

Configuring DSCP Policing and Media Bandwidth Policing

This module explains the following features:

- AS SIP—DSCP Policing
- AS SIP—Media Bandwidth Policing

The Assured Services over Session Initiation Protocol Differentiated Services Code Point (AS SIP—DSCP Policing) Policing and the AS SIP—Media Bandwidth Policing feature adds the media policy functionality to the Cisco Unified Border Element (Cisco UBE) on a per-call basis to control the bandwidth. Real Time Protocol (RTP) packets are dropped, and MIB and system logs are generated if there is any DSCP policy, marking, and media bandwidth profiling violation.

- Feature Information for Configuring DSCP Policing and Media Bandwidth Policing, on page 1
- Restrictions for Configuring DSCP Policing and Media Bandwidth Policing, on page 2
- Information About Configuring DSCP Policing and Media Bandwidth Policing, on page 3
- How to Configure DSCP Policing and Media Bandwidth Policing Features, on page 4
- Configuration Examples for Configuring DSCP Policing and Media Bandwidth Policing, on page 24
- Additional References, on page 26

Feature Information for Configuring DSCP Policing and Media Bandwidth Policing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

Table 1: Feature Information for Configuring DSCP Policing and Media Bandwidth Policing

Feature Name	Releases	Feature Information
AS SIP—DSCP Policing	15.2(2)T	The AS SIP—DSCP Policing feature provides the following functionalities: • A mechanism to map the RPH to the DSCP values in the IP header for audio and video calls. • A policy to match DSCP values of incoming media calls to the preconfigured value and take an action depending upon the configuration. The following commands were introduced or modified: **dscp media**, **dscp-profile**, **snmp enable peer-trap**, **snmp-server enable traps voice (dscp profile)**, **violation**, **voice-class sip resource priority dscp-profile**.
AS SIP—Media Bandwidth Policing	15.2(2)T	The AS SIP—Media Bandwidth Policing feature introduces traffic policing on the Cisco UBE to limit media bandwidth usage to the negotiated rate. Excess traffic is dropped when the traffic rate reaches the configured maximum value. The following commands were introduced or modified: **media police-profile**, **media profile police**, **overhead**, **police profile**, **violation (media profile)**.

Restrictions for Configuring DSCP Policing and Media Bandwidth Policing

Following are the restrictions for the AS SIP—DSCP Policing feature:

- The Session Description Protocol (SDP) pass-through feature along with Resource Priority Header (RPH) to DSCP marking and policing are not supported.

- High availability (HA) is not supported.

Following are the restrictions for the AS SIP—Media Bandwidth Policing feature:

- The SDP pass-through feature along with the Media Bandwidth Policing feature are not supported.
- Flow-around cases are not applicable to the Media Bandwidth Policing feature.
- HA is not supported.

Information About Configuring DSCP Policing and Media Bandwidth Policing

AS SIP—DSCP Policing

The AS SIP—DSCP Policing feature provides the following functionalities:

- A mechanism to map the RPH to the DSCP values in the IP header for audio and video calls.
- A policy to match DSCP values of incoming media calls to the preconfigured value and take an action depending upon the configuration.

You must map RPH to DSCP values to provide priority and precedence for VoIP calls at all layers. DSCP policing and marking are supported as part of the AS SIP—DSCP Policing feature for RTP media. The DSCP policing functionality checks DSCP values for media packets (RTP) and informs incorrect marking of DSCP values. The DSCP marking functionality marks packets with the correct DSCP value as per the SIP RPH.

The AS SIP—DSCP Policing feature supports two new namespaces, UC and CUC. The namespace support is enabled by default and no configuration is required. Asymmetric call leg configuration is also supported: that is, you can have the RPH pass-through configuration on one call leg and RPH to DSCP policing on the another.

AS SIP—Media Bandwidth Policing

In releases prior to Cisco IOS Release 15.2(2)T, Cisco UBE does not support media on a policing per-call basis. Hence, few endpoints negotiate the G729 codec using the SIP offer answer model and send RTP packets with the payload of G711. Few endpoints negotiate with G729 10 ms (one packet per 10 ms) but send two packets as a response to the request of 10 ms. In both cases, more bandwidth than the negotiated bandwidth is used. Cisco UBE has no mechanism to detect bandwidth violation and enforce policing on media policing approaches.

To overcome this problem, the AS SIP—Media Bandwidth Policing feature was introduced in Cisco IOS Release 15.2(2)T. This feature introduces traffic policing on the Cisco UBE to limit media bandwidth usage to the negotiated rate. Excess traffic is dropped when the traffic rate reaches the configured maximum value. The AS SIP—Media Bandwidth Policing feature is supported only on RTP packets.

The AS SIP—Media Bandwidth Policing feature identifies violations in the bandwidth and triggers the following policing actions on additional RTP packets received:

- Drops all violated packets.

- Drops all violated packets and disconnects the call once it reaches the configured number of violations.
- Ignores the violations.

You can enable system log and Simple Network Management Protocol (SNMP) trap generations to inform system administrators about policing violations.

Resource Priority Header

RPH is a SIP header. A SIP request with a RPH is treated as follows:

- The request is given an elevated priority to access public switched telephone network (PSTN) gateway resources, such as trunk circuits.
- The request can interrupt lower priority requests at a user terminal, such as an IP phone.
- The request can carry information from one multilevel priority domain in a telephone network to another, without SIP proxies inspecting or modifying the header field.
- In SIP proxies and back-to-back user agents, requests of higher priorities can displace the existing signaling requests or bypass the PSTN gateway capacity limits in effect for lower priorities.

This RPH header provides priority and precedence at Layer 7. It is not treated the same way in lower layers.

Differentiated Services Code Point

DSCP or differentiated services code point (DiffServ) is a computer networking architecture that specifies a simple, scalable, and coarse-grained mechanism for classifying and managing network traffic, and providing quality of service (QoS) on modern IP networks.

How to Configure DSCP Policing and Media Bandwidth Policing Features

Configuring AS SIP—DSCP Policing Feature at the Global Level

Perform this task to configure the AS SIP—DSCP Policing feature at the global level, that is on all dial peers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class dscp-profile** *tag*
4. **dscp media** {**audio** | **video**} {**flah-override-override** | **flash-override** | **flsh** | **immediate** | **priority** | **routine**} {*dscp-value* | *set-af* | *set-cf* | **ef** | **zero**}
5. **violation** *number* **action** {**disconnect** | **ignore**} [**no-syslog**]
6. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice class dscp-profile** *tag* **Example:** `Router(config)# voice class dscp-profile 1`	Configures a DSCP profile and enters voice class configuration mode.
Step 4	**dscp media** {**audio** | **video**} {**flah-override-override** | **flash-override** | **flsh** | **immediate** | **priority** | **routine**} {*dscp-value* | *set-af* | *set-cf* | **ef** | **zero**} **Example:** `Router(config-class)# dscp media audio routine ef`	Specifies the RPH to DSCP mapping.
Step 5	**violation** *number* **action** {**disconnect** | **ignore**} [**no-syslog**] **Example:** `Router(config-class)# violation 20000 action ignore`	Specifies the action that needs to be performed on any violation in the DSCP policy.
Step 6	**end** **Example:** `Router(config-class)# end`	Exits voice class configuration mode and enters privileged EXEC mode.

Applying the DSCP Policing Profile at the Global Level

Perform this task to apply the DSCP policing profile at the global level, that is to apply the profile to all dial peers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **dscp-profile** *tag*
6. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service configuration mode.
Step 4	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters service SIP configuration mode.
Step 5	**dscp-profile** *tag* **Example:** `Router(conf-serv-sip)# dscp-profile 1`	Applies a DSCP policing profile at the global level. • If a DSCP policy is applied globally and to a dial peer, the dial peer configuration takes precedence over the global configuration.
Step 6	**end** **Example:** `Router(conf-serv-sip)# end`	Exits service SIP configuration mode and enters privileged EXEC mode.

Applying the DSCP Policing Profile at the Dial Peer Level

Perform this task to apply the DSCP policing profile at the dial peer level.

When the DSCP policing profile is applied to a dial peer and the mode is configured as RPH pass-through, the policy will be enforced if there is any match for the “r-priority” value in the RPH. If there is no match in the namespace, the domain name system (DNS) will be used to match the “r-priority”.

If the RPH pass-through mode is configured, the RPH is passed as it is. The RPH is truncated if the following values are above the specified limits:

- Only the namespace is changed and there is no change in the subdomain and priority.
- Maximum namespace allowed is up to ten characters.
- Maximum subdomains supported range is from 000000 to FFFFFF.
- Maximum priority values allowed are 24 characters.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* {**pots** | **voatm** | **vofr** | **voip**}
4. **voice-class sip resource priority dscp-profile** *tag*
5. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* {**pots**	**voatm**	**vofr**	**voip**} **Example:** `Router(config)# dial-peer voice 4 voip`	Enters dial peer voice configuration mode.

	Command or Action	Purpose
Step 4	**voice-class sip resource priority dscp-profile** *tag* **Example:** `Router(config-dial-peer)# voice-class sip resource priority dscp-profile 1`	Applies a DSCP profile parameter. • If a DSCP policy is applied globally and to a dial peer, the dial peer configuration takes precedence over the global configuration.
Step 5	**end** **Example:** `Router(config-dial-peer)# end`	Exits dial peer configuration mode.

Enabling the SNMP Trap for the DSCP Policing Feature at the Global Level

Perform this task to enable the SNMP trap for the DSCP Policing feature at the global level, that is on all dial peers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps voice** [**dscp-profile**] [**fallback**] [**high-ds0-util**] [**low-ds0-util**] [**media-policy**]
4. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps voice** [**dscp-profile**] [**fallback**] [**high-ds0-util**] [**low-ds0-util**] [**media-policy**] **Example:** `Router(config)# snmp-server enable traps voice dscp-profile`	Enables SNMP DSCP profile voice notifications.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

Enabling the SNMP Trap for the DSCP Policing Feature at the Dial Peer Level

Perform this task to enable the SNMP trap for the DSCP policing feature for a specific dial peer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **snmp enable peer-trap dscp-profile**
5. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 1 voip`	Enters dial peer voice configuration mode.
Step 4	**snmp enable peer-trap dscp-profile** **Example:** `Router(config-dial-peer)# snmp enable peer-trap dscp-profile`	Enables DSCP profile violation traps.
Step 5	**end** **Example:**	Exits dial peer configuration mode and enters privileged EXEC mode.

	Command or Action	Purpose
	Router(config-dial-peer)# end	

Verifying the AS SIP-DSCP Policing Feature

Perform this task to verify the configuration for AS SIP-DSCP Policing feature on Cisco UBE. The **show** commands need not be entered in any specific order.

SUMMARY STEPS

1. **enable**
2. **show ip interface brief**
3. **show call active voice brief**

DETAILED STEPS

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

Step 2 **show ip interface brief**

Example:

```
Router# show ip interface brief

Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         10.0.35.11      YES manual up                    up
GigabitEthernet0/1         10.1.3.3        YES NVRAM  administratively down down
```

Displays a brief summary of an interface's IP information and status.

Step 3 **show call active voice brief**

Example:

```
Router# show call active voice brief

<ID>: <CallID> <start>.<index> +<connect> pid:<peer_id> <dir> <addr> <state>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> dscp:<packets violation> media:<packets
violation>
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec> <textrelay> <transcoded

 media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>

 long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
  MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
```

```
  last <buf event time>s dur:<Min>/<Max>s
 FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm
  MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
         speeds(bps): local <rx>/<tx> remote <rx>/<tx>
 Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
 bw: <req>/<act> codec: <audio>/<video>
  tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
 rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>


Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
0    : 21 23:08:52.157 IST Tue Jul 12 2011.1 +8900 pid:3 Answer 1000 active
 dur 00:00:56 tx:2766/442560 rx:2811/449760 dscp:2814 media:0
 IP 9.44.46.21:20332 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: No
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a

0    : 22 23:08:52.707 IST Tue Jul 12 2011.1 +7780 pid:4 Originate 2000 active
 dur 00:00:57 tx:2811/449760 rx:2766/442560 dscp:2767 media:0
 IP 9.44.46.25:31290 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: No
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a


Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
```

Displays call information for voice calls in progress.

Configuring the AS SIP—Media Bandwidth Policing Profile at the Global Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media profile police** *tag*
4. **violation** *number* **action** {**disconnect** | **drop** | **ignore**} [**no-syslog**]
5. **overhead** {**audio** | **video**} *percentage*

6. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**media profile police** *tag* **Example:** `Router(config)# media profile police 1`	Configures the media bandwidth policing profile at the global level and enters media profile configuration mode.
Step 4	**violation** *number* **action** {**disconnect** | **drop** | **ignore**} [**no-syslog**] **Example:** `Router(cfg-mediaprofile)# violation 20000 action drop no-syslog`	Specifies the number of violations after which the action needs to be taken. • Use the **no-syslog** keyword to configure the Cisco UBE to disable the system log.
Step 5	**overhead** {**audio** | **video**} *percentage* **Example:** `Router(cfg-mediaprofile)# overhead audio 10`	Configures the overhead bandwidth percentage above the negotiated bandwidth.
Step 6	**end** **Example:** `Router(cfg-mediaprofile)# end`	Exits media profile configuration mode and enters privileged EXEC mode.

Applying the Media Bandwidth Policing Profile at the Global Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **media police-profile** *tag*

5. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service configuration mode.
Step 4	**media police-profile** *tag* **Example:** `Router(conf-voi-serv)# media police-profile 1`	Applies the media bandwidth policing profile at the global level.
Step 5	**end** **Example:** `Router(conf-voi-serv)# end`	Exits voice service configuration mode and enters privileged EXEC mode.

Applying the Media Bandwidth Policing Profile at the Dial Peer Level

Applying the media bandwidth policing profile at the dial peer level involves two actions: applying the profile for a media class and then applying the corresponding media class to a dial peer.

Perform this task to apply the media bandwidth policing profile at the dial peer level.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media class** *tag*
4. **police profile** *tag*
5. **exit**
6. **dial-peer voice** *tag* **voip**

7. **media-class** *tag*
8. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**media class** *tag* **Example:** `Router(config)# media class 1`	Configures a media class and enters media class configuration mode.
Step 4	**police profile** *tag* **Example:** `Router(cfg-mediaclass)# police profile 1`	Applies the media bandwidth policing profile to the media class.
Step 5	**exit** **Example:** `Router(cfg-mediaclass)# exit`	Exits media class configuration mode and enters global configuration mode.
Step 6	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 1 voip`	Enters dial peer voice configuration mode.
Step 7	**media-class** *tag* **Example:** `Router(config-dial-peer)# media-class 1`	Applies the media class at the dial peer level.
Step 8	**end** **Example:** `Router(config-dial-peer)# end`	Exits dial peer voice configuration mode and enters privileged EXEC mode.

Enabling SNMP Traps for the Media Bandwidth Policing Feature at the Global Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps voice media-policy**
4. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps voice media-policy** **Example:** `Router(config)# snmp-server enable traps voice media-policy`	Enables SNMP media policy voice traps at the global level.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

Enabling SNMP Traps for the Media Bandwidth Policing Feature at the Dial Peer Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **snmp enable peer-trap media-policy**

5. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 4 voip`	Enters dial peer voice configuration mode.
Step 4	**snmp enable peer-trap media-policy** **Example:** `Router(config-dial-peer)# snmp enable peer-trap media-policy`	Enables SNMP media policy voice traps at the dial peer level.
Step 5	**end** **Example:** `Router(config-dial-peer)# end`	Exits dial peer configuration mode and enters privileged EXEC mode.

Verifying the AS SIP-Media Bandwidth Policing Profile Feature

Perform this task to verify the configuration for AS SIP-Media Bandwidth Policing Profile feature on Cisco UBE. The **show** commands need not be entered in any specific order.

SUMMARY STEPS

1. **enable**
2. **show call history voice brief**
3. **show call history voice stats**
4. **show call history voice stats**
5. **show call history video brief**
6. **show call history video stats**
7. **show call active voice brief**

8. **show call active voice stats**
9. **show call active video brief**
10. **show call history video stats**
11. **show dial-peer voice**

DETAILED STEPS

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

Step 2 **show call history voice brief**

Example:

```
Router# show call history voice brief

<ID>: <CallID> <start>ms.<index> (<start>) +<connect> +<disc> pid:<peer_id> <direction> <addr>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>) dscp:<packets violation>
 media:<packets violation> audio tos:<audio tos value> video tos:<video tos value>
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>  <textrelay> <transcoded>

 media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>

 long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
  MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
   last <buf event time>s dur:<Min>/<Max>s
 FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 Telephony <int> (callID) [channel_id] tx:<tot>/<voice>/<fax>ms <codec> noise:<lvl>dBm acom:<lvl>dBm

  MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops> disc:<cause
 code>
             speeds(bps): local <rx>/<tx> remote <rx>/<tx>
 Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
 bw: <req>/<act> codec: <audio>/<video>
  tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
 rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>



Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
Total call-legs: 0
```

Displays a truncated version of the call history table for voice calls.

Step 3 **show call history voice stats**

Example:

```
Router# show call history voice stats

<ID>: <CallID> <start>ms.<index> (<start>) +<connect> +<disc> pid:<peer_id> <direction> <addr>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>) dscp:<packets violation>
 media:<packets violation> audio tos:<audio tos value> video tos:<video tos value>
DSP/TX: PK=, SG=, NS=, DU=, VO=
DSP/RX: PK=, SG=, CF=, RX=, VO=, BS=, BP=, LP=, EP=
DSP/PD: CU=, MI=, MA=, CO=, IJ=
DSP/PE: PC=, IC=, SC=, RM=, BO=, EE=
DSP/LE: TP=, TX=, RP=, RM=, BN=, ER=, AC=
DSP/ER: RD=, TD=, RC=, TC=
DSP/IC: IC=

DSP/EC: CI=, FM=, FP=, VS=, GT=, GR=, JD=, JN=, JM=, JX=
DSP/KF: KF=, AV=, MI=, BS=, NB=, FL=, NW=, VR=
DSP/CS: CR=, AV=, MX=, CT=, TT=, OK=, CS=, SC=, TS=, DC=
DSP/RF: ML=, MC=, R1=, R2=, IF=, ID=, IE=, BL=, R0=, VR=
DSP/UC: U1=, U2=, T1=, T2=
DSP/DL: RT=, ED=

MIC Direction:

DSP/NR: NR=, ND=, LV=, IN=
DSP/AS: AE=, AD=, AM=, AV=, NT=, DT=, TT=, TD=, LF=, LD=
EAR Direction:

DSP/NR: NR=, ND=, LV=, IN=
DSP/AS: AE=, AD=, AM=, AV=, NT=, DT=, TT=, TD=, LF=, LD=

Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
Total call-legs: 0
```

Displays the call history table for voice calls.

Step 4 **show call history voice stats**

Example:

```
Router#  show call history voice stats

<ID>: <CallID> <start>ms.<index> (<start>) +<connect> +<disc> pid:<peer_id> <direction> <addr>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>) dscp:<packets violation>
 media:<packets violation> audio tos:<audio tos value> video tos:<video tos value>
DSP/TX: PK=, SG=, NS=, DU=, VO=
DSP/RX: PK=, SG=, CF=, RX=, VO=, BS=, BP=, LP=, EP=
DSP/PD: CU=, MI=, MA=, CO=, IJ=
DSP/PE: PC=, IC=, SC=, RM=, BO=, EE=
DSP/LE: TP=, TX=, RP=, RM=, BN=, ER=, AC=
DSP/ER: RD=, TD=, RC=, TC=
DSP/IC: IC=

DSP/EC: CI=, FM=, FP=, VS=, GT=, GR=, JD=, JN=, JM=, JX=
DSP/KF: KF=, AV=, MI=, BS=, NB=, FL=, NW=, VR=
DSP/CS: CR=, AV=, MX=, CT=, TT=, OK=, CS=, SC=, TS=, DC=
DSP/RF: ML=, MC=, R1=, R2=, IF=, ID=, IE=, BL=, R0=, VR=
DSP/UC: U1=, U2=, T1=, T2=
DSP/DL: RT=, ED=
```

```
MIC Direction:

DSP/NR: NR=, ND=, LV=, IN=
DSP/AS: AE=, AD=, AM=, AV=, NT=, DT=, TT=, TD=, LF=, LD=
EAR Direction:

DSP/NR: NR=, ND=, LV=, IN=
DSP/AS: AE=, AD=, AM=, AV=, NT=, DT=, TT=, TD=, LF=, LD=

Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
Total call-legs: 0
```

Displays information about digital signal processing (DSP) voice quality metrics.

Step 5 **show call history video brief**

Example:

```
Router# show call history video brief

<ID>: <CallID> <start>ms.<index> (<start>) +<connect> +<disc> pid:<peer_id> <direction> <addr>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>) dscp:<packets violation>
 media:<packets violation> audio tos:<audio tos value> video tos:<video tos value>
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>  <textrelay> <transcoded>

 media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>

 long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
  MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
   last <buf event time>s dur:<Min>/<Max>s
 FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 Telephony <int> (callID) [channel_id] tx:<tot>/<voice>/<fax>ms <codec> noise:<lvl>dBm acom:<lvl>dBm

   video: h320:<call type> tx:<video codec> <video pkts>/<video bytes> rx:<video codec> <video
pkts>/<video bytes>
  MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops> disc:<cause
 code>
             speeds(bps): local <rx>/<tx> remote <rx>/<tx>
 Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
 bw: <req>/<act> codec: <audio>/<video>
  tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
 rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>

Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
Total call-legs: 0
```

Displays a truncated version of video call history information.

Step 6 **show call history video stats**

Example:

```
Router# show call history video stats

<ID>: <CallID> <start>ms.<index> (<start>) +<connect> +<disc> pid:<peer_id> <direction> <addr>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>) dscp:<packets violation>
 media:<packets violation> audio tos:<audio tos value> video tos:<video tos value>
Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
Total call-legs: 0
```

Displays call history information for signaling connection control protocol (SCCP) video calls.

Step 7 **show call active voice brief**

Example:

```
Router# show call active voice brief

<ID>: <CallID> <start>ms.<index> (<start>) +<connect> pid:<peer_id> <dir> <addr> <state>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> dscp:<packets violation> media:<packets
violation> audio tos:<audio tos value> video tos:<video tos value>
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec> <textrelay> <transcoded

 media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>

 long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
  MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
   last <buf event time>s dur:<Min>/<Max>s
 FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm
  MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
         speeds(bps): local <rx>/<tx> remote <rx>/<tx>
 Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
 bw: <req>/<act> codec: <audio>/<video>
  tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
 rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
```

Step 8 **show call active voice stats**

Example:

```
Router# show call active voice stats

<ID>: <CallID> <start>ms.<index> (<start>) +<connect> +<disc> pid:<peer_id> <direction> <addr>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> dscp:<packets violation> audio tos:<audio
 tos value> video tos:<video tos value>

DSP/TX: PK=, SG=, NS=, DU=, VO=
DSP/RX: PK=, SG=, CF=, RX=, VO=, BS=, BP=, LP=, EP=
DSP/PD: CU=, MI=, MA=, CO=, IJ=
DSP/PE: PC=, IC=, SC=, RM=, BO=, EE=
DSP/LE: TP=, TX=, RP=, RM=, BN=, ER=, AC=
DSP/ER: RD=, TD=, RC=, TC=
DSP/IC: IC=

DSP/EC: CI=, FM=, FP=, VS=, GT=, GR=, JD=, JN=, JM=, JX=
DSP/KF: KF=, AV=, MI=, BS=, NB=, FL=, NW=, VR=
DSP/CS: CR=, AV=, MX=, CT=, TT=, OK=, CS=, SC=, TS=, DC=
```

```
DSP/RF: ML=, MC=, R1=, R2=, IF=, ID=, IE=, BL=, R0=, VR=
DSP/UC: U1=, U2=, T1=, T2=
DSP/DL: RT=, ED=

MIC Direction:

DSP/NR: NR=, ND=, LV=, IN=
DSP/AS: AE=, AD=, AM=, AV=, NT=, DT=, TT=, TD=, LF=, LD=
EAR Direction:

DSP/NR: NR=, ND=, LV=, IN=
DSP/AS: AE=, AD=, AM=, AV=, NT=, DT=, TT=, TD=, LF=, LD=

Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 0
```

Displays information about DSP voice quality metrics.

Step 9 **show call active video brief**

Example:

```
Router# show call active video brief

<ID>: <CallID> <start>ms.<index> (<start>) +<connect> pid:<peer_id> <dir> <addr> <state>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> dscp:<packets violation> media:<packets
violation> audio tos:<audio tos value> video tos:<video tos value>
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec> <textrelay> <transcoded

 media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>

 long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
  MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
   last <buf event time>s dur:<Min>/<Max>s
 FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm
  video: h320:<type> tx:<video codec> <video pkts>/<video bytes> rx:<video codec> <video pkts>/<video
 bytes>
  MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
         speeds(bps): local <rx>/<tx> remote <rx>/<tx>
 Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
 bw: <req>/<act> codec: <audio>/<video>
  tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
 rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
```

Displays a truncated version of active video call information.

Step 10 **show call history video stats**

Example:

```
Router# show call history video stats

<ID>: <CallID> <start>ms.<index> (<start>) +<connect> +<disc> pid:<peer_id> <direction> <addr>
```

```
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>) dscp:<packets violation>
 media:<packets violation> audio tos:<audio tos value> video tos:<video tos value>
Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
Total call-legs: 0
```

Displays call history information for SCCP video calls.

Step 11 **show dial-peer voice**

Example:

```
Router# show dial-peer voice

VoiceOverIpPeer565656
        peer type = voice, system default peer = FALSE, information type = voice,
        description = `',
        tag = 565656, destination-pattern = `',
        voice reg type = 0, corresponding tag = 0,
        allow watch = FALSE
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
        CLID Override RDNIS = disabled,
        rtp-ssrc mux = system
        source carrier-id = `', target carrier-id = `',
        source trunk-group-label = `',  target trunk-group-label = `',
        numbering Type = `unknown'
        group = 565656, Admin state is up, Operation state is down,
        incoming called-number = `', connections/maximum = 0/unlimited,
        bandwidth/maximum = 0/unlimited,
        DTMF Relay = disabled,
        modem transport = system,
        URI classes:
            Incoming (Request) =
            Incoming (Via) =
            Incoming (To) =
            Incoming (From) =
            Destination =
        huntstop = disabled,
        in bound application associated: 'DEFAULT'
        out bound application associated: ''
        dnis-map =
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        outgoing LPCOR:
        Translation profile (Incoming):
        Translation profile (Outgoing):
        incoming call blocking:
        translation-profile = `'
        disconnect-cause = `no-service'
        advertise 0x40 capacity_update_timer 25 addrFamily 4 oldAddrFamily 4
        mailbox selection policy: none
        type = voip, session-target = `',
        technology prefix:
        settle-call = disabled
        ip media DSCP = ef, ip media rsvp-pass DSCP = ef
        ip media rsvp-fail DSCP = ef, ip signaling DSCP = af31,
        ip video rsvp-none DSCP = af41,ip video rsvp-pass DSCP = af41
        ip video rsvp-fail DSCP = af41,
```

```
ip defending Priority = 0, ip preemption priority = 0
ip policy locator voice:
ip policy locator video:
UDP checksum = disabled,
session-protocol = sipv2, session-transport = system,
req-qos = best-effort, acc-qos = best-effort,
req-qos video = best-effort, acc-qos video = best-effort,
req-qos audio def bandwidth = 64, req-qos audio max bandwidth = 0,
req-qos video def bandwidth = 384, req-qos video max bandwidth = 0,
RTP dynamic payload type values: NTE = 101
Cisco: NSE=100, fax=96, fax-ack=97, dtmf=121, fax-relay=122
       CAS=123, TTY=119, ClearChan=125, PCM switch over u-law=0,
       A-law=8, GSMAMR-NB=117 iLBC=116, AAC-ld=114, iSAC=124
       lmr_tone=0, nte_tone=0
       h263+=118, h264=119
       G726r16 using static payload
       G726r24 using static payload
RTP comfort noise payload type = 19
fax rate = voice,   payload size =  20 bytes
fax protocol = system
fax-relay ecm enable
Fax Relay ans enabled
Fax Relay SG3-to-G3 Enabled (by system configuration)
fax NSF = 0xAD0051 (default)
codec = g729r8,   payload size =  20 bytes,
video codec = None
voice class codec = `'
voice class sip session refresh system
voice class sip rsvp-fail-policy voice post-alert mandatory keep-alive interval 30
voice class sip rsvp-fail-policy voice post-alert optional keep-alive interval 30
voice class sip rsvp-fail-policy video post-alert mandatory keep-alive interval 30
voice class sip rsvp-fail-policy video post-alert optional keep-alive interval 30
text relay = disabled
Media Setting = forking (disabled) flow-through (global)stats-disconnect (disabled)
Expect factor = 10, Icpif = 20,
Playout Mode is set to adaptive,
Initial 60 ms, Max 1000 ms
Playout-delay Minimum mode is set to default, value 40 ms
Fax nominal 300 ms
Max Redirects = 1, signaling-type = cas,
VAD = enabled, Poor QOV Trap = disabled,
Source Interface = NONE
voice class sip url = system,
voice class sip tel-config url = system,
voice class sip rel1xx = system,
voice class sip anat = system,
voice class sip outbound-proxy = "system",
voice class sip associate registered-number = system,
voice class sip asserted-id system,
voice class sip privacy system
voice class sip e911 = system,
voice class sip history-info = system,
voice class sip reset timer expires 183 = system,
voice class sip pass-thru headers = system,
voice class sip pass-thru content unsupp = system,
voice class sip pass-thru content sdp = system,
voice class sip copy-list = system,
voice class sip g729 annexb-all = system,
voice class sip early-offer forced = system,
voice calss sip delay-offer forced = disable,
voice class sip negotiate cisco = system,
voice class sip block 180 = system,
voice class sip block 183 = system,
voice class sip block 181 = system,
```

```
voice class sip preloaded-route = system,
voice class sip random-contact = system,
voice class sip random-request-uri validate = system,
voice class sip call-route p-called-party-id = system,
voice class sip call-route history-info = system,
voice class sip call-route url = system,
voice class sip privacy-policy send-always = system,
voice class sip privacy-policy passthru = system,
voice class sip privacy-policy strip history-info = system,
voice class sip privacy-policy strip diversion = system,
voice class sip map resp-code 181 = system,
voice class sip bind control = system,
voice class sip bind media = system,
voice class sip bandwidth audio = system,
voice class sip bandwidth video = system,
voice class sip encap clear-channel = system,
voice class sip error-code-override options-keepalive failure = system,
voice class sip error-code-override cac-bandwidth failure = 488
voice class sip calltype-video = false
voice class sip registration passthrough = System
voice class sip authenticate redirecting-number  = system,
voice class sip referto-passing = system,
redirect ip2ip = disabled
local peer = false
probe disabled,
Secure RTP: system (use the global setting)
mobility=0, snr=, snr_noan=, snr_delay=0, snr_timeout=0
snr calling-number local=disabled, snr ring-stop=disabled, snr answer-too-soon timer=0
voice class perm tag = `'
Time elapsed since last clearing of voice call statistics never
Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Bandwidth CAC Accepted Calls = 0, Bandwidth CAC Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
Last Disconnect Time = 0.
```

Displays information for voice dial peers.

Configuration Examples for Configuring DSCP Policing and Media Bandwidth Policing

Example: Configuring the AS SIP—DSCP Policing Feature at the Global Level

The following example shows how to configure the AS SIP—DSCP Policing feature on the Cisco UBE when the incoming invite is an RPH invite:

```
Router(config)# voice class dscp-profile 1
Router(config-class)# dscp media audio priority 11
Router(config-class)# dscp media audio flsh af11

Router(config)# voice class dscp-profile 2
```

```
Router(config-class)# dscp media audio priority 60
Router(config-class)# dscp media audio flash-override af11

Router(config)# voice class dscp-profile 3
Router(config-class)# violation 10 action disconnect

Router(config)# voice class dscp-profile 4
Router(config-class)# dscp media audio immediate 2
Router(config-class)# dscp media audio flsh 63
Router(config-class)# dscp media audio flash-override af33

Router(config)# voice class dscp-profile 5
Router(config-class)# dscp media audio immediate 1
```

Example: Applying DSCP Policing

The following example shows how to apply DSCP policing globally and at the dial peer level:



Note The dial peer configuration will have precedence over the global configuration.

```
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# dscp-profile 2

Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# session protocol sipv2
Router(config-dial-peer)# voice-class sip resource priority dscp-profile 1
```

Example: Configuring the AS SIP—Media Bandwidth Policing Profile at the Global Level

```
Router(config)# media profile police 1
Router(cfg-mediaprofile)# violation 20000 action disconnect no-syslog
Router(cfg-mediaprofile)# overhead audio 15
```

Example: Applying the Media Bandwidth Policing Profile

The following example shows how to apply the media bandwidth policing profile globally and at the dial peer level:

```
Router(config)# voice service voip
Router(conf-voi-serv)# media police-profile 1

Router(config)# media class 1
Router(cfg-mediaclass)# police profile 1
Router(cfg-mediaclass)# end
Router# configure terminal
```

```
Router(config)# dial-peer voice 4 voip
Router(config-dial-peer)# media-class 1
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
Cisco IOS voice commands	• *Cisco IOS Voice Command Reference - A through C* • *Cisco IOS Voice Command Reference - D through I* • *Cisco IOS Voice Command Reference - K through R* • *Cisco IOS Voice Command Reference - S Commands* • *Cisco IOS Voice Command Reference - T through Z*
Modular quality of service CLI overview	*Modular Quality of Service Command-Line Interface Overview*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html