



Cisco Unified Presence Server Interoperability Guide, Release 1.0(3)

This document describes the overall architecture of the Cisco Unified Presence Server system and provides a detailed description of the messages and interfaces that are related to the Cisco Unified Presence Engine and the CTI gateway.

Contents

This document covers the following topics:

- [Introduction, page 2](#)
- [Overall Architecture, page 2](#)
- [Address of Record Definition, page 3](#)
- [SIMPLE Interface, page 4](#)
- [Composition and Filtering, page 3](#)
- [Industry Standards Requirements, page 4](#)
- [Other pidf Extensions, page 5](#)
- [Call Flows, page 5](#)
- [Transport, page 7](#)
- [Security, page 7](#)
- [Subscription Description, page 7](#)
- [Notification Description, page 10](#)
- [Event List Notification, page 13](#)
- [Publication Description, page 15](#)
- [Back-end Subscription Description, page 19](#)
- [Notification From Foreign Server Description, page 20](#)
- [Instant Messaging Applications, page 21](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2006 Cisco Systems, Inc. All rights reserved.

- [CTI Gateway, page 23](#)
- [Related Documentation, page 26](#)
- [Obtaining Documentation, page 26](#)
- [Documentation Feedback, page 27](#)
- [Cisco Product Security Overview, page 27](#)
- [Product Alerts and Field Notices, page 28](#)
- [Obtaining Technical Assistance, page 28](#)
- [Obtaining Additional Publications and Information, page 30](#)

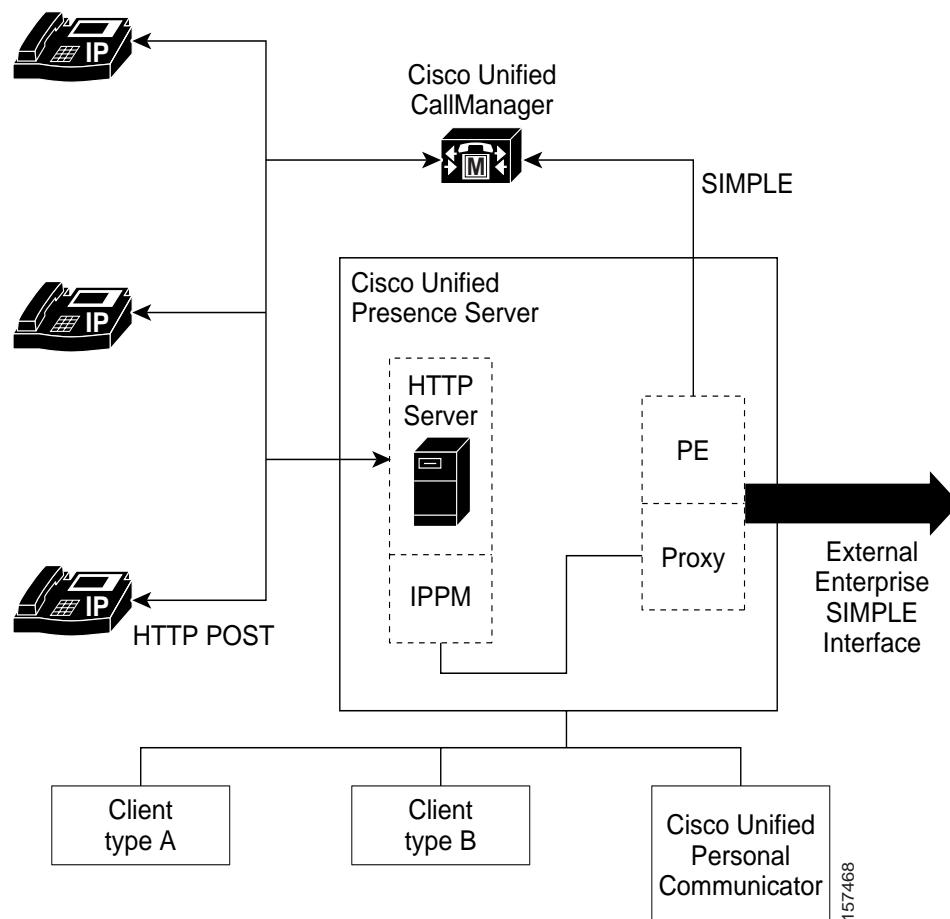
Introduction

The SUBSCRIBE, NOTIFY, and PUBLISH interfaces for the presence event package that the Cisco Unified Presence Engine provides are compliant to the SIMPLE specifications that are provided in the [“Industry Standards Requirements” section on page 4](#). This document provides the expected contents of each of the fields in the messages, specifically for the Enterprise Presence application, and describes how those contents correlate to the provisioned information on the Cisco Unified Presence Engine.

Overall Architecture

The Cisco Unified Presence Server contains the following main pieces: IP Phone Messenger (IPPM), proxy, and the Cisco Unified Presence Engine. It also works with third-party SIMPLE-based instant messaging clients, such as Sametime, Xten, and GAIM. An entity can send the Cisco Unified Presence Engine a SUBSCRIBE message through the proxy. After policy is applied, the Cisco Unified Presence Engine sends the appropriate presence status in NOTIFY messages. Also, a SIMPLE interface exists that is available external to the Enterprise. [Figure 1](#) shows the overall Cisco Unified Presence Server system architecture.

Figure 1 Cisco Unified Presence Server System Architecture



Address of Record Definition

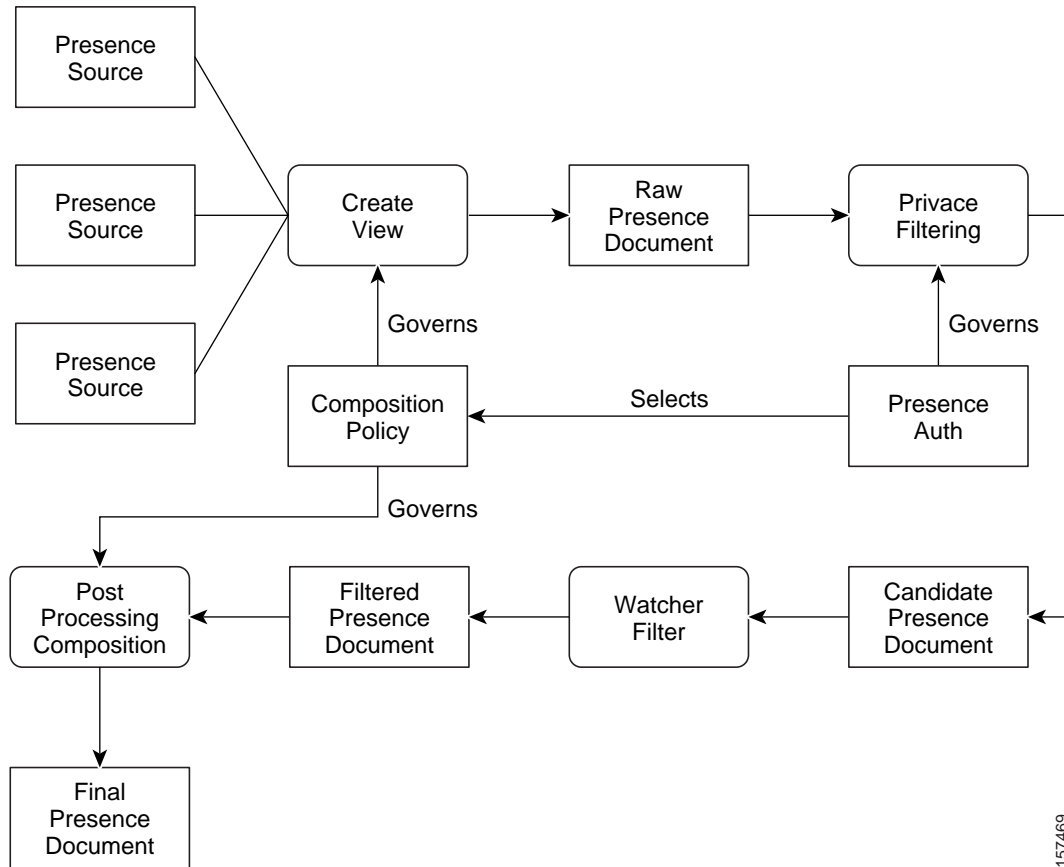
In this architecture, a single Address of Record (AOR) represents or addresses a human user. This AOR typically has the form of *username@domain.com*. The user who is represented by this AOR may have multiple devices and/or components of state. The AOR itself gets provisioned as a distinct resource on the Cisco Unified Presence Engine, whereas the individual does not.

Some components of state get received through a PUBLISH from the client (through the proxy). The Cisco Unified Presence Engine retrieves other components of state through a series of back-end subscriptions. The back-end sources of state must get provisioned at the Cisco Unified Presence Engine. Each component of state gets assigned a provisioned priority.

Composition and Filtering

Figure 2 shows generically how composition and filtering are applied after the components of state are collected.

Figure 2 *Presence Data Model Processing*



157469

Persona composition policy governs the combination of all components of state. After the state is composed, privacy (presentity asserted) and watcher (subscriber asserted) filtering rules get applied to modify the composed state prior to sending to the watcher. The privacy filters remain outside the scope of this interface document because they involve a non-SIMPLE means for a presentity to define filtering rules concerning who can watch what subset of persona state. The subscriber determines watcher filtering rules.

SIMPLE Interface

This section describes the SIP (Session Initiation Protocol) for Instant Messaging and Presence Leveraging Extensions (SIMPLE) interface for Cisco Unified Presence Server.

Industry Standards Requirements

The following list shows the applicable industry standards that describe the SIMPLE interface supported for the presence package by the Cisco Unified Presence Engine:

- RFC3261—SIP: Session Initiation Protocol
- RFC3265—Session Initiation Protocol (SIP)-Specific Event Notification
- RFC3856—A Presence Event Package for the Session Initiation Protocol (SIP)

- RFC 3863—Presence Information Data Format (PIDF)
- RFC3903—Session Initiation Protocol (SIP) Extension for Event State Publication
- RFC4480—RPID: Rich Presence: Extensions to the Presence Information Data Format (PIDF)
- RFC4480—A Data Model for Presence
- draft-ietf-simple-prescaps-ext-03—User Agent Capability Extension to Presence Information Data Format (PIDF)
- draft-ietf-simple-event-list-07—A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists

Other pidf Extensions

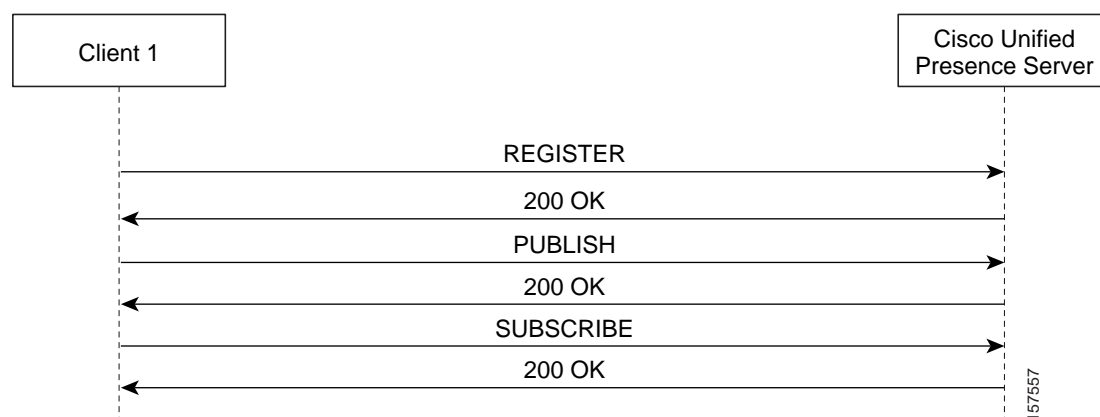
Because the Cisco Unified Presence Engine is agnostic to pidf extensions, any Presence User Agent Client or Presence User Agent Server that interfaces with the Cisco Unified Presence Engine must be prepared to handle these extensions.

Call Flows

This section provides examples of call flows to show the interfaces into and out of Cisco Unified Presence Server.

[Figure 3](#) shows the messaging exchange for a client to log in to the Cisco Unified Presence Server.

Figure 3 Call Flow for a Client Log In to the Cisco Unified Presence Server



[Figure 4](#) shows the messaging exchange for Client 2 to PUBLISH its own state to the Cisco Unified Presence Server, as well as the messaging exchange for a separate Client 1 to subscribe to that presence state.

Figure 4 Call flow for PUBLISH and Subscribe to Local Resource

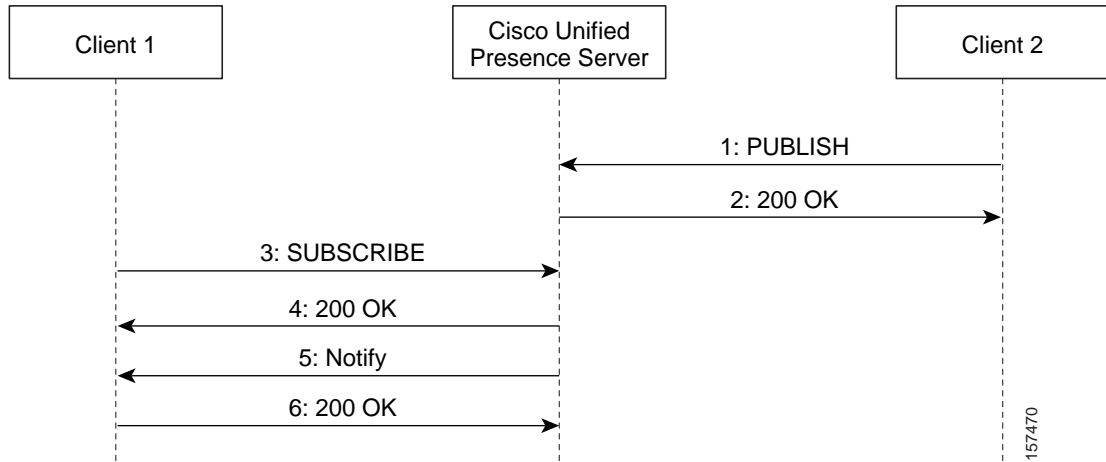


Figure 5 shows the messaging exchange for the case when a client subscribes to the presence state of a resource that is not stored locally on the Cisco Unified Presence Engine. In this scenario, the Cisco Unified Presence Engine will create a back-end subscription to the Cisco Unified Presence Server that has the presence state stored locally to retrieve the state and send it on in a NOTIFY to the watcher/subscriber.

Figure 5 Call Flow for SUBSCRIBE to Foreign Resource

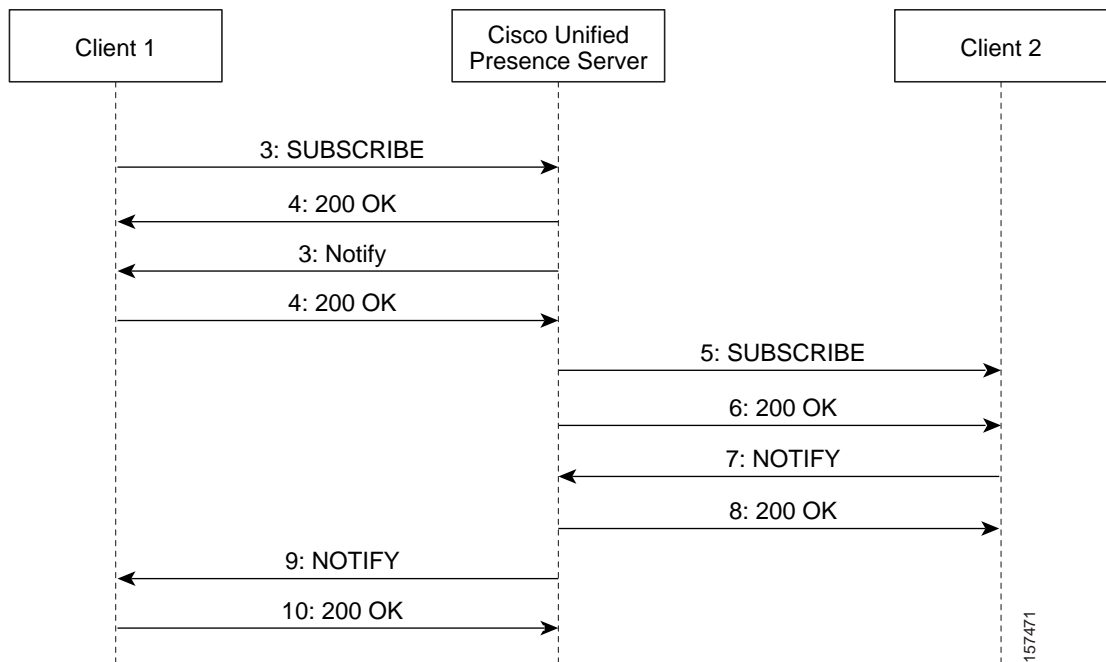
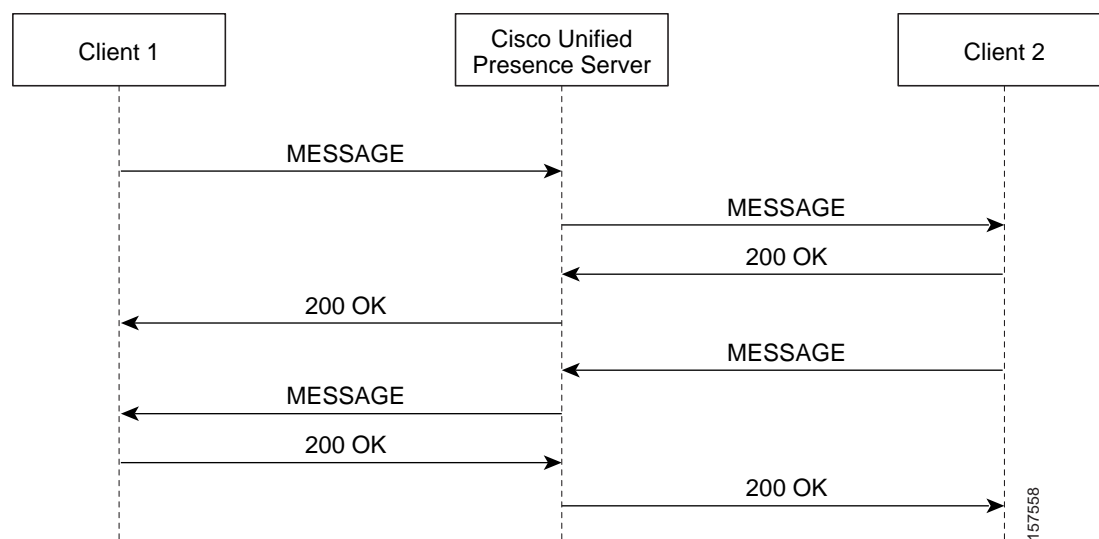


Figure 6 shows the call flow into and out of the instant messaging clients. Each client registers with the Cisco Unified Presence Server registrar and publishes its own status. Each client then subscribes to the status of its buddy and receives notifications. At this point, either client can send an instant message to the other.

Figure 6 Call Flow for IP Phone Messenger



Transport

The Cisco Unified Presence Engine uses the protocols, TLS, TCP, or UDP, for the transport type for the SIP messages. See the [“Security” section on page 7](#) for more information.

Security

In the Enterprise Presence product, no support exists on the Cisco Unified Presence Engine for MD5 authentication. A proxy server in the Cisco Unified Presence Server architecture performs authentication of the users. After configuration, the Cisco Unified Presence Engine only accepts requests from “trusted peers”. The authentication that is performed at the Cisco Unified Presence Engine involves the configuration of these trusted peer elements, by using either IP addresses for nodes that communicate over IPsec or TLS Subject Alt names for nodes that communicate over TLS.

In Cisco Unified Presence Server 1.0, the list of trusted peers gets configured automatically to include the proxy and Cisco Unified CallManager nodes. This configuration does not include TLS.

Subscription Description

[Example 1](#) shows the SUBSCRIBE message that gets sent from the watcher device to the Cisco Unified Presence Engine. [Table 1](#) describes the bold Headers that need mapping to the provisioned information for the Cisco Unified Presence Engine. For the headers that are not in bold, refer to the appropriate SIMPLE/SIP specification.

On a refresh SUBSCRIBE, only the expiration time gets extended. The characteristics that define the subscription, that is, the other bold fields, should not change in a refresh SUBSCRIBE. If the client wants to change the characteristics of the subscription, terminate the existing subscription and create a new subscription.

Example 1 Subscribe message

```

SUBSCRIBE sip:xten3@compB.cisco.com:5060;transport=tcp SIP/2.0
Via: SIP/2.0/TCP 57.1.1.15:5060;branch=7d37939e-f68c2040-34226455-fb8872e6-1
Via: SIP/2.0/UDP 57.1.1.15:5051;received=57.1.1.15
From: <sip:ippm4@compB.cisco.com>;tag=82c1000
To: <sip:xten3@compB.cisco.com:5060;transport=TCP>
Call-ID: 4207647f-178-2f538b99-8c4@57.1.1.15
Csque: 166 SUBSCRIBE
Contact: <sip:ippm4@57.1.1.15:5060>
Content-Length: 0
Event: presence
Accept: application/pidf+xml
Expires: 300
User-Agent: MeetingPlace/5.1
P-Asserted-Identity: <sip:ippm4@compB.cisco.com>

```

Table 1 Subscription Header Descriptions

Header Name	Description	Mapping to provisioning
RequestURI	This field contains the URI of the presentity to be watched.	Ensure that the value in this field corresponds to a provisioned alias for a user/persona.
P-Asserted-Identity	This field provides the preferred method for passing the identity of the watcher to the Cisco Unified Presence Engine. It either gets inserted by the proxy, or if included by the end-user client, it gets validated by the proxy.	<p>If the presentity has a URIACL list that is defined for authorization, the value in this field gets matched with the provisioned URI in that list.</p> <p>If the presentity has a URIACL list that is defined for authorization, the value in this field gets matched with the provisioned URI in that list.</p> <p>In addition, if a domain-based watcher filter is provisioned, the domain portion of this URI gets used to match with the provisioned domain filter.</p>
Remote-Party-ID	<p>If P-Asserted-Identity is not supported by the sender, the identity of the watcher gets sent in this field. The Cisco Unified Presence Engine does not use this field if P-Asserted-Identity is present.</p> <p>Example</p> <pre>Remote-Party-ID: <sip:ippm4@compB.cisco.com></pre>	Same as P-Asserted-Identity
From	If the sender supports neither P-Asserted-Identity nor Remote-Party-ID, the identity of the watcher should get sent in this field. This field will get used only if neither a P-Asserted-Identity nor a Remote-Party-ID header is present.	Same as P-Asserted-Identity

Table 1 **Subscription Header Descriptions (continued)**

Header Name	Description	Mapping to provisioning
User-Agent	This field contains the client type and version information for the sender of the request.	The client type and version information in this field gets matched to provisioned filter information for the specified client type and version. For example, if all Cisco Unified MeetingPlace clients should have a phone only state filter applied, this filter gets provisioned for a client type of Cisco Unified MeetingPlace. Any SUBSCRIBE request with a User-Agent header of MeetingPlace results in the phone-only filter being applied.
Expires	This field contains the relative expiration time of the subscription. The value must fall between the configured minimum and maximum expires times that are configured on the Cisco Unified Presence Engine. If it is too small, the Cisco Unified Presence Engine rejects the subscription. If it is too large, the subscription gets accepted but the expiration of the subscription gets set to the configured default expiration time on the Cisco Unified Presence Engine. If the Expires header is not present, the expiration of the subscription gets set to the configured default expiration time on the Cisco Unified Presence Engine.	Not applicable
Event	For Enterprise Presence, the value of this field specifies “presence”. This specification does not cover other Event packages.	Not applicable

Table 1 **Subscription Header Descriptions (continued)**

Header Name	Description	Mapping to provisioning
Accept	Set this field to the list of accepted mime types for the subscription. Mime types other than those supported by the Cisco Unified Presence Engine exist in the header as long as one or more of the mime types match those that the Cisco Unified Presence Engine supports.	The following mime types gets used for Cisco Unified Presence Server for an Event type of 'presence': <ul style="list-style-type: none"> • application/pdf+xml • multipart/related (used for list subscriptions) • application/rfmi+xml (used for list subscriptions) • application/cpim-pidf+xml (support of legacy Sametime, will eventually be deprecated) The Cisco Unified Presence Engine may receive or ignore other mime types.
Supported	Set the header to the extensions that are supported.	For list subscriptions, specify the value of "eventlist".

Subscription Response

No message body/payload exists in the response to the subscription. It comes in the Notify, as per RFC3903.

Notification Description

[Example 2](#) shows a Notify request that is sent by the Cisco Unified Presence Engine to a watcher for an authorized subscription. [Table 2](#) provides a description of the usage portions of the message that are in bold.

Example 2 **Notification Description**

```
NOTIFY sip:ippm4@compB.cisco.com:5060 SIP/2.0
Call-ID: 42078b79-e0-30e78af6-8c4@57.1.1.15
From: <sip:xten3@compB.cisco.com:5060;transport=TCP>;tag=52fc53ae
To: <sip:ippm4@compB.cisco.com>;tag=82d1158
Event: presence
CSeq: 1073741825 NOTIFY
Contact: <sip:57.1.1.14:5060>
Content-Length: 599
Content-Type: application/pdf+xml
Subscription-State: active;expires=300
Via: SIP/2.0/UDP 57.1.1.14:5060;branch=z9hG4bK76d2e702-1dd2-11b2-8fe0-b1c8ef4f8c83
Max-Forwards: 69

<?xml version="1.0" encoding="UTF-8"?>
<presence entity="sip:xten3@compB.cisco.com" xmlns="urn:ietf:params:xml:ns:pidf"
>
  <dm:person xmlns:dm=" urn:ietf:params:xml:ns:pidf:data-model" id="p1" >
    <r:activities xmlns:r="urn:ietf:params:xml:pidf:rpidd">
      <ce:available xmlns:ce=" urn:cisco:params:xml:ns:pidf:rpidd"/>
    </r:activities>
  </dm:person>
</presence>
```

```

        </r:activities>
    </dm:person>
    <tuple xmlns="urn:ietf:params:xml:ns:pidf" id="t31">
        <contact priority="1">sip:xten3@57.1.1.15</contact>
        <sc:sercvaps xmlns:sc="urn:ietf:params:xml:ns:pidf:sercvaps">
            <sc:audio>true</sc:audio>
            <sc:video>false</sc:video>
            <sc:text>true</sc:text>
        </sc:sercvaps>
        <r:user-input
xmlns:r="urn:ietf:params:xml:ns:pidf:rpidd:status:rpidd">active</r:user-input>
            <status>
                <basic>open</basic>
            </status>
        </tuple>
    <tuple xmlns="urn:ietf:params:xml:ns:pidf" id="t32">
        <contact priority="1">sip:xten4@57.1.1.16</contact>
        <sc:sercvaps xmlns:sc="urn:ietf:params:xml:ns:pidf:sercvaps">
            <sc:audio>true</sc:audio>
            <sc:video>false</sc:video>
            <sc:text>true</sc:text>
        </sc:sercvaps>
        <r:user-input xmlns:es="urn:ietf:params:xml:ns:pidf:rpidd:status:rpidd"
>active</r:user-input>
            <status>
                <basic>open</basic>
            </status>
        </tuple>
    </presence>

```

Table 2 Notify Message Description

Field Name	Description
Subscription-State	This field contains the state of the subscription. If the subscription is active, the field includes expiration time of the subscription. Otherwise, the field includes the reason for the termination of the subscription.
Content-Type	This field contains the mime type of the message body. It will correlate to one of the mime types that were sent in the Accept header of the initial SUBSCRIBE request.
Message body	<p>This XML document describes the state of the presentity. It represents the resulting document after any composition, privacy filtering, or watcher filtering has been applied. Because this may contain composed state, the client must be able to accept multiple tuples that correspond to the multiple device states for the presentity.</p> <p>Extensions to base pidf get sent from the Cisco Unified Presence Engine, and the client must handle them appropriately; for example, the client ignores extensions that it does not use.</p> <p>Typically, one tuple exists per device.</p>
<audio>	<p>This element in the published document indicates whether the class of service of audio (for example, phone) is available.</p> <p>Note Multiple classes of services can get published from the same device.</p>
<text>	<p>This element in the published document indicates whether the class of service of text (for example, IM) is available.</p> <p>Note Multiple classes of services can get published from the same device.</p>

Table 2 **Notify Message Description (continued)**

Field Name	Description
<user-input>	This element in the published document indicates activity on the device (for example, keyboard, pointing device, or voice).
<video>	<p>This element in the published document indicates whether the class of service of video is available.</p> <p>Note Multiple classes of services can get published from the same device.</p>
<person>	<p>This element provides information about the “reachability” status of the persona. It also includes elements that indicate certain activities that are reported from the user devices, such as “meeting”, and so on, as defined in the rpid draft. The following mapping shows the Cisco Unified Presence Server defined reachability status values in the that way they get reported by the Cisco Unified Presence Engine in the <person> element, where id represents a mandatory parameter for the person element that was introduced in RFC4479.</p> <p>Available</p> <pre data-bbox="602 772 894 905"><dm:person id="p1" > <r:activities> <ce:available/> </r:activities> </dm:person></pre> <p>Busy</p> <pre data-bbox="602 961 867 1087"><dm:person id="p2" > <r:activities> <r:busy/> </r:activities> </dm:person></pre> <p>Do Not Disturb</p> <pre data-bbox="602 1144 867 1270"><dm:person id="p3" > <r:activities> <ce:dnd/> </r:activities> </dm:person></pre> <p>Away</p> <pre data-bbox="602 1327 867 1453"><dm:person id="p4" > <r:activities> <r:away/> </r:activities> </dm:person></pre>

Table 2 *Notify Message Description (continued)*

Field Name	Description
<person> (continued)	<p>On Vacation</p> <pre><dm:person id="p5" > <r:activities> <r:vacation/> </r:activities> </dm:person></pre> <p>Unavailable</p> <pre><dm:person id="p6" > <r:activities> <ce:unavailable/> </r:activities> </dm:person></pre> <p>Unknown</p> <pre><dm:person id="p7" > <r:activities> <r:unknown/> </r:activities> </dm:person></pre>

Event List Notification

[Example 3](#) shows a NOTIFY request for the state of a list subscription. The Require header gets included with a value of eventlist for a Notification due to a list subscription.

Example 3 *Notify Request of the State of a List Subscription*

```
NOTIFY sip:handset0@10.21.91.156:5060 SIP/2.0
Call-ID: 2085017328@10.21.91.156
From: <sip:publisher@cisco.com>;tag=970c4542
To: <sip:publisher@cisco.com>
Event: presence
CSeq: 2045 NOTIFY
Contact: <sip:10.89.51.203:5060>
Content-Length: 1344
Content-Type:
multipart/related;type="application/rlmi+xml";start="<972014@10.89.51.203>";boundary="97201414-1dd1-11b2-b"
Require: eventlist
Subscription-State: terminated;reason=timeout
Via: SIP/2.0/UDP 10.89.51.203:5060;branch=z9hG4bK9721baee-1dd1-11b2-b7c3-f9efc6ad7818
Max-Forwards: 69

--97201414-1dd1-11b2-b
Content-Transfer-Encoding: binary
Content-ID: <972014@10.89.51.203>
Content-Type: application/rlmi+xml;charset="UTF-8"

<?xml version="1.0" encoding="UTF-8"?>
<list xmlns="urn:ietf:params:xml:ns:rlmi" uri="sip:publisher@cisco.com" version="0"
fullState="true"><resource uri="sip:scalar1@cisco.com">

  <instance cid="971a00@10.89.51.203" id="1" state="active"/>

</resource>
<resource uri="sip:scalar2@cisco.com">
```

```

    <instance cid="971a28@10.89.51.203" id="1" state="active"/>
</resource>
</list>

--97201414-1dd1-11b2-b
Content-Transfer-Encoding: binary
Content-ID: <971a00@10.89.51.203>
Content-Type: application/pidf+xml

<?xml version="1.0" encoding="UTF-8"?>

<presence entity="sip:scalar1@cisco.com" >
    <dm:person xmlns:dm="urn:ietf:params:xml:ns:pidf:data-model" id="p1" >

        <r:activities xmlns:r="urn:ietf:params:xml:ns:pidf:rpidd" >
            <ce:available xmlns:ce="urn:cisco:params:xml:ns:pidf:rpidd" />
        </r:activities>

    </dm:person>
    <tuple xmlns="urn:ietf:params:xml:ns:pidf" id="t31">
        <contact priority="1">sip:scalar1@57.1.1.15</contact>
        <sc:servcaps xmlns:sc="urn:ietf:params:xml:ns:pidf:servcaps">
            <sc:audio>true</sc:audio>
            <sc:video>false</sc:video>
            <sc:text>true</sc:text>
        </sc:servcaps>
        <r:user-input
xmlns:r="urn:ietf:params:xml:ns:pidf:rpidd:status:rpidd">active</r:user-input>
        <status>
            <basic>open</basic>
        </status>
    </tuple>
    <tuple xmlns="urn:ietf:params:xml:ns:pidf" id="t32">
        <contact priority="1">sip:xten4@57.1.1.16</contact>
        <sc:servcaps xmlns:sc="urn:ietf:params:xml:ns:pidf:servcaps">>
            <sc:audio>true</sc:audio>
            <sc:video>false</sc:video>
            <sc:text>true</sc:text>
        </sc:servcaps>
        <r:user-input
xmlns:r="urn:ietf:params:xml:ns:pidf:rpidd:status:rpidd">active</r:user-input>
        <status>
            <basic>open</basic>
        </status>
    </tuple>

</presence>
--97201414-1dd1-11b2-b
Content-Transfer-Encoding: binary
Content-ID: <971a28@10.89.51.203>
Content-Type: application/pidf+xml

<?xml version="1.0" encoding="UTF-8"?>
<presence entity="sip:scalar2@cisco.com"
>
    <dm:person xmlns:dm="urn:ietf:params:xml:ns:pidf:data-model" id= "p2">

        <r:activities xmlns:r="urn:ietf:params:xml:ns:pidf:rpidd" >
            <ce:available xmlns:ce="urn:cisco:params:xml:ns:pidf:rpidd" />
        </r:activities>
    </dm:person>

```

```

    <tuple xmlns="urn:ietf:params:xml:ns:pidf" id="t31">
      <contact priority="1">sip:scalar2@57.1.1.15</contact>
    <sc:sercvaps xmlns:sc="urn:ietf:params:xml:ns:pidf:sercvaps">
      <sc:audio>true</sc:audio>
      <sc:video>>false</sc:video>
      <sc:text>true</sc:text>
    </sc:sercvaps>
    <r:user-input xmlns:es="urn:ietf:params:xml:ns:pidf:rpiddata-model:status:rpiddata-model"
>active</r:user-input>
      <status>
        <basic>open</basic>
      </status>
    </tuple>
    <tuple xmlns="urn:ietf:params:xml:ns:pidf" id="t32">
      <contact priority="1">sip:xten4@57.1.1.16</contact>
    <sc:sercvaps xmlns:sc="urn:ietf:params:xml:ns:pidf:sercvaps">
      <sc:audio>true</sc:audio>
      <sc:video>>false</sc:video>
      <sc:text>true</sc:text>
    </sc:sercvaps>
    <r:user-input xmlns:r="urn:ietf:params:xml:ns:pidf:rpiddata-model:status:rpiddata-model"
>active</r:user-input>
      <status>
        <basic>open</basic>
      </status>
    </tuple>
  </presence>
--97201414-1dd1-11b2-b--

```

Publication Description

[Example 4](#) shows a Publish request that is sent to the Cisco Unified Presence Engine from a Presence UAC. [Table 3](#) describes the usage portions of the message that are in bold.

Example 4 Publish Request

```

PUBLISH sip:xten3@compB.cisco.com:5060;transport=tcp SIP/2.0
Via: SIP/2.0/TCP 57.1.1.15:5060;branch=42fe6223-25e92eae-dd09f88a-7fcf9be6-1
To: <sip:xten3@57.1.1.15>
From: xten3<sip:xten3@compB.cisco.com>;tag=5577e92b
Via: SIP/2.0/UDP
57.1.1.83:6756;received=57.1.1.83;rport=6756;branch=z9hG4bK-d87543-1071201803-1--d87543-
Call-ID: 3178d777074bee32
CSeq: 1 PUBLISH
Contact: <sip:xten3@57.1.1.83:6756>
Expires: 3600
Max-Forwards: 69
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE
Content-Type: application/pidf+xml
User-Agent: eyeBeam release 8888a stamp 16336 (sn:a0d46d0c5ff5ecfbb8d8)
P-Asserted-Identity: < sip:xten3@compB.cisco.com >

Event: presence
Content-Length: 591

<?xml version="1.0" encoding="UTF-8"?>
<presence xmlns="urn:ietf:params:xml:ns:pidf"

  xmlns:r="urn:ietf:params:xml:ns:pidf:rpiddata-model"
  xmlns:dm="urn:ietf:params:xml:ns:pidf:data-model"

```

```

xmlns:ce="urn:cisco:params:xml:ns:pidf:rpid"
xmlns:ci="urn:ietf:params:xml:ns:pidf:cipid"
xmlns:sc="urn:ietf:params:xml:ns:pidf:servcaps"
xmlns:so="urn:cisco:params:xml:ns:pidf:source"
entity="sip:xten3@57.1.1.15">
  <dm:person id="p3">

    <r:activities >
      <ce:available />
    </r :activities >
  </dm:person>
<tuple id="t0">
  <contact priority="1">sip:xten3@57.1.1.15</contact>
<so:source> Manually set by persona </so:source>
  <sc:servcaps>
    <sc:audio>true</sc:audio>
    <sc:video>false</sc:video>
    <sc:text>true</sc:text>
  </sc:servcaps>

  <r:user-input>active</r:user-input>
  <status>
    <basic>open</basic>
  </status>
</tuple>
</presence>

```

Table 3 Publish Message Description

Header/Field Name	Description	Mapping to Provisioning
RequestURI	This field contains the URI of the presentity for which the state belongs.	Ensure that the value in this field corresponds to a provisioned alias for a user/persona.
P-Asserted-Identity	This field provides the preferred method to pass the identity of the presentity to the Cisco Unified Presence Engine. It either gets inserted by the proxy, or, if included by the end-user client, the proxy validates it.	This field authorizes the Publish request according to the authorization policy. For Publish authorization, you typically set to “self”, which means that the URI in the P-asserted-Identity needs to map to the same user that corresponds to the RequestURI.
Remote-Party-ID	If the sender does not support P-Asserted-Identity, the identity of the presentity gets sent in this field. The Cisco Unified Presence Engine does not use this field if P-Asserted-Identity is present. Example: Remote-Party-ID: <sip:xten3@compB.cisco.com>	Same as P-Asserted-Identity

Table 3 Publish Message Description (continued)

Header/Field Name	Description	Mapping to Provisioning
From	If the sender does not support either P-Asserted-Identity or Remote-Party-ID, the identity of the presentity gets sent in this field. This field only gets used if neither a P-Asserted-Identity nor a Remote-Party-ID header is present.	Same as P-Asserted-Identity
Content-Type	This header contains the mime type of the document that the message body contains.	For the presence package, the appropriate mime type specifies application/pidf+xml
<source>	<p>This element in the Published document indicates the source of the publish request to determine whether this source has a specific “priority” associated with it. This proprietary element resides within the following namespace: "urn:cisco:params:xml:ns:pidf:source"</p> <p>For example, the instant messaging client or Cisco Unified Personal Communicator applications send a specific value in <i>source</i> when they want to invoke the manual override of state functionality.</p>	<p>The value in this field must match the provisioned value in the Source Priority provisioning. Any value that is received that does not match a provisioned value gets ignored.</p> <p>This element gets compared against the reachability rules definition.</p>
<audio>	<p>This element in the published document indicates whether the class of service of audio (for example, phone) is available.</p> <p>Note Multiple classes of services can get published from the same device.</p>	<p>The value of “true” in this field indicates that the state being published is that of a phone device.</p> <p>Phone only watcher or privacy filters get compared against this field to distinguish which pieces of state are associated with “phone” devices.</p>
<text>	<p>This element in the published document indicates whether the class of service of text (for example, IM) is available.</p> <p>Note Multiple classes of services can be published from the same device.</p>	<p>Use the value of “true” to indicate that the state that is being published is that of an IM device.</p> <p>IM only type filters get compared against this field to distinguish which pieces of state are associated with “IM” devices.</p>
<video>	<p>This element in the published document indicates whether the class of service of video is available.</p> <p>Note Multiple classes of services can get published from the same device.</p>	<p>Use the value of “true” in this field to indicate that the state that is being published is that of a video-capable device.</p>

Table 3 *Publish Message Description (continued)*

Header/Field Name	Description	Mapping to Provisioning
<user-input>	This element in the published document indicates activity on the device (for example, keyboard, pointing device, or voice).	This value gets transmitted to a watcher without a filter in this release.
<activities>	This element in the published document indicates whether the device is on-the-phone, busy, and so on.	Values of on-the-phone or busy identify reachability states of Busy or Interruptible But Busy when the reachability rules algorithm is applied. Other activities do not affect the reachability algorithm but get included in the composed document that is sent to the watchers in the NOTIFY.
Expires	<p>This field contains the relative expiration time of the publish. The value must fall between the configured minimum and maximum expires times that are configured on the Cisco Unified Presence Engine. If it is too small, the Cisco Unified Presence Engine rejects the publication. If it is too large, the publication gets accepted, but the expiration of the publication gets set to the configured default expiration time on the Cisco Unified Presence Engine.</p> <p>If the Expires header is not present, the expiration of the publication gets set to the configured default expiration time on the Cisco Unified Presence Engine.</p>	On a periodic basis, the expired published state gets removed from the Cisco Unified Presence Engine soft-state information.
User-Agent	This field contains the client type and version information for the sender of the request.	<p>The client type and version information in this field get compared to a pre-configured table that identifies the class of service that is available from that client type. Use this configuration to determine class of service if the information is not provided in the pidf body of the message.</p> <p>If the class of service information is not provided in the message body and no configuration for the type of User-Agent exists (or the User-Agent header is missing), the default set of capabilities for the device specifies IM/text.</p>

Publication Response

No message body/payload occurs in the response to the publication. All presence status gets retrieved from the Cisco Unified Presence Engine via SUBSCRIBE/NOTIFY as per RFC3903.

Back-end Subscription Description

When some or all the state for a user is not stored locally at the Cisco Unified Presence Engine, it may create a back-end subscription to the element that is responsible for storing that state. Refer to the [“Subscription Description” section on page 7](#) for an example of a SUBSCRIBE message.

Table 4 *Back-end Subscription Header Descriptions*

Header Name	Description	Mapping to Provisioning
RequestURI	This field contains the URI of the presentity to be watched. This may differ from the URI of the presentity that the received.	The Cisco Unified Presence Engine provides a provisioned mapping of local presentity URIs to foreign back-end presentity URIs when applicable. An example would be a subscription received by the Cisco Unified Presence Engine for a whole persona, 'sip:joe@cisco.com', that may result in a back-end subscription to obtain phone state for the phone that is owned by Joe, 'sip:5555@cm.cisco.com'.
P-Asserted-Identity	This header gets set to the original watcher identity that Cisco Unified Presence Engine receives. That identity comes from the P-Asserted-Identity, Remote-Party-ID, or from headers as described in Table 3 .	Not applicable
From	This header gets set to the original watcher identity that the Cisco Unified Presence Engine receives. That identity comes from the P-Asserted-Identity, Remote-Party-ID, or from headers as described in Table 3 .	Not applicable
Expires	This field contains the relative expiration time of the back-end subscription.	This value comes from either a foreign- server specific provisioned value, or a global default value for all back-end subscriptions.

Table 4 Back-end Subscription Header Descriptions (continued)

Header Name	Description	Mapping to Provisioning
Event	For Enterprise Presence, ensure that the value of this field specifies “presence”. This specification does not cover other Event packages.	Not applicable
Accept	This field gets sent the list of accepted mime types for the subscription that Cisco Unified Presence Engine received from the original watcher.	<p>The following mime types get used for Cisco Unified Presence Server for an Event type of “presence”:</p> <ul style="list-style-type: none"> • application/pdf+xml • application/cpim-pdf+xml <p>Note If Cisco Unified Presence Engine received additional mime types, they get transmitted to the foreign server.</p>

Notification From Foreign Server Description

The foreign server that receives a back-end subscription request from the Cisco Unified Presence Engine sends the state of the requested resource back to the Cisco Unified Presence Engine in a NOTIFY request. [Example 3](#) shows a NOTIFY request in the “[Notification Description](#)” section on page 10.

The main difference occurs because NOTIFY requests from foreign servers need to also contain a User-Agent header as described in [Table 5](#).

Table 5 NOTIFY Message Description

Field Name	Description
Subscription-State	This field contains the state and expiration time of the subscription that is currently at the foreign server.
Content-Type	This field contains the mime type of the message body. It correlates to one of the mime types that was sent in the Accept header of the back-end SUBSCRIBE request.
Message body	<p>This XML document describes the state of the foreign presentity. It gets fed into the appropriate composition and filtering algorithms before being sent to the original watcher. Also, the foreign presentity gets translated to the local presentity prior to sending in a NOTIFY to the original watcher.</p> <p>See description of specific elements in the following message body.</p>
<source>	<p>Use this element in the message body document to indicate the source of the state to determine whether this source has a specific priority that is associated with it. This proprietary element occurs within the following namespace: "urn:cisco:params:xml:ns:pdf:source"</p> <p>Ensure that the value in this field matches the provisioned value in the Source Priority provisioning. Any value that is received that does not match a provisioned value gets ignored.</p>

Table 5 NOTIFY Message Description (continued)

Field Name	Description
<audio>	<p>This element in the published document indicates whether the class of service of audio (for example, phone) is available.</p> <p>Note Multiple classes of services may get published from the same device.</p> <p>The value of “true” in this field indicates that the state that is being published is a phone device.</p> <p>Phone only watcher or privacy filters get compared against this field to distinguish which pieces of state are associated with phone devices.</p>
<text>	<p>This element in the published document indicates whether the class of service of text (for example, IM) is available.</p> <p>Note Multiple classes of services may get published from the same device.</p> <p>The value of “true” in this field indicates that the state that is being published is an IM device.</p> <p>IM only type of filters get compared against this field to distinguish which pieces of state are associated with IM devices.</p>
<video>	<p>This element in the published document indicates whether the class of service of video is available.</p> <p>Note Multiple classes of service may get published from the same device.</p> <p>The value of “true” in this field indicates that the state that is being published is that of a video-capable device.</p>
<user-input>	<p>This element in the published document indicates activity on the device (for example, keyboard, pointing device, or voice)</p> <p>This value gets transmitted to a watcher without a filter.</p>
<activities>	<p>This element in the published document indicates whether the device is on-the-phone, busy, and so on.</p>
User-Agent	<p>This field contains the client type and version information for the sender of the request.</p> <p>The client type and version information in this field gets matched to a preconfigured table that identifies the class of service that is available from that client type. Use this configuration to determine the class of service when the information is not provided in the pidf body of the message.</p> <p>If the class of service information is not provided in the message body and no configuration for the type of User-Agent exists (or the User-Agent header is missing), the default set of capabilities for the device specifies IM/text.</p>

Instant Messaging Applications

This section provides information related to instant messaging applications. The following standard provides the basis for the Cisco Unified Presence Server instant messaging interface:

RFC3428—Session Initiation Protocol (SIP) Extension for Instant Messaging

Subscription Description

Instant messaging applications subscribe to the presence status of each buddy that you have provisioned. You can configure the duration of the subscription, and it gets refreshed as long as the user is logged in to the instant messaging application. All subscriptions get terminated when the user logs out.

Notification Description

The instant messaging application receives presence event notifications from the Cisco Unified Presence Engine while the subscription remains active. See [“Notification Description” section on page 10](#) for more information.

Publication Description

The instant messaging application publishes status changes to the Cisco Unified Presence Engine whenever the user logs in, logs out, or manually overrides his status. See the [“Publication Description” section on page 15](#) for more information.

Register Description

[Example 5](#) shows an example Register request by which clients receive instant messages. [Table 6](#) provides a description of the Register Description fields.

Example 5 Register Request

```
REGISTER sip:cisco.com:5060;transport=tcp SIP/2.0
Via: SIP/2.0/TDP 172.18.201.90:5060;branch=z9hG4bK-8337e00
To: xten4<sip:xten4@comB.cisco.com>
From: xten4<sip:xten4@compB.cisco.com>;tag=5577e92b
Call-ID: 5543173d19-c8-6825acfd-767b@comB.cisco.com
CSeq: 101 REGISTER
Contact: <sip:xten4@172.18.201.90:5060>;q=0.5
Max-Forwards: 69
P-Asserted-Identity: <sip:xten3@cisco.com>
Expires: 3600
Content-Type: text/plain; charset=UTF-8
User-Agent: CSCO/IPPM-1.0
Content-Length: 0
```

Table 6 Register Description Field Descriptions

Field Name	Description
RequestURI	This field specifies the recipient and has the following format: <i>recipient@domain</i>
q-value	This parameter specifies the relative preference of this client to receive IMs addressed to this user.

Table 6 Register Description Field Descriptions (continued)

Field Name	Description
P-Asserted-Identity	This field gets added by the proxy after it authenticates the client.
Expires	This field specifies the duration that this client will accept incoming message requests and gets set to 0 when the client unregisters.

Message Description

[Example 6](#) shows an example Message request that gets sent between clients. [Table 7](#) provides a description of the Message Description fields.

Example 6 Message Description

```
MESSAGE sip:xten4@esp.compB.cisco.com:5060;transport=tcp SIP/2.0
Via: SIP/2.0/TDP 172.18.201.90:5060;received=172.18.201.90;branch=z9hG4bK-8337e00
To: xten4<sip:xten4@cisco.com>
From: xten3<sip:xten3@compB.cisco.com>;tag=5577e92b
Call-ID: 43173d19-c8-6825abfd-767b@comB.cisco.com
CSeq: 101 MESSAGE
Contact: <sip:xten3@57.1.1.2:5060>
Max-Forwards: 69
P-Asserted-Identity: <sip:xten3@cisco.com>
Content-Type: text/plain; charset=UTF-8
User-Agent: CSCO/IPPM-1.0
Content-Length: 12
```

Hello xten4!

Table 7 Message Description Field Descriptions

Field Name	Description
RequestURI	This field specifies the recipient and has the following format: <i>recipient@domain</i>
P-Asserted-Identity	This field gets added by the proxy after it authenticates the client.
Content-Type	This field is always set to text/plain.

CTI Gateway

The Computer Telephony Integration (CTI) gateway supports receiving and sending messages, as defined in ECMA 323, 3rd edition, between a client and a CTI gateway.

Events

CTI Gateway supports the following events:

- Connection cleared
- Delivered

- Established
- Diverted
- Failed
- Held
- Retrieved
- Transferred
- Originated
- Conferenced
- Do not disturb
- Forwarding
- Service completion failure

Services

CTI gateway supports the following services:

- Make call
- Answer call
- Clear connection
- Deflect
- Hold
- Retrieve
- Consultation
- Single step transfer
- Transfer
- Conference call
- Alternate
- Reconnect
- Generate digits
- Set forwarding
- Set DND
- Get forwarding
- Get DND

System Services

CTI gateway supports the following system services:

- Start Monitor
- Stop Monitor

- Request System Status
- Get CSTA Features

Connection States

CTI gateway supports the following connection states:

- Alerting
- Connected
- Failed
- Held
- Initiated
- Null

Error Conditions

CTI gateway supports the following error conditions:

- serviceNotSupported
- invalidMonitorObjectType
- invalidCrossReferenceIdentifier
- invalidCallingDeviceIdentifier
- invalidCalledDeviceIdentifier
- noCallToAnswer
- invalidConnectionIdentifier
- invalidConnectionState
- noConnectionToClear
- invalidDestination
- invalidDestinationDeviceObject
- invalidDivertingDeviceIdentifier
- invalidHeldDeviceIdentifier
- invalidHeldDeviceState
- NoHeldCall
- invalidParameterValue
- invalidForwardingDestination.

Related Documentation

The following documents contain additional information related to Cisco Unified Presence Server:

- *Cisco Unified Presence Server Administration Guide*
- Cisco Unified Presence Server Serviceability Administration Guide
- Cisco Unified Communications Operating System Administration Guide
- Cisco IP Phone Messenger User Guide for Cisco Unified Presence Server

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302

- 1 408 525-6532

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

To register as a Cisco.com user, go to this URL:

<http://tools.cisco.com/RPF/register/register.do>

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

<http://www.cisco.com/en/US/support/index.html>

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

**Tip****Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

<http://www.cisco.com/offer/subscribe>

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

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

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:
<http://www.cisco.com/univercd/cc/td/doc/abtnucd/136957.htm>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

