

map-class atm

This command is no longer supported.

map-class frame-relay

To specify a map class to define quality of service (QoS) values for a switched virtual circuit (SVC), use the **map-class frame-relay** command in global configuration mode.

map-class frame-relay *map-class-name*

Syntax Description	<i>map-class-name</i>	Name of this map class.
---------------------------	-----------------------	-------------------------

Defaults A map class is not specified.

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines After you specify the named map class, you can specify the QoS parameters—such as incoming and outgoing committed information rate (CIR), committed burst rate, excess burst rate, and the idle timer—for the map class.

To specify the protocol-and-address combination to which the QoS parameters are to be applied, associate this map class with the static maps under a map list.

Examples The following example specifies a map class called “hawaii” and defines three QoS parameters for it. The “hawaii” map class is associated with a protocol-and-address static map defined under the **map-list** command.

```
map-list bermuda source-addr E164 123456 dest-addr E164 654321
 ip 10.108.177.100 class hawaii
 appletalk 1000.2 class hawaii

map-class frame-relay hawaii
 frame-relay cir in 2000000
 frame-relay cir out 56000
 frame-relay be out 9000
```

Related Commands	Command	Description
	frame-relay bc	Specifies the incoming or outgoing Bc for a Frame Relay VC.
	frame-relay be	Sets the incoming or outgoing Be for a Frame Relay VC.
	frame-relay cir	Specifies the incoming or outgoing CIR for a Frame Relay VC.
	frame-relay idle-timer	Specifies the idle timeout interval for an SVC.

map-group

To associate a map list with a specific interface, use the **map-group** command in interface configuration mode.

map-group *group-name*

Syntax Description	<i>group-name</i>	Name used in a map-list command.
--------------------	-------------------	---

Defaults A map list is not associated with an interface.

Command Modes Interface configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines A map-group association with an interface is required for switched virtual circuit (SVC) operation. In addition, a map list must be configured.

The **map-group** command applies to the interface or subinterface on which it is configured. The associated E.164 or X.121 address is defined by the **map-list** command, and the associated protocol addresses are defined by using the **class** command under the **map-list** command.

Examples The following example configures a physical interface, applies a map group to the physical interface, and then defines the map group:

```
interface serial 0
 ip address 172.10.8.6
 encapsulation frame-relay
 map-group bermuda
 frame-relay lmi-type q933a
 frame-relay svc

map-list bermuda source-addr E164 123456 dest-addr E164 654321
 ip 10.1.1.1 class hawaii
 appletalk 1000.2 class rainbow
```

Related Commands	Command	Description
	class (map-list)	Associates a map class with a protocol-and-address combination.
	map-list	Specifies a map group and link it to a local E.164 or X.121 source address and a remote E.164 or X.121 destination address for Frame Relay SVCs.

map-list

To specify a map group and link it to a local E.164 or X.121 source address and a remote E.164 or X.121 destination address for Frame Relay switched virtual circuits (SVCs), use the **map-list** command in global configuration mode. To delete a previous map-group link, use the **no** form of this command.

map-list *map-group-name* **source-addr** { **e164** | **x121** } *source-address* **dest-addr** { **e164** | **x121** } *destination-address*

no map-list *map-group-name* **source-addr** { **e164** | **x121** } *source-address* **dest-addr** { **e164** | **x121** } *destination-address*

Syntax Description

<i>map-group-name</i>	Name of the map group. This map group must be associated with a physical interface.
source-addr { e164 x121 }	Type of source address.
<i>source-address</i>	Address of the type specified (E.164 or X.121).
dest-addr { e164 x121 }	Type of destination address.
<i>destination-address</i>	Address of the type specified (E.164 or X.121).

Defaults

A map group is not linked to a source and destination address.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use the **map-class** command and its subcommands to define quality of service (QoS) parameters—such as incoming and outgoing committed information rate (CIR), committed burst rate, excess burst rate, and the idle timer—for the static maps defined under a map list.

Each SVC needs to use a source and destination number, in much the same way that a public telephone network needs to use source and destination numbers. These numbers allow the network to route calls from a specific source to a specific destination. This specification is done through map lists.

Depending on switch configuration, addressing can take either of two forms: E.164 or X.121.

An X.121 address number is 14 digits long and has the following form:

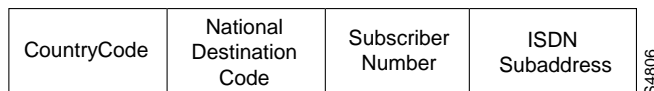
Z CC P NNNNNNNNNN

[Table 5](#) describes the codes in an X.121 address number form.

Table 5 X.121 Address Numbers

Code	Meaning	Value
Z	Zone code	3 for North America
C	Country code	10–16 for the United States
P	Public data network (PDN) code	Provided by the PDN
N	10-digit number	Set by the network for the specific destination

An E.164 number has a variable length; the maximum length is 15 digits. An E.164 number has the fields shown in [Figure 1](#) and described in [Table 6](#).

Figure 1 E.164 Address Format**Table 6** E.164 Address Field Descriptions

Field	Description
Country code	Can be 1, 2, or 3 digits long. Some current values are the following: <ul style="list-style-type: none"> • Code 1—United States of America • Code 44—United Kingdom • Code 61—Australia
National destination code + subscriber number	Referred to as the National ISDN number; the maximum length is 12, 13, or 14 digits, based on the country code.
ISDN subaddress	Identifies one of many devices at the termination point. An ISDN subaddress is similar to an extension on a PBX.

Examples

In the following SVC example, if IP or AppleTalk triggers the call, the SVC is set up with the QoS parameters defined within the class “hawaii”. An SVC triggered by either protocol results in two SVC maps, one for IP and one for AppleTalk. Two maps are set up because these protocol-and-address combinations are heading for the same destination, as defined by the **dest-addr** keyword and the values following it in the **map-list** command.

```
map-list bermuda source-addr e164 123456 dest-addr e164 654321
 ip 10.1.1.1 class hawaii
 appletalk 1000.2 class hawaii
```

Related Commands	Command	Description
	class (map-list)	Associates a map class with a protocol-and-address combination.
	map-class frame-relay	Specifies a map class to define QoS values for an SVC.

match

To specify whether to use the first three bits in the type of service (ToS) octet or the first six bits of the Differentiated Services Code Point (DSCP) octet of the IP header for mapping packet service levels to Frame Relay permanent virtual circuit (PVC) bundle members, use the **match** command in Frame Relay VC-bundle configuration mode. To change the mapping scheme used, override the current configuration by using the **match** command with the other keyword. This command does not have a **no** form.

match { dscp | precedence }

Syntax Description

dscp	Specifies that the DSCP octet in the IPv4 header is used to map packet service levels to specific Frame Relay PVC bundle members. Currently the first six bits of the DSCP octet are used for mapping, providing 64 packet service levels numbered 0 through 63.
precedence	Specifies that the precedence field of the ToS octet is used to map packet service levels to specific Frame Relay PVC bundle members. The precedence field consists of the first three bits of the ToS octet, providing eight precedence levels numbered 0 through 7.

Defaults

precedence

Command Modes

Frame Relay VC-bundle configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

The default PVC bundle match type is **precedence**. To change the match type to DSCP, use the **match dscp** command. When this command is executed, the system displays the message “Resetting vc-bundle configuration” on the console. When the match type is changed, the system removes all level designations that were previously configured.

To return the PVC bundle match type to the default setting of **precedence**, use the **match precedence** command.

A PVC bundle cannot perform precedence matching and DSCP matching at the same time. If the wrong matching scheme is configured for the traffic type, unpredictable behavior will result.

When tag-switching is enabled on the interface by using the **tag-switching ip** command, PVC bundles that are configured for IP precedence mapping are automatically converted to MPLS EXP mapping. The PVC bundle functionality remains the same with respect to priority levels, bumping, and so on, but the **match precedence** command is replaced by “match exp”, and each **precedence** command is replaced by the **exp** command. The result is that a bundle-member PVC previously configured to carry precedence level 1 IP traffic now carries EXP level 1 MPLS traffic.

PVC bundles configured for DSCP mapping go down when tag-switching is enabled. The DSCP configuration for each bundle-member PVC is reset, causing the PVCs to be unmapped and Inverse ARP, bumping, and protection settings to be unconfigured. The **match dscp** command is replaced by “match exp”.

When tag-switching is disabled, the **match precedence** and **match dscp** commands are restored.

Examples

The following example sets the match type to DSCP for the PVC bundle MP-4-dynamic:

```
Router(config)# interface serial 1/4.1 multipoint
Router(config-if)# frame-relay vc-bundle MP-4-dynamic
Router(config-fr-vcb)# match dscp
%Resetting vc-bundle configuration.
```

Related Commands

Command	Description
dscp (Frame Relay VC-bundle-member)	Configures the DSCP value or values for a Frame Relay PVC bundle member.
exp	Configures MPLS EXP levels for a Frame Relay PVC bundle member.
precedence (Frame Relay VC-bundle-member)	Configures the precedence levels for a Frame Relay PVC bundle member.

max bandwidth

To specify the total amount of outgoing bandwidth available to switched virtual circuits (SVCs) in the current configuration, use the **max bandwidth** command in interface-ATM-VC configuration mode. To remove the current bandwidth setting, use the **no** form of this command.

max bandwidth *kbps*

no max bandwidth *kbps*

Syntax Description	<i>kbps</i>	Total amount of outgoing bandwidth in kilobits per second available to all SVCs in the current configuration.
---------------------------	-------------	---

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	Interface-ATM-VC configuration
----------------------	--------------------------------

Command History	Release	Modification
	12.1(3)T	This command was introduced.

Usage Guidelines	Only the guaranteed cell rate of an SVC is counted toward the maximum bandwidth.
-------------------------	--

Examples In following example, an SVC called “anna” on ATM interface 2/0/0 is configured using the **max bandwidth** command to allow a maximum of 50 Mbps of bandwidth to be used by all of the SVCs in this configuration:

```
interface ATM 2/0/0
  svc anna
  encapsulation aal5auto
  protocol ppp virtual-template 1
  max bandwidth 50000
```

Related Commands	Command	Description
	max vc	Specifies the maximum number of SVCs that can be established using the current configuration.

max vc

To specify the maximum number of switched virtual circuits (SVCs) that can be established using the current configuration, use the **max vc** command in interface-ATM-VC configuration mode. To restore the maximum number of SVCs to the default setting, use the **no** form of this command.

max vc *number*

no max vc *number*

Syntax Description	<i>number</i>	Maximum number of SVCs to be established using the current SVC configuration.
---------------------------	---------------	---

Defaults	4096 SVCs
-----------------	-----------

Command Modes	Interface-ATM-VC configuration
----------------------	--------------------------------

Command History	Release	Modification
	12.1(3)T	This command was introduced.

Examples In following example, an SVC called “anna” on ATM interface 2/0/0 is configured using the **max vc** command to allow a maximum of 100 SVCs to be established using this configuration:

```
interface ATM 2/0/0
  svc anna
  encapsulation aal5auto
  protocol ppp virtual-template 1
  max vc 100
```

Related Commands	Command	Description
	max bandwidth	Specifies the maximum amount of bandwidth available to all SVCs in the current configuration.
	svc	Creates an ATM SVC.

mid

To set the range of message identifier (MID) values on a permanent virtual circuit (PVC), use the **mid** interface-ATM-VC configuration command. To remove MID value range settings, use the **no** form of this command.

mid *midlow midhigh*

no mid *midlow midhigh*

Syntax Description		
	<i>midlow</i>	Starting MID number for this PVC. This can be set between 0 and 1023.
	<i>midhigh</i>	Ending MID number for this PVC. This can be set between 0 and 1023.

Defaults 0

Command Modes Interface-ATM-VC configuration

Command History	Release	Modification
	11.3(2)T	This command was introduced.

Usage Guidelines This command is only available when SMDS encapsulation is configured on a PVC. Use this command to assign different ranges of message identifiers to different PVCs.

Examples In the following example, the **atm mid-per-vc** command limits the maximum number of message identifiers to 32 for each VC on the ATM interface. Using the **mid** command, the selected range of numbers that are available for the message identifiers on PVC 1/40 is 0 to 31. For PVC 2/50, the range is 32 to 63.

```
interface atm 2/0
  atm mid-per-vc 32
  pvc 1/40 smds
  mid 0 31
  pvc 2/50 smds
  mid 32 63
```

mode extended

To select extended Autodomain mode, use the **mode extended** command in SSG-auto-domain configuration mode. To reenable basic Autodomain mode, use the **no** form of this command.

mode extended

no mode extended

Syntax Description This command has no arguments or keywords.

Defaults Basic Autodomain mode is selected.

Command Modes SSG-auto-domain configuration

Command History	Release	Modification
	12.2(4)B	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines Use the **mode extended** command to select the extended Autodomain mode. In basic Autodomain mode, the profile downloaded from the AAA server for the selected Autodomain name is a service profile, which may or may not contain attributes specific to Service Selection Gateway (SSG). In extended Autodomain mode, the profile is a “virtual user” profile, which may contain a list of services in addition to other account attributes. The “virtual user” profile contains one autoservice to an authenticated service such as a proxy, VPDN, or tunnel. Connection to the autoservice occurs in the same way as in basic Autodomain mode. The host object is not activated until the user is authenticated at the service. The presence of SSD allows the user to access any other service in the specified user profile. Extended mode also enables users with multiple service selection to log on.

Examples The following example shows how to enable extended Autodomain mode:

```
ssg enable
ssg auto-domain
mode extended
select username
exclude apn company
exclude domain cisco
download exclude-profile abc password1
nat user-address
```

Related Commands	Command	Description
	download exclude-profile	Adds to the Autodomain download exclusion list.
	exclude	Configures the Autodomain exclusion list.

Command	Description
nat user-address	Enables NAT on Autodomain tunnel service.
select	Configures the Autodomain selection mode.
show ssg auto-domain exclude-profile	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.
ssg auto-domain	Enables SSG Autodomain mode.
ssg enable	Enables SSG functionality.

nat user-address

To enable Network Address Translation (NAT) toward Autodomain service, use the **nat user-address** command in SSG-auto-domain mode. To disable NAT on Autodomain service, use the **no** form of this command.

nat user-address

no nat user-address

Syntax Description This command has no arguments or keywords.

Defaults NAT is not applied toward Autodomain services and IP addresses assigned at the tunnel, VPDN, or proxy service will be assigned at the host and then sent back to the RADIUS client. NAT is always applied towards the Autodomain connection regardless of the configuration of the **nat user-address** command when the Access-Request from the RADIUS client contains an IP address.

Command Modes SSG-auto-domain

Command History	Release	Modification
	12.2(4)B	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines Use the **nat user-address** command to enable NAT toward the Autodomain connection. When a host object has not been assigned an IP address using the Access-Request from the RADIUS client, Service Selection Gateway (SSG) by default passes an IP address assigned at the tunnel, VPDN, or proxy service back to the RADIUS client and NAT does not happen toward the Autodomain connection. The **nat user-address** command overrides the default behavior and specifies that NAT should be performed towards Autodomain services. If a host has been assigned an IP address via the Access-Request, NAT happens toward the Autodomain connection regardless of the status of this command.

Examples The following example enables NAT toward the Autodomain connection:

```

ssg enable
ssg auto-domain
mode extended
select username
exclude apn motorola
exclude domain cisco
download exclude-profile abc password1
nat user-address

```

Related Commands

Command	Description
download exclude-profile	Adds to the Autodomain download exclusion list.
exclude	Configures the Autodomain exclusion list.
mode extended	Enables extended mode for SSG Autodomain.
select	Configures the Autodomain selection mode.
show ssg auto-domain exclude-profile	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.
ssg enable	Enables SSG functionality.

network (ssg-redirect)

To add an IP address to a named network list, use the **network** command in SSG-redirect-network configuration mode. To remove an IP address from a named network list, use the **no** form of this command.

network *ip-address mask*

no network *ip-address mask*

Syntax Description

<i>ip-address</i>	IP address that is to be added to a named network list.
<i>mask</i>	Mask for the associated IP subnet.

Defaults

No default behavior or values.

Command Modes

SSG-redirect-network configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use this command to define an individual network that is found in a named network list. Use the **network-list** command to define and name the network list and the **network** command to add an individual IP address to the named network list.

Packets arriving from an authorized user who is attempting to access an unauthorized service from an IP address that is part of a named network list can be redirected to a captive portal group that presents the user with an appropriate response, such as a logon screen. Service Selection Gateway (SSG) TCP Redirect for Services uses a marked TCP port or TCP port list in addition to the destination IP address to determine if a packet is redirected to a captive portal group.

Define a named TCP port list using the **port-list** command, and add TCP ports to the named TCP port list using the **port (ssg-redirect)** command.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a named network list.

Examples

The following example creates a network list named “RedirectNw” and adds IP address 10.0.0.0 255.0.0.0 and address 10.2.2.0 255.255.255.0 to the “RedirectNw” network list:

```
ssg tcp-redirect
network-list RedirectNw
network 10.0.0.0 255.0.0.0
network 10.2.2.0 255.255.255.0
```

Related Commands

Command	Description
network-list	Defines a list of one or more IP networks that make up a named network list.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

network-clock-select (ATM)

To establish the sources and priorities of the requisite clocking signals for an ATM-CES port adapter, use the **network-clock-select** global configuration command. To remove the clock source, use the **no** form of this command.

network-clock-select *priority* { **cbr** | **atm** } *slot/port*

no network-clock-select *priority* { **cbr** | **atm** } *slot/port*

Syntax Description

<i>priority</i>	Priority of the clock source. Values are 1 (high priority) to 4 (low priority).
cbr	Specifies a CBR interface to supply the clock source.
atm	Specifies an ATM interface to supply the clock source.
<i>slot</i>	Backplane slot number.
<i>port</i>	Interface port number.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

To support synchronous or synchronous residual time stamp (SRTS) clocking modes on the CBR interface, you must specify a primary reference source to synchronize the flow of CBR data from its source to its destination.

You can specify up to four clock priorities. The highest priority active interface in the router supplies primary reference source to all other interfaces that require network clock synchronization services. The fifth priority is the local oscillator on the ATM-CES port adapter.

Use the **show network-locks** command to display currently configured clock priorities on the router.

Examples

The following example defines two clock priorities on the router:

```
network-clock-select 1 cbr 2/0
network-clock-select 2 atm 2/0
```

Related Commands

Command	Description
ces aal1 clock	Configures the AAL1 timing recovery clock for the CBR interface.

Command	Description
ces dsx1 clock source	Configures a transmit clock source for the CBR interface.
show network-clocks	Displays which ports are designated as network clock sources.

network-list

To define a list of one or more IP networks that make up a named network list and to enter SSG-redirect-network configuration mode, use the **network-list** command in SSG-redirect configuration mode. To remove a named network list, use the **no** form of this command.

network-list *network-listname*

no network-list *network-listname*

Syntax Description

network-listname Defines the name of the network list.

Defaults

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use this command to define a list of one or more IP networks that make up a named network list. Use the *network-listname* attribute to name the IP network list.

Packets arriving from an authorized user who is attempting to access an unauthorized service from an IP address that is part of a named network list can be redirected to a captive portal group that presents the user with an appropriate response, such as a logon screen. Service Selection Gateway (SSG) TCP Redirect for Services uses a marked TCP port or TCP port list in addition to the destination IP address to determine if a packet is redirected to a captive portal group.

Define a named TCP port list using the **port-list** command, and add TCP ports to the named TCP port list using the **port (ssg-redirect)** command.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a named network list.

Examples

The following example defines an IP network list named "RedirectNw":

```
network-list RedirectNw
```

Related Commands

Command	Description
network (ssg-redirect)	Adds an IP address to a named network list.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.

Command	Description
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

oam ais-rdi

To configure an ATM permanent virtual circuit (PVC) to be brought down after a specified number of Operation, Administration, and Maintenance (OAM) alarm indication signal/remote defect indication (AIS/RDI) cells have been received on the PVC or brought up if no OAM AIS/RDI cells have been received in a specified interval, use the **oam ais-rdi** command in ATM VC configuration or VC class configuration mode. To return OAM AIS/RDI behavior to the default, use the **no** form of this command.

oam ais-rdi [*down-count* [*up-count*]]

no oam ais-rdi [*down-count* [*up-count*]]

Syntax Description		
	<i>down-count</i>	(Optional) Number of consecutive OAM AIS/RDI cells received before the PVC is brought down. The range is from 1 to 60. The default is 1.
	<i>up-count</i>	(Optional) Number of seconds after which a PVC will be brought up if no OAM AIS/RDI cells are received. The range is from 3 to 60. The default is 3.

Defaults	
	Down count: 1 Up count: 3

Command Modes	
	ATM VC configuration VC class configuration

Command History	Release	Modification
	12.1(2)T	This command was introduced.

Usage Guidelines	
	The default values for the OAM AIS/RDI down count and up count are used in the following situations: <ul style="list-style-type: none"> • If the oam ais-rdi command has not been entered • If the oam ais-rdi command is entered without the <i>up-count</i> or <i>down-count</i> argument • If the no oam ais-rdi command is entered

If the **oam ais-rdi** command is entered without the *up-count* or *down-count* argument, the command will not appear in the **show running-config** command output.

Examples	
	In the following example, PVC 0/400 will be brought down after 25 consecutive OAM AIS/RDI cells have been received on the PVC. The PVC will be brought up when no OAM AIS/RDI cells have been received for 5 seconds.

```
interface ATM2/0/0
 ip address 172.2.222.20 255.255.255.0
 no ip route-cache cef
 no ip route-cache distributed
 no atm ilmi-keepalive
 pvc 0/400
```

```
protocol ip 172.2.223.21
oam-pvc manage 30
oam ais-rdi 25 5
```

oam retry

To configure parameters related to Operation, Administration, and Maintenance (OAM) management for an ATM permanent virtual circuit (PVC), switched virtual circuit (SVC), VC class, or VC bundle, use the **oam retry** command in the appropriate command mode. To remove OAM management parameters, use the **no** form of this command.

oam retry *up-count down-count retry-frequency*

no oam retry *up-count down-count retry-frequency*

Syntax Description		
	<i>up-count</i>	Number of consecutive end-to-end F5 OAM loopback cell responses that must be received in order to change a PVC connection state to up. This argument does not apply to SVCs.
	<i>down-count</i>	Number of consecutive end-to-end F5 OAM loopback cell responses that are not received in order to change a PVC state to down or tear down an SVC connection.
	<i>retry-frequency</i>	The frequency (in seconds) that end-to-end F5 OAM loopback cells are transmitted when a change in the up/down state of a PVC or SVC is being verified. For example, if a PVC is up and a loopback cell response is not received after the <i>frequency</i> (in seconds) argument is specified using the oam-pvc command, then loopback cells are sent at the <i>retry-frequency</i> to verify whether the PVC is down.

Defaults

up-count = 3

down-count = 5

retry-frequency = 1 second

This set of defaults assumes that OAM management is enabled using the **oam-pvc** or **oam-svc** command.

Command Modes

Interface-ATM-VC configuration (for an ATM PVC or SVC)

VC-class configuration (for a VC class)

Bundle configuration mode (for a VC bundle)

PVC range configuration (for an ATM PVC range)

PVC-in-range configuration (for an individual PVC within a PVC range)

Command History

Release	Modification
11.3 T	This command was introduced.
12.0(3)T	This command allows you to configure parameters related to OAM management for ATM VC bundles.
12.1(5)T	This command was made available in PVC range and PVC-in-range configuration modes.

Usage Guidelines

The *up-count* argument does not apply to SVCs.

If the **oam retry** command is not explicitly configured on an ATM PVC, SVC, or VC bundle, the VC inherits the following default configuration (listed in order of precedence):

- Configuration of the **oam retry** command in a VC class assigned to the PVC or SVC itself.
- Configuration of the **oam retry** command in a VC class assigned to the PVC's or SVC's ATM subinterface.
- Configuration of the **oam retry** command in a VC class assigned to the PVC's or SVC's ATM main interface.
- Global default: *up-count* = 3, *down-count* = 5, *retry-frequency* = 1 second. This set of defaults assumes that OAM management is enabled using the **oam-pvc** or **oam-svc** command. The *up-count* and *retry-frequency* arguments do not apply to SVCs.

To use this command in bundle configuration mode, enter the bundle command to create the bundle or to specify an existing bundle before you enter this command.

If you use the **oam retry** command to configure a VC bundle, you configure all VC members of that bundle. VCs in a VC bundle are further subject to the following inheritance rules (listed in order of precedence):

- VC configuration in bundle-vc mode
- Bundle configuration in bundle mode (with effect of assigned VC-class configuration)
- Subinterface configuration in subinterface mode

Examples

The following example configures the OAM management parameters with *up-count* 3, *down-count* 3, and the *retry-frequency* at 10 seconds:

```
oam retry 3 3 10
```

Related Commands

Command	Description
broadcast	Configures broadcast packet duplication and transmission for an ATM VC class, PVC, SVC, or VC bundle.
class-int	Assigns a VC class to an ATM main interface or subinterface.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
encapsulation	Sets the encapsulation method used by the interface.
inarp	Configures the Inverse ARP time period for an ATM PVC, VC class, or VC bundle.
oam-bundle	Enables end-to-end F5 OAM loopback cell generation and OAM management for a virtual circuit class that can be applied to a virtual circuit bundle.
oam-pvc	Enables end-to-end F5 OAM loopback cell generation and OAM management for an ATM PVC or virtual circuit class.
oam-svc	Enables end-to-end F5 OAM loopback cell generation and OAM management for an ATM SVC or virtual circuit class.
protocol (ATM)	Configures a static map for an ATM PVC, SVC, VC class, or VC bundle. Enables Inverse ARP or Inverse ARP broadcasts on an ATM PVC by either configuring Inverse ARP directly on the PVC, on the VC bundle, or in a VC class (applies to IP and IPX protocols only).

Command	Description
ubr	Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
ubr+	Configures UBR QoS and specifies the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.

oam retry cc

To set the frequency at which ATM Operation, Administration, and Maintenance (OAM) F5 continuity check (CC) activation and deactivation requests are sent to a device at the other end of a segment or permanent virtual circuit (PVC), use the **oam retry cc** command in ATM virtual circuit configuration mode. To remove the retry settings, use the **no** form of this command.

```
oam retry cc {end | segment} [activation-count [deactivation-count [retry-frequency]]]
```

```
no oam retry cc {end | segment} [activation-count [deactivation-count [retry-frequency]]]
```

Syntax Description	end	End-to-end continuity check.
	segment	Segment continuity check.
	<i>activation-count</i>	(Optional) Maximum number of times the activation request will be sent before the receipt of an acknowledgment. The range is from 3 to 600. The default is 3.
	<i>deactivation-count</i>	(Optional) Maximum number of times the deactivation request will be sent before the receipt of an acknowledgment. The range is from 3 to 600. The default is 3.
	<i>retry-frequency</i>	(Optional) Interval between retries, in seconds. The default is 30 seconds.

Defaults	Activation count: 3 Deactivation count: 3 Retry frequency: 30 seconds
----------	---

Command Modes	ATM virtual circuit configuration
---------------	-----------------------------------

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Examples The following example shows how to configure ATM OAM F5 CC support over the segment and configure the router to function as the source. The frequency at which CC activation and deactivation requests will be sent over the segment is also configured.

```
interface atm 0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/40
  oam-pvc manage cc segment direction source
  oam retry cc segment 10 10 30
```

Related Commands

Command	Description
oam-pvc manage cc deny	Configures ATM OAM F5 CC management.
oam-pvc manage cc deny	Disables ATM OAM F5 CC support and configures the PVC to deny CC activation requests.

oam-pvc

To enable end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for an ATM permanent virtual circuit (PVC) or virtual circuit (VC) class, use the **oam-pvc** command in the appropriate command mode. To disable generation of OAM loopback cells and OAM management, use the **no** form of this command.

oam-pvc [**manage**] [*frequency*]

no oam-pvc [**manage**] [*frequency*]

Syntax Description	manage	(Optional) Enable OAM management.
	<i>frequency</i>	(Optional) Time delay (0 to 600 seconds) between transmitting OAM loopback cells.

Defaults	10 seconds
----------	------------

Command Modes	Interface-ATM-VC configuration (for an ATM PVC) VC-class configuration (for a VC class) PVC-in-range configuration (for an individual PVC within a PVC range)
---------------	---

Command History	Release	Modification
	11.3	This command was introduced.
	12.1(5)T	This command was made available in PVC-in-range configuration mode.

Usage Guidelines If OAM management is enabled, further control of OAM management is configured using the **oam retry** command.

If the **oam-pvc** command is not explicitly configured on an ATM PVC, the PVC inherits the following default configuration (listed in order of precedence):

- Configuration of the **oam-pvc** command in a VC class assigned to the PVC itself.
- Configuration of the **oam-pvc** command in a VC class assigned to the PVC's ATM subinterface.
- Configuration of the **oam-pvc** command in a VC class assigned to the PVC's ATM main interface.
- Global default: End-to-end F5 OAM loopback cell generation and OAM management are disabled, but if OAM cells are received, they are looped back. The default value for the *frequency* argument is 10 seconds.

Examples The following example enables end-to-end F5 OAM loopback cell transmission and OAM management on an ATM PVC with a transmission frequency of 3 seconds:

```
oam-pvc manage 3
```

Related Commands	Command	Description
	ilmi manage	Enables ILMI management on an ATM PVC.
	oam retry	Configures parameters related to OAM management for ATM PVC, SVC, or VC class.

oam-pvc manage cc

To configure ATM Operation, Administration, and Maintenance (OAM) F5 continuity check (CC) management, use the **oam-pvc manage cc** command in ATM virtual circuit configuration mode. To disable OAM F5 continuity checking, use the **no** form of this command.

```
oam-pvc manage cc { end | segment } [direction { both | sink | source }] [keep-vc-up [end aisrdi failure | seg aisrdi failure]]
```

```
no oam-pvc manage cc { end | segment } [deactivate-down-vc] [direction { both | sink | source }] [keep-vc-up [end aisrdi failure | seg aisrdi failure]]
```

Syntax Description		
end	End-to-end continuity checking. Monitoring occurs on the entire VC between two ATM end stations.	
segment	Segment continuity checking. Monitoring occurs on a VC segment between a router and a first-hop ATM switch.	
direction	(Optional) Direction of CC cell transmission.	
both	(Optional) Specifies that CC cells transmit toward and away from the activator.	
sink	(Optional) Specifies that CC cells transmit toward the activator. This is the default direction.	
source	(Optional) Specifies that CC cells transmit away from the activator.	
keep-vc-up	(Optional) Specifies that VC will be kept in the UP state when CC cells detect connectivity failure.	
end aisrdi failure	(Optional) Specifies that if end alarm indication signals/remote defect indications (AIS/RDI) cells are received, the VC will not be brought down because of segment CC failure.	
seg aisrdi failure	(Optional) Specifies that if segment AIS/RDI cells are received, the VC will not be brought down because of end CC failure or loopback failure.	
deactivate-down-vc	(Optional) Specifies that an OAM F5 CC deactivation message will be sent when the VC is operationally down and in the CC active state. This keyword is available only when the no form of this command is used.	

Defaults The default direction is **sink**.

Command Modes ATM virtual circuit configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines ATM OAM F5 continuity checking enables OAM to support the use of F5 segment and end-to-end CC cells to detect connectivity failures.

It is not necessary to enter a CC configuration on the router at the other end of a segment. The router on which CC management has been configured sends a CC activation request to the router at the other end of the segment, directing it to act as either a source or a sink.

Use the **oam-pvc manage cc deny** command to configure a permanent virtual circuit (PVC) to respond to activation requests from a peer device with “activation denied” messages. The **oam-pvc manage cc deny** command prevents ATM OAM F5 CC management from being activated on the PVC.

Use the **no oam-pvc manage cc** command to send a deactivation request to the peer device. The **no oam-pvc manage cc** command will disable ATM OAM F5 CC management on the PVC until the PVC receives an activation request. When the PVC receives an activation request, ATM OAM F5 CC management will be reenabled.

The **no oam-pvc manage cc {end | segment} deactivate-down-vc** command does not disable ATM OAM F5 CC support. This command causes OAM F5 CC deactivation messages to be sent over the VC when the VC goes down.

To enable the SNMP notifications that support ATM OAM F5 continuity checking, use the **snmp-server enable traps atm pvc extension** command.

Examples

ATM OAM F5 CC Support on a PVC Configuration Example

The following example shows how to configure ATM OAM F5 CC support over the segment and configure the router to function as the source. The frequency at which CC activation and deactivation requests will be sent over the segment is also configured.

```
interface atm 0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/40
  oam-pvc manage cc segment direction source
  oam retry cc segment 10 10 30
```

Deactivation of ATM OAM F5 CC upon VC Failure Example

The following example shows how to configure OAM to send a CC deactivation request across the segment when PVC 0/1 goes down:

```
interface atm 0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/40
  no oam-pvc manage cc segment deactivate-down-vc
```

Related Commands

Command	Description
debug atm oam cc	Displays ATM OAM F5 CC management activity.
oam-pvc manage cc deny	Disables ATM OAM F5 CC support and configures the PVC to deny CC activation requests.
oam retry cc	Sets the frequency at which ATM OAM F5 CC activation and deactivation requests are sent to the device at the other end of a segment or PVC.
show atm pvc	Displays all ATM PVCs and traffic information.

Command	Description
vpn service	Enables the sending of extended ATM PVC SNMP notifications and SNMP notifications for ATM OAM F5 CC, ATM OAM F5 AIS/RDI, and loopback failures.
snmp-server enable traps atm pvc extension mibversion	Specifies the MIB that supports extended ATM PVC SNMP notifications or the MIB that supports SNMP notifications for ATM OAM F5 CC management, ATM OAM F5 AIS/RDI management, and F5 loopback failure management.

oam-pvc manage cc deny

To disable ATM Operation, Administration, and Maintenance (OAM) F5 continuity check (CC) support and configure a PVC to deny CC activation requests, use the **oam-pvc manage cc deny** command in ATM virtual circuit configuration mode. To reenable OAM F5 CC support and allow CC activation requests, use the **no** form of this command.

oam-pvc manage cc {end | segment} deny

no oam-pvc manage cc {end | segment} deny

Syntax Description	end	End-to-end continuity checking.
	segment	Segment continuity checking.

Defaults If the peer device sends the activation message, F5 CC management will be enabled on the PVC.

Command Modes ATM virtual circuit configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines Use the **oam-pvc manage cc deny** command to configure a permanent virtual circuit (PVC) to respond to activation requests from a peer device with “activation denied” messages. The **oam-pvc manage cc deny** command prevents ATM OAM F5 CC management from being activated on the PVC.

Use the **no oam-pvc manage cc** command to send a deactivation request to the peer device. The **no oam-pvc manage cc** command will disable ATM OAM F5 CC management on the PVC until the PVC receives an activation request. When the PVC receives an activation request, ATM OAM F5 CC management will be reenabled.

Examples The following example shows how to disable ATM OAM F5 CC support and configure the VC to deny CC activation requests:

```
interface atm 0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/40
  oam-pvc manage cc segment deny
```

Related Commands

Command	Description
oam-pvc manage cc deny	Configures ATM OAM F5 CC management.
oam retry cc	Sets the frequency at which ATM OAM F5 CC activation and deactivation requests are sent to the device at the other end of a segment or PVC.

oam-range

To enable end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for an ATM permanent virtual circuit (PVC) range, use the **oam-range** PVC range configuration command. To disable generation of OAM loopback cells and OAM management, use the **no** form of this command.

oam-range [**manage**] [*frequency*]

no oam-range [**manage**] [*frequency*]

Syntax Description	manage	(Optional) Enables OAM management.
	<i>frequency</i>	(Optional) Time delay (0 to 600 seconds) between transmissions of OAM loopback cells.

Defaults	10 seconds
----------	------------

Command Modes	PVC range configuration
---------------	-------------------------

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines	If OAM management is enabled, further control of OAM management is configured using the oam retry command.
------------------	---

If the **oam-range** command is not explicitly configured for an ATM PVC range, the range inherits the following default configuration (listed in order of precedence):

- Configuration of the **oam-range** command in a VC class assigned to the range.
- Configuration of the **oam-range** command in a VC class assigned to the ATM subinterface for the range.
- Configuration of the **oam-range** command in a VC class assigned to the ATM main interface for the range.
- Global default: End-to-end F5 OAM loopback cell generation and OAM management are disabled, but if OAM cells are received, they are looped back. The default value for the *frequency* argument is 10 seconds.

Examples	The following example enables end-to-end F5 OAM loopback cell transmission and OAM management on an ATM PVC range called “range1” with a transmission frequency of 11 seconds:
----------	--

```
interface atm 6/0.1
 range range1 pvc 7/101 7/103
  oam-range manage 11
  oam retry 8 9 10
```

Related Commands	Command	Description
	ilmi manage	Enables ILMI management on an ATM PVC.
	oam-pvc	Enables end-to-end F5 OAM loopback cell generation and OAM management for an ATM PVC or VC class.
	oam retry	Configures parameters related to OAM management for ATM PVC, SVC, or VC class.

oam-svc

To enable end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for an ATM switched virtual circuit (SVC) or virtual circuit (VC) class, use the **oam-svc** command in the appropriate command mode. To disable generation of OAM loopback cells and OAM management, use the **no** form of this command.

oam-svc [**manage**] [*frequency*]

no oam-svc [**manage**] [*frequency*]

Syntax Description

manage (Optional) Enable OAM management.

frequency (Optional) Time delay (0 to 600 seconds) between transmitting OAM loopback cells.

Defaults

10 seconds

Command Modes

Interface-ATM-VC configuration (for an ATM SVC)
VC-class configuration (for a VC class)

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

If OAM management is enabled, further control of OAM management is configured using the **oam retry** command.



Note

Generally, ATM signalling manages ATM SVCs. Configuring the **oam-svc** command on an SVC verifies the inband integrity of the SVC.

If the **oam-svc** command is not explicitly configured on an ATM SVC, the SVC inherits the following default configuration (listed in order of precedence):

- Configuration of the **oam-svc** command in a VC class assigned to the SVC itself.
- Configuration of the **oam-svc** command in a VC class assigned to the SVC's ATM subinterface.
- Configuration of the **oam-svc** command in a VC class assigned to the SVC's ATM main interface.
- Global default: End-to-end F5 OAM loopback cell generation and OAM management are disabled, but if OAM cells are received, they are looped back. The default value for *frequency* is 10 seconds.

Examples

The following example enables end-to-end F5 OAM loopback cell transmission and OAM management on an ATM SVC with a transmission frequency of 3 seconds:

```
oam-svc manage 3
```

Related Commands

Command	Description
oam retry	Configures parameters related to OAM management for an ATM PVC, SVC, or VC class.

partial-fill

To configure the number of AAL1 user octets per cell for the ATM circuit emulation service (CES) on the OC-3/STM-1 Circuit Emulation Service network module, use the **partial-fill** interface-CES-VC command. To delete the CES partial-fill value, use the **no** form of this command.

partial-fill *octet*

no partial-fill *octet*

Syntax Description	<i>octet</i>	Number of user octets per cell for the CES. Possible values of octet range from 1 to 47.
---------------------------	--------------	--

Defaults	No partial-fill
-----------------	-----------------

Command Modes	Interface-CES-VC configuration
----------------------	--------------------------------

Command History	Release	Modification
	12.1(2)T	This command was introduced.

Usage Guidelines	The partial-fill command applies to CES SVCs and PVCs configured on Cisco 2600 series and Cisco 3600 series routers that have OC-3/STM-1 ATM CES network modules.
-------------------------	--

Examples	The following example sets the CES partial cell fill to 50 octets per cell for SVC "ces1":
-----------------	--

```
interface atm 1/0
  svc ces1 nsap 47.00.00.....01.01.00 ces
  partial fill 40
```

Related Commands	Command	Description
	svc	Creates an ATM SVC and specifies the destination NSAP address on a main interface or subinterface.

ping atm interface atm

To perform an ATM Operation, Administration, and Maintenance (OAM) ping to confirm connectivity for a specific permanent virtual circuit (PVC), use the **ping atm interface atm** command in privileged EXEC mode.

```
ping atm interface atm interface vpi vci [seg-loopback | end-loopback] [repeat [timeout]]
```

Syntax Description	
<i>interface</i>	ATM interface.
<i>vpi</i>	Virtual path identifier.
<i>vci</i>	Virtual channel identifier.
seg-loopback	(Optional) Sends ATM ping to segment loopback.
end-loopback	(Optional) Sends ATM ping to end loopback. This is the default.
<i>repeat</i>	(Optional) Number of ping packets that are sent to the destination address. Default is 5.
<i>timeout</i>	(Optional) Timeout interval. Default is 2 seconds.

Defaults

Send ping to end loopback.
5 repeat pings.
2-second timeout interval.

Command Modes

Privileged EXEC

Command History	Release	Modification
	11.4	This command was introduced on the LightStream 1010.
	12.0(21)S	This command was integrated into Cisco IOS Release 12.0(21)S.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The **ping atm interface atm** command sends an OAM packet and indicates when a response is received. You can choose one of two ping options:

- End loopback—Verifies end-to-end PVC integrity.
- Segment loopback—Verifies PVC integrity to the neighboring ATM device.

Examples

In the following example, an ATM OAM ping with a 5-second timeout verifies end-to-end connectivity for PVC 0/5:

```
Router# ping atm interface atm 0/0/0 0 5 end-loopback 5 5
```

```
Type escape sequence to abort.  
Sending 5, 53-byte end-to-end OAM echoes, timeout is 5 seconds:  
!!!!!
```

ping atm interface atm

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

In the following example, an ATM OAM ping verifies connectivity to the first-hop ATM switch on PVC 1/100:

```
Router# ping atm interface atm 0/0/0 1 100 seg-loopback
```

Type escape sequence to abort.

Sending 5, 53-byte segment OAM echoes, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Related Commands

Command	Description
debug atm oam	Displays information about ATM OAM events.
ping (privileged)	Checks host reachability and network connectivity.

port (ssg-redirect)

To add a TCP port to a named port list, use the **port** command in SSG-redirect-port configuration mode. To remove a TCP port from a named port list, use the **no port** form of this command.

port *port-number*

no port *port-number*

Syntax Description	<i>port-number</i>	Incoming destination port number.
--------------------	--------------------	-----------------------------------

Defaults No default behavior or values.

Command Modes SSG-redirect-port configuration

Command History	Release	Modification
	12.2(4)B	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines Use this command to add incoming destination ports to a named TCP port list. Incoming packets directed to a port in the named TCP port list can be redirected by the named captive portal group. Configure the named captive portal group using the **server-group** command, and add servers to the captive portal group using the **server (SSG)** command. Define and name the TCP port list using the **port-list** command.

You must enable Service Selection Gateway (SSG) using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define or add incoming destination ports to a named TCP port list.

Examples The following example creates a named TCP port list named “WebPorts” and adds TCP ports 80 and 8080:

```
ssg enable
ssg tcp-redirect
  port-list WebPorts
    port 80
    port 8080
```

Related Commands	Command	Description
	port-list	Defines a list of one or more TCP ports that make up a named port list and enters SSG-redirect-port configuration mode.
	server (SSG)	Adds a server to a captive portal group.

Command	Description
server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

port-list

To define a list of one or more TCP ports that make up a named port list and to enter SSG-redirect-port configuration mode, use the **port-list** command in SSG-redirect configuration mode. To disable a port list, use the **no** form of this command.

port-list *port-listname*

no port-list *port-listname*

Syntax Description	<i>port-listname</i>	Defines the name of the port list.
--------------------	----------------------	------------------------------------

Defaults	No default behavior or values.
----------	--------------------------------

Command Modes	SSG-redirect configuration
---------------	----------------------------

Command History	Release	Modification
	12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.	

Usage Guidelines Use this command to define a named port list. Use this command to create a list of TCP ports that can be redirected by the captive portal group. Use the **port (ssg-redirect)** command in SSG-redirect-port configuration mode to add TCP ports to the named port list.

You must enable Service Selection Gateway (SSG) using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a named port list.

Examples The following example creates a port list named “WebPorts”:

```
ssg enable
ssg tcp-redirect
port-list WebPorts
```

Related Commands	Command	Description
	port (ssg-redirect)	Adds a TCP port to a named port list.
	redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
	server (SSG)	Adds a server to a captive portal group.
	server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.

Command	Description
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

pppoe enable

To enable PPP over Ethernet (PPPoE) sessions on an Ethernet interface or subinterface, use the **pppoe enable** command in interface configuration mode. To disable PPPoE, use the **no** form of this command.

pppoe enable [**group** *group-name*]

no pppoe enable

Syntax Description	group	(Optional) Specifies that a PPPoE profile will be used by PPPoE sessions on the interface.
	<i>group-name</i>	(Optional) Name of the PPPoE profile to be used by PPPoE sessions on the interface.

Defaults PPPoE is disabled by default.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(2)T	This command was introduced.
	12.1(5)T	This command was modified to enable PPPoE on IEEE 802.1Q encapsulated VLAN interfaces.
	12.2(15)T	The group option was added.

Usage Guidelines If a PPPoE profile is not specified by using the **group** option, PPPoE sessions will be established using values from the global PPPoE profile. PPPoE profiles must be configured using the **bba-group pppoe** command.

Examples

PPPoE on an Ethernet Interface Example

The following example enables PPPoE sessions on Ethernet interface 1/0. PPPoE sessions will be established using the PPPoE parameters in the global PPPoE profile.

```
interface ethernet1/0
  pppoe enable
!
bba-group pppoe global
  virtual-template 1
  sessions max limit 8000
  sessions per-vc limit 8
  sessions per-mac limit 2
```

PPPoE on an 802.1Q VLAN Subinterface Example

The following example shows how to enable PPPoE on an 802.1Q VLAN subinterface. PPPoE sessions will be established using the PPPoE parameters in PPPoE profile “vpn1”.

pppoe enable

```

interface Ethernet2/3.1
  encapsulation dot1Q 1
  pppoe enable group vpn1
!
bba-group pppoe vpn1
  virtual-template 1
  sessions per-vc limit 2
  sessions per-mac limit 1

```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
debug pppoe	Displays debugging information for PPPoE sessions.
sessions max limit	Configures a PPPoE global profile with the maximum number of PPPoE sessions permitted on a router and sets the PPPoE session-count threshold.
sessions per-vlan limit	Specifies the maximum number of PPPoE sessions under each VLAN.

pppoe limit max-sessions

To specify the maximum number of PPP over Ethernet (PPPoE) sessions that will be permitted on a router, use the **pppoe limit max-sessions** command in VPDN group configuration mode. To remove this specification, use the **no** form of this command.

pppoe limit max-sessions *number-of-sessions*

no pppoe limit max-sessions

Syntax Description	<i>number-of-sessions</i>	Maximum number of PPPoE sessions that will be permitted on the router. The range is from 0 to the maximum number of interfaces on the router.
--------------------	---------------------------	---

Defaults	Maximum <i>number-of-sessions</i> is not set.
----------	---

Command Modes	VPDN group configuration
---------------	--------------------------

Command History	Release	Modification
	12.2(1)DX	This command was introduced.
	12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines	PPPoE session limits configured using the pppoe limit per-vc , pppoe limit per-vlan , pppoe max-sessions , pppoe max-sessions (VC) , and pppoe max-sessions (subinterface) commands take precedence over limits configured for the router using the pppoe limit max-sessions command.
------------------	---

Examples	The following example shows a limit of 100 PPPoE sessions configured for the router.
----------	--

```
vpdn enable

vpdn-group 1
 accept dialin
  protocol pppoe
  virtual-template 1
  pppoe limit max-sessions 100
```

Related Commands	Command	Description
	debug vpdn pppoe-errors	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.
	pppoe limit per-mac	Specifies the maximum number of PPPoE sessions to be sourced from a MAC address.

Command	Description
pppoe limit per-vc	Specifies the maximum number of PPPoE sessions permitted on all VCs.
pppoe limit per-vlan	Specifies the maximum number of PPPoE sessions permitted on a VLAN.
pppoe max-sessions	Specifies the maximum number of PPPoE sessions permitted on an ATM PVC, PVC range, VC class, or Ethernet subinterface.

pppoe limit per-mac

To specify the maximum number of PPPoE sessions to be sourced from a MAC address, use the **pppoe limit per-mac** command in VPDN configuration mode.

pppoe limit per-mac *number*

Syntax Description	<i>number</i>	Maximum number of PPPoE sessions that can be sourced from a MAC address.
--------------------	---------------	--

Defaults	100 sessions
----------	--------------

Command Modes	VPDN configuration
---------------	--------------------

Command History	Release	Modification
	12.1(1)T	This command was introduced.

Examples The following example sets a limit of 10 sessions to be sourced from a MAC address:

```
pppoe limit per-mac 10
```

Related Commands	Command	Description
	pppoe limit per-vc	Specifies the maximum number of PPPoE sessions to be established over a VC.
pppoe limit per-vlan	Specifies the maximum number of PPPoE sessions under each VLAN.	

pppoe limit per-vc

To specify the maximum number of PPPoE sessions to be established over a VC, use the **pppoe limit per-vc** command in VPDN configuration mode.

pppoe limit per-vc *number*

Syntax Description	<i>number</i>	Maximum number of PPPoE sessions that can be established over an ATM PVC.
---------------------------	---------------	---

Defaults	100 sessions
-----------------	--------------

Command Modes	VPDN configuration
----------------------	--------------------

Command History	Release	Modification
	12.1(1)T	This command was introduced.

Examples The following example sets a limit of 10 sessions to be established over a VC:

```
pppoe limit per-vc 10
```

Related Commands	Command	Description
	pppoe limit max-sessions	Specifies the maximum number of PPPoE sessions to be sourced from a MAC address.
	pppoe limit per-vlan	Specifies the maximum number of PPPoE sessions under each VLAN.

pppoe limit per-vlan

To specify the maximum number of PPP over Ethernet (PPPoE) sessions permitted under each virtual LAN (VLAN), use the **pppoe limit per-vlan** VPDN configuration command. To remove this specification, use the **no** form of this command.

pppoe limit per-vlan *number*

no pppoe limit per-vlan

Syntax Description	<i>number</i>	Maximum number of PPP over Ethernet sessions permitted under each VLAN.
--------------------	---------------	---

Defaults	100 PPPoE sessions per VLAN
----------	-----------------------------

Command Modes	VPDN configuration
---------------	--------------------

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines

If the **pppoe max-session** command is configured on a VLAN, that command will take precedence over the **pppoe limit per-vlan** command. The **pppoe limit per-vlan** command applies to all VLANs on which the **pppoe max-session** command has not been configured.

The **pppoe limit per-vlan** command must be configured after the accept dial-in VPDN group has been configured using the **accept-dialin** VPDN configuration command.

Examples

The following example shows a maximum of 200 PPPoE sessions configured for an 802.1Q VLAN subinterface:

```
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 pppoe enable
 !
 vpdn enable
 vpdn-group 1
 accept dialin
 protocol pppoe
 virtual-template 1
 pppoe limit per-vlan 200
```

Related Commands	Command	Description
	accept dial-in	Creates an accept dial-in VPDN subgroup.
	debug vpdn pppoe-data	Displays data packets of PPPoE sessions.

Command	Description
debug vpdn pppoe-error	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.
debug vpdn pppoe-events	Displays PPPoE protocol messages about events that are part of normal session establishment or shutdown.
debug vpdn pppoe-packet	Displays each PPPoE protocol packet exchanged.
pppoe enable	Enables PPPoE sessions on an Ethernet interface.
pppoe limit max-sessions	Specifies the maximum number of PPPoE sessions to be sourced from a MAC address.
pppoe limit per-vc	Specifies the maximum number of PPPoE sessions to be established over a VC.
pppoe max-sessions	Specifies the maximum number of PPPoE sessions permitted under a VLAN.

pppoe max-sessions

To specify the maximum number of PPP over Ethernet (PPPoE) sessions that will be permitted on an ATM permanent virtual circuit (PVC), PVC range, virtual circuit (VC) class, or Ethernet subinterface, use the **pppoe max-sessions** command in the appropriate mode. To remove this specification, use the **no** form of this command.

pppoe max-sessions *number-of-sessions*

no pppoe max-sessions

Syntax Description	<i>number-of-sessions</i>	Maximum number of PPPoE sessions that will be permitted.
	Note	The PPPoE session limit in the case of a PVC range applies to <i>each</i> PVC in the range. This limit is not cumulative on <i>all</i> PVCs belonging to the range.

Defaults Maximum number of sessions is not set.

Command Modes Ethernet subinterface configuration
Interface-ATM-VC configuration
VC-class configuration
ATM PVC range configuration
PVC-in-range configuration

Command History	Release	Modification
	12.1(5)T	This command was introduced.
	12.2(4)T	This command was modified to limit PPPoE sessions on ATM PVCs, PVC ranges, and VC classes.

Usage Guidelines PPPoE sessions can be limited in the following ways:

- The **pppoe limit max-sessions** command limits the total number of PPPoE sessions on the router, regardless of the type of medium the sessions are using.
- The **pppoe limit per-mac** command limits the number of PPPoE sessions that can be sourced from a single MAC address. This limit also applies to all PPPoE sessions on the router.
- The **pppoe limit per-vc** and **pppoe limit per-vlan** commands limit the number of PPPoE sessions on all PVCs or VLANs on the router. The **pppoe max-sessions** command limits the number of PPPoE sessions on a specific PVC or VLAN. Limits created for a specific PVC or VLAN using the **pppoe max-session** command take precedence over the global limits created with the **pppoe limit per-vc** and **pppoe limit per-vlan** commands.

PPPoE session limits created on an ATM PVC take precedence over limits created in a VC class or ATM PVC range.

PPPoE session limits created in an ATM PVC range take precedence over limits created in a VC class.

Examples**Ethernet Subinterface Example**

The following example shows a limit of 200 PPPoE sessions configured for the subinterface:

```
interface FastEthernet 0/0.10
 encapsulation dot1Q 10
 pppoe enable
 pppoe max-sessions 200
```

ATM PVC Example

The following example shows a limit of 10 PPPoE sessions configured for the PVC:

```
interface ATM1/0.102 multipoint
 pvc 3/304
 encapsulation aal5snap
 protocol pppoe
 pppoe max-sessions 10
```

VC Class Example

The following example shows a limit of 20 PPPoE sessions that will be permitted per PVC in the VC class called “main”:

```
vc-class atm main
 pppoe max-sessions 20
```

ATM PVC Range Example

The following example shows a limit of 30 PPPoE sessions that will be permitted per PVC in the PVC range called “range-1”:

```
interface atm 6/0.110 multipoint
 range range-1 pvc 100 4/199
 encapsulation aal5snap
 protocol ppp virtual-template 2
 pppoe max-sessions 30
```

Individual PVC Within a PVC Range Example

The following example shows a limit of 10 PPPoE sessions configured for “pvc1”, which is part of the ATM PVC range called “range1”:

```
interface atm 6/0.110 multipoint
 range range1 pvc 100 4/199
 pvc-in-range pvc1 3/104
 pppoe max-sessions 10
```

Related Commands

Command	Description
debug vpdn pppoe-errors	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.
pppoe limit max-sessions	Specifies the maximum number of PPPoE sessions that will be permitted on a router.
pppoe limit per-mac	Specifies the maximum number of PPPoE sessions to be sourced from a MAC address.
pppoe limit per-vc	Specifies the maximum number of PPPoE sessions permitted on all VCs.
pppoe limit per-vlan	Specifies the maximum number of PPPoE sessions permitted on a VLAN.

pppoe-client dial-pool-number

To configure a PPP over Ethernet (PPPoE) client and to specify dial-on-demand routing (DDR) functionality, use the **pppoe-client dial-pool-number** command in either interface configuration mode or ATM virtual circuit configuration mode. To disable any configured functionality, use the **no** form of this command.

pppoe-client dial-pool-number *number* [**dial-on-demand**]

no pppoe-client dial-pool-number *number* [**dial-on-demand**]

Syntax Description	<i>number</i>	Unique number of a dial group configured with the dialer-group dialer interface command.
dial-on-demand	(Optional)	Enables DDR functionality for the PPPoE connection.

Defaults A PPPoE client is not configured, and DDR functionality is disabled.

Command Modes Interface configuration
ATM virtual circuit configuration

Command History	Release	Modification
	12.1(3)XG	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
	12.2(13)T	The dial-on-demand keyword was added to allow the configuration of DDR interesting traffic control list functionality.

Usage Guidelines One PVC will support only one PPPoE client. Multiple PPPoE clients can run concurrently on different permanent virtual circuits (PVCs), but each PPPoE client must use a separate dialer interface and a separate dialer pool.

Use this command to configure dial-on-demand routing (DDR) interesting traffic control list functionality of the dialer interface with a PPP over Ethernet (PPPoE) client. When the DDR functionality is configured for this command, the following DDR commands must also be configured: **dialer-group**, **dialer hold-queue**, **dialer idle-timeout**, and **dialer-list**.

Tips for Configuring the Dialer Interface

If you are configuring a hard-coded IP address under the dialer interface, you can configure a default IP route using the **ip route** command as follows:

```
ip route 0.0.0.0 0.0.0.0 dialer1
```

But if you are configuring a negotiated IP address using the **ip address negotiated** command under the dialer interface, you must configure a default IP route using the **ip route** command as follows:

```
ip route 0.0.0.0 0.0.0.0 dialer1 permanent
```

The reason is that the dialer interface will lose its IP address when a PPPoE session is brought down (even if the dialer does not go down), and hence the route removal routine will take effect and remove all IP routes pointed at the dialer interface, even the default IP route. Although the default IP route will be added back about one minute later by IP background processes, you may risk losing incoming packets during the interval.

Examples

PPPoE Client DDR Idle-Timer on an Ethernet Interface

The following example shows how to configure the PPPoE client DDR idle-timer on an Ethernet interface and includes the required DDR commands:

```
!
vpdn enable
no vpdn logging
!
vpdn-group 1
 request-dialin
 protocol pppoe
!
interface Ethernet1
 pppoe enable
 pppoe-client dial-pool-number 1 dial-on-demand
!
interface Dialer1
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 180 either
 dialer hold-queue 100
 dialer-group 1
!
dialer-list 1 protocol ip permit
!
ip route 0.0.0.0 0.0.0.0 Dialer1
```

PPPoE client DDR Idle-Timer on an ATM PVC

The following example shows how to configure the PPPoE client DDR idle-timer on an ATM PVC interface and includes the required DDR commands:

```
!
vpdn enable
no vpdn logging
!
vpdn-group 1
 request-dialin
 protocol pppoe
!
interface ATM2/0
 pvc 2/100
 pppoe-client dial-pool-number 1 dial-on-demand
!
interface Dialer1
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 180 either
 dialer hold-queue 100
 dialer-group 1
!
```

```
dialer-list 1 protocol ip permit
!
ip route 0.0.0.0 0.0.0.0 Dialer1
```

Related Commands

Command	Description
debug vpdn pppoe-data	Displays PPPoE session data packets.
debug vpdn pppoe-errors	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be terminated.
debug vpdn pppoe-events	Displays PPPoE protocol messages about events that are part of normal session establishment or shutdown.
debug vpdn pppoe-packets	Displays each PPPoE protocol packet exchanged.
dialer-group	Controls access by configuring a virtual access interface to belong to a specific dialing group.
dialer hold-queue	Allows interesting outgoing packets to be queued until a modem connection is established.
dialer idle-timeout	Specifies the idle time before the line is disconnected.
dialer-list	Defines a DDR dialer list to control dialing by protocol or by a combination of protocol and an access list.

precedence (Frame Relay VC-bundle-member)

To configure the precedence levels for a Frame Relay permanent virtual circuit (PVC) bundle member, use the **precedence** command in Frame Relay VC-bundle-member configuration mode. To remove the precedence level configuration from the PVC, use the **no** form of this command.

precedence {*level* | **other**}

no precedence

Syntax Description		
	<i>level</i>	Specifies the precedence level or levels for this Frame Relay PVC bundle member. The range is from 0 to 7. A PVC bundle member can be configured with a single precedence level, multiple individual precedence levels, a range of precedence levels, multiple ranges of precedence levels, or a combination of individual levels and level ranges. Examples are as follows: <ul style="list-style-type: none"> • 0 • 0,2,3 • 0-2,4-5 • 0,1,2-4,7
	other	Specifies that this Frame Relay PVC bundle member will handle all of the remaining precedence levels that are not explicitly configured on any other bundle member PVCs.

Defaults Precedence levels are not configured.

Command Modes Frame Relay VC-bundle-member configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines Assignment of precedence levels to PVC bundle members allows you to create differentiated service because you can distribute the IP precedence levels over the various PVC bundle members. You can map a single precedence level or a range of levels to each discrete PVC in the bundle, thereby enabling PVCs in the bundle to carry packets marked with different precedence levels. Use the **precedence other** command to indicate that a PVC can carry traffic marked with precedence levels not specifically configured for other PVCs. Only one PVC in the bundle can be configured using the **precedence other** command.

This command is available only when the match type for the PVC bundle is set to precedence using the **match precedence** command in Frame Relay VC-bundle configuration mode.

You can overwrite the precedence level configuration on a PVC by reentering the **precedence** command with a new level value.

All precedence levels must be accounted for in the PVC bundle configuration, or the bundle will not come up. Note, however, that a PVC may be a bundle member but have no precedence level associated with it. As long as all valid precedence levels are handled by other PVCs in the bundle, the bundle can come up, but the PVC that has no precedence level configured will not participate in it.

A precedence level can be configured on one PVC bundle member per bundle. If you configure the same precedence level on more than one PVC within a bundle, the following error warning appears on the console:

```
%Overlapping precedence levels
```

When tag-switching is enabled on the interface by using the **tag-switching ip** command, MPLS and IP packets can flow across the interface, and PVC bundles that are configured for IP precedence mapping are converted to MPLS EXP mapping. The PVC bundle functionality remains the same with respect to priority levels, bumping, and so on, but the **match precedence** command is replaced by “match exp”, and each **precedence** command is replaced by the **exp** command. The result is that a bundle-member PVC previously configured to carry precedence level 1 IP traffic now carries EXP level 1 MPLS traffic.

When tag-switching is disabled, the **match precedence** and **match dscp** commands are restored, and the **exp** commands are replaced by **precedence** commands.

When tag-switching is enabled or disabled, PVC bundles configured for IP precedence mapping or MPLS EXP mapping will stay up, and traffic will be transmitted over the appropriate bundle-member PVCs.

Examples

The following example configures Frame Relay PVC bundle member 101 to carry traffic with IP precedence level 5:

```
frame-relay vc-bundle new-york
 match precedence
 pvc 101
 precedence 5
```

Related Commands

Command	Description
bump	Configures the bumping rules for a specific PVC member of a bundle.
class	Associates a map class with a specified DLCI.
dscp (Frame Relay VC-bundle-member)	Configures the DSCP value or values for a Frame Relay PVC bundle member.
exp	Configures MPLS EXP levels for a Frame Relay PVC bundle member.
match	Specifies which bits of the IP header to use for mapping packet service levels to Frame Relay PVC bundle members.
protect (Frame Relay VC-bundle-member)	Configures a Frame Relay PVC bundle member with protected group or protected PVC status.

protect (Frame Relay VC-bundle-member)

To configure a Frame Relay protected permanent virtual circuit (PVC) bundle member with protected group or protected PVC status, use the **protect** command in Frame Relay VC-bundle-member configuration mode. To remove the protected status from the PVC, use the **no** form of this command.

```
protect {group | vc}
```

```
no protect {group | vc}
```

Syntax Description	group	Configures the PVC bundle member as part of a collection of protected PVCs within the PVC bundle.
	vc	Configures the PVC member as individually protected.

Defaults The PVC neither belongs to the protected group nor is an individually protected PVC.

Command Modes Frame Relay VC-bundle-member configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines When an individually protected PVC goes down, it takes the bundle down. When all members of a protected group go down, the bundle goes down.

Despite any protection configurations, the PVC bundle will go down if a downed PVC has no PVC to which to bump its traffic or if the last PVC that is up in a PVC bundle goes down.

Examples The following example configures Frame Relay PVC bundle member 101 as an individually protected PVC:

```
frame-relay vc-bundle new york
pvc 101
protect vc
```

Related Commands	Command	Description
	bump	Configures the bumping rules for a specific PVC member of a bundle.
	bundle	Creates a bundle or modifies an existing bundle to enter bundle configuration mode.
	dscp (Frame Relay VC-bundle-member)	Configures the DSCP value or values for a Frame Relay PVC bundle member.

■ protect (Frame Relay VC-bundle-member)

Command	Description
exp	Configures MPLS EXP levels for a Frame Relay PVC bundle member.
precedence (Frame Relay VC-bundle-member)	Configures the precedence levels for a Frame Relay PVC bundle member.

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]
```

```
no protocol protocol [protocol-address [virtual-template] | inarp] [[no] broadcast]
```

Syntax Description	
<i>protocol</i>	Choose one of the following values: aarp —AppleTalk ARP appletalk —AppleTalk arp —IP ARP bridge —bridging bstun —block serial tunnel 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 decnet —DECnet decnet_node —DECnet node decnet_prime_router —DECnet prime router decnet_router-11 —DECnet router L1 decnet_router-12 —DECnet router L2 dlsw —data link switching ip —IP ipx —Novell IPX llc2 —llc2 pad —packet assembler/disassembler (PAD) links ppp —Point-to-Point Protocol carried on the VC pppoe —PPP over Ethernet qllc —Qualified Logical Link Control protocol rsrb —remote source-route bridging snapshot —snapshot routing support stun —serial tunnel
<i>protocol-address</i>	Destination address that is being mapped to a PVC.
virtual-template	(Optional) Specifies parameters that the point-to-point protocol over ATM (PPoA) sessions will use.
	Note This keyword is valid only for the ppp protocol.

inarp	(Valid only for IP and IPX protocols on PVCs) Enables Inverse ARP on an ATM PVC. If you specify a <i>protocol-address</i> instead of inarp , Inverse ARP is automatically disabled for that protocol.
[no] broadcast	(Optional) broadcast 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.

Defaults

Inverse ARP is enabled for IP and IPX if the protocol is running on the interface and no static map is configured.

Command Modes

Interface-ATM-VC configuration (for an ATM PVC or SVC)
 VC-class configuration (for a VC class)
 PVC range configuration (for an ATM PVC range)
 PVC-in-range configuration (for an individual PVC within a PVC range)

Command History

Release	Modification
11.3	This command was introduced.
12.1	The ppp and virtual-template keywords were added.
12.1(5)T	The ip and ipx options were made available in PVC range and PVC-in-range configuration modes.
12.2(13)T	The apollo , vines , and xns arguments were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems are no longer supported in the Cisco IOS software.

Usage Guidelines**Command Application**

Use this command to perform either of the following tasks:

- Configure a static map for an ATM PVC, SVC, or VC class.
- Enable Inverse ARP or Inverse ARP broadcasts on an ATM PVC or PVC range by configuring Inverse ARP directly on the PVC, in the PVC range, or in a VC class (applies to IP and IPX protocols only).

PVC range and PVC-in-range configuration modes support only the protocols that do not require static map configuration. Those protocol options are **ip** and **ipx**.

Default Configurations

If the **protocol** command is not explicitly configured on an ATM PVC or SVC, the VC inherits the following default configuration (listed in order of precedence):

- Configuration of the **protocol ip inarp** or **protocol ipx inarp** command in a VC class assigned to the PVC or SVC itself.
- Configuration of the **protocol ip inarp** or **protocol ipx inarp** command in a VC class assigned to the ATM subinterface of the PVC or SVC.

- Configuration of the **protocol ip inarp** or **protocol ipx inarp** command in a VC class assigned to the ATM main interface of the PVC or SVC.
- Global default: Inverse ARP is enabled for IP and IPX if the protocol is running on the interface and no static map is configured.

Examples

The following example creates a static map on a VC, indicates that 10.68.34.237 is connected to this VC, and sends ATM pseudobroadcasts:

```
protocol ip 10.68.34.237 broadcast
```

The following example enables Inverse ARP for IPX and does not send ATM pseudobroadcasts:

```
protocol ipx inarp no broadcast
```

The following example removes a static map from a VC and restores the default behavior for Inverse ARP (Refer to the “Default” section described above):

```
no protocol ip 10.68.34.237
```

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

```
protocol ppp 10.68.34.237 virtual-template
```

protocol pppoe (ATM VC)

To enable PPP over Ethernet (PPPoE) sessions to be established on permanent virtual circuits (PVCs), use the **protocol pppoe** command in the appropriate configuration mode. To disable PPPoE, use the **no** form of this command.

```
protocol pppoe [group group-name]
```

```
no protocol pppoe [group group-name]
```

Syntax Description

group	(Optional) Specifies a PPPoE profile to be used by PPPoE sessions on the interface.
<i>group-name</i>	(Optional) Name of the PPPoE profile to be used by PPPoE sessions on the interface.

Defaults

PPPoE is not enabled.

Command Modes

ATM VC configuration
 ATM VC class configuration
 ATM PVC range configuration
 ATM PVC-in-range configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

If a PPPoE profile is not specified by using the **group** option, PPPoE sessions will be established using values from the global PPPoE profile. PPPoE profiles must be configured using the **bba-group pppoe** command.

Examples

The following example shows PPPoE configured in virtual circuit (VC) class “class-pppoe-global” and on the range of PVCs from 100 to 109. PVCs that use VC class “class-pppoe-global” will establish PPPoE sessions using the parameters configured in the global PPPoE profile. PVCs in the PVC range will use PPPoE parameters defined in PPPoE profile “vpn1”.

```
bba-group pppoe global
  virtual-template 1
  sessions max limit 8000
  sessions per-vc limit 8
  sessions per-mac limit 2
!
bba-group pppoe vpn1
  virtual-template 1
  sessions per-vc limit 2
  sessions per-mac limit 1
!
```

```

vc-class atm class-pppoe-global
  protocol pppoe
  !
interface ATM1/0.10 multipoint
  range range-pppoe-1 pvc 100 109
  protocol pppoe group vpn1
  !
interface ATM1/0.20 multipoint
  class-int class-pppoe-global
  pvc 0/200
  !
  pvc 0/201
  !

```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
debug pppoe	Displays debugging information for PPPoE sessions.
sessions max limit	Configures a PPPoE global profile with the maximum number of PPPoE sessions permitted on a router and sets the PPPoE session-count threshold.
sessions per-mac limit	Sets the maximum number of PPPoE sessions allowed per MAC address in a PPPoE profile.
sessions per-vc limit	Sets the maximum number of PPPoE sessions to be established over a VC and sets the PPPoE session-count threshold.

pvc

To create or assign a name to an ATM permanent virtual circuit (PVC), to specify the encapsulation type on an ATM PVC, and to enter ATM virtual circuit configuration mode, use the **pvc** command in interface configuration or subinterface configuration mode. To remove an ATM PVC from an interface, use the **no** form of this command.

```
pvc [name] vpi/vci [ces | ilmi | qsaal | smds | l2transport]
```

```
no pvc [name] vpi/vci [ces | ilmi | qsaal | smds | l2transport]
```

Syntax Description	
<i>name</i>	(Optional) The name of the PVC or map. The name can be up to 15 characters long.
<i>vpi</i>	<p>ATM network virtual path identifier (VPI) for this PVC. The absence of the “/” and a <i>vpi</i> value causes the <i>vpi</i> value to default to 0.</p> <p>The range of valid values is 0 to 255 except for the following routers:</p> <ul style="list-style-type: none"> • Cisco 4500 and 4700 routers: 0 to 1 less than the quotient of 8192 divided by the value set by the atm vc-per-vp command • Cisco 2600 and 3600 series routers using Inverse Multiplexing for ATM (IMA): 0 to 15, 64 to 79, 128 to 143, and 192 to 207 <p>A value that is out of range is interpreted as a string and is treated as the connection ID. The arguments <i>vpi</i> and <i>vci</i> cannot both be set to 0; if one is 0, the other cannot be 0.</p>
<i>vci</i>	<p>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, lower values from 0 to 31 are reserved for specific traffic (for example, F4 OAM, SVC signaling, ILMI, and so on) and should not be used.</p> <p>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.</p> <p>A value that is out of range causes an “unrecognized command” error message.</p> <p>The arguments <i>vpi</i> and <i>vci</i> cannot both be set to 0; if one is 0, the other cannot be 0.</p>
ces	(Optional) Circuit Emulation Service encapsulation. This keyword is available on the OC-3/STM-1 ATM Circuit Emulation Service network module only.
ilmi	(Optional) Used to set up communication with the Interim Local Management Interface (ILMI); the associated <i>vpi</i> and <i>vci</i> values ordinarily are 0 and 16, respectively.

qsaal	(Optional) A signaling-type PVC used for setting up or tearing down SVCs; the associated <i>vpi</i> and <i>vci</i> values ordinarily are 0 and 5, respectively.
smds	(Optional) Encapsulation for SMDS networks. If you are configuring an ATM PVC on the ATM Interface Processor (AIP), you must configure AAL3/4SMDS using the atm aal aal3/4 command before specifying smds encapsulation. If you are configuring an ATM network processor module (NPM), the atm aal aal3/4 command is not required. SMDS encapsulation is not supported on the ATM port adapter.
l2transport	(Optional) Used to specify that the PVC is switched and not terminated.

Defaults

No PVC is defined. When a PVC is defined, the global default of the **encapsulation** command applies (**aal5snap**).

Command Modes

Interface configuration
Subinterface configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.1(2)T	The ranges for the VPI were increased for Cisco 2600 and Cisco 3600 series routers using Inverse Multiplexing for ATM (IMA). The ces keyword was added for configuring CES encapsulation when using the OC-3/STM-1 ATM Circuit Emulation Service network module on Cisco 2600 and Cisco 3600 series routers.
12.1(5)XM	This command was extended to the merged Simple Gateway Control Protocol (SGCP)/Media Gateway Control Protocol (MGCP) software.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.0(23)S	The l2transport keyword was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines**Creating and Configuring PVCs**

The **pvc** command replaces the **atm pvc** command. Use the **pvc** command to configure a single ATM VC only, not a VC that is a bundle member. We recommend that you use the **pvc** command in conjunction with the **encapsulation** and **random-detect attach** commands instead of the **atm pvc** command.

The **pvc** command creates a PVC and attaches it to the VPI and VCI specified. Both the *vpi* and *vci* arguments cannot be simultaneously specified as 0; if one is 0, the other cannot be 0.

When configuring an SVC, use the **pvc** command to configure the PVC that handles SVC call setup and termination. In this case, specify the **qsaal** keyword. See the second example that follows.

ATM PVC Names

Once you specify a name for a PVC, you can reenter ATM virtual circuit configuration mode by simply entering the **pvc name** command. You can remove a PVC and any associated parameters by entering **no pvc name** or **no pvc vpi/vci**.



Note

After configuring the parameters for an ATM PVC, you must exit the ATM virtual circuit configuration mode in order to create the PVC and enable the settings.

Encapsulation Types on ATM PVCs

Specify CES, ILMI, QSAAL, or SMDS as the encapsulation type on an ATM PVC. (To configure other encapsulations types, see the **encapsulation** command.)

Configuring CES encapsulation on a PVC is equivalent to creating a constant bit rate (CBR) class of service.

Rate Queues

The Cisco IOS software dynamically creates rate queues as necessary to satisfy the requests of the **pvc** commands.

Default Configurations

If **ilmi**, **qsaal**, or **smds** encapsulation is not explicitly configured on the ATM PVC, the PVC inherits the following default configuration (listed in order of precedence):

- Configuration of the **encapsulation** command in a VC class assigned to the PVC itself.
- Configuration of the **encapsulation** command in a VC class assigned to the ATM subinterface of the PVC.
- Configuration of the **encapsulation** command in a VC class assigned to the ATM main interface of the PVC.
- Global default: The global default value of the **encapsulation** command applies (**aal5snap**).

Examples

The following example creates a PVC with VPI 0 and VCI 16, and communication is set up with the ILMI:

```
pvc cisco 0/16 ilmi
exit
```

The following example creates a PVC used for ATM signaling for an SVC. It specifies VPI 0 and VCI 5:

```
pvc cisco 0/5 qsaal
exit
```

The following example configures the PVC called “cisco” to use class-based weighted fair queueing (CBWFQ). It attaches a policy map called “policy1” to the PVC. The classes that make up “policy1” determine the service policy for the PVC:

```
pvc cisco 0/5
service-policy output policy1
vbr-nrt 2000 2000
encap aal5snap
```

Related Commands	Command	Description
	atm vc-per-vp	Sets the maximum number of VCIs to support per VPI.
	pvc-bundle	Adds a PVC to a bundle as a member of the bundle.

pvc (Frame Relay VC-bundle)

To create a permanent virtual circuit (PVC) that is a Frame Relay PVC bundle member, and to enter Frame Relay VC-bundle-member configuration mode, use the **pvc** command in Frame Relay VC-bundle configuration mode. To delete the PVC from the Frame Relay PVC bundle, use the **no** form of this command.

```
pvc dcli [vc-name]
```

```
no pvc dcli [vc-name]
```

Syntax Description		
	<i>dcli</i>	Data-link connection identifier (DLCI) number used to identify the PVC.
	<i>vc-name</i>	(Optional) An alphanumeric name for the PVC.

Defaults	
	No PVC is defined.

Command Modes	
	Frame Relay VC-bundle configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines	
	To use this command, you must first create a Frame Relay PVC bundle and enter Frame Relay VC-bundle configuration mode.
	A PVC bundle must have at least one PVC for the bundle to come up. A PVC bundle cannot have more than eight PVCs. If you try to configure more than eight PVCs in a bundle, the following message will appear on the console:

```
%FR vc-bundle contains 8 members. Cannot add another.
```

Dynamic PVCs can be specified as PVC bundle members; however, if a PVC has already been created by using some other configuration command, you will not be able to add it to a PVC bundle. If you try to add it to a bundle, the following message will appear on the console:

```
%DLCI 200 is not a dynamic PVC. Cannot add to VC-Bundle.
```

If a PVC is already a member of a PVC bundle, any attempt to reuse that same PVC in a command that creates a PVC (e.g. **frame-relay interface-dcli**, **frame-relay local-dcli**) will result in the following error message:

```
%Command is inapplicable to vc-bundle PVCs.
```

Examples	
	The following example creates PVC 101 belonging to the Frame Relay PVC bundle named "new_york":

```
frame-relay vc-bundle new_york
pvc 101
```

Related Commands	Command	Description
	dscp (frame-relay vc-bundle-member)	Configures the DSCP value or values for a Frame Relay PVC bundle member.
	exp	Configures MPLS EXP levels for a Frame Relay PVC bundle member.
	frame-relay vc-bundle	Creates a Frame Relay PVC bundle and enters Frame Relay VC-bundle configuration mode.
	match	Specifies which bits of the IP header to use for mapping packet service levels to Frame Relay PVC bundle members
	precedence (Frame Relay VC-bundle-member)	Configures the precedence levels for a Frame Relay PVC bundle member.

pvc-in-range

To configure an individual permanent virtual circuit (PVC) within a PVC range, use the **pvc-in-range** PVC range configuration command. To delete the individual PVC configuration, use the **no** form of this command.

```
pvc-in-range [pvc-name] [vpi/vci]
```

```
no pvc-in-range [pvc-name] [vpi/vci]
```

Syntax Description

<i>pvc-name</i>	(Optional) Name given to the PVC. The PVC name can have a maximum of 15 characters.
<i>vpi</i>	(Optional) ATM network virtual path identifier (VPI) for this PVC. In the absence of the “/” and a <i>vpi</i> value, the <i>vpi</i> value defaults to 0. The <i>vpi</i> value ranges from 0 to 255.
<i>vci</i>	(Optional) ATM network virtual channel identifier (VCI) for this PVC. The <i>vci</i> value ranges from 32 to 2047.

Defaults

No default behavior or values.

Command Modes

PVC range configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

The **pvc-in-range** command defines an individual PVC within a PVC range and enables PVC-in-range configuration mode.

Examples

In the following example, a PVC called “pppoa” is deactivated. The PVC “pppoa” is an individual PVC within a configured PVC range.

```
pvc-in-range pppoa 0/130
shutdown
```

Related Commands

Command	Description
range pvc	Defines a range of ATM PVCs.

range pvc

To define a range of ATM permanent virtual circuits (PVCs), use the **range pvc** command in subinterface configuration mode. To delete the range of ATM PVCs, use the **no** form of this command.

```
range [range-name] pvc start-vpilstart-vci end-vpilend-vci
```

```
no range [range-name] pvc
```

Syntax Description

<i>range-name</i>	(Optional) Name of the range. The range name can be a maximum of 15 characters.
<i>start-vpil</i>	Beginning value for a range of virtual path identifiers (VPIs). In the absence of the “/” and a <i>vpi</i> value, the <i>vpi</i> value defaults to 0. The <i>vpi</i> value ranges from 0 to 255.
<i>start-vcil</i>	Beginning value for a range of virtual channel identifiers (VCIs). The <i>vci</i> value ranges from 32 to 65535.
<i>end-vpil</i>	End value for a range of virtual path identifiers (VPIs). In the absence of an <i>end-vpi</i> value, the <i>end-vpi</i> value defaults to the <i>start-vpi</i> value. The <i>vpi</i> value ranges from 0 to 255.
<i>end-vci</i>	End value for a range of virtual channel identifiers (VCIs). The <i>vci</i> value ranges from 32 to 65535.

Defaults

An ATM PVC range is not configured.

Command Modes

Subinterface configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

The **range pvc** command defines a range of PVCs and enables PVC range configuration mode.

The number of PVCs in a range can be calculated using the following formula:

$$\text{number of PVCs} = (\text{end-vpi} - \text{start-vpi} + 1) \times (\text{end-vci} - \text{start-vci} + 1).$$

The *start-vpi* argument may be omitted if it is zero. The *end-vpi* argument may be omitted, but if it is omitted, it is assigned the value of *start-vpi*. The *end-vpi* and *end-vci* arguments are always greater than or equal to *start-vpi* and *start-vci* respectively.

When applied to multipoint subinterfaces, the **range pvc** command creates a range of ATM PVCs. When applied to point-to-point subinterfaces, the **range pvc** command creates range of PVCs and a corresponding range of point-to-point subinterfaces.

For point-to-point subinterfaces, subinterface numbering begins with the subinterface on which the PVC range is configured and increases sequentially through the range.

Examples**ATM PVC Range Example**

In the following example, 100 PVCs with VCI values from 100 to 199 for each VPI value from 0 to 4 are created for a PVC range called “range-pppoa-1”. This configuration creates a total of 500 PVCs in the range. PVC parameters are then configured for the range.

```
interface atm 6/0.110 multipoint
range range-pppoa-1 pvc 100 4/199
class-range class-pppoa-1
ubr 1000
encapsulation aal5snap
protocol ppp virtual-Template 2
```

Subinterface Grouping by PVC Range for Routed Bridge Encapsulation Example

In the following example, a PVC range called “range1” is created with a total of 100 PVCs in the range. A point-to-point subinterface will be created for each PVC in the range. ATM routed bridge encapsulation is also configured.

```
interface atm 6/0.200 point-to-point
ip unnumbered loopback 1
atm route-bridged ip
range range1 pvc 1/200 1/299
# end
```

Related Commands

Command	Description
pvc-in-range	Configures an individual PVC within a PVC range.

rbe nasip

To specify the IP address of an interface on the Dynamic Host Configuration Protocol (DHCP) relay agent that will be sent to the DHCP server via the agent remote ID option, use the **rbe nasip** command in global configuration mode. To remove this specification, use the **no** form of this command.

rbe nasip *source-interface*

no rbe nasip *source-interface*

Syntax Description	<i>source-interface</i>	The type and number of one of the interfaces on the router. The IP address for this interface will be forwarded in the agent remote ID option and can be used by the DHCP server to uniquely identify the DHCP relay agent.
---------------------------	-------------------------	---

Defaults	No IP address is specified.
-----------------	-----------------------------

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

Command History	Release	Modification
	12.2(2)T	This command was introduced.

Usage Guidelines	<p>The rbe nasip command is used to configure support for the DHCP relay agent information option (option 82) for ATM routed bridge encapsulation (RBE).</p> <p>Support for the DHCP relay agent information option must be configured on the DHCP relay agent using the ip dhcp relay information option command in order for the rbe nasip command to be effective.</p>
-------------------------	--

Examples	<p>In the following example, support for DHCP option 82 is enabled on the DHCP relay agent by the use of the ip dhcp relay agent information option command. The rbe nasip command configures the router to forward the IP address for Loopback0 to the DHCP server. ATM routed bridge encapsulation is configured on ATM subinterface 4/0.1.</p>
-----------------	---

```
ip dhcp-server 10.1.1.1
!
ip dhcp relay information option
!
interface Loopback0
 ip address 10.5.1.1 255.255.255.0
!
interface ATM4/0
 no ip address
!
interface ATM4/0.1 point-to-point
 ip unnumbered Loopback0
 ip helper-address 10.1.1.1
 atm route-bridged ip
 pvc 88/800
```

```
    encapsulation aal5snap
!
router eigrp 100
  network 10.0.0.0
!
rbe nasip loopback0
```

Related Commands

Command	Description
ip dhcp relay information option	Enables the system to insert the DHCP relay agent information option in forwarded BOOT REQUEST messages to a Cisco IOS DHCP server.

redirect captivate advertising default group

To configure the default captive portal group, duration, and frequency for advertising captivation, use the **redirect captivate advertising default group** command in SSG-redirect configuration mode. To deselect a captive portal group as the default for advertising captivation, use the **no** form of this command.

redirect captivate advertising default group *group-name* **duration** *seconds* **frequency** *frequency*

no redirect captivate advertising default group *group-name* **duration** *seconds* **frequency** *frequency*

Syntax Description

<i>group-name</i>	Name of the captive portal group.
duration <i>seconds</i>	The duration in seconds of the advertising captivation. The valid range is from 1 to 65536 seconds.
frequency <i>frequency</i>	The frequency in seconds at which TCP packets are redirected to the captive portal group. The valid range is from 1 to 65536 seconds.

Defaults

No default behavior or values

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use this command to select the default captive portal group for advertising captivation of users upon Account Logon. Use the *seconds* argument to configure the duration, in seconds, of the advertising captivation. Any packets arriving from the user and marked for one of the TCP ports configured in the captive portal group *group-name* are redirected to one of the captive portals defined in that captive portal group for the duration configured by the *seconds* argument.

Use the *frequency* argument to configure how often Service Selection Gateway (SSG) attempts to forward packets from the user to the captive portal.

The parameters set by this command can be overridden by the RADIUS attributes set for a user.

Examples

The following example shows how to configure the captive portal group named “CaptivateServer” to forward packets from a user for 30 seconds at intervals of 3600 seconds:

```
server-group SSD
 server 10.0.0.253 8080
 !
 redirect port-list WebPorts to SSD
 !
```

■ redirect captive advertising default group

```

redirect unauthenticated-user to RedirectServer
redirect unauthorized-service to SSD
redirect smtp group SMTPServer all
redirect captive initial default group CaptivateServer duration 10
redirect captive advertising default group CaptivateServer duration 30 frequency 3600

```

Related Commands

Command	Description
redirect captive initial default group	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
redirect smtp group	Selects a captive portal group for redirection of SMTP traffic.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
redirect unauthenticated-user to	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect captive initial default group

To select a default captive portal group and duration of the initial captivation of users on Account Logon, use the **redirect captive initial default group** command in SSG-redirect configuration mode. To deselect a captive portal group as the default for initial captivation, use the **no** form of this command.

redirect captive initial default group *group-name* **duration** *seconds*

no redirect captive initial default group *group-name* **duration** *seconds*

Syntax Description		
	<i>group-name</i>	Name of the captive portal group.
	duration <i>seconds</i>	Duration in seconds of the initial captivation. The valid range is from 1 to 65536 seconds.

Defaults No default behavior or values

Command Modes SSG-redirect configuration

Command History	Release	Modification
	12.2(4)B	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines Use this command to select the default captive portal group for initial captivation of users on Account Logon. Use the *seconds* argument to configure the duration, in seconds, of the initial captivation. Any packets arriving from the user and marked for one of the TCP ports configured in the captive portal group *group-name* are redirected to one of the captive portals defined in that captive portal group for the duration configured by the *seconds* argument.

The parameters set by this command can be overridden by the RADIUS attributes set for a user.

Examples The following example shows that the captive portal group named “CaptiveServer” will be used to forward packets from a user for the first 10 seconds that the user is connected:

```
server-group SSD
server 10.0.0.253 8080
!
redirect port-list WebPorts to SSD
!
redirect unauthenticated-user to RedirectServer
redirect unauthorized-service to SSD
redirect smtp group SMTPServer all
redirect captive initial default group CaptivateServer duration 10
redirect captive advertising default group CaptivateServer duration 30 frequency 3600
```

Related Commands	Command	Description
	redirect captive advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
	redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
	redirect smtp group	Selects a captive portal group for redirection of SMTP traffic.
	redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
	redirect unauthenticated-user to	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
	show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
	show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
	ssg enable	Enables SSG.
	ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect to

To configure a TCP port or named TCP port list for Service Selection Gateway (SSG) TCP Redirect for Services, use the **redirect to** command in SSG-redirect configuration mode. To disable SSG TCP Redirect for Services on a TCP port or named TCP port list, use the **no** form of this command.

redirect {**port-list** *port-listname* | **port** *port-number*} **to** *group-name*

no redirect {**port-list** *port-listname* | **port** *port-number*} **to** *group-name*

Syntax Description

port-list	Specifies the named TCP port list to mark for SSG TCP redirection.
<i>port-listname</i>	Specifies the name of the named TCP port list.
port	Specifies a TCP port to mark for SSG TCP redirection.
<i>port-number</i>	Specifies the incoming destination port number of the TCP port to mark for SSG TCP redirection.
<i>group-name</i>	Defines the name of the captive portal group to redirect packets to that are marked for a destination port or named TCP port list.

Defaults

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use this command to mark a TCP port or a named TCP port list for SSG TCP Redirect for Services. Define a named TCP port list using the **port-list** command and add TCP ports to the named TCP port list using the **port** (ssg-redirect) command. Packets arriving from an authorized user, or from an authorized user attempting to access an unauthorized service at a marked TCP port or named TCP port list can be redirected to a captive portal group that presents the user with an appropriate response, such as a logon screen.



Note

You can associate only one port or port list with a portal group.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a TCP port or named TCP port list for SSG TCP redirection.



Note

This command replaces the **ssg http-redirect port group** command.

Examples

The following example marks TCP port 8080 for SSG TCP redirection. Packets with a destination port of 8080 are redirected to the captive portal group named “RedirectServer”:

```
server-group RedirectServer
  server 10.2.36.253 8080
!
  redirect port 8080 to RedirectServer
  redirect unauthorized-service destination network-list RedirectNw to RedirectServer
```

The following example marks the named TCP port “WebPorts” for SSG TCP redirection. Packets with a destination port that is one of the ports in the port list “WebPorts” are redirected to the captive portal group named “RedirectServer”:

```
server-group SSD
  server 10.0.0.253 8080
!
  redirect port-list WebPorts to RedirectServer
!
```

Related Commands

Command	Description
port (ssg-redirect)	Adds a TCP port to a named port list.
port-list	Defines a list of one or more TCP ports that make up a named port list and enters SSG-redirect-port configuration mode.
redirect captivate advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captivate initial default group	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
server (SSG)	Adds a server to a captive portal group.
server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect smtp group

To select a captive portal group for redirection of Simple Mail Transfer Protocol (SMTP) traffic, use the **redirect smtp group** command in SSG-redirect configuration mode. To stop redirecting SMTP traffic to a captive portal group, use the **no** form of this command.

```
redirect smtp group group-name [all | user]
```

```
no redirect smtp group group-name [all | user]
```

Syntax Description	
<i>group-name</i>	Name of the captive portal group.
all	(Optional) Any SMTP packets are forwarded.
user	(Optional) SMTP packets from users that have SMTP forwarding permission are forwarded.

Defaults	
all	

Command Modes	
SSG-redirect configuration	

Command History	Release	Modification
	12.2(4)B	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines	
Use this command to select a captive portal group for redirection of SMTP traffic. If you select the all keyword, all SMTP packets (TCP port 25) from authorized users are redirected to one of the servers in the captive portal group specified by the <i>group-name</i> argument. If you select the user keyword, only SMTP packets from authorized users that have SMTP forwarding permission set through a RADIUS attribute are redirected. If you do not select a keyword, the default is the all keyword.	

Examples	
The following example shows how to configure all SMTP packets from authorized users to be redirected to the captive portal group named "SMTPServer":	

```
server-group SSD
server 10.0.0.253 8080
!
redirect port-list WebPorts to SSD
!
redirect unauthenticated-user to RedirectServer
redirect unauthorized-service to SSD
redirect smtp group SMTPServer all
redirect captivate initial default group CaptivateServer duration 10
redirect captivate advertising default group CaptivateServer duration 30 frequency 3600
```

The following example shows how to configure SMTP packets from any authorized user with the SMTP forwarding permission set through a RADIUS attribute to be redirected to the captive portal group named “SMTPServer”:

```
redirect smtp group SMTPServer user
```

Related Commands	Command	Description
	redirect captivate advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
	redirect captivate initial default group	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
	redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
	redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
	redirect unauthenticated-user to	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
	show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
	show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
	ssg enable	Enables SSG.
	ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect unauthenticated-user to

To redirect TCP traffic from unauthenticated users to a specified captive portal group, use the **redirect unauthenticated-user to** command in Service Selection Gateway SSG-redirect configuration mode. To stop redirecting traffic from unauthenticated users to the specified captive portal group, use the **no** form of this command.

redirect unauthenticated-user to *group-name*

no redirect unauthenticated-user to *group-name*

Syntax Description	<i>group-name</i>	The name of the captive portal group.
---------------------------	-------------------	---------------------------------------

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	SSG-redirect configuration
----------------------	----------------------------

Command History	Release	Modification
	12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.	

Usage Guidelines	Use this command to redirect traffic from unauthenticated users to a specified captive portal group.
-------------------------	--



Note

This command replaces the **ssg http-redirect unauthorized-user group** command.

Examples	The following example sets redirection of traffic from unauthenticated users to the captive portal group named "RedirectServer":
-----------------	--

```
server-group SSD
  server 10.0.0.253 8080
!
  redirect port-list WebPorts to SSD
!
  redirect unauthenticated-user to RedirectServer
  redirect unauthorized-service to SSD
  redirect smtp group SMTPServer all
  redirect captivate initial default group CaptivateServer duration 10
  redirect captivate advertising default group CaptivateServer duration 30 frequency 3600
```

Related Commands	Command	Description
	redirect captivate advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
	redirect captivate initial default group	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
	redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
	redirect smtp group	Selects a captive portal group for redirection of SMTP traffic.
	redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
	show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
	show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
	ssg enable	Enables SSG.
	ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect unauthorized-service to

To set a list of destination IP networks that can be redirected by a specified, named captive portal group, use the **redirect unauthorized-service to** command in SSG-redirect configuration mode. To remove the list of IP networks that can be redirected by a specified named captive portal group, use the **no** form of this command.

redirect unauthorized-service [**destination network-list** *network-listname*] **to** *group-name*

no redirect unauthorized-service [**destination network-list** *network-listname*] **to** *group-name*

Syntax Description	destination network list	(Optional) Checks incoming packets from authenticated hosts to networks that they are not authorized to access to determine if they need redirection.
	<i>network-listname</i>	(Optional) Name of the list of destination IP networks.
	<i>group-name</i>	Name of the captive portal group.

Defaults No default behavior or values.

Command Modes SSG-redirect configuration

Command History	Release	Modification
	12.2(4)B	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines Use this command to set a list of destination IP networks that can be redirected by the named captive portal group specified by the *group-name* argument. Incoming packets from authenticated hosts to networks that they are not authorized to access are checked against the destination IP network list to determine if they need redirection. If you do not specify a destination IP network by configuring the optional **destination network-list** keywords, the captive portal group specified in the *group-name* argument is used as the default group for unauthorized service redirection when the IP address of the unauthorized packet does not fall into any network list associated with any captive portal group.

You can associate only one destination IP network list with a captive portal group. You can associate a destination IP network list with multiple captive portal groups.

When you associate a destination IP network list with a captive portal group, packets arriving marked with a destination IP network that matches an IP network list may be redirected via SSG TCP redirection. The incoming destination TCP port also determines whether a packet is a candidate for SSG TCP redirection.

You can associate different server groups with overlapping IP network addresses. You must configure the captive portal group associated with a more specific network group first. For example, you must configure

```
redirect 10.1.0.0/255.255.0.0 to IPTVGroup
```

before you can configure

```
redirect 10.0.0.0/255.0.0.0 to ISPGroup
```

Examples

The following example shows how to set the captive portal group called “RedirectServer” as a possible candidate for redirection when the destination of a packet matches one of the networks in the destination IP network list named “RedirectNW”:

```
server-group RedirectServer
  server 10.2.36.253 8080
!
redirect port 80 to RedirectServer
redirect unauthorized-service destination network-list RedirectNw to RedirectServer
```

The following example shows how to set the captive portal group called “DefaultRedirectServer” as a possible candidate for redirection when the destination of a packet does not match any of the networks defined in any destination IP network list:

```
redirect unauthorized-service to DefaultRedirectServer
```

Related Commands

Command	Description
redirect captive advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captive initial default group	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
redirect smtp group	Selects a captive portal group for redirection of SMTP traffic.
redirect unauthenticated-user to	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

retry (SVC)

To configure a router to periodically attempt to bring up an active SVC connection after the initial call setup failed, use the **retry** interface-CES-VC command. To disable the retry mechanism, use the **no** form of this command.

```
retry timeout_value [retry_limit] [first_retry_interval]
```

```
no retry
```

Syntax Description		
<i>timeout_value</i>		Number of seconds between attempts to bring up the connection. The range is from 1 to 86400 seconds.
<i>retry_limit</i>		(Optional) Number of attempts the router will make to bring up the connection. The range is from 0 to 65535. The default value of 0 indicates no limit.
<i>first_retry_interval</i>		(Optional) Number of seconds the router will wait after the first call attempt failed before trying the call again. The default is 10 seconds.

Defaults

There is no default *timeout_value*.

The default *retry_limit* is 0.

The default *first_retry_interval* argument is 10 seconds.

Command Modes

Interface-CES-VC configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

This command is used on Cisco 2600 series and 3600 series routers that have OC-3/STM-1 ATM CES network modules.

The **retry** command applies only to active SVCs.

Examples

In the following example, the router is configured to make up to 20 attempts to bring up a connection on SVC "ces1". The interval between attempts is set at 10 seconds.

```
interface atm 1/0
  svc ces1 nsap 47.0091.81.000000.0040.0B0A.2501.ABC1.3333.3333.05 ces
  retry 10 20
```

Related Commands	Command	Description
	ces	Configures CES on a router port and enters CES configuration mode.
	svc	Creates an ATM SVC and specifies the destination NSAP address on a main interface or subinterface.