errors	Displays platform-specific error counters for all CEM circuits.		

show cem platform

To display platform-specific error counters for all CEM circuits, use the **show cem platform** command in privileged EXEC mode.

show cem platform [interface]

Syntax Description	<i>interface</i> (Optional) Identifies the CEM interface (for example, CEM0/1).					
Command Modes	Privileged EXEC					
Command History	Release Modification					
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.				
Examples	The following exa	mples show the output generated by this command:				
	Router# show cem	platform				
	CEM0/0 errors:					
	_	========= 50/527658758				
		s_underflow === 26 s_overflow ==== 24				
	Last cleared 60					
	CEM0/1 errors:					
	net2cem_drops =	=======================================				
	net2cem_drops	s_underflow === 25				
	-	s_overflow ==== 25				
	Last cleared 6d02h					
	CEMO/2 errors:					
	<pre>net2cem_drops ============== 2/526990836 net2cem_drops_overflow ==== 2</pre>					
	net2cem_drops_over11ow ==== 2 Last cleared never					
	Last cleared never CEM0/3 errors:					
		=======================================				
	_	s_overflow ==== 1				
	Last cleared ne	ever				
	CEM0/4 errors:					
	net2cem_drops ====================================					
	<pre>net2cem_drops_underflow === 26</pre>					
	<pre>net2cem_drops_overflow ==== 25</pre>					
	Last cleared 6d02h					
	CEM0/5 errors: net2cem_drops ====================================					
	—					
	net2cem_drops_underflow === 24 net2cem_drops_overflow ==== 24					
	Last cleared 6d02h					
	Router# show cem	platform cem0/1				
	CEM0/1 errors: net2cem_drops ========= 50/527678398					
		s_underflow === 25				
	-	s_overflow ==== 25				
	Last cleared 60	-				

Related Commands

Command	Description		
show cem circuit	Displays a summary of CEM circuits.		
show cem circuit detail	Displays detailed information about all CEM circuits.		
show cem platform errors	Displays platform-specific error counters for all CEM circuits.		
	show cem circuit detail		

show etherchannel

To display EtherChannel information for a channel, use the **show etherchannel** command in privileged EXEC mode.

show etherchannel [channel-group] {port-channel | detail | summary | port | load-balance}

Syntax Description	channel-group	(Optional) Number of the channel group. If you do not specify a value for the channel-group argument, all channel groups are displayed.					
	port-channel	Displays port channel information					
	detail	Displays detailed EtherChannel information.					
	summary	Displays a one-line summary per channel group.					
	port	Displays EtherChannel port information.					
	load-balance	Displays load-balance information.					
	protocol	Displays the enabled protocol.					
Command Modes	Privileged EXEC (#)					
Command History	Release	Modification					
Commanu History	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.					
Usage Guidelines	If you do not specify a value for the channel-group argument, all channel groups are displayed. If the interface is configured as part of the channel in ON mode, the show etherchannel protocol command displays Protocol: - (Mode ON).						
	• In the output of the show etherchannel summary command, the following conventions apply:						
	• In the column that displays the protocol that is used for the channel, if the channel mode is ON, a hyphen (-) is displayed.						
	For LACP, multiple aggregators are supported. For example, if two different bundles are created, Po1 indicates the primary aggregator, and Po1A and Po1B indicates the secondary aggregators.						
	In the output of the show etherchannel load-balance command, the following conventions apply:						
	• For EtherChannel load balancing of IPv6 traffic, if the traffic is bridged onto an EtherChannel (for example, it is a Layer 2 channel and traffic in the same VLAN is bridged across it), the traffic is always load balanced by the IPv6 addresses or src, dest, or src-dest, depending on the configuration. For this reason, the switch ignores the MAC/IP/ports for bridged IPv6 traffic. If you configure src-dst-mac, the src-dst-ip(v6) address is displayed. If you configure src-mac, the src-ip(v6) address is displayed.						
	• IPv6 traffic that is routed over a Layer 2 or a Layer 3 channel is load balanced based on MAC addresses or IPv6 addresses, depending on the configuration. The MAC/IP and the src/dst/src-dst are supported, but load balancing that is based on Layer 4 ports is not supported. If you use the port keyword, the IPv6 addresses or either src, dst, or src-dst, is displayed.						

Examples	The following example shows how to verify the configuration:					
	Router# show etherchannel load-balance EtherChannel Load-Balancing Configuration:					
	src-dst-mac					
	EtherChannel Load-Balancing Addresses Used Per-Protocol:					
	Non-IP: Source XOR Destination MAC address					
	IPv4: Source XOR Destination MAC address					
	IPv6: Source XOR Destination MAC address (routed packets					
	Source XOR Destination IP address (bridged packets)					

Related Commands	Command	Description		
	channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.		
	channel-protocol	Sets the protocol that is used on an interface to manage channeling.		

show ethernet loopback

To display information about the per port Ethernet loopbacks configured on a router or an interface, use the **show ethernet loopback** command in privileged EXEC mode.

show ethernet loopback active [brief | [interface-id] [service-instance id]]

Syntax Description	active	Displays active ethernet loopback sessions. Displays brief description of the current loopback sessions (Optional) Displays loopback information for the specified interface. Only physical interfaces support ethernet loopback.					
	brief						
	interface-id						
	service-instance id	e <i>id</i> Specifies the service instance ID.					
Command Modes	Privileged EXEC						
Command History	Release	Modification					
	15.2(2)SNG	This command was introduced on the Cisco ASR 901 router.					
Usage Guidelines		n <i>interface-id</i> , all configured loopbacks appear. The router supports a maximum					
-	of two Ethernet loopba The following example	ck configurations.					
	of two Ethernet loopba The following example Router# show etherne	ck configurations. shows how to verify the configuration: t loopback active					
	of two Ethernet loopba The following example Router# show etherne Interface	ck configurations. e shows how to verify the configuration: t loopback active : GigabitEthernet0/3					
	of two Ethernet loopba The following example Router# show etherne	ck configurations. shows how to verify the configuration: t loopback active					
	of two Ethernet loopba The following example Router# show etherne Interface Service Instance	<pre>ck configurations. e shows how to verify the configuration: t loopback active</pre>					
	of two Ethernet loopba The following example Router# show etherne ====================================	<pre>ck configurations. e shows how to verify the configuration: t loopback active ====================================</pre>					
	of two Ethernet loopba The following example Router# show etherne Interface Service Instance Direction Time out(sec) Status Start time	ck configurations. e shows how to verify the configuration: t loopback active : GigabitEthernet0/3 : 32 : Terminal : 300 : on : 14:15:01.742 IST Tue Jun 18 2013					
	of two Ethernet loopba The following example Router# show etherne ====================================	<pre>ck configurations. e shows how to verify the configuration: t loopback active ====================================</pre>					
	of two Ethernet loopba The following example Router# show etherne Interface Service Instance Direction Time out(sec) Status Start time Time left	ck configurations. e shows how to verify the configuration: t loopback active ====================================					
Examples	of two Ethernet loopba The following example Router# show etherne Interface Service Instance Direction Time out(sec) Status Start time Time left Source Mac Address	ck configurations. e shows how to verify the configuration: t loopback active ====================================					
Usage Guidelines Examples Related Commands	of two Ethernet loopba The following example Router# show etherne Interface Service Instance Direction Time out(sec) Status Start time Time left Source Mac Address Destination Mac Addr	ck configurations. e shows how to verify the configuration: t loopback active : GigabitEthernet0/3 : 32 : Terminal : 300 : on : 14:15:01.742 IST Tue Jun 18 2013 : 00:04:48 : 0000.0002.0002 ess : 4055.3989.751c					
Examples	of two Ethernet loopba The following example Router# show etherne Interface Service Instance Direction Time out(sec) Status Start time Time left Source Mac Address Destination Mac Addr	ck configurations. e shows how to verify the configuration: t loopback active : GigabitEthernet0/3 : 32 : Terminal : 300 : on : 14:15:01.742 IST Tue Jun 18 2013 : 00:04:48 : 0000.0002.0002 ess : 4055.3989.751c					

show interface port-channel

To display the EtherChannel interfaces and channel identifiers, with their mode and operational status, use the **show interface port-channel** command in privileged EXEC mode.

show interface port-channel {number}

Syntax Description	number	Optional value enables the display of information for one port channel interface number. The range is from 1 to 8.
Command Default	No default behavio	ors or values.
Command Modes	Privileged EXEC	
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.

show interfaces rep

Use the **show interfaces rep** User EXEC command to display Resilient Ethernet Protocol (REP) configuration and status for a specified interface or for all interfaces.

show interfaces [interface-id] rep [detail] [| {begin | exclude | include} expression]

Syntax Description	interface-id	(Optional) Display REP configuration and status for a specified physical interface or port channel ID.					
	detail	detail (Optional) Display detailed REP configuration and status information.					
	begin	 begin (Optional) Display begins with the line that matches the <i>expression</i> .					
	exclude	(Optional) Display excludes lines that match the expression.					
	include	(Optional) Display includes lines that match the specified expression.					
	expression	Expression in the output to use as a reference point.					
Command Modes	User EXEC						
Command History	Release	Modification					
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.					
Usage Guidelines	port) state, the (<i>FailNoNbr</i>). T	r the show interface rep [detail] command, in addition to an <i>Open</i> , <i>Fail</i> , or AP (alternate Port Role might show as <i>Fail Logical Open</i> (<i>FailLogOpen</i>) or <i>Fail No Ext Neighbor</i> hese states indicate that the port is physically up, but REP is not configured on the					
	neighboring port. In this case, one port goes into a forwarding state for the data path to help maintain connectivity during configuration. The Port Role for this port shows as Fail Logical Open; the port forwards all data traffic on all VLANs. The other failed Port Role shows as <i>Fail No Ext Neighbor</i> ; this port blocks traffic for all VLANs.						
	When the external neighbors for the failed ports are configured, the failed ports go through the alternate port state transitions and eventually go to an Open state or remain as the alternate port, based on the alternate port election mechanism.						
	The output of the output.	his command is also included in the show tech-support privileged EXEC command					
	г ·						

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is sample output from the **show interface rep** command:

Switch # show interface rep

Interface	Seg-id	Туре	LinkOp	Role
GigabitEthernet 0/1	1	Primary Edge	TWO_WAY	Open
GigabitEthernet 0/2	1	Edge	TWO_WAY	Open

This is sample output from the **show interface rep** command when the edge port is configured to have no REP neighbor. Note the asterisk (*) next to *Primary Edge*.

Router# show interface	rep			
Interface	Seg-id	Туре	LinkOp	Role
GigabitEthernet0/1	2		TWO_WAY	Open
GigabitEthernet0/2	2	Primary Edge*	TWO_WAY	Open

This is sample output from the **show interface rep** command when external neighbors are not configured:

Switch # show interface rep						
Interface	Seg-id	Туре	LinkOp	Role		
GigabitEthernet0/1	1		NO_NEIGHBOR	FailNoNbr		
GigabitEthernet0/2	2		NO_NEIGHBOR	FailLogOpen		

This is sample output from the **show interface rep detail** command for a specified interface:

```
Switch # show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2 REP enabled
Segment-id: 1 (Segment)
PortID: 00030019E85BDD00
Preferred flag: No
Operational Link Status: INIT_DOWN
Current Key: 0000000000000000000
Port Role: Fail
Blocked VLAN: 1-4094
Admin-vlan: 1
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: 1234567890123456
Configured Load-balancing Block VLAN: 1-4094
STCN Propagate to: none
LSL PDU rx: 0, tx: 0
HFL PDU rx: 0, tx: 0
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

Related Commands	Command	Description
	repsegment	Enables REP on an interface and assigns a segment ID. This command is also used to configure a port as an edge port, a primary edge port, or a preferred port.
	show reptopology [detail]	Displays information about all ports in the segment, including which one was configured and selected as the primary edge port.

show ip vrf

To display the set of defined Virtual Private Network (VPN) routing and forwarding (VRF) instances and associated interfaces, use the **show ip vrf** command in privileged EXEC mode.

show ip vrf [brief | detail | interfaces | id] [vrf-name] [output-modifiers]

brief	(Optional) Displays concise information on the VRFs and associated interfaces.			
detail	(Optional) Displays detailed information on the VRFs and associated interfaces.			
interfaces	(Optional) Displays detailed information about all interfaces bound to a particular VRF or any VRF.			
id	(Optional) Displays the VPN IDs that are configured in a PE router for different VPNs.			
vrf-name	(Optional) Name assigned to a VRF.			
output-modifiers	(Optional) For a list of associated keywords and arguments, use context-sensitive help.			
•	ds or arguments are specified, the command shows concise information about all			
Privileged EXEC				
Release	Modification			
15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.			
Use this comman	d to display information about VRFs. Two levels of detail are available:			
• The brief keyword (or no keyword) displays concise information.				
• The detail keyword displays all information.				
To display information about all interfaces bound to a particular VRF, or to any VRF, use the interfaces keyword. To display information about VPN IDs assigned to a PE router, use the id keyword.				
downstream VRF	ample displays information about all the VRFs configured on the router, including the for each associated VAI. The lines that are highlighted (for documentation purposes downstream VRF.			
Router# show ip	vrf			
Name Defaul	t RD Interface			
	detailinterfacesidvrf-nameoutput-modifiersWhen no keyword configured VRFs.Privileged EXECRelease15.1(2)SNGUse this command • The brief key • The detail ke To display inform keyword. To displayThe following exa downstream VRF only) indicate the Router# show ip			

Cisco ASR 901 Aggregation Services Router Command Reference Guide

Virtual-Access4 [D]

U	2:1	Virtual-Access3
		Virtual-Access4

Table 2-6 describes the significant fields shown in the display.

Table 2-6 show ip vrf Field Descriptions

Field	Description	
Name	Specifies the VRF name.	
Default RD	Specifies the default route distinguisher.	
Interface	Specifies the network interface.	

The following example displays detailed information about all of the VRFs configured on the router, including all of the VAIs associated with each VRF:

```
Router# show ip vrf detail
```

```
VRF D; default RD 2:0; default VPNID <not set>
 Interfaces:
        Loopback2
                            Virtual-Access3 [D] Virtual-Access4 [D]
 Connected addresses are not in global routing table
 Export VPN route-target communities
   RT:2:0
 Import VPN route-target communities
   RT:2:1
 No import route-map
 No export route-map
VRF U; default RD 2:1; default VPNID <not set>
 Interfaces:
   Virtual-Access3
                            Virtual-Access4
 Connected addresses are not in global routing table
 No Export VPN route-target communities
 Import VPN route-target communities
   RT:2:1
 No import route-map
 No export route-map
```

Table 2-7 describes the significant fields shown in the display.

Table 2-7 show ip vrf detail Field Descriptions

Field	Description	
VPNID	Specifies the VPN ID assigned to the VRF.	
Interfaces	Specifies the network interfaces.	
Virtual-Accessn [D]	Specifies the downstream VRF.	
Export	Specifies VPN route-target export communities.	
Import	Specifies VPN route-target import communities.	

The following example shows the interfaces bound to a particular VRF:

Router# show ip vrf interfaces

InterfaceIP-AddressVRFProtocol

```
Ethernet210.22.0.33vrflup
Ethernet410.77.0.33hubup
Router#
```

Table 2-8 describes the significant fields shown in the display.

Table 2-8 show ip vrf interfaces Field Descriptions

Field	Description	
Interface	Specifies the network interfaces for a VRF.	
IP-Address	Specifies the IP address of a VRF interface.	
VRF	Specifies the VRF name.	
Protocol	Displays the state of the protocol (up or down) for each VRF interface.	

The following is sample output that shows all the VPN IDs that are configured in the router and their associated VRF names and VRF route distinguishers (RDs):

Router# show ip vrf id

VPN Id	Name	RD
2:3	vpn2	<not set=""></not>
A1:3F6C	vpnl	100:1

Table 2-9 describes the significant fields shown in the display.

Field	ield Description	
VPN Id	Specifies the VPN ID assigned to the VRF.	
Name	Specifies the VRF name.	
RD	Specifies the route distinguisher.	

Table 2-9 show ip vrf id Field Descriptions

show mac-address-table

To display the MAC address table, use the show mac-address-table command in privileged EXEC mode.

show mac-address-table [address mac-addr] [aging-time vlan-id] [count vlan-id] [dynamic
[address mac-address | interface type slot/port | vlan vlan-id]] [interface type/number]
[multicast [{igmp-snooping | mld-snooping | vlan vlan-id}]] [static [[{address mac-addr} |
{interface interface/switch-num//slot/port} | vlan vlan-id] [vlan vlan-id]

Syntax Description	address mac-addr	Displays information about the MAC-address table for a specific MAC address; see the "Usage Guidelines" section for format guidelines.		
	vlan vlan-id	(Optional) Displays information for a specific VLAN only. Range: 1 to 4094.		
	aging-time	Displays information about the MAC-address aging time.		
	count	Displays the number of entries that are currently in the MAC-address table.		
	dynamic	Displays information about the dynamic MAC-address table entries only.		
	interface interface	(Optional) Displays information about a specific interface type; possible valid values are gigabitethernet and tengigabitethernet.		
	multicast	Displays information about the multicast MAC-address table entries only.		
	igmp-snooping	Displays the addresses learned by Internet Group Management Protocol (IGMP0 snooping.		
	mld-snooping	Displays the addresses learned by multicast listener discovery version 2 (MLDv2) snooping.		
	static	Displays information about the static MAC-address table entries only.		
	This command has no Privileged EXEC (#)	default settings.		
Command Modes	Privileged EXEC (#)			
Command Modes	Privileged EXEC (#) Release	Modification		
Command Modes Command History	Privileged EXEC (#)			
Command Modes Command History	Privileged EXEC (#) Release 15.1(2)SNG	Modification		
Command Modes Command History	Privileged EXEC (#) Release 15.1(2)SNG The mac-addr is a 48-1	Modification Support for this command was introduced on the Cisco ASR 901 router.		
Command Modes Command History	Privileged EXEC (#) Release 15.1(2)SNG The mac-addr is a 48-1 The count keyword dia The multicast keyword	Modification Support for this command was introduced on the Cisco ASR 901 router. bit MAC address and the valid format is H.H.H.		
Command Default Command Modes Command History Usage Guidelines	Privileged EXEC (#) Release 15.1(2)SNG The mac-addr is a 48-1 The count keyword dia The multicast keyword statically installed or I	Modification Support for this command was introduced on the Cisco ASR 901 router. bit MAC address and the valid format is H.H.H. splays the number of multicast entries. d displays the multicast MAC addresses (groups) in a VLAN or displays all		
Command Modes Command History	Privileged EXEC (#) Release 15.1(2)SNG The mac-addr is a 48-1 The count keyword dia The multicast keyword statically installed or I The dynamic entries the state of t	Modification Support for this command was introduced on the Cisco ASR 901 router. bit MAC address and the valid format is H.H.H. splays the number of multicast entries. d displays the multicast MAC addresses (groups) in a VLAN or displays all GMP snooping-learned entries in the Layer 2 table.		

show network-clock synchronization

Displays the information about network-clock synchronization.

show network-clock synchronization [detail]

Command Modes Privileged EXEC **Command History** Release Modification 15.1(2)SNG Support for this command was introduced on the Cisco ASR 901 router. **Usage Guidelines** This command confirms if the system is in revertive mode or non-revertive mode and verify the non-revertive configurations. **Examples** This command shows the output of the show network-clock synchronization command to confirm if the system is in revertive mode: RouterB#show network-clocks synchronization Symbols: En - Enable, Dis - Disable, Adis - Admin Disable NA - Not Applicable * - Synchronization source selected # - Synchronization source force selected & - Synchronization source manually switched Automatic selection process : Enable Equipment Clock : 2048 (EEC-Option1) Clock Mode : QL-Disable ESMC : Disabled SSM Option : 1 T0 : GigabitEthernet0/4 Hold-off (global) : 300 ms Wait-to-restore (global) : 300 sec Tsm Delay : 180 ms Revertive : No Nominated Interfaces Interface Mode/QL Prio ESMC Tx ESMC Rx SigType QL_IN Internal NA NA/Dis 251 QL-SEC NA NΑ то0/12 NA/En QL-FAILED NA NA NA 1 External 0/0/0 10M 2 NA/Dis OL-FAILED NA NA Gi0/1 20 NA Sync/En QL-FAILED -*Gi0/4 NA Sync/En 21 QL-DNU T4 Out External Interface SigType Input Prio Squelch AIS External 0/0/0 E1 CRC4 Internal 1 FALSE FALSE Use the show network-clock synchronization detail command to display all details of network-clock synchronization parameters at the global and interface levels.

> Router# **show network-clocks synchronization detail** Symbols: En - Enable, Dis - Disable, Adis - Admin Disable NA - Not Applicable

L

* - Synchronization source selected # - Synchronization source force selected & - Synchronization source manually switched Automatic selection process : Enable Equipment Clock : 2048 (EEC-Option1) Clock Mode : QL-Disable ESMC : Disabled SSM Option : 1 T0 : External 0/0/0 10m Hold-off (global) : 300 ms Wait-to-restore (global) : 0 sec Tsm Delay : 180 ms Revertive : Yes Force Switch: FALSE Manual Switch: FALSE Number of synchronization sources: 3 sm(netsync NETCLK_QL_DISABLE), running yes, state 2A Last transition recorded: (begin) -> 2A (sf_change) -> 2A

Nominated Interfaces

Interface	SigType	Mode/QL	Prio	QL_IN	ESMC Tx	ESMC Rx
Internal	NA	NA/Dis	251	QL-SEC	NA	NA
То0/12	NA	NA/En	3	QL-SEC	NA	NA
*External 0/0/	0 10M	NA/Dis	1	QL-SEC	NA	NA
Gi0/11	NA	Sync/En	2	QL-DNU	-	-

T4 Out

External Interface	SigType	Input	Prio	Squelch	AIS
External 0/0/0 E1	CRC4	Internal	1	FALSE	FALSE

Interface:

_____ _____ Local Interface: Internal Signal Type: NA Mode: NA(Ql-disabled) SSM Tx: DISABLED SSM Rx: DISABLED Priority: 251 QL Receive: QL-SEC QL Receive Configured: -QL Receive Overrided: -QL Transmit: -QL Transmit Configured: -Hold-off: 0 Wait-to-restore: 0 Lock Out: FALSE Signal Fail: FALSE Alarms: FALSE Slot Disabled: FALSE SNMP input source index: 1 SNMP parent list index: 0

Local Interface: To0/12 Signal Type: NA Mode: NA(Ql-disabled) SSM Tx: DISABLED SSM Rx: ENABLED Priority: 3 QL Receive: QL-SEC

QL Receive Configured: -QL Receive Overrided: -QL Transmit: -QL Transmit Configured: -Hold-off: 300 Wait-to-restore: 0 Lock Out: FALSE Signal Fail: FALSE Alarms: FALSE Slot Disabled: FALSE SNMP input source index: 2 SNMP parent list index: 0 Local Interface: External 0/0/0 Signal Type: 10M Mode: NA(Q1-disabled) SSM Tx: DISABLED SSM Rx: DISABLED Priority: 1 QL Receive: QL-SEC QL Receive Configured: -QL Receive Overrided: -QL Transmit: -QL Transmit Configured: -Hold-off: 300 Wait-to-restore: 0 Lock Out: FALSE Signal Fail: FALSE Alarms: FALSE Active Alarms : None Slot Disabled: FALSE SNMP input source index: 3 SNMP parent list index: 0 Local Interface: Gi0/11 Signal Type: NA Mode: Synchronous(Ql-disabled) ESMC Tx: ENABLED ESMC Rx: ENABLED Priority: 2 QL Receive: QL-DNU QL Receive Configured: -QL Receive Overrided: -QL Transmit: -QL Transmit Configured: -Hold-off: 300 Wait-to-restore: 0 Lock Out: FALSE Signal Fail: FALSE Alarms: FALSE None Slot Disabled: FALSE SNMP input source index: 4 SNMP parent list index: 0

External 0/0/0 el crc4's Input: Internal Local Interface: Internal Signal Type: NA Mode: NA(Ql-disabled) SSM Tx: DISABLED SSM Rx: DISABLED Priority: 1 QL Receive: QL-SEC QL Receive Configured: -QL Receive Overrided: -QL Transmit: -QL Transmit Configured: -Hold-off: 300 Wait-to-restore: 0 Lock Out: FALSE Signal Fail: FALSE Slot Disabled: FALSE SNMP input source index: 1 SNMP parent list index: 1

show platform hardware

To display the status of hardware devices on the Cisco ASR 901, use the **show platform hardware** command. The command displays information about hardware devices on the Cisco ASR 901 for troubleshooting and debugging purposes.

show platform hardware {adrian | bits | cpld | cpu | ethernet | fio | hwic | rtm | stratum | ufe winpath

Syntax Description	adrian	Displays information about the adrian hardware.
	bits	Displays information about the BITS hardware.
	cpld	Displays information about the CPLD hardware.
	сри	Displays information about the CPU.
	ethernet	Displays information about the ethernet interfaces on the Cisco ASR 901.
	fio	Displays information about the FIO fpga hardware.
	hwic	Displays information about the HWICs installed on the Cisco ASR 901.
	rtm	Displays information about the RTM Module (ASM-M2900-TOP daughter card).
	stratum	Displays information about the stratum hardware.
	ufe	Displays information about the UFE hardware.
	winpath	Displays information about the Winpath hardware.
Command Modes	Privileged EXEC	
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
	Command	Description
Related Commands	oommana	-

show platform ptp state

To display the status of ptp protocol on the Cisco ASR 901 router, use the **show platform ptp state** command.

show platform ptp state

Syntax Description This command has no arguments.

Command Modes Privileged EXEC

Examples

Command History	Release	Modification	
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	

TT1 C 11 C	1 1	1			
I be tollowing	example snows	sample outr	NULTOT chow n	latform ntn	state comamnd:
The ronowing	example shows	Sumple Outp	Juciol Blow P	racrorm pcp	Beace comunita.

	1
Router# show platform ptp state	
flag = 2	
	2 (Fast Loop)
FLL Status Duration :	7049 (sec)
Forward Flow Weight :	
Forward Flow Transient-Free :	
Forward Flow Transient-Free :	3600 (3600 sec Window)
Forward Flow Transactions Used:	23.0 (%)
Forward Flow Oper. Min TDEV :	4254.0 (nsec)
	38.0
Forward Flow Min Cluster Width:	7550.0 (nsec)
Forward Flow Mode Width :	21400.0 (nsec)
Reverse Flow Weight :	100.0
Reverse Flow Transient-Free :	900 (900 sec Window)
Reverse Flow Transient-Free :	3600 (3600 sec Window)
Reverse Flow Transactions Used:	200.0 (%)
Reverse Flow Oper. Min TDEV :	487.0 (nsec)
Reverse Mafie :	36.0
Reverse Flow Min Cluster Width:	225.0 (nsec)
Reverse Flow Mode Width :	450.0 (nsec)
Frequency Correction :	257.0 (ppb)
Phase Correction :	0.0 (ppb)
Output TDEV Estimate :	1057.0 (nsec)
Output MDEV Estimate :	1.0 (ppb)
Residual Phase Error :	0.0 (nsec)
Min. Roundtrip Delay :	45.0 (nsec)
Sync Packet Rate :	65 (pkts/sec)
Delay Packet Rate :	65 (pkts/sec)
Forward IPDV % Below Threshold:	0.0
Forward Maximum IPDV :	0.0 (usec)

Cisco ASR 901 Aggregation Services Router Command Reference Guide

Forward Interpacket Jitter : 0.0 (usec) Reverse IPDV % Below Threshold: 0.0 Reverse Maximum IPDV : 0.0 (usec) Reverse Interpacket Jitter : 0.0 (usec)

Related Commands	Command	Description
	show platform ptp stats	Displays statistics about the ptp protocol on the Cisco ASR 901
		router.

show platform ptp stats

To display statistics about ptp protocol on the Cisco ASR 901 router, use the **show platform ptp stats** command.

show platform ptp stats

- Syntax Description This command has no arguments.
- **Command Modes** Privileged EXEC

Command History	Release	Modification	
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	

Examples

The following example shows sample output for **show platform ptp stats** comamnd:

Statistics for PTP clock 0	

Number of ports : 1	
Pkts Sent : 1811997	
Pkts Rcvd : 619038	
Pkts Discarded : 0	
Statistics for PTP clock port 1	
*****	##
Pkts Sent : 1811997	
Pkts Rcvd : 619038	
Pkts Discarded : 0	
Signals Rejected : 0	
Statistics for peer 1	
#######################################	
IP addr : 9.9.9.14	
Pkts Sent : 355660	
Pkts Rcvd : 124008	
Statistics for peer 2	
##############################	
IP addr : 9.9.9.13	
Pkts Sent : 355550	
Pkts Rcvd : 123973	
Statistics for peer 3	
##############################	
IP addr : 9.9.9.11	
Pkts Sent : 354904	
Pkts Rcvd : 123972	
Statistics for peer 4	
############################	
IP addr : 9.9.9.12	
Pkts Sent : 353815	
Pkts Rcvd : 123525	
Statistics for peer 5	
############################	
IP addr : 9.9.9.10	
Pkts Sent : 352973	

Pkts Rcvd : 123326

Related Commands

Command	Description
show platform ptp status	Displays the status of the ptp protocol on the Cisco ASR 901 router.

show platform ptp stats detailed

To display detailed statistics about ptp protocol on the Cisco ASR 901 router, use the **show platform ptp stats detailed** command.

show platform ptp stats detailed

- **Syntax Description** This command has no arguments.
- Command Modes Privileged EXEC

Examples

 Release
 Modification

 15.1(2)SNG
 Support for this command was introduced on the Cisco ASR 901 router.

The following example shows sample output for **show platform ptp stats detailed** comamnd:

Statistics for PTP clock 0 ####################################	
Number of ports : 1 Pkts Sent : 37416 Pkts Rcvd : 113563 Invalid Pkts Rcvd : 0	
Pkts Sent : 37416 Pkts Rcvd : 113563 Invalid Pkts Rcvd : 0	
Pkts Rcvd : 113563 Invalid Pkts Rcvd : 0	
Invalid Pkts Rcvd : 0	
Statistics for PTP clock port 1	
stabled for fit ofoon port f	

Pkts Sent : 37416	
Pkts Rcvd : 113563	
Invalid Pkts Rcvd : 0	
Statistics for peer 0	

IP address : 10.10.10.	10
Announces Sent : 0	
Announces Rcvd : 297	
Syncs Sent : 0	
Syncs Revd : 37925	
Follow Ups Sent : 0	
Follow Ups Rcvd : 37925	
Delay Reqs Sent : 37404	
Delay Reqs Rcvd : 0	
Delay Resps Sent : 0	
Delay Resps Rcvd : 37404	
Mgmts Sent Rcvd : 0	
Mgmts Rovd : 0	
Signals Sent : 12	
Signals Rcvd : 12	
Invalid Packets Royd : 0	

Related Commands

Command	Description
show platform ptp stats	Displays the statistics of the ptp protocol on the Cisco ASR 901 router.

show platform tcam detailed

To display the current occupancy that includes per-TCAM rules information such as number of TCAM rules used or free and feature(s) using the TCAM rule, use the show platform tcam detailed command.

show platform tcam detailed

- **Syntax Description** This command has no arguments.
- Command Modes Privileged EXEC

 Command History
 Release
 Modification

 15.3(2)S
 This command was introduced on the Cisco ASR 901 Series Aggregation Services Routers.

Examples The following is sample output from the **show platform tcam detailed** command:

Router# show platform tcam detailed

Ingress : 2/8 slices, 512/2048 entries used Pre-Ingress: 3/4 slices, 768/1024 entries used Egress : 0/4 slices, 0/512 entries used

Slice ID: 1 Stage: Pre-Ingress Mode: Single Entries used: 28/256 Slice allocated to: Layer-2 Classify and Assign Group

Slice ID: 4 Stage: Pre-Ingress Mode: Double Entries used: 10/128 Slice allocated to: L2CP

Slice ID: 2 Stage: Ingress Mode: Double Entries used: 29/128 Slice allocated to: L2 Post-Switch Processing Group

Slice ID: 3
Stage: Ingress
Mode: Single
Entries used: 13/256
Slice allocated to: CESoPSN-UDP, CEF, Layer-3 Control Protocols

show platform tcam summary

To display the current occupancy of TCAM with summary of the number of TCAM rules allocated or free, use the show platform tcam summary command.

show platform tcam summary

Syntax Description	This command has no arguments.		
Command Modes	Privileged EXEC	:	
Command History	Release	Modification	
	15.3(2)S	This command was introduced on the Cisco ASR 901 Series Aggregation Services Routers.	
Examples	The following is	sample output freom the show platform tcam summary command:	
	Router# show pl	atform tcam summary	
	5	8 slices, 512/2048 entries used	
	Pre-Ingress: 3/	4 slices, 768/1024 entries used	
	Egress : 0/	4 slices, 0/512 entries used	

show policy-map

To display the configuration of all classes for a specified service policy map or of all classes for all existing policy maps, use the **show policy-map** command in user EXEC or privileged EXEC mode.

show policy-map [policy-map]

Syntax Description	policy-map	(Optional) Name of the service policy map whose complete configuration is to be displayed. The name can be a maximum of 40 characters.	
Command Default	All existing policy	map configurations are displayed.	
Command Modes	User EXEC (>) Privileged EXEC (i	¥)	
Command History	Release	Modification	
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
Usage Guidelines	 The show policy-map command displays the configuration of a policy map created using the policy-map command. You can use the show policy-map command to display all class configurations comprising any existing service policy map, whether or not that policy map has been attached to an interface. The command displays: ECN marking information only if ECN is enabled on the interface. Bandwidth-remaining ratio configuration and statistical information, if configured and used to 		
Examples	determine the a congestion.	amount of unused (excess) bandwidth to allocate to a class queue during periods of es sample output from typical show policy-map commands. Depending upon the	
	interface or platform in use and the options enabled (for example, Weighted Fair Queueing [WFQ]), the output you see may vary slightly.		
	Traffic Policing: Exa	nple	
	contents of a policy information rate (C	mple output from the show policy-map command. This sample output displays the map called "policy1." In policy 1, traffic policing on the basis of a committed IR) of 20 percent has been configured, and the bc and be have been specified in art of the traffic policing configuration, optional conform, exceed, and violate actions l.	
	Router# show poli	cy-map policy1	
	Policy Map poli Class class1 police cir p	cyl percent 20 bc 300 ms pir percent 40 be 400 ms	

conform-action transmit exceed-action drop violate-action drop

Table 2-10 describes the significant fields shown in the display.

 Table 2-10
 show policy-map Field Descriptions – Configured for Traffic Policing

Field	Description
Policy Map	Name of policy map displayed.
Class	Name of the class configured in the policy map displayed.
police	Indicates that traffic policing on the basis of specified percentage of bandwidth has been enabled. The committed burst (Bc) and excess burst (Be) sizes have been specified in milliseconds (ms), and optional conform, exceed, and violate actions have been specified.

Related Commands	Command	Description	
	bandwidth	Specifies or modifies the bandwidth allocated for a class belonging to a policy map, and enables ATM overhead accounting.	
	class (policy map)	Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.	
	class-map	Creates a class map to be used for matching packets to a specified class.	
	drop	Configures a traffic class to discard packets belonging to a specific class.	
	police	Configures traffic policing.	
	police (two rates)	Configures traffic policing using two rates, the CIR and the PIR.	
	policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.	
	shape	Shapes traffic to the indicated bit rate according to the algorithm specified, and enables ATM overhead accounting.	
	show policy-map class	Displays the configuration for the specified class of the specified policy map.	
	show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.	
	show running-config	Displays the current configuration of the router. If configured, the command output includes information about ATM overhead accounting.	
	show table-map	Displays the configuration of a specified table map or of all table maps.	
	table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.	

show policy-map interface

To display the statistics and the configurations of the input and output policies that are attached to an interface, use the **show policy-map interface** command in user EXEC or privileged EXEC mode.

show policy-map interface [type access-control] type number [vc [vpi/] vci] [dlci dlci]
[input | output]

Syntax Description	type	Type of interface or subinterface whose policy configuration is to be displayed.
	number	Port, connector, or interface card number.
	vc	(Optional) For ATM interfaces only, shows the policy configuration for a specified PVC.
	vpil	(Optional) ATM network virtual path identifier (VPI) for this permanent virtual circuit (PVC).
		The <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.
		The absence of both the forward slash (<i>I</i>) and a <i>vpi</i> value defaults the <i>vpi</i> value to 0. If this value is omitted, information for all virtual circuits (VCs) on the specified ATM interface or subinterface is displayed.
	vci	(Optional) ATM network virtual channel identifier (VCI) for this PVC. This value ranges from 0 to 1 less than the maximum value set for this interface by the atm vc-per-vp command. Typically, the lower values 0 to 31 are reserved for specific traffic (F4 Operation, Administration, and Maintenance [OAM], switched virtual circuit [SVC] signaling, Integrated Local Management Interface [ILMI], and so on) and should not be used.
		The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only.
		The <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.
	dlci	(Optional) Indicates a specific PVC for which policy configuration will be displayed.
	dlci	(Optional) A specific data-link connection identifier (DLCI) number used on the interface. Policy configuration for the corresponding PVC will be displayed when a DLCI is specified.
	input	(Optional) Indicates that the statistics for the attached input policy will be displayed.
	output	(Optional) Indicates that the statistics for the attached output policy will be displayed.
	slot	(ATM shared port adapter only) Chassis slot number. See the appropriate hardware manual for slot information. For SIPs, see the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.

	Isubslot(ATM shared port adapter only) Secondary slot number on an SPA interprocessor (SIP) where a SPA is installed. See the platform-specific SP hardware installation guide and the corresponding "Specifying the Interprocessor"		
		Address on an SPA" topic in the platform-specific SPA software configuration guide for subslot information.	
	lport	(ATM shared port adapter only) Port or interface number. See the appropriate hardware manual for port information. For SPAs, see the corresponding "Specifying the Interface Address" topics in the platform-specific SPA software configuration guide.	
	.subinterface	(ATM shared port adapter only—Optional) Subinterface number. The number that precedes the period must match the number to which this subinterface belongs. The range is 1 to 4,294,967,293.	
	interface-type	(Optional) Interface type; possible valid values are ethernet , gigabitethernet , tengigabitethernet	
	interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.	
	null 0	(Optional) Specifies the null interface; the only valid value is 0.	
	vlan vlan-id	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.	
	detailed	(Optional) Displays additional statistics.	
	class class-name	(Optional) Displays the QoS policy actions for the specified class.	
	port-channel channel-number	(Optional) Displays the EtherChannel port-channel interface.	
Command Default	This command displays the packet statistics of all classes that are configured for all service policies or the specified interface or subinterface or on a specific permanent virtual circuit (PVC) on the interface. The absence of both the forward slash (<i>I</i>) and a <i>vpi</i> value defaults the <i>vpi</i> value to 0. If this value is		
	omitted, information displayed.	for all virtual circuits (VCs) on the specified ATM interface or subinterface is	
Command Modes	Privileged EXEC (#)		
Command History	Release	Modification	
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
Usage Guidelines	The show policy-map interface command displays the packet statistics for classes on the specified interface or the specified PVC only if a service policy has been attached to the interface or the PVC.		
	The counters displaye congestion is present	ed after the show policy-map interface command is entered are updated only if on the interface.	

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
police	Configures traffic policing.
police (percent)	Configures traffic policing on the basis of a percentage of bandwidth available on an interface.
police (two rates)	Configures traffic policing using two rates, the CIR and the PIR.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
priority	Specifies that low-latency behavior must be given to a traffic class and configures multiple priority queues.
shape (percent)	Specifies average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface.
show class-map	Display all class maps and their matching criteria.
show interfaces	Displays statistics for all interfaces configured on a router or access server.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map class	Displays the configuration for the specified class of the specified policy map.

show ptp port running detail

To display the running details of the PTP port, use the show ptp port running detail command.

show ptp port running detail

Syntax Description	n This command has no arguments or keywords.			
Command Modes	Privileged EXEC	(#)		
Command History	Release	Modification		
	15.4(1)S	This command was introduced on the Cisco ASR 901 Series Aggregation Services Routers.		
Usage Guidelines	This command is	used to display running details of the PTP port.		
 Note	Accuracy and log selecting the best	variance are not displayed for the telecom profile since the fields are not required for master.		
Examples	This example shows the output from show ptp port running detail command on a Cisco ASR 901 router: Router# show ptp port running detail			
	PORT [SLAVE] CUP Protocol Addre	RRENT PTP MASTER PORT ess: 10.10.10.10 y: 0xE4:D3:F1:FF:FE:22:FD:B8		
	PORT [SLAVE] PREVIOUS PTP MASTER PORT Protocol Address: 30.30.30. Clock Identity: 0xE0:2F:6D:FF:FE:74:EF:70 Reason:			
	PORT [SLAVE] LIST OF PTP MASTER PORTS			
	Clock Identity PTSF Status: Alarm In Strea Clock Stream I Priority1: 128 Priority2: 128 Class: 84 Accuracy: Unkr	ess: 10.10.10 y: 0xE4:D3:F1:FF:FE:22:FD:B8 am: Id: 0 3 3		

LOCAL PRIORITY 1 Protocol Address: 30.30.30.30 Clock Identity: 0xE0:2F:6D:FF:FE:74:EF:70 PTSF Status: Alarm In Stream: Clock Stream Id: 0 Priority1: 1 Priority2: 1 Class: 104 Accuracy: Unknown <======= Offset (log variance): 0 <===== Steps Removed: 0

show rep topology

Use the **show rep topology** User EXEC command to display Resilient Ethernet Protocol (REP) topology information for a segment or for all segments, including the primary and secondary edge ports in the segment.

show rep topology [segment segment_id] [archive] [detail] [| {begin | exclude | include}
expression]

Syntax Description	segment-id	(Optional) Display REP topology information for the specified segment. The ID range is from 1 to 1024.
	archive	(Optional) Display the previous topology of the segment. This keyword can be useful for troubleshooting a link failure.
	detail	(Optional) Display detailed REP topology information.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	expression	Expression in the output to use as a reference point.

Command Modes User EXEC

Command History	Release	Modification
15.1(2)SNG		Support for this command was introduced on the Cisco ASR 901 router.

Usage Guidelines The output of this command is also included in the **show tech-support** privileged EXEC command output.

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is a sample output from the **show rep topology segment** privileged EXEC command:

Switch # show re	p topology	segmer	nt 1
REP Segment 1			
BridgeName	PortName	Edge	Role
sw1_multseg_3750	Gi1/1/1	Pri	Alt
sw3_multseg_3400	Gi0/13		Open
sw3_multseg_3400	Gi0/14		Alt
sw4_multseg_3400	Gi0/13		Open
sw4_multseg_3400	Gi0/14		Open
sw5_multseg_3400	Gi0/13		Open
sw5_multseg_3400	Gi0/14		Open
sw2_multseg_3750	Gi1/1/2		Open
sw2_multseg_3750	Gi1/1/1		Open
sw1_multseg_3750	Gi1/1/2	Sec	Open

This is a sample output from the **show rep topology** command when the edge ports are configured to have no REP neighbor:

 Switch # show rep topology

 REP Segment 2

 BridgeName
 PortName
 Edge
 Role

 sw8-ts8-51
 Gi0/2
 Pri*
 Open

 sw9-ts11-50
 Gi1/0/4
 Open

 sw9-ts11-50
 Gi0/2
 Alt

 sw1-ts11-45
 Gi0/2
 Alt

 sw8-ts8-51
 Gi0/1
 Sec*

This example shows output from the **show rep topology detail** command:

Router# show rep topology detail REP Segment 2 repc_2_24ts, Fa0/2 (Primary Edge) Alternate Port, some vlans blocked Bridge MAC: 0019.e714.5380 Port Number: 004 Port Priority: 080 Neighbor Number: 1 / [-10] repc_3_12cs, Gi0/1 (Intermediate) Open Port, all vlans forwarding Bridge MAC: 001a.a292.3580 Port Number: 001 Port Priority: 000 Neighbor Number: 2 / [-9] repc_3_12cs, Po10 (Intermediate) Open Port, all vlans forwarding Bridge MAC: 001a.a292.3580 Port Number: 080 Port Priority: 000 Neighbor Number: 3 / [-8] repc_4_12cs, Po10 (Intermediate) Open Port, all vlans forwarding Bridge MAC: 001a.a19d.7c80 Port Number: 080 Port Priority: 000 Neighbor Number: 4 / [-7] repc_4_12cs, Gi0/2 (Intermediate) Alternate Port, some vlans blocked Bridge MAC: 001a.a19d.7c80 Port Number: 002 Port Priority: 040 Neighbor Number: 5 / [-6]

<output truncated>

This example shows output from the **show rep topology segment archive** command:

Router# show rep REP Segment 1	topology	segment	: 1 archive
BridgeName	PortName	Edge	Role
sw1_multseg_3750	Gi1/1/1	Pri	Open
sw3_multseg_3400	Gi0/13		Open
sw3_multseg_3400	Gi0/14		Open
sw4_multseg_3400	Gi0/13		Open
sw4_multseg_3400	Gi0/14		Open
sw5_multseg_3400	Gi0/13		Open
sw5_multseg_3400	Gi0/14		Open
sw2_multseg_3750	Gi1/1/2		Alt
sw2_multseg_3750	Gi1/1/1		Open
sw1_multseg_3750	Gi1/1/2	Sec	Open

Related Commands	Command	Description
	rep segment	Enables REP on an interface and assigns a segment ID. This command is also used to configure a port as an edge port, a primary edge port, or a preferred port.

show table-map

To display the configuration of a specified table map or all table maps, use the **show table-map** command in EXEC mode.

show table-map *table-map-name*

Syntax Description	table-map-name	Name of table map used to map one packet-marking value to another. The name can be a maximum of 64 alphanumeric characters.		
Command Modes	EXEC			
Command History	Release	Modification		
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.		
Examples	In "map1", a "to–fror for establishing the "	The show table-map command shows the contents of a table map called "map 1". n" relationship has been established and a default value has been defined. The fields to-from" mappings are further defined by the policy map in which the table map Configuring a policy map is the next logical step after creating a table map.)		
	For instance, a precedence or differentiated services code point (DSCP) value of 0 could be mapped to a class of service (CoS) value of 1, or vice versa, depending on the how the values are defined in the table map. Any values not explicitly defined in a "to-from" relationship will be set to a default value. The following sample output of the show table-map command displays the contents of a table map called "map1". In this table map, a packet-marking value of 0 is mapped to a packet-marking value of 1. All other packet-marking values are mapped to the default value 3. Router# show table-map map1 Table Map map1 from 0 to 1 default 3			
	Table 2-11 describes the fields shown in the display.			
	Table 2-11 show tal	ble-map Field Descriptions		
	Field	Description		
	Table Map	The name of the table map being displayed.		
	from, to	The values of the "to–from" relationship established by the table-map (value mapping) command and further defined by the policy map in which		

the table map will be configured.

default

Related Commands	Command	Description
	policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
	show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
	show policy-map class	Displays the configuration for the specified class of the specified policy map.
	table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

show xconnect

To display information about xconnect attachment circuits and pseudowires (PWs), use the **show xconnect all** command in privileged EXEC mode.

show xconnect {all | interface interface | peer ip-address {all | vcid vcid}} [detail]

Syntax Description	all	Displays information about all xconnect attachment circuits and PWs.			
-	interface	Displays information about xconnect attachment circuits and PWs on the specified			
	interface	interface. Valid values for the argument are as follows:			
		• atm <i>number</i> —Displays xconnect information for a specific ATM interface or subinterface.			
		• atm <i>number</i> vp <i>vpi-value</i> —Displays virtual path (VP) xconnect information for a specific ATM virtual path identifier (VPI). This command does not display information about virtual connect (VC) xconnects using the specified VPI.			
		• atm <i>number</i> vp <i>vpi-value/vci-value</i> —Displays VC xconnect information for a specific ATM VPI and virtual circuit identifier (VCI) combination.			
		• serial <i>number</i> —Displays xconnect information for a specific serial interface.			
		• serial <i>number dlci-number</i> —Displays xconnect information for a specific Frame Relay data-link connection identifier (DLCI).			
		 vlan <i>vlan-number</i>—Displays vlan-mode xconnect information for a specific VLAN interface. Displays information about xconnect attachment circuits and PWs associated with the specified peer IP address. 			
	<pre>peer ip-address {all vcid vcid}</pre>				
		• all —Displays all xconnect information associated with the specified peer IP address.			
		• vcid <i>vcid</i> —Displays xconnect information associated with the specified peer IP address and the specified VC ID.			
	detail	(Optional) Displays detailed information about the specified xconnect attachment circuits and PWs.			
Command Modes	Privileged EXEC				
Command History	Release	Modification			
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.			
	The charment				
Usage Guidelines		ct all command can be used to display, sort, and filter basic information about all ent circuits and PWs.			

You can use the **show xconnect all** command output to help determine the appropriate steps to troubleshoot an xconnect configuration problem. More specific information about a particular type of xconnect can be displayed using the commands listed in the Related Commands table.

Examples

The following example shows **show xconnect all** command output in the brief (default) display format. The output shows information about the interfaces and VCs that have been configured to transport various Layer 2 packets on the router.

Router# show xconnect all

5	DN=Do	ST=Xconnect State, S1=Segment: own, AD=Admin Down, IA=Inactiv egment 1 S1 Segment 2 S2			
ST	Segme	ent 1		egment 2	S2
UP	ac	Et0/0(Ethernet)	UP m	pls 10.55.55.2:1000	UP
UP	ac	Et1/0.1:200(Eth VLAN)	UP m	pls 10.55.55.2:5200	UP
IA pri	ac	Et1/0.2:100(Eth VLAN)	UP a	c Et2/0.2:100(Eth VLAN)	UP
UP sec	ac	Et1/0.2:100(Eth VLAN)	UP m	pls 10.55.55.3:1101	UP

Table 2-12 describes the significant fields shown in the display.

Table 2-12 show xconnect all Field Descriptions

Field	Description		
XC ST	• State of the xconnect attachment circuit or PW. Valid states are:		
	• UP—The xconnect attachment circuit or PW is up. Both segment 1 and segment 2 must be up for the xconnect to be up.		
	• DN—The xconnect attachment circuit or PW is down. Either segment 1, segment 2, or both segments are down.		
	• IA—The xconnect attachment circuit or PW is inactive. This state is valid only when PW redundancy is configured.		
	• NH—One or both segments of this xconnect no longer has the required hardware resources available to the system.		
Segment 1 or	Information about the type of xconnect, the interface type, and the IP address the segment is using. Types of xconnects are:		
Segment 2	• ac—Attachment circuit.		
C	• pri ac—Primary attachment circuit.		
	• sec ac—Secondary attachment circuit.		
	mpls—Multiprotocol Label Switching.		
	• 12tp—Layer 2 Tunnel Protocol.		
S1	State of the segment. Valid states are:		
or	• UP—The segment is up.		
S2	• DN—The segment is down.		
	• AD—The segment is administratively down.		

The following example shows show xconnect all command output in the detailed display format:

5		ST=Xconnect State, S1=Segment Nown, AD=Admin Down, IA=Inacti		
ST	-	ent 1		Segment 2 S2
		Et0/0(Ethernet) Interworking: ip		mpls 10.55.55.2:1000 UP Local VC label 16 Remote VC label 16 pw-class: mpls-ip
UP	ac	Et1/0.1:200(Eth VLAN) Interworking: ip	UP mr	mpls 10.55.55.2:5200 UP Local VC label 17 Remote VC label 20 pw-class: mpls-ip
IA pri	ac	Et1/0.2:100(Eth VLAN) Interworking: none	UP ac	ac Et2/0.2:100(Eth VLAN) UP Interworking: none
UP sec	ac	Et1/0.2:100(Eth VLAN) Interworking: none	UP mr	mpls 10.55.55.3:1101 UP Local VC label 23 Remote VC label 17 pw-class: mpls

Router# show xconnect all detail

The additional fields displayed in the detailed output are self-explanatory.

Related Commands	Command	Description
Related Commanus	Commanu	Description
	show atm pvc	Displays all ATM PVCs and traffic information.
	show atm vc	Displays all ATM PVCs and SVCs and traffic information.
	show atm vp	Displays the statistics for all VPs on an interface or for a specific VP.
	show connect	Displays configuration information about drop-and-insert connections that have been configured on a router.
	show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
	show interfaces	Displays statistics for all interfaces configured on the router or access server.
	show mpls l2transport binding	Displays VC label binding information.
	show mpls l2transport vc	Displays information about AToM VCs that have been enabled to route Layer 2 packets on a router.

snmp mib rep trap-rate

To enable the router to send REP traps and sets the number of traps sent per second, use the **snmp mib rep trap-rate** command. To remove the traps, enter the **no snmp mib rep trap-rate** command.

snmp mib rep trap-rate value

no snmp mib rep trap-rate

Syntax Description	value	Specifies the number of traps sent per second. The range is from 0 to 1000. The default is 0 (no limit imposed; a trap is sent at every occurrence).	
Command Modes	Global Configuration		
Command History	Release	Modification	
ooninana mistory	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.	
Usage Guidelines		p-rate command configures the switch to send REP-specific traps to notify the perational status changes and port role changes.	
Examples	The example shows how to configure the switch to send REP-specific traps: Router(config)# snmp mib rep trap-rate 500		

speed

To configure the speed for a Fast Ethernet or Gigabit Ethernet interface, use the **speed** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

speed {**10** | **100** | **1000** }

no speed

Syntax Description	10 Configures the interface to transmit at 10 Mbps.					
	 100 Configures the interface to transmit at 100 Mbps. 1000 Configures the interface to transmit at 1000 Mbps. This keyword is valid only for interfaces that support Gigabit Ethernet. 					
Defaults	1000M					
Command Modes	Interface configura	ation				
Command History	Release	Modification				
	15.1(2)SNG	Support for this	command was introd	luced on the Cisco ASR 901 router.		
Usage Guidelines	Gigabit Ethernet Internet	orts.	for 10/100/1000 por	ts and the speed 1000 command for		
	•		nlav only. Vou conno	t change the duplex mode on the Gigabit		
	U U			configured for Gigabit Ethernet.		
	Speed Command Sy	ntax Combinations				
	Table 2-1 lists the	supported command op	tions by interface.			
	Table 2-13 Suppo	orted speed Command (Options			
	Interface Type	Supported Syntax	Default Setting	Usage Guidelines		
	Gigabit Ethernet module	speed 1000	Speed is 1000.	Speed, duplex, and flow control are enabled.		
	10-Mbps ports	Factory set	Not applicable.			

When manually configuring the interface speed to either 10 or 100 Mbps, the switch prompts you to configure duplex mode on the interface.

Speed and Duplex Combinations

Table 2-14 describes the interface behavior for various combinations of the **duplex** and **speed** command settings. The specified **duplex** command configured with the specified **speed** command produces the resulting system action.

If you decide to configure the interface speed and duplex commands manually, and enter a value (for example, speed 10 or speed 100), ensure that you configure the connecting interface speed command to a matching speed.

You cannot set the duplex mode to **half** when the port speed is set at 1000 and similarly, you cannot set the port speed to **1000** when the mode is set to half duplex.



Changing the interface speed and duplex mode might shut down and reenable the interface during the reconfiguration.

duplex Command	speed Command	Resulting System Action
duplex half	speed 10	Forces 10-Mbps and half-duplex operation, and disables autonegotiation on the interface.
duplex full	speed 10	Forces 10-Mbps and full-duplex operation, and disables autonegotiation on the interface.
duplex half	speed 100	Forces 100-Mbps and half-duplex operation, and disables autonegotiation on the interface.
duplex full	speed 100	Forces 100-Mbps and full-duplex operation, and disables autonegotiation on the interface.
duplex full	speed 1000	Forces 1000-Mbps and full-duplex operation, and disables autonegotiation on the interface (Gigabit Ethernet only).

Table 2-14 Relationship Between duplex and speed Commands

```
Examples
```

The following example specifies advertisement of 10 Mbps operation only, and either full-duplex or half-duplex capability during autonegotiation:

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/1
Router(config-if)# speed 10
Router(config-if)# duplex full
```

With this configuration, the interface advertises the following capabilities during autonegotiation:

- 10 Mbps and half duplex
- 10 Mbps and full duplex

Related Commands	Command	Description
	duplex	Configures the duplex operation on an interface.
	interface gigabitethernet	Selects a particular Gigabit Ethernet interface for configuration.

Command	Description
show controllers gigabitethernet	Displays Gigabit Ethernet interface information, transmission statistics and errors, and applicable MAC destination address and VLAN filtering tables.
show interfaces gigabitethernet	Displays information about the Gigabit Ethernet interfaces.

synce state master

To configure the synchronous ethernet copper port as master, use the **synche state master** command. Use the **no** form of the command to disable the configuration.

synce state master

no synce state master

Syntax Description	This command has no arguments.
--------------------	--------------------------------

Command Default None

Command Modes Interface configuration

Command History	Release	Modification
	15.1(2)SNG	This command was introduced on the Cisco ASR 901 router.
Usage Guidelines	The synce state ma interface configura	aster command configures the synchronous ethernet copper port as the master in the tion mode.
Examples	C	mand configures the ethernet copper port as master:

Related Commands	Command	Description
	synce state slave	Configures the synchronous ethernet copper port as slave.

synce state slave

To configure the synchronous ethernet copper port as slave, use the **synche state slave** command. Use the **no** form of the command to disable the configuration.

synce state slave

no synce state slave

Syntax Description	This command has no arguments.
--------------------	--------------------------------

Command Default None.

Command Modes Interface configuration mode.

Command History	Release	Modification
	15.1(2)SNG	This command was introduced on the Cisco ASR 901 router.
Usage Guidelines	The synce state sla	we command configures the synchronous ethernet copper port as the slave in the

age Guidelines The **synce state slave** command configures the synchronous ethernet copper port as the slave in the interface configuration mode.

The following command configures the ethernet copper port as slave:

Router(config-if)# **synce state slave**

Related Commands	Command	Description
	synce state master	Configures the synchronous ethernet copper port as master.

Examples

synchronous mode

To configure the ethernet interface to synchronous mode, use the **synchronous mode** command. Use the **no** form of the command to disable the configuration.

synchronous mode

no synchronous mode

- **Command Default** Asynchronous mode.
- **Command Modes** Interface configuration.

Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.

Usage Guidelines This command is applicable to Synchronous Ethernet capable interfaces. The default value is asynchronous mode.

Examples This example configures the ethernet interface to synchronous mode: Router(config-if)#synchronous mode

table-map

To modify metric and tag values when the IP routing table is updated with BGP learned routes, use the **table-map** command in address family or router configuration mode. To disable this function, use the **no** form of the command.

table-map map-name

no table-map map-name

Syntax Description	map-name	Route map name from the route-map command.		
Defaults	This command is c	This command is disabled by default.		
Command Modes	Address family co Router configurati	•		
Command History	Release	Modification		
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.		
Usage Guidelines	This command is u You can use match	Is the route map name defined by the route-map command to the IP routing table. used to set the tag name and the route metric to implement redistribution. In clauses of route maps in the table-map command. IP access list, autonomous system p match clauses are supported.		
Examples	In the following read	outer configuration mode example, the Cisco IOS software is configured to		

router bgp 100 address-family ipv4 unicast table-map tag

Related Commands	Command	Description
	address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
	address-family vpn4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
	match as-path	Matches a BGP autonomous system path access list.
	match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
	match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
	route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

termination

Configures the DSL interface to function as central office equipment or customer premises equipment. Use the **no** form of this command to remove the configuration.

termination {co | cpe}

no termination {co | cpe}

SyntaDescription	со	The WIC functions as central office equipment and can interface with another G.SHDSL WIC configured as cpe
	сре	The WIC functions as customer premises equipment and can interface with a DSLAM or with another G.SHDSL WIC configured as co.
Defaults	The default setting	; is cpe .
Command Modes	Controller configu	ration
Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.
Examples	The following exa	mple shows how to use the termination command:
	. 5,	e terminal controller shdsl2/0 ntroller)# equipment-type co
Related Commands	Command	Description
	controller	Configures the digital subscriber line (DSL) controller.

transport ipv4

Specifies the IP version, traffic type (multicast or unicast), and interface that a PTP clock port uses to send traffic.

transport ipv4 {unicast | multicast} interface slot/port [negotiation]

no transport ipv4 {unicast | multicast} interface slot/port [negotiation]

Syntax Description	unicast	Specifies that the router sends unicast PTP traffic.		
	multicast	Specifies that the router sends multicast PTP traffic.		
	interface	Specifies the interface used to send PTP traffic.		
	slotlport	Backplane slot number and port number on the interface. Refer to your hardware installation manual for the specific values and slot numbers.		
	subslot number	Defines the subslot on the router in which the HWIC is installed.		
	port	Port number of the controller. Valid numbers are 0 and 1. The slash mark (<i>l</i>) is required between the <i>slot</i> argument and the <i>port</i> argument.		
	negotiation	(Optional) Enables dynamic discovery of slave devices and their preferred format for sync interval and announce interval messages.		
Defaults	The IP version, transmission mode, and interface are not specified for exchanging timing packets. PTP clock-port configuration mode			
	I II CIOCK-poit co			
Command History	Release	Modification		
Command History	Release 15.1(2)SNG			
	15.1(2)SNG	Modification		
Command History Examples	The following examples of the following exam	Modification Support for this command was introduced on the Cisco ASR 901 router. mple shows how to enable ptp priority1 value: e terminal ptp clock ordinary domain 0 tp-clk)# clock-port MASTER Master tp-port)# transport ipv4 unicast interface loopback 23 negotiation p-port)# exit		
Examples	15.1(2)SNG The following exam Router # configur Router (config)# ; Router (config-pt; Router (config-pt; Router (config-pt;	Modification Support for this command was introduced on the Cisco ASR 901 router. mple shows how to enable ptp priority1 value: e terminal ptp clock ordinary domain 0 tp-clk)# clock-port MASTER Master tp-port)# transport ipv4 unicast interface loopback 23 negotiation p-port)# exit p-clk)# exit		
	The following examples of the following exam	Modification Support for this command was introduced on the Cisco ASR 901 router. mple shows how to enable ptp priority1 value: e terminal ptp clock ordinary domain 0 tp-clk)# clock-port MASTER Master tp-port)# transport ipv4 unicast interface loopback 23 negotiation p-port)# exit		

tune-buffer port

To configure hardware buffer values on the port to avoid traffic drops due to congestion, use the **tune-buffer port** command in global configuration mode. To remove this configuration, use the **no** form of this command.

tune-buffer port port-no

Syntax Description	port-no	Port number associated with Gigabit Ethernet interfaces. Valid values range from 0 to 11.			
Command Default	This configuration is disabled by default.				
Command Modes	Global configurat	ion (config#)			
Command History	Release	Modification This command was introduced.			
Usage Guidelines	This command is used only on the Gigabit Ethernet interfaces. Use this command to avoid traffic drop that occur due to congestion, as a result of formation of micro loops during link recovery.				
Examples	The following example shows how to avoid traffic drops: Router# configure terminal Router(config)# tune-buffer port 2				

xconnect logging redundancy

To enable system message log (syslog) reporting of the status of the xconnect redundancy group, use the **xconnect logging redundancy** command in global configuration mode. To disable syslog reporting of the status of the xconnect redundancy group, use the **no** form of this command.

xconnect logging redundancy

no xconnect logging redundancy

Defaults Syslog reporting of the status of the xconnect redundancy group is disabled.

Command Modes Global configuration

Command History	Release	Modification
	15.1(2)SNG	Support for this command was introduced on the Cisco ASR 901 router.

Usage Guidelines Use this command to enable syslog reporting of the status of the xconnect redundancy group.

Examples

The following example enables syslog reporting of the status of the xconnect redundancy group and shows the messages that are generated during switchover events:

Router# config t Router(config)# xconnect logging redundancy Router(config)# exit

Activating the Primary Member

00:01:07: %XCONNECT-5-REDUNDANCY: Activating primary member 10.55.55.2:1000

Activating the Backup Member:

00:01:05: %XCONNECT-5-REDUNDANCY: Activating secondary member 10.55.55.3:1001

Related Commands	Command	Description
	xconnect	Binds an Ethernet, 802.1q VLAN, or Frame Relay attachment circuit to an Layer 2 PW for xconnect service and enters xconnect configuration mode.

