



# Frame Relay Queueing and Fragmentation at the Interface

---

## Feature History

Release	Modification
12.2(14)S	This feature was introduced.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T

This document describes the Frame Relay Queueing and Fragmentation at the Interface feature in Cisco IOS Release 12.2(13)T and includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Prerequisites, page 5](#)
- [Configuration Tasks, page 5](#)
- [Monitoring and Maintaining Frame Relay Queueing and Fragmentation at the Interface, page 11](#)
- [Configuration Examples, page 11](#)
- [Command Reference, page 12](#)

## Feature Overview

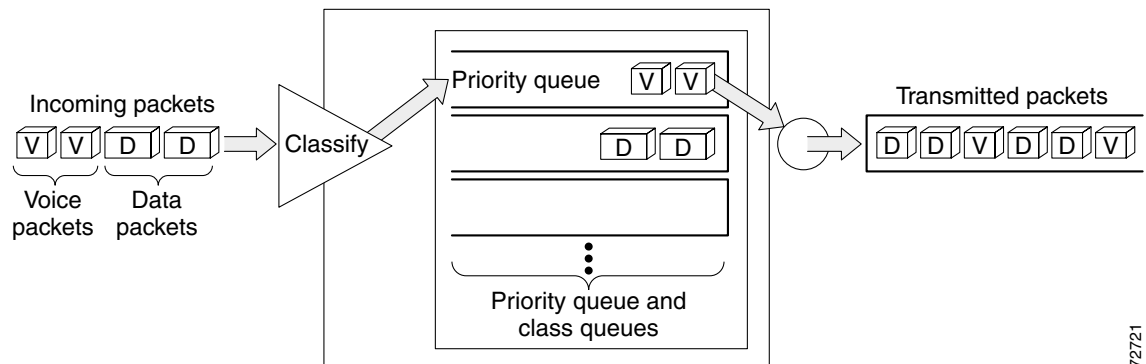
The Frame Relay Queueing and Fragmentation at the Interface feature introduces support for low-latency queueing (LLQ) and FRF.12 end-to-end fragmentation on a Frame Relay interface. This new feature simplifies the configuration of low-latency, low-jitter quality of service (QoS) by enabling the queueing policy and fragmentation configured on the main interface to apply to all permanent virtual circuits (PVCs) and subinterfaces under that interface. Before the introduction of this feature, queueing and fragmentation had to be configured on each individual PVC. Subrate shaping can also be configured on the interface.

## How Frame Relay Queueing and Fragmentation at the Interface Works

When FRF.12 end-to-end fragmentation is enabled on an interface, all PVCs on the main interface and its subinterfaces will have fragmentation enabled with the same configured fragment size. To maintain low latency and low jitter for high-priority traffic, the configured fragment size must be greater than the largest high-priority frames. This configuration will prevent high-priority traffic from being fragmented and queued behind lower-priority fragmented frames. If the size of a high-priority frame is larger than the configured fragment size, the high-priority frame will be fragmented. Local Management Interface (LMI) traffic will not be fragmented and is guaranteed its required bandwidth.

When a low-latency queueing policy map is applied to the interface, traffic through the interface is identified using class maps and is directed to the appropriate queue. Time-sensitive traffic such as voice should be classified as high priority and will be queued on the priority queue. Traffic that does not fall into one of the defined classes will be queued on the class-default queue. Frames from the priority queue and class queues are subject to fragmentation and interleaving. As long as the configured fragment size is larger than the high-priority frames, the priority queue traffic will not be fragmented and will be interleaved with fragmented frames from other class queues. This approach provides the highest QoS transmission for priority queue traffic. [Figure 1](#) illustrates the interface queueing and fragmentation process.

**Figure 1** Frame Relay Queueing and Fragmentation at the Interface



Subrate shaping can also be applied to the interface, but interleaving of high-priority frames will not work when shaping is configured. If shaping is not configured, each PVC will be allowed to send bursts of traffic up to the physical line rate.

When shaping is configured and traffic exceeds the rate at which the shaper can send frames, the traffic is queued at the shaping layer using fair queueing. After a frame passes through the shaper, the frame is queued at the interface using whatever queueing method is configured. If shaping is not configured, then queueing occurs only at the interface.



**Note**

For interleaving to work, both fragmentation and the low-latency queueing policy must be configured with shaping disabled.

The Frame Relay Queueing and Fragmentation at the Interface feature supports the following functionality:

- Voice over Frame Relay
- Weighted Random Early Detection

- Frame Relay payload compression



**Note** When payload compression and Frame Relay fragmentation are used at the same time, payload compression is always performed before fragmentation.

- IP header compression

## Benefits

### Simple Configuration

The Frame Relay Queueing and Fragmentation at the Interface feature allows fragmentation, low-latency queueing, and subrate shaping to be configured on a Frame Relay interface queue. The fragmentation and queueing and shaping policy will apply to all PVCs and subinterfaces under the main interface, eliminating the need to configure QoS on each PVC individually.

### Flexible Bandwidth

This feature allows PVCs to preserve the logical separation of traffic from different services while reducing bandwidth partitioning between PVCs. Each PVC can send bursts of traffic up to the interface shaping rate or, if shaping is not configured, the physical interface line rate.

## Restrictions

- Interface fragmentation and Frame Relay traffic shaping cannot be configured at the same time.
- Interface fragmentation and class-based fragmentation cannot be configured at the same time.
- Frame Relay switched virtual circuits (SVCs) are not supported.
- Hierarchical shaping and multiple shapers are not supported.

## Related Documents

For more information about shaping and low-latency queueing for Frame Relay, refer to the following documents:

- *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2
- *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.2
- *Low Latency Queueing for Frame Relay*, Cisco IOS Release 12.1(2)T feature module

For more information about Frame Relay fragmentation, refer to the following documents:

- *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2
- *Cisco IOS Wide-Area Networking Command Reference*, Release 12.2

## Supported Platforms

- Cisco 800 series
- Cisco 1400 series

- Cisco 1600 series
- Cisco 2500 series
- Cisco 2600 series
- Cisco 3600 series
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series
- Cisco AS5300 series
- Cisco AS5400
- Cisco AS5800
- Cisco MC3810
- Cisco ubr7200 series

### Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

### Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

## Supported Standards, MIBs, and RFCs

### Standards

FRF.12, *Frame Relay Fragmentation Implementation Agreement*, December 1997

**MIBs**

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

**RFCs**

No new or modified RFCs are supported by this feature.

## Prerequisites

The tasks in this document assume that you know how to configure low-latency queueing and shaping service policies.

The following prerequisites are specific to the Cisco 7500 series:

- The Frame Relay Queueing and Fragmentation at the Interface feature is supported on VIP-based interfaces with VIP2-50 or higher.
- Distributed Cisco Express Forwarding (dCEF) must be enabled both globally and on the Frame Relay interface.

## Configuration Tasks

See the following sections for configuration tasks for the Frame Relay Queueing and Fragmentation at the Interface feature. Each task in the list is identified as either required or optional.

- [Configuring Class Policy for the Priority Queue](#) (required)
- [Configuring Class Policy for the Bandwidth Queues](#) (optional)
- [Configuring the Shaping Policy Using the Class-Default Class](#) (optional)
- [Configuring Queueing and Fragmentation on the Frame Relay Interface](#) (required)
- [Verifying Frame Relay Queueing and Fragmentation at the Interface](#) (optional)

## Configuring Class Policy for the Priority Queue

To configure a policy map for the priority class, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>policy-map</b> <i>policy-map</i>	Specifies the name of the policy map to be created or modified. <ul style="list-style-type: none"> <li>Use this command to define the queuing policy for the priority queue.</li> </ul>
Step 2	Router(config-pmap)# <b>class</b> <i>class-name</i>	Specifies the name of a class to be created and included in the service policy. <ul style="list-style-type: none"> <li>The class name that you specify in the policy map defines the characteristics for that class and its match criteria as configured using the <b>class-map</b> command.</li> </ul>
Step 3	Router(config-pmap-c)# <b>priority</b> <i>bandwidth-kbps</i>	Creates a strict priority class and specifies the amount of bandwidth, in kbps, to be assigned to the class.

## Configuring Class Policy for the Bandwidth Queues

To configure a policy map and create class policies that make up the service policy, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>policy-map</b> <i>policy-map</i>	Specifies the name of the policy map to be created or modified. <ul style="list-style-type: none"> <li>The bandwidth queues and the priority queue use the same policy map.</li> </ul>

	Command	Purpose
Step 2	Router(config-pmap)# <b>class</b> <i>class-name</i>	Specifies the name of a class to be created and included in the service policy. <ul style="list-style-type: none"> <li>The class name that you specify in the policy map defines the characteristics for that class and its match criteria as configured using the <b>class-map</b> command.</li> </ul>
Step 3	Router(config-pmap-c)# <b>bandwidth</b> <i>bandwidth-kbps</i>	Specifies the amount of bandwidth to be assigned to the class, in kbps, or as a percentage of the available bandwidth. Bandwidth must be specified in kbps or as a percentage consistently across classes. (Bandwidth of the priority queue must be specified in kbps.) <ul style="list-style-type: none"> <li>The sum of all bandwidth allocation on an interface cannot exceed 75 percent of the total available interface bandwidth. However, if you need to configure more than 75 percent of the interface bandwidth to classes, you can override the 75 percent maximum by using the <b>max-reserved-bandwidth</b> command.</li> </ul>

## Configuring the Shaping Policy Using the Class-Default Class

In general, the class-default class is used to classify traffic that does not fall into one of the defined classes. Even though the class-default class is predefined when you create the policy map, you still have to configure it. If a default class is not configured, traffic that does not match any of the configured classes is given best-effort treatment, which means that the network will deliver the traffic if it can, without any assurance of reliability, delay prevention, or throughput.

If you configure shaping in addition to queueing on the interface, use the class-default class to configure the shaping policy. The shaping policy will serve as the parent in a hierarchical traffic policy. The queueing policy will serve as the child policy. The class-default class is used for the shaping policy so that all traffic for the entire interface is shaped and a bandwidth-limited stream can be created.

To configure the shaping policy in the class-default class, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>policy-map</b> <i>policy-map</i>	Specifies the name of the policy map to be created or modified. <ul style="list-style-type: none"> <li>Use this command to define the shaping policy.</li> </ul>
Step 2	Router(config-pmap)# <b>class</b> <b>class-default</b>	Specifies the default class so that you can configure or modify its policy.

<b>Step 3</b>	Router(config-pmap-c)# <b>shape</b> [ <b>average</b>   <b>peak</b> ] <i>mean-rate</i> [[ <i>burst-size</i> ] [ <i>excess-burst-size</i> ]]	(Optional) Shapes traffic to the indicated bit rate according to the algorithm specified.
<b>Step 4</b>	Router(config-pmap-c)# <b>service-policy</b> <i>policy-map-name</i>	Specifies the name of a policy map to be used as a matching criterion (for nesting traffic policies [hierarchical traffic policies] within one another). <ul style="list-style-type: none"> <li>Use this command to attach the policy map for the priority queue (the child policy) to the shaping policy (the parent policy).</li> </ul>

## Configuring Queueing and Fragmentation on the Frame Relay Interface

To configure low-latency queueing and FRF.12 end-to-end fragmentation on a Frame Relay interface, use the following commands beginning in global configuration mode:

	Command	Purpose
<b>Step 1</b>	Router(config)# <b>interface</b> <i>type number</i>	Configures an interface type and enters interface configuration mode.
<b>Step 2</b>	Router(config-if)# <b>encapsulation frame-relay</b>	Enables Frame Relay encapsulation.
<b>Step 3</b>	Router(config-if)# <b>service-policy output</b> <i>policy-map-name</i>	Attaches a policy map to an output interface, to be used as the service policy for that interface. <ul style="list-style-type: none"> <li>If shaping is being used, use this command to attach the shaping policy (which includes the nested queueing policy) to the interface.</li> <li>Interleaving of high-priority frames will not work if shaping is configured on the interface.</li> <li>If shaping is not being used, use this command to attach the queueing policy to the interface.</li> </ul>
<b>Step 4</b>	Router(config-if)# <b>frame-relay fragment</b> <i>fragment-size</i> <b>end-to-end</b>	Enables fragmentation of Frame Relay frames. <ul style="list-style-type: none"> <li>To maintain low latency and low jitter for priority queue traffic, configure the fragment size to be greater than the largest high-priority frame that would be expected.</li> </ul>

## Verifying Frame Relay Queueing and Fragmentation at the Interface

To verify the configuration and performance of Frame Relay queueing and fragmentation at the interface, perform the following steps:

- Step 1** Enter the **show running-config** command to verify the configuration.

```
Router# show running-config
Building configuration...

.
.
.

class-map match-all voice
  match ip precedence 5
!
!policy-map llq
  class voice
    priority 64
policy-map shaper
  class class-default
    shape peak 96000
    service-policy llq
!
!interface Serial1/1
  ip address 16.0.0.1 255.255.255.0
  encapsulation frame-relay
  service-policy output shaper
  frame-relay fragment 80 end-to-end
!
```

- Step 2** Enter the **show policy-map interface** command to display low-latency queueing information, packet counters, and statistics for the policy map applied to the interface. Compare the values in the “packets” and the “pkts matched” counters; under normal circumstances, the “packets” counter is much larger than the “pkts matched” counter. If the values of the two counters are nearly equal, then the interface is receiving a large number of process-switched packets or is heavily congested.

The following sample output for the **show policy-map interface** command is based on the configuration in Step 1:

```
Router# show policy-map interface serial 1/1

Serial1/1

Service-policy output:shaper

Class-map:class-default (match-any)
 12617 packets, 1321846 bytes
 5 minute offered rate 33000 bps, drop rate 0 bps
Match:any
Traffic Shaping
      Target/Average   Byte   Sustain   Excess   Interval   Increment
      Rate             Limit  bits/int  bits/int  (ms)      (bytes)
      192000/96000     1992   7968      7968      83        1992

Adapt Queue   Packets  Bytes   Packets  Bytes  Shaping
Active Depth             12586   1321540 0        0      Active
-      0
```

```

Service-policy :llq

Class-map:voice (match-all)
  3146 packets, 283140 bytes
  5 minute offered rate 7000 bps, drop rate 0 bps
  Match:ip precedence 1
  Weighted Fair Queuing
    Strict Priority
    Output Queue:Conversation 24
    Bandwidth 64 (kbps) Burst 1600 (Bytes)
    (pkts matched/bytes matched) 0/0
    (total drops/bytes drops) 0/0

Class-map:class-default (match-any)
  9471 packets, 1038706 bytes
  5 minute offered rate 26000 bps
  Match:any

```

- Step 3** Enter the **show interfaces serial** command to display information about the queuing strategy, priority queue interleaving, and type of fragmentation configured on the interface. You can determine whether the interface has reached a congestion condition and packets have been queued by looking at the “Conversations” fields. A nonzero value for “max active” counter shows whether any queues have been active. If the “active” counter is a nonzero value, you can use the **show queue** command to view the contents of the queues.

The following sample output for the **show interfaces serial** command is based on the configuration in Step 1:

```

Router# show interfaces serial 1/1

Serial1/1 is up, line protocol is up
  Hardware is M4T
  Internet address is 16.0.0.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 5/255, rxload 1/255
  Encapsulation FRAME-RELAY, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  LMI enq sent 40, LMI stat recvd 40, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
  LMI DLCI 1023 LMI type is CISCO frame relay DTE
  Fragmentation type:end-to-end, size 80, PQ interleaves 0
  Broadcast queue 0/64, broadcasts sent/dropped 0/0, interface broadcasts 0
  Last input 00:00:03, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:06:34
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queuing strategy:weighted fair
  Output queue:0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/1/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 33000 bits/sec, 40 packets/sec
    40 packets input, 576 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    15929 packets output, 1668870 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions DCD=up DSR=up DTR=up RTS=up CTS=up

```

# Monitoring and Maintaining Frame Relay Queueing and Fragmentation at the Interface

To monitor and maintain Frame Relay queueing and fragmentation at the interface, use the following commands in privileged EXEC mode:

Command	Purpose
Router# <b>debug frame-relay fragment</b> [ <i>event</i>   <b>interface</b> <i>type number dlci</i> ]	Displays information related to Frame Relay fragmentation on a PVC.
Router# <b>show frame-relay fragment</b> [ <b>interface</b> <i>type number</i> [ <i>dlci</i> ]]	Displays information about Frame Relay fragmentation.
Router# <b>show interfaces serial</b> <i>number</i>	Displays information about a serial interface.
Router# <b>show queue</b> <i>interface-type interface-number</i>	Displays the contents of packets inside a queue for a particular interface.
Router# <b>show policy-map interface</b> <i>number</i> [ <b>input</b>   <b>output</b> ]	Displays the packet statistics of all classes that are configured for all service policies on the specified interface.

## Configuration Examples

This section provides the following configuration examples:

- [Frame Relay Queueing, Shaping, and Fragmentation at the Interface Example](#)
- [Frame Relay Queueing and Fragmentation at the Interface Example](#)

### Frame Relay Queueing, Shaping, and Fragmentation at the Interface Example

The following example shows the configuration of a hierarchical policy for low-latency queueing, FRF.12 fragmentation, and shaping on serial interface 3/2. Note that traffic from the priority queue will not be interleaved with fragments from the class-default queue because shaping is configured.

```
class-map voice
  match access-group 101

policy-map llq
  class voice
    priority 64

policy-map shaper
  class class-default
    shape average 96000
    service-policy llq

interface serial 3/2
  ip address 10.0.0.1 255.0.0.0
  encapsulation frame-relay
  bandwidth 128
  clock rate 128000
  service-policy output shaper
  frame-relay fragment 80 end-to-end

access-list 101 match ip any host 10.0.0.2
```

## Frame Relay Queueing and Fragmentation at the Interface Example

The following example shows the configuration of low-latency queueing and FRF.12 fragmentation on serial interface 3/2. Because shaping is not being used, a hierarchical traffic policy is not needed and traffic from the priority queue will be interleaved with fragments from the other queues. Without shaping, the output rate of the interface is equal to the line rate or configured clock rate. In this example, the clock rate is 128,000 bps.

```
class-map voice
  match access-group 101

policy-map llq
  class voice
    priority 64
  class video
    bandwidth 32

interface serial 3/2
  ip address 10.0.0.1 255.0.0.0
  encapsulation frame-relay
  bandwidth 128
  clock rate 128000
  service-policy output llq
  frame-relay fragment 80 end-to-end

access-list 101 match ip any host 10.0.0.2
```

## Command Reference

This section documents modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- [frame-relay fragment end-to-end](#)
- [show interfaces serial](#)

## frame-relay fragment end-to-end

To enable fragmentation of Frame Relay frames on an interface, use the **frame-relay fragment end-to-end** command in interface configuration mode. To disable Frame Relay fragmentation, use the **no** form of this command.

**frame-relay fragment** *fragment-size* **end-to-end**

**no frame-relay fragment**

### Syntax Description

*fragment-size* Specifies the number of payload bytes from the original Frame Relay frame that will go into each fragment. This number excludes the Frame Relay header of the original frame.

All the fragments of a Frame Relay frame except the last will have a payload size equal to *fragment-size*; the last fragment will have a payload less than or equal to *fragment-size*. Valid values are from 16 to 1600 bytes; the default is 53.

### Defaults

Fragmentation is disabled.  
*fragment-size*: 53

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(14)S	This command was introduced to enable fragmentation on a Frame Relay interface.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

### Usage Guidelines

Interface fragmentation and class-based fragmentation cannot be configured at the same time. To configure class-based fragmentation that can be applied to individual permanent virtual circuits (PVCs), use the **frame-relay fragment** command in map-class configuration mode.

Interface fragmentation supports the following types of fragment formats:

- End-to-end FRF.12 format
- FRF.11 Annex C format
- Cisco proprietary format

When fragmentation is enabled on an interface, all PVCs on the main interface and its subinterfaces will have fragmentation enabled with the same configured fragment size.

All the fragments of a Frame Relay frame except the last will have a payload size equal to the configured *fragment-size* value; the last fragment will have a payload less than or equal to *fragment-size*.

When configuring fragmentation on an interface that has low-latency queuing, configure the fragment size to be greater than the largest high-priority frame that would be expected. This configuration will prevent higher-priority traffic from being fragmented and queued up behind lower priority fragmented frames. If the size of a priority frame is larger than the configured fragment size, the priority frame will be fragmented.

Local Management Interface (LMI) traffic will not be fragmented.

Note the following interface fragmentation restrictions:

- Interface fragmentation and Frame Relay traffic shaping cannot be configured at the same time.
- Interface fragmentation and class-based fragmentation cannot be configured at the same time.

## Examples

The following example shows the configuration of low-latency queuing, FRF.12 fragmentation, and shaping on serial interface 3/2. Note that traffic from the priority queue will not be interleaved with fragments from the class-default queue because shaping is configured.

```
class-map voice
  match access-group 101

policy-map llq
  class voice
    priority 64

policy-map shaper
  class class-default
    shape average 96000
    service-policy llq

interface serial 3/2
  ip address 10.0.0.1 255.0.0.0
  encapsulation frame-relay
  bandwidth 128
  clock rate 128000
  service-policy output shaper
  frame-relay fragment 80 end-to-end

access-list 101 match ip any host 10.0.0.2
```

## Related Commands

Command	Description
<b>class (policy-map)</b>	Specifies the name of the class whose policy you want to create or change or specifies the default class before you configure its policy.
<b>debug frame-relay fragment</b>	Displays information related to Frame Relay fragmentation on a PVC.

# show interfaces serial

To display information about a serial interface, use the **show interfaces serial** command in privileged EXEC mode.

## Cisco 4000 Series

```
show interfaces serial [number [:channel-group]] [accounting]
```

## Cisco 7200 Series

```
show interfaces serial [slot/port] [accounting]
```

## Cisco 7000 and Cisco 7500 Series with the RSP7000, RSP7000CI, or Ports on VIPs

```
show interfaces serial [slot/port-adapter/port]
```

## Cisco 7500 Series

```
show interfaces serial [slot/port [:channel-group]] [accounting]
```

## Cisco 7500 Series with a CT3IP

```
show interfaces serial [slot/port-adapter/port] [:t1-channel] [accounting | crb]
```

## Cisco AS5800 Access Servers

```
show interfaces serial dial-shelf/slot/t3-port:t1-num:chan-group
```

Syntax	Description
<i>number</i>	(Optional) Number of the port being configured.
<i>:channel-group</i>	(Optional) On the Cisco 4000 series with an NPM or Cisco 7500 series routers with a MIP (MultiChannel Interface Processor), specifies the T1 channel-group number in the range from 0 to 23 defined with the <b>channel-group</b> controller configuration command.
<b>accounting</b>	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
<i>slot/port</i>	(Optional) Number of the slot and port being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port-adapter</i>	(Optional) Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.
<i>:t1-channel</i>	(Optional) For the CT3IP, the T1 channel is a number from 1 to 28.  T1 channels on the CT3IP are numbered from 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This convention is used to ensure consistency with telco numbering schemes for T1 channels within channelized T3 equipment.
<b>crb</b>	(Optional) Shows interface routing and bridging information.
<i>dial-shelf</i>	Dial shelf chassis in the Cisco AS5800 access server containing the CT3 interface card.
<i>slot</i>	Location of the CT3 interface card in the dial shelf chassis.

---

**show interfaces serial**

<i>t3-port</i>	T3 port number. The only valid value is 0.
<i>:t1-num</i>	T1 time slot in the T3 line. The value can be from 1 to 28.
<i>:chan-group</i>	Channel group identifier.

---

**Command Modes**

Privileged EXEC

---

**Command History**

Release	Modification
10.0	This command was introduced for the Cisco 4000 series routers.
11.0	This command was introduced for the Cisco 7000 series routers.
11.1 CA	This command was modified to include sample output for the PA-2JT2 serial port adapter, PA-E3 serial port adapter, and PA-T3 serial port adapter.
11.3	This command was modified to include the CT3IP.
12.0(3)T	This command was modified to include support for the Cisco AS5800 access servers.
12.2(14)S	This command was modified to display information about Frame Relay interface queuing and fragmentation.
12.2(13)T	The modifications for Frame Relay interface queuing and fragmentation were integrated into Cisco IOS Release 12.2(13)T.

---

**Usage Guidelines**

Use this command to determine the status of the Frame Relay link. This display also indicates Layer 2 status if switched virtual circuits (SVCs) are configured.

---

**Examples**

The following is sample output from the **show interfaces serial** command for a synchronous serial interface:

```
Router# show interfaces serial

Serial 0 is up, line protocol is up
  Hardware is MCI Serial
  Internet address is 131.136.190.203, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 0:00:07, output 0:00:00, output hang never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
    16263 packets input, 1347238 bytes, 0 no buffer
    Received 13983 broadcasts, 0 runts, 0 giants
    2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort
  1 carrier transitions

    22146 packets output, 2383680 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets, 0 restarts
```

[Table 1](#) describes significant fields shown in the display.

**Table 1** *show interfaces serial Field Descriptions*

Field	Description
Serial ... is {up   down} ... is administratively down	Indicates whether the interface hardware is currently active (whether carrier detect is present), is inactive, or has been taken down by an administrator.
line protocol is {up   down}	Indicates whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful) or the line protocol has been taken down by an administrator.
Hardware is	Specifies the hardware type.
Internet address is	Specifies the Internet address and subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Indicates the value of the bandwidth parameter that has been configured for the interface (in kilobits per second). The bandwidth parameter is used to compute IGRP metrics only. If the interface is attached to a serial line with a line speed that does not match the default (1536 or 1544 for T1 and 56 for a standard synchronous serial line), use the <b>bandwidth</b> command to specify the correct line speed for this serial line.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether loopback is set or not.
keepalive	Indicates whether keepalives are set or not.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed.  This field is not updated by fast-switched traffic.
Last output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface.
output hang	Number of hours, minutes, and seconds since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because of a full queue.

**Table 1** *show interfaces serial Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
5 minute input rate 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes.  The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet networks and bursts of noise on serial lines are often responsible for “no buffer” events.
Received... broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
input errors	Total counts of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort events. Other input-related errors can also increment the count, so this sum might not balance with the other counts.
CRC	Cyclic redundancy checksum generated by the originating station or far-end device does not match the checksum calculated from the data received. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to pass received data to a hardware buffer because the input rate exceeded the receiver’s ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. “Ignored” errors often occur when a fast ingress interface feeds a slower egress interface. Broadcast storms and bursts of noise can also cause the “ignored” count to be increased.
abort	Illegal sequence of one bits on a serial interface. This usually indicates a clocking problem between the serial interface and the data link equipment.
carrier transitions	Number of times the carrier detect signal of a serial interface has changed state. For example, if data carrier detect (DCD) goes down and comes up, the carrier transition counter will increment two times. Indicates modem or line problems if the carrier detect line is changing state often.
packets output	Total number of messages transmitted by the system.

**Table 1** *show interfaces serial Field Descriptions (continued)*

Field	Description
bytes output	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle. This might never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors, as some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. This usually is the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). Some collisions are normal. However, if your collision rate climbs to 4 or 5 percent, you should consider verifying that there is no faulty equipment on the segment or moving some existing stations to a new segment. A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds' time. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
restarts	Number of times the controller was restarted because of errors.
alarm indications, remote alarms, rx LOF, rx LOS	Number of channel service unit/data service unit (CSU/DSU) alarms, and number of occurrences of receive loss of frame and receive loss of signal.
BER inactive, NELR inactive, FELR inactive	Status of G.703-E1 counters for bit-error rate (BER) alarm, near-end loop remote (NELR), and far-end loop remote (FELR). Note that you cannot set the NELR or FELR.

**Frame Relay Queuing and Fragmentation at the Interface Example**

The following is sample output from the **show interfaces serial** command when low-latency queuing and FRF.12 end-to-end fragmentation are configured on a Frame Relay interface:

```
Router# show interfaces serial 3/2

Serial3/2 is up, line protocol is up
  Hardware is M4T
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, crc 16, loopback not set
  Keepalive set (10 sec)
  LMI enq sent 0, LMI stat recvd 0, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
  LMI DLCI 1023 LMI type is CISCO frame relay DTE
  Fragmentation type: end-to-end, size 80, PQ interleaves 0
  Broadcast queue 0/64, broadcasts sent/dropped 0/0, interface broadcasts 0
```

```
show interfaces serial
```

```
Last input 2d15h, output 2d15h, output hang never
Last clearing of "show interface" counters 00:01:31
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
  Conversations 0/0/256 (active/max active/max total)
  Reserved Conversations 0/0 (allocated/max allocated)
  Available Bandwidth 1094 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 output buffer failures, 0 output buffers swapped out
  1 carrier transitions      DCD=up DSR=up DTR=up RTS=up CTS=up
```

Table 2 describes significant fields shown in the display that are different from the fields described in Table 1.

**Table 2** *show interfaces serial Field Descriptions—Frame Relay Interface Queueing and Fragmentation*

Field	Description
txload	Interface load in the transmit direction.
rxload	Interface load in the receive direction.
crc	Number of Layer 1 checksum errors during reception.
LMI enq sent	Number of Frame Relay status inquiry messages sent.
LMI stat recvd	Number of Frame Relay status request messages received.
LMI upd recvd	Number of single PVC asynchronous status messages received.
DTE LMI up	LMI peers are synchronized.
LMI enq recvd	Number of Frame Relay status inquiry messages received.
LMI stat sent	Number of Frame Relay status request messages sent.
LMI upd sent	Number of single PVC asynchronous status messages sent.
Fragmentation type	Type of fragmentation: end-to-end, Cisco, or VoFR
size	Fragmentation size.
PQ interleaves	Number of priority queue frames that have interleaved data fragments.
Broadcast queue	Number on queue/queue depth
broadcasts sent/dropped	Number of broadcasts sent and dropped.
interface broadcasts	Number of broadcasts sent on interface.
Input queue:	size—Current size of the input queue. max—Maximum size of the queue. drops—Number of messages discarded. flushes—Number of times data on queue has been discarded.
Queueing strategy	Type of queueing configured on the interface.

**Table 2** *show interfaces serial Field Descriptions—Frame Relay Interface Queueing and Fragmentation (continued)*

Field	Description
Output queue:	size—Current size of the output queue. max total—Maximum number of frames that can be queued. threshold—Congestive-discard threshold. Number of messages in the queue after which new messages for high-bandwidth conversations are dropped. drops—Number of dropped messages.
Conversations:	active—Number of currently active conversations. max active— Maximum number of conversations that have ever occurred at one time. max total—Maximum number of active conversations allowed.
throttles	Number of times the receiver on the port was disabled, possibly because of processor or buffer overload.
output buffer failures	Number of “no resource” errors received on the output.
output buffers swapped out	Number of packets swapped to DRAM.

■ show interfaces serial