Call Admission Control

Overview

The Call Admission Control feature enables you to control the audio quality and video quality of calls over a wide-area (IP WAN) link by limiting the number of calls that are allowed on that link at the same time. Audio and video quality can begin to degrade when too many active calls exist on a link and the amount of bandwidth is oversubscribed. Call Admission Control regulates audio and video quality by limiting the number of calls that can be active on a particular link at the same time.

The Call Admission Control feature controls number of calls based on resources and bandwidth, proactively reserve resources for good quality video calls, ensures that traffic adheres to QoS policies within each network.

Cisco Unified Border Element (CUBE) provides different CAC mechanisms that are based on:

- Total Calls, CPU, or Memory
- Call Spike Detection
- Maximum Calls per Destination
- Dial-peer or Interface Bandwidth

Feature Information

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Bandwidth-Based Call Admission Control

Feature Name	Releases	Feature Information
Bandwidth-Based Call Admission Control	Baseline Feature	The following commands were introduced or modified: **call threshold interface**, **error-code-override**, **max-bandwidth**, **show call threshold**, **voice-class sip**

Configure CAC Based on Total Calls, CPU or Memory

The Call Admission Control (CAC) based on CPU Utilization feature permits the Cisco Voice Gateways to deny incoming calls exceeding a pre-configured threshold, permitting the selection of a system CPU load level value.

The '**Call Threshold**' command allows you to configure two thresholds, high and low. The 'Call Treatment' is triggered when the current value of a resource goes beyond the configured high value. The 'Call Treatment' remains in effect until the current resource value falls below the configured low value.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call threshold global [cpu-5sec | cpu-avg | io-mem | proc-mem | total-calls | total-mem] low** *low-threshold* **high** *high-threshold*
4. **call treatment on**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device>enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**call threshold global [cpu-5sec | cpu-avg | io-mem | proc-mem | total-calls | total-mem] low** *low-threshold* **high** *high-threshold* **Example:**	Configures the Call Admission Control feature based on the total calls, cpu, and memory usage at the interface level to reject SIP calls when the bandwidth that is required for the calls exceed the aggregate bandwidth threshold.

	Command or Action	Purpose

	`Device(config)# call threshold global total-calls low 1 high 1`
	
	or
	`Device(config)# call threshold global cupu-avg low 75 high 85`
	
	or
	
	`Device(config)# call threshold global toal-mem low 75 high 85`
		Note By default, the system rejects incoming calls if the 5 second CPU utilization on the gateway exceeds 95%, and if the in-use process memory on the gateway exceeds 98%.

Step 4	**call treatment on** **Example:** `Device(config)# call treatment on`	Enables the call treatment feature.
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Example: Internal Error Code (IEC) for Default Call Rejection Based on CPU Utilization and Memory

Following is the sample Internal Error Code (IEC) that explains default call rejection based on CPU utilization and memory:

```
%VOICE_IEC-3-GW: C SCRIPTS: Internal Error (Low memory): IEC=1.1.181.11.4.0 on callID
1GUID=00000000000000000000000000000000
%IVR-3-LOW_MEMORY_RESOURCE: IVR: System running low on memory (99/100 in use). Call (callID=1)
 is rejected.

%VOICE_IEC-3-GW: C SCRIPTS: Internal Error (CPU high): IEC=1.1.181.11.3.0 on callID 2
%IVR-3-LOW_CPU_RESOURCE: IVR: System experiencing high cpu utilization (97/100). Call
(callID=2) is rejected.

%VOICE_IEC-3-GW: CCAPI: Internal Error (Call spike threshold): IEC=1.1.181.1.29.0 on callID
 3
%SIP-3-MEMCAC: Call rejected due to CAC based on Memory usage, sent response 503
```

Configure CAC Based on Call Spike Detection

The Call Admission Control (CAC) based on Call Spike Detection feature permits the Cisco Voice Gateways to monitor call arrival rate over a moving window of time. Calls exceeding the configured rate threshold are rejected. This feature helps in protecting against unexpected high call volumes, and INVITE-based DoS attacks.

You can configure this feature globally or on a per dial-peer level. Error code is sent when a call spike occurs, the error code is configurable globally or on a per dial-peer level.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call spike threshold** *call number <1-2147483647>steps<3-10> size<100-250>*
4. **call treatment on**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device>enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**call spike threshold** *call number <1-2147483647>steps<3-10> size<100-250>*
	Example:
	`Device(config)# call spike 10 steps 3 size 100`
	`Device(config)# call spike 12`
		Configures the Call Spike Call Admission Control feature at the device level to reject SIP calls when the call spike is detected as per the configuration (10 incoming call requests per 300 milliseconds)

Step 4	**call treatment on** **Example:** `Device(config)# call treatment on`	Enables the call treatment feature.
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Configure CAC Based on Maximum Calls per Destination

The Call Admission Control (CAC) based on Maximum Calls per Destination feature permits the Cisco Voice Gateways to restricting the number of concurrent calls that can be active on a VoIP dial peer. Maximum connections work on individual dial-peers and do not provide CAC for the entire gateway.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **session protocol sipv2**
5. **max-conn**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device>**enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** Device(config)# dial-peer voice 10 voip	Enters dial peer voice configuration mode.
Step 4	**session protocol sipv2** **Example:** Device(config-dial-peer)# session protocol sipv2	Configures SIP as the session protocol type.
Step 5	**max-conn** **Example:** Device(config)# **max-conn <1-214748364>**	Configures the Maximum Calls per Destination Call Admission Control feature at the device level to allow only 2 toll calls.
Step 6	**end** **Example:** Device# **end**	Exits global configuration mode and enters privileged EXEC mode.

Bandwidth-Based Call Admission Control

The Bandwidth-Based Call Admission Control (CAC) feature provides the functionality to reject SIP calls when the bandwidth accounted by the SIP signaling layer exceeds the aggregate bandwidth threshold for VoIP media traffic—voice, video, and fax. This functionality helps you prevent Quality of Service (QoS) degradation of VoIP media traffic for existing calls when the bandwidth allocated for VoIP traffic is fully utilized.

Midcall media renegotiation can also be rejected if the configured maximum bandwidth threshold for the VoIP media traffic is exceeded. The call continues as per the previously negotiated media codecs if midcall media renegotiation is rejected.

The excess subscription of the bandwidth allocated for VoIP traffic results in VoIP media packets being dropped or delayed, irrespective of the VoIP call to which they belong. Under such circumstances, it is better to deny new calls to prevent QoS deterioration for existing VoIP call traffic. The existing traffic congestion resolution mechanisms do not differentiate between media packets of existing calls (admitted) and new calls (oversubscribed). Similarly, existing call signaling is unaware of the media traffic congestion. The Bandwidth-Based Call Admission Control feature fills this gap by rejecting new SIP calls when the bandwidth allocated for VoIP traffic is fully utilized. The actual bandwidth usage is not measured and policed. The lower-level QoS policies control the traffic characteristics for the specified traffic class.

Note The Bandwidth-Based Call Admission Control feature is applicable only to VoIP traffic.

Maximum Bandwidth Calculation

The bandwidth requirement for each SIP call leg is calculated using the codec information available in the SDP. Here, the actual media bandwidth used is not measured.

Bandwidth in Kilo bits per second (Kbps) = [codec bytes + RTP header (12) + UDP (8) + IP Header (20 or 40)] * Packets per seconds * 8/1000

Where, codec bytes = Codec payload size, in bytes, for a given packetization interval.

RTP header = Size of the RTP header, in bytes.

UDP = Size of the UDP header, in bytes.

IP Header = Size of the IP header, in bytes. The IPV4 header is 20 bytes and the IPV6 header is 40 bytes.

Packets per second = Number of RTP packets sent or received per second. This value is as per the negotiated packetization interval. The SDP media attribute "ptime" indicates the number of packets per second.

Bandwidth Tables

This section provides the sample maximum bandwidth calculation for audio and fax calls.

Table 2: Audio Bandwidth Table

Codec and Bit Rate (Kbps)	Codec Sample Size in Bytes	Voice Payload Size in Bytes	Voice Payload Size in Milliseconds	Packets Per Second	Bandwidth for IPv4 (excluding Layer 2) in Kbps	Bandwidth for IPv6 (excluding Layer 2) in Kbps
G.711 (64 Kbps)	80	160	20	50	80	88
G.729 (8 Kbps)	10	20	20	50	24	32

G.723.1 (6.3 Kbps)	24	24	30	33.3	17	22
G.723.1 (5.3 Kbps)	20	20	30	33.3	16	21
G.726 (32 Kbps)	20	80	20	50	48	56
G.726 (24 Kbps)	15	60	20	50	40	48
G.726 (16 Kbps)	10	40	20	50	32	40
G.728 (16 Kbps)	10	40	20	50	32	40
G722_64k (64 Kbps)	80	160	20	50	80	88
ilbc_mode_20 (15.2 Kbps)	38	38	20	50	31	39
ilbc_mode_30 (13.33 Kbps)	50	50	30	33.3	24	29
gsm (13 Kbps)	33	33	20	50	30	37
gsm (12 Kbps)	32	32	20	50	29	37
G.Clear (64 Kbps)	80	160	20	50	80	88
GSM AMR	—	—	—	—	15	15
ISAC (32 Kbps)	—	—	—	—	37	37
Aacld (mpeg4)	—	—	—	—	Derived from the SDP bandwidth attribute (TIAS)	Derived from the SDP bandwidth attribute (TIAS)

Table 3: Fax Bandwidth Table

T.38 Fax Bit Rate	Redundancy	Maximum Bandwidth in Kbps

2400	None	8
2400	Redundancy	17
9600 (default)	None	16
9600 (default)	Redundancy	46
14400	None	20
14400	Redundancy	65
33600	None	40
33600	Redundancy	142

Restrictions

- CUBE, configured with the Bandwidth-Based Call Admission Control feature, will not reject the call if the bandwidth of the SDP answer is greater than the bandwidth of the SDP offer.
- Layer 2 overhead is not included in the bandwidth calculation.
- A midcall delayed-offer (DO) to DO call is disconnected if the bandwidth requested in an offer message (200 OK) exceeds the threshold bandwidth.
- Real Time Transport Control Protocol (RTCP) and RTP Named phone Event (RTP-NTE) bandwidth requirement is not computed.
- The Bandwidth-Based Call Admission Control feature does not support:
  - Cisco fax relay.
  - Filtering of codecs to accommodate calls within the available bandwidth.
  - Media flow-around, Session Description Protocol (SDP) pass-through, out-of-box low-density transcoding, high-density transcoding, video transcoding, and midcall consumption functionalities.
  - Non-SIP call legs.
  - Subinterfaces for bandwidth-based CAC on an interface.

Configure Bandwidth-Based Call Admission Control

Configure Bandwidth-Based Call Admission Control at the Interface Level

Configure the Bandwidth-Based Call Admission Control feature at the interface level to reject SIP calls when the bandwidth that is required for the call exceeds the aggregate bandwidth threshold.

Configure the Bandwidth-Based Call Admission Control feature for the following interfaces:

- ATM
- Ethernet (Fast Ethernet, Gigabit Ethernet)

- Loopback
- Serial

Note It is recommended that you configure a bind media to associate a specific interface for SIP calls. Otherwise, the interface that is used for the calls is determined based on the best local address that can access the remote media source address (for early offer calls) or the remote signaling source address (for delayed offer calls). When you use a Loopback interface to configure CAC, you must configure an additional bind-to-bind media with the Loopback interface at the global level or the dial peer level. Configure the **bind media source-interface loopback** *number* command in service SIP configuration mode to configure a bind media.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call threshold interface** *type number* **int-bandwidth** {**class-map** *name* [**l2-overhead** *percentage*] | **low** *low-threshold* **high** *high-threshold*} [**midcall-exceed**]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**call threshold interface** *type number* **int-bandwidth** {**class-map** *name* [**l2-overhead** *percentage*] | **low** *low-threshold* **high** *high-threshold*} [**midcall-exceed**]
	Example:
	`Device(config)# call threshold interface GigabitEthernet 0/0 int-bandwidth low 1000 high 20000 midcall-exceed`
	or
	`Device(config)# call threshold interface GigabitEthernet 0/0 int-bandwidth class-map voip-traffic l2-overhead 20 midcall-exceed`
		Configures the Bandwidth-Based Call Admission Control feature at the interface level to reject SIP calls when the bandwidth that is required for the calls exceed the aggregate bandwidth threshold.
		• You can configure the **call threshold interface** *type number* **low** *low-threshold* **high** *high-threshold* [**midcall-exceed**] command to apply call admission control to reject SIP calls once the accounted bandwidth reaches the *high-threshold* value and remains above the *low-threshold* value.
		• You can configure the **call threshold interface** *type number* **int-bandwidth class-map** *name* [**l2-overhead** *percentage*] [**midcall-exceed**] command to use the

	Command or Action	Purpose
		bandwidth value provisioned in the QoS policy under the interface for VoIP media traffic for CAC. See the Modular Quality of Service Command-Line Interface Overview document at http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfmdcli.html for information on the usage of the QoS policy with Call Admission Control. • SIP calls are rejected when the calculated aggregate bandwidth of VoIP media traffic on the specified interface exceeds the configured bandwidth threshold.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Configure Bandwidth-Based Call Admission Control at the Dial Peer Level

You can configure the Bandwidth-Based Call Admission Control feature at the dial peer level to reject SIP calls when the bandwidth that is required for the calls exceeds the aggregate bandwidth threshold.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **session protocol sipv2**
5. **max-bandwidth** *bandwidth-value* [**midcall-exceed**]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:**	Enters dial peer voice configuration mode.

	Command or Action	Purpose
	`Device(config)# dial-peer voice 44 voip`	
Step 4	**session protocol sipv2** **Example:** `Device(config-dial-peer)# session protocol sipv2`	Configures the Bandwidth-Based Call Admission Control feature for SIP dial peers only.
Step 5	**max-bandwidth** *bandwidth-value* [**midcall-exceed**] **Example:** `Device(config-dial-peer)# max-bandwidth 24 midcall-exceed`	Configures the Bandwidth-Based Call Admission Control feature at the dial peer level to reject SIP calls when the bandwidth that is required for the calls exceed the aggregate bandwidth threshold. • Configuring the **midcall-exceed** keyword allows exceeding the bandwidth threshold during mid-call media renegotiation. Media renegotiation exceeding the bandwidth threshold is rejected by default.
Step 6	**end** **Example:** `Device(config-dial-peer)# end`	Exits dial peer configuration mode and enters privileged EXEC mode.

Configure the Bandwidth-Based Call Admission Control SIP Error Response Code Mapping

Mapping of the call rejection cause code to a specific SIP error response code is known as error response code mapping. The cause code for the call rejected because of the bandwidth-based CAC can be mapped to a SIP error response code 400–600. The default SIP error response code is 488.

You can configure SIP error response codes for calls that are rejected by the Bandwidth-Based Call Admission Control feature at the global level, dial peer level, or both.

Configure Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Global Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **error-code-override cac-bandwidth failure** *sip-status-code-number*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice-service configuration mode.
Step 4	**sip** **Example:** `Device(conf-voi-serv)# sip`	Enters service SIP configuration mode.
Step 5	**error-code-override cac-bandwidth failure** *sip-status-code-number* **Example:** `Device(conf-serv-sip)# error-code-override cac-bandwidth failure 500`	Configures bandwidth-based CAC SIP error response code mapping at the global level.
Step 6	**end** **Example:** `Device(conf-serv-sip)# end`	Exits service SIP configuration mode and enters privileged EXEC mode.

Configure Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Dial Peer Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* {**pots** | **voatm** | **vofr** | **voip**}
4. **voice-class sip error-code-override cac-bandwidth failure** {*sip-status-code-number* | **system**}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* {**pots** | **voatm** | **vofr** | **voip**} **Example:** `Device(config)# dial-peer voice 88 voip`	Enters dial peer voice configuration mode.
Step 4	**voice-class sip error-code-override cac-bandwidth failure** {*sip-status-code-number* | **system**} **Example:** `Device(config-dial-peer)# voice-class sip error-code-override cac-bandwidth failure 500`	Configures bandwidth-based CAC SIP error response code mapping at the dial peer level.
Step 5	**end** **Example:** `Device(config-dial-peer)# end`	Exits dial peer configuration mode and enters privileged EXEC mode.

Verify Bandwidth-Based Call Admission Control

Perform this task to verify the configuration for the Bandwidth-Based Call Admission Control feature on CUBE. The **show** commands need not be entered in any specific order.

SUMMARY STEPS

1. **enable**
2. **show call threshold config**
3. **show call threshold status**
4. **show call threshold stats**
5. **show dial-peer voice**

DETAILED STEPS

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode.

Step 2 **show call threshold config**

Example:

```
Device# show call threshold config

Some resource polling interval:
  CPU_AVG interval: 60
  Memory interval:  5

IF                  Type            Value   Low     High    Enable
-----               ----            -----   ----    ----    ------
GigabitEthernet0/0  int-bandwidth   0       100     400      N/A
```

Displays the active call threshold configuration at the interface level for all resources.

Step 3 **show call threshold status**

Example:

```
Device# show call threshold status

Status  IF                  Type            Value   Low     High    Enable
------  ---                 ------          ----    ----    ----    -----
Avail   GigabitEthernet0/0  int-bandwidth   0       100     400      N/A
```

Displays the availability status of resources that are configured when the Bandwidth-Based Call Admission Control feature is enabled at an interface level.

Step 4 **show call threshold stats**

Example:

```
Device# show call threshold stats

Total resource check: 2
successful: 1
 failed:   1

1: ------------------------
  Failed resources: int-bandwidth,
  related interface: GigabitEthernet0/0; related option:N/A
  Recorded time: 04:49:39 UTC Wed Dec 8 2010
2: ------------------------
Successful
  All resources are available for this check.
  Recorded time: 04:29:39 UTC Wed Dec 8 2010
```

Displays the statistics of resources that are configured when the Bandwidth-Based Call Admission Control feature is enabled at an interface level.

Step 5 **show dial-peer voice**

Example:

```
Device# show dial-peer voice

incoming called-number = `2000', connections/maximum = 0/unlimited,
bandwidth/maximum = 0/400,
…….
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 3, Refused Calls = 0,
Bandwidth CAC Accepted Calls = 3, Bandwidth CAC Refused Calls = 0
```

Displays information for the voice dial peer.

Tips to Troubleshoot

The following commands can help troubleshoot the Bandwidth-Based Call Admission Control feature:

- **debug ccsip all**
- **debug voice ccapi all**

Configuration Examples for Bandwidth-Based Call Admission Control

Example: Configuring Bandwidth-Based Call Admission Control at the Interface Level

The following example shows how to configure CUBE to reject new SIP calls if the accounted VoIP media bandwidth on Gigabit Ethernet interface 0/0 exceeds 400 Kbps of bandwidth and continues to have a bandwidth above 100 Kbps:

```
Device> enable
Device# configure terminal
Device(config)# call threshold interface GigabitEthernet 0/0 int-bandwidth  low 100 high
400
```

The following example shows how to configure CUBE to reject new SIP calls if the VoIP media bandwidth on Gigabit Ethernet interface 0/0 exceeds the configured bandwidth for priority traffic in the “voip_traffic” class:

```
Device>enable
Device# configure terminal
Device(config)# class-map match-all voip-traffic

Device(config-cmap)# policy-map voip-policy
Device(config-pmap)# class voip-traffic
Device(config-pmap-c)# priority 440
Device(config-pmap-c)# end

Device# enaconfigure terminalble
Device(config)# call threshold interface GigabitEthernet 0/0 int-bandwidth class-map
voip-traffic l2-overhead 10
```

Note Layer 2 overhead of 10 percent in the **call threshold** command indicates that the IP bandwidth, excluding Layer 2, is 90 percent of the configured priority bandwidth.

Example: Configuring Bandwidth-Based Call Admission Control at the Dial Peer Level

The following example shows how to configure CUBE to reject calls once the accounted aggregate bandwidth of active calls exceeds 400 Kbps for a SIP dial peer:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 2000 voip
Device(config)# session protocol sipv2
Device(config-dial-peer)# max-bandwidth 400
```

Example: Configuring the Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Global Level

The following example shows how to configure CUBE for bandwidth-based CAC SIP error response code mapping at the global level:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# error-code-override cac-bandwidth 500
```

Example: Configuring the Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Dial Peer Level

The following example shows how to configure CUBE for bandwidth-based CAC SIP error response code mapping at the dial peer level:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 88 voip
Device(config-dial-peer)# voice-class sip error-code-override cac-bandwidth failure 500
```