



VoIP Interoperability with Cisco Express Forwarding and Policy Based Routing

Document Update Alert

This document was originally produced for Cisco IOS Release 12.2(11)T. This feature has been updated in subsequent releases, and more recent documentation is available.

If you are using Cisco IOS Release 12.2(11)T or higher, refer to the following documentation in the Cisco IOS Voice Configuration Library, Release 12.3:

- [VoIP Interoperability with Cisco Express Forwarding and Policy-Based Routing](#)
-

Feature History

Release	Modification
12.2(11)T	This feature was introduced on the Cisco IAD2420 series, Cisco 2600 series, Cisco 3620 routers, Cisco 3640routers, Cisco 3660 routers, Cisco 3700 series routers and Cisco MC3810 multiservice access concentrators.

This document describes the VoIP Interoperability with Cisco Express Forwarding and Policy Based Routing feature in Cisco IOS Release 12.2(11)T. This document includes the following sections:

- [Feature Overview, page 2](#)
- [Supported Platforms, page 8](#)
- [Supported Standards, MIBs, and RFCs, page 9](#)
- [Prerequisites, page 9](#)
- [Configuration Examples, page 19](#)
- [Command Reference, page 22](#)
- [Glossary, page 33](#)

Feature Overview

This feature enables Cisco Express Forwarding (CEF) of VoIP signaling and payload packets that originate from voice interfaces and interactive voice response (IVR) application. This feature also enables Policy Based Routing of VoIP traffic that originates or terminates on the specified voice gateways and introduces voice packet Differentiated Services Code Point (DSCP) marking for Media Gateway Control Protocol (MGCP) voice gateways.

This feature modifies the Voice over IP (VoIP) and IVR programming so that they can interoperate with features that are supported only in the CEF path (not in the fast switching path that VoX uses). Voice and IVR only work in the fast path on the routers where they are originated and terminated (Voice and IVR on "transit" routers are just data packets and of course can be CEF switched).

Cisco Express Forwarding (CEF) is advanced Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as the Internet, on networks characterized by intensive Web-based applications, or interactive sessions.

Although you can use CEF in any part of a network, it is designed for high-performance, highly resilient Layer 3 IP backbone switching.

CEF Components

Information conventionally stored in a route cache is stored in several data structures for CEF switching. The data structures provide optimized lookup for efficient packet forwarding. The two main components of CEF operation are:

- Forwarding Information Base
- Adjacency Tables

Forwarding Information Base

CEF uses a Forwarding Information Base (FIB) to make IP destination prefix-based switching decisions. The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and those changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table.

Because there is a one-to-one correlation between FIB entries and routing table entries, the FIB contains all known routes and eliminates the need for route cache maintenance that is associated with earlier switching paths such as fast switching and optimum switching.

Adjacency Tables

Network nodes in the network are said to be adjacent if they can reach each other with a single hop across a link layer. In addition to the FIB, CEF uses adjacency tables to prepend Layer 2 addressing information. The adjacency table maintains Layer 2 next-hop addresses for all FIB entries.

Adjacency Discovery

The adjacency table is populated as adjacencies are discovered. Each time an adjacency entry is created (such as through the ARP protocol), a link-layer header for that adjacent node is precomputed and stored in the adjacency table. When a route is determined, it points to a next hop and corresponding adjacency entry. It is subsequently used for encapsulation during CEF switching of packets.

Adjacency Resolution

A route might have several paths to a destination prefix, such as when a router is configured for simultaneous load balancing and redundancy. For each resolved path, a pointer is added for the adjacency corresponding to the next-hop interface for that path. This mechanism is used for load balancing across several paths.

Adjacency Types That Require Special Handling

In addition to adjacencies associated with next-hop interfaces (host-route adjacencies), other types of adjacencies are used to expedite switching when certain exception conditions exist. When the prefix is defined, prefixes requiring exception processing are cached with one of the special adjacencies listed in Table 1.

Table 1 Adjacency Types for Exception Processing

This adjacency type...	Receives this processing..
Null adjacency	Packets destined for a Null0 interface are dropped. This can be used as an effective form of access filtering.
Glean adjacency	When a router is connected directly to several hosts, the FIB table on the router maintains a prefix for the subnet rather than for the individual host prefixes. The subnet prefix point to a glean adjacency. When packets need to be forwarded to a specific host, the adjacency database is gleaned for the specific prefix.
Punt adjacency	Features that require special handling or features that are not yet supported in conjunction with CEF switching paths are forwarded to the next switching layer for handling. Features that are not supported are forwarded to the next higher switching level.
Discard adjacency	Packets are discarded. This type of adjacency occurs only on the Cisco 12000 series routers.
Drop adjacency	Packets are dropped, but the prefix is checked.

Unresolved Adjacency

When a link-layer header is prepended to packets, FIB requires the prepend to point to an adjacency corresponding to the next hop. If an adjacency was created by FIB and not discovered through a mechanism, such as ARP, the Layer 2 addressing information is not known and the adjacency is considered incomplete. After the Layer 2 information is known, the packet is forwarded to the route processor, and the adjacency is determined through ARP.

Supported Media

CEF supports ATM/AAL5 SNAP, ATM/AAL5mux, ATM/AAL5nlpid, Frame Relay, Ethernet, FDDI, PPP, HDLC, and tunnels.

Central CEF Mode

When CEF mode is enabled, the CEF FIB and adjacency tables reside on the route processor, and the route processor performs the express forwarding. You can use CEF mode when line cards are not available for CEF switching or when you need to use features not compatible with distributed CEF switching.

Policy-Based Routing

PBR (policy based routing) gives you a flexible means of routing packets by allowing you to configure a defined policy for traffic flows, lessening reliance on routes derived from routing protocols. To this end, PBR gives you more control over routing by extending and complementing the existing mechanisms provided by routing protocols. PBR allows you to set the IP precedence. It also allows you to specify a path for certain traffic, such as priority traffic over a high-cost link.

You can set up PBR as a way to route packets based on configured policies. For example, you can implement routing policies to allow or deny paths based on the identity of a particular end system, an application protocol, or the size of packets.

PBR allows you to perform the following tasks:

- Classify traffic based on extended access list criteria. Access lists, then, establish the match criteria.
- Set IP precedence bits, giving the network the ability to enable differentiated classes of service.
- Route packets to specific traffic-engineered paths; you might need to route them to allow a specific QoS through the network.

Policies can be based on IP address, port numbers, protocols, or size of packets. For a simple policy, you can use any one of these descriptors; for a complicated policy, you can use all of them.

For example, classification of traffic through PBR allows you to identify traffic for different classes of service at the edge of the network and then implement quality of service (QoS) defined for each class of service (CoS) in the core of the network using priority queuing (PQ), custom queuing (CQ), or weighted fair queuing (WFQ) techniques. This process obviates the need to classify traffic explicitly at each wide-area network (WAN) interface in the core-backbone network.

How It Works

All packets received on an interface with PBR enabled are passed through enhanced packet filters known as route maps. The route maps used by PBR dictate the policy, determining to where the packets are forwarded.

Route maps are composed of statements. The route map statements can be marked as permit or deny, and they are interpreted in the following ways:

- If the packets do not match any route map statements, then all the set clauses are applied.
- If a statement is marked as deny, the packets meeting the match criteria are sent back through the normal forwarding channels and destination-based routing is performed.
- If the statement is marked as permit and the packets do not match any route map statements, the packets are sent back through the normal forwarding channels and destination-based routing is performed.

You specify PBR on the interface that receives the packet, not on the interface from which the packet is sent.

When To Use Policy-Based Routing

You might enable PBR if you want certain packets to be routed some way other than the obvious shortest path. For example, PBR can be used to provide the following functionality:

- Equal access
- Protocol-sensitive routing
- Source-sensitive routing

- Routing based on interactive versus batch traffic
- Routing based on dedicated links

About Differentiated Services

Differentiated services (DiffServ) describes a set of end-to-end QoS (Quality of Service) capabilities. End-to-end QoS is the ability of the network to deliver service required by specific network traffic from one end of the network to another. Cisco IOS QoS software supports three types of service models: best-effort services, integrated services (IntServ), and differentiated services.

Differentiated services is a multiple service model that can satisfy differing QoS requirements. With Differentiated Services, the network tries to deliver a particular kind of service based on the QoS specified by each packet. This specification can occur in different ways, for example, using the 6-bit DSCP setting in IP packets or source and destination addresses. The network uses the QoS specification to classify, mark, shape, and police traffic, and to perform intelligent queuing.

Differentiated services is used for several mission-critical applications and for providing end-to-end QoS. Typically, Differentiated services is appropriate for aggregate flows because it performs a relatively coarse level of traffic classification.

DS Field Definition

A replacement header field, called the DS field, is defined by differentiated services. The DS field supersedes the existing definitions of the IPv4 type of service (ToS) octet (RFC 791) and the IPv6 traffic class octet. Six bits of the DS field are used as the DSCP to select the per hop behavior (PHB) at each interface. A currently unused (CU) 2-bit field is reserved for explicit congestion notification (ECN). The value of the CU bits is ignored by DS-compliant interfaces when determining the PHB to apply to a received packet.

Per-Hop Behaviors

RFC 2475 defines PHB as the externally observable forwarding behavior applied at a DiffServ-compliant node to a DiffServ behavior aggregate (BA).

With the ability of the system to mark packets according to DSCP setting, collections of packets with the same DSCP setting and sent in a specific direction can be grouped into a BA. Packets from multiple sources or applications can belong to the same BA.

In other words, a PHB refers to the packet scheduling, queuing, policing, or shaping behavior of a node on any given packet belonging to a BA, as configured by a service level agreement (SLA) or a policy map.

The following sections describe the four available standard PHBs:

- Default PHB (as defined in RFC 2474).
- Class-Selector PHB (as defined in RFC 2474).
- Assured Forwarding (AFny) PHB (as defined in RFC 2597).
- Expedited Forwarding (EF) PHB (as defined in RFC 2598).

Default PHB

The default PHB essentially specifies that a packet marked with a DSCP value of 000000 (recommended) receives the traditional best-effort service from a DS-compliant node (that is, a network node that complies with all of the core DiffServ requirements). Also, if a packet arrives at a DS-compliant node, and the DSCP value is not mapped to any other PHB, the packet will get mapped to the default PHB.

Class-Selector PHB

To preserve backward-compatibility with any IP Precedence scheme currently in use on the network, DiffServ has defined a DSCP value in the form xxx000, where x is either 0 or 1. These DSCP values are called Class-Selector Code Points. (The DSCP value for a packet with default PHB 000000 is also called the Class-Selector Code Point.)

The PHB associated with a Class-Selector Code Point is a Class-Selector PHB. These Class-Selector PHBs retain most of the forwarding behavior as nodes that implement IP Precedence-based classification and forwarding.

For example, packets with a DSCP value of 110000 (the equivalent of the IP Precedence-based value of 110) have preferential forwarding treatment (for scheduling, queueing, and so on), as compared to packets with a DSCP value of 100000 (the equivalent of the IP Precedence-based value of 100). These Class-Selector PHBs ensure that DS-compliant nodes can coexist with IP Precedence-based nodes.

Assured Forwarding PHB

Assured Forwarding PHB is nearly equivalent to Controlled Load Service available in the integrated services model. AFny PHB defines a method by which BAs can be given different forwarding assurances.

For example, network traffic can be divided into the following classes:

- Gold: 50% of the available bandwidth.
- Silver: 30% of the available bandwidth.
- Bronze: 20% of the available bandwidth.

Further, the AFny PHB defines four AF classes: AF1, AF2, AF3, and AF4. Each class is assigned a specific amount of buffer space and interface bandwidth, according to the SLA with the service provider or policy map.

Within each AF class, you can specify three drop precedence (dP) values: 1, 2, and 3. Assured Forwarding PHB can be expressed as shown in the following example: AFny. In this example, n represents the AF class number (1, 2, or 3) and y represents the dP value (1, 2, or 3) within the AFn class.

In instances of network traffic congestion, if packets in a particular AF class (for example, AF1) need to be dropped, packets in the AF1 class will be dropped according to the following guideline:

$$dP(AFny) \geq dP(AFnz) \geq dP(AFnx)$$

where dP (AFny) is the probability that packets of the AFny class will be dropped. In other words, y denotes the dP within an AFn class.

In the following example, packets in the AF13 class will be dropped before packets in the AF12 class, which in turn will be dropped before packets in the AF11 class:

$$dP(AF13) \geq dP(AF12) \geq dP(AF11)$$

The dP method penalizes traffic flows within a particular BA that exceed the assigned bandwidth. Packets on these offending flows could be re-marked by a policer to a higher drop precedence.

An AFx class can be denoted by the DSCP value, xyzab0, where xyz can be 001, 010, 011, or 100, and ab represents the dP value.

Table 1 lists the DSCP value and corresponding dP value for each AF PHB class.

Table 2 DSCP Values and Corresponding Drop Precedence Values for Each AF PHB Class

Drop Precedence	Class 1	Class 2	Class 3	Class 4
Low drop precedence	001010	010010	011010	100010
Medium drop precedence	001100	010100	011100	100100
High drop precedence	001110	010110	011110	100110

Expedited Forwarding PHB

Resource Reservation Protocol (RSVP), a component of the integrated services model, provides a Guaranteed Bandwidth Service. Applications such as Voice over IP (VoIP), video, and online trading programs require this kind of robust service. The EF PHB, a key ingredient of DiffServ, supplies this type of robust service by providing low loss, low latency, low jitter, and assured bandwidth service.

EF can be implemented using priority queueing (PQ), along with rate-limiting on the class (or BA). When implemented in a DiffServ network, EF PHB provides a virtual leased line, or premium service. For optimal efficiency, however, EF PHB should be reserved for only the most critical applications because, in instances of traffic congestion, it is not feasible to treat all or most traffic as high priority.

EF PHB is ideally suited for applications such as VoIP that require low bandwidth, guaranteed bandwidth, low delay, and low jitter.

Benefits

- The DS-compliant CLI s provide a means by which you can specify different priority levels for voice payload traffic and signaling traffic at the originating gateway.
- This feature gives you better granularity for controlling traffic.

Restrictions

- CEF capabilities are not added to Hoot and Holler VoIP virtual interfaces.
- Performance is dependent upon the number of CEF features configured on the output ports. Voice Quality must be monitored as features are added to ensure the number of features does not degrade the voice quality.
- Performance impact is highly dependent on the number of CEF features configured on the output ports. Because there are more features available in the CEF path, it is possible that the voice quality will actually decrease in case of heavy feature utilization on the output IP/MPLS interface. However, in the more common case, CEF should provide slightly better performance than the IP fastswitching-based solution.

Related Documents

- [Cisco IOS Voice, Video, and Fax Configuration Guide](#), Release 12.2
- [Cisco IOS Voice, Video, and Fax Command Reference](#), Release 12.2
- [Cisco IOS IP Configuration Guide](#), Release 12.2.
- [Configuration Guide for Cisco DSLAMs with NI-2.](#)
- [Cisco IAD2420 Series Integrated Access Devices Software Configuration Guide](#)
- [Software Configuration Guide for the Cisco 2600, Cisco 3600 and Cisco 3700 series](#)
- [Important Information on Debug Commands](#)
- [Quick Start Guide: Cisco MC3810 Series Multiservice Access Concentrators Installation and Startup](#)

Supported Platforms

- Cisco IAD2420 series
- Cisco 2600 series
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco 3700 series
- Cisco MC3810

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on 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 quickly 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. 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 found at this URL:

<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

None

MIBs

None

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

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

To access Cisco MIB Locator, 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. 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 found at this URL:

<http://www.cisco.com/register>

RFCs

- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2475, *An Architecture for Differentiated Services*
- RFC 2597, *Assured Forwarding PHB Group*
- RFC 2598, *An Expedited Forwarding PHB*

Prerequisites

- Cisco IOS Release 12.2(11)T or a later release must be running.

Configuration Tasks

See the following sections for configuration tasks for the for the VoIP Interoperability with Cisco Express Forwarding and Policy Based Routing feature. Each task in the list is identified as either required or optional.

- [Configuring Standard IP Access Lists](#) (required)
- [Configuring IP Route Mapping](#) (required)
- [Enabling Policy Based Routing on a Loopback Interface](#) (required)
- [Enabling Policy Based Routing for VoIP Signaling Packets](#) (required)
- [Configuring IP DSCP](#) (optional)
- [Configuring MGCP IP DSCP](#) (required)
- [Configuring IP CEF \(minimum\)](#) (required)
- [Configuring Voice Class Source Interface](#) (required)
- [Configuring Source Interface Loopback for MGCP](#) (required)
- [Verifying Configuration](#) (optional)

Configuring Standard IP Access Lists

To define a standard IP access list, use the following command beginning in global configuration mode.

Command	Purpose
<p>Step 1</p> <pre>Router(config)# access-list access-list-number {deny permit} source [source-wildcard] [log]</pre>	<p>Defines a standard IP access list.</p> <p><i>access-list-number</i>—Number of an access list. This is a decimal number from 1 to 99 or from 1300 to 1999.</p> <p>deny—Denies access if the conditions are matched.</p> <p>permit—Permits access if the conditions are matched.</p> <p><i>source</i>—Number of the network or host from which the packet is being sent. There are two alternative ways to specify the source:</p> <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the any keyword as an abbreviation for a source and source-wildcard of 0.0.0.0 255.255.255.255. <p><i>source-wildcard</i>—(Optional) Wildcard bits to be applied to the source. There are two alternative ways to specify the source wildcard:</p> <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore. • Use the any keyword as an abbreviation for a source and source-wildcard of 0.0.0.0 255.255.255.255. <p>log—(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the logging console command.)</p> <p>The message includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.</p> <p>The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.</p>

Configuring IP Route Mapping

To enable route mapping, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# route-map <i>map-tag</i> [permit deny] <i>sequence-number</i>	<p>Identifies a route-map to use for policy routing on an interface.</p> <p><i>map-tag</i>—Defines a meaningful name for the route map. The redistribute router configuration command uses this name to reference this route map. Multiple route maps may share the same map tag name.</p> <p>permit—(Optional) If the match criteria are met for this route map, and the permit keyword is specified, the route is redistributed as controlled by the set actions. In the case of policy routing, the packet is policy routed.</p> <p>If the match criteria are not met, and the permit keyword is specified, the next route map with the same map tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.</p> <p>The permit keyword is the default.</p> <p>deny—(Optional) If the match criteria are met for the route map, and the deny keyword is specified, the route is not redistributed or in the case of policy routing, the packet is not policy routed, and no further route maps sharing the same map tag name will be examined. If the packet is not policy routed, the normal forwarding algorithm is used.</p> <p><i>sequence-number</i>—(Optional) Number that indicates the position a new route map is to have in the list of route maps already configured with the same name. If given with the no form of this command, the position of the route map should be deleted. Valid entries are 0 through 65535.</p>
Step 2	Router(config-route-map)# match ip address { <i>access-list-number</i> <i>access-list-name</i> } [... <i>access-list-number</i> ... <i>access-list-name</i>]	<p>Enables you to perform policy routing on packets.</p> <p>{<i>access-list-number</i> <i>access-list-name</i>}—Number or name of a standard or extended access list. It can be an integer from 1 to 199.</p>
Step 3	Router(config-route-map)# set interface <i>interface-type interface-number</i> [... <i>interface-type interface-number</i>]	<p>(Optional) Specifies the outbound interface for the policy-routed packets. Configure either set interface or set ip next-hop.</p>
Step 4	Router(config-route-map)# set ip next-hop <i>ip-address</i> [... <i>ip-address</i>]	<p>(Optional) Specifies the next-hop IP address for the policy-routed packets. Configure either set interface or set ip next-hop.</p>

Enabling Policy Based Routing on a Loopback Interface

To enable policy based routing on a loopback interface, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>Router(config)# interface loopback int-number</code>	Specifies a loopback interface and enters interface configuration mode. <i>int-number</i> —Specifies a number for the interface. Valid entries are from 0 to 2147483647.
Step 2	<code>Router(config-if)# ip policy route-map map-tag</code>	Attaches route-map tag to the loopback interface. The <i>map-tag</i> must match the setting specified by the route-map command.
Step 3	<code>Router(config-if)# ip route-cache policy</code>	Enables policy-based fastswitching on an interface. If you do not issue this command on an interface that has a policy attached, all policy routing happens at the process level.

Enabling Policy Based Routing for VoIP Signaling Packets

To enable policy based routing for VoIP signaling packets, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>Router(config-if)# ip local policy route-map map-tag</code>	Identifies the route map to use for local policy routing.

Configuring IP DSCP

To set the DSCP for the quality of service, use the following commands starting in global configuration mode:

	Command	Purpose
Step 1	Router(config)# dial-peer voice tag voip	Enters dial-peer configuration mode and specifies VoIP voice encapsulation.
Step 2	Router(config-dial-peer)# ip qos dscp [<i>number</i> <i>set-af</i> <i>set-cs</i> default ef] [media signaling]	Specifies IP DSCP. The optional keywords and arguments are as follows: <ul style="list-style-type: none"> • <i>number</i>—DSCP value. Valid entries are from 0 to 63. • <i>set-af</i>—Sets DSCP to assured forwarding bit pattern. The recommended value is af31, which sets the DSCP to assured forwarding (af31) bit pattern 011010. For a complete list of acceptable values, see Command Reference, page 22. • <i>set-cs</i>—Sets DSCP to class-selector code point. For a complete list of acceptable values, see Command Reference, page 22. • default—Sets DSCP to default bit pattern 000000. • ef—Sets DSCP to expedited forwarding bit pattern 101110. • media—Applies DSCP to media payload packets. • signaling—Applies DSCP to signaling packets.

Configuring MGCP IP DSCP

To set the DSCP for the quality of service, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<pre>Router(config)# mgcp ip qos dscp [number set-af set-cs default ef] [media signaling]</pre>	<p>To set the DSCP for the quality of service</p> <p>The optional keywords and arguments are as follows:</p> <ul style="list-style-type: none"> • <i>number</i>—DSCP value. Valid entries are from 0 to 63. • <i>set-af</i>—Sets DSCP to assured forwarding bit pattern. For a complete list of acceptable values, see the "Command Reference" section. • <i>set-cs</i>—Sets DSCP to class-selector code point. For a complete list of acceptable values, see the "Command Reference" section. • default—Sets DSCP to default bit pattern 000000. • ef—Sets DSCP to expedited forwarding bit pattern 101110. • media—Applies DSCP to media payload packets. • signaling—Applies DSCP to signaling packets.

Configuring IP CEF (minimum)

To configure minimum IP Cisco Express Forwarding, use the following command starting in global configuration mode:

	Command	Purpose
Step 1	<pre>Router(config)# ip cef</pre>	Enables standard CEF operation.

Configuring Voice Class Source Interface

To configure the dial peer source loopback interface to enable PBR for voice originating at this dial peer, use the following commands starting in global configuration mode:

	Command	Purpose
Step 1	<code>Router(config)# dial-peer voice tag voip</code>	Enters dial-peer configuration mode and specifies VoIP voice encapsulation. Valid entries for the <i>tag</i> are from 0 through 2147483647.
Step 2	<code>Router(config-dial-peer)# voice-class source interface loopback int-number</code>	Configures the dial peer source loopback interface to enable PBR for voice originating at this dial peer. loopback —Specifies loopback mode. <i>int-number</i> —Specifies a name for the interface. Valid entries are from 0 to 2147483647.
Step 3	<code>Router(config-dial-peer)# incoming called-number string</code>	(Optional) Specifies a digit string that can be matched by an incoming call to associate the call with a dial peer. If the policy routing of return RTP traffic is also desired, the incoming called-number command should be configured to ensure proper dial-peer matching. On the terminating voice gateway, the incoming called-number string value should match the destination-pattern configured on the terminating POTS dial-peer. Appropriate PBR commands also have to be configured on the terminating voice gateway. Note The <i>string</i> value may use wildcards to match the destination-patterns on multiple POTS dial-peers.

Configuring Source Interface Loopback for MGCP

To configure the MGCP profile source loopback interface at this interface, use the following commands starting in global configuration mode:

	Command	Purpose
Step 1	Router(config)# mgcp profile <i>profile-name</i>	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints. Use the <i>profile-name</i> default to apply to all of the endpoints on the MGCP gateway or specify your own unique name if only a subset of the available endpoints is desired. If you choose a unique profile name, ensure that Steps 3 and 4 are also followed.
Step 2	Router(config-mgcp-profile)# source interface loopback <i>int-number</i>	Configures the MGCP profile source loopback interface at this interface. Valid entries for <i>int-number</i> are from 0 to 2147483647.
Step 3	Router(config-mgcp-profile)# call-agent <i>call-agent-address</i>	(Optional) Specifies the IP address of the MGCP Call Agent to be associated with this MGCP profile. This option is available only when an MGCP profile other than default is specified.
Step 4	Router(config-mgcp-profile)# port <i>voice-port-number</i>	(Optional) Specifies a list of voice-ports (MGCP endpoints) that are associated with this MGCP profile. This option is available only when an MGCP profile other than default is specified.

Verifying Configuration

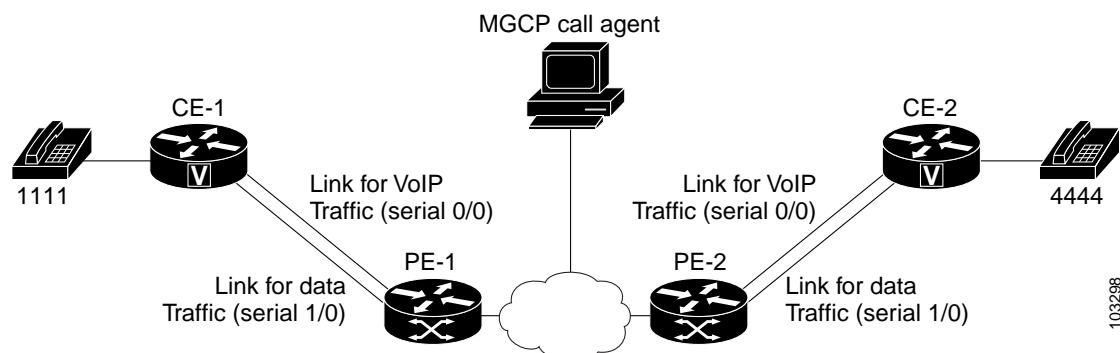
To verify that the Policy-based Routing is configured correctly, enter the **show running-config** privileged EXEC command to display the command settings for the router, as shown in the “Configuration Examples” section.

Configuration Examples

The following are configuration examples for the topology shown in [Figure 1](#):

- [FXS-to-FXS Call with Policy Based Routing and DSCP Marking \(H.323 and SIP\)](#)
- [FXS-to-FXS call with Policy Based Routing and DSCP Marking \(MGCP\)](#)

Figure 1 Example Topology



FXS-to-FXS Call with Policy Based Routing and DSCP Marking (H.323 and SIP)

The following are CE-1 and CE-2 configuration examples as shown in [Figure 1](#):

- [CE-1 Configuration](#)
- [CE-2 Configuration](#)



Note

Only relevant commands are included in the examples.

CE-1 Configuration

```
!
ip cef
!
interface loopback0
 ip address 10.0.0.1 255.255.255.255
 ip policy route-map VoIP_PBR
 ip route-cache policy
!
ip local policy route-map VoIP_PBR
!
access-list 101 permit udp any any range 16384 32767
access-list 101 permit udp any range 16384 32767 any
access-list 101 permit tcp any any eq 1720
access-list 101 permit tcp any eq 1720 any
!
route-map VoIP_PBR permit 10
 match ip address 101
 <set interface serial0/0 | set ip next-hop ...>
```

```

!
dial-peer voice 1 pots
 destination-pattern 1111
 port 1/0/0
!
dial-peer voice 2 voip
 destination-pattern 4444
 incoming called-number 1111
 session protocol <cisco | sipv2>
 session target ipv4:60.0.0.6
 ip qos dscp af31 signaling
 ip qos dscp ef media
 voice-class source interface loopback0

```

CE-2 Configuration

```

!
ip cef
!
interface loopback0
 ip address 60.0.0.6 255.255.255.255
 ip policy route-map VoIP_PBR
 ip route-cache policy
!
ip local policy route-map VoIP_PBR
!
access-list 101 permit udp any any range 16384 32767
access-list 101 permit udp any range 16384 32767 any
access-list 101 permit tcp any any eq 1720
access-list 101 permit tcp any eq 1720 any
!
route-map VoIP_PBR permit 10
 match ip address 101
 <set interface serial0/0 | set ip next-hop ...>
!
dial-peer voice 1 pots
 destination-pattern 4444
 port 2/0/0
!
dial-peer voice 2 voip
 destination-pattern 1111
 incoming called-number 4444
 session protocol <cisco | sipv2>
 session target ipv4:10.0.0.1
 ip qos dscp af31 signaling
 ip qos dscp ef media
 voice-class source interface loopback0

```

FXS-to-FXS call with Policy Based Routing and DSCP Marking (MGCP)

The following are CE-1 and CE-2 configuration examples as shown in [Figure 1](#):

- [CE-1 Configuration](#)
- [CE-2 Configuration](#)



Note

Only relevant commands are included in the examples.

CE-1 Configuration

```
!  
ip cef  
!  
interface loopback0  
 ip address 10.0.0.1 255.255.255.255  
 ip policy route-map VoIP_PBR  
 ip route-cache policy  
!  
ip local policy route-map VoIP_PBR  
!  
access-list 101 permit udp any any range 16384 32767  
access-list 101 permit udp any range 16384 32767 any  
access-list 101 permit tcp any any eq 1720  
access-list 101 permit tcp any eq 1720 any  
!  
route-map VoIP_PBR permit 10  
 match ip address 101  
 <set interface serial0/0 | set ip next-hop ...>  
!  
mgcp  
mgcp call-agent 1.8.14.11 service-type mgcp version 0.1  
mgcp modem passthrough voip mode ca  
no mgcp timer receive-rtcp  
mgcp ip qos dscp af31 signaling  
mgcp ip qos dscp ef media  
mgcp profile default  
 source interface loopback0  
!  
dial-peer voice 1 pots  
 application mgcpapp  
 port 1/0/0  
!
```

CE-2 Configuration

```
!  
ip cef  
!  
interface loopback0  
 ip address 60.0.0.6 255.255.255.255  
 ip policy route-map VoIP_PBR  
 ip route-cache policy  
!  
ip local policy route-map VoIP_PBR  
!  
access-list 101 permit udp any any range 16384 32767  
access-list 101 permit udp any range 16384 32767 any  
access-list 101 permit tcp any any eq 1720  
access-list 101 permit tcp any eq 1720 any  
!  
route-map VoIP_PBR permit 10  
 match ip address 101  
 <set interface serial0/0 | set ip next-hop ...>  
!  
mgcp  
mgcp call-agent 1.8.14.11 service-type mgcp version 0.1  
mgcp modem passthrough voip mode ca  
mgcp default-package line-package  
no mgcp timer receive-rtcp
```

```
mgcp ip qos dscp af31 signaling
mgcp ip qos dscp ef media
mgcp profile default
  source interface loopback0
!
dial-peer voice 1 pots
  application mgcpapp
  port 2/0/0
!
```

Command Reference

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

New Commands

- [mgcp ip qos dscp](#)
- [source interface](#)
- [voice-class source interface](#)

Modified Commands

- [debug ip policy](#)
- [ip cef](#)

mgcp ip qos dscp

To set the differentiated services code point (DSCP) for the quality of service, use the **mgcp ip qos dscp** command in global configuration mode. To enable the default, use the **no** form of this command.

mgcp ip qos dscp [*number* | *set-af* | *set-cs* | **default** | **ef**] [**media** | **signaling**]

no mgcp ip qos dscp [*number* | *set-af* | *set-cs* | **default** | **ef**] [**media** | **signaling**]

Syntax Description	
<i>number</i>	(Optional) DSCP value. Valid entries are from 0 to 63.
<i>set-af</i>	(Optional) Sets DSCP to assured forwarding bit pattern. <ul style="list-style-type: none"> • af11—Bit pattern 001010 • af12—Bit pattern 001100 • af13—Bit pattern 001110 • af21—Bit pattern 010010 • af22—Bit pattern 010100 • af23—Bit pattern 010110 • af31—Bit pattern 011010 • af32—Bit pattern 011100 • af33—Bit pattern 011110 • af41—Bit pattern 100010 • af42—Bit pattern 100100 • af43—Bit pattern 100110
<i>set-cs</i>	(Optional) Sets DSCP to class-selector codepoint. <ul style="list-style-type: none"> • cs1—Codepoint 1 (precedence 1) • cs2—Codepoint 2 (precedence 2) • cs3—Codepoint 3 (precedence 3) • cs4—Codepoint 4 (precedence 4) • cs5—Codepoint 5 (precedence 5) • cs6—Codepoint 6 (precedence 6) • cs7—Codepoint 7 (precedence 7)
default	(Optional) Sets DSCP to default bit pattern of 000000.
ef	(Optional) Sets DSCP to expedited forwarding bit pattern 101110.
media	(Optional) Applies DSCP to media payload packets.
signaling	(Optional) Applies DSCP to signaling packets.

Defaults

For signaling DSCP is set to bit pattern **af31** for voice **ef**.

Command Modes Global configuration

Command History	Release	Modification
	12.2(11)T	This command was introduced on the following platforms: Cisco IAD2420 series, Cisco 2600 series, Cisco 3620 routers, Cisco 3640routers, Cisco 3660 routers, Cisco 3700 series routers and Cisco MC3810 multiservice access concentrators.

Usage Guidelines To configure voice and signaling traffic priorities for MGCP, use the **mgcp ip qos dscp** command. Recommended values are **mgcp ip qos dscp ef** media and **mgcp ip qos dscp af31** signaling

Examples The following example specifies DSCP is set to precedence 1 and is applied to media payload packets.

```
dial-peer voice 1 voip
mgcp ip qos dscp cs1 media
```

Related Commands	Command	Description
	call rsvp-sync	Enables synchronization between Resource Reservation Protocol (RSVP) signaling and voice signaling protocol.
	ip qos dscp	Sets the DSCP for the quality of service.
	ip rsvp signalling dscp	Specifies the DSCP to be used on all RSVP messages transmitted on an interface.

source interface

To configure the MGCP profile source loopback interface at this interface, use the **source interface** command in MGCP profile configuration mode. To remove the loopback interface, use the **no** form of this command.

source interface loopback *int_name*

no source interface

Syntax Description	loopback	Configures the loopback interface.
	<i>int_name</i>	Defines the name of the loopback interface. Valid entries for <i>int-name</i> are from 0 to 2147483647.

Defaults No loopback is configured.

Command Modes MGCP profile configuration

Command History	Release	Modification
	12.2(11)T	This command was introduced on the following platforms: Cisco IAD2420 series, Cisco 2600 series, Cisco 3620 routers, Cisco 3640routers, Cisco 3660 routers, Cisco 3700 series routers and Cisco MC3810 multiservice access concentrators.

Usage Guidelines To specify a loopback interface to be used for policy-based routing of all media traffic specified by a specific MGCP profile, use the MGCP profile **source interface** command.

Examples The following example shows the loopback configured at the interface designated 0:

```
mgcp profile default
  source interface loopback 0
```

voice-class source interface

To configure the dial peer source interface parameter to loopback, use the **voice-class source interface** command in dial-peer voice configuration mode. To remove the loopback interface, use the **no** form of this command.

voice-class source interface loopback *int-name*

no voice-class source interface

Syntax Description	loopback	Configures the loopback interface.
	<i>int-name</i>	Defines the name of the loopback interface. Valid entries are from 0 through 2147483647.

Defaults No loopback is configured.

Command Modes Dial-peer voice configuration

Command History	Release	Modification
	12.2(11)T	This command was introduced on the following platforms: Cisco IAD2420 series, Cisco 2600 series, Cisco 3620 routers, Cisco 3640routers, Cisco 3660 routers, Cisco 3700 series routers and Cisco MC3810 multiservice access concentrators.

Usage Guidelines To specify a loopback interface to be used for policy-based routing of all media traffic traveling through a specific dial peer, use the dial-peer **voice-class source interface** command.

Examples The following example shows the loopback configured at the interface designated 0:

```
dial-peer voice 1 voip
voice-class source interface loopback 0
```

debug ip policy

To display IP policy routing packet activity, use the **debug ip policy** command in privileged EXEC configuration mode. The **no** form of this command disables debugging output.

debug ip policy [*access-list-name*]

no debug ip policy

Syntax Description	<i>access-list-name</i>
	(Optional) The name of the access list. Displays packets permitted by the access list that are policy routed in process level, CEF, DCEF (with Netflow enabled or disabled). If no access list is specified, information about all policy-matched and policy-routed packets is displayed.

Defaults This command is not enabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(3)T	This command was introduced.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the following platforms: Cisco IAD2420 series, Cisco 2600 series, Cisco 3620 routers, Cisco 3640routers, Cisco 3660 routers, Cisco 3700 series routers and Cisco MC3810 multiservice access concentrators.

Usage Guidelines After you configure IP policy routing with the **ip policy** and **route-map** commands, use the **debug ip policy** command to ensure that the IP policy is configured correctly.

Policy routing looks at various parts of the packet and then routes the packet based on certain user-defined attributes in the packet.

The **debug ip policy** command helps you determine what policy routing is following. It displays information about whether a packet matches the criteria, and if so, the resulting routing information for the packet.



Caution

Because the **debug ip policy** command generates a substantial amount of output, use it only when traffic on the IP network is low, so other activity on the system is not adversely affected.

Examples The following is sample output from the **debug ip policy** command:

```
4d15h:IP:s=6.0.0.6 (local), d=10.0.0.1, len 331, policy match
```

```

4d15h:IP:route map voice, item 10, permit
4d15h:IP:s=6.0.0.6 (Local), d=10.0.0.1 (Serial1/1), len 331, policy
routed
4d15h:IP:local to Serial1/1 10.0.0.1
4d15h:IP:s=6.0.0.6 (Local), d=10.0.0.1, len 40, policy match
4d15h:IP:route map voice, item 10, permit
4d15h:IP:s=6.0.0.6 (Local), d=10.0.0.1 (Serial1/1), len 40, policy
routed
4d15h:IP:local to Serial1/1 10.0.0.1
4d15h:IP:s=6.0.0.6 (Local), d=10.0.0.1, len 40, policy match
4d15h:IP:route map voice, item 10, permit
4d15h:IP:s=6.0.0.6 (Local), d=10.0.0.1 (Serial1/1), len 40, policy
routed
4d15h:IP:local to Serial1/1 10.0.0.1
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1, len 60, FIB policy match
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1 (Serial1/1), len 60, FIB
policy routed
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1, len 60, FIB policy match
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1 (Serial1/1), len 60, FIB
policy routed
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1, len 60, FIB policy match
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1 (Serial1/1), len 60, FIB
policy routed
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1, len 60, FIB policy match
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1 (Serial1/1), len 60, FIB
policy routed
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1, len 60, FIB policy match
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1 (Serial1/1), len 60, FIB
policy routed
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1, len 60, FIB policy match
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1 (Serial1/1), len 60, FIB
policy routed
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1, len 60, FIB policy match
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1 (Serial1/1), len 60, FIB
policy routed
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1, len 60, FIB policy match
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1 (Serial1/1), len 60, FIB
policy routed
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1, len 60, FIB policy match
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1 (Serial1/1), len 60, FIB
policy routed
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1, len 60, FIB policy match
4d15h:IP:s=60.0.0.6 (Loopback0), d=2.0.0.1 (Serial1/1), len 60, FIB
policy routed
.....

```

Table 3 *debug ip policy* Field Description

Field	Description
IP: s=	IP source address and interface of the packet being routed.
d=	IP destination address of the packet being routed.
len	Length of the packet.
g=	IP gateway address of the packet being routed.

ip cef

To enable Cisco Express Forwarding (CEF) on the route processor card, use the **ip cef** command in global configuration mode. To disable CEF, use the **no** form of this command.

ip cef [**accounting** | **load-sharing** | **table type** | **traffic-statistics**]

no ip cef [**accounting** | **load-sharing** | **table type** | **traffic-statistics**]

Syntax Description	
accounting type	(Optional) Enables CEF accounting. The options are as follows: <ul style="list-style-type: none"> - non-recursive—Enables accounting for traffic through non-recursive prefixes. - per-prefix—Enables per prefix accounting. - prefix-length—Enables prefix length accounting.
load -sharing	(Optional) Enables load sharing. <ul style="list-style-type: none"> • algorithm—Per-destination load sharing algorithm selection. The options are as follow: <ul style="list-style-type: none"> - original—Selects the original algorithm. - tunnel—Selects the algorithm for use in tunnel only environments. - universal—Selects the algorithm for use in most environments.
table type	(Optional) Sets CEF forwarding table characteristics. The options are as follows: <ul style="list-style-type: none"> - adjacency-prefix override—Sets adjacency prefixes to override other FIB entries. - consistency-check—Sets consistency checking characteristics. - event-log—Sets table log characteristics. - resolution-timer—Sets background resolution timer. Valid entries are from 0 to 30 seconds. <p>Note Set timer to 0 for automatic exponential back-off scheme.</p>
traffic-statistics	Enables the collection of traffic statistics.

Defaults CEF is disabled by default.

Command Modes Global configuration

Command History	Release	Modification
	11.1 CC	This command was introduced.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the following platforms: Cisco IAD2420 series, Cisco 2600 series, Cisco 3620 routers, Cisco 3640routers, Cisco 3660 routers, Cisco 3700 series routers and Cisco MC3810 multiservice access concentrators.

Usage Guidelines Use the **ip cef** command to control whether voice is switched on the router.

Examples The following example shows ip cef configured for load sharing using the original algorithm:

```
ip cef load-sharing algorithm original
```

Related Commands	Command	Description
	ip cache-route	Controls the use of high-speed switching caches for IP routing.

ip qos dscp

To set the differentiated services code point (DSCP) for the quality of service, use the **ip qos dscp** command in dial-peer configuration mode. To disable DSCP, use the **no** form of this command.

ip qos dscp [*number* | *set-af* | *set-cs* | **default** | **ef**] [**media** | **signaling**]

no ip qos dscp [*number* | *set-af* | *set-cs* | **default** | **ef**] [**media** | **signaling**]

Syntax Description	
<i>number</i>	(Optional) DSCP value. Valid entries are from 0 to 63.
<i>set-af</i>	(Optional) Sets DSCP to assured forwarding bit pattern. <ul style="list-style-type: none"> • af11—Bit pattern 001010 • af12—Bit pattern 001100 • af13—Bit pattern 001110 • af21—Bit pattern 010010 • af22—Bit pattern 010100 • af23—Bit pattern 010110 • af31—Bit pattern 011010 • af32—Bit pattern 011100 • af33—Bit pattern 011110 • af41—Bit pattern 100010 • af42—Bit pattern 100100 • af43—Bit pattern 100110
<i>set-cs</i>	(Optional) Sets DSCP to class-selector codepoint. <ul style="list-style-type: none"> • cs1—Codepoint 1 (precedence 1) • cs2—Codepoint 2 (precedence 2) • cs3—Codepoint 3 (precedence 3) • cs4—Codepoint 4 (precedence 4) • cs5—Codepoint 5 (precedence 5) • cs6—Codepoint 6 (precedence 6) • cs7—Codepoint 7 (precedence 7)
default	(Optional) Sets DSCP to default bit pattern of 000000.
ef	(Optional) Sets DSCP to expedited forwarding bit pattern 101110.
media	(Optional) Applies DSCP to media payload packets.
signaling	(Optional) Applies DSCP to signaling packets.

Defaults

DSCP is set to bit pattern 000000.

Command Modes Dial-peer configuration

Command History	Release	Modification
	12.2(2)T	This command was introduced. It replaced the ip precedence (dial-peer) command.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3700 series routers.

Usage Guidelines To configure voice and signaling traffic priorities for SIP and H.323, use the **ip qos dscp** command. Recommended values are **ip qos dscp ef** media and **ip qos dscp af31** signaling

Examples The following example specifies DSCP is set to precedence 1 and is applied to media payload packets.

```
dial-peer voice 1 voip
 ip qos dscp cs1 media
```

Related Commands	Command	Description
	call rsvp-sync	Enables synchronization between Resource Reservation Protocol (RSVP) signaling and the voice signaling protocol.
	ip rsvp signalling dscp	Specifies the DSCP to be used on all RSVP messages transmitted on an interface.

Glossary

AAL5—ATM adaptation layer 5. One of four AALs recommended by the ITU-T. AAL5 supports connection-oriented VBR services and is used predominantly for the transfer of classical IP over ATM and LANE traffic. AAL5 uses SEAL and is the least complex of the current AAL recommendations. It offers low bandwidth overhead and simpler processing requirements in exchange for reduced bandwidth capacity and error-recovery capability.

BA—

CEF—Cisco Express Forwarding. Layer 3 switching technology. CEF can also refer to central CEF mode, one of the two modes of CEF operation that enables a route processor to perform express forwarding

CQ—customer queue.

CLI—command-line interface. An interface that allows the user to interact with the operating system by entering commands and optional arguments. The UNIX operating system and DOS provide CLIs.

dCEF—Distributed CEF. One of two modes of CEF operation that enables line cards to perform the express forwarding between port adapters.

DSCP—Differentiated Services Code Point. An IP packet classification mechanism

DSP—digital signal processor. A DSP segments the voice signal into frames and stores them in voice packets.

FIB—Forwarding Information Base. A component of CEF. It is the lookup table the router uses to make destination-based switching decisions during CEF operation. It maintains a mirror image of the forwarding information stored in the IP routing table.

IVR—interactive voice response. Term used to describe systems that provide information in the form of recorded messages over telephone lines in response to user input in the form of spoken words or, more commonly, DTMF signaling. Examples include banks that allow you to check your balance from any telephone and automated stock quote systems.

MGCP—Media Gateway Control Protocol. A merging of the IPDC and SGCP protocols.

MPLS—Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

PBR—policy based routing. Routing scheme that forwards packets to specific interfaces based on user-configured policies. Such policies might specify that traffic sent from a particular network should be forwarded out one interface, and all other traffic should be forwarded out another interface.

PQ—priority queue. Routing feature in which frames in an output queue are prioritized based on various characteristics, such as packet size and interface type.

VoIP—Voice over IP. The capability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323.

WAN—wide-area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs

WFQ—weighted fair queuing. Congestion management algorithm that identifies conversations (in the form of traffic streams), separates packets that belong to each conversation, and ensures that capacity is shared fairly between these individual conversations. WFQ is an automatic way of stabilizing network behavior during congestion and results in increased performance and reduced retransmission.