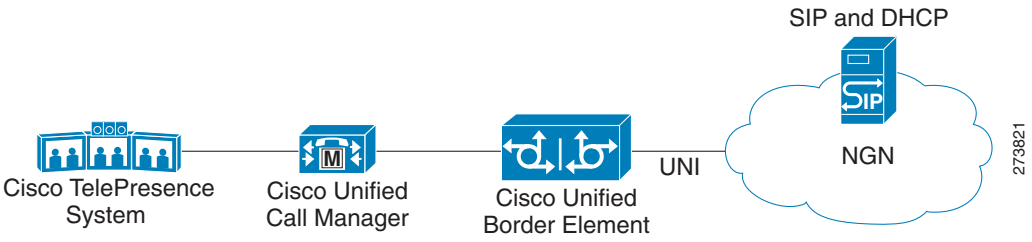
Support for PAID, PPID, Privacy, PCPID, and PAURI Headers on the Cisco Unified Border Element

Figure 1 shows a typical network topology where the Cisco Unified Border Element is configured to route messages between a call manager system (such as the Cisco Unified Call Manager) and a Next Generation Network (NGN).

Figure 1 Cisco Unified Border Element and Next Generation Topology



Devices that connect to an NGN must comply with the User-Network Interface (UNI) specification. The Cisco Unified Border Element supports the NGN UNI specification and can be configured to interconnect NGN with other call manager systems, such us the Cisco Unified Call Manager.

The Cisco Unified Border Element supports the following:

- the use of P-Preferred Identity (PPID), P-Asserted Identity (PAID), Privacy, P-Called Party Identity (PCPID), in INVITE messages
- the translation of PAID headers to PPID headers and vice versa
- the translation of From: or RPID headers to PAID or PPID headers and vice versa
- the configuration and/or pass through of privacy header values
- the use of the PCPID header to route INVITE messages
- the use of multiple PAURI headers in the response messages (200 OK) it receives to REGISTER messages

P-Preferred Identity and P-Asserted Identity Headers

NGN servers use the PPID header to identify the preferred number that the caller wants to use. The PPID is part of INVITE messages sent to the NGN. When the NGN receives the PPID, it authorizes the value, generates a PAID based on the preferred number, and inserts it into the outgoing INVITE message towards the called party.

However, some call manager systems, such as Cisco Unified Call Manager 5.0, use the Remote-Party Identity (RPID) value to send calling party information. Therefore, the Cisco Unified Border Element must support building the PPID value for an outgoing INVITE message to the NGN, using the RPID value or the From: value received in the incoming INVITE message. Similarly, CUBE supports building the RPID and/or From: header values for an outgoing INVITE message to the call manager, using the PAID value received in the incoming INVITE message from the NGN.

In non-NGN systems, the Cisco Unified Border Element can be configured to translate between PPID and PAID values, and between From: or RPID values and PAID/PPID values, at global and dial-peer levels.

In configurations where all relevant servers support the PPID or PAID headers, the Cisco Unified Border Element can be configured to transparently pass the header.

Note If the NGN sets the From: value to anonymous, the PAID is the only value that identifies the caller.

Table 1 describes the types of INVITE message header translations supported by the Cisco Unified Border Element. It also includes information on the configuration commands to use to configure P-header translations.

Table 1 shows the P-header translation configuration settings only. In addition to configuring these settings, you must configure other system settings (such as the session protocol).

Table 1 P-header Configuration Settings

Incoming Header	Outgoing Header	Configuration Notes
From:	PPID	To enable the translation to PPID headers in the outgoing header at a global level, use the **asserted-id ppi** command in voice service VoIP SIP configuration mode. For example: `Router(conf-serv-sip)# asserted-id ppi` To enable the translation to PPID headers in the outgoing header on a specific dial peer, use the **voice-class sip asserted-id ppi** command in dial peer voice configuration mode. For example: `Router(config-dial-peer)# voice-class sip asserted-id ppi`
From:	PAID	To enable the translation to PAID headers in the outgoing header at a global level, use the **asserted-id pai** command in voice service VoIP SIP configuration mode. For example: `Router(conf-serv-sip)# asserted-id pai` To enable the translation to PAID headers in the outgoing header on a specific dial peer, use the **voice-class sip asserted-id pai** command in dial peer voice configuration mode. For example: `Router(config-dial-peer)# voice-class sip asserted-id pai`
From:	RPID	To enable the translation to RPID headers in the outgoing header, use the **remote-party-id** command in SIP user-agent configuration mode. For example: `Router(config-sip-ua)# remote-party-id` This is the default system behavior. **Note** If both, **remote-party-id** and **asserted-id** commands are configured, then the **asserted-id** command takes precedence over the **remote-part-id** command.
PPID	PAID	To enable the translation to PAID privacy headers in the outgoing header at a global level, use the **asserted-id pai** command in voice service VoIP SIP configuration mode. For example: `Router(conf-serv-sip)# asserted-id pai` To enable the translation to PAID privacy headers in the outgoing header on a specific dial peer, use the **voice-class sip asserted-id pai** command in dial peer voice configuration mode. For example: `Router(config-dial-peer)# voice-class sip asserted-id pai`
PPID	From:	By default, the translation to RPID headers is enabled and the system translates PPID headers in incoming messages to RPID headers in the outgoing messages. To disable the default behavior and enable the translation from PPID to From: headers, use the **no remote-party-id** command in SIP user-agent configuration mode. For example: `Router(config-sip-ua)# no remote-party-id`

Table 1 P-header Configuration Settings (continued)

Incoming Header	Outgoing Header	Configuration Notes
PPID	RPID	To enable the translation to RPID headers in the outgoing header, use the **remote-party-id** command in SIP user-agent configuration mode. For example: `Router(config-sip-ua)# remote-party-id` This is the default system behavior.
PAID	PPID	To enable the translation to PPID privacy headers in the outgoing header at a global level, use the **asserted-id ppi** command in voice service VoIP SIP configuration mode. For example: `Router(conf-serv-sip)# asserted-id ppi` To enable the translation to PPID privacy headers in the outgoing header on a specific dial peer, use the **voice-class sip asserted-id ppi** command in dial peer voice configuration mode. For example: `Router(config-dial-peer)# voice-class sip asserted-id ppi`
PAID	From:	By default, the translation to RPID headers is enabled and the system translates PPID headers in incoming messages to RPID headers in the outgoing messages. To disable the default behavior and enable the translation from PPID to From: headers, use the **no remote-party-id** command in SIP user-agent configuration mode. For example: `Router(config-sip-ua)# no remote-party-id`
PAID	RPID	To enable the translation to RPID headers in the outgoing header, use the **remote-party-id** command in SIP user-agent configuration mode. For example: `Router(config-sip-ua)# remote-party-id` This is the default system behavior.
RPID	PPID	To enable the translation to PPID privacy headers in the outgoing header at a global level, use the **asserted-id ppi** command in voice service VoIP SIP configuration mode. For example: `Router(conf-serv-sip)# asserted-id ppi` To enable the translation to PPID privacy headers in the outgoing header on a specific dial peer, use the **voice-class sip asserted-id ppi** command in dial peer voice configuration mode. For example: `Router(config-dial-peer)# voice-class sip asserted-id ppi`
RPID	PAID	To enable the translation to PAID privacy headers in the outgoing header at a global level, use the **asserted-id pai** command in voice service VoIP SIP configuration mode. For example: `Router(conf-serv-sip)# asserted-id pai` To enable the translation to PAID privacy headers in the outgoing header on a specific dial peer, use the **voice-class sip asserted-id pai** command in dial peer voice configuration mode. For example: `Router(config-dial-peer)# voice-class sip asserted-id pai`
RPID	From:	By default, the translation to RPID headers is enabled and the system translates PPID headers in incoming messages to RPID headers in the outgoing messages. To disable the default behavior and enable the translation from PPID to From: headers, use the **no remote-party-id** command in SIP user-agent configuration mode. For example: `Router(config-sip-ua)# no remote-party-id`

Privacy

If the user is subscribed to a privacy service, the Cisco Unified Border Element can support privacy using one of the following methods:

- Using prefixes

  The NGN dial plan can specify prefixes to enable privacy settings. For example, the dial plan may specify that if the caller dials a prefix of 184, the calling number is not sent to the called party.

  The dial plan may also specify that the caller can choose to send the calling number to the called party by dialing a prefix of 186. Here, the Cisco Unified Border Element transparently passes the prefix as part of the called number in the INVITE message.

  The actual prefixes for the network are specified in the dial plan for the NGN, and can vary from one NGN to another.

- Using the Privacy header

  If the Privacy header is set to None, the calling number is delivered to the called party. If the Privacy header is set to a Privacy:id value, the calling number is not delivered to the called party.

- Using Privacy values from the peer call leg

  If the incoming INVITE has a Privacy header or a RPID with privacy on, the outgoing INVITE can be set to Privacy: id. This behavior is enabled by configuring **privacy pstn** command globally or **voice-class sip privacy pstn** command on the selected dial-per.

  Incoming INVITE can have multiple privacy header values, id, user, session, and so on. Configure the **privacy-policy passthru** command globally or **voice-class sip privacy-policy passthru** command to transparently pass across these multiple privacy header values.

  Some NGN servers require a Privacy header to be sent even though privacy is not required. In this case the Privacy header must be set to none. The Cisco Unified Border Element can add a privacy header with the value None while forwarding the outgoing INVITE to NGN. Configure the **privacy-policy send-always** globally or **voice-class sip privacy-policy send-always** command in dial-peer to enable this behavior.

If the user is not subscribed to a privacy service, the Cisco Unified Border Element can be configured with no Privacy settings.

P-Called Party Identity

The Cisco Unified Border Element can be configured to use the PCPID header in an incoming INVITE message to route the call, and to use the PCPID value to set the To: value of outgoing INVITE messages.

The PCPID header is part of the INVITE messages sent by the NGN, and is used by Third Generation Partnership Project (3GPP) networks. The Cisco Unified Border Element uses the PCPID from incoming INVITE messages (from the NGN) to route calls to the Cisco Unified Call Manager.

Note The PCPID header supports the use of E.164 numbers only.

P-Associated URI

The Cisco Unified Border Element supports the use of PAURI headers sent as part of the registration process. After the Cisco Unified Border Element sends REGISTER messages using the configured E.164 number, it receives a 200 OK message with one or more PAURIs. The number in the first PAURI (if present) must match the contract number. The Cisco Unified Border Element supports a maximum of six PAURIs for each registration.

Note The Cisco Unified Border Element performs the validation process only when a PAURI is present in the 200 OK response.

The registration validation process works as follows:

- The Cisco Unified Border Element receives a REGISTER response message that includes PAURI headers that include the contract number and up to five secondary numbers.
- The Cisco Unified Border Element validates the contract number against the E.164 number that it is registering:
  - If the values match, the Cisco Unified Border Element completes the registration process and stores the PAURI value. This allows administration tools to view or retrieve the PAURI if needed.
  - If the values do not match, the Cisco Unified Border Element unregisters and then reregisters the contract number. The Cisco Unified Border Element performs this step until the values match.

Random Contact Support

The Cisco Unified Border Element can use random-contact information in REGISTER and INVITE messages so that user information is not revealed in the contact header.

To provide random contact support, the Cisco Unified Border Element performs SIP registration based on the random-contact value. The Cisco Unified Border Element then populates outgoing INVITE requests with the random-contact value and validates the association between the called number and the random value in the Request-URI of the incoming INVITE. The Cisco Unified Border Element routes calls based on the PCPID, instead of the Request-URI which contains the random value used in contact header of the REGISTER message.

The default contact header in REGISTER messages is the calling number. The Cisco Unified Border Element can generate a string of 32 random alphanumeric characters to replace the calling number in the REGISTER contact header. A different random character string is generated for each pilot or contract number being registered. All subsequent registration requests will use the same random character string.

The Cisco Unified Border Element uses the random character string in the contact header for INVITE messages that it forwards to the NGN. The NGN sends INVITE messages to the Cisco Unified Border Element with random-contact information in the Request URI. For example: INVITE sip:FefhH3zIHe9i8ImcGjDD1PEc5XfFy51G@10.12.1.46:5060.

The Cisco Unified Border Element will not use the To: value of the incoming INVITE message to route the call because it might not identify the correct user agent if supplementary services are invoked. Therefore, the Cisco Unified Border Element must use the PCPID to route the call to the Cisco Unified Call Manager. You can configure routing based on the PCPID at global and dial-peer levels.

Prerequisites

Cisco Unified Border Element

- Cisco IOS Release 12.4(22)YB or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions

- To enable random-contact support, you must configure the Cisco Unified Border Element to support SIP registration with random-contact information. In addition, you must configure random-contact support in VoIP voice-service configuration mode or on the dial peer.
- If random-contact support is configured for SIP registration only, the system generates the random-contact information, includes it in the SIP REGISTER message, but does not include it in the SIP INVITE message.
- If random-contact support is configured in VoIP voice-service configuration mode or on the dial peer only, no random contact is sent in either the SIP REGISTER or INVITE message.

Configuring P-Header and Random-Contact Support on the Cisco Unified Border Element

To enable random contact support you must configure the Cisco Unified Border Element to support Session Initiation Protocol (SIP) registration with random-contact information, as described in this section.

To enable the Cisco Unified Border Element to use the PCPID header in an incoming INVITE message to route the call, and to use the PCPID value to set the To: value of outgoing INVITE messages, you must configure P-Header support as described in this section.

This section contains the following tasks:

Configuring P-Header Translation on a Cisco Unified Border Element

To configure P-Header translations on a Cisco Unified Border Element, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **asserted-id** *header-type*
6. **exit**

DETAILED STEPS

	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 VoIP voice-service configuration mode.
Step 4	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters voice service VoIP SIP configuration mode.
Step 5	**asserted-id** *header-type* **Example:** `Router(conf-serv-sip)# asserted-id ppi`	Specifies the type of privacy header in the outgoing SIP requests and response messages.
Step 6	**exit** **Example:** `Router(conf-serv-sip)# exit`	Exits the current mode.

Configuring P-Header Translation on an Individual Dial Peer

To configure P-Header translation on an individual dial peer, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **voice-class sip asserted-id** *header-type*
5. **exit**

DETAILED STEPS

	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 2611 voip`	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.
Step 4	**voice-class sip asserted-id** *header-type* **Example:** `Router(config-dial-peer)# voice-class sip asserted-id ppi`	Specifies the type of privacy header in the outgoing SIP requests and response messages, on this dial peer.
Step 5	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Configuring P-Called-Party-Id Support on a Cisco Unified Border Element

To configure P-Called-Party-Id support on a Cisco Unified Border Element, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **call-route p-called-party-id**
6. **random-request-uri validate**
7. **exit**

DETAILED STEPS

	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 VoIP voice-service configuration mode.
Step 4	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters voice service VoIP SIP configuration mode.
Step 5	**call-route p-called-party-id** **Example:** `Router(conf-serv-sip)# call-route p-called-party-id`	Enables the routing of calls based on the PCPID header.
Step 6	**random-request-uri validate** **Example:** `Router(conf-serv-sip)# random-request-uri validate`	Enables the validation of the random string in the Request URI of the incoming INVITE message.
Step 7	**exit** **Example:** `Router(conf-serv-sip)# exit`	Exits the current mode.

Configuring P-Called-Party-Id Support on an Individual Dial Peer

To configure P-Called-Party-Id support on an individual dial peer, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **voice-class sip call-route p-called-party-id**
5. **voice-class sip random-request-uri validate**
6. **exit**

DETAILED STEPS

	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 2611 voip`	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.
Step 4	**voice-class sip call-route p-called-party-id** **Example:** `Router(config-dial-peer)# voice-class sip call-route p-called-party-id`	Enables the routing of calls based on the PCPID header on this dial peer.
Step 5	**voice-class sip random-request-uri validate** **Example:** `Router(config-dial-peer)# voice-class sip random-request-uri validate`	Enables the validation of the random string in the Request URI of the incoming INVITE message on this dial peer.
Step 6	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Configuring Privacy Support on a Cisco Unified Border Element

To configure privacy support on a Cisco Unified Border Element, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **privacy** *privacy-option*
6. **privacy-policy** *privacy-policy-option*
7. **exit**

DETAILED STEPS

	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 VoIP voice-service configuration mode.
Step 4	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters voice service VoIP SIP configuration mode.
Step 5	**privacy** *privacy-option* **Example:** `Router(conf-serv-sip)# privacy id`	Enables the privacy settings for the header.
Step 6	**privacy-policy** *privacy-policy-option* **Example:** `Router(conf-serv-sip)# privacy-policy passthru`	Specifies the privacy policy to use when passing the privacy header from one SIP leg to the next.
Step 7	**exit** **Example:** `Router(conf-serv-sip)# exit`	Exits the current mode.

Configuring Privacy Support on an Individual Dial Peer

To configure privacy support on an individual dial peer, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **voice-class sip privacy** *privacy-option*
5. **voice-class sip privacy-policy** *privacy-policy-option*
6. **exit**

DETAILED STEPS

	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 2611 voip`	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.
Step 4	**voice-class sip privacy** *privacy-option* **Example:** `Router(config-dial-peer)# voice-class sip privacy id`	Enables the privacy settings for the header on this dial peer.
Step 5	**voice-class sip privacy-policy** *privacy-policy-option* **Example:** `Router(config-dial-peer)# voice-class sip privacy-policy passthru`	Specifies the privacy policy to use when passing the privacy header from one SIP leg to the next, on this dial peer.
Step 6	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Configuring Random-Contact Support on a Cisco Unified Border Element

To configure random-contact support on a Cisco Unified Border Element, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **credentials username** *username* **password** *password* **realm** *domain-name*
5. **registrar ipv4:***destination-address* **random-contact expires** *expiry*
6. **exit**
7. **voice service voip**
8. **sip**

9. **random-contact**
10. **exit**

DETAILED STEPS

	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	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters SIP user-agent configuration mode.
Step 4	**credentials username** *username* **password** *password* **realm** *domain-name* **Example:** `Router(config-sip-ua)# credentials username 123456 password cisco realm cisco`	Sends a SIP registration message from the Cisco Unified Border Element.
Step 5	**registrar ipv4:***destination-address* **random-contact expires** *expiry* **Example:** `Router(config-sip-ua)# registrar ipv4:10.1.2.2 random-contact expires 200`	Enables the SIP gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and Skinny Client Control Protocol (SCCP) phones with an external SIP proxy or SIP registrar. • The **random-contact** keyword configures the Cisco Unified Border Element to send the random string from the REGISTER message to the registrar.
Step 6	**exit** **Example:** `Router(config-sip-ua)# exit`	Exits the current mode.
Step 7	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters VoIP voice-service configuration mode.
Step 8	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters voice service VoIP SIP configuration mode.

	Command or Action	Purpose
Step 9	**random-contact** **Example:** `Router(conf-serv-sip)# random-contact`	Enables random-contact support on a Cisco Unified Border Element.
Step 10	**exit** **Example:** `Router(conf-serv-sip)# exit`	Exits the current mode.

Configuring Random-Contact Support for an Individual Dial Peer

To configure configure random-contact support for an individual dial peer, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **credentials username** *username* **password** *password* **realm** *domain-name*
5. **registrar ipv4:***destination-address* **random-contact expires** *expiry*
6. **exit**
7. **dial-peer voice** *tag* **voip**
8. **voice-class sip random-contact**
9. **exit**

DETAILED STEPS

	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	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters SIP user-agent configuration mode.

	Command or Action	Purpose
Step 4	**credentials username** *username* **password** *password* **realm** *domain-name* **Example:** `Router(config-sip-ua)# credentials username 123456 password cisco realm cisco`	Sends a SIP registration message from the Cisco Unified Border Element.
Step 5	**registrar ipv4:***destination-address* **random-contact expires** *expiry* **Example:** `Router(config-sip-ua)# registrar ipv4:10.1.2.2 random-contact expires 200`	Enables the SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar. • The **random-contact** keyword configures the Cisco Unified Border Element to send the random string from the REGISTER message to the registrar.
Step 6	**exit** **Example:** `Router(config-sip-ua)# exit`	Exits the current mode.
Step 7	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 2611 voip`	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.
Step 8	**voice-class sip random-contact** **Example:** `Router(config-dial-peer)# voice-class sip random-contact`	Enables random-contact support on this dial peer.
Step 9	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.