# Voice Source−Group Feature

**Document ID: 116440**

Contributed by Bakthavatsal Muralidharan and Dilip Singh, Cisco TAC Engineers.
Sep 04, 2013

## Contents



## Introduction

This document describes the Voice Source−Group (VSG) feature in Cisco IOS® that allows the gateway, or Cisco Unified Border Element (CUBE), to identify the source and control the routing of VoIP calls.

***Note***: The terms CUBE and IP−to−IP Gateway (IPIPGW) are used interchangeably throughout this document.

## Background Information

If you have encountered a situation where you want to implement toll−fraud by blocking call signaling from rogue IP addresses, then you could use the toll−fraud prevention feature, introduced in Cisco IOS 15.1(2)T. Refer to the Toll−Fraud Prevention Feature in IOS Release 15.1(2)T article for more information.

However, if you have an older version of Cisco IOS, or need these additional controls, then you should consider the VSG feature:

- configurable reject cause−code
- change calling/called numbers based on who originates the call
- control routing (route to specific carrier, for example)

The VSG feature allows you to identify the source of the VoIP call such that selected services are provided to the call. These services include number translation, inbound dial− peer matching, and call acceptance/rejection control. In addition, the feature allows you to control the routing of the (permitted) call in ways that the toll−fraud application cannot. For example, you can associate voice translations to the VSG in order to manipulate the calling/called numbers *BEFORE* the call reaches the inbound dial−peer. This is powerful because calls with the ***same*** dialed number could be routed through different inbound dial−peers.

VSG uses the Cisco IOS Access Control List (ACL) in order to accomplish the identifcation.

# VSG Attributes

## Access List

A standard IOS ACL is configured in order to specify the IP addresses of the sources from which calls are accepted and processed. The ACL is then referenced in the associated VSG.

If the IP address of the source (of an incoming call) does not have an entry in the ACL, the gateway does NOT associate the VSG to the call. This means that the call is not subject to any of the manipulations configured under the VSG.

If calls from a particular IP address are to be rejected, that IP address must be included in a ***deny*** statement under the ACL.

Alternatively, the ***deny any*** statement is configured in order to reject calls from any IP address that is not explicitly allowed or denied.

## Disconnect Cause

The cause code with which the incoming call is rejected is configureable under the VSG. By default, the disconnect−cause is ***no−service***. This translates to the ***500 internal server error*** for Session Initiation Protocol (SIP) calls and ***ReleaseComplete*** with cause−code 63 (Service or option not available, unspecified) for H.323 calls.

User−defined disconnect reasons are:

- Invalid number
- Unassigned number
- User busy
- Call rejected

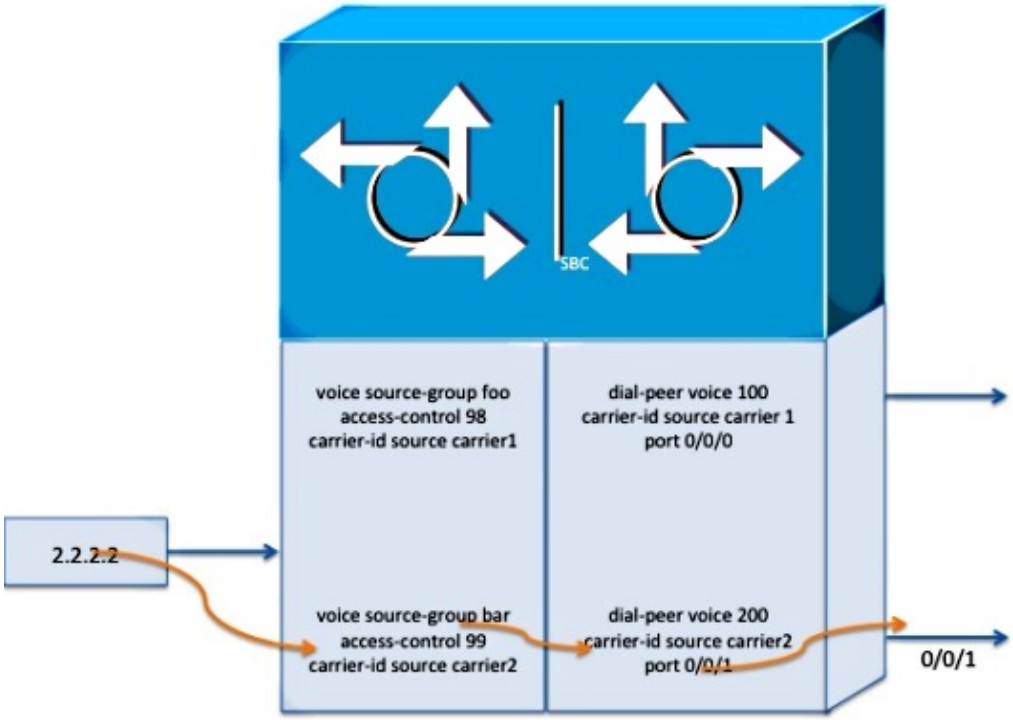
## Carrier−ID

The carrier−ID attribute is configured on the VSG so that calls that match the associated ACL are tagged with the carrier−ID. This enables calls with the *same* called number to be routed (on the outbound side) through different carriers, based on the IP address of the source. For example, if you have two groups of IP addresses, calls from one group of addresses could flow through one VSG and could get tagged with one carrier−ID, and calls (to the same called number) from the other group could be tagged with a different carrier−ID. Here is an example:

```
voice source−group foo
access−control 98
carrier−id source carrier1

voice source−group bar
access−control 99
carrier−id source carrier2

dial−peer voice 100 pots
carrier−id source carrier1
...

dial−peer voice 200 pots
carrier−id source carrier2
...
```

```
ip access-control standard 98
permit 1.1.1.1

ip access-control standard 99
permit 2.2.2.2
deny any any
```

With the previous configuration, calls from 1.1.1.1 are routed through dial−peer 100, and calls from 2.2.2.2 are routed through dial−peer 200.




### Trunk−Group−Label

The trunk−group−label works similarly to the carrier−ID. The incoming VoIP call is tagged with the configured trunk−group, which is then used in order to select the appropriate dial−peer when the call is routed through the outbound leg.

### H.323 Zone ID

This is applicable for H.323 protocol only and is used in order to match the source zone of the incoming H.323 call to a VSG. The source zone ID is carried in an incoming H.323 call that uses H.323V4 signaling protocol and originates from a H.323 gatekeeper.

## Multiple Voice Service Groups

You can configure multiple VSGs on an IPIPGW where each allows or disallows calls from a different set of IP addresses.

Be careful to add ***deny any*** ONLY to the ACL of the last VSG, when you have multiple VSGs. Otherwise, if an intermediate ACL has ***deny any***, then calls from any IP address that is explicitly permitted in another ACL will still be rejected if that ACL is AFTER the ACL with the ***deny any***. For example, here are two VSGs:

```
voice source-group foo
access-list 98

voice source-group bar
access-list 99
```

Here are the ACLs for the VSGs:

```
ip access-list standard 98
permit 1.1.1.1
deny any

ip access-list standard 99
permit 2.2.2.2
deny any
```

In this example, calls from 2.2.2.2 are rejected, since the ACL that permits the IP address is AFTER the ACL (98) with ***deny any***.

You can use this command in order to confirm that the calls are rejected.

```
Router#test source-group ip-address 2.2.2.2
A source-group is found with ip address=2.2.2.2
An ip address 2.2.2.2 is rejected with disc-cause="no-service"
```

In order to permit the call, you must remove the ***deny any*** from access-list 98.

```
ip access-list standard 98
permit 1.1.1.1
```

You can use the ***test source-group ip 2.2.2.2*** command again in order to verify that calls from the IP address in question are not rejected anymore.

```
Router#test  source-group ip-address 2.2.2.2
A source-group is found with ip address=2.2.2.2
```

# Verify

The ***test source-group <VSG>*** command can be used for basic verification − whether calls from a given IP address will be processed by a VSG.

# Troubleshoot

As mentioned in the previous section, the ***test source-group <VSG>*** command is useful in order to discover whether a given call will be permitted or rejected. In addition, if the call will be permitted, this command also shows which VSG will ?route? the call. Similarly, if the call will be rejected, it shows the rejection cause. This command finds the routing VSG based on other attributes, in addition to the IP address.

The other troubleshooting aid is the ***debug voice source-group*** debug command. For example, when an H.323 call is rejected (with the default cause-code), the debug produces this output:

```
092347: .Apr  7 10:53:46.132: SIPG:src_grp_check_config() src_grp or src_grp
acl is defined
```

```
092348: .Apr  7 10:53:46.136: %VOICE_IEC-3-GW: H323: Internal Error (H323
Interworking Error): IEC=1.1.127.5.21.0 on callID 264
```

# Cautions and Caveats

Here are some important caveats with the VSG:

- VSG is much less flexible than the toll−fraud application. It prevents the calls from reaching the call−control layer and does not log any error messages. This is true regardless of whether a call is allowed or blocked.
- Some have experienced an issue with Global Load Balancing Protocol (GLBP) enabled for that gateway. There seems to be an obscure dependency on the relative order in which GLBP and VSG are configured. If you encounter such issues, complete these steps:
    1. Disable ***GLBP***.
    2. Reapply ***VSG***.
    3. Reboot the ***gateway***.
    4. Test/verify that VSG works.
    5. Enable ***GLBP***.

# Related Information

- ***Understanding Toll−Fraud Enhancements in 15.1(2)T***
- ***Cisco CCA Tool SIP Security methods***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Sep 04, 2013 Document ID: 116440