The In-Reply-To header field enumerates the Call-IDs that this call references or returns. These Call-IDs may have been cached by the client then included in this header field in a return call.

This allows automatic call distribution systems to route return calls to the originator of the first call. This also allows callees to filter calls, so that only return calls for calls they originated will be accepted. This field is not a substitute for request authentication.

Example:

In-Reply-To: 70710@saturn.bell-tel.com, 17320@saturn.bell-tel.com

20.22 Max-Forwards

The Max-Forwards header field must be used with any SIP method to limit the number of proxies or gateways that can forward the request to the next downstream server. This can also be useful when the client is attempting to trace a request chain that appears to be failing or looping in mid-chain.

The Max-Forwards value is an integer in the range 0-255 indicating the remaining number of times this request message is allowed to be forwarded. This count is decremented by each server that forwards the request. The recommended initial value is 70.

This header field should be inserted by elements that can not otherwise guarantee loop detection. For example, a B2BUA should insert a Max-Forwards header field.

Example:

Max-Forwards: 6

20.23 Min-Expires

The Min-Expires header field conveys the minimum refresh interval supported for soft-state elements managed by that server. This includes Contact header fields that are stored by a registrar. The header field contains a decimal integer number of seconds from 0 to (2**32)-1. The use of the header field in a 423 (Interval Too Brief) response is described in Sections 10.2.8, 10.3, and 21.4.17.

Example:

Min-Expires: 60

20.24 MIME-Version

See [H19.4.1].

Example:

MIME-Version: 1.0

Page 1541
T-Mobile Exhibit 1002
Part 5 of 6

20.25 Organization

The Organization header field conveys the name of the organization to which the SIP element issuing the request or response belongs.

The field MAY be used by client software to filter calls.

Example:

```
Organization: Boxes by Bob
```

20.26 Priority

The Priority header field indicates the urgency of the request as perceived by the client. The Priority header field describes the priority that the SIP request should have to the receiving human or its agent. For example, it may be factored into decisions about call routing and acceptance. For these decisions, a message containing no Priority header field SHOULD be treated as if it specified a Priority of "normal". The Priority header field does not influence the use of communications resources such as packet forwarding priority in routers or access to circuits in PSTN gateways. The header field can have the values "non-urgent", "normal", "urgent", and "emergency", but additional values can be defined elsewhere. It is RECOMMENDED that the value of "emergency" only be used when life, limb, or property are in imminent danger. Otherwise, there are no semantics defined for this header field.

These are the values of RFC 2076 [38], with the addition of "emergency".

Examples:

```
Subject: A tornado is heading our way!
Priority: emergency
```

or

```
Subject: Weekend plans
Priority: non-urgent
```

20.27 Proxy-Authenticate

A Proxy-Authenticate header field value contains an authentication challenge.

The use of this header field is defined in [H14.33]. See Section 22.3 for further details on its usage.

Example:

```
Proxy-Authenticate: Digest realm="atlanta.com",
 domain="sip:ss1.carrier.com", qop="auth",
 nonce="f84f1cec41e6cbe5aea9c8e88d359",
 opaque="", stale=FALSE, algorithm=MD5
```

20.28 Proxy-Authorization

The Proxy-Authorization header field allows the client to identify itself (or its user) to a proxy that requires authentication. A Proxy-Authorization field value consists of credentials containing the authentication information of the user agent for the proxy and/or realm of the resource being requested.

See Section 22.3 for a definition of the usage of this header field.

This header field, along with Authorization, breaks the general rules about multiple header field names. Although not a comma-separated list, this header field name may be present multiple times, and MUST NOT be combined into a single header line using the usual rules described in Section 7.3.1.

Example:

```
Proxy-Authorization: Digest username="Alice", realm="atlanta.com",
   nonce="c60f3082ee1212b402a21831ae",
   response="245f23415f11432b3434341c022"
```

20.29 Proxy-Require

The Proxy-Require header field is used to indicate proxy-sensitive features that must be supported by the proxy. See Section 20.32 for more details on the mechanics of this message and a usage example.

Example:

```
Proxy-Require: foo
```

20.30 Record-Route

The Record-Route header field is inserted by proxies in a request to force future requests in the dialog to be routed through the proxy.

Examples of its use with the Route header field are described in Sections 16.12.1.

Example:

```
Record-Route: <sip:server10.biloxi.com;lr>,
              <sip:bigbox3.site3.atlanta.com;lr>
```

20.31 Reply-To

The Reply-To header field contains a logical return URI that may be

different from the From header field. For example, the URI MAY be used to return missed calls or unestablished sessions. If the user wished to remain anonymous, the header field SHOULD either be omitted from the request or populated in such a way that does not reveal any private information.

Even if the "display-name" is empty, the "name-addr" form MUST be used if the "addr-spec" contains a comma, question mark, or semicolon. Syntax issues are discussed in Section 7.3.1.

Example:

```
Reply-To: Bob <sip:bob@biloxi.com>
```

20.32 Require

The Require header field is used by UACs to tell UASs about options that the UAC expects the UAS to support in order to process the request. Although an optional header field, the Require MUST NOT be ignored if it is present.

The Require header field contains a list of option tags, described in Section 19.2. Each option tag defines a SIP extension that MUST be understood to process the request. Frequently, this is used to indicate that a specific set of extension header fields need to be understood. A UAC compliant to this specification MUST only include option tags corresponding to standards-track RFCs.

Example:

```
Require: 100rel
```

20.33 Retry-After

The Retry-After header field can be used with a 500 (Server Internal Error) or 503 (Service Unavailable) response to indicate how long the service is expected to be unavailable to the requesting client and with a 404 (Not Found), 413 (Request Entity Too Large), 480 (Temporarily Unavailable), 486 (Busy Here), 600 (Busy), or 603

(Decline) response to indicate when the called party anticipates being available again. The value of this field is a positive integer number of seconds (in decimal) after the time of the response.

An optional comment can be used to indicate additional information about the time of callback. An optional "duration" parameter indicates how long the called party will be reachable starting at the initial time of availability. If no duration parameter is given, the service is assumed to be available indefinitely.

Examples:

```
Retry-After: 18000;duration=3600
Retry-After: 120 (I'm in a meeting)
```

20.34 Route

The Route header field is used to force routing for a request through the listed set of proxies. Examples of the use of the Route header field are in Section 16.12.1.

Example:

```
Route: <sip:bigbox3.site3.atlanta.com;lr>,
       <sip:server10.biloxi.com;lr>
```

20.35 Server

The Server header field contains information about the software used by the UAS to handle the request.

Revealing the specific software version of the server might allow the server to become more vulnerable to attacks against software that is known to contain security holes. Implementers SHOULD make the Server header field a configurable option.

Example:

```
Server: HomeServer v2
```

20.36 Subject

The Subject header field provides a summary or indicates the nature of the call, allowing call filtering without having to parse the session description. The session description does not have to use the same subject indication as the invitation.

The compact form of the Subject header field is s.

Example:

```
Subject: Need more boxes
s: Tech Support
```

20.37 Supported

The Supported header field enumerates all the extensions supported by the UAC or UAS.

The Supported header field contains a list of option tags, described in Section 19.2, that are understood by the UAC or UAS. A UA compliant to this specification MUST only include option tags corresponding to standards-track RFCs. If empty, it means that no extensions are supported.

The compact form of the Supported header field is k.

Example:

```
Supported: 100rel
```

20.38 Timestamp

The Timestamp header field describes when the UAC sent the request to the UAS.

Page 1545
T-Mobile Exhibit 1002
Part 5 of 6

See Section 8.2.6 for details on how to generate a response to a request that contains the header field. Although there is no normative behavior defined here that makes use of the header, it allows for extensions or SIP applications to obtain RTT estimates.

Example:

```
Timestamp: 54
```

20.39 To

The To header field specifies the logical recipient of the request.

The optional "display-name" is meant to be rendered by a human-user interface. The "tag" parameter serves as a general mechanism for dialog identification.

See Section 19.3 for details of the "tag" parameter.

Comparison of To header fields for equality is identical to comparison of From header fields. See Section 20.10 for the rules for parsing a display name, URI and URI parameters, and header field parameters.

The compact form of the To header field is t.

The following are examples of valid To header fields:

```
To: The Operator <sip:operator@cs.columbia.edu>;tag=287447
t: sip:+12125551212@server.phone2net.com
```

20.40 Unsupported

The Unsupported header field lists the features not supported by the UAS. See Section 20.32 for motivation.

Example:

```
Unsupported: foo
```

20.41 User-Agent

The User-Agent header field contains information about the UAC originating the request. The semantics of this header field are defined in [H14.43].

Revealing the specific software version of the user agent might allow the user agent to become more vulnerable to attacks against software that is known to contain security holes. Implementers SHOULD make the User-Agent header field a configurable option.

Example:

```
User-Agent: Softphone Beta1.5
```


Page 1546
T-Mobile Exhibit 1002
Part 5 of 6

20.42 Via

The Via header field indicates the path taken by the request so far and indicates the path that should be followed in routing responses. The branch ID parameter in the Via header field values serves as a transaction identifier, and is used by proxies to detect loops.

A Via header field value contains the transport protocol used to send the message, the client's host name or network address, and possibly the port number at which it wishes to receive responses. A Via header field value can also contain parameters such as "maddr", "ttl", "received", and "branch", whose meaning and use are described

in other sections. For implementations compliant to this specification, the value of the branch parameter MUST start with the magic cookie "z9hG4bK", as discussed in Section 8.1.1.7.

Transport protocols defined here are "UDP", "TCP", "TLS", and "SCTP". "TLS" means TLS over TCP. When a request is sent to a SIPS URI, the protocol still indicates "SIP", and the transport protocol is TLS.

```
Via: SIP/2.0/UDP erlang.bell-telephone.com:5060;branch=z9hG4bK87asdks7
Via: SIP/2.0/UDP 192.0.2.1:5060 ;received=192.0.2.207
     ;branch=z9hG4bK77asjd
```

The compact form of the Via header field is v.

In this example, the message originated from a multi-homed host with two addresses, 192.0.2.1 and 192.0.2.207. The sender guessed wrong as to which network interface would be used. Erlang.bell-telephone.com noticed the mismatch and added a parameter to the previous hop's Via header field value, containing the address that the packet actually came from.

The host or network address and port number are not required to follow the SIP URI syntax. Specifically, LWS on either side of the ":" or "/" is allowed, as shown here:

```
   Via: SIP / 2.0 / UDP first.example.com: 4000;ttl=16
     ;maddr=224.2.0.1 ;branch=z9hG4bKa7c6a8dlze.1
```

Even though this specification mandates that the branch parameter be present in all requests, the BNF for the header field indicates that it is optional. This allows interoperation with RFC 2543 elements, which did not have to insert the branch parameter.

Two Via header fields are equal if their sent-protocol and sent-by fields are equal, both have the same set of parameters, and the values of all parameters are equal.

20.43 Warning

The Warning header field is used to carry additional information about the status of a response. Warning header field values are sent with responses and contain a three-digit warning code, host name, and warning text.

The "warn-text" should be in a natural language that is most likely to be intelligible to the human user receiving the response. This decision can be based on any available knowledge, such as the location of the user, the Accept-Language field in a request, or the

Content-Language field in a response. The default language is i-default [23].

The currently-defined "warn-code"s are listed below, with a recommended warn-text in English and a description of their meaning. These warnings describe failures induced by the session description. The first digit of warning codes beginning with "3" indicates warnings specific to SIP. Warnings 300 through 329 are reserved for indicating problems with keywords in the session description, 330 through 339 are warnings related to basic network services requested in the session description, 370 through 379 are warnings related to quantitative QoS parameters requested in the session description, and 390 through 399 are miscellaneous warnings that do not fall into one of the above categories.

300 Incompatible network protocol: One or more network protocols contained in the session description are not available.

301 Incompatible network address formats: One or more network address formats contained in the session description are not available.

302 Incompatible transport protocol: One or more transport protocols described in the session description are not available.

303 Incompatible bandwidth units: One or more bandwidth measurement units contained in the session description were not understood.

304 Media type not available: One or more media types contained in the session description are not available.

305 Incompatible media format: One or more media formats contained in the session description are not available.

306 Attribute not understood: One or more of the media attributes in the session description are not supported.

307 Session description parameter not understood: A parameter other than those listed above was not understood.

330 Multicast not available: The site where the user is located does not support multicast.

331 Unicast not available: The site where the user is located does not support unicast communication (usually due to the presence of a firewall).

Page 1548
T-Mobile Exhibit 1002
Part 5 of 6

370 Insufficient bandwidth: The bandwidth specified in the session description or defined by the media exceeds that known to be available.

399 Miscellaneous warning: The warning text can include arbitrary information to be presented to a human user or logged. A system receiving this warning MUST NOT take any automated action.

1xx and 2xx have been taken by HTTP/1.1.

Additional "warn-code"s can be defined through IANA, as defined in Section 27.2.

Examples:

```
Warning: 307 isi.edu "Session parameter 'foo' not understood"
Warning: 301 isi.edu "Incompatible network address type 'E.164'"
```

20.44 WWW-Authenticate

A WWW-Authenticate header field value contains an authentication challenge. See Section 22.2 for further details on its usage.

Example:

```
WWW-Authenticate: Digest realm="atlanta.com",
  domain="sip:boxesbybob.com", qop="auth",
  nonce="f84f1cec41e6cbe5aea9c8e88d359",
  opaque="", stale=FALSE, algorithm=MD5
```

21 Response Codes

The response codes are consistent with, and extend, HTTP/1.1 response codes. Not all HTTP/1.1 response codes are appropriate, and only those that are appropriate are given here. Other HTTP/1.1 response codes SHOULD NOT be used. Also, SIP defines a new class, 6xx.

21.1 Provisional 1xx

Provisional responses, also known as informational responses, indicate that the server contacted is performing some further action and does not yet have a definitive response. A server sends a 1xx response if it expects to take more than 200 ms to obtain a final response. Note that 1xx responses are not transmitted reliably. They never cause the client to send an ACK. Provisional (1xx) responses MAY contain message bodies, including session descriptions.

21.1.1 100 Trying

This response indicates that the request has been received by the next-hop server and that some unspecified action is being taken on behalf of this call (for example, a database is being consulted). This response, like all other provisional responses, stops

retransmissions of an INVITE by a UAC. The 100 (Trying) response is different from other provisional responses, in that it is never forwarded upstream by a stateful proxy.

21.1.2 180 Ringing

The UA receiving the INVITE is trying to alert the user. This response MAY be used to initiate local ringback.

21.1.3 181 Call Is Being Forwarded

A server MAY use this status code to indicate that the call is being forwarded to a different set of destinations.

21.1.4 182 Queued

The called party is temporarily unavailable, but the server has decided to queue the call rather than reject it. When the callee becomes available, it will return the appropriate final status response. The reason phrase MAY give further details about the status of the call, for example, "5 calls queued; expected waiting time is 15 minutes". The server MAY issue several 182 (Queued) responses to update the caller about the status of the queued call.

21.1.5 183 Session Progress

The 183 (Session Progress) response is used to convey information about the progress of the call that is not otherwise classified. The Reason-Phrase, header fields, or message body MAY be used to convey more details about the call progress.

21.2 Successful 2xx

The request was successful.

21.2.1 200 OK

The request has succeeded. The information returned with the response depends on the method used in the request.

21.3 Redirection 3xx

3xx responses give information about the user's new location, or about alternative services that might be able to satisfy the call.

21.3.1 300 Multiple Choices

The address in the request resolved to several choices, each with its own specific location, and the user (or UA) can select a preferred communication end point and redirect its request to that location.

The response MAY include a message body containing a list of resource characteristics and location(s) from which the user or UA can choose the one most appropriate, if allowed by the Accept request header field. However, no MIME types have been defined for this message

Page 1550
T-Mobile Exhibit 1002
Part 5 of 6

body.

The choices SHOULD also be listed as Contact fields (Section 20.10). Unlike HTTP, the SIP response MAY contain several Contact fields or a list of addresses in a Contact field. UAs MAY use the Contact header field value for automatic redirection or MAY ask the user to confirm a choice. However, this specification does not define any standard for such automatic selection.

This status response is appropriate if the callee can be reached at several different locations and the server cannot or prefers not to proxy the request.

21.3.2 301 Moved Permanently

The user can no longer be found at the address in the Request-URI, and the requesting client SHOULD retry at the new address given by the Contact header field (Section 20.10). The requestor SHOULD update any local directories, address books, and user location caches with this new value and redirect future requests to the address(es) listed.

21.3.3 302 Moved Temporarily

The requesting client SHOULD retry the request at the new address(es) given by the Contact header field (Section 20.10). The Request-URI of the new request uses the value of the Contact header field in the response.

The duration of the validity of the Contact URI can be indicated through an Expires (Section 20.19) header field or an expires parameter in the Contact header field. Both proxies and UAs MAY cache this URI for the duration of the expiration time. If there is no explicit expiration time, the address is only valid once for recursing, and MUST NOT be cached for future transactions.

If the URI cached from the Contact header field fails, the Request-URI from the redirected request MAY be tried again a single time.

The temporary URI may have become out-of-date sooner than the expiration time, and a new temporary URI may be available.

21.3.4 305 Use Proxy

The requested resource MUST be accessed through the proxy given by the Contact field. The Contact field gives the URI of the proxy. The recipient is expected to repeat this single request via the proxy. 305 (Use Proxy) responses MUST only be generated by UASs.

21.3.5 380 Alternative Service

The call was not successful, but alternative services are possible.

Page 1551
T-Mobile Exhibit 1002
Part 5 of 6

The alternative services are described in the message body of the response. Formats for such bodies are not defined here, and may be the subject of future standardization.

21.4 Request Failure 4xx

4xx responses are definite failure responses from a particular server. The client SHOULD NOT retry the same request without modification (for example, adding appropriate authorization). However, the same request to a different server might be successful.

21.4.1 400 Bad Request

The request could not be understood due to malformed syntax. The Reason-Phrase SHOULD identify the syntax problem in more detail, for example, "Missing Call-ID header field".

21.4.2 401 Unauthorized

The request requires user authentication. This response is issued by UASs and registrars, while 407 (Proxy Authentication Required) is used by proxy servers.

21.4.3 402 Payment Required

Reserved for future use.

21.4.4 403 Forbidden

The server understood the request, but is refusing to fulfill it. Authorization will not help, and the request SHOULD NOT be repeated.

21.4.5 404 Not Found

The server has definitive information that the user does not exist at the domain specified in the Request-URI. This status is also returned if the domain in the Request-URI does not match any of the domains handled by the recipient of the request.

21.4.6 405 Method Not Allowed

The method specified in the Request-Line is understood, but not allowed for the address identified by the Request-URI.

The response MUST include an Allow header field containing a list of valid methods for the indicated address.

21.4.7 406 Not Acceptable

The resource identified by the request is only capable of generating response entities that have content characteristics not acceptable according to the Accept header field sent in the request.

21.4.8 407 Proxy Authentication Required

This code is similar to 401 (Unauthorized), but indicates that the

client MUST first authenticate itself with the proxy. SIP access authentication is explained in Sections 26 and 22.3.

This status code can be used for applications where access to the communication channel (for example, a telephony gateway) rather than the callee requires authentication.

21.4.9 408 Request Timeout

The server could not produce a response within a suitable amount of time, for example, if it could not determine the location of the user in time. The client MAY repeat the request without modifications at any later time.

21.4.10 410 Gone

The requested resource is no longer available at the server and no forwarding address is known. This condition is expected to be considered permanent. If the server does not know, or has no facility to determine, whether or not the condition is permanent, the status code 404 (Not Found) SHOULD be used instead.

21.4.11 413 Request Entity Too Large

The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process. The server MAY close the connection to prevent the client from continuing the request.

If the condition is temporary, the server SHOULD include a Retry-After header field to indicate that it is temporary and after what time the client MAY try again.

21.4.12 414 Request-URI Too Long

The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.

21.4.13 415 Unsupported Media Type

The server is refusing to service the request because the message body of the request is in a format not supported by the server for the requested method. The server MUST return a list of acceptable formats using the Accept, Accept-Encoding, or Accept-Language header field, depending on the specific problem with the content. UAC processing of this response is described in Section 8.1.3.5.

21.4.14 416 Unsupported URI Scheme

The server cannot process the request because the scheme of the URI in the Request-URI is unknown to the server. Client processing of this response is described in Section 8.1.3.5.

21.4.15 420 Bad Extension

The server did not understand the protocol extension specified in a

Page 1553
T-Mobile Exhibit 1002
Part 5 of 6

Proxy-Require (Section 20.29) or Require (Section 20.32) header field. The server MUST include a list of the unsupported extensions in an Unsupported header field in the response. UAC processing of this response is described in Section 8.1.3.5.

21.4.16 421 Extension Required

The UAS needs a particular extension to process the request, but this extension is not listed in a Supported header field in the request. Responses with this status code MUST contain a Require header field listing the required extensions.

A UAS SHOULD NOT use this response unless it truly cannot provide any useful service to the client. Instead, if a desirable extension is not listed in the Supported header field, servers SHOULD process the request using baseline SIP capabilities and any extensions supported by the client.

21.4.17 423 Interval Too Brief

The server is rejecting the request because the expiration time of the resource refreshed by the request is too short. This response can be used by a registrar to reject a registration whose Contact header field expiration time was too small. The use of this response and the related Min-Expires header field are described in Sections 10.2.8, 10.3, and 20.23.

21.4.18 480 Temporarily Unavailable

The callee's end system was contacted successfully but the callee is currently unavailable (for example, is not logged in, logged in but in a state that precludes communication with the callee, or has activated the "do not disturb" feature). The response MAY indicate a better time to call in the Retry-After header field. The user could also be available elsewhere (unbeknownst to this server). The reason phrase SHOULD indicate a more precise cause as to why the callee is unavailable. This value SHOULD be settable by the UA. Status 486 (Busy Here) MAY be used to more precisely indicate a particular reason for the call failure.

This status is also returned by a redirect or proxy server that recognizes the user identified by the Request-URI, but does not currently have a valid forwarding location for that user.

21.4.19 481 Call/Transaction Does Not Exist

This status indicates that the UAS received a request that does not match any existing dialog or transaction.

21.4.20 482 Loop Detected

The server has detected a loop (Section 16.3 Item 4).

21.4.21 483 Too Many Hops

The server received a request that contains a Max-Forwards (Section 20.22) header field with the value zero.

21.4.22 484 Address Incomplete

The server received a request with a Request-URI that was incomplete. Additional information SHOULD be provided in the reason phrase.

This status code allows overlapped dialing. With overlapped dialing, the client does not know the length of the dialing string. It sends strings of increasing lengths, prompting the user for more input, until it no longer receives a 484 (Address Incomplete) status response.

21.4.23 485 Ambiguous

The Request-URI was ambiguous. The response MAY contain a listing of possible unambiguous addresses in Contact header fields. Revealing alternatives can infringe on privacy of the user or the organization. It MUST be possible to configure a server to respond with status 404 (Not Found) or to suppress the listing of possible choices for ambiguous Request-URIs.

Example response to a request with the Request-URI sip:lee@example.com:

```
SIP/2.0 485 Ambiguous
Contact: Carol Lee <sip:carol.lee@example.com>
Contact: Ping Lee <sip:p.lee@example.com>
Contact: Lee M. Foote <sips:lee.foote@example.com>
```

Some email and voice mail systems provide this functionality. A status code separate from 3xx is used since the semantics are different: for 300, it is assumed that the same person or service will be reached by the choices provided. While an automated choice or sequential search makes sense for a 3xx response, user intervention is required for a 485 (Ambiguous) response.

21.4.24 486 Busy Here

The callee's end system was contacted successfully, but the callee is currently not willing or able to take additional calls at this end system. The response MAY indicate a better time to call in the Retry-After header field. The user could also be available

elsewhere, such as through a voice mail service. Status 600 (Busy Everywhere) SHOULD be used if the client knows that no other end system will be able to accept this call.

21.4.25 487 Request Terminated

The request was terminated by a BYE or CANCEL request. This response is never returned for a CANCEL request itself.

21.4.26 488 Not Acceptable Here

The response has the same meaning as 606 (Not Acceptable), but only applies to the specific resource addressed by the Request-URI and the request may succeed elsewhere.

A message body containing a description of media capabilities MAY be present in the response, which is formatted according to the Accept header field in the INVITE (or application/sdp if not present), the same as a message body in a 200 (OK) response to an OPTIONS request.

21.4.27 491 Request Pending

The request was received by a UAS that had a pending request within the same dialog. Section 14.2 describes how such "glare" situations are resolved.

21.4.28 493 Undecipherable

The request was received by a UAS that contained an encrypted MIME body for which the recipient does not possess or will not provide an appropriate decryption key. This response MAY have a single body containing an appropriate public key that should be used to encrypt MIME bodies sent to this UA. Details of the usage of this response code can be found in Section 23.2.

21.5 Server Failure 5xx

5xx responses are failure responses given when a server itself has erred.

21.5.1 500 Server Internal Error

The server encountered an unexpected condition that prevented it from fulfilling the request. The client MAY display the specific error condition and MAY retry the request after several seconds.

If the condition is temporary, the server MAY indicate when the client may retry the request using the Retry-After header field.

21.5.2 501 Not Implemented

The server does not support the functionality required to fulfill the request. This is the appropriate response when a UAS does not recognize the request method and is not capable of supporting it for any user. (Proxies forward all requests regardless of method.)

Note that a 405 (Method Not Allowed) is sent when the server recognizes the request method, but that method is not allowed or supported.

21.5.3 502 Bad Gateway

The server, while acting as a gateway or proxy, received an invalid response from the downstream server it accessed in attempting to fulfill the request.

21.5.4 503 Service Unavailable

The server is temporarily unable to process the request due to a temporary overloading or maintenance of the server. The server MAY indicate when the client should retry the request in a Retry-After header field. If no Retry-After is given, the client MUST act as if it had received a 500 (Server Internal Error) response.

A client (proxy or UAC) receiving a 503 (Service Unavailable) SHOULD attempt to forward the request to an alternate server. It SHOULD NOT forward any other requests to that server for the duration specified in the Retry-After header field, if present.

Servers MAY refuse the connection or drop the request instead of responding with 503 (Service Unavailable).

21.5.5 504 Server Time-out

The server did not receive a timely response from an external server it accessed in attempting to process the request. 408 (Request Timeout) should be used instead if there was no response within the period specified in the Expires header field from the upstream server.

21.5.6 505 Version Not Supported

The server does not support, or refuses to support, the SIP protocol version that was used in the request. The server is indicating that it is unable or unwilling to complete the request using the same major version as the client, other than with this error message.

21.5.7 513 Message Too Large

The server was unable to process the request since the message length exceeded its capabilities.

21.6 Global Failures 6xx

6xx responses indicate that a server has definitive information about a particular user, not just the particular instance indicated in the Request-URI.

21.6.1 600 Busy Everywhere

The callee's end system was contacted successfully but the callee is busy and does not wish to take the call at this time. The response MAY indicate a better time to call in the Retry-After header field. If the callee does not wish to reveal the reason for declining the call, the callee uses status code 603 (Decline) instead. This status response is returned only if the client knows that no other end point (such as a voice mail system) will answer the request. Otherwise, 486 (Busy Here) should be returned.

21.6.2 603 Decline

The callee's machine was successfully contacted but the user explicitly does not wish to or cannot participate. The response MAY indicate a better time to call in the Retry-After header field. This status response is returned only if the client knows that no other end point will answer the request.

21.6.3 604 Does Not Exist Anywhere

The server has authoritative information that the user indicated in the Request-URI does not exist anywhere.

21.6.4 606 Not Acceptable

The user's agent was contacted successfully but some aspects of the session description such as the requested media, bandwidth, or addressing style were not acceptable.

A 606 (Not Acceptable) response means that the user wishes to communicate, but cannot adequately support the session described. The 606 (Not Acceptable) response MAY contain a list of reasons in a Warning header field describing why the session described cannot be supported. Warning reason codes are listed in Section 20.43.

A message body containing a description of media capabilities MAY be present in the response, which is formatted according to the Accept header field in the INVITE (or application/sdp if not present), the same as a message body in a 200 (OK) response to an OPTIONS request.

It is hoped that negotiation will not frequently be needed, and when a new user is being invited to join an already existing conference, negotiation may not be possible. It is up to the invitation initiator to decide whether or not to act on a 606 (Not Acceptable) response.

This status response is returned only if the client knows that no other end point will answer the request.

22 Usage of HTTP Authentication

SIP provides a stateless, challenge-based mechanism for authentication that is based on authentication in HTTP. Any time that a proxy server or UA receives a request (with the exceptions given in Section 22.3), it MAY challenge the initiator of the request to provide assurance of its identity. Once the originator has been identified, the recipient of the request SHOULD ascertain whether or not this user is authorized to make the request in question. No authorization systems are recommended or discussed in this document.

The "Digest" authentication mechanism described in this section provides message authentication and replay protection only, without message integrity or confidentiality. Protective measures above and beyond those provided by Digest need to be taken to prevent active attackers from modifying SIP requests and responses.

Note that due to its weak security, the usage of "Basic" authentication has been deprecated. Servers MUST NOT accept credentials using the "Basic" authorization scheme, and servers also MUST NOT challenge with "Basic". This is a change from RFC 2543.

22.1 Framework

The framework for SIP authentication closely parallels that of HTTP (RFC 2617 [17]). In particular, the BNF for auth-scheme, auth-param, challenge, realm, realm-value, and credentials is identical (although the usage of "Basic" as a scheme is not permitted). In SIP, a UAS uses the 401 (Unauthorized) response to challenge the identity of a UAC. Additionally, registrars and redirect servers MAY make use of 401 (Unauthorized) responses for authentication, but proxies MUST NOT, and instead MAY use the 407 (Proxy Authentication Required)

response. The requirements for inclusion of the Proxy-Authenticate, Proxy-Authorization, WWW-Authenticate, and Authorization in the various messages are identical to those described in RFC 2617 [17].

Since SIP does not have the concept of a canonical root URL, the notion of protection spaces is interpreted differently in SIP. The realm string alone defines the protection domain. This is a change from RFC 2543, in which the Request-URI and the realm together defined the protection domain.

> This previous definition of protection domain caused some amount of confusion since the Request-URI sent by the UAC and the Request-URI received by the challenging server might be different, and indeed the final form of the Request-URI might not be known to the UAC. Also, the previous definition depended on the presence of a SIP URI in the Request-URI and seemed to rule out alternative URI schemes (for example, the tel URL).

Operators of user agents or proxy servers that will authenticate received requests MUST adhere to the following guidelines for creation of a realm string for their server:

- Realm strings MUST be globally unique. It is RECOMMENDED that a realm string contain a hostname or domain name, following the recommendation in Section 3.2.1 of RFC 2617 [17].

- Realm strings SHOULD present a human-readable identifier that can be rendered to a user.

For example:

```
INVITE sip:bob@biloxi.com SIP/2.0
Authorization: Digest realm="biloxi.com", <...>
```

Generally, SIP authentication is meaningful for a specific realm, a protection domain. Thus, for Digest authentication, each such protection domain has its own set of usernames and passwords. If a server does not require authentication for a particular request, it MAY accept a default username, "anonymous", which has no password (password of ""). Similarly, UACs representing many users, such as

PSTN gateways, MAY have their own device-specific username and password, rather than accounts for particular users, for their realm.

While a server can legitimately challenge most SIP requests, there are two requests defined by this document that require special handling for authentication: ACK and CANCEL.

Under an authentication scheme that uses responses to carry values used to compute nonces (such as Digest), some problems come up for any requests that take no response, including ACK. For this reason, any credentials in the INVITE that were accepted by a server MUST be accepted by that server for the ACK. UACs creating an ACK message will duplicate all of the Authorization and Proxy-Authorization header field values that appeared in the INVITE to which the ACK corresponds. Servers MUST NOT attempt to challenge an ACK.

Although the CANCEL method does take a response (a 2xx), servers MUST NOT attempt to challenge CANCEL requests since these requests cannot be resubmitted. Generally, a CANCEL request SHOULD be accepted by a server if it comes from the same hop that sent the request being canceled (provided that some sort of transport or network layer security association, as described in Section 26.2.1, is in place).

When a UAC receives a challenge, it SHOULD render to the user the contents of the "realm" parameter in the challenge (which appears in either a WWW-Authenticate header field or Proxy-Authenticate header field) if the UAC device does not already know of a credential for the realm in question. A service provider that pre-configures UAs with credentials for its realm should be aware that users will not have the opportunity to present their own credentials for this realm when challenged at a pre-configured device.

Finally, note that even if a UAC can locate credentials that are associated with the proper realm, the potential exists that these credentials may no longer be valid or that the challenging server will not accept these credentials for whatever reason (especially when "anonymous" with no password is submitted). In this instance a server may repeat its challenge, or it may respond with a 403 Forbidden. A UAC MUST NOT re-attempt requests with the credentials that have just been rejected (though the request may be retried if the nonce was stale).

22.2 User-to-User Authentication

When a UAS receives a request from a UAC, the UAS MAY authenticate the originator before the request is processed. If no credentials (in the Authorization header field) are provided in the request, the UAS can challenge the originator to provide credentials by rejecting the request with a 401 (Unauthorized) status code.

The WWW-Authenticate response-header field MUST be included in 401 (Unauthorized) response messages. The field value consists of at least one challenge that indicates the authentication scheme(s) and parameters applicable to the realm.

Page 1560
T-Mobile Exhibit 1002
Part 5 of 6

An example of the WWW-Authenticate header field in a 401 challenge is:

```
WWW-Authenticate: Digest
        realm="biloxi.com",
        qop="auth,auth-int",
        nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
        opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

When the originating UAC receives the 401 (Unauthorized), it SHOULD, if it is able, re-originate the request with the proper credentials. The UAC may require input from the originating user before proceeding. Once authentication credentials have been supplied (either directly by the user, or discovered in an internal keyring), UAs SHOULD cache the credentials for a given value of the To header field and "realm" and attempt to re-use these values on the next request for that destination. UAs MAY cache credentials in any way they would like.

If no credentials for a realm can be located, UACs MAY attempt to retry the request with a username of "anonymous" and no password (a password of "").

Once credentials have been located, any UA that wishes to authenticate itself with a UAS or registrar -- usually, but not necessarily, after receiving a 401 (Unauthorized) response -- MAY do so by including an Authorization header field with the request. The Authorization field value consists of credentials containing the authentication information of the UA for the realm of the resource being requested as well as parameters required in support of authentication and replay protection.

An example of the Authorization header field is:

```
Authorization: Digest username="bob",
        realm="biloxi.com",
        nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
        uri="sip:bob@biloxi.com",
        qop=auth,
        nc=00000001,
        cnonce="0a4f113b",
        response="6629fae49393a05397450978507c4ef1",
        opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

When a UAC resubmits a request with its credentials after receiving a 401 (Unauthorized) or 407 (Proxy Authentication Required) response, it MUST increment the CSeq header field value as it would normally when sending an updated request.

22.3 Proxy-to-User Authentication

Similarly, when a UAC sends a request to a proxy server, the proxy server MAY authenticate the originator before the request is processed. If no credentials (in the Proxy-Authorization header field) are provided in the request, the proxy can challenge the originator to provide credentials by rejecting the request with a 407 (Proxy Authentication Required) status code. The proxy MUST populate the 407 (Proxy Authentication Required) message with a Proxy-Authenticate header field value applicable to the proxy for the requested resource.

The use of Proxy-Authenticate and Proxy-Authorization parallel that described in [17], with one difference. Proxies MUST NOT add values to the Proxy-Authorization header field. All 407 (Proxy Authentication Required) responses MUST be forwarded upstream toward the UAC following the procedures for any other response. It is the UAC's responsibility to add the Proxy-Authorization header field value containing credentials for the realm of the proxy that has asked for authentication.

> If a proxy were to resubmit a request adding a Proxy-Authorization header field value, it would need to increment the CSeq in the new request. However, this would cause the UAC that submitted the original request to discard a response from the UAS, as the CSeq value would be different.

When the originating UAC receives the 407 (Proxy Authentication Required) it SHOULD, if it is able, re-originate the request with the proper credentials. It should follow the same procedures for the display of the "realm" parameter that are given above for responding to 401.

If no credentials for a realm can be located, UACs MAY attempt to retry the request with a username of "anonymous" and no password (a password of "").

The UAC SHOULD also cache the credentials used in the re-originated request.

The following rule is RECOMMENDED for proxy credential caching:

If a UA receives a Proxy-Authenticate header field value in a 401/407 response to a request with a particular Call-ID, it should incorporate credentials for that realm in all subsequent requests that contain the same Call-ID. These credentials MUST NOT be cached across dialogs; however, if a UA is configured with the realm of its local outbound proxy, when one exists, then the UA MAY cache

credentials for that realm across dialogs. Note that this does mean a future request in a dialog could contain credentials that are not needed by any proxy along the Route header path.

Any UA that wishes to authenticate itself to a proxy server -- usually, but not necessarily, after receiving a 407 (Proxy Authentication Required) response -- MAY do so by including a Proxy-Authorization header field value with the request. The Proxy-Authorization request-header field allows the client to identify itself (or its user) to a proxy that requires authentication. The Proxy-Authorization header field value consists of credentials

containing the authentication information of the UA for the proxy and/or realm of the resource being requested.

A Proxy-Authorization header field value applies only to the proxy whose realm is identified in the "realm" parameter (this proxy may previously have demanded authentication using the Proxy-Authenticate field). When multiple proxies are used in a chain, a Proxy-Authorization header field value MUST NOT be consumed by any proxy whose realm does not match the "realm" parameter specified in that value.

Note that if an authentication scheme that does not support realms is used in the Proxy-Authorization header field, a proxy server MUST attempt to parse all Proxy-Authorization header field values to determine whether one of them has what the proxy server considers to be valid credentials. Because this is potentially very time-consuming in large networks, proxy servers SHOULD use an authentication scheme that supports realms in the Proxy-Authorization header field.

If a request is forked (as described in Section 16.7), various proxy servers and/or UAs may wish to challenge the UAC. In this case, the forking proxy server is responsible for aggregating these challenges into a single response. Each WWW-Authenticate and Proxy-Authenticate value received in responses to the forked request MUST be placed into the single response that is sent by the forking proxy to the UA; the ordering of these header field values is not significant.

> When a proxy server issues a challenge in response to a request, it will not proxy the request until the UAC has retried the request with valid credentials. A forking proxy may forward a request simultaneously to multiple proxy servers that require authentication, each of which in turn will not forward the request until the originating UAC has authenticated itself in their respective realm. If the UAC does not provide credentials for

> each challenge, the proxy servers that issued the challenges will not forward requests to the UA where the destination user might be located, and therefore, the virtues of forking are largely lost.

When resubmitting its request in response to a 401 (Unauthorized) or 407 (Proxy Authentication Required) that contains multiple challenges, a UAC MAY include an Authorization value for each WWW-Authenticate value and a Proxy-Authorization value for each Proxy-Authenticate value for which the UAC wishes to supply a credential. As noted above, multiple credentials in a request SHOULD be differentiated by the "realm" parameter.

It is possible for multiple challenges associated with the same realm to appear in the same 401 (Unauthorized) or 407 (Proxy Authentication Required). This can occur, for example, when multiple proxies within the same administrative domain, which use a common realm, are reached by a forking request. When it retries a request, a UAC MAY therefore supply multiple credentials in Authorization or Proxy-Authorization header fields with the same "realm" parameter value. The same credentials SHOULD be used for the same realm.

22.4 The Digest Authentication Scheme

This section describes the modifications and clarifications required to apply the HTTP Digest authentication scheme to SIP. The SIP scheme usage is almost completely identical to that for HTTP [17].

Since RFC 2543 is based on HTTP Digest as defined in RFC 2069 [39], SIP servers supporting RFC 2617 MUST ensure they are backwards compatible with RFC 2069. Procedures for this backwards compatibility are specified in RFC 2617. Note, however, that SIP servers MUST NOT accept or request Basic authentication.

The rules for Digest authentication follow those defined in [17], with "HTTP/1.1" replaced by "SIP/2.0" in addition to the following differences:

1. The URI included in the challenge has the following BNF:

   URI = SIP-URI / SIPS-URI

2. The BNF in RFC 2617 has an error in that the 'uri' parameter of the Authorization header field for HTTP Digest

authentication is not enclosed in quotation marks. (The example in Section 3.5 of RFC 2617 is correct.) For SIP, the 'uri' MUST be enclosed in quotation marks.

3. The BNF for digest-uri-value is:

   digest-uri-value = Request-URI ; as defined in Section 25

4. The example procedure for choosing a nonce based on Etag does not work for SIP.

5. The text in RFC 2617 [17] regarding cache operation does not apply to SIP.

6. RFC 2617 [17] requires that a server check that the URI in the request line and the URI included in the Authorization header field point to the same resource. In a SIP context, these two URIs may refer to different users, due to forwarding at some proxy. Therefore, in SIP, a server MAY check that the Request-URI in the Authorization header field value corresponds to a user for whom the server is willing to accept forwarded or direct requests, but it is not necessarily a failure if the two fields are not equivalent.

7. As a clarification to the calculation of the A2 value for message integrity assurance in the Digest authentication scheme, implementers should assume, when the entity-body is empty (that is, when SIP messages have no body) that the hash of the entity-body resolves to the MD5 hash of an empty

string, or:

H(entity-body) = MD5("") =
"d41d8cd98f00b204e9800998ecf8427e"

8. RFC 2617 notes that a cnonce value MUST NOT be sent in an Authorization (and by extension Proxy-Authorization) header field if no qop directive has been sent. Therefore, any algorithms that have a dependency on the cnonce (including "MD5-Sess") require that the qop directive be sent. Use of the "qop" parameter is optional in RFC 2617 for the purposes of backwards compatibility with RFC 2069; since RFC 2543 was based on RFC 2069, the "qop" parameter must unfortunately remain optional for clients and servers to receive. However, servers MUST always send a "qop" parameter in WWW-Authenticate and Proxy-Authenticate header field values. If a client receives a "qop" parameter in a challenge header field, it MUST send the "qop" parameter in any resulting authorization header field.

RFC 2543 did not allow usage of the Authentication-Info header field (it effectively used RFC 2069). However, we now allow usage of this header field, since it provides integrity checks over the bodies and provides mutual authentication. RFC 2617 [17] defines mechanisms for backwards compatibility using the qop attribute in the request. These mechanisms MUST be used by a server to determine if the client supports the new mechanisms in RFC 2617 that were not specified in RFC 2069.

23 S/MIME

SIP messages carry MIME bodies and the MIME standard includes mechanisms for securing MIME contents to ensure both integrity and confidentiality (including the 'multipart/signed' and 'application/pkcs7-mime' MIME types, see RFC 1847 [22], RFC 2630 [23] and RFC 2633 [24]). Implementers should note, however, that there may be rare network intermediaries (not typical proxy servers) that rely on viewing or modifying the bodies of SIP messages (especially SDP), and that secure MIME may prevent these sorts of intermediaries from functioning.

This applies particularly to certain types of firewalls.

The PGP mechanism for encrypting the header fields and bodies of SIP messages described in RFC 2543 has been deprecated.

23.1 S/MIME Certificates

The certificates that are used to identify an end-user for the purposes of S/MIME differ from those used by servers in one important respect – rather than asserting that the identity of the holder corresponds to a particular hostname, these certificates assert that the holder is identified by an end-user address. This address is composed of the concatenation of the "userinfo" "@" and "domainname" portions of a SIP or SIPS URI (in other words, an email address of the form "bob@biloxi.com"), most commonly corresponding to a user's address-of-record.

These certificates are also associated with keys that are used to sign or encrypt bodies of SIP messages. Bodies are signed with the private key of the sender (who may include their public key with the message as appropriate), but bodies are encrypted with the public key of the intended recipient. Obviously, senders must have foreknowledge of the public key of recipients in order to encrypt message bodies. Public keys can be stored within a UA on a virtual keyring.

Each user agent that supports S/MIME MUST contain a keyring specifically for end-users' certificates. This keyring should map between addresses of record and corresponding certificates. Over time, users SHOULD use the same certificate when they populate the originating URI of signaling (the From header field) with the same address-of-record.

Any mechanisms depending on the existence of end-user certificates are seriously limited in that there is virtually no consolidated authority today that provides certificates for end-user applications. However, users SHOULD acquire certificates from known public certificate authorities. As an alternative, users MAY create self-signed certificates. The implications of self-signed certificates are explored further in Section 26.4.2. Implementations may also use pre-configured certificates in deployments in which a previous trust relationship exists between all SIP entities.

Above and beyond the problem of acquiring an end-user certificate, there are few well-known centralized directories that distribute end-user certificates. However, the holder of a certificate SHOULD publish their certificate in any public directories as appropriate. Similarly, UACs SHOULD support a mechanism for importing (manually or automatically) certificates discovered in public directories corresponding to the target URIs of SIP requests.

23.2 S/MIME Key Exchange

SIP itself can also be used as a means to distribute public keys in the following manner.

Whenever the CMS SignedData message is used in S/MIME for SIP, it MUST contain the certificate bearing the public key necessary to verify the signature.

When a UAC sends a request containing an S/MIME body that initiates a dialog, or sends a non-INVITE request outside the context of a dialog, the UAC SHOULD structure the body as an S/MIME 'multipart/signed' CMS SignedData body. If the desired CMS service is EnvelopedData (and the public key of the target user is known), the UAC SHOULD send the EnvelopedData message encapsulated within a SignedData message.

When a UAS receives a request containing an S/MIME CMS body that includes a certificate, the UAS SHOULD first validate the certificate, if possible, with any available root certificates for certificate authorities. The UAS SHOULD also determine the subject of the certificate (for S/MIME, the SubjectAltName will contain the

Page 1566
T-Mobile Exhibit 1002
Part 5 of 6

appropriate identity) and compare this value to the From header field

of the request. If the certificate cannot be verified, because it is self-signed, or signed by no known authority, or if it is verifiable but its subject does not correspond to the From header field of request, the UAS MUST notify its user of the status of the certificate (including the subject of the certificate, its signer, and any key fingerprint information) and request explicit permission before proceeding. If the certificate was successfully verified and the subject of the certificate corresponds to the From header field of the SIP request, or if the user (after notification) explicitly authorizes the use of the certificate, the UAS SHOULD add this certificate to a local keyring, indexed by the address-of-record of the holder of the certificate.

When a UAS sends a response containing an S/MIME body that answers the first request in a dialog, or a response to a non-INVITE request outside the context of a dialog, the UAS SHOULD structure the body as an S/MIME 'multipart/signed' CMS SignedData body. If the desired CMS service is EnvelopedData, the UAS SHOULD send the EnvelopedData message encapsulated within a SignedData message.

When a UAC receives a response containing an S/MIME CMS body that includes a certificate, the UAC SHOULD first validate the certificate, if possible, with any appropriate root certificate. The UAC SHOULD also determine the subject of the certificate and compare this value to the To field of the response; although the two may very well be different, and this is not necessarily indicative of a security breach. If the certificate cannot be verified because it is self-signed, or signed by no known authority, the UAC MUST notify its user of the status of the certificate (including the subject of the certificate, its signator, and any key fingerprint information) and request explicit permission before proceeding. If the certificate was successfully verified, and the subject of the certificate corresponds to the To header field in the response, or if the user (after notification) explicitly authorizes the use of the certificate, the UAC SHOULD add this certificate to a local keyring, indexed by the address-of-record of the holder of the certificate. If the UAC had not transmitted its own certificate to the UAS in any previous transaction, it SHOULD use a CMS SignedData body for its next request or response.

On future occasions, when the UA receives requests or responses that contain a From header field corresponding to a value in its keyring, the UA SHOULD compare the certificate offered in these messages with the existing certificate in its keyring. If there is a discrepancy, the UA MUST notify its user of a change of the certificate (preferably in terms that indicate that this is a potential security breach) and acquire the user's permission before continuing to

Page 1567
T-Mobile Exhibit 1002
Part 5 of 6

process the signaling. If the user authorizes this certificate, it SHOULD be added to the keyring alongside any previous value(s) for this address-of-record.

Note well however, that this key exchange mechanism does not guarantee the secure exchange of keys when self-signed certificates, or certificates signed by an obscure authority, are used - it is vulnerable to well-known attacks. In the opinion of the authors, however, the security it provides is proverbially better than nothing; it is in fact comparable to the widely used SSH application. These limitations are explored in greater detail in Section 26.4.2.

If a UA receives an S/MIME body that has been encrypted with a public key unknown to the recipient, it MUST reject the request with a 493 (Undecipherable) response. This response SHOULD contain a valid certificate for the respondent (corresponding, if possible, to any address of record given in the To header field of the rejected request) within a MIME body with a 'certs-only' "smime-type" parameter.

A 493 (Undecipherable) sent without any certificate indicates that the respondent cannot or will not utilize S/MIME encrypted messages, though they may still support S/MIME signatures.

Note that a user agent that receives a request containing an S/MIME body that is not optional (with a Content-Disposition header "handling" parameter of "required") MUST reject the request with a 415 Unsupported Media Type response if the MIME type is not understood. A user agent that receives such a response when S/MIME is sent SHOULD notify its user that the remote device does not support S/MIME, and it MAY subsequently resend the request without S/MIME, if appropriate; however, this 415 response may constitute a downgrade attack.

If a user agent sends an S/MIME body in a request, but receives a response that contains a MIME body that is not secured, the UAC SHOULD notify its user that the session could not be secured. However, if a user agent that supports S/MIME receives a request with an unsecured body, it SHOULD NOT respond with a secured body, but if it expects S/MIME from the sender (for example, because the sender's From header field value corresponds to an identity on its keychain), the UAS SHOULD notify its user that the session could not be secured.

A number of conditions that arise in the previous text call for the notification of the user when an anomalous certificate-management event occurs. Users might well ask what they should do under these circumstances. First and foremost, an unexpected change in a certificate, or an absence of security when security is expected, are

causes for caution but not necessarily indications that an attack is in progress. Users might abort any connection attempt or refuse a connection request they have received; in telephony parlance, they could hang up and call back. Users may wish to find an alternate means to contact the other party and confirm that their key has legitimately changed. Note that users are sometimes compelled to change their certificates, for example when they suspect that the secrecy of their private key has been compromised. When their private key is no longer private, users must legitimately generate a

new key and re-establish trust with any users that held their old key.

Finally, if during the course of a dialog a UA receives a certificate in a CMS SignedData message that does not correspond with the certificates previously exchanged during a dialog, the UA MUST notify its user of the change, preferably in terms that indicate that this is a potential security breach.

23.3 Securing MIME bodies

There are two types of secure MIME bodies that are of interest to SIP: use of these bodies should follow the S/MIME specification [24] with a few variations:

- "multipart/signed" MUST be used only with CMS detached signatures.

  This allows backwards compatibility with non-S/MIME-compliant recipients.

- S/MIME bodies SHOULD have a Content-Disposition header field, and the value of the "handling" parameter SHOULD be "required."

- If a UAC has no certificate on its keyring associated with the address-of-record to which it wants to send a request, it cannot send an encrypted "application/pkcs7-mime" MIME message. UACs MAY send an initial request such as an OPTIONS message with a CMS detached signature in order to solicit the certificate of the remote side (the signature SHOULD be over a "message/sip" body of the type described in Section 23.4).

  Note that future standardization work on S/MIME may define non-certificate based keys.

- Senders of S/MIME bodies SHOULD use the "SMIMECapabilities" (see Section 2.5.2 of [24]) attribute to express their capabilities and preferences for further communications. Note especially that senders MAY use the "preferSignedData"

capability to encourage receivers to respond with CMS SignedData messages (for example, when sending an OPTIONS request as described above).

- S/MIME implementations MUST at a minimum support SHA1 as a digital signature algorithm, and 3DES as an encryption algorithm. All other signature and encryption algorithms MAY be supported. Implementations can negotiate support for these algorithms with the "SMIMECapabilities" attribute.

- Each S/MIME body in a SIP message SHOULD be signed with only one certificate. If a UA receives a message with multiple signatures, the outermost signature should be treated as the single certificate for this body. Parallel signatures SHOULD NOT be used.

  The following is an example of an encrypted S/MIME SDP body within a SIP message:

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
     name=smime.p7m
Content-Disposition: attachment; filename=smime.p7m
   handling=required

*******************************************************
* Content-Type: application/sdp                       *
*                                                     *
* v=0                                                 *
* o=alice 53655765 2353687637 IN IP4 pc33.atlanta.com *
* s=-                                                 *
* t=0 0                                               *
* c=IN IP4 pc33.atlanta.com                           *
* m=audio 3456 RTP/AVP 0 1 3 99                       *
* a=rtpmap:0 PCMU/8000                                *
*******************************************************
```


23.4 SIP Header Privacy and Integrity using S/MIME: Tunneling SIP

As a means of providing some degree of end-to-end authentication, integrity or confidentiality for SIP header fields, S/MIME can encapsulate entire SIP messages within MIME bodies of type "message/sip" and then apply MIME security to these bodies in the same manner as typical SIP bodies. These encapsulated SIP requests and responses do not constitute a separate dialog or transaction, they are a copy of the "outer" message that is used to verify integrity or to supply additional information.

If a UAS receives a request that contains a tunneled "message/sip" S/MIME body, it SHOULD include a tunneled "message/sip" body in the response with the same smime-type.

Any traditional MIME bodies (such as SDP) SHOULD be attached to the "inner" message so that they can also benefit from S/MIME security. Note that "message/sip" bodies can be sent as a part of a MIME "multipart/mixed" body if any unsecured MIME types should also be transmitted in a request.

23.4.1 Integrity and Confidentiality Properties of SIP Headers

When the S/MIME integrity or confidentiality mechanisms are used, there may be discrepancies between the values in the "inner" message and values in the "outer" message. The rules for handling any such differences for all of the header fields described in this document

are given in this section.

Note that for the purposes of loose timestamping, all SIP messages that tunnel "message/sip" SHOULD contain a Date header in both the "inner" and "outer" headers.

23.4.1.1 Integrity

Whenever integrity checks are performed, the integrity of a header field should be determined by matching the value of the header field in the signed body with that in the "outer" messages using the comparison rules of SIP as described in 20.

Header fields that can be legitimately modified by proxy servers are: Request-URI, Via, Record-Route, Route, Max-Forwards, and Proxy-Authorization. If these header fields are not intact end-to-end, implementations SHOULD NOT consider this a breach of security. Changes to any other header fields defined in this document constitute an integrity violation; users MUST be notified of a discrepancy.

23.4.1.2 Confidentiality

When messages are encrypted, header fields may be included in the encrypted body that are not present in the "outer" message.

Some header fields must always have a plaintext version because they are required header fields in requests and responses - these include:

To, From, Call-ID, CSeq, Contact. While it is probably not useful to provide an encrypted alternative for the Call-ID, CSeq, or Contact, providing an alternative to the information in the "outer" To or From is permitted. Note that the values in an encrypted body are not used for the purposes of identifying transactions or dialogs - they are merely informational. If the From header field in an encrypted body differs from the value in the "outer" message, the value within the encrypted body SHOULD be displayed to the user, but MUST NOT be used in the "outer" header fields of any future messages.

Primarily, a user agent will want to encrypt header fields that have an end-to-end semantic, including: Subject, Reply-To, Organization, Accept, Accept-Encoding, Accept-Language, Alert-Info, Error-Info, Authentication-Info, Expires, In-Reply-To, Require, Supported, Unsupported, Retry-After, User-Agent, Server, and Warning. If any of these header fields are present in an encrypted body, they should be used instead of any "outer" header fields, whether this entails displaying the header field values to users or setting internal states in the UA. They SHOULD NOT however be used in the "outer" headers of any future messages.

If present, the Date header field MUST always be the same in the "inner" and "outer" headers.

Since MIME bodies are attached to the "inner" message, implementations will usually encrypt MIME-specific header fields, including: MIME-Version, Content-Type, Content-Length, Content-Language, Content-Encoding and Content-Disposition. The "outer"

Page 1571
T-Mobile Exhibit 1002
Part 5 of 6

message will have the proper MIME header fields for S/MIME bodies. These header fields (and any MIME bodies they preface) should be treated as normal MIME header fields and bodies received in a SIP message.

It is not particularly useful to encrypt the following header fields: Min-Expires, Timestamp, Authorization, Priority, and WWW-Authenticate. This category also includes those header fields that can be changed by proxy servers (described in the preceding section). UAs SHOULD never include these in an "inner" message if they are not

included in the "outer" message. UAs that receive any of these header fields in an encrypted body SHOULD ignore the encrypted values.

Note that extensions to SIP may define additional header fields; the authors of these extensions should describe the integrity and confidentiality properties of such header fields. If a SIP UA encounters an unknown header field with an integrity violation, it MUST ignore the header field.

23.4.2 Tunneling Integrity and Authentication

Tunneling SIP messages within S/MIME bodies can provide integrity for SIP header fields if the header fields that the sender wishes to secure are replicated in a "message/sip" MIME body signed with a CMS detached signature.

Provided that the "message/sip" body contains at least the fundamental dialog identifiers (To, From, Call-ID, CSeq), then a signed MIME body can provide limited authentication. At the very least, if the certificate used to sign the body is unknown to the recipient and cannot be verified, the signature can be used to ascertain that a later request in a dialog was transmitted by the same certificate-holder that initiated the dialog. If the recipient of the signed MIME body has some stronger incentive to trust the certificate (they were able to validate it, they acquired it from a trusted repository, or they have used it frequently) then the signature can be taken as a stronger assertion of the identity of the subject of the certificate.

In order to eliminate possible confusions about the addition or subtraction of entire header fields, senders SHOULD replicate all header fields from the request within the signed body. Any message bodies that require integrity protection MUST be attached to the "inner" message.

If a Date header is present in a message with a signed body, the recipient SHOULD compare the header field value with its own internal clock, if applicable. If a significant time discrepancy is detected (on the order of an hour or more), the user agent SHOULD alert the user to the anomaly, and note that it is a potential security breach.

If an integrity violation in a message is detected by its recipient, the message MAY be rejected with a 403 (Forbidden) response if it is a request, or any existing dialog MAY be terminated. UAs SHOULD

notify users of this circumstance and request explicit guidance on how to proceed.

The following is an example of the use of a tunneled "message/sip" body:

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: multipart/signed;
  protocol="application/pkcs7-signature";
  micalg=sha1; boundary=boundary42
Content-Length: 568

--boundary42
Content-Type: message/sip

INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
To: Bob <bob@biloxi.com>
From: Alice <alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 147

v=0
o=UserA 2890844526 2890844526 IN IP4 here.com
s=Session SDP
c=IN IP4 pc33.atlanta.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s;
   handling=required
```

```
ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756

--boundary42-
```

23.4.3 Tunneling Encryption

It may also be desirable to use this mechanism to encrypt a "message/sip" MIME body within a CMS EnvelopedData message S/MIME body, but in practice, most header fields are of at least some use to the network; the general use of encryption with S/MIME is to secure message bodies like SDP rather than message headers. Some informational header fields, such as the Subject or Organization could perhaps warrant end-to-end security. Headers defined by future SIP applications might also require obfuscation.

Another possible application of encrypting header fields is selective anonymity. A request could be constructed with a From header field that contains no personal information (for example, sip:anonymous@anonymizer.invalid). However, a second From header field containing the genuine address-of-record of the originator could be encrypted within a "message/sip" MIME body where it will only be visible to the endpoints of a dialog.

> Note that if this mechanism is used for anonymity, the From header field will no longer be usable by the recipient of a message as an index to their certificate keychain for retrieving the proper S/MIME key to associated with the sender. The message must first be decrypted, and the "inner" From header field MUST be used as an index.

In order to provide end-to-end integrity, encrypted "message/sip" MIME bodies SHOULD be signed by the sender. This creates a "multipart/signed" MIME body that contains an encrypted body and a signature, both of type "application/pkcs7-mime".

In the following example, of an encrypted and signed message, the text boxed in asterisks ("*") is encrypted:

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.com>
From: Anonymous <sip:anonymous@atlanta.com>;tag=1928301774
```


Page 1574
T-Mobile Exhibit 1002
Part 5 of 6

```
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:pc33.atlanta.com>
Content-Type: multipart/signed;
  protocol="application/pkcs7-signature";
  micalg=sha1; boundary=boundary42
Content-Length: 568

--boundary42
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
     name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m
   handling=required
Content-Length: 231

**************************************************************
* Content-Type: message/sip                                  *
*                                                            *
* INVITE sip:bob@biloxi.com SIP/2.0                          *
* Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8    *
* To: Bob <bob@biloxi.com>                                   *
* From: Alice <alice@atlanta.com>;tag=1928301774             *
* Call-ID: a84b4c76e66710                                    *
* CSeq: 314159 INVITE                                        *
* Max-Forwards: 70                                           *
* Date: Thu, 21 Feb 2002 13:02:03 GMT                        *
* Contact: <sip:alice@pc33.atlanta.com>                      *
*                                                            *
* Content-Type: application/sdp                              *
*                                                            *
* v=0                                                        *
* o=alice 53655765 2353687637 IN IP4 pc33.atlanta.com        *
* s=Session SDP                                              *
* t=0 0                                                      *
* c=IN IP4 pc33.atlanta.com                                  *
* m=audio 3456 RTP/AVP 0 1 3 99                              *
* a=rtpmap:0 PCMU/8000                                       *
**************************************************************
```



```
--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s;
   handling=required

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756

--boundary42-
```

24 Examples

In the following examples, we often omit the message body and the

corresponding Content-Length and Content-Type header fields for brevity.

24.1 Registration

Bob registers on start-up. The message flow is shown in Figure 9. Note that the authentication usually required for registration is not shown for simplicity.



Figure 9: SIP Registration Example

F1 REGISTER Bob -> Registrar

```
REGISTER sip:registrar.biloxi.com SIP/2.0
Via: SIP/2.0/UDP bobspc.biloxi.com:5060;branch=z9hG4bKnashds7
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Bob <sip:bob@biloxi.com>;tag=456248
Call-ID: 843817637684230@998sdasdh09
CSeq: 1826 REGISTER
Contact: <sip:bob@192.0.2.4>
Expires: 7200
Content-Length: 0
```


The registration expires after two hours. The registrar responds with a 200 OK:

F2 200 OK Registrar -> Bob

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP bobspc.biloxi.com:5060;branch=z9hG4bKnashds7
 ;received=192.0.2.4
To: Bob <sip:bob@biloxi.com>;tag=2493k59kd
From: Bob <sip:bob@biloxi.com>;tag=456248
Call-ID: 843817637684230@998sdasdh09
CSeq: 1826 REGISTER
Contact: <sip:bob@192.0.2.4>
Expires: 7200
Content-Length: 0
```

24.2 Session Setup

This example contains the full details of the example session setup in Section 4. The message flow is shown in Figure 1. Note that these flows show the minimum required set of header fields - some other header fields such as Allow and Supported would normally be present.

F1 INVITE Alice -> atlanta.com proxy

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```


F2 100 Trying atlanta.com proxy -> Alice

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
 ;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Content-Length: 0
```

F3 INVITE atlanta.com proxy -> biloxi.com proxy

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com;branch=z9hG4bK77ef4c2312983.1
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
 ;received=192.0.2.1
Max-Forwards: 69
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

F4 100 Trying biloxi.com proxy -> atlanta.com proxy

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com;branch=z9hG4bK77ef4c2312983.1
 ;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
```

```
 ;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Content-Length: 0
```


F5 INVITE biloxi.com proxy -> Bob

```
INVITE sip:bob@192.0.2.4 SIP/2.0
Via: SIP/2.0/UDP server10.biloxi.com;branch=z9hG4bK4b43c2ff8.1
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com;branch=z9hG4bK77ef4c2312983.1
 ;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
 ;received=192.0.2.1
Max-Forwards: 68
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

F6 180 Ringing Bob -> biloxi.com proxy

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP server10.biloxi.com;branch=z9hG4bK4b43c2ff8.1
 ;received=192.0.2.3
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com;branch=z9hG4bK77ef4c2312983.1
 ;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
 ;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
Contact: <sip:bob@192.0.2.4>
CSeq: 314159 INVITE
Content-Length: 0
```

F7 180 Ringing biloxi.com proxy -> atlanta.com proxy

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com;branch=z9hG4bK77ef4c2312983.1
 ;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
 ;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
```

```
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
Contact: <sip:bob@192.0.2.4>
CSeq: 314159 INVITE
Content-Length: 0
```


F8 180 Ringing atlanta.com proxy -> Alice

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
 ;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
Contact: <sip:bob@192.0.2.4>
CSeq: 314159 INVITE
Content-Length: 0
```

F9 200 OK Bob -> biloxi.com proxy

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP server10.biloxi.com;branch=z9hG4bK4b43c2ff8.1
 ;received=192.0.2.3
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com;branch=z9hG4bK77ef4c2312983.1
 ;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
 ;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:bob@192.0.2.4>
Content-Type: application/sdp
Content-Length: 131

(Bob's SDP not shown)
```

F10 200 OK biloxi.com proxy -> atlanta.com proxy

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com;branch=z9hG4bK77ef4c2312983.1
 ;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
 ;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:bob@192.0.2.4>
Content-Type: application/sdp
Content-Length: 131

(Bob's SDP not shown)
```

F11 200 OK atlanta.com proxy -> Alice

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
 ;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:bob@192.0.2.4>
Content-Type: application/sdp
Content-Length: 131

(Bob's SDP not shown)
```

F12 ACK Alice -> Bob

```
ACK sip:bob@192.0.2.4 SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds9
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 ACK
Content-Length: 0
```

The media session between Alice and Bob is now established.

Bob hangs up first. Note that Bob's SIP phone maintains its own CSeq numbering space, which, in this example, begins with 231. Since Bob is making the request, the To and From URIs and tags have been swapped.

F13 BYE Bob -> Alice

```
BYE sip:alice@pc33.atlanta.com SIP/2.0
Via: SIP/2.0/UDP 192.0.2.4;branch=z9hG4bKnashds10
Max-Forwards: 70
From: Bob <sip:bob@biloxi.com>;tag=a6c85cf
To: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 231 BYE
Content-Length: 0
```


F14 200 OK Alice -> Bob

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.2.4;branch=z9hG4bKnashds10
From: Bob <sip:bob@biloxi.com>;tag=a6c85cf
```


T-Mobile Exhibit 1002
Part 5 of 6

```
To: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 231 BYE
Content-Length: 0
```

The SIP Call Flows document [40] contains further examples of SIP messages.

25 Augmented BNF for the SIP Protocol

All of the mechanisms specified in this document are described in both prose and an augmented Backus-Naur Form (BNF) defined in RFC 2234 [10]. Section 6.1 of RFC 2234 defines a set of core rules that are used by this specification, and not repeated here. Implementers need to be familiar with the notation and content of RFC 2234 in order to understand this specification. Certain basic rules are in uppercase, such as SP, LWS, HTAB, CRLF, DIGIT, ALPHA, etc. Angle brackets are used within definitions to clarify the use of rule names.

The use of square brackets is redundant syntactically. It is used as a semantic hint that the specific parameter is optional to use.

25.1 Basic Rules

The following rules are used throughout this specification to describe basic parsing constructs. The US-ASCII coded character set is defined by ANSI X3.4-1986.

```
alphanum  =  ALPHA / DIGIT
```


Several rules are incorporated from RFC 2396 [5] but are updated to make them compliant with RFC 2234 [10]. These include:

```
reserved    =  ";" / "/" / "?" / ":" / "@" / "&" / "=" / "+"
               / "$" / ","
unreserved  =  alphanum / mark
mark        =  "-" / "_" / "." / "!" / "~" / "*" / "'"
               / "(" / ")"
escaped     =  "%" HEXDIG HEXDIG
```

SIP header field values can be folded onto multiple lines if the continuation line begins with a space or horizontal tab. All linear white space, including folding, has the same semantics as SP. A recipient MAY replace any linear white space with a single SP before

Page 1581
T-Mobile Exhibit 1002
Part 5 of 6

interpreting the field value or forwarding the message downstream. This is intended to behave exactly as HTTP/1.1 as described in RFC 2616 [8]. The SWS construct is used when linear white space is optional, generally between tokens and separators.

```
LWS  =  [*WSP CRLF] 1*WSP ; linear whitespace
SWS  =  [LWS] ; sep whitespace
```

To separate the header name from the rest of value, a colon is used, which, by the above rule, allows whitespace before, but no line break, and whitespace after, including a linebreak. The HCOLON defines this construct.

```
HCOLON  =  *( SP / HTAB ) ":" SWS
```

The TEXT-UTF8 rule is only used for descriptive field contents and values that are not intended to be interpreted by the message parser. Words of *TEXT-UTF8 contain characters from the UTF-8 charset (RFC 2279 [7]). The TEXT-UTF8-TRIM rule is used for descriptive field contents that are n t quoted strings, where leading and trailing LWS is not meaningful. In this regard, SIP differs from HTTP, which uses the ISO 8859-1 character set.

```
TEXT-UTF8-TRIM  =  1*TEXT-UTF8char *(*LWS TEXT-UTF8char)
TEXT-UTF8char   =  %x21-7E / UTF8-NONASCII
UTF8-NONASCII   =  %xC0-DF 1UTF8-CONT
                /  %xE0-EF 2UTF8-CONT
                /  %xF0-F7 3UTF8-CONT
                /  %xF8-Fb 4UTF8-CONT
                /  %xFC-FD 5UTF8-CONT
UTF8-CONT       =  %x80-BF
```


A CRLF is allowed in the definition of TEXT-UTF8-TRIM only as part of a header field continuation. It is expected that the folding LWS will be replaced with a single SP before interpretation of the TEXT-UTF8-TRIM value.

Hexadecimal numeric characters are used in several protocol elements. Some elements (authentication) force hex alphas to be lower case.

```
LHEX  =  DIGIT / %x61-66 ;lowercase a-f
```

Many SIP header field values consist of words separated by LWS or special characters. Unless otherwise stated, tokens are case-insensitive. These special characters MUST be in a quoted string to be used within a parameter value. The word construct is used in Call-ID to allow most separators to be used.

```
token       =  1*(alphanum / "-" / "." / "!" / "%" / "*"
               / "_" / "+" / "`" / "'" / "~" )
separators  =  "(" / ")" / "<" / ">" / "@" /
               "," / ";" / ":" / "\" / DQUOTE /
               "/" / "[" / "]" / "?" / "=" /
               "{" / "}" / SP / HTAB
word        =  1*(alphanum / "-" / "." / "!" / "%" / "*" /
```


Page 1582
T-Mobile Exhibit 1002
Part 5 of 6

```
                    "_" / "+" / "`" / "'" / "~" /
                    "(" / ")" / "<" / ">" /
                    ":" / "\" / DQUOTE /
                    "/" / "[" / "]" / "?" /
                    "{" / "}" )
```

When tokens are used or separators are used between elements, whitespace is often allowed before or after these characters:

```
   STAR    =  SWS "*" SWS ; asterisk
   SLASH   =  SWS "/" SWS ; slash
   EQUAL   =  SWS "=" SWS ; equal
   LPAREN  =  SWS "(" SWS ; left parenthesis
   RPAREN  =  SWS ")" SWS ; right parenthesis
   RAQUOT  =  ">" SWS ; right angle quote
   LAQUOT  =  SWS "<"; left angle quote
   COMMA   =  SWS "," SWS ; comma
   SEMI    =  SWS ";" SWS ; semicolon
   COLON   =  SWS ":" SWS ; colon
   LDQUOT  =  SWS DQUOTE; open double quotation mark
   RDQUOT  =  DQUOTE SWS ; close double quotation mark
```


Comments can be included in some SIP header fields by surrounding the comment text with parentheses. Comments are only allowed in fields containing "comment" as part of their field value definition. In all other fields, parentheses are considered part of the field value.

```
   comment  =  LPAREN *(ctext / quoted-pair / comment) RPAREN
   ctext    =  %x21-27 / %x2A-5B / %x5D-7E / UTF8-NONASCII
               / LWS
```

ctext includes all chars except left and right parens and backslash. A string of text is parsed as a single word if it is quoted using double-quote marks. In quoted strings, quotation marks (") and backslashes (\) need to be escaped.

```
   quoted-string  =  SWS DQUOTE *(qdtext / quoted-pair ) DQUOTE
   qdtext         =  LWS / %x21 / %x23-5B / %x5D-7E
                     / UTF8-NONASCII
```

The backslash character ("\") MAY be used as a single-character quoting mechanism only within quoted-string and comment constructs. Unlike HTTP/1.1, the characters CR and LF cannot be escaped by this mechanism to avoid conflict with line folding and header separation.

```
quoted-pair  =  "\" (%x00-09 / %x0B-0C
                / %x0E-7F)

SIP-URI          =  "sip:" [ userinfo ] hostport
                    uri-parameters [ headers ]
SIPS-URI         =  "sips:" [ userinfo ] hostport
                    uri-parameters [ headers ]
userinfo         =  ( user / telephone-subscriber ) [ ":" password ] "@"
user             =  1*( unreserved / escaped / user-unreserved )
```


T-Mobile Exhibit 1002
Part 5 of 6

```
user-unreserved  =  "&" / "=" / "+" / "$" / "," / ";" / "?" / "/"
password         =  *( unreserved / escaped /
                    "&" / "=" / "+" / "$" / "," )
hostport         =  host [ ":" port ]
host             =  hostname / IPv4address / IPv6reference
hostname         =  *( domainlabel "." ) toplabel [ "." ]
domainlabel      =  alphanum
                    / alphanum *( alphanum / "-" ) alphanum
toplabel         =  ALPHA / ALPHA *( alphanum / "-" ) alphanum
```



```
IPv4address    =  1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT
IPv6reference  =  "[" IPv6address "]"
IPv6address    =  hexpart [ ":" IPv4address ]
hexpart        =  hexseq / hexseq "::" [ hexseq ] / "::" [ hexseq ]
hexseq         =  hex4 *( ":" hex4)
hex4           =  1*4HEXDIG
port           =  1*DIGIT
```

The BNF for telephone-subscriber can be found in RFC 2806 [9]. Note, however, that any characters allowed there that are not allowed in the user part of the SIP URI MUST be escaped.

```
uri-parameters    =  *( ";" uri-parameter)
uri-parameter     =  transport-param / user-param / method-param
                     / ttl-param / maddr-param / lr-param / other-param
transport-param   =  "transport="
                     ( "udp" / "tcp" / "sctp" / "tls"
                     / other-transport)
other-transport   =  token
user-param        =  "user=" ( "phone" / "ip" / other-user)
other-user        =  token
method-param      =  "method=" Method
ttl-param         =  "ttl=" ttl
maddr-param       =  "maddr=" host
lr-param          =  "lr"
other-param       =  pname [ "=" pvalue ]
pname             =  1*paramchar
pvalue            =  1*paramchar
paramchar         =  param-unreserved / unreserved / escaped
param-unreserved  =  "[" / "]" / "/" / ":" / "&" / "+" / "$"

headers         =  "?" header *( "&" header )
header          =  hname "=" hvalue
hname           =  1*( hnv-unreserved / unreserved / escaped )
hvalue          =  *( hnv-unreserved / unreserved / escaped )
hnv-unreserved  =  "[" / "]" / "/" / "?" / ":" / "+" / "$"

SIP-message    =  Request / Response
Request        =  Request-Line
                  *( message-header )
                  CRLF
```

```
                  [ message-body ]
Request-Line    =  Method SP Request-URI SP SIP-Version CRLF
Request-URI     =  SIP-URI / SIPS-URI / absoluteURI
absoluteURI     =  scheme ":" ( hier-part / opaque-part )
hier-part       =  ( net-path / abs-path ) [ "?" query ]
net-path        =  "//" authority [ abs-path ]
abs-path        =  "/" path-segments
```



```
opaque-part     =  uric-no-slash *uric
uric            =  reserved / unreserved / escaped
uric-no-slash   =  unreserved / escaped / ";" / "?" / ":" / "@"
                   / "&" / "=" / "+" / "$" / ","
path-segments   =  segment *( "/" segment )
segment         =  *pchar *( ";" param )
param           =  *pchar
pchar           =  unreserved / escaped /
                   ":" / "@" / "&" / "=" / "+" / "$" / ","
scheme          =  ALPHA *( ALPHA / DIGIT / "+" / "-" / "." )
authority       =  srvr / reg-name
srvr            =  [ [ userinfo "@" ] hostport ]
reg-name        =  1*( unreserved / escaped / "$" / ","
                   / ";" / ":" / "@" / "&" / "=" / "+" )
query           =  *uric
SIP-Version     =  "SIP" "/" 1*DIGIT "." 1*DIGIT

message-header  =  (Accept
                /  Accept-Encoding
                /  Accept-Language
                /  Alert-Info
                /  Allow
                /  Authentication-Info
                /  Authorization
                /  Call-ID
                /  Call-Info
                /  Contact
                /  Content-Disposition
                /  Content-Encoding
                /  Content-Language
                /  Content-Length
                /  Content-Type
                /  CSeq
                /  Date
                /  Error-Info
                /  Expires
                /  From
                /  In-Reply-To
                /  Max-Forwards
                /  MIME-Version
                /  Min-Expires
                /  Organization
                /  Priority
                /  Proxy-Authenticate
                /  Proxy-Authorization
                /  Proxy-Require
                /  Record-Route
                /  Reply-To
```

```
                / Require
                / Retry-After
                / Route
                / Server
                / Subject
                / Supported
                / Timestamp
                / To
                / Unsupported
                / User-Agent
                / Via
                / Warning
                / WWW-Authenticate
                / extension-header) CRLF

INVITEm           =  %x49.4E.56.49.54.45 ; INVITE in caps
ACKm              =  %x41.43.4B ; ACK in caps
OPTIONSm          =  %x4F.50.54.49.4F.4E.53 ; OPTIONS in caps
BYEm              =  %x42.59.45 ; BYE in caps
CANCELm           =  %x43.41.4E.43.45.4C ; CANCEL in caps
REGISTERm         =  %x52.45.47.49.53.54.45.52 ; REGISTER in caps
Method            =  INVITEm / ACKm / OPTIONSm / BYEm
                     / CANCELm / REGISTERm
                     / extension-method
extension-method  =  token
Response          =  Status-Line
                     *( message-header )
                     CRLF
                     [ message-body ]

Status-Line     =  SIP-Version SP Status-Code SP Reason-Phrase CRLF
Status-Code     =  Informational
                /  Redirection
                /  Success
                /  Client-Error
                /  Server-Error
                /  Global-Failure
                /  extension-code
extension-code  =  3DIGIT
Reason-Phrase   =  *(reserved / unreserved / escaped
                   / UTF8-NONASCII / UTF8-CONT / SP / HTAB)

Informational  =  "100"  ;  Trying
               /  "180"  ;  Ringing
               /  "181"  ;  Call Is Being Forwarded
               /  "182"  ;  Queued
               /  "183"  ;  Session Progress
```



```
Success  =  "200"  ;  OK

Redirection  =  "300"  ;  Multiple Choices
```

```
            /   "301"  ;  Moved Permanently
            /   "302"  ;  Moved Temporarily
            /   "305"  ;  Use Proxy
            /   "380"  ;  Alternative Service

Client-Error  =  "400"  ;  Bad Request
             /   "401"  ;  Unauthorized
             /   "402"  ;  Payment Required
             /   "403"  ;  Forbidden
             /   "404"  ;  Not Found
             /   "405"  ;  Method Not Allowed
             /   "406"  ;  Not Acceptable
             /   "407"  ;  Proxy Authentication Required
             /   "408"  ;  Request Timeout
             /   "410"  ;  Gone
             /   "413"  ;  Request Entity Too Large
             /   "414"  ;  Request-URI Too Large
             /   "415"  ;  Unsupported Media Type
             /   "416"  ;  Unsupported URI Scheme
             /   "420"  ;  Bad Extension
             /   "421"  ;  Extension Required
             /   "423"  ;  Interval Too Brief
             /   "480"  ;  Temporarily not available
             /   "481"  ;  Call Leg/Transaction Does Not Exist
             /   "482"  ;  Loop Detected
             /   "483"  ;  Too Many Hops
             /   "484"  ;  Address Incomplete
             /   "485"  ;  Ambiguous
             /   "486"  ;  Busy Here
             /   "487"  ;  Request Terminated
             /   "488"  ;  Not Acceptable Here
             /   "491"  ;  Request Pending
             /   "493"  ;  Undecipherable

Server-Error  =  "500"  ;  Internal Server Error
             /   "501"  ;  Not Implemented
             /   "502"  ;  Bad Gateway
             /   "503"  ;  Service Unavailable
             /   "504"  ;  Server Time-out
             /   "505"  ;  SIP Version not supported
             /   "513"  ;  Message Too Large
```



```
Global-Failure  =  "600"  ;  Busy Everywhere
               /   "603"  ;  Decline
               /   "604"  ;  Does not exist anywhere
               /   "606"  ;  Not Acceptable

Accept         =  "Accept" HCOLON
                  [ accept-range *(COMMA accept-range) ]
accept-range   =  media-range *(SEMI accept-param)
media-range    =  ( "*/*"
                  / ( m-type SLASH "*" )
                  / ( m-type SLASH m-subtype )
                  ) *( SEMI m-parameter )
```

```
accept-param    =  ("q" EQUAL qvalue) / generic-param
qvalue          =  ( "0" [ "." 0*3DIGIT ] )
                   / ( "1" [ "." 0*3("0") ] )
generic-param   =  token [ EQUAL gen-value ]
gen-value       =  token / host / quoted-string

Accept-Encoding  =  "Accept-Encoding" HCOLON
                    [ encoding *(COMMA encoding) ]
encoding         =  codings *(SEMI accept-param)
codings          =  content-coding / "*"
content-coding   =  token

Accept-Language  =  "Accept-Language" HCOLON
                    [ language *(COMMA language) ]
language         =  language-range *(SEMI accept-param)
language-range   =  ( ( 1*8ALPHA *( "-" 1*8ALPHA ) ) / "*" )

Alert-Info   =  "Alert-Info" HCOLON alert-param *(COMMA alert-param)
alert-param  =  LAQUOT absoluteURI RAQUOT *( SEMI generic-param )

Allow  =  "Allow" HCOLON [Method *(COMMA Method)]

Authorization     =  "Authorization" HCOLON credentials
credentials       =  ("Digest" LWS digest-response)
                     / other-response
digest-response   =  dig-resp *(COMMA dig-resp)
dig-resp          =  username / realm / nonce / digest-uri
                      / dresponse / algorithm / cnonce
                      / opaque / message-qop
                      / nonce-count / auth-param
username          =  "username" EQUAL username-value
username-value    =  quoted-string
digest-uri        =  "uri" EQUAL LDQUOT digest-uri-value RDQUOT
digest-uri-value  =  rquest-uri ; Equal to request-uri as specified
                     by HTTP/1.1
message-qop       =  "qop" EQUAL qop-value
```



```
cnonce             =  "cnonce" EQUAL cnonce-value
cnonce-value       =  nonce-value
nonce-count        =  "nc" EQUAL nc-value
nc-value           =  8LHEX
dresponse          =  "response" EQUAL request-digest
request-digest     =  LDQUOT 32LHEX RDQUOT
auth-param         =  auth-param-name EQUAL
                      ( token / quoted-string )
auth-param-name    =  token
other-response     =  auth-scheme LWS auth-param
                      *(COMMA auth-param)
auth-scheme        =  token

Authentication-Info  =  "Authentication-Info" HCOLON ainfo
                        *(COMMA ainfo)
ainfo                =  nextnonce / message-qop
                        / response-auth / cnonce
                        / nonce-count
nextnonce            =  "nextnonce" EQUAL nonce-value
response-auth        =  "rspauth" EQUAL response-digest
response-digest      =  LDQUOT *LHEX RDQUOT
```

```
Call-ID  =  ( "Call-ID" / "i" ) HCOLON callid
callid   =  word [ "@" word ]

Call-Info   =  "Call-Info" HCOLON info *(COMMA info)
info        =  LAQUOT absoluteURI RAQUOT *( SEMI info-param)
info-param  =  ( "purpose" EQUAL ( "icon" / "info"
               / "card" / token ) ) / generic-param

Contact        =  ("Contact" / "m" ) HCOLON
                  ( STAR / (contact-param *(COMMA contact-param)))
contact-param  =  (name-addr / addr-spec) *(SEMI contact-params)
name-addr      =  [ display-name ] LAQUOT addr-spec RAQUOT
addr-spec      =  SIP-URI / SIPS-URI / absoluteURI
display-name   =  *(token LWS)/ quoted-string

contact-params     =  c-p-q / c-p-expires
                      / contact-extension
c-p-q              =  "q" EQUAL qvalue
c-p-expires        =  "expires" EQUAL delta-seconds
contact-extension  =  generic-param
delta-seconds      =  1*DIGIT

Content-Disposition   =  "Content-Disposition" HCOLON
                         disp-type *( SEMI disp-param )
disp-type             =  "render" / "session" / "icon" / "alert"
                         / disp-extension-token
```



```
disp-param            =  handling-param / generic-param
handling-param        =  "handling" EQUAL
                         ( "optional" / "required"
                         / other-handling )
other-handling        =  token
disp-extension-token  =  token

Content-Encoding  =  ( "Content-Encoding" / "e" ) HCOLON
                     content-coding *(COMMA content-coding)

Content-Language  =  "Content-Language" HCOLON
                     language-tag *(COMMA language-tag)
language-tag      =  primary-tag *( "-" subtag )
primary-tag       =  1*8ALPHA
subtag            =  1*8ALPHA

Content-Length  =  ( "Content-Length" / "l" ) HCOLON 1*DIGIT
Content-Type    =  ( "Content-Type" / "c" ) HCOLON media-type
media-type      =  m-type SLASH m-subtype *(SEMI m-parameter)
m-type          =  discrete-type / composite-type
discrete-type   =  "text" / "image" / "audio" / "video"
                   / "application" / extension-token
composite-type  =  "message" / "multipart" / extension-token
extension-token =  ietf-token / x-token
ietf-token      =  token
x-token         =  "x-" token
m-subtype       =  extension-token / iana-token
iana-token      =  token
m-parameter     =  m-attribute EQUAL m-value
m-attribute     =  token
```

```
m-value          =  token / quoted-string

CSeq  =  "CSeq" HCOLON 1*DIGIT LWS Method

Date           =  "Date" HCOLON SIP-date
SIP-date       =  rfc1123-date
rfc1123-date   =  wkday "," SP date1 SP time SP "GMT"
date1          =  2DIGIT SP month SP 4DIGIT
                  ; day month year (e.g., 02 Jun 1982)
time           =  2DIGIT ":" 2DIGIT ":" 2DIGIT
                  ; 00:00:00 - 23:59:59
wkday          =  "Mon" / "Tue" / "Wed"
                  / "Thu" / "Fri" / "Sat" / "Sun"
month          =  "Jan" / "Feb" / "Mar" / "Apr"
                  / "May" / "Jun" / "Jul" / "Aug"
                  / "Sep" / "Oct" / "Nov" / "Dec"

Error-Info  =  "Error-Info" HCOLON error-uri *(COMMA error-uri)
```



```
error-uri   =  LAQUOT absoluteURI RAQUOT *( SEMI generic-param )

Expires     =  "Expires" HCOLON delta-seconds
From        =  ( "From" / "f" ) HCOLON from-spec
from-spec   =  ( name-addr / addr-spec )
               *( SEMI from-param )
from-param  =  tag-param / generic-param
tag-param   =  "tag" EQUAL token

In-Reply-To  =  "In-Reply-To" HCOLON callid *(COMMA callid)

Max-Forwards  =  "Max-Forwards" HCOLON 1*DIGIT

MIME-Version  =  "MIME-Version" HCOLON 1*DIGIT "." 1*DIGIT

Min-Expires  =  "Min-Expires" HCOLON delta-seconds

Organization  =  "Organization" HCOLON [TEXT-UTF8-TRIM]

Priority        =  "Priority" HCOLON priority-value
priority-value  =  "emergency" / "urgent" / "normal"
                   / "non-urgent" / other-priority
other-priority  =  token

Proxy-Authenticate  =  "Proxy-Authenticate" HCOLON challenge
challenge           =  ("Digest" LWS digest-cln *(COMMA digest-cln))
                       / other-challenge
other-challenge     =  auth-scheme LWS auth-param
                       *(COMMA auth-param)
digest-cln          =  realm / domain / nonce
                        / opaque / stale / algorithm
                        / qop-options / auth-param
realm               =  "realm" EQUAL realm-value
realm-value         =  quoted-string
domain              =  "domain" EQUAL LDQUOT URI
                       *( 1*SP URI ) RDQUOT
URI                 =  absoluteURI / abs-path
nonce               =  "nonce" EQUAL nonce-value
nonce-value         =  quoted-string
```

```
opaque              =  "opaque" EQUAL quoted-string
stale               =  "stale" EQUAL ( "true" / "false" )
algorithm           =  "algorithm" EQUAL ( "MD5" / "MD5-sess"
                       / token )
qop-options         =  "qop" EQUAL LDQUOT qop-value
                       *("," qop-value) RDQUOT
qop-value           =  "auth" / "auth-int" / token

Proxy-Authorization  =  "Proxy-Authorization" HCOLON credentials
```



```
Proxy-Require  =  "Proxy-Require" HCOLON option-tag
                  *(COMMA option-tag)
option-tag     =  token

Record-Route  =  "Record-Route" HCOLON rec-route *(COMMA rec-route)
rec-route     =  name-addr *( SEMI rr-param )
rr-param      =  generic-param

Reply-To      =  "Reply-To" HCOLON rplyto-spec
rplyto-spec   =  ( name-addr / addr-spec )
                 *( SEMI rplyto-param )
rplyto-param  =  generic-param
Require       =  "Require" HCOLON option-tag *(COMMA option-tag)

Retry-After  =  "Retry-After" HCOLON delta-seconds
                [ comment ] *( SEMI retry-param )

retry-param  =  ("duration" EQUAL delta-seconds)
                / generic-param

Route        =  "Route" HCOLON route-param *(COMMA route-param)
route-param  =  name-addr *( SEMI rr-param )

Server           =  "Server" HCOLON server-val *(LWS server-val)
server-val       =  product / comment
product          =  token [SLASH product-version]
product-version  =  token

Subject  =  ( "Subject" / "s" ) HCOLON [TEXT-UTF8-TRIM]

Supported  =  ( "Supported" / "k" ) HCOLON
              [option-tag *(COMMA option-tag)]

Timestamp  =  "Timestamp" HCOLON 1*(DIGIT)
               [ "." *(DIGIT) ] [ LWS delay ]
delay      =  *(DIGIT) [ "." *(DIGIT) ]

To         =  ( "To" / "t" ) HCOLON ( name-addr
              / addr-spec ) *( SEMI to-param )
to-param  =  tag-param / generic-param

Unsupported  =  "Unsupported" HCOLON option-tag *(COMMA option-tag)
User-Agent   =  "User-Agent" HCOLON server-val *(LWS server-val)
```

```
Via               =  ( "Via" / "v" ) HCOLON via-parm *(COMMA via-parm)
via-parm          =  sent-protocol LWS sent-by *( SEMI via-params )
via-params        =  via-ttl / via-maddr
                     / via-received / via-branch
                     / via-extension
via-ttl           =  "ttl" EQUAL ttl
via-maddr         =  "maddr" EQUAL host
via-received      =  "received" EQUAL (IPv4address / IPv6address)
via-branch        =  "branch" EQUAL token
via-extension     =  generic-param
sent-protocol     =  protocol-name SLASH protocol-version
                     SLASH transport
protocol-name     =  "SIP" / token
protocol-version  =  token
transport         =  "UDP" / "TCP" / "TLS" / "SCTP"
                     / other-transport
sent-by           =  host [ COLON port ]
ttl               =  1*3DIGIT ; 0 to 255

Warning        =  "Warning" HCOLON warning-value *(COMMA warning-value)
warning-value  =  warn-code SP warn-agent SP warn-text
warn-code      =  3DIGIT
warn-agent     =  hostport / pseudonym
                  ;  the name or pseudonym of the server adding
                  ;  the Warning header, for use in debugging
warn-text      =  quoted-string
pseudonym      =  token

WWW-Authenticate  =  "WWW-Authenticate" HCOLON challenge

extension-header  =  header-name HCOLON header-value
header-name       =  token
header-value      =  *(TEXT-UTF8char / UTF8-CONT / LWS)
message-body  =  *OCTET
```

26 Security Considerations: Threat Model and Security Usage Recommendations

SIP is not an easy protocol to secure. Its use of intermediaries, its multi-faceted trust relationships, its expected usage between elements with no trust at all, and its user-to-user operation make security far from trivial. Security solutions are needed that are deployable today, without extensive coordination, in a wide variety of environments and usages. In order to meet these diverse needs, several distinct mechanisms applicable to different aspects and usages of SIP will be required.

Note that the security of SIP signaling itself has no bearing on the

security of protocols used in concert with SIP such as RTP, or with the security implications of any specific bodies SIP might carry (although MIME security plays a substantial role in securing SIP). Any media associated with a session can be encrypted end-to-end independently of any associated SIP signaling. Media encryption is outside the scope of this document.

The considerations that follow first examine a set of classic threat models that broadly identify the security needs of SIP. The set of security services required to address these threats is then detailed, followed by an explanation of several security mechanisms that can be used to provide these services. Next, the requirements for implementers of SIP are enumerated, along with exemplary deployments in which these security mechanisms could be used to improve the security of SIP. Some notes on privacy conclude this section.

26.1 Attacks and Threat Models

This section details some threats that should be common to most deployments of SIP. These threats have been chosen specifically to illustrate each of the security services that SIP requires.

The following examples by no means provide an exhaustive list of the threats against SIP; rather, these are "classic" threats that demonstrate the need for particular security services that can potentially prevent whole categories of threats.

These attacks assume an environment in which attackers can potentially read any packet on the network - it is anticipated that SIP will frequently be used on the public Internet. Attackers on the network may be able to modify packets (perhaps at some compromised intermediary). Attackers may wish to steal services, eavesdrop on communications, or disrupt sessions.

26.1.1 Registration Hijacking

The SIP registration mechanism allows a user agent to identify itself to a registrar as a device at which a user (designated by an address of record) is located. A registrar assesses the identity asserted in the From header field of a REGISTER message to determine whether this request can modify the contact addresses associated with the address-of-record in the To header field. While these two fields are frequently the same, there are many valid deployments in which a third-party may register contacts on a user's behalf.

The From header field of a SIP request, however, can be modified arbitrarily by the owner of a UA, and this opens the door to malicious registrations. An attacker that successfully impersonates a party authorized to change contacts associated with an address-of-record could, for example, de-register all existing contacts for a URI and then register their own device as the appropriate contact address, thereby directing all requests for the affected user to the attacker's device.

This threat belongs to a family of threats that rely on the absence

of cryptographic assurance of a request's originator. Any SIP UAS that represents a valuable service (a gateway that interworks SIP requests with traditional telephone calls, for example) might want to control access to its resources by authenticating requests that it receives. Even end-user UAs, for example SIP phones, have an interest in ascertaining the identities of originators of requests.

This threat demonstrates the need for security services that enable SIP entities to authenticate the originators of requests.

26.1.2 Impersonating a Server

The domain to which a request is destined is generally specified in the Request-URI. UAs commonly contact a server in this domain directly in order to deliver a request. However, there is always a possibility that an attacker could impersonate the remote server, and that the UA's request could be intercepted by some other party.

For example, consider a case in which a redirect server at one domain, chicago.com, impersonates a redirect server at another domain, biloxi.com. A user agent sends a request to biloxi.com, but the redirect server at chicago.com answers with a forged response that has appropriate SIP header fields for a response from biloxi.com. The forged contact addresses in the redirection response could direct the originating UA to inappropriate or insecure resources, or simply prevent requests for biloxi.com from succeeding.

This family of threats has a vast membership, many of which are critical. As a converse to the registration hijacking threat, consider the case in which a registration sent to biloxi.com is intercepted by chicago.com, which replies to the intercepted registration with a forged 301 (Moved Permanently) response. This response might seem to come from biloxi.com yet designate chicago.com as the appropriate registrar. All future REGISTER requests from the originating UA would then go to chicago.com.

Prevention of this threat requires a means by which UAs can authenticate the servers to whom they send requests.

26.1.3 Tampering with Message Bodies

As a matter of course, SIP UAs route requests through trusted proxy servers. Regardless of how that trust is established (authentication of proxies is discussed elsewhere in this section), a UA may trust a proxy server to route a request, but not to inspect or possibly modify the bodies contained in that request.

Consider a UA that is using SIP message bodies to communicate session encryption keys for a media session. Although it trusts the proxy server of the domain it is contacting to deliver signaling properly, it may not want the administrators of that domain to be capable of decrypting any subsequent media session. Worse yet, if the proxy server were actively malicious, it could modify the session key, either acting as a man-in-the-middle, or perhaps changing the security characteristics requested by the originating UA.

This family of threats applies not only to session keys, but to most conceivable forms of content carried end-to-end in SIP. These might

include MIME bodies that should be rendered to the user, SDP, or encapsulated telephony signals, among others. Attackers might attempt to modify SDP bodies, for example, in order to point RTP media streams to a wiretapping device in order to eavesdrop on subsequent voice communications.

Also note that some header fields in SIP are meaningful end-to-end, for example, Subject. UAs might be protective of these header fields as well as bodies (a malicious intermediary changing the Subject header field might make an important request appear to be spam, for example). However, since many header fields are legitimately inspected or altered by proxy servers as a request is routed, not all header fields should be secured end-to-end.

For these reasons, the UA might want to secure SIP message bodies, and in some limited cases header fields, end-to-end. The security services required for bodies include confidentiality, integrity, and authentication. These end-to-end services should be independent of the means used to secure interactions with intermediaries such as proxy servers.

26.1.4 Tearing Down Sessions

Once a dialog has been established by initial messaging, subsequent requests can be sent that modify the state of the dialog and/or session. It is critical that principals in a session can be certain that such requests are not forged by attackers.

Consider a case in which a third-party attacker captures some initial messages in a dialog shared by two parties in order to learn the parameters of the session (To tag, From tag, and so forth) and then inserts a BYE request into the session. The attacker could opt to forge the request such that it seemed to come from either participant. Once the BYE is received by its target, the session will be torn down prematurely.

Similar mid-session threats include the transmission of forged re-INVITEs that alter the session (possibly to reduce session security or redirect media streams as part of a wiretapping attack).

The most effective countermeasure to this threat is the authentication of the sender of the BYE. In this instance, the recipient needs only know that the BYE came from the same party with whom the corresponding dialog was established (as opposed to ascertaining the absolute identity of the sender). Also, if the attacker is unable to learn the parameters of the session due to confidentiality, it would not be possible to forge the BYE. However, some intermediaries (like proxy servers) will need to inspect those parameters as the session is established.

26.1.5 Denial of Service and Amplification

Denial-of-service attacks focus on rendering a particular network element unavailable, usually by directing an excessive amount of network traffic at its interfaces. A distributed denial-of-service attack allows one network user to cause multiple network hosts to

flood a target host with a large amount of network traffic.

In many architectures, SIP proxy servers face the public Internet in order to accept requests from worldwide IP endpoints. SIP creates a number of potential opportunities for distributed denial-of-service attacks that must be recognized and addressed by the implementers and operators of SIP systems.

Attackers can create bogus requests that contain a falsified source IP address and a corresponding Via header field that identify a targeted host as the originator of the request and then send this request to a large number of SIP network elements, thereby using hapless SIP UAs or proxies to generate denial-of-service traffic aimed at the target.

Similarly, attackers might use falsified Route header field values in a request that identify the target host and then send such messages to forking proxies that will amplify messaging sent to the target.

Record-Route could be used to similar effect when the attacker is certain that the SIP dialog initiated by the request will result in numerous transactions originating in the backwards direction.

A number of denial-of-service attacks open up if REGISTER requests are not properly authenticated and authorized by registrars. Attackers could de-register some or all users in an administrative domain, thereby preventing these users from being invited to new sessions. An attacker could also register a large number of contacts designating the same host for a given address-of-record in order to use the registrar and any associated proxy servers as amplifiers in a denial-of-service attack. Attackers might also attempt to deplete available memory and disk resources of a registrar by registering huge numbers of bindings.

The use of multicast to transmit SIP requests can greatly increase the potential for denial-of-service attacks.

These problems demonstrate a general need to define architectures that minimize the risks of denial-of-service, and the need to be mindful in recommendations for security mechanisms of this class of attacks.

26.2 Security Mechanisms

From the threats described above, we gather that the fundamental security services required for the SIP protocol are: preserving the confidentiality and integrity of messaging, preventing replay attacks or message spoofing, providing for the authentication and privacy of the participants in a session, and preventing denial-of-service attacks. Bodies within SIP messages separately require the security services of confidentiality, integrity, and authentication.

Rather than defining new security mechanisms specific to SIP, SIP reuses wherever possible existing security models derived from the HTTP and SMTP space.

Page 1596
T-Mobile Exhibit 1002
Part 5 of 6

Full encryption of messages provides the best means to preserve the confidentiality of signaling - it can also guarantee that messages are not modified by any malicious intermediaries. However, SIP requests and responses cannot be naively encrypted end-to-end in their entirety because message fields such as the Request-URI, Route, and Via need to be visible to proxies in most network architectures so that SIP requests are routed correctly. Note that proxy servers need to modify some features of messages as well (such as adding Via header field values) in order for SIP to function. Proxy servers must therefore be trusted, to some degree, by SIP UAs. To this purpose, low-layer security mechanisms for SIP are recommended, which

encrypt the entire SIP requests or responses on the wire on a hop-by-hop basis, and that allow endpoints to verify the identity of proxy servers to whom they send requests.

SIP entities also have a need to identify one another in a secure fashion. When a SIP endpoint asserts the identity of its user to a peer UA or to a proxy server, that identity should in some way be verifiable. A cryptographic authentication mechanism is provided in SIP to address this requirement.

An independent security mechanism for SIP message bodies supplies an alternative means of end-to-end mutual authentication, as well as providing a limit on the degree to which user agents must trust intermediaries.

26.2.1 Transport and Network Layer Security

Transport or network layer security encrypts signaling traffic, guaranteeing message confidentiality and integrity.

Oftentimes, certificates are used in the establishment of lower-layer security, and these certificates can also be used to provide a means of authentication in many architectures.

Two popular alternatives for providing security at the transport and network layer are, respectively, TLS [25] and IPSec [26].

IPSec is a set of network-layer protocol tools that collectively can be used as a secure replacement for traditional IP (Internet Protocol). IPSec is most commonly used in architectures in which a set of hosts or administrative domains have an existing trust relationship with one another. IPSec is usually implemented at the operating system level in a host, or on a security gateway that provides confidentiality and integrity for all traffic it receives from a particular interface (as in a VPN architecture). IPSec can also be used on a hop-by-hop basis.

In many architectures IPSec does not require integration with SIP applications; IPSec is perhaps best suited to deployments in which adding security directly to SIP hosts would be arduous. UAs that have a pre-shared keying relationship with their first-hop proxy server are also good candidates to use IPSec. Any deployment of IPSec for SIP would require an IPSec profile describing the protocol tools that would be required to secure SIP. No such profile is given in this document.

Page 1597
T-Mobile Exhibit 1002
Part 5 of 6

TLS provides transport-layer security over connection-oriented protocols (for the purposes of this document, TCP); "tls" (signifying TLS over TCP) can be specified as the desired transport protocol within a Via header field value or a SIP-URI. TLS is most suited to architectures in which hop-by-hop security is required between hosts with no pre-existing trust association. For example, Alice trusts her local proxy server, which after a certificate exchange decides to trust Bob's local proxy server, which Bob trusts, hence Bob and Alice can communicate securely.

TLS must be tightly coupled with a SIP application. Note that transport mechanisms are specified on a hop-by-hop basis in SIP, thus a UA that sends requests over TLS to a proxy server has no assurance that TLS will be used end-to-end.

The TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite [6] MUST be supported at a minimum by implementers when TLS is used in a SIP application. For purposes of backwards compatibility, proxy servers, redirect servers, and registrars SHOULD support TLS_RSA_WITH_3DES_EDE_CBC_SHA. Implementers MAY also support any other ciphersuite.

26.2.2 SIPS URI Scheme

The SIPS URI scheme adheres to the syntax of the SIP URI (described in 19), although the scheme string is "sips" rather than "sip". The semantics of SIPS are very different from the SIP URI, however. SIPS allows resources to specify that they should be reached securely.

A SIPS URI can be used as an address-of-record for a particular user - the URI by which the user is canonically known (on their business cards, in the From header field of their requests, in the To header field of REGISTER requests). When used as the Request-URI of a request, the SIPS scheme signifies that each hop over which the request is forwarded, until the request reaches the SIP entity responsible for the domain portion of the Request-URI, must be secured with TLS; once it reaches the domain in question it is handled in accordance with local security and routing policy, quite possibly using TLS for any last hop to a UAS. When used by the originator of a request (as would be the case if they employed a SIPS URI as the address-of-record of the target), SIPS dictates that the entire request path to the target domain be so secured.

The SIPS scheme is applicable to many of the other ways in which SIP URIs are used in SIP today in addition to the Request-URI, including in addresses-of-record, contact addresses (the contents of Contact headers, including those of REGISTER methods), and Route headers. In each instance, the SIPS URI scheme allows these existing fields to

designate secure resources. The manner in which a SIPS URI is dereferenced in any of these contexts has its own security properties which are detailed in [4].

The use of SIPS in particular entails that mutual TLS authentication SHOULD be employed, as SHOULD the ciphersuite TLS_RSA_WITH_AES_128_CBC_SHA. Certificates received in the authentication process SHOULD be validated with root certificates held by the client; failure to validate a certificate SHOULD result in the failure of the request.

Note that in the SIPS URI scheme, transport is independent of TLS, and thus "sips:alice@atlanta.com;transport=tcp" and "sips:alice@atlanta.com;transport=sctp" are both valid (although note that UDP is not a valid transport for SIPS). The use of "transport=tls" has consequently been deprecated, partly because it was specific to a single hop of the request. This is a change since RFC 2543.

Users that distribute a SIPS URI as an address-of-record may elect to operate devices that refuse requests over insecure transports.

26.2.3 HTTP Authentication

SIP provides a challenge capability, based on HTTP authentication, that relies on the 401 and 407 response codes as well as header fields for carrying challenges and credentials. Without significant modification, the reuse of the HTTP Digest authentication scheme in SIP allows for replay protection and one-way authentication.

The usage of Digest authentication in SIP is detailed in Section 22.

26.2.4 S/MIME

As is discussed above, encrypting entire SIP messages end-to-end for the purpose of confidentiality is not appropriate because network intermediaries (like proxy servers) need to view certain header fields in order to route messages correctly, and if these intermediaries are excluded from security associations, then SIP messages will essentially be non-routable.

However, S/MIME allows SIP UAs to encrypt MIME bodies within SIP, securing these bodies end-to-end without affecting message headers. S/MIME can provide end-to-end confidentiality and integrity for message bodies, as well as mutual authentication. It is also possible to use S/MIME to provide a form of integrity and confidentiality for SIP header fields through SIP message tunneling.

The usage of S/MIME in SIP is detailed in Section 23.

26.3 Implementing Security Mechanisms

26.3.1 Requirements for Implementers of SIP

Proxy servers, redirect servers, and registrars MUST implement TLS, and MUST support both mutual and one-way authentication. It is

strongly RECOMMENDED that UAs be capable initiating TLS; UAs MAY also be capable of acting as a TLS server. Proxy servers, redirect servers, and registrars SHOULD possess a site certificate whose subject corresponds to their canonical hostname. UAs MAY have certificates of their own for mutual authentication with TLS, but no provisions are set forth in this document for their use. All SIP elements that support TLS MUST have a mechanism for validating certificates received during TLS negotiation; this entails possession of one or more root certificates issued by certificate authorities (preferably well-known distributors of site certificates comparable to those that issue root certificates for web browsers).

All SIP elements that support TLS MUST also support the SIPS URI scheme.

Proxy servers, redirect servers, registrars, and UAs MAY also implement IPSec or other lower-layer security protocols.

When a UA attempts to contact a proxy server, redirect server, or registrar, the UAC SHOULD initiate a TLS connection over which it will send SIP messages. In some architectures, UASs MAY receive requests over such TLS connections as well.

Proxy servers, redirect servers, registrars, and UAs MUST implement Digest Authorization, encompassing all of the aspects required in 22. Proxy servers, redirect servers, and registrars SHOULD be configured with at least one Digest realm, and at least one "realm" string supported by a given server SHOULD correspond to the server's hostname or domainname.

UAs MAY support the signing and encrypting of MIME bodies, and transference of credentials with S/MIME as described in Section 23. If a UA holds one or more root certificates of certificate authorities in order to validate certificates for TLS or IPSec, it SHOULD be capable of reusing these to verify S/MIME certificates, as appropriate. A UA MAY hold root certificates specifically for validating S/MIME certificates.

Note that is it anticipated that future security extensions may upgrade the normative strength associated with S/MIME as S/MIME implementations appear and the problem space becomes better understood.

26.3.2 Security Solutions

The operation of these security mechanisms in concert can follow the existing web and email security models to some degree. At a high level, UAs authenticate themselves to servers (proxy servers, redirect servers, and registrars) with a Digest username and password; servers authenticate themselves to UAs one hop away, or to another server one hop away (and vice versa), with a site certificate delivered by TLS.

On a peer-to-peer level, UAs trust the network to authenticate one another ordinarily; however, S/MIME can also be used to provide

direct authentication when the network does not, or if the network itself is not trusted.

The following is an illustrative example in which these security mechanisms are used by various UAs and servers to prevent the sorts of threats described in Section 26.1. While implementers and network administrators MAY follow the normative guidelines given in the remainder of this section, these are provided only as example implementations.

26.3.2.1 Registration

When a UA comes online and registers with its local administrative domain, it SHOULD establish a TLS connection with its registrar (Section 10 describes how the UA reaches its registrar). The registrar SHOULD offer a certificate to the UA, and the site identified by the certificate MUST correspond with the domain in which the UA intends to register; for example, if the UA intends to register the address-of-record 'alice@atlanta.com', the site certificate must identify a host within the atlanta.com domain (such as sip.atlanta.com). When it receives the TLS Certificate message, the UA SHOULD verify the certificate and inspect the site identified by the certificate. If the certificate is invalid, revoked, or if it does not identify the appropriate party, the UA MUST NOT send the REGISTER message and otherwise proceed with the registration.

When a valid certificate has been provided by the registrar, the UA knows that the registrar is not an attacker who might redirect the UA, steal passwords, or attempt any similar attacks.

The UA then creates a REGISTER request that SHOULD be addressed to a Request-URI corresponding to the site certificate received from the registrar. When the UA sends the REGISTER request over the existing TLS connection, the registrar SHOULD challenge the request with a 401 (Proxy Authentication Required) response. The "realm" parameter within the Proxy-Authenticate header field of the response SHOULD correspond to the domain previously given by the site certificate. When the UAC receives the challenge, it SHOULD either prompt the user for credentials or take an appropriate credential from a keyring corresponding to the "realm" parameter in the challenge. The username of this credential SHOULD correspond with the "userinfo" portion of the URI in the To header field of the REGISTER request. Once the Digest credentials have been inserted into an appropriate Proxy-Authorization header field, the REGISTER should be resubmitted to the registrar.

Since the registrar requires the user agent to authenticate itself, it would be difficult for an attacker to forge REGISTER requests for the user's address-of-record. Also note that since the REGISTER is sent over a confidential TLS connection, attackers will not be able to intercept the REGISTER to record credentials for any possible replay attack.

Once the registration has been accepted by the registrar, the UA SHOULD leave this TLS connection open provided that the registrar also acts as the proxy server to which requests are sent for users in

this administrative domain. The existing TLS connection will be reused to deliver incoming requests to the UA that has just completed registration.

Because the UA has already authenticated the server on the other side of the TLS connection, all requests that come over this connection are known to have passed through the proxy server - attackers cannot create spoofed requests that appear to have been sent through that proxy server.

26.3.2.2 Interdomain Requests

Now let's say that Alice's UA would like to initiate a session with a user in a remote administrative domain, namely "bob@biloxi.com". We will also say that the local administrative domain (atlanta.com) has a local outbound proxy.

The proxy server that handles inbound requests for an administrative domain MAY also act as a local outbound proxy; for simplicity's sake we'll assume this to be the case for atlanta.com (otherwise the user agent would initiate a new TLS connection to a separate server at this point). Assuming that the client has completed the registration

process described in the preceding section, it SHOULD reuse the TLS connection to the local proxy server when it sends an INVITE request to another user. The UA SHOULD reuse cached credentials in the INVITE to avoid prompting the user unnecessarily.

When the local outbound proxy server has validated the credentials presented by the UA in the INVITE, it SHOULD inspect the Request-URI to determine how the message should be routed (see [4]). If the "domainname" portion of the Request-URI had corresponded to the local domain (atlanta.com) rather than biloxi.com, then the proxy server would have consulted its location service to determine how best to reach the requested user.

Had "alice@atlanta.com" been attempting to contact, say, "alex@atlanta.com", the local proxy would have proxied to the request to the TLS connection Alex had established with the registrar when he registered. Since Alex would receive this request over his authenticated channel, he would be assured that Alice's request had been authorized by the proxy server of the local administrative domain.

However, in this instance the Request-URI designates a remote domain. The local outbound proxy server at atlanta.com SHOULD therefore establish a TLS connection with the remote proxy server at biloxi.com. Since both of the participants in this TLS connection are servers that possess site certificates, mutual TLS authentication SHOULD occur. Each side of the connection SHOULD verify and inspect the certificate of the other, noting the domain name that appears in the certificate for comparison with the header fields of SIP messages. The atlanta.com proxy server, for example, SHOULD verify at this stage that the certificate received from the remote side corresponds with the biloxi.com domain. Once it has done so, and TLS negotiation has completed, resulting in a secure channel between the two proxies, the atlanta.com proxy can forward the INVITE request to biloxi.com.

The proxy server at biloxi.com SHOULD inspect the certificate of the proxy server at atlanta.com in turn and compare the domain asserted by the certificate with the "domainname" portion of the From header field in the INVITE request. The biloxi proxy MAY have a strict security policy that requires it to reject requests that do not match the administrative domain from which they have been proxied.

> Such security policies could be instituted to prevent the SIP equivalent of SMTP 'open relays' that are frequently exploited to generate spam.

This policy, however, only guarantees that the request came from the domain it ascribes to itself; it does not allow biloxi.com to ascertain how atlanta.com authenticated Alice. Only if biloxi.com has some other way of knowing atlanta.com's authentication policies could it possibly ascertain how Alice proved her identity. biloxi.com might then institute an even stricter policy that forbids requests that come from domains that are not known administratively to share a common authentication policy with biloxi.com.

Once the INVITE has been approved by the biloxi proxy, the proxy server SHOULD identify the existing TLS channel, if any, associated with the user targeted by this request (in this case "bob@biloxi.com"). The INVITE should be proxied through this channel to Bob. Since the request is received over a TLS connection that had previously been authenticated as the biloxi proxy, Bob knows that the From header field was not tampered with and that atlanta.com has validated Alice, although not necessarily whether or not to trust Alice's identity.

Before they forward the request, both proxy servers SHOULD add a Record-Route header field to the request so that all future requests in this dialog will pass through the proxy servers. The proxy servers can thereby continue to provide security services for the lifetime of this dialog. If the proxy servers do not add themselves to the Record-Route, future messages will pass directly end-to-end between Alice and Bob without any security services (unless the two parties agree on some independent end-to-end security such as S/MIME). In this respect the SIP trapezoid model can provide a nice structure where conventions of agreement between the site proxies can provide a reasonably secure channel between Alice and Bob.

> An attacker preying on this architecture would, for example, be unable to forge a BYE request and insert it into the signaling stream between Bob and Alice because the attacker has no way of ascertaining the parameters of the session and also because the integrity mechanism transitively protects the traffic between Alice and Bob.

26.3.2.3 Peer-to-Peer Requests

Alternatively, consider a UA asserting the identity "carol@chicago.com" that has no local outbound proxy. When Carol wishes to send an INVITE to "bob@biloxi.com", her UA SHOULD initiate a TLS connection with the biloxi proxy directly (using the mechanism

Page 1603
T-Mobile Exhibit 1002
Part 5 of 6

described in [4] to determine how to best to reach the given Request-URI). When her UA receives a certificate from the biloxi proxy, it SHOULD be verified normally before she passes her INVITE across the TLS connection. However, Carol has no means of proving

her identity to the biloxi proxy, but she does have a CMS-detached signature over a "message/sip" body in the INVITE. It is unlikely in this instance that Carol would have any credentials in the biloxi.com realm, since she has no formal association with biloxi.com. The biloxi proxy MAY also have a strict policy that precludes it from even bothering to challenge requests that do not have biloxi.com in the "domainname" portion of the From header field - it treats these users as unauthenticated.

The biloxi proxy has a policy for Bob that all non-authenticated requests should be redirected to the appropriate contact address registered against 'bob@biloxi.com', namely <sip:bob@192.0.2.4>. Carol receives the redirection response over the TLS connection she established with the biloxi proxy, so she trusts the veracity of the contact address.

Carol SHOULD then establish a TCP connection with the designated address and send a new INVITE with a Request-URI containing the received contact address (recomputing the signature in the body as the request is readied). Bob receives this INVITE on an insecure interface, but his UA inspects and, in this instance, recognizes the From header field of the request and subsequently matches a locally cached certificate with the one presented in the signature of the body of the INVITE. He replies in similar fashion, authenticating himself to Carol, and a secure dialog begins.

> Sometimes firewalls or NATs in an administrative domain could preclude the establishment of a direct TCP connection to a UA. In these cases, proxy servers could also potentially relay requests to UAs in a way that has no trust implications (for example, forgoing an existing TLS connection and forwarding the request over cleartext TCP) as local policy dictates.

26.3.2.4 DoS Protection

In order to minimize the risk of a denial-of-service attack against architectures using these security solutions, implementers should take note of the following guidelines.

When the host on which a SIP proxy server is operating is routable from the public Internet, it SHOULD be deployed in an administrative domain with defensive operational policies (blocking source-routed traffic, preferably filtering ping traffic). Both TLS and IPSec can also make use of bastion hosts at the edges of administrative domains that participate in the security associations to aggregate secure tunnels and sockets. These bastion hosts can also take the brunt of denial-of-service attacks, ensuring that SIP hosts within the administrative domain are not encumbered with superfluous messaging.

T-Mobile Exhibit 1002
Part 5 of 6

No matter what security solutions are deployed, floods of messages directed at proxy servers can lock up proxy server resources and prevent desirable traffic from reaching its destination. There is a computational expense associated with processing a SIP transaction at a proxy server, and that expense is greater for stateful proxy servers than it is for stateless proxy servers. Therefore, stateful proxies are more susceptible to flooding than stateless proxy servers.

UAs and proxy servers SHOULD challenge questionable requests with only a single 401 (Unauthorized) or 407 (Proxy Authentication Required), forgoing the normal response retransmission algorithm, and thus behaving statelessly towards unauthenticated requests.

> Retransmitting the 401 (Unauthorized) or 407 (Proxy Authentication Required) status response amplifies the problem of an attacker using a falsified header field value (such as Via) to direct traffic to a third party.

In summary, the mutual authentication of proxy servers through mechanisms such as TLS significantly reduces the potential for rogue intermediaries to introduce falsified requests or responses that can deny service. This commensurately makes it harder for attackers to make innocent SIP nodes into agents of amplification.

26.4 Limitations

Although these security mechanisms, when applied in a judicious manner, can thwart many threats, there are limitations in the scope of the mechanisms that must be understood by implementers and network operators.

26.4.1 HTTP Digest

One of the primary limitations of using HTTP Digest in SIP is that the integrity mechanisms in Digest do not work very well for SIP. Specifically, they offer protection of the Request-URI and the method of a message, but not for any of the header fields that UAs would most likely wish to secure.

The existing replay protection mechanisms described in RFC 2617 also have some limitations for SIP. The next-nonce mechanism, for example, does not support pipelined requests. The nonce-count mechanism should be used for replay protection.

Another limitation of HTTP Digest is the scope of realms. Digest is valuable when a user wants to authenticate themselves to a resource with which they have a pre-existing association, like a service

provider of which the user is a customer (which is quite a common scenario and thus Digest provides an extremely useful function). By way of contrast, the scope of TLS is interdomain or multirealm, since certificates are often globally verifiable, so that the UA can authenticate the server with no pre-existing association.

26.4.2 S/MIME

The largest outstanding defect with the S/MIME mechanism is the lack of a prevalent public key infrastructure for end users. If self-signed certificates (or certificates that cannot be verified by one of the participants in a dialog) are used, the SIP-based key exchange mechanism described in Section 23.2 is susceptible to a man-in-the-middle attack with which an attacker can potentially inspect and modify S/MIME bodies. The attacker needs to intercept the first exchange of keys between the two parties in a dialog, remove the existing CMS-detached signatures from the request and response, and insert a different CMS-detached signature containing a certificate supplied by the attacker (but which seems to be a certificate for the proper address-of-record). Each party will think they have exchanged keys with the other, when in fact each has the public key of the attacker.

It is important to note that the attacker can only leverage this vulnerability on the first exchange of keys between two parties - on subsequent occasions, the alteration of the key would be noticeable to the UAs. It would also be difficult for the attacker to remain in the path of all future dialogs between the two parties over time (as potentially days, weeks, or years pass).

SSH is susceptible to the same man-in-the-middle attack on the first exchange of keys; however, it is widely acknowledged that while SSH is not perfect, it does improve the security of connections. The use of key fingerprints could provide some assistance to SIP, just as it does for SSH. For example, if two parties use SIP to establish a voice communications session, each could read off the fingerprint of the key they received from the other, which could be compared against the original. It would certainly be more difficult for the man-in-the-middle to emulate the voices of the participants than their signaling (a practice that was used with the Clipper chip-based secure telephone).

The S/MIME mechanism allows UAs to send encrypted requests without preamble if they possess a certificate for the destination address-of-record on their keyring. However, it is possible that any particular device registered for an address-of-record will not hold the certificate that has been previously employed by the device's current user, and that it will therefore be unable to process an

encrypted request properly, which could lead to some avoidable error signaling. This is especially likely when an encrypted request is forked.

The keys associated with S/MIME are most useful when associated with a particular user (an address-of-record) rather than a device (a UA). When users move between devices, it may be difficult to transport private keys securely between UAs; how such keys might be acquired by a device is outside the scope of this document.

Another, more prosaic difficulty with the S/MIME mechanism is that it can result in very large messages, especially when the SIP tunneling mechanism described in Section 23.4 is used. For that reason, it is RECOMMENDED that TCP should be used as a transport protocol when S/MIME tunneling is employed.

26.4.3 TLS

The most commonly voiced concern about TLS is that it cannot run over UDP; TLS requires a connection-oriented underlying transport protocol, which for the purposes of this document means TCP.

It may also be arduous for a local outbound proxy server and/or registrar to maintain many simultaneous long-lived TLS connections with numerous UAs. This introduces some valid scalability concerns, especially for intensive ciphersuites. Maintaining redundancy of long-lived TLS connections, especially when a UA is solely responsible for their establishment, could also be cumbersome.

TLS only allows SIP entities to authenticate servers to which they are adjacent; TLS offers strictly hop-by-hop security. Neither TLS, nor any other mechanism specified in this document, allows clients to authenticate proxy servers to whom they cannot form a direct TCP connection.

26.4.4 SIPS URIs

Actually using TLS on every segment of a request path entails that the terminating UAS must be reachable over TLS (perhaps registering with a SIPS URI as a contact address). This is the preferred use of SIPS. Many valid architectures, however, use TLS to secure part of the request path, but rely on some other mechanism for the final hop to a UAS, for example. Thus SIPS cannot guarantee that TLS usage will be truly end-to-end. Note that since many UAs will not accept incoming TLS connections, even those UAs that do support TLS may be required to maintain persistent TLS connections as described in the TLS limitations section above in order to receive requests over TLS as a UAS.

Location services are not required to provide a SIPS binding for a SIPS Request-URI. Although location services are commonly populated by user registrations (as described in Section 10.2.1), various other protocols and interfaces could conceivably supply contact addresses for an AOR, and these tools are free to map SIPS URIs to SIP URIs as appropriate. When queried for bindings, a location service returns its contact addresses without regard for whether it received a request with a SIPS Request-URI. If a redirect server is accessing the location service, it is up to the entity that processes the Contact header field of a redirection to determine the propriety of the contact addresses.

Ensuring that TLS will be used for all of the request segments up to the target domain is somewhat complex. It is possible that cryptographically authenticated proxy servers along the way that are non-compliant or compromised may choose to disregard the forwarding rules associated with SIPS (and the general forwarding rules in Section 16.6). Such malicious intermediaries could, for example, retarget a request from a SIPS URI to a SIP URI in an attempt to downgrade security.

Alternatively, an intermediary might legitimately retarget a request from a SIP to a SIPS URI. Recipients of a request whose Request-URI uses the SIPS URI scheme thus cannot assume on the basis of the

T-Mobile Exhibit 1002
Part 5 of 6

Request-URI alone that SIPS was used for the entire request path (from the client onwards).

To address these concerns, it is RECOMMENDED that recipients of a request whose Request-URI contains a SIP or SIPS URI inspect the To header field value to see if it contains a SIPS URI (though note that it does not constitute a breach of security if this URI has the same scheme but is not equivalent to the URI in the To header field). Although clients may choose to populate the Request-URI and To header field of a request differently, when SIPS is used this disparity could be interpreted as a possible security violation, and the request could consequently be rejected by its recipient. Recipients MAY also inspect the Via header chain in order to double-check whether or not TLS was used for the entire request path until the local administrative domain was reached. S/MIME may also be used by the originating UAC to help ensure that the original form of the To header field is carried end-to-end.

If the UAS has reason to believe that the scheme of the Request-URI has been improperly modified in transit, the UA SHOULD notify its user of a potential security breach.

As a further measure to prevent downgrade attacks, entities that accept only SIPS requests MAY also refuse connections on insecure ports.

End users will undoubtedly discern the difference between SIPS and SIP URIs, and they may manually edit them in response to stimuli. This can either benefit or degrade security. For example, if an attacker corrupts a DNS cache, inserting a fake record set that effectively removes all SIPS records for a proxy server, then any SIPS requests that traverse this proxy server may fail. When a user, however, sees that repeated calls to a SIPS AOR are failing, they could on some devices manually convert the scheme from SIPS to SIP and retry. Of course, there are some safeguards against this (if the destination UA is truly paranoid it could refuse all non-SIPS requests), but it is a limitation worth noting. On the bright side, users might also divine that 'SIPS' would be valid even when they are presented only with a SIP URI.

26.5 Privacy

SIP messages frequently contain sensitive information about their senders - not just what they have to say, but with whom they communicate, when they communicate and for how long, and from where they participate in sessions. Many applications and their users require that this sort of private information be hidden from any parties that do not need to know it.

Note that there are also less direct ways in which private information can be divulged. If a user or service chooses to be reachable at an address that is guessable from the person's name and organizational affiliation (which describes most addresses-of-record), the traditional method of ensuring privacy by having an unlisted "phone number" is compromised. A user location service can

Page 1608
T-Mobile Exhibit 1002
Part 5 of 6

infringe on the privacy of the recipient of a session invitation by divulging their specific whereabouts to the caller; an implementation consequently SHOULD be able to restrict, on a per-user basis, what kind of location and availability information is given out to certain classes of callers. This is a whole class of problem that is expected to be studied further in ongoing SIP work.

In some cases, users may want to conceal personal information in header fields that convey identity. This can apply not only to the From and related headers representing the originator of the request, but also the To - it may not be appropriate to convey to the final destination a speed-dialing nickname, or an unexpanded identifier for a group of targets, either of which would be removed from the Request-URI as the request is routed, but not changed in the To

header field if the two were initially identical. Thus it MAY be desirable for privacy reasons to create a To header field that differs from the Request-URI.

27 IANA Considerations

All method names, header field names, status codes, and option tags used in SIP applications are registered with IANA through instructions in an IANA Considerations section in an RFC.

The specification instructs the IANA to create four new sub-registries under http://www.iana.org/assignments/sip-parameters: Option Tags, Warning Codes (warn-codes), Methods and Response Codes, added to the sub-registry of Header Fields that is already present there.

27.1 Option Tags

This specification establishes the Option Tags sub-registry under http://www.iana.org/assignments/sip-parameters.

Option tags are used in header fields such as Require, Supported, Proxy-Require, and Unsupported in support of SIP compatibility mechanisms for extensions (Section 19.2). The option tag itself is a string that is associated with a particular SIP option (that is, an extension). It identifies the option to SIP endpoints.

Option tags are registered by the IANA when they are published in standards track RFCs. The IANA Considerations section of the RFC must include the following information, which appears in the IANA registry along with the RFC number of the publication.

- Name of the option tag. The name MAY be of any length, but SHOULD be no more than twenty characters long. The name MUST consist of alphanum (Section 25) characters only.

- Descriptive text that describes the extension.

27.2 Warn-Codes

This specification establishes the Warn-codes sub-registry under http://www.iana.org/assignments/sip-parameters and initiates its

Page 1609
T-Mobile Exhibit 1002
Part 5 of 6

population with the warn-codes listed in Section 20.43. Additional warn-codes are registered by RFC publication.

The descriptive text for the table of warn-codes is:

Warning codes provide information supplemental to the status code in SIP response messages when the failure of the transaction results from a Session Description Protocol (SDP) (RFC 2327 [1]) problem.

The "warn-code" consists of three digits. A first digit of "3" indicates warnings specific to SIP. Until a future specification describes uses of warn-codes other than 3xx, only 3xx warn-codes may be registered.

Warnings 300 through 329 are reserved for indicating problems with keywords in the session description, 330 through 339 are warnings related to basic network services requested in the session description, 370 through 379 are warnings related to quantitative QoS parameters requested in the session description, and 390 through 399 are miscellaneous warnings that do not fall into one of the above categories.

27.3 Header Field Names

This obsoletes the IANA instructions about the header sub-registry under http://www.iana.org/assignments/sip-parameters.

The following information needs to be provided in an RFC publication in order to register a new header field name:

- The RFC number in which the header is registered;
- the name of the header field being registered;
- a compact form version for that header field, if one is defined;

Some common and widely used header fields MAY be assigned one-letter compact forms (Section 7.3.3). Compact forms can only be assigned after SIP working group review, followed by RFC publication.

27.4 Method and Response Codes

This specification establishes the Method and Response-Code sub-registries under http://www.iana.org/assignments/sip-parameters and initiates their population as follows. The initial Methods table is:

INVITE	[RFC3261]
ACK	[RFC3261]
BYE	[RFC3261]
CANCEL	[RFC3261]
REGISTER	[RFC3261]
OPTIONS	[RFC3261]
INFO	[RFC2976]

The response code table is initially populated from Section 21, the portions labeled Informational, Success, Redirection, Client-Error, Server-Error, and Global-Failure. The table has the following format:

Type (e.g., Informational)
Number Default Reason Phrase [RFC3261]

The following information needs to be provided in an RFC publication in order to register a new response code or method:

- The RFC number in which the method or response code is registered;
- the number of the response code or name of the method being registered;
- the default reason phrase for that response code, if applicable;

27.5 The "message/sip" MIME type.

This document registers the "message/sip" MIME media type in order to allow SIP messages to be tunneled as bodies within SIP, primarily for end-to-end security purposes. This media type is defined by the following information:

Media type name: message
Media subtype name: sip
Required parameters: none

Optional parameters: version
version: The SIP-Version number of the enclosed message (e.g., "2.0"). If not present, the version defaults to "2.0".
Encoding scheme: SIP messages consist of an 8-bit header optionally followed by a binary MIME data object. As such, SIP messages must be treated as binary. Under normal circumstances SIP messages are transported over binary-capable transports, no special encodings are needed.

Security considerations: see below
Motivation and examples of this usage as a security mechanism in concert with S/MIME are given in 23.4.

27.6 New Content-Disposition Parameter Registrations

This document also registers four new Content-Disposition header "disposition-types": alert, icon, session and render. The authors request that these values be recorded in the IANA registry for Content-Dispositions.

Descriptions of these "disposition-types", including motivation and examples, are given in Section 20.11.

Short descriptions suitable for the IANA registry are:

alert	the body is a custom ring tone to alert the user
icon	the body is displayed as an icon to the user
render	the body should be displayed to the user
session	the body describes a communications session, for example, as RFC 2327 SDP body

28 Changes From RFC 2543

This RFC revises RFC 2543. It is mostly backwards compatible with RFC 2543. The changes described here fix many errors discovered in RFC 2543 and provide information on scenarios not detailed in RFC 2543. The protocol has been presented in a more cleanly layered model here.

We break the differences into functional behavior that is a substantial change from RFC 2543, which has impact on interoperability or correct operation in some cases, and functional behavior that is different from RFC 2543 but not a potential source of interoperability problems. There have been countless clarifications as well, which are not documented here.

28.1 Major Functional Changes

- When a UAC wishes to terminate a call before it has been answered, it sends CANCEL. If the original INVITE still returns a 2xx, the UAC then sends BYE. BYE can only be sent on an existing call leg (now called a dialog in this RFC), whereas it could be sent at any time in RFC 2543.

- The SIP BNF was converted to be RFC 2234 compliant.

- SIP URL BNF was made more general, allowing a greater set of characters in the user part. Furthermore, comparison rules were simplified to be primarily case-insensitive, and detailed handling of comparison in the presence of parameters was described. The most substantial change is that a URI with a parameter with the default value does not match a URI without that parameter.

- Removed Via hiding. It had serious trust issues, since it relied on the next hop to perform the obfuscation process. Instead, Via hiding can be done as a local implementation choice in stateful proxies, and thus is no longer documented.

- In RFC 2543, CANCEL and INVITE transactions were intermingled.

They are separated now. When a user sends an INVITE and then a CANCEL, the INVITE transaction still terminates normally. A UAS needs to respond to the original INVITE request with a 487 response.

- Similarly, CANCEL and BYE transactions were intermingled; RFC 2543 allowed the UAS not to send a response to INVITE when a BYE was received. That is disallowed here. The original INVITE needs a response.

- In RFC 2543, UAs needed to support only UDP. In this RFC, UAs need to support both UDP and TCP.

- In RFC 2543, a forking proxy only passed up one challenge from downstream elements in the event of multiple challenges. In this RFC, proxies are supposed to collect all challenges and place them into the forwarded response.

- In Digest credentials, the URI needs to be quoted; this is unclear from RFC 2617 and RFC 2069 which are both inconsistent on it.

- SDP processing has been split off into a separate specification [13], and more fully specified as a formal offer/answer exchange process that is effectively tunneled through SIP. SDP is allowed in INVITE/200 or 200/ACK for baseline SIP implementations; RFC 2543 alluded to the ability to use it in INVITE, 200, and ACK in a single transaction, but this was not well specified. More complex SDP usages are allowed in extensions.

- Added full support for IPv6 in URIs and in the Via header field. Support for IPv6 in Via has required that its header field parameters allow the square bracket and colon characters. These characters were previously not permitted. In theory, this could cause interop problems with older implementations. However, we have observed that most implementations accept any non-control ASCII character in these parameters.

- DNS SRV procedure is now documented in a separate specification [4]. This procedure uses both SRV and NAPTR resource records and no longer combines data from across SRV records as described in RFC 2543.

- Loop detection has been made optional, supplanted by a mandatory usage of Max-Forwards. The loop detection procedure in RFC 2543 had a serious bug which would report "spirals" as an error condition when it was not. The optional loop detection procedure is more fully and correctly specified here.

- Usage of tags is now mandatory (they were optional in RFC 2543), as they are now the fundamental building blocks of dialog identification.

- Added the Supported header field, allowing for clients to indicate what extensions are supported to a server, which can apply those extensions to the response, and indicate their usage with a Require in the response.

- Extension parameters were missing from the BNF for several header fields, and they have been added.

- Handling of Route and Record-Route construction was very underspecified in RFC 2543, and also not the right approach. It has been substantially reworked in this specification (and made vastly simpler), and this is arguably the largest change. Backwards compatibility is still provided for deployments that do not use "pre-loaded routes", where the initial request has a set of Route header field values obtained in some way outside of Record-Route. In those situations, the new mechanism is not interoperable.

- In RFC 2543, lines in a message could be terminated with CR, LF, or CRLF. This specification only allows CRLF.

- Usage of Route in CANCEL and ACK was not well defined in RFC 2543. It is now well specified; if a request had a Route header field, its CANCEL or ACK for a non-2xx response to the request need to carry the same Route header field values. ACKs for 2xx responses use the Route values learned from the Record-Route of the 2xx responses.

- RFC 2543 allowed multiple requests in a single UDP packet. This usage has been removed.

- Usage of absolute time in the Expires header field and parameter has been removed. It caused interoperability problems in elements that were not time synchronized, a common occurrence. Relative times are used instead.

- The branch parameter of the Via header field value is now mandatory for all elements to use. It now plays the role of a unique transaction identifier. This avoids the complex and bug-laden transaction identification rules from RFC 2543. A magic cookie is used in the parameter value to determine if the previous hop has made the parameter globally unique, and comparison falls back to the old rules when it is not present. Thus, interoperability is assured.

- In RFC 2543, closure of a TCP connection was made equivalent to a CANCEL. This was nearly impossible to implement (and wrong) for TCP connections between proxies. This has been eliminated, so that there is no coupling between TCP connection state and SIP processing.

- RFC 2543 was silent on whether a UA could initiate a new

transaction to a peer while another was in progress. That is now specified here. It is allowed for non-INVITE requests, disallowed for INVITE.

- PGP was removed. It was not sufficiently specified, and not compatible with the more complete PGP MIME. It was replaced with S/MIME.

- Added the "sips" URI scheme for end-to-end TLS. This scheme is not backwards compatible with RFC 2543. Existing elements that receive a request with a SIPS URI scheme in the Request-URI will likely reject the request. This is actually a feature; it ensures that a call to a SIPS URI is only delivered if all path hops can be secured.

- Additional security features were added with TLS, and these are described in a much larger and complete security considerations section.

- In RFC 2543, a proxy was not required to forward provisional responses from 101 to 199 upstream. This was changed to MUST. This is important, since many subsequent features depend on delivery of all provisional responses from 101 to 199.

- Little was said about the 503 response code in RFC 2543. It has since found substantial use in indicating failure or overload conditions in proxies. This requires somewhat special treatment. Specifically, receipt of a 503 should trigger an attempt to contact the next element in the result of a DNS SRV lookup. Also, 503 response is only forwarded upstream by a proxy under certain conditions.

- RFC 2543 defined, but did no sufficiently specify, a mechanism for UA authentication of a server. That has been removed. Instead, the mutual authentication procedures of RFC 2617 are allowed.

- A UA cannot send a BYE for a call until it has received an ACK for the initial INVITE. This was allowed in RFC 2543 but leads to a potential race condition.

- A UA or proxy cannot send CANCEL for a transaction until it gets a provisional response for the request. This was allowed in RFC 2543 but leads to potential race conditions.

- The action parameter in registrations has been deprecated. It was insufficient for any useful services, and caused conflicts when application processing was applied in proxies.

- RFC 2543 had a number of special cases for multicast. For example, certain responses were suppressed, timers were adjusted, and so on. Multicast now plays a more limited role, and the protocol operation is unaffected by usage of multicast as opposed to unicast. The limitations as a result of that are documented.

- Basic authentication has been removed entirely and its usage

forbidden.

- Proxies no longer forward a 6xx immediately on receiving it. Instead, they CANCEL pending branches immediately. This avoids a potential race condition that would result in a UAC getting a 6xx followed by a 2xx. In all cases except this race condition, the result will be the same - the 6xx is forwarded upstream.

- RFC 2543 did not address the problem of request merging. This occurs when a request forks at a proxy and later rejoins at an element. Handling of merging is done only at a UA, and procedures are defined for rejecting all but the first request.

28.2 Minor Functional Changes

- Added the Alert-Info, Error-Info, and Call-Info header fields for optional content presentation to users.

- Added the Content-Language, Content-Disposition and MIME-Version header fields.

- Added a "glare handling" mechanism to deal with the case where both parties send each other a re-INVITE simultaneously. It uses the new 491 (Request Pending) error code.

- Added the In-Reply-To and Reply-To header fields for supporting the return of missed calls or messages at a later time.

- Added TLS and SCTP as valid SIP transports.

- There were a variety of mechanisms described for handling failures at any time during a call; those are now generally unified. BYE is sent to terminate.

- RFC 2543 mandated retransmission of INVITE responses over TCP, but noted it was really only needed for 2xx. That was an artifact of insufficient protocol layering. With a more coherent transaction layer defined here, that is no longer needed. Only 2xx responses to INVITEs are retransmitted over TCP.

- Client and server transaction machines are now driven based on timeouts rather than retransmit counts. This allows the state machines to be properly specified for TCP and UDP.

- The Date header field is used in REGISTER responses to provide a simple means for auto-configuration of dates in user agents.

- Allowed a registrar to reject registrations with expirations that are too short in duration. Defined the 423 response code and the Min-Expires for this purpose.

29 Normative References

[1] Handley, M. and V. Jacobson, "SDP: Session Description Protocol", RFC 2327, April 1998.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[3] Resnick, P., "Internet Message Format", RFC 2822, April 2001.

[4] Rosenberg, J. and H. Schulzrinne, "SIP: Locating SIP Servers", RFC 3263, June 2002.

[5] Berners-Lee, T., Fielding, R. and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[6] Chown, P., "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)", RFC 3268, June 2002.

[7] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998.

[8] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[9] Vaha-Sipila, A., "URLs for Telephone Calls", RFC 2806, April 2000.

[10] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[11] Freed, F. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, November 1996.

[12] Eastlake, D., Crocker, S. and J. Schiller, "Randomness Recommendations for Security", RFC 1750, December 1994.

[13] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with SDP", RFC 3264, June 2002.

[14] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[15] Postel, J., "DoD Standard Transmission Control Protocol", RFC 761, January 1980.

[16] Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, L. and V. Paxson,

"Stream Control Transmission Protocol", RFC 2960, October 2000.

[17] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A. and L. Stewart, "HTTP authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[18] Troost, R., Dorner, S. and K. Moore, "Communicating Presentation Information in Internet Messages: The Content-Disposition Header Field", RFC 2183, August 1997.

[19] Zimmerer, E., Peterson, J., Vemuri, A., Ong, L., Audet, F., Watson, M. and M. Zonoun, "MIME media types for ISUP and QSIG Objects", RFC 3204, December 2001.

[20] Braden, R., "Requirements for Internet Hosts - Application and Support", STD 3, RFC 1123, October 1989.

[21] Alvestrand, H., "IETF Policy on Character Sets and Languages", BCP 18, RFC 2277, January 1998.

[22] Galvin, J., Murphy, S., Crocker, S. and N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", RFC 1847, October 1995.

[23] Housley, R., "Cryptographic Message Syntax", RFC 2630, June 1999.

[24] Ramsdell B., "S/MIME Version 3 Message Specification", RFC 2633, June 1999.

[25] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[26] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

30 Informative References

[27] R. Pandya, "Emerging mobile and personal communication systems," IEEE Communications Magazine, Vol. 33, pp. 44--52, June 1995.

[28] Schulzrinne, H., Casner, S., Frederick, R. and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", RFC 1889, January 1996.

[29] Schulzrinne, H., Rao, R. and R. Lanphier, "Real Time Streaming Protocol (RTSP)", RFC 2326, April 1998.

[30] Cuervo, F., Greene, N., Rayhan, A., Huitema, C., Rosen, B. and J. Segers, "Megaco Protocol Version 1.0", RFC 3015, November 2000.

[31] Handley, M., Schulzrinne, H., Schooler, E. and J. Rosenberg, "SIP: Session Initiation Protocol", RFC 2543, March 1999.

[32] Hoffman, P., Masinter, L. and J. Zawinski, "The mailto URL

Page 1618

T-Mobile Exhibit 1002
Part 5 of 6

scheme", RFC 2368, July 1998.

[33] E. M. Schooler, "A multicast user directory service for synchronous rendezvous," Master's Thesis CS-TR-96-18, Department of Computer Science, California Institute of Technology, Pasadena, California, Aug. 1996.

[34] Donovan, S., "The SIP INFO Method", RFC 2976, October 2000.

[35] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[36] Dawson, F. and T. Howes, "vCard MIME Directory Profile", RFC 2426, September 1998.

[37] Good, G., "The LDAP Data Interchange Format (LDIF) - Technical Specification", RFC 2849, June 2000.

[38] Palme, J., "Common Internet Message Headers", RFC 2076, February 1997.

[39] Franks, J., Hallam-Baker, P., Hostetler, J., Leach, P., Luotonen, A., Sink, E. and L. Stewart, "An Extension to HTTP: Digest Access Authentication", RFC 2069, January 1997.

[40] Johnston, A., Donovan, S., Sparks, R., Cunningham, C., Willis, D., Rosenberg, J., Summers, K. and H. Schulzrinne, "SIP Call Flow Examples", Work in Progress.

[41] E. M. Schooler, "Case study: multimedia conference control in a packet-switched teleconferencing system," Journal of Internetworking: Research and Experience, Vol. 4, pp. 99--120, June 1993. ISI reprint series ISI/RS-93-359.

[42] H. Schulzrinne, "Personal mobility for multimedia services in the Internet," in European Workshop on Interactive Distributed Multimedia Systems and Services (IDMS), (Berlin, Germany), Mar. 1996.

[43] Floyd, S., "Congestion Control Principles", RFC 2914, September 2000.

A Table of Timer Values

Table 4 summarizes the meaning and defaults of the various timers used by this specification.

Timer	Value	Section	Meaning
T1	500ms default	Section 17.1.1.1	RTT Estimate
T2	4s	Section 17.1.2.2	The maximum retransmit interval for non-INVITE requests and INVITE responses
T4	5s	Section 17.1.2.2	Maximum duration a message will remain in the network
Timer A	initially T1	Section 17.1.1.2	INVITE request retransmit interval, for UDP only
Timer B	64*T1	Section 17.1.1.2	INVITE transaction timeout timer
Timer C	> 3min	Section 16.6 bullet 11	proxy INVITE transaction timeout
Timer D	> 32s for UDP 0s for TCP/SCTP	Section 17.1.1.2	Wait time for response retransmits
Timer E	initially T1	Section 17.1.2.2	non-INVITE request retransmit interval, UDP only
Timer F	64*T1	Section 17.1.2.2	non-INVITE transaction timeout timer
Timer G	initially T1	Section 17.2.1	INVITE response

			retransmit interval
Timer H	64*T1	Section 17.2.1	Wait time for ACK receipt
Timer I	T4 for UDP 0s for TCP/SCTP	Section 17.2.1	Wait time for ACK retransmits
Timer J	64*T1 for UDP 0s for TCP/SCTP	Section 17.2.2	Wait time for non-INVITE request retransmits
Timer K	T4 for UDP 0s for TCP/SCTP	Section 17.1.2.2	Wait time for response retransmits

Table 4: Summary of timers

Acknowledgments

We wish to thank the members of the IETF MMUSIC and SIP WGs for their comments and suggestions. Detailed comments were provided by Ofir Arkin, Brian Bidulock, Jim Buller, Neil Deason, Dave Devanathan, Keith Drage, Bill Fenner, Cedric Fluckiger, Yaron Goland, John Hearty, Bernie Hoeneisen, Jo Hornsby, Phil Hoffer, Christian Huitema, Hisham Khartabil, Jean Jervis, Cadi Karmi, Peter Kjellerstedt, Anders Kristensen, Jonathan Lennox, Gethin Liddell, Allison Mankin, William Marshall, Rohan Mahy, Keith Moore, Vern Paxson, Bob Penfield, Moshe J. Sambol, Chip Sharp, Igor Slepchin, Eric Tremblay, and Rick Workman.

Brian Rosen provided the compiled BNF.

Jean Mahoney provided technical writing assistance.

This work is based, inter alia, on [41,42].

Authors' Addresses

Authors addresses are listed alphabetically for the editors, the writers, and then the original authors of RFC 2543. All listed authors actively contributed large amounts of text to this document.

Jonathan Rosenberg
dynamicsoft
72 Eagle Rock Ave
East Hanover, NJ 07936
USA

EMail: jdrosen@dynamicsoft.com

Henning Schulzrinne
Dept. of Computer Science
Columbia University
1214 Amsterdam Avenue
New York, NY 10027
USA

EMail: schulzrinne@cs.columbia.edu

Gonzalo Camarillo
Ericsson
Advanced Signalling Research Lab.
FIN-02420 Jorvas
Finland

EMail: Gonzalo.Camarillo@ericsson.com

Alan Johnston
WorldCom
100 South 4th Street
St. Louis, MO 63102
USA

EMail: alan.johnston@wcom.com

Jon Peterson
NeuStar, Inc
1800 Sutter Street, Suite 570
Concord, CA 94520
USA

EMail: jon.peterson@neustar.com

Robert Sparks
dynamicsoft, Inc.
5100 Tennyson Parkway
Suite 1200
Plano, Texas 75024
USA

EMail: rsparks@dynamicsoft.com

Mark Handley
International Computer Science Institute
1947 Center St, Suite 600
Berkeley, CA 94704
USA

EMail: mjh@icir.org

Eve Schooler
AT&T Labs-Research
75 Willow Road
Menlo Park, CA 94025
USA

EMail: schooler@research.att.com

Full Copyright Statement

Copyright (C) The Internet Society (2002). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

T-Mobile Exhibit 1002
Part 5 of 6

Electronic Acknowledgement Receipt

EFS ID:	13077124
Application Number:	13056277
International Application Number:	
Confirmation Number:	2403
Title of Invention:	MOBILE GATEWAY
First Named Inventor/Applicant Name:	Johan Emil Viktor Bjorsell
Customer Number:	20995
Filer:	Raimond J Salenieks/Jessica Egigian
Filer Authorized By:	Raimond J Salenieks
Attorney Docket Number:	SMARB19.004APC
Receipt Date:	21-JUN-2012
Filing Date:	27-JAN-2011
Time Stamp:	19:09:19
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		SMARB19_004APC_IDS.pdf	95612 9c1cce83696a2f62ddfdabe5020ccfee1b8e024c	yes	2

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	1	
	Information Disclosure Statement (IDS) Form (SB08)		2	2	
Warnings:					
Information:					
2	Foreign Reference	EP_1389862_B1_Shen.pdf	600995 51f99faf0cb67daa8ca156b1766306fe4b90f066	no	9
Warnings:					
Information:					
3	Non Patent Literature	IPRP_PCTCA2008000545_09292009.pdf	191084 6367b5a9b63e6455efcf350e67e1102ed0bdbd96	no	6
Warnings:					
Information:					
4	Non Patent Literature	IPRP_PCTCA2009001317_03202012.pdf	199609 8016fc296c452d2bf6a5110264d714b7fcddb79a	no	5
Warnings:					
Information:					
5	Non Patent Literature	Townsley_RFC2661.pdf	2687119 73bea52a5c7379715b5d7662f3bf633b4be650a5	no	69
Warnings:					
Information:					
6	Non Patent Literature	IP2Location.pdf	186325 3e92bd32f5262d45afc4083142811fa49203eb8e	no	2
Warnings:					
Information:					
7	Non Patent Literature	DOTS_IP_Address_Validation.pdf	81650 c6c7eddd8aedc86d1e91287e3e7fc22c697c02ef	no	1
Warnings:					
Information:					
8	Non Patent Literature	List_of_North_American_Numbering_Plan_area_codes.pdf	3469194 53995f3a6fdcb3e411494494489e115f706c1299	no	45
Warnings:					
Information:					

9	Non Patent Literature	DOTS_Phone_Exchange.pdf	77864 aea0e6f8600b8e1f73ee20933b3b96166acd17d6	no	1
Warnings:					
Information:					
10	Non Patent Literature	Rosenburg_RFC3261.pdf	19972958 0bf0bed951959461ef343d77deeae1135ce8a131	no	232
Warnings:					
Information:					
			Total Files Size (in bytes):	27562410	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

INFORMATION DISCLOSURE STATEMENT

Applicant	:	Johan Emil Viktor Bjorsell, et al.
App. No.	:	13/056,277
Filed	:	January 27, 2011
For	:	MOBILE GATEWAY
Examiner	:	Kwang Bin Yao
Art Unit	:	2473
Conf. No.	:	2403

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

References and Listing

Submitted herewith in the above-identified application is an Information Disclosure Statement listing references for consideration. Copies of any listed foreign and non-patent literature references are being submitted.

Timing of Disclosure

This Information Disclosure Statement is being filed before the receipt of a first Office Action on the merits, and presumably no fee is required. If a first Office Action on the merits was mailed before the mailing date of this Statement, the Commissioner is authorized to charge the fee set forth in 37 CFR 1.17(p) to Deposit Account No. 11-1410.

Respectfully submitted,
KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 6-21-2012

By: _____

Raimond J. Salenieks
Registration No. 37,924
Agent of Record
Customer No. 20995
(858) 707-4000

13465339-sjw 061512

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/056,277
	Filing Date	January 27, 2011
	First Named Inventor	Johan Emil Viktor Bjorsell et al.
	Art Unit	2473
(Multiple sheets used when necessary)	Examiner	Kwang Bin Yao
SHEET 1 OF 1	Attorney Docket No.	SMARB19.004APC

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	1	8,116,307	2/14/2012	Thesayi et al.	
	2	2006/0093135 A1	5/4/2006	Fiatal et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T^1

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T^1

13685123-sjw 072612

Examiner Signature	Date Considered
***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

T^1 - Place a check mark in this area when an English language Translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	13411932
Application Number:	13056277
International Application Number:	
Confirmation Number:	2403
Title of Invention:	MOBILE GATEWAY
First Named Inventor/Applicant Name:	Johan Emil Viktor Bjorsell
Customer Number:	20995
Filer:	Raimond J Salenieks/Lori Larson
Filer Authorized By:	Raimond J Salenieks
Attorney Docket Number:	SMARB19.004APC
Receipt Date:	03-AUG-2012
Filing Date:	27-JAN-2011
Time Stamp:	15:13:58
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		SMARB19_004APC_IDS.pdf	75936 678cf7e187aa2966916b765e70871e93fe3a2a5a	yes	2

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	1
	Information Disclosure Statement (IDS) Form (SB08)	2	2
Warnings:			
Information:			
	Total Files Size (in bytes):	75936	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

INFORMATION DISCLOSURE STATEMENT

Applicant	:	Johan Emil Viktor Bjorsell et al.
App. No.	:	13/056,277
Filed	:	January 27, 2011
For	:	MOBILE GATEWAY
Examiner	:	Kwang Bin Yao
Art Unit	:	2473
Conf. No.	:	2403

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

References and Listing

Submitted herewith in the above-identified application is an Information Disclosure Statement listing references for consideration. Copies of any listed foreign and non-patent literature references are being submitted.

Timing of Disclosure

This Information Disclosure Statement is being filed before the receipt of a first Office Action on the merits, and presumably no fee is required. If a first Office Action on the merits was mailed before the mailing date of this Statement, the Commissioner is authorized to charge the fee set forth in 37 CFR 1.17(p) to Deposit Account No. 11-1410.

Respectfully submitted,
KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: August 3, 2012 By: Raimond Salenieks

Raimond J. Salenieks
Registration No. 37,924
Agent of Record
Customer No. 20995
(858) 707-4000

13685143-sjw 072612

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/056,277
	Filing Date	January 27, 2011
	First Named Inventor	Johan Emil Viktor Bjorsell et al.
	Art Unit	2473
(Multiple sheets used when necessary)	Examiner	Kwang Bin Yao
SHEET 1 OF 1	Attorney Docket No.	SMARB19.004APC

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	1	6,151,385	11/21/2000	Reich et al.	
	2	6,597,686	7/22/2003	Darek A Smyk	
	3	6,724,860	4/20/2004	Stumer et al.	
	4	6,744,858	6/1/2004	Ryan et al.	
	5	6,963,557	11/8/2005	Mark Clinton Knox	
	6	7,046,658	5/16/2006	Vinay Kundaje	
	7	2005/025043 A1	2/3/2005	Mussman et al	
	8	2006/0153342 A1	7/13/2006	Syouichi Sasaki	
	9	2006/0258328 A1	11/16/2006	Mario Francisco Godoy	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T[1]

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[1]
	10	Lind AT&T S: "ENUM Call Flows for VoIP Interworking; draft-lind-enum-callflows-03.txt", 20020201, no. 3, 1 February 2002, pages 1-17.	
	11	IETF ENUM WG R STASTNY OEFEG INFORMATIONAL NUMBERING FOR VOIP AND OTHER IP COMMUNICATIONS: "Numbering for VoIP and other IP Communications, draft-stastny-enum-numbering-voip-00.txt", 20031001, 1 October 2003, pages 1-43.	

13893588-sjw 083112

Examiner Signature	Date Considered
***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

T[1] - Place a check mark in this area when an English language Translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	13677023
Application Number:	13056277
International Application Number:	
Confirmation Number:	2403
Title of Invention:	MOBILE GATEWAY
First Named Inventor/Applicant Name:	Johan Emil Viktor Bjorsell
Customer Number:	20995
Filer:	Raimond J Salenieks/ThuyQuyen Nguyen
Filer Authorized By:	Raimond J Salenieks
Attorney Docket Number:	SMARB19.004APC
Receipt Date:	06-SEP-2012
Filing Date:	27-JAN-2011
Time Stamp:	18:24:34
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	ENUM_Call_Flows_for_VOIP_Interworking.pdf	655943 2e107052eda6dc6e2c59d87b242a6eadc16523b7	no	18

Warnings:

Information:

2	Non Patent Literature	Numbering_for_VOIP.pdf	1961611 696280310d5968b5c122b757a200e820b3aba73a	no	44
Warnings:					
Information:					
3		SMARB19_004APC_IDS2.pdf	77386 213cc1ec24b72cd1408ec6ead816edb6cc97f922	yes	2

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	1
	Information Disclosure Statement (IDS) Form (SB08)	2	2

Warnings:	
Information:	
Total Files Size (in bytes):	2694940

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

S. Lind
Internet Draft
Document: draft-lind-enum-callflows-03.txt
Category: Informational
AT&T
February 2002

ENUM Call Flows for VoIP Interworking

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026 [1].

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or made obsolete by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ôwork in progress.ó

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

1. Abstract

This document provides illustrations of the use of ENUM [2] functionality within the larger context of service-level call flows for Voice over IP communication where interworking between the PSTN and IP-based networks are necessary to complete a call. Details are presented for simple calls made on a ôdirect dialö basis. Some details are also provided for calls made using the ITU-defined "Global Services" [3,4,5]. The impact of number portability within the call scenarios is discussed. The objective of this document is to identify areas where gaps exist in the provision of services and suggest where protocol extensions for ENUM, SIP, TRIP, etc. are needed.

The document does not propose that the examples represent the only or best approach for interworking between the PSTN and IP-based networks.

2. Conventions used in this document

The key words ôMUSTö, ôMUST NOTö, ôREQUIREDö, ôSHALLö, ôSHALL NOTó, ôSHOULDò, ôSHOULD NOTö, ôRECOMMENDEDö, óMAYò, and ôOPTIONALö in this document are to be interpreted as described in RFC-2119 [6].

T-Mobile Exhibit 1002
Part 5 of 6

2.1 Definitions

ITSP - Internet Telephony Service Provider. An entity that provides (originates and completes) voice telephony service using IP technology.

3. Scope of Work

It is envisaged that this document could be used by the ITU to cull the various service requirements out of the examples presented and to use those requirements as the main part of a new draft Recommendation (preliminarily called ôE.callflowsö). An example of such a requirement would be that the ENUM-enabled client should take the local dialing plan into account.

It is also envisaged that this document could be used by various working groups within the IETF to identify areas where protocol enhancements need to be developed. Some of these areas are pointed out within this document. Other areas may become apparent after further service requirements are identified by the ITU.

Some of this work may already be in progress within the IETF and close co-operation between the ITU and the IETF will speed this process of discovering existing work and initiating new work. Some areas that need exploration include the ability to obtain and transport number portability information within the call process (e.g., SIP messages), the ability for the TRIP protocol to address global service codes and network-specific numbers, and the need to interface with IN databases to ensure that interworking is fully functional.

4. Background

ENUM provides the capability to translate an E.164 Telephone Number into a set of URIs using the Domain Name System (DNS). This capability has different uses depending on the applications being used and, in the case of voice services, the technology available at the source and destination of the communication.

In a pure IP environment, ENUM will allow end users to be identified by a commonly used name (i.e., their telephone number) for a variety of applications. The potential for this capability simplifies the requirements spelled out in ITU-T Recommendation E.123, ôNotation for National and International Telephone Numbers, E-Mail Addresses and Web Addressesö. It also implies that end users can change IP service providers without having to change their destination identification. For example, an end user can change their underlying e-mail address from ôjohn@abc.comö to ôjohn@xyz.comö but, with ENUM set up to handle e-mail using the ôE2Uö records specified in RFC 2916, still be reached by having ENUM-enabled mail clients send mail

T-Mobile Exhibit 1002
Part 5 of 6

addressed to their ôtelephone numberö (e.g., mailto:+1-973-236-6787).

For voice services, ENUM will allow the easy end user identification described above as well as interworking between terminals on the PSTN and on the IP-based network. It may also allow for the implementation of more advanced services, such as ôfind-me.o For voice communication starting on an IP-based network, ENUM can be used on each call to determine the preferred type of destination based on the priority of the network termination available. For voice communication starting on the PSTN, ENUM is more likely to be used where at least one of the destinations of the call exists on an IP-based network.

Termination / Origination	IP-based Network Only	Both	PSTN Only
IP-based Network	ENUM used for address translation and, to some extent, service priority	ENUM used to determine destination (based on service priority) and address translation	ENUM used to determine address translation
PSTN	ENUM used for address translation	ENUM may be used	ENUM may or may not be used

Table 1 - Use of ENUM resources

5. Simple Voice Service Interworking

5.1 Call from the PSTN to a Terminal on an IP-based Network

This scenario is illustrated in figure 1. A customer on the PSTN wishes to reach another customer whose terminal (ôphoneö) is connected to an IP-based network. In the illustration, the destination terminal is a SIP client, but other client protocols may be equally applicable. The various steps are denoted in parentheses within the figure and explained below. No aspects of number portability are included in the scenario.

T-Mobile Exhibit 1002
Part 5 of 6

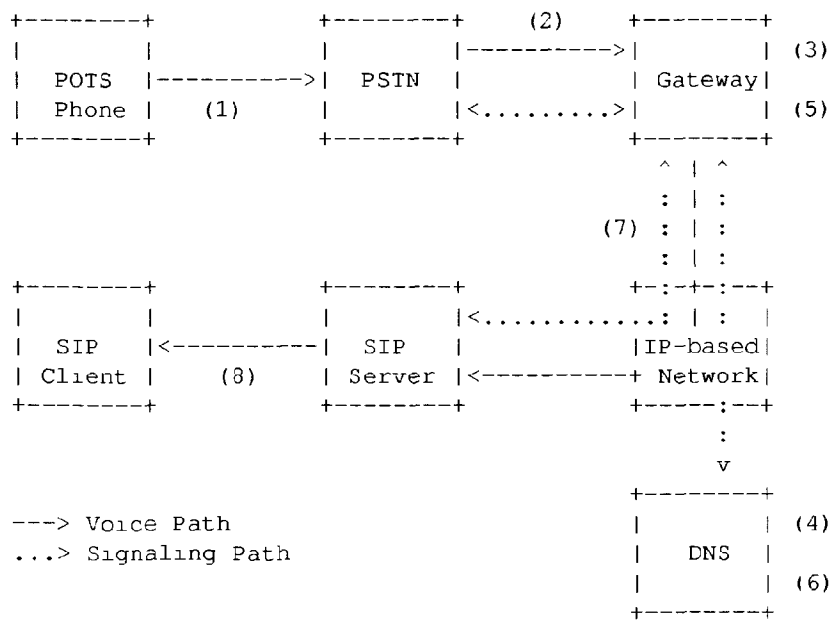


Figure 1
Call From PSTN to IP-based Network

Step 1 - The originating customer dials an E.164 number. The actual digits dialed depend on the dialing plan in effect at the point of origination. The customer may dial a local number (or intra-NPA within the US), an intercity number (or inter-NPA within the US), or international number. Any dialing prefixes required by the dialing plan must be entered.

As an example, John Smith, whose phone number in the US is 301-555-1234, wants to call Jenny Jones. The number that John Smith has for Jenny, also in the US, is 301-236-6787. John dials ô236-6787ö [the hyphens are provided for readability and are not dialed]. It is worth noting that any dialed prefixes are usually dropped at the first switching point within the PSTN.

As a second example, John Smith wants to call Franz Himmel in Switzerland. FranzÆs local number is 022-730-5887. John Smith would dial ô011-41-22-730-5887o (011 being the dialing prefix for international calls placed from the United States and 41 being the country code for Switzerland).

Step 2 - The PSTN Service Provider forwards the call to the appropriate Gateway. Selection of the appropriate Gateway may depend on a number of different factors, including regulatory factors in effect at the point of call origination. The physical location of the Gateway in relation to the point of origination may also depend on several factors including the relationships between the PSTN Service Provider and the Internet Telephony Service Provider (ITSP) at the point of termination.

T-Mobile Exhibit 1002
Part 5 of 6

Within the first example, John SmithÆs local service provider determines that the call is local, but not served by this provider. The originating provider forwards it to JennyÆs ITSP as the terminating local service provider.

In the second example, the international carrier is handed the call. The call could be routed to an international switching center where the call is handed to another international carrier (where a gateway might be selected) or, if it can be determined that the destination is on an IP-based network, the gateway can be selected earlier in the call flow.

Step 3 - The Gateway looks up the domain name in DNS. The Gateway at which the call enters the IP-based network must contain any ENUM functionality to transform the dialed digits to a fully qualified domain name (FQDN). The gateway must supply any missing digits in order to obtain a fully qualified E.164 number as part of the transformation.

In the first example, the gateway transforms the dialed number into a FQDN of ô7.8.7.6.6.3.2.1.0.3.1.e164.arpaö. During the transformation, the country and area codes for the destination are added to the number by the gateway. In the second example, the gateway transforms the dialed number into a FQDN of ô7.8.8.5.0.3.7.2.2.1.4.e164.arpaö. In this second example, the country code is already present in the dialed digit stream.

Step 4 - The DNS returns any service records associated with the URL.

In the first example, the DNS returns among the records one containing the URI ôsip:jennyjones@sipservice.fooö. In the second example, the DNS returns a record containing the URI ôsip:franz.himmel@sipserver.bar.chö.

Step 5 - The Gateway looks up the address (A) record for the specified host (e.g., ôsipservice.fooö) in DNS.

Step 6 - DNS returns the IP address of the SIP server for the specified host.

Step 7 - The call is routed through the IP-based network to the designated IP address.

Step 8 - The SIP Server routes the call to the user agent client of the specified user (e.g., ôjennyjonesö). When the destination party answers, answer supervision must be returned to the originating local switch.

A protocol diagram of this call flow is contained in Appendix 1.

T-Mobile Exhibit 1002
Part 5 of 6

5.2 Options In Identifying the Gateway

The most significant problem in the above scenario is the determination of when the call must be routed to the IP-based network via the gateway. The easiest way to solve the problem would be to use different E.164 numbers for terminals on the IP-based network. However, this solution may not be feasible in certain regulatory environments where the available numbering resources are scarce.

Another way to solve the problem is to route all calls to a gateway to transport the calls over an IP-based network, completing those calls to IP terminals where possible and allowing the remaining calls to egress back to the PSTN close to their destination. In the latter case, it may be useful, but not mandatory, to have ôtel:ö records to facilitate the routing to the destination gateway.

There may be other solutions that lie between the previously described methods. Those possible solutions are outside the scope of this paper, but development work would be needed to implement such capabilities.

5.3 Call from a Terminal on an IP-based Network to a phone on the PSTN

This scenario is illustrated in figure 2. A customer on an IP-based network wishes to reach another customer whose phone is connected to the PSTN. In the illustration, the originating terminal is a SIP client, but other client protocols may be equally applicable. No aspects of number portability are included in this scenario. The various steps are denoted in parentheses within the figure and explained below.

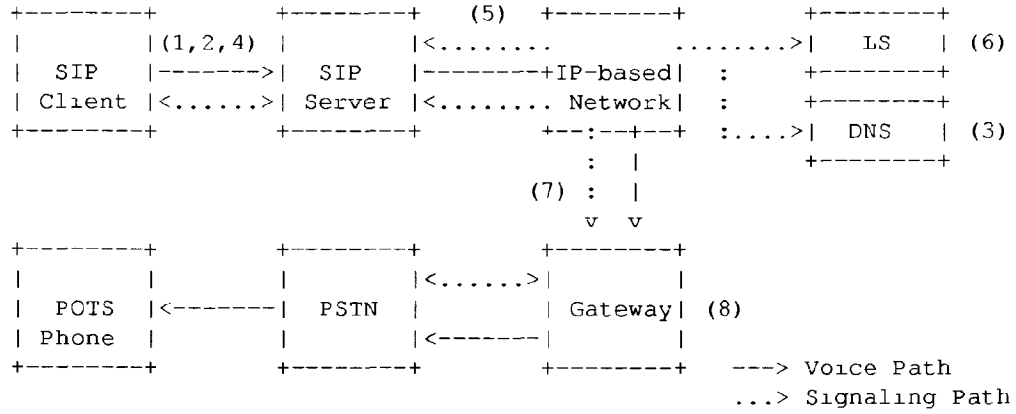


Figure 2
Call from IP-based Network to PSTN

Step 1 - The originating customer dials an E.164 number. The actual digits dialed depend on the dialing plan in effect at the point of

T-Mobile Exhibit 1002
Part 5 of 6

origination. The customer may dial a local number (or intra-NPA within the US), an intercity number (or inter-NPA within the US), or international number. Any dialing prefixes required by the dialing plan must be entered.

As an example, Jenny Jones, who has a SIP client and whose ôphone numberö (the same number as assigned by her TSP) in the US is 301-236-6787, wants to call John Smith. The number that Jenny has for John, also in the US is 301-555-1234. Jenny dials ô555-1234ö.

Step 2 - The SIP Client looks up the name in DNS. The SIP Client must contain any ENUM functionality to transform the dialed digits to an Fully Qualified Domain Name (FQDN). The SIP Client must supply any missing digits in order to obtain a fully qualified E.164 number as part of the transformation.

In the example, the SIP Client transforms the dialed number into a FQDN of ô4.3.2.1.5.5.5.1.0.3.1.e164.arpaö. During the transformation, the country and area codes for the destination are added to the number by the client.

Step 3 - The DNS returns any NAPTR service records associated with the FQDN.

In the example, the DNS returns at least one record containing the URI ôtel:+13015551234ö.

If no ENUM record exists for the URL, the call should be attempted for termination on the PSTN using the dialed digits as the target for further steps in the call flow.

Step 4 - The SIP Client initiates a SIP INVITE to the SIP Server using the ôtel:ö URI.

Step 5 - The SIP Server may query a location server (LS) if the point of origination and the point of termination on the IP-based network are in different ITAD, using one of the Front End Protocols suggested within the TRIP framework [7] and maintained by the userÆs ITSP, for the IP address of a Gateway for this telephone number. As input to the query, the server will supply the telephone number from the ôtel:ö URI or the local routing number (LRN) if one was obtained when and if a local number portability (LNP) query was done (see section 7.2 for the discussion of LNP).

Step 6 - The LS returns the IP address of the appropriate Gateway for the destination number.

Step 7 - The SIP Server routes the call to the designated Gateway IP address.

Step 8 - The Gateway completes the call through the PSTN to the destination phone. It must respond to any signaling (e.g., ringing,

T-Mobile Exhibit 1002
Part 5 of 6

busy) from the PSTN and send the appropriate information back to the call originator.

A protocol diagram of this call flow is contained in Appendix 2. It should be noted that this protocol diagram also contains some of the number portability functionality not covered above.

6. Calls to E.164 Numbers using Non-Geographic Numbering Plans (Global Service Codes)

In general, all Global Services, including International Freephone, International Premium Rate, and International Shared Cost, should process in a similar manner. The first step in handling a Global Service call is to determine, based on the number dialed, who the appropriate service provider is that can process and complete the call. In the case of PSTN-originated calls, that process is in place today and should not be impacted by interworking with IP-based networks. If the designated Global Service provider is an ITSP, then the originating PSTN access provider should route the call to the appropriate Gateway. The Global Service provider would then be responsible for any necessary call processing and final number translation using IN-based (i.e., SS7 signaling to an SCP), IP-based (e.g., ENUM and/or other infrastructure used by the ITSP), or a combination of facilities, as the service provider sees fit.

For IP-originated calls, the same general principle holds true. Using the DNS, a query for the Global Service number as a FQDN should return information that would allow the call to be routed to a proxy, redirect, or other server operated by the Global Service provider, which would then provide any call processing and termination required by the Global Service customer. Again, the service provider would be able to choose whether that processing used IN-based, IP-based or a combination of facilities. Once the necessary call processing was completed, the server could then redirect or forward the call to the appropriate point of termination.

Figure 3 illustrates some of the steps necessary to provide such services originating from an IP-based terminal. This example is just one possible way of completing a global service call using ENUM. Other possibilities exist and need to be explored in conjunction with the Services Question (i.e., Q.3/2) in ITU-T Study Group 2

Step 1 - The originating customer dials an E.164 number. In the case of a global service, the end user dials the international access code for their country of origination (e.g., "011" in North America, "00" in other locations) and the destination number.

As an example, Jenny Jones, who has a SIP client and whose ôphone numberó (the same number as assigned by her TSP) in the US is 301-236-6787, wants to call the XYZ Company. The number that Jenny has

T-Mobile Exhibit 1002
Part 5 of 6

for the XYZ Company is +800 123 456 7890. Jenny dials "011 800 123 456 7890".

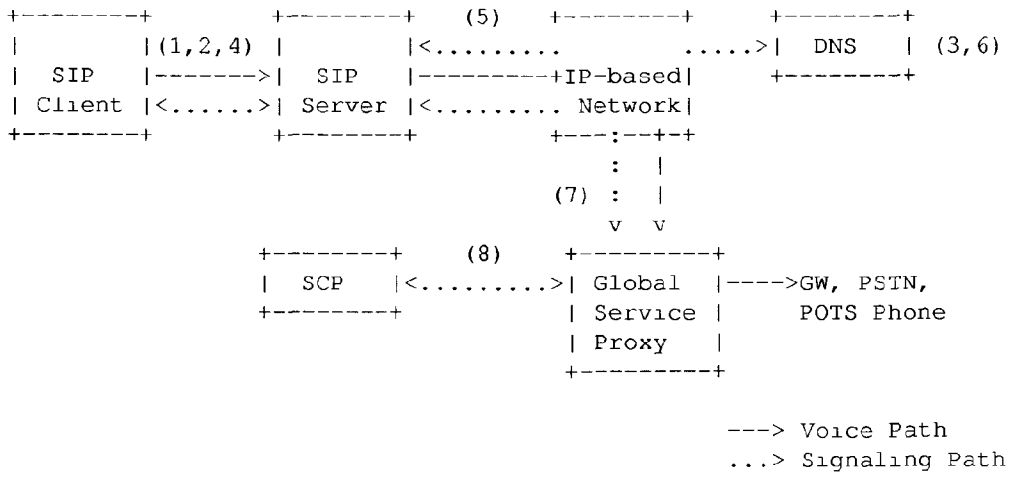


Figure 3
Global Service Call from IP-based Network to PSTN

Step 2 - The SIP Client looks up the name in DNS. The SIP Client must contain any ENUM functionality to transform the dialed digits to an Fully Qualified Domain Name (FQDN).

In the example, the SIP Client transforms the dialed number into a FQDN of "0.9.8.7.6.5.4.3.2.1.0.0.8.e164.arpa".

Step 3 - The DNS returns any NAPTR service records associated with the FQDN.

In the example, the DNS returns at least one record containing the URI "sip:8001234567890@provider.host.foo".

Step 4 - The SIP Client initiates a SIP INVITE to the SIP Server using the "sip:" URI.

Step 5 - The SIP Server looks up the address (A) record for the specified host (e.g., "provider.host.foo") in DNS.

Step 6 - DNS returns the IP address of a Global Service Proxy server for the specified host.

Step 7 - The call is routed through the IP-based network to the designated IP address.

Step 8 - The Global Service Proxy server uses the user name (i.e., "8001234567890") as well as interacting with the originating SIP client or server to collect any necessary information (e.g., time of day, place of origin) to process the call. The Global Service Proxy may have to interact with some data store of service information to

T-Mobile Exhibit 1002
Part 5 of 6

know how to route the call. In the illustration, the data store is a Signaling Control Point (SCP) located in the signaling path of the PSTN.

The data store may return various pieces of routing information including an International Routing Address (INRA) and a Serving Service Provider Identity. This information can then be used by the Global Service Proxy to complete the call via a gateway to the appropriate destination on the PSTN. ITU-T Question 2/2 is working on the provision of routing information for calls on an IP-based network [8].

A protocol diagram of this call flow is contained in Appendix 3.

7. Issues Surrounding Calls to Ported Numbers

Portability issues exist whether or not ENUM is used during the call processing. There are three types of number portability: service provider portability, geographic portability, and service portability. This document will only deal with service provider portability as it is the one type that is most likely to be implemented.

For service provider portability [9], three scenarios need to be examined that may impact processing of calls that go between the PSTN and an IP-based network. The first is that a customer may switch between two different PSTN service providers. As an example in the US, a customer might switch between an ôincumbent local service providero and a ôcompetitive local service providero or vice versa. The second scenario is that a customer may switch between a service provider on the PSTN to an ITSP (or vice versa). The third scenario is that a customer may switch between two different ITSPs.

Other examples need to be developed that represent the number portability requirements and implementations in other countries.

7.1 Calls originating on the PSTN

Calls under the first scenario should be handled already in todayÆs PSTN environment. For the second scenario, there are issues about what gets populated in the LNP database on the PSTN side of the interface to route the call to a Gateway as described in section 5.1 above. In the US, where Location Routing Numbers (LRNs) is mandated by regulation [10], it might be necessary for Gateways of the ITSP at the destination end to be identified by a LRN.

For scenario 3, assuming the call reaches a Gateway, the change should be reflected in a different URI for the destination subscriber in the first DNS lookup. In our example in section 5.1, step 4, the DNS might contain a different record now containing the URI osip:jennyjones@newsipservice.fooo. The Gateway would then

T-Mobile Exhibit 1002
Part 5 of 6

resolve the URI in a different DNS to obtain the correct IP address for the new SIP server.

7.2 Calls originating on an IP-based network

It appears that, under scenario 1, the primary impact would be that a different gateway for a given number might be used or the gateway would need to determine that the terminating PSTN service provider has changed. The DNS might need to contain the LRN for the new termination point. The LS would have to be responsive to point to the new Gateway, if appropriate, for that destination number. The SIP Server or the Gateway, if the LRN was not available from the DNS, may have to perform additional LNP queries on an IN-basis. If such queries are not performed at or somewhere upstream from the Gateway, the call may be routed to the wrong service provider or the ITSP may be charged for the necessary LNP queries performed on its behalf by the PSTN. It is important that the LRN be carried forward from the point at which it is obtained in order for the PSTN to know that a portability query has been done.

Under scenario 2, it would appear that the change would occur within the DNS in that instead of returning a ôtel:ö-based URI, the DNS might now return a URI pointing to a SIP or H.323 terminal. Under scenario 3, the call would not terminate on the PSTN and the DNS would simply point to a different URI similar to the change described in section 7.1 for scenario 3.

Lastly, for whatever solutions may be chosen and developed, the solutions must meet any operational and performance requirements mandated by regulation.

7.3 Further Work on Number Portability

ITU-T Question 3/2 is working on a draft new Supplement to Recommendation E.370 [11]. This text should reflect information on the impacts of interworking between the PSTN and an IP-based Network when E.164 numbers are ported. The text should be shared with the IETF as it becomes more stable.

8. Conclusions and Further Work

Use of ENUM functionality is fairly straightforward for simple call flows. Unfortunately, the reality of todayÆs telecommunication environment is that calling is far from simple. The issues identified within this document include:

ò Identification of the need to route a call from the PSTN to a gateway at the edge of an IP-based network (this work, if necessary, would be on the PSTN),

T-Mobile Exhibit 1002
Part 5 of 6

- Source of local number portability information for queries (probably as an extension to the SIP protocol) from IP-based infrastructure, and

- mechanisms for transport of LNP information to the final switching destination, (see draft-yu-tel-url-01.txt for one such example of a proposed SIP extension).

While some of these issues may be outside the scope of ENUM, they nevertheless have to be addressed if IP-based communication will be viable. Between the IETF and the ITU, core competencies exist to address these issues; continued cooperation will be beneficial.

9. References

1 Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

2 Falstrom, P., "E.164 number and DNS", RFC 2916, September, 2000

3 ITU-T Recommendation E.152, International Freephone Service, February 2001

4 ITU-T Recommendation E.154, International Shared Cost Service, March 1998

5 ITU-T Recommendation E.155, International Premium Rate Service, March 1998

6 Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

7 Rosenberg, J. and Schulzrinne, H., "A Framework for Telephone Routing over IP", RFC 2871, June 2000

8 ITU I draft new Recommendation E.INRA.IP, Interworking of Routing Addresses and IP-Nmaes/Addresses

9 ITU-T Recommendation E.164, The international public telecommunication numbering plan - Supplement 2: Number Portability, November 1998 (see also draft-ietf-enum-e164s2-np-00.txt)

10 Second Report and Order In the Matter of Telephone Number Portability (FCC Docket No. 95-116), FCC 97-289, Adopted August 14, 1997 (see http://www.fcc.gov/Bureaus/Common_Carrier/Orders/1997/fcc97289.txt)

T-Mobile Exhibit 1002
Part 5 of 6

11 ITU-T COM 2-R 80, "Recommendations requiring further development, WP 1/2", March 2000

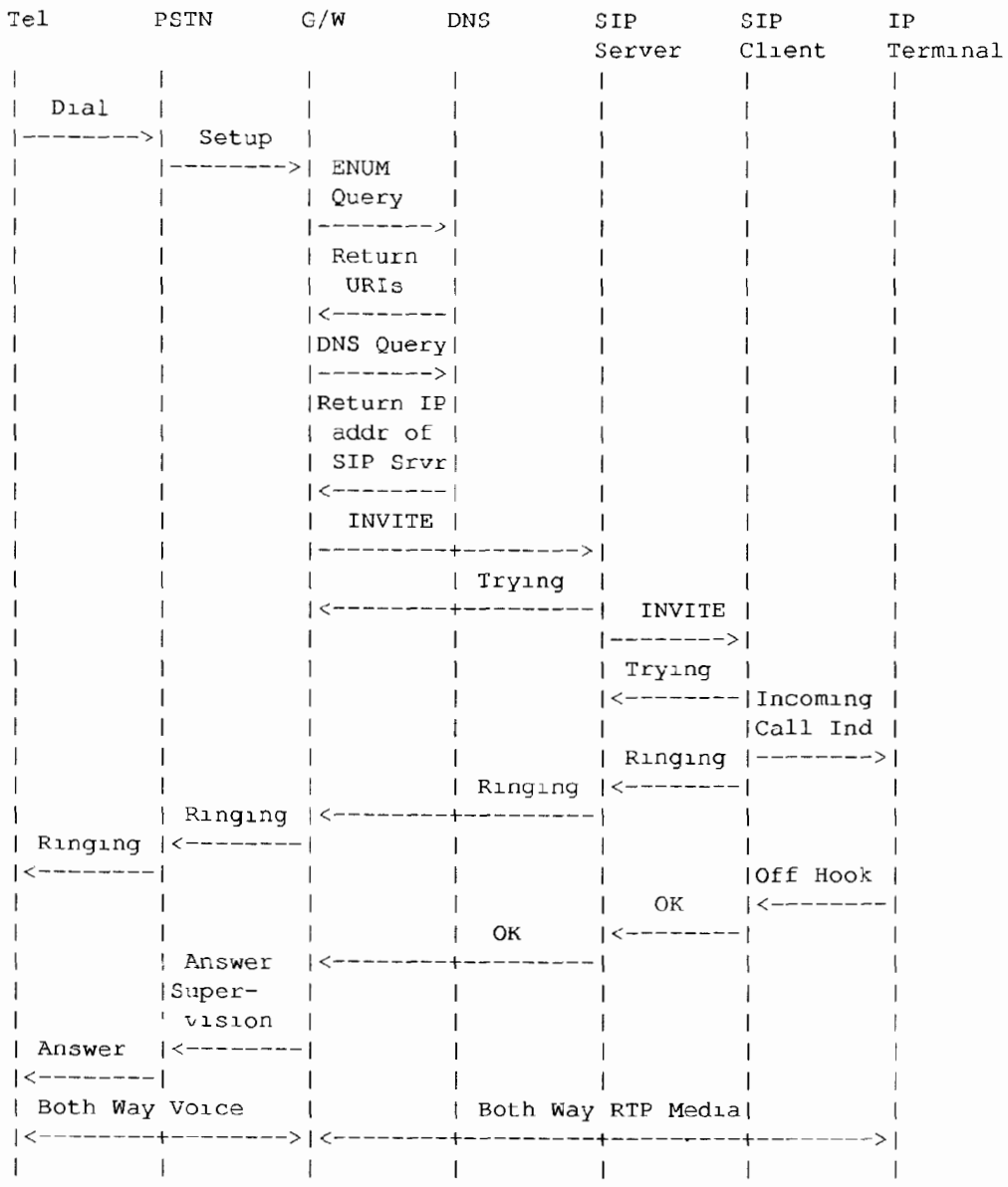
10. AuthorÆs Addresses

Steven D. Lind
AT&T
Bldg. 2, Room 2G25
180 Park Avenue
Florham Park, NJ 07932
U.S.A.

Phone: +1 973 236 6787
Email: sdlind@att.com

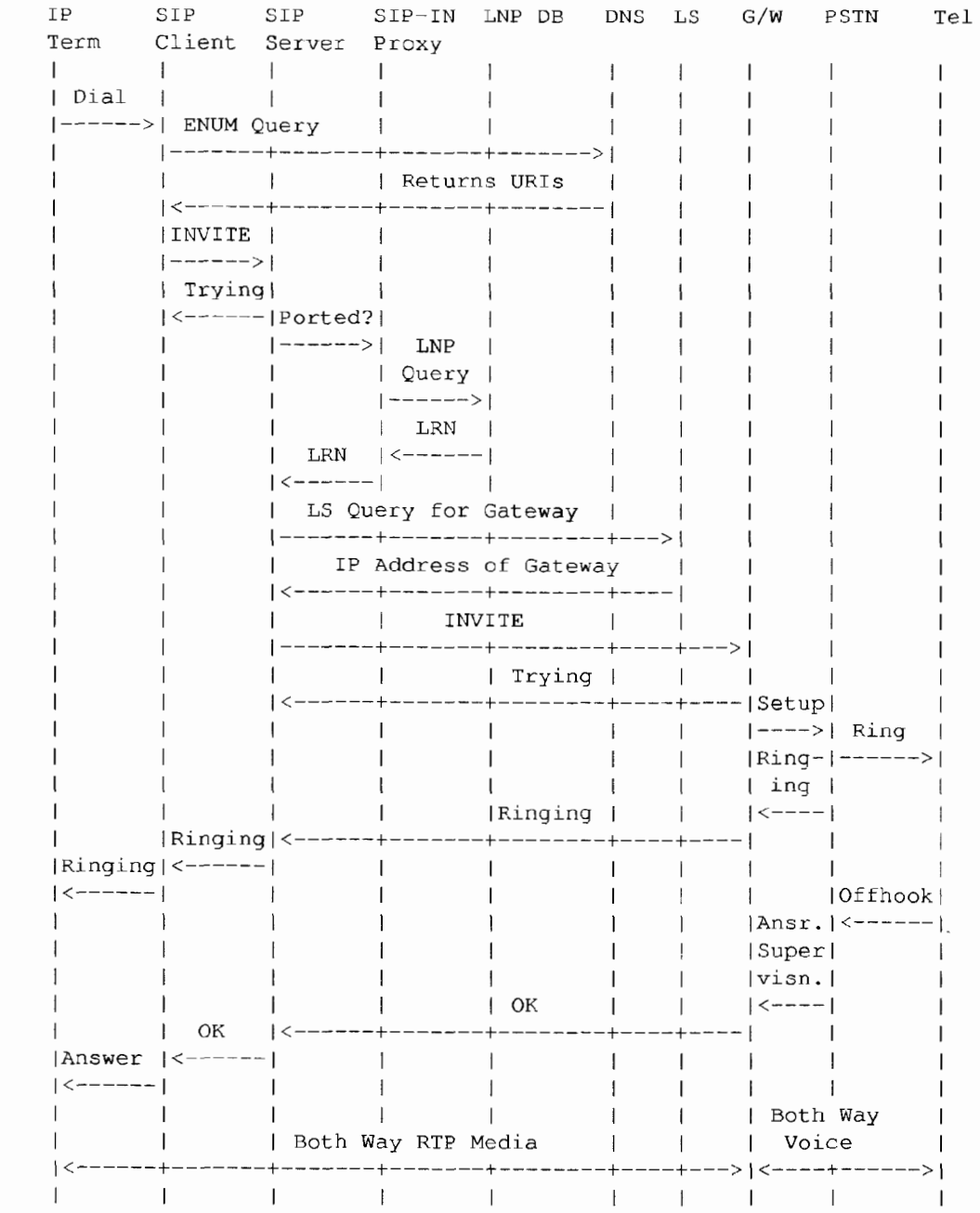
T-Mobile Exhibit 1002
Part 5 of 6

Appendix 1 û Protocol Diagram of the PSTN-to-IP Call Flow

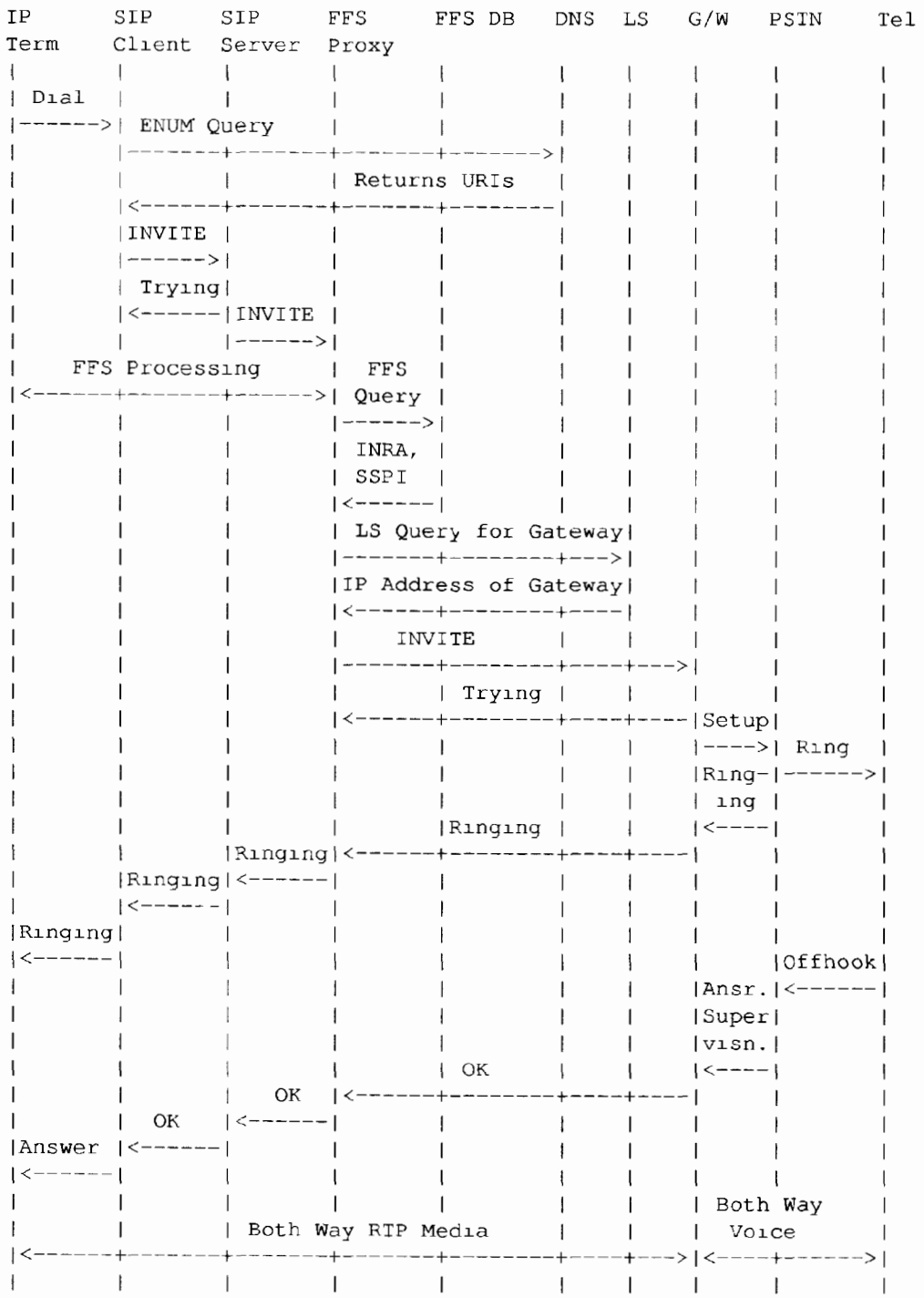


T-Mobile Exhibit 1002
Part 5 of 6

Appendix 2 û Protocol Diagram of the IP-to-PSTN Call Flow



Appendix 3 û Protocol Diagram of the IP-to-PSTN Freephone Service Call Flow



Full Copyright Statement

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an ôAS ISö basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Generated by unregistered txt2pdf PRO v.6.7 © SANFACE Software 2003
Available at http://www.sanface.com/txt2pdf.html

IETF ENUM WG
Internet Draft — R Stastny
Document: — OeFEG
draft-stastny-enum-numbering-voip-00.txt
Expires: April 2004 — October 2003
Informational

Numbering for VoIP and other IP Communications

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026 [1].

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt
The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html.

Abstract

This document gives advice in setting up E.164 compatible numbering and dialing plans in administrative domains set up for IP Communications in general and VoIP applications in detail. After explaining numbering and dialing plans in principle, it discusses which types of E.164 numbers should be used for IP based terminals, to achieve proper routing of calls and other communications on the PSTN/ISDN and also on the Internet, using ENUM technology.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [2].

Table of Contents

1. Introduction and Overview.....2
2. The Problem.....4
2.1 IP Communications as Applications on the Internet.....4
2.2 How to reach VoIP users from the PSTN/ISDN.....4
2.3 The Global Public Telephony Service.....5
2.4 ENUM.....5
2.5 Why using E.164 numbers natively on the Internet?.....7
3. Numbering and Dialing plans.....8
3.1 Numbering Plans.....8
3.2 Types of Numbering Plans.....9
3.3 Dialing Plans.....12
4. Types of numbers in existing numbering plans.....16
4.1 International Public Telecommunication Numbers (E.164 Numbers) 16
4.2 National E.164 Numbers.....18
4.3 Partial Numbers.....23
4.4 Calling line identification (CLI).....25
5. E.164 Numbers for VoIP.....26
5.1 E.164 Numbers for VoIP-only.....26
5.2 Potential E.164 Number types for VoIP-only.....27
6. How to set up numbering and dialing plans for VoIP domains....28
6.1 Basic Requirements.....28
6.2 Which E.164 Numbers to use for mapping of partial numbers?30
6.3 Dialing Plans for administrative domains.....31
6.4 Numbering Plans for administrative domains.....34
7. Routing of calls to E.164 numbers terminating on VoIP.....36
7.1 Routing on the PSTN.....37
7.2 ENUM Support for Routing of E.164 numbers on the Internet.39
7.3 Routing from Gateways and between domains with ENUM.....39
8. Security Considerations.....42
Author's Addresses.....43

1. Introduction and Overview

Currently a number of Administrative Domains for IP communications are implemented allowing users to register IP phones or soft clients and place VoIP calls or establish other types of IP communications via broadband connections to other users registered in the same or in other administrative domains by using Internet Naming and Addressing schemes.

As a courtesy to users having only IP phones with numeric keypads or terminal adaptors for steam phones, numeric aliases are used exclusively or in addition. This allows users placing calls using dialing strings. For "cross trunks" or "cross connections" to other

T-Mobile Exhibit 1002
Part 5 of 6

administrative domains and to the PSTN/ISDN different combinations of access codes are implemented in an ad-hoc uncoordinated manner.

The advantage of this approach is that registered users may be reached also from the PSTN/ISDN and other administrative domains if a proper mapping of E.164 numbers to these numeric aliases as partial numbers is achieved.

This situation is similar to the mess existing in the PSTN with automatic trunk dialing in the '50s of the last century and with international automatic dialing in the '60s, before the International Public Telecommunication Numbering Plan (E.164 numbers) [3] was introduced by ITU-T (CCITT). Traces of this messy situation can still be recognized in the existing national dialing and numbering plans. To prevent this from happening again on the Internet, the purpose of this document is to give guidance to the definition of numbering and dialing plans and the provision E.164 numbers in IP û based administrative domains.

After stating the problem, the terminology used is defined, especially the definitions of numbering and dialing plans are given and their differences are explained.

The types of number ranges used in existing numbering plans are explained and a new grouping of the type of number ranges is proposed:

- Pure geographic numbers
- Non-geographic numbers for private networks
- Non-geographic numbers for networks and personal numbers (including mobile networks and personal services using VoIP networks)
- Non-geographic numbers for tariff related services

The types of number ranges usable for VoIP and IP Communications are analyzed and discussed. In principle any number range could be used for VoIP, but for the direct mapping of administrative domains using partial numbers the usage of national geographic numbers, national non-geographic numbers for private and mobile networks and global numbers for networks is recommended.

The document explains the routing of calls to these number ranges on the PSTN/ISDN to the appropriate VoIP gateways. It is also proposed to use ENUM for routing of calls on the Internet from the VoIP gateways used or from other administrative domains to the E.164 numbers hosted by these administrative domains.

To map administrative domains with partial numbers to E.164 numbers it is necessary to set up the administrative domains with numeric

T-Mobile Exhibit 1002
Part 5 of 6

userinfo (aliases). It is therefore required to set up numbering and dialing plans within these administrative domains.

These numbering and dialing plans should allow to access the own users, users in other administrative domains and users on the PSTN/ISDN in a consistent manner and also allow the mapping of this numbering plan to the International Public Telecommunication Numbering Plan E.164 as partial numbers.

The basic requirements and rules to achieve this are proposed in this document.

2. The Problem

2.1 IP Communications as Applications on the Internet

IP Communications (VoIP, IP Telephony, Internet Telephony, Voice over the Net, Instant Messaging, Presence, Video, etc.) are applications based on the Internet (IP) protocols, and are therefore like any other applications on the Internet basically using the IP addressing scheme.

For various reasons the direct usage of the IP addressing scheme has many drawbacks, most applications on the Internet use in addition a more user-friendly and comfortable naming scheme. This naming scheme is based on the Domain Name System (DNS) and Universal Resource Locators and Identifiers (URLs, URIs). The usage of a naming scheme has also an important advantage. IP addresses may dynamically change and are also related to a network endpoint (device). Since a user may attach to different and multiple devices, the usage of a naming scheme is adding one level of indirection and therefore allows addressing the user independently of the device currently used.

For VoIP, the most commonly used URLs and URIs are sip:, h323: and tel:. These URIs are called contact addresses, if used for a specific device, or Address-of-Records, if used to address a user or a generic service via a location service (see RFC3261). Address-of-records allow VoIP users to reach each other on the Internet and also to reach users on the PSTN/ISDN, if a proper gateway is provided. This can e.g. be done with the tel: URI, which contains a phone number (see RFC2806bis [4]).

2.2 How to reach VoIP users from the PSTN/ISDN

On the other hand it is in most cases not possible for users on the PSTN/ISDN to reach users on the Internet, because URIs cannot be entered on most telephone devices and also the signaling systems are not able to deal with URIs. The PSTN/ISDN is using "phone numbers",

mainly the numbering scheme defined in ITU-T Rec. E.164 or compatible national variants. These phone numbers are called International Public Telecommunication Numbers, or E.164 numbers.

It is therefore necessary to provide a translation service between the naming and addressing (numbering) scheme used on the PSTN/ISDN and the naming scheme used on the Internet. This can be done in different ways; one of these translation services is ENUM (see RFC2916bis [5]).

2.3 The Global Public Telephony Service

This implies that an E.164 number is attached in addition to the existing Address-of-Record of a VoIP user. If a user on the PSTN/ISDN is now dialing such an E.164 number the call needs to be routed to a VoIP-gateway located on the boundary between the PSTN/ISDN and the Internet.

The VoIP-gateway is translating the E.164 Number to the Address-of-Record (e.g. a sip: URI) assigned to the user. The call is then routed on the Internet to the VoIP user, or more precisely to the VoIP server pointed to by the host part of the Address-of-Record. This implies also that the VoIP application is part of the global public telephony service as defined in ITU-T Rec. E.105 [6], and therefore has to fulfill a minimum of basic requirements to be compliant.

Within this document, some of these basic requirements will be discussed.

2.4 ENUM

One possibility to translate E.164 numbers to URIs is ENUM.

ENUM is based technically on the Domain Name System and allows a mapping or translation from an E.164 number to one or more URIs. ENUM is achieving this by providing a distinct domain (e164.arpa) for a unique and 1:1 mapping of E.164 numbers to a specific and unique domain name. Within this domain name the user may store pointers to URIs. This may be any URI (e.g. an e-mail address or a pointer to a web-page), but specifically also a VoIP URI. Only these mappings will be discussed within this document.

ENUM raises two questions:

1. Which type of E.164 numbers may be entered in ENUM?

The type of numbers available will be discussed later in this document.

T-Mobile Exhibit 1002
Part 5 of 6

The current status of discussion is that geographic numbers, numbers for private networks, mobile numbers and personal numbers may be used in ENUM. The usage of the other numbers, especially service numbers like freephone and premium rate services are under discussion.

2. Are E.164 numbers entered in ENUM only or additionally to existing phone services?

The more important question is if the ENUM entries are made IN ADDITION to existing phone services if the subscriber requests it (opt-in) or is it required to have an ENUM entry to get a phone service (infrastructure ENUM)

2.4.1 ENUM as additional service with opt-in (User ENUM)

In this case ENUM domain names are entered in ADDITION to existing phone services available on the PSTN/ISDN. Therefore any call originating on the PSTN/ISDN will be routed normally on the PSTN/ISDN to the existing termination as usual. Only calls originating on the Internet MAY query ENUM and MAY route the call to the termination on the Internet given by the ENUM entry. This is called the opt-in principle.

The called user is opting-in in ENUM, because the entry in ENUM is optional. The calling user is also opting-in, because he may query ENUM or not, and even if he is querying ENUM, he still may decide to terminate the call on the PSTN via a gateway.

In this case the VoIP application is a second line service in addition to the primary line on the PSTN. This approach may be feasible in conjunction with other services and applications on the Internet (e.g. e-mail), but it has one serious drawback for VoIP: it suffers from Metcalfe's Law.

Metcalfe's Law states that "the usefulness, or utility, of a network equals the square of the number of users", which may translate to: "a new communication application will probably be stillborn anyway, because the initial value will be so small that no one will have sufficient incentive for purchase".

Is there a way to overcome this problem? Eventually by using ENUM also as infrastructure service. Here users rely on ENUM regarding VoIP and get used to it, so User ENUM maybe introduced later additionally for other services.

There is another disadvantage with User ENUM: Since the E.164 assignments to the phone services on the PSTN/ISDN and the delegations of the corresponding e164.arpa domains have to be kept in

T-Mobile Exhibit 1002
Part 5 of 6

sync, it has to be validated that only the proper number assignee may request the corresponding ENUM domain. This requires complicated validation procedures to be established.

2.4.2 ENUM as infrastructure service (Infrastructure ENUM)

If the E.164 number is entered only in ENUM, there is no synchronization with PSTN/ISDN services and therefore no validation necessary, which simplifies matters. The E.164 number is then used natively on the Internet.
In this case ENUM is implemented as a kind of IN-Service on the Internet to route voice and other multimedia real-time applications (IP Communications) using E.164 numbers to destinations primarily on the Internet.

The problem to be solved here is how a call originating on the PSTN/ISDN may be routed to such destinations. Routing on the PSTN/ISDN is still done primarily by digit analysis of the dialed destination number. IN services e.g. for Number Portability (NP) are available only on a local or national scale.

This immediately raises the question: which E.164 numbering resources could be used for such destinations?

A simple solution is to use specific numbering resources for this purpose. This would allow to route (and also bill) any call to this number from the PSTN/ISDN to the nearest ENUM-enabled gateway (Point-of-Interconnect). Note: this can be done even on a global scale, if the first 6 to 7 digits of an E.164 number are used (e.g. CC + NDC). End Note.

This has a severe drawback insofar that most numbering plans established by the national authorities (NRA) responsible claim to be technology independent (which is not completely true in all cases anyway), so specific number ranges for "VoIP-only" are currently not possible in some countries and also not on a global scale. Although this may change, other possibilities need to be considered. This document will try to propose different solutions for this problem.

2.5 Why using E.164 numbers natively on the Internet?

It was stated above that users on the Internet may use URIs to communicate with each other. Although this is true in principle, the usage of phone numbers also has advantages.

Some existing Administrative Domains implementing VoIP and other IP Communications use numbers to identify their user agents (subscribers). This may be done either directly by giving the user agents a numeric user(info) to be used in the sip: URI or h323: URI

Address-of-Record, or by providing them in addition with an alias tel: URI Address-of-Record of a global E.164 number, or both.

It is proposed to provide the numeric userinfo in such a way that it maps as partial number to the global E.164 number as defined in ITU-Rec. E.164 Annex B.

There are two main reasons to do this:

1. Most VoIP terminals in use are similar to normal phone terminals (or even use POTS Phones with a terminal adaptor) and provide only a numeric keypad, and

2. if VoIP Applications are migrating from existing PBX or Centrex Systems, they want to provide their users with the same environment as before.

The task of a system administrator of such an administrative domain is to set up a consistent numbering and dialing plans, leaving room for future extensions and also for access codes to reach other numbering plans.

This document tries to give advice in setting up consistent global and local (private) numbering and dialing plans including access codes to be used within and across administrative domains.

The proposed numbering and dialing plans are also compatible with existing numbering and dialing plans on the PSTN/ISDN and especially with the global numbering plan as defined in ITU-T Rec. E.164. The proposed numbering plans can also easily implemented in ENUM for routing within and between administrative domains.

3. Numbering and Dialing plans

This section explains existing numbering and dialing plans in general and also some basic definitions.

3.1 Numbering Plans

A numbering plan defines the structure of a namespace consisting only of strings of decimal digits. It is an inverted tree, consisting of nodes, called number blocks or number ranges and of leaves, called numbers. In a telecommunication numbering plan the numbers are called phone numbers and uniquely identify either directly end-points in a telecommunication network (e.g. a subscriber line), or indirectly temporarily connected users (e.g. mobile or personal devices), or also indirectly specific services (e.g. a freephone service).

Note for net-heads: A numbering plan is very similar to the structure of the DNS. If you take an E.164 number e.g. +436644204100, the '+' can be considered as the root and each single digit can be considered as a label. There are only two minor and one big difference:

- the root and the "top level domain" is on the left side
- a label can be only be a single decimal digit

Therefore a mapping from a phone number to DNS is very easy: if one swaps the order of the digits, places dots between the digits and replaces '+' with 'e164.arpa', you get exactly a domain name as specified in ENUM.

Now to the big difference: in the DNS each node may contain data, e.g. it is possible to have the following e-mail addresses: user@acme.com and user@dept.acme.com, because there are different MX records in acme.com and dept.acme.com.

In a numbering plan only the leaves of the tree are phone numbers, that is, they define end-points, users or services. The +43664 part of a number is called a number block, or if dialed (see below), it is called an incomplete number (not a partial number) and (almost) never leads to a destination (with the exception of pilot numbers for PBX with direct-dialing-in (DDI or DID), see below).

In some numbering plans also hexadecimal digits are allowed, but only for internal network specific purposes and not for the normal user. These digits are not considered any further here. E.164 numbers consist only of decimal digits (and so do the labels in ENUM, except e164.arpa)

End Note for net-heads.

As stated above, a numbering plan specifies the format and structure of the numbers used within that plan. It typically consists of decimal digits segmented into groups in order to identify specific elements used for identification, routing and charging capabilities, e.g. within the E.164 global numbering plan to identify countries, national destinations, and subscribers.

A numbering plan does NOT include the prefixes to be dialed by the calling user (this is part of the dialing plan), and it also does not include suffixes and additional information required to complete a call.

3.2 Types of Numbering Plans

The following types of numbering plans exist in principle:

T-Mobile Exhibit 1002
Part 5 of 6

- ò The global E.164 Numbering Plan
- ò National numbering plans
- ò Local or network specific numbering plans
- o Private numbering plans.

They will be discussed below. Some additional useful terminology in advance:

Closed and open numbering plans

Only the leaves of the inverted tree are phone numbers. To allow the users and also the phone systems to find out if a number is complete, some numbering plans define a fixed length for all numbers or at least for certain numbering blocks (ranges).

A closed numbering plan refers to a telephone numbering scheme that has a fixed number of digits, not counting special service codes. The North American Numbering Plan +1 is an example for a closed numbering plan, because there are always ten digits (10D) associated with each national number: 3 digits area code (NPA) followed by the 7 digits of the subscriber number. Australia +61 is another example of a closed numbering plan.

Note: this term is sometimes confused with a closed dialing plan: A closed dialing plan refers to a national requirement to use all digits of a national number (often including a trunk prefix) to place a call, whether local or long distance. End Note.

There are other numbering plans which have variable number length, only defining the minimum and maximum length of digits, e.g. in Austria the area codes may be 1 to 4 digits and the local numbers may be 3 to 8 digits. This is an open numbering plan.

3.2.1 The Global E.164 Numbering Plan

This is also called the International Public Telecommunication Numbering Plan according to ITU-T Rec. E.164. The numbers are called International Public Telecommunications Numbers (IPTN) in the international format (or E.164 numbers).

A number according to ITU-T Rec. E.164 is a string of decimal digits that uniquely identifies a user-network interface, e.g. PSTN/ISDN or mobile terminals and individuals utilizing specific global services, e.g. Universal International Freephone Numbers (UIFNs). Most of the services/subscribers can be addressed directly, but in cases where indirect addressing is used number translation is required, e.g. for UIFNs. The number contains directly or leads to the information necessary to route the call to the termination point.

T-Mobile Exhibit 1002
Part 5 of 6

A number can be in a format determined nationally or in an international format. The international format is known as the International Public Telecommunication Number (often also known as E.164 Number) which includes the country code and subsequent digits, but not the international prefix.

The global E.164 Numbering Plan defines the International Public Telecommunication Numbers and their structure (e.g. Country Code <CC> and National (Significant) Number <N(S)N> or Global Subscriber Number <GSN>).

3.2.2 National Numbering Plans

A national numbering plan is the national implementation of the E.164 global numbering plan (e.g. N(S)N = National Destination Code <NDC> and Subscriber Number <SN>

3.2.3 Local or network specific Numbering Plans

A local or network specific numbering plan is a local or network specific implementation of a national numbering plan and therefore part of the E.164 numbering plan. It may not exist in some national numbering plans (e.g. in closed dialing plans).

3.2.4 Private Numbering Plans

A private numbering plan is an implementation of a numbering in a private telephone network. It may or may not be part of the national or local numbering plan.

If a private numbering plan maps to the global E.164 Numbering Plan the private numbers are part of the International Public Telecommunication Number as partial numbers, as defined in ITU-T Rec. E.164 Annex B. Only these private numbering plans are considered within this document.

Note: The tel: URI as defined in RFC2806bis uses the terms global and local number. Within RFC2806bis the term global number is used only for IPTN (E.164 numbers) in the format 'tel:+43179780'. All other numbers e.g. in the format 'tel:32;phone-context=+43179780' or 'tel:7978032;phone-context=+431 are called local numbers. Therefore local numbers may be numbers from national, local or private numbering plans. End Note.

3.2.5 Non-E.164 numbers

Any international number which does not conform to the structure, length and uniqueness as defined ITU-T Rec. E.164 is not an E.164

T-Mobile Exhibit 1002
Part 5 of 6

number. Non-E.164 numbers may not be passed across any Network boundaries without a specific bilateral agreement.

Some examples are local special numbers, network specific numbers, etc. For more information see ITU-T Rec. E.164 Annex A.

'911' and other emergency numbers (e.g. '112' in Europe) are a typical examples of non E.164 ûnumbers. Even if they may be dialed from another country in principle, they lack the uniqueness.

3.3 Dialing Plans

A numbering plan is a name space and defines the end-points from the point of the called user. Phone numbers are assigned to network-end points, users or services.

A user normally does not enter in most cases a number in his device. The user is entering a "dialing string", depending on his local context.

A dialing plan is a string or combination of decimal digits, symbols, and additional information that defines the method by which a defined numbering plan is used by the calling user. A dialing plan includes the use of prefixes, suffixes, and additional information, supplemental to the numbering plan, required to complete the call. It is therefore the method to access the given name space.

Depending on the mapping of the dialing plan to the numbering plan, it may be necessary to leave certain number blocks of the namespace of the numbering plan unused for use of prefixes (access codes) to access other numbering plans or network specific services.

Prefix

A prefix is an indicator consisting of one or more digits that allow the selection of different types of number formats or numbering plans to be used.

Another type of a prefix is a Carrier Access Code (CAC) followed by a Carrier Identification Code (CIC) and then the requested numbe- (eventually including again a prefix). This is used to select within the originating network the carrier network to be used to route the call to the destination network. This is a different type of prefix and should NOT be confused with the access code to select the dialing plan.

International Prefix

T-Mobile Exhibit 1002
Part 5 of 6

A digit or combination of digits used to indicate that the number following is a full E.164 Number.

Note: A numbering plan consists only of decimal digits (with the above mentioned exception of network specific hexadecimal digits). A dialing plan may also consist of symbols (e.g. '+') and hexadecimal digits (e.g. '*', '#', 'A-F'). Their use is up to the administrator of the dialing plan. A normal user may not be able to dial all of these 'digits'. End Note.
The symbol '+' has a special predefined meaning, originating from mobile networks: If a number is preceded by a '+', the '+' has to be replaced by the digits equivalent to the international prefix valid within this dialing plan, e.g. '00' in most European national dialing plans or '011' in the North American dialing plan.

Important note: The hexadecimal digits may be used '*' and '#' to manipulate supplementary services and are always network-specific. They should therefore only be used as prefixes to access other numbering plans if it is not planned to use them for supplementary services in the future. End of important note.

3.3.1 Types of Dialing Plans

A user on the PSTN/ISDN is always in one defined dialing plan at a given time. That means, if he is going off-hook and starting dialing digits, or if he enters the digits in his device and submits them in one block, there is always ONE defined dialing plan assumed by the system receiving the dialed digits (dialing string). The user has to know the dialing plan in use, e.g. by reading the manual (phone book). The dialing plan does never change on a device connected to a phone system via a fixed line; it may change in case of a mobile phone while roaming.

Basically the dialing plan can be

- private,
- local,
- network-specific or
- national.

Note that there is no global dialing plan.

3.3.2 Access to numbering and dialing plans

The basic principle of a dialing plan is a follows (although there are exceptions):

- If you dial a number without any prefix, you are accessing a number of the associated numbering plan.

T-Mobile Exhibit 1002
Part 5 of 6

ò If you dial a prefix (access code), you are accessing another numbering or dialing plan.

Normally the dialing plans are hierarchically, especially if the numbering plans are compatible, as it is in the case of E.164 numbers. It is recommended by ITU to use '0' as access code for going up the hierarchy, but this is not implemented in all countries (mostly because for historical reasons the number range is not available).

1. If your phone is connected to a PBX line, you dial either the extension directly or an access code (e.g. '0' or '9') to access the local dialing plan. If your phone is directly connected to the PSTN/ISDN, goto step 2.

2. Now you may dial either a local number or again an access code (e.g. '0') to access the national numbering or dialing plan.

3. There you may dial a national number or again an access code (e.g. '0') to access the international numbering plan.

There is normally no way to go to another numbering or dialing plan directly on the same hierarchy level or to go down the hierarchy. The only way to access another numbering or dialing plan normally is to go via the lowest common hierarchy. This requires that the other numbering plan is mapped into the next higher hierarchy. To reach another local numbering plan in the same country requires going via the national dialing plan, to reach a local numbering plan in another country requires dialing the international access code and the E.164 number including the country code.

3.3.3 Mapping of private numbering plans as partial numbers

To reach another private numbering plan with DDI via the PSTN/ISDN requires a mapping of the private numbering plan to the E.164 numbering plan as partial numbers. In some cases a given private number may even be reached with two or three different E.164 numbers (e.g. from one or more local numbering plans, from one or more national numbering plans, and here either from a mobile number or a number for corporate networks.

The extension 3184 of a Vienna company may be reached via +43 1 60501 3184 (Vienna), +43 664 67070 3184 (mobile) or +43 50811 3184 (corporate networks).

3.3.4 Cross trunks or cross connections

In some case there may exist additional access codes to directly access other numbering plans as a short cut. These access codes are called cross trunks or cross connections. For technical reasons these cross connections have been implemented also in the public PSTN/ISDN in the past when the E.164 numbering plan was not fully implemented yet. They still exist and are widely used between private networks with heavy traffic relations. These cross trunks may be implemented also with physical trunks or only virtually as cross connections. Often numbers out of the number range '9' are used for this purpose.

It is depending on the system administrator of the destination network if the dialing plan or only the numbering plan can be accessed via these cross connections. Normally only the numbering plan may be accessed and sometimes the access is even more restricted to certain number ranges. The reason for the blocking of the dialing plan (especially the access code to the next hierarchy) is to prevent transit calls (for billing reasons).

Of course the number ranges (blocks) used for these access numbers cannot be used within the numbering plan. Since often the number range '1' is used for network-specific services, it is quite common to use only the number ranges from '2' to '8' for subscriber numbers.

3.3.5 Closed Dialing Plans

In some countries and networks closed dialing plans are used. A closed dialing plan refers to a national requirement to use all digits of a national number (often including a trunk prefix) to place a call, whether local or long distance. The current systems in France (as of October 1996) and Belgium (as of January 2000) are examples of closed dialing plans.

The issue of closed dialing plans can be somewhat confusing. Not only that the terms closed dialing plan and closed numbering plan are used ambiguously in literature, there are two types of closed dialing plans.

Type I is derived by canceling the direct access to the local numbering plan, but leaving the rest of the local dialing plan as is: one always has to dial the national access code (e.g. '0') to reach national E.164 numbers. Only network-specific numbers and service code may be dialed without prefix. Examples are Switzerland and France. Also many mobile networks use this type. This is less logical, but easier to tell the customers: "You have to dial now the area code for local numbers also." People are also used to this approach from mobile phones anyway.

Type II is derived by canceling both the local numbering plan and dialing plan: one may dial national numbers directly without a

T-Mobile Exhibit 1002
Part 5 of 6

prefix. One example is Portugal. This approach seems more logical and also saves one digit to dial, but is harder to explain: "You have to dial now the area code for local numbers also, but you must not dial the national access code". To confuse things even further from a logical point, but to make things easier for customers, the international access code in Portugal is still '00'.

In the North American Numbering plan all variants exist, normally you may dial 7 digits xxx-xxxx to access the local dialing plan, and 1-xxx-xxx-xxxx (1+10D) to access the national dialing plan, but in some NPAs you also may dial only the 10 digits. In some NPA the dialing plan is closed, so you may only use 1-10D. With mobile phones you also must use 1+10D always.

In general, the NANP is moving to 1+10D in all NPAs (for more information see www.nanpa.com).

4. Types of numbers in existing numbering plans

Phone numbers in the PSTN/ISDN serve two main purposes: to route calls properly to their destination and to be able to tariff the call. Before the introduction of IN-services and all-call-query (ACQ) for all numbers dialed (also still today), a switching system must be able to analyze the first digits dialed and deduce the routing information and the tariff information. For E.164 numbers in the international format this is limited to the first 7 digits.

It is therefore necessary to group the numbers in certain number blocks to be able to derive routing and/or billing information. This is also required to enable the customers to derive especially the expected cost and/or service of the call by looking at the number.

4.1 International Public Telecommunication Numbers (E.164 Numbers)

The ITU-T Rec. E.164 defines the following types of International Public Telecommunication Numbers (IPTN). A distinction between the types of numbers can be made within the first three digits.

- IPTN for Geographic Areas

These are the "real" Country Codes (CC) and are one to three digits in length. The maximum length of an IPTN is 15 digits in principle, but nationally shorter length may be required (e.g. a number of the NANPA has a maximum length of 11 digits). The further structure is a national matter and will be discussed in the next section.

In order to determine the country of destination, the most appropriate network routing and the proper charging, the originating country must analyze a number of digits of the E.164 international

T-Mobile Exhibit 1002
Part 5 of 6

number (maximum of 7). The length of the National Destination Code (NDC) increases the potential requirement for number analysis because it provides for a combination of either a Trunk Code (TC) and/or a network identification function. Careful consideration should be given to the preparation of the National Destination Code (NDC) assignments.

o IPTN for Global Services

The numbering plan for global services is service specific. Each use of an E.164 country code for a global service needs to comply with numbering assignment principles, as specified in Recommendation E.190, as identified for the specific service, and the criteria and procedures as specified in Recommendation E.164.1. Refer to the appropriate numbering Recommendation for documentation regarding the numbering scheme and any service specific principles, e.g. Recommendation E.168 û Application of E.164 numbering plan for UPT.

The international public telecommunication number for global services is composed of the 3-digit country code applied for the global service and the Global Subscriber Number (GSN). The maximum length is 15 digits.

Digit analysis for global services is service specific. In order to determine the specific global service, and the call routing and charging, the digit analysis should not exceed 7 digits, e.g. 3-digit CC + 4 digits of N(S)N. Refer to the appropriate ITU-T numbering Recommendation for documentation regarding the number analysis requirements for the specific global service.

Currently the following Global Services are defined:

o ITU-T Recommendation E.168 (1999), Application of E.164 numbering plan for UPT.

o ITU-T Recommendation E.169 (1998), Application of Recommendation E.164 numbering plan for universal international freephone numbers for international freephone service.

o ITU-T Recommendation E.169.2 (2000), Application of Recommendation E.164 numbering plan for universal international premium rate numbers for the international premium rate service.

o ITU-T Recommendation E.169.3 (2000), Application of Recommendation E.164 numbering plan for universal international shared cost numbers for the international shared cost service.

ò IPTN for Networks

T-Mobile Exhibit 1002
Part 5 of 6

International public telecommunication numbers used by Networks consist of three parts: a shared 3 digit E.164 country code; an identification code; and a subscriber number. The maximum length of international public telecommunication numbers used by Networks is fifteen (15) digits.

For calls utilizing the international public telecommunication number for Networks, the maximum number of digits to be analyzed is seven, which includes the three digits of the E.164 country code, the identification code, and the initial significant digits (if any) of the subscriber number. A minimum of the 3-digit country code and IC must always be analyzed to determine the appropriate routing and charging.

o IPTN for Groups of Countries

International public telecommunication numbers used by Groups of Countries consist of three fields: a shared three digit Rec. E.164 Country Code; a one digit Group Identification Code; and a Subscriber Number to a maximum length of eleven digits. The maximum length of international public telecommunication number used by Groups of Countries is fifteen digits.

These are the first three digits of international public telecommunication number for Groups of Countries. A country code for Groups of Countries is a shared (i.e., shared between GoC's) three digit CC used in combination with a single digit GIC to uniquely identify a Group of Countries.

The maximum number of digits to be analyzed for the processing of calls to international public telecommunication numbers for Groups of Countries is seven. This includes the CC field (three digits) plus the GIC field (one digit) plus the first three digits of the Subscriber Number (SN). A minimum of four digits (i.e., CC + GIC) must always be analyzed to determine the appropriate routing and charging.

4.2 National E.164 Numbers

Since the structure and also the types of numbers and services provided are a national matter, there exists a big variety of implementations, although there are some recommendations from ITU and also some common international and regional approaches.

Note: One should consider that national numbering plans have historically evolved and a complete alignment of these numbering plans would cause major changes to the existing numbering plans. Since these changes are very costly and causing major resistance by the public, they are either avoided at all or are long term projects.

T-Mobile Exhibit 1002
Part 5 of 6

Even such a simple change to introduce the recommended access code '0' for international calls has not been implemented globally yet. The introduction of a new globally unique access code in all national dialing plans (e.g. for VoIP) is absolutely impossible ù don't even think of it. End Note.

In most countries the following types of numbers have been introduced. In most cases a distinction between the types of numbers can be made within the first three or four digits.
Since the grouping or categorization differs in most countries, a new and simplified grouping is proposed:

4.2.1 'Pure' Geographic numbers

These are the "original" phone numbers for fixed line end-points. In open numbering plans they consist of a "trunk code û TC" or "area code", giving the geographic area or region and the "subscriber number û SN". The SN may be dialed in open dialing plans directly out of the local dialing plan. Customers may derive the TC (and also the tariff for distance) by knowing the address of the called user.

The TC is used to route the call to the switching system(s) serving the geographic region and also to derive the tariff from the distance between the originating and termination end-point.

In many countries local number portability is possible if the customer is moving to another location within the same TC range. A customer may also port these numbers to another service provider without changing his location; this is called service provider portability.

In most countries also databases are available giving the exact location of the end-point e.g. for emergency services.

These geographic numbers are using up most of the numbering space and have been the reason for earlier discussions on numbering exhaust. For historic technical reasons the numbering space is not used economically. Since some years the number of fixed lines using mostly these geographic numbers is decreasing.

For this type of numbers number ranges out of each TC are assigned to network operators or service providers, which in turn assign the numbers to the end-users.

4.2.2 Non-geographic numbers for private networks

A range of non-geographic numbers may be used for networks private networks with more then one connection to the PSTN/ISDN. These connections normally have also geographic numbers assigned. These

T-Mobile Exhibit 1002
Part 5 of 6

numbers consist of a "national subscriber number" and can only be dialed locally by accessing the national dialing plan and by prefixing the national access code. The "national subscriber number" consists of a pilot number for the private network (company) and a mapping of the private numbering plan as partial number.

The "pilot" number is translated to the nearest geographic number providing access to the private network and also to derive the tariff. This tariff is in the most cases only dependent on the type of number (the number ranges assigned for private networks), and not on the pilot number.

For this type of numbers service provider portability is available.

For this type of numbers the pilot numbers are assigned to the private networks, which in turn assign the partial numbers to the end-users.

4.2.3 Non-geographic numbers for networks

Non-geographic number ranges may also be used for networks (e.g. mobile networks). They consist in open numbering plans of a "network destination code û NDC" and also a "subscriber number ûSN".

The NDC is used to route the call to the nearest Point-of-Interconnect of the network given by the NDC and also to derive the tariff. The tariff may either be dependant on the type of network or dependant on the specific network.

Between the same types of networks (e.g. mobile networks) service provider portability may be available in some countries.

For this type of numbers NDCs are assigned to network operators or service providers, which in turn assign the numbers to the end-users.

Note that in some countries also geographic numbers may be used for mobile subscribers. End Note.

4.2.4 Non-geographic numbers for personal services

Non-geographic numbers may also be used for personal services . They consist in open numbering plans of a "network destination code û NDC" and also a "subscriber number ûSN".

Depending on the implementation of the personal services, either the NDC is used to route the call to the nearest Point-of-Interconnect of the network providing the personal service, or the full number is translated to route the call again the a PoI, or directly to the

geographic number where the user is currently connected to. The number range is also used to derive the tariff.

Personal numbers are normally service provider portable by definition, especially if the number is assigned directly to the end-user. Number ranges may also be assigned to service providers, which in turn assign the numbers to the end-users.

4.2.5 Non-geographic numbers for services (tariff related)
Non-geographic number ranges are used for services. They consist in open numbering plans of a "network destination code û NDC" and also a "subscriber number ûSN". The NDC defines the type of service.

Since most of these services are related to billing, the NDC is primarily used to derive the tariff. This becomes clear if we look at the services in question: these are freephone, shared cost and premium rate or other value added services.

Services may be hosted with different service providers and are also translated finally to a geographic number for termination. These services are normally implemented as IN-services and two IN-dips are required for completion: the first to find out the network or service provider hosting the service and a second to translate the service number to the final destination number. This second translation may be dependant on date, time and origination of the call.

In most case service provider portability is available, but only between the same types of service.

This type of numbers is in most cases directly assigned to the end user and then hosted by a service provider.

It should be noted that even if some of this services may be reached uniquely by e.164 numbers, but are blocked for international incoming calls because they cannot be billed properly.

4.2.6 Discussion of the existing schemes for types of numbers

The boundaries between the classifications of the types of numbers are already blurred in the existing schemes and may differ in the various national implementations.

Some examples (not exhaustive):

Some countries assign numbers out of geographic numbering blocks for access to mobile wireless terminals e.g. in the NANP. Therefore the same tariffs are charged to calling users regardless of destination in the fixed or mobile networks and also regardless of mobile

T-Mobile Exhibit 1002
Part 5 of 6

network. The mobile networks therefore may charge air-time to the called subscriber.

Personal services are currently classified as non-geographic numbers in most countries and also within the global international E.164 numbers. The reason for this is that existing number ranges for personal numbers are implemented as Personal Services along the service description of for Universal Personal Telecommunications (UPT) as specified in ITU-T Rec. F.85x series. The basic assumption of UPT is that an UPT user may register on any other fixed or mobile terminal and receive calls to the personal number and also may make calls from this terminal in his/her account. This requires an IN-type service with All Call Query (ACQ) to translate the dialed UPT number to the number of the line where the user is currently registered. This service is currently implemented rarely and if, only on a national scale, because there is no global interworking of IN-services available. For this reason and also because of the pricing of the service it was not very successful on the market.

A global implementation using the assigned CC for UPT +878 and IP technology is under development. Although here the users may also attach to PSTN/ISDN lines, the prime intention of the service is for "mobile" users on the Internet.

On the other hand, one may consider mobile numbers also as "personal" numbers and mobile services as "personal" services, because a mobile numbers are (at least in GSM and UMTS) linked to Subscriber Identity Modules (SIM). These SIMs are attached temporarily to a device (the mobile phone). The device also gets a (temporary) number (MSRN) and the routing of the call is done by this numbers. This also requires a translation of the number dialed (the mobile number) to the number assigned currently to the device, the mobile subscriber roaming number (MSRN). The MSRN is also a E.164 number but used only within or between mobile networks to route the call properly to the destination mobile switching center (MSC) of the roaming subscriber (user). The translation is also done by an IN-type service with ACQ via the home location register (HLR) of the subscriber.

The technical implementations of personal and mobile numbers are very similar, with one exception: there is a globally interworking IN-service available, but only within and between the GSM/UMTS networks.

Therefore one may question the classification of mobile numbers in the existing categories ûgeographic or non-geographic for networks (they may also be classified as type non-geographic for services) and one may also question the statement that numbering resources are allocated technology independent.

T-Mobile Exhibit 1002
Part 5 of 6

It is therefore proposed to classify both personal and mobile numbers as equivalent and also as non-geographic number for networks.

4.2.7 Proposed new scheme for types of numbers

It is therefore proposed to use a new classification scheme:
o Pure geographic numbers
o Non-geographic numbers for private networks
o Non-geographic numbers for networks and personal numbers (including mobile networks and personal services using VoIP networks) û or better:
mobile personal services.
o Non-geographic numbers for tariff related services

Even if mobile (wireless) and mobile (VoIP) networks (or services) are keep distinct for some time, the may merge into one group of services, namely mobile personal services very soon, especially with so-called dual mode devices.

Note: These devices are announced for the 4Q2003 and will have both GSM and WiFi (VoIP) capabilities and may even use the same SIM card for identification and authentication. End Note.

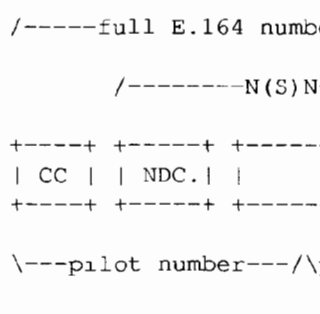
4.3 Partial Numbers

Private numbering plans may map part or all of their numbers to an E.164 Number in such a manner that destinations (extensions) within the private network may be reached form the public PSTN/ISDN by direct-dialing-in (DDI). This is described in more detail in ITU-T Rec. E.164Annex B "Application of international public telecommunication numbers for ISDN".

This is done currently in the following way: a number block of an E.164 number is assigned to a company or provider. This numbering block is called pilot number. Then the numbering plan of the private network is attached as partial number.

Pilot number and partial number together are a full E.164 number. The full E.164 number MUST fit into the national or international numbering plan, especially concerning digit length.

T-Mobile Exhibit 1002
Part 5 of 6



Types of numbers used for this purpose are:

- National Geographic numbers
- National non-geographic numbers for private networks
- National non-geographic numbers for mobile networks
- Global numbers for networks

Note: If a pilot number is in a numbering range supporting number portability, only the pilot number (at the endpoint of the PSTN/ISDN) is portable. End Note.

This is the reason why personal numbers should not be used for this purpose, or a distinction must be made between single portable numbers and pilot numbers. This is already the case for mobile (personal) numbers.

Note: I received a comment to this section from John Elwell, stating that

"In 4.3 the term "pilot number" is possibly misleading. The fact is that two private networks could have the same pilot number, e.g., one network has nnnnnn1xxx and another has nnnnnn2xxx, where pilot number nnnnnn is the same in each case. The term pilot number implies it is a kind of lead-in to a private network, but in fact it is (in such cases) insufficient to identify a particular network."

To which I replied:
This is a very crucial point.
As you see, I copied out the picture from E.164 Annex B, which defines everything EXCEPT the pilot number (I suspect on purpose, because there seems to be no clear definition).

According to your explanation, the term pilot number defines the endpoint in the public network, and I know, there may be split PRI connecting more then one PBX with different ranges.

T-Mobile Exhibit 1002
Part 5 of 6

Here I have now the problem that on IP there is not really a clear definition of an "endpoint".

The next problem I have is that in your example in ENUM (DNS) I could define the "endpoint" or pilot number (delegation-wise) to be nnnnnn1 and nnnnnn2. The "endpoint" in the case is a change of authority and this can be in DNS only at a "point" or in numbering speak only with a full digit. If you have the case (and such cases exist) that one private network (PBX) has number ranges nnnnnn1 and 2 and the other has nnnnnn3 and 4, you could solve this in DNS only with four separate delegations, two for one network and two for the other.

So if one hand the term pilot number is defined as network endpoint and this is meaningless on IP, I need another term for a point of delegation of authority in DNS. So either I come up with another term or I explicitly define in my document "pilot" number as boundary of authority to the number range holder. End of Note.

4.4 Calling line identification (CLI)

Phone numbers are also used to identify the identity of the calling user. For this reason the number of the calling user is transmitted as CLI to the called user.

The CLI serves many different purposes:

- Call-back information to the called user.
- Identification of the user and his location to emergency services and legal intercept
- Identification of the user for malicious call identification (MCI)
- Identification of the user for accounting purposes

These purposes have different requirements on the trustworthiness of the CLI. In some signaling systems two numbers may be transmitted, one un-trusted (user provided) for call back and a trusted (network provided and screened) for the other thee items.

Regarding the types of numbers, in case of geo-graphic and non-geographic numbers the CLI of the user should be displayed if this user is making an originating call using this number. In case on non-geographic numbers for private networks, both numbers may be displayed if a translation is used.

In case of non-geographic numbers for services either only the number of the terminating line is displayed, or also both numbers if available.

T-Mobile Exhibit 1002
Part 5 of 6

The usage of CLI with VoIP and the possibility to provide secure signaling of this information via the Internet will be discussed in detail in a separate document

5. E.164 Numbers for VoIP

5.1 E.164 Numbers for VoIP-only

In principle any E.164 number may already terminate on IP-based networks or the Internet using VoIP technology. Numbering Plans claim to be technology independent. A telecommunication network provider may claim a number range out of an area code reserved for geographic numbers or a number range out of a network destination code for (mobile) networks. Since he may use any technology within his network, he may also use VoIP technology.

There are already network providers using IP technology internally (e.g. cable network providers), mobile operators are planning to use VoIP technology for UMTS.

Currently these networks are mainly 'private' IP networks with no direct connection to the Internet. All interconnections with the public telephony network and to other networks are done via circuit-switched Points-of-Interconnect. All calls are routed via the PSTN, even if they originate and terminate on IP terminals. This is not efficient for various reasons, the two most important being the unnecessary double use of expensive equipment (gateways) and the reduction in Quality of Service (QoS) (delays) also caused by the unnecessary double use of gateways.

Another drawback of these closed networks is that the VoIP service may only be accessed from within the networks. If users want to be mobile and use their terminal equipment anywhere on the public Internet they need to be able to connect and register on any (broadband) Internet access (e.g. via a WiFi hotspot or in a hotel or meeting broadband connection).

So we have two basic requirements for VoIP:

1. Calls originating on the Internet and terminating on the Internet must stay on the Internet or terminals using IP technology should be reachable via the public Internet.

2. Users want to have an E.164 number independent of the PSTN, want to connect to the Internet anywhere and want to be reached via this E.164 number from anywhere, including the PSTN/ISDN.

In this section the possible types of numbers for VoIP-only usage are discussed

5.2 Potential E.164 Number types for VoIP-only

5.2.1 National Geographic Numbers

Geographic numbers have a geographic significance. A caller may determine by looking at the number the geographic region, in some countries, depending on the numbering plan even the town or village. What is even more important is that emergency services in most countries may derive from the displayed number not only the identity but also the exact location of the caller.

This is considered an important feature and should therefore be implemented also for VOIP.

So if geographic numbers are allocated to VoIP terminals, it should be required that the terminal can only be used at the given location. This is no technical problem e.g. with cable or xDSL access.

To be more precise: it is required that the user may only register (any terminal) via the given access and make outgoing call using the geographic number in CLI from this location.

This does not imply that he may not receive calls to this number anywhere in the world. This can easily be achieved via simple call forwarding to another number.

Geographic numbers may either be used for residential subscribers or for private networks. In case of private networks the same is valid as stated in the next section.

5.2.2 National non-geographic numbers for private networks

Private networks may migrate to VoIP on their own discretion anyway. So a private network may use VoIP internally anyway. The question here is the access to the private network itself, which is done normally via the pilot number and a translation of the national non-geographic number to one or more geographic numbers. It is also up to the private network if may be reached from the Internet directly.

5.2.3 National non-geographic numbers for mobile networks

This is a question of definition if VoIP networks are also considered as mobile networks.

T-Mobile Exhibit 1002
Part 5 of 6

One could imagine that the definition for mobile networks is extended or that there is no distinction between numbers for mobile networks and personal numbers.

5.2.4 National non-geographic personal numbers

This is the most convenient number range candidate to be used for mobile VoIP, because it fits the purpose best. Furthermore number range(s) for personal numbers are already reserved in most countries, but in most cases not or not extensively used.

5.2.5 Global numbers for networks

These numbers may be considered equivalent to national non-geographic numbers for private networks. It is up to the customer and his business if he prefers a national or global numbering resource or both.

5.2.6 Global personal numbers
These numbers are equivalent to national non-geographic personal numbers. It is up to the subscriber if he prefers a national or global numbering resource or both.

6. How to set up numbering and dialing plans for VoIP domains

6.1 Basic Requirements

Note: the requirements in this section are only valid for numbering plans if the administrative domain wants to map its numbering plan to the global numbering plan and/or to a national numbering plan, to be reachable by E-164 numbers from the outside, either from the PSTN, from the Internet or both. End Note.

They are only valid for dialing plans if the administrative domain wants to access the global numbering plan and/or national dialing plans to reach other administrative domains or the PSTN/ISDN via E.164 numbers.

These requirements are not valid for administrative domains hosting single E.164 numbers, e.g. local numbers, mobile numbers or personal numbers requiring number portability. In this case a mapping of an own numbering plan is not required, although a dialing plan may exist.

Recommendation 1:

If existing numbering and dialing plans are used, e.g. if an administrative domain is migrating an existing private, local or

T-Mobile Exhibit 1002
Part 5 of 6

national network to IP-technology, the numbering and dialing plans MUST be compliant to these existing numbering and dialing plans.

Recommendation 2:

The global numbering plan as defined in ITU-T recommendation SHALL be accessible directly and in the same way from all numbering and dialing plans defined in this document (e.g. with an international prefix).

Recommendation 3:

The numbering and dialing plans defined in this document SHALL be compatible with the global numbering plan as defined in ITU-T Recommendation E.164 Annex B.

Recommendation 4:

It SHALL be possible to address private numbers (extensions) within an administrative as defined in ITU-T Rec. E.164 Annex B.3.2 by an ISDN Number to be reached either with Direct-Dialing-In (DDI) (Overdialing) or via MSN. This implies that the private numbering plan maps to the E.164 numbers as partial numbers. Sub-addressing (network address extensions) SHALL not be used.

Recommendation 5:

All private numbering plans according to this document SHOULD use a fixed length of numbers. This is to allow also for fixed length E.164 numbers and a defined end-of dialing for terminals.

But: Note A private numbering plan could have variable number length, but the corresponding E.164 numbers are fixed length. For example: Site 1 has private numbers 77xxxx mapping to E.164 numbers +44 123 4567 xxxx and site 2 has private numbers 666 xxxx mapping to E.164 numbers +44 234 5678 xxxx. End Note:

Recommendation 6:

If the administrative domain has to be reachable from the outside, it is recommended to start setting up numbering and dialing plans first with the selection of the E.164 number range (pilot number) where the numbering plan will be mapped into as partial number.

After the selection of the number range assigned to the administrative domain the according dialing plan has to be selected and defined.

T-Mobile Exhibit 1002
Part 5 of 6

After the definition of the dialing plan it is known which number ranges are used up eventually for access codes, allowing defining the available numbering ranges for local numbers.

6.2 Which E.164 Numbers to use for mapping of partial numbers?

As stated above all types of numbers may be used for VoIP, but only certain E.164 number types are recommended for partial number mapping to administrative domains and therefore require the creation of an own numbering and dialing plan. With all other options the numbering and dialing plans are already predefined.

o Global Numbers for Networks

These types of numbers are recommended for administrative domains hosting subscribers from many different countries. In this case a dialing plan for global access is recommended.

ò National non-geographic numbers for private networks

These types of numbers are recommended for administrative domains hosting subscribers from mainly this specific country. The selection is also dependent on national regulations. In this case a dialing plan for national access is recommended.

o National non-geographic numbers for mobile networks

These types of numbers are also recommended for administrative domains hosting subscribers from mainly this specific country. The selection is also dependent on national regulations. In this case also a dialing plan for national access is recommended.

Note: this is only possible if the mobile network allows partial numbers and DDI. If the administrative domain is also mapped to another number range, it is recommended to use the dialing plan of the other numbering range and let the system convert the digits to access the mobile network. End Note.

o Geographic numbers

These types of numbers are recommended for administrative domains hosting subscribers from mainly this specific location (city). In this case a dialing plan for local access is recommended.

Note on number assignment to administrative domains

E.164 numbers may be assigned to an administrative domain in two different ways, depending on policy.

T-Mobile Exhibit 1002
Part 5 of 6

1. The administrative domain is the End User
2. The administrative domain is the number range holder

This has implications on ENUM and Number Portability.

The administrative domain is the End User

In this case the administrative is equivalent to a private company implementing an IP PBX or IP Centrex. The company is the End User holding the E.164 Number minus the partial number range (also called pilot number) and has the right to opt-in into ENUM with this number. The full E.164 numbers may or may not be entered in ENUM. If the numbers are entered in ENUM, the company may in addition decide to provision the entries as a whole or give the provisioning of the single entries to the employees using the number.

Number Portability never applies.

Examples are administrative domains (companies) with national geographic numbers or national non-geographic numbers for private networks.

The administrative domain is the number range holder

This is the case the administrative domain is equivalent to a Telephony Service Provider (TSP) in the PSTN/ISDN sense. The administrative domain may now assign in turn E.164 Numbers out of the number range to End Users.

In this case the End User is the holder of the E.164 Number and has the right to opt-in to ENUM on his own.

If Number Portability also applies within the number range, the administrative domain must be aware of this fact and allow for porting in and out of numbers.

Examples are administrative domains implementing local numbering plans as Local Exchange Carriers or administrative domains implementing service numbers e.g. personal numbers.

6.3 Dialing Plans for administrative domains

6.3.1 General Recommendations for all Dialing Plans

These recommendations concern dialing strings and are proposals for discussion.

Recommendation 7:

Any dialing plan of an administrative domain SHALL recognize a global (E.164) number in the format as defined in rfc2806bis and E.123 with a leading '+'. The server of the administrative domain SHALL translate the '+' to the international access code used within this administrative domain. This is also necessary for a potential interworking with dual-mode mobile devices (e.g. GSM and WiFi), because it is common to store numbers in this format.

Note: these numbers may be transmitted to the administrative domain from the user device (User agent) either in the format tel:+43179780, sip:+43179780@acme.com or h323:+43179780@acme.com. If a server receives such a request, he may either forward the call to the PSTN or launch an ENUM-query. If the result is a NAPTR with a (different) tel:+xxxx, he may launch another ENUM query. If the result of an ENUM query is the same number as the previous number queried or no NAPTR is found for this number, the call shall be forwarded to the PSTN or forwarded to another proxy with tel:+xxxx;edi (ENUM dip indicator).

Recommendation 8:

Any dialing plan of an administrative domain SHALL recognize the international access code either in the format '00' or '011', e.g. 0043179780 or 01143179780. Only administrative domains with global access SHALL recognize both access codes.

Recommendation 9:

For customer convenience, the '+' character MAY be replaced by the '*' symbol, e.g. international calls MAY also be dialed *43197980.

Recommendation 10:

The administrative domain MAY decide to use '**' for the selection of a cross trunk or cross connection. In this case the format of the dialing string is '**yyyxxxxx' where yyy is the selection of the cross trunk to another numbering plan and xxxxx is a number of the other numbering plan selected. It is suggested to use not more then 3 digits for cross trunk selection.

In addition or instead of '**' also a digit MAY be used as access code for cross trunking. It is recommended to use the digit '9' for this purpose.

Recommendation 11:

The character '#' may be used as end-of-dial signal.

T-Mobile Exhibit 1002
Part 5 of 6

The further selection of the variant of dialing plan used within an administrative domain is an internal matter, but the choice has to be communicated to the users (subscribers)

6.3.2 Types of dialing plans

The dialing plans for domains come in four variants:

1. Dialing Plan for domains with global access
2. Dialing Plans for domains with national access
3. ITADs within Local Dialing plans
4. Dialing Plans for domains with local access

6.3.3 Dialing Plans for domains with global access

This dialing plan is for administrative domains with no specifically defined local or national access. This is intended for administrative domains hosting users (subscribers) from various nationalities or countries.

1. All generic recommendations from above may apply.

2. All other numbers dialed are treated like private (local) numbers out of the selected numbering plan (see numbering plans below).

3. Network specific numbers may be introduced in the number ranges 1 and 9 (see below).

As long as the problems of user location and the routing of emergency calls is not solved, it is not recommended to provide routing to national energency services, but this may be implemented later if the numbers 112 and 911 are reserved from the beginning.

6.3.4 Dialing Plans for domains with national access

Administrative domains with national access will be domains using national mobile or personal ENUM numbers, where most of the users (subscribers) may come out of this country. Nevertheless, a domain may also decide to use only global access.

1. All generic recommendations from above may apply, with the exception of '00' or '011'. The reason is that in this case either '00' or '011' may be valid, depending on the national dialing plan.

2. Only one national access SHALL be provided. It MUST be made clear to all subscribers which national dialing plan is accessed. Example: If the Austrian national dialing plan is accessed, a number dialed as 019793321 or 004319793321 is equivalent to +4319793321.

T-Mobile Exhibit 1002
Part 5 of 6

3. It is up to the dialing plan administrator of the ITAD if a Type I or Type II dialing plan is selected.

4. The access code to the national dialing plan depends on the national dialing plan itself, e.g. in Europe '0' is recommended, in the NANPA '1' is recommended.

5. Network specific numbers may be implemented depending on the Type of dialing plan selected

ITADS with national access may provide routing to national emergency services, e.g. to the European Emergency Number 112.

6.3.5 Domains within Local Dialing Plans

If a local dialing plan has to be implemented, the administrator has no choice. He has to implement the local dialing plan in question and also use local numbers as assigned by the numbering authority.

6.3.6 Dialing Plans for domains with local access
Administrative domains with local access will be domains created by migration from enterprise PBX or Centrex and therefore may already have implemented a dialing plan. In this case this dialing plan may be migrated as is to the ITAD and in most cases this means that the users are used to dial out to a local dialing plan.

1. All numbers dialed starting with 0 SHALL be treated as access to ONE specific well defined local dialing plan. The numbers dialed after the 0 belong always to the local dialing plan selected.

2. Only ONE local access SHALL be provided. It MUST be made clear to all subscribers which local dialing plan is accessed. Example: If the Vienna local dialing plan is accessed, a number dialed as 09793321 or 0004319793321 is equivalent to +4319793321.

3. Since with 0 the local dialing plan is reached, further prefixes to be used within this local dialing plan are already defined.

4. All other numbers are treated like private (local) numbers.

5. Network specific numbers may be introduced in the number ranges 1 and 9 (see below).

Domains with local access may provide routing to local emergency services, e.g. to 911, 112 or 133 in Vienna.

6.4
Numbering Plans for administrative domains

6.4.1 General

T-Mobile Exhibit 1002
Part 5 of 6

The private numbering plan is either taken over from an existing numbering plan, in case of a PBX or Centrex migration to VoIP (IP PBX or IP Centrex), or defined from scratch. It the first case it is assumed that the numbering and dialing plan is already compatible with ITU-T Rec. E.164 and proper access codes to the local or national E.164 numbering plan exists.

In the second case, the following is recommended:

1. Define the number of digits N of the local number. The possible number length is dependent on the E.164 number range where the local number is mapped as partial number. The minimum number of digits is the maximum will be dependant on expected final number of users and the type of E.164 number to be used to address the domain from E.164 (4, 5 or even 6 digits).

It should be noted that the possible flexibility may be very restricted here, especially in closed numbering plans.
Example: If the number should be mapped to an E.164 number of the NANP, and only number ranges smaller then 1-xxx-xxx are assignable, the choice is between 2 to 4 digits.

2. The E.164 number requested to address the administrative domain as a whole SHALL be according to ITU-T Rec E.164 Annex B.3.2 in such a way that the CC N(S)N SN or CC GSN including the private number as partial number gives a full E.164 number and does not exceed 15 digits (in national numbering plans additional restrictions may apply)

3. No private number SHALL start with digit 0.

4. It is also recommended that no number related to a user starts with 1 and 9, so it is recommended to use the digits from 2 to 8. Therefore private numbers MAY start from e.g. 2000 to 8999.

5. There is one exception from this rule. if the dialing plan is closed and of type I (which means that always an access code has to be used to dial a local number), then, depending on the access code also the ranges x0, x1 or x9 may be used for local numbers, where x is the access code. In this case all other number ranges can be used for network specific numbers.

6.4.2 Network specific numbers and access numbers

Administrative domains may provide network specific numbers for internal use only. This numbers SHALL not be reachable from the outside, since they are NOT E.164 numbers.

A domain may decide on the use network specific numbers on its own discretion, but the following principles are recommended to be common for user convenience.

Network specific numbers may be used for the following main purposes: providing internal services specific for this administrative domain and providing access to emergency services.

Network specific service numbers SHALL start with digit 1 (or 9).

Numbers starting with 9 may also be used as access numbers to cross connections to other domains, e.g. if an AD1 has cross connections to an AD2 and an AD3, it may decide to use access code 99 to access directly the private numbers of AD2 and 98 to access directly the private numbers to AD3.

6.4.3 Emergency Numbers

As long as the problems of user location and the routing of emergency calls is not solved, it is not recommended to provide routing to national emergency services from domains with global access, but this may be implemented later if the numbers 112 and 911 are reserved from the beginning.

Domains with national access may provide routing to national emergency services, e.g. to the European Emergency Number 112.

Domains with local access may provide routing to local emergency services, e.g. to 911 or 133 in Vienna, but only if they map to geographic numbers.

6.4.4 Adress-of-Records and userinfo

Subscribers of these administrative domains may be provided with the following types of Address-of-Records and alias userinfo:

sip:private number@acme.com (or h323:)
sip:+e164 number@acme.com (or h323:)
tel:+e164 number

In addition, the following types may be used within the domain:

tel:<private number>;phone-context=acme.com
tel:<private number>;phone-context=+e164number - partial number
but these are not recommended.

7. Routing of calls to E.164 numbers terminating on VoIP

T-Mobile Exhibit 1002
Part 5 of 6

7.1 Routing on the PSTN

In principle routing on the PSTN/ISDN is done via digit analysis. Up to seven digits may be used in a given network for this purpose. Normally the originating network (a local network e.g. a LEC) is analyzing the first digits to determine if the call is local or long distance. If it is long distance, the call is forwarded to a long-distance carrier. The long-distance carrier is again analyzing the digits, and routing the call either to the destination network (nationally) or routing the call to the country in question internationally. This is done either to another long-distance carrier or to the destination network

If a number is ported, an intermediate step may be necessary to determine the final destination network. How this is done depends on the method of NP implemented and is not discussed detail here. The primary aim should be to allow for a number terminating on VoIP to be recognized via digit analysis as soon as possible. This requires the information to be in the fist 7 digits maximum.

In this case the call could be routed immediately within the LEC or by the IXC to the nearest VoIP gateway. In case of E.164 numbers contained in ENUM, all such calls should be routed to the same type of gateway, namely to a gateway capable of querying ENUM (an ENUM-enabled gateway).

7.1.1 National Geographic Numbers

National geographic numbers will always be routed on the PSTN/ISDN network to the destination network. There is currently no way to find out on the PSTN (e.g. in the originating network) if the number terminates on VoIP (except with ACQ).

7.1.2 National non-geographic numbers for private networks

National non-geographic numbers for private networks will always be routed internationally to the country hosting the number. Nationally there are three options.

1. The private network has a direct connection(s) to the PSTN/ISDN which is assigned a geographic number. In this case the call will routed (e.g. via IN-translation) to the nearest connection.

2. The private network has no direct connection, but has a geographic number terminating on VoIP assigned. In this case the number is translated like in option 1 and then routed like a geographic number terminating on VoIP

3. The private network has no direct connection to the PSTN/ISDN, but has a routing number to a gateway assigned. In this case the call will be routed to the nearest VoIP-gateway capable of routing the call further on the Internet (e.g. with ENUM).

7.1.3 National non-geographic numbers for mobile networks

These numbers will always be routed to the mobile network defined by the number as defined in the national network. If the "mobile" network is using VoIP technology and is assigned a separate national destination code, the call may be routed by digit analysis directly to a VoIP gateway.

7.1.4 National non-geographic personal numbers

If number ranges assigned for personal numbers can be assumed to terminate on VoIP, the same applies as for mobile numbers. The number range may be analyzed in the originating network and routed directly to the nearest VoIP gateway.

7.1.5 Global numbers for networks

In this case the routing will be very easy, because the originating network may determine the VoIP and ENUM-enabled number by the first 5 digits (e.g. +882xx)

7.1.6 Global personal numbers

In this case the routing will be very easy, because the originating network may determine the VoIP and ENUM-enabled number by the first 5 digits (e.g. +87810)

7.1.7 User-ENUM and access codes

In case of User ENUM (see also section à) any geographic and non-geographic number for networks could in principle terminate also on the Internet as second line service, providing the national regulation authority has opted into e164.arpa.

The only question here is how a user on the PSTN may force the PSTN to make an ENUM lookup to terminate the call not on the PSTN by default.

This may be done by various ways, one could be to provide a specific access code similar to a carrier selection code to route the call to a VoIP gateway. This will be a matter of the originating PSTN network and is not discussed here any further.

T-Mobile Exhibit 1002
Part 5 of 6

7.2 ENUM Support for Routing of E.164 numbers on the Internet

On the Internet, E.164 numbers may be routed by different means. Administrative domains may have e.g. their own translation and routing tables, but in this case the calls need to be routed on the PSTN/ISDN directly to a gateway operated by this administrative domain. Examples may be PBXes connected to the PSTN or local networks based on IP technology.

To be reachable from anywhere on the Internet, a global mapping is necessary. This is provided by ENUM using the DNS. ENUM maps E.164 numbers to URIs. If a domain provides URIs for its users, a mapping from any E.164 number to the given URIs is possible.

For calls originating on the Internet it is of no difference if the E.164 number is also used on the PSTN or only on the Internet. The call is normally routed to the URI given in ENUM first.

Only if for a given number no ENUM entry or no URI pointing to a VoIP application is found, the call may be routed to the PSTN, proper connectivity provided.

7.3 Routing from Gateways and between domains with ENUM

This section needs work ú feedback requested.

This section deals with the routing between administrative domains and also with the routing from Gateways to the destination domain.

As stated above, a subscriber may have the following types of address-of-records within his domain:

sip:partial-number@acme.com
sip:+e164-number@acme.com
tel:+e164-number

Additionally he may also have as an alias an alphanumeric user(info), but this is of no concern within this document (e.g.

sip:firstname.lastname@acme.com).

Another user may enter either the full sip URI to access the user or dial within the domain by entering the private (partial) number directly. Outside the domain this private (partial) number alone is not meaningful and cannot be used, except with cross connections using access codes.

Therefore to access a user in another domain from a given domain a sip: or h323 Address-of-Record must be used. If the user does not

T-Mobile Exhibit 1002
Part 5 of 6

know Address-of-Record, or is using an IP Phone with a numeric keypad he may want to use the E.164 number instead.

If the call is coming in via a Gateway, only the E.164 number is available.

ENUM is providing a mapping from E.164 Numbers to sip: or h323: Address-of-Records, it is therefore proposed to use ENUM for the routing of these calls.

7.3.1 The administrative domain is the End User

In this case the domain has the full control over the ENUM entries. He may decide to enter only the domain of the pilot number into ENUM or to enter domains for every extension. In the latter case he may also decide to control the entries centrally by a system administrator or delegate the rights to his employees.

One ENUM entry within domain of the pilot number

There is a very simple way to implement a default routing to domains with ENUM: since all partial numbers are mapped in the same way to the domains main (pilot) E.164 number, one ENUM domain with the pilot E.164 number containing one wildcard NAPTR is sufficient.

If e.g. OeFEG has an ENUM entry for +43 1 79780, the following entry is sufficient:

```
$ORIGIN 0.8.7.9.7.1.3.4.e164.arpa.
* IN NAPTR 10 10 "u" "E2U+voice:sip"
"!^\\+4379780(.*)$!sip:\\1@sip.oefeg.at!" .
```

to route all calls dialed including the partial numbers to this domain.

ENUM entry with centralized administration

If there is a centralized administration by a system administrator there could also be only one ENUM domain for the pilot number with the following entries:

```
$ORIGIN 0.8.7.9.7.1.3.4.e164.arpa.
IN NAPTR 10 10 "u" "E2U+voice:sip" "!^.*$!sip:operator@sip.oefeg.at!"
.
IN NAPTR 10 10 "u" "E2U+email:mailto" "!^.*$!mailto:office@oefeg.at!"
.
IN NAPTR 10 10 "u" "E2U+web:http" "!^.*$!http://www.oefeg.at!" .
0 IN NAPTR 10 10 "u" "E2U+voice:sip"
"!^.*$!sip:operator@sip.oefeg.at!" .
```


T-Mobile Exhibit 1002
Part 5 of 6

```
0 IN NAPTR 10 10 "u" "E2U+email:mailto"
"!^.*$!mailto:office@oefeg.at!" .
2.3 IN NAPTR 10 10 "u" "E2U+voice:sip" "!^.*$!sip:32@sip.oefeg.at!" .
2.3 IN NAPTR 10 10 "u" "E2U+email:mailto"
"!^.*$!mailto:richard.stastny@oefeg.at!" .
etc.
```

ENUM entries with per user administration

If there is a separate administration of each partial number by the employees of the company a sub-delegation to an ENUM Tier 3 Name Server operated by the company could be done. There could either be a wildcard NS Resource Record for all sub-delegations or separate NS RR for each partial number visible from the outside.

```
$ORIGIN 0.8.7.9.7.1.3.4.e164.arpa.
IN NAPTR 10 10 "u" "E2U+voice:sip" "!^.*$!sip:operator@sip.oefeg.at!"
.
IN NAPTR 10 10 "u" "E2U+email:mailto" "!^.*$!mailto:office@oefeg.at!"
.
IN NAPTR 10 10 "u" "E2U+web:http" "!^.*$!http://www.oefeg.at!" .
* IN NS enumns1.oefeg.at.
* IN NS enumns2.oefeg.at.
oder
0 IN NS enumns1.oefeg.at.
0 IN NS enumns2.oefeg.at.
2.3 IN NS enumns1.oefeg.at.
2.3 IN NS enumns2.oefeg.at .
etc.
```

7.3.2 The administrative domain is the number range holder

If the domain is hosting full E.164 numbers, the user has the right to opt-into ENUM on his own behalf and also he may have the right to port his number out of the domain regarding the telecommunication service.

In this case all full E.164 numbers MUST be delegated directly from the ENUM Tier 1.

But consider the following example:

All numbers from the number range +8781012345 are hosted by the domain sip.nic.at

All users originally are not interested in own ENUM entries and also happy with the nic.at sip service. For all this users the first NAPTR is sufficient.

T-Mobile Exhibit 1002
Part 5 of 6

Now the user with the number +8781012345543210 wants to have an ENUM service but still provided by the ENUM Tier 2 Name Sever of nic.at. He gets the second NS RR. He may or may not leave his sip service within sip.nic.at.

The user with the E.164 number +8781012345543211 wants to have an ENUM service, but with another ENUM Tier 2 Nameserver Provider. He gets the third NS RR. He may or may not leave his sip service within nic.at.

```
$ORIGIN 5.4.3.2.1.0.1.8.7.8.e164.arpa.
* IN NAPTR 10 10 "u" "E2U+voice:sip"
"!^\\+8781012345(.*)$!sip:\\1@sip.nic.at!" .
0.1.2.3.4.5 IN NS enumns1.nic.at.
1.1.2.3.4.5 IN NS enumns1.otherprovider.net.
```

8. Security Considerations

This document deals primarily with routing of VoIP calls and other communications on the Internet using ENUM. Regarding the usage of ENUM and DNS technology see the security considerations in RFC2916bis. For more general aspects of privacy and security in the context of ENUM, see [7].

References

1 Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

2 Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

3 "The International Public Telecommunication Number Plan", ITU-T Recommendation E.164, May 1997.

4 Schulzrinne H. & Vaha-Sipila A., "The tel URI for Telephone Calls", draft-iptel-rfc2806-01.txt, (work in progress), June 2003

5 Faltstrom, P.& Mealling,M. "The E.164 to URI DDDS Applications", draft-ietf-enum-rfc2916bis-06.txt, (work in progress), May 2003

6 "International Telephone Service", ITU-T Recommendation E.105, August 1992

7 Shockey R. & Morris. J., "Privacy and Security Considerations in ENUM", draft-ietf-enum-privacy-security-01.txt, (work in progress), July 2003

Acknowledgments

Thanks to John Elwell for his comments.

Author's Addresses

Richard Stastny
OeFEG
Arsenal Objekt 24, Postbox 147
1140 Vienna
Austria
Phone: +43 664 420 4100
Email: richard.stastny@oefeg.at

Full Copyright Statement

Copyright (C) The Internet Society (2002). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

T-Mobile Exhibit 1002
Part 5 of 6

Funding for the RFC Editor function is currently provided by the Internet Society.

T-Mobile Exhibit 1002
Part 5 of 6

INFORMATION DISCLOSURE STATEMENT

Applicant	:	Johan Emil Viktor Bjorsell, et al.
App. No.	:	13/056,277
Filed	:	January 27, 2011
For	:	MOBILE GATEWAY
Examiner	:	Yao, Kwang Bin
Art Unit	:	2473
Conf. No.	:	2403

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

References and Listing

Submitted herewith in the above-identified application is an Information Disclosure Statement listing references for consideration. Copies of any listed foreign and non-patent literature references are being submitted.

Timing of Disclosure

This Information Disclosure Statement is being filed before the receipt of a first Office Action on the merits, and presumably no fee is required. If a first Office Action on the merits was mailed before the mailing date of this Statement, the Commissioner is authorized to charge the fee set forth in 37 CFR 1.17(p) to Deposit Account No. 11-1410.

Respectfully submitted,
KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 9-6-2012 By: _____

Raimond J. Salenieks
Registration No. 37,924
Agent of Record
Customer No. 20995
(858) 707-4000

13894810-sjw 083112

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/056,277
	Filing Date	January 27, 2011
	First Named Inventor	Johan Emil Viktor Bjorsell et al.
	Art Unit	2473
(Multiple sheets used when necessary)	Examiner	Kwang Bin Yao
SHEET 1 OF 1	Attorney Docket No.	SMARB19.004APC

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T^1

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T^1
	1	Supplementary European Search Report for European Application No. 07816106 dated June 18, 2012.	

13927989-sjw 090712

Examiner Signature	Date Considered
***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

T^1 - Place a check mark in this area when an English language Translation is attached.

Europäisches Patentamt
European Patent Office
Office européen des brevets

SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application Number
EP 07 81 6106

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 7 046 658 B1 (KUNDAJE VINAY [US] ET AL) 16 May 2006 (2006-05-16) * column 4, line 34 - column 10, line 28 *	1-47	INV. H04L12/66 H04L12/14 H04M11/06 H04M15/00 H04Q3/64 H04Q3/66 H04Q3/70
X	US 6 597 686 B1 (SMYK DAREK A [US]) 22 July 2003 (2003-07-22) * column 5, line 6 - column 7, line 20 *	1-47	
A	US 2005/025043 A1 (MUSSMAN HARRY [US] ET AL) 3 February 2005 (2005-02-03) * paragraph [0019] - paragraph [0053] *	1-47	
A	LIND AT&T S: "ENUM Call Flows for VoIP Interworking ; draft-lind-enum-callflows-03.txt", 20020201, no. 3, 1 February 2002 (2002-02-01), pages 1-17, XP015004214, ISSN: 0000-0004 * page 1 - page 7 *	1-47	
A	IETF ENUM WG R STASTNY OEFEG INFORMATIONAL NUMBERING FOR VOIP AND OTHER IP COMMUNICATIONS: "Numbering for VoIP and other IP Communications; draft-stastny-enum-numbering-voip-00.txt", 20031001, 1 October 2003 (2003-10-01), pages 1-43, XP015035676, ISSN: 0000-0004 * page 2 - page 14 * * page 27 - page 29 * * page 37 - page 39 *	1-47	TECHNICAL FIELDS SEARCHED (IPC) H04M

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

Place of search	Date of completion of the search	Examiner
Munich	18 June 2012	Jurca, Alexandru

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

1

EPO FORM 1503 03.82 (P04C04)

T-Mobile Exhibit 1002
Part 5 of 6

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 07 81 6106

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

18-06-2012

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7046658 B1	16-05-2006	NONE	
US 6597686 B1	22-07-2003	CA 2286338 A1	29-10-1998
		EP 0978180 A1	09-02-2000
		JP 2001500712 A	16-01-2001
		US 6597686 B1	22-07-2003
		WO 9848542 A1	29-10-1998
US 2005025043 A1	03-02-2005	US 2005025043 A1	03-02-2005
		US 2007165607 A1	19-07-2007
		US 2010157983 A1	24-06-2010
		WO 2005013541 A2	10-02-2005

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

T-Mobile Exhibit 1002
Part 5 of 6

Electronic Acknowledgement Receipt

EFS ID:	13699270
Application Number:	13056277
International Application Number:	
Confirmation Number:	2403
Title of Invention:	MOBILE GATEWAY
First Named Inventor/Applicant Name:	Johan Emil Viktor Bjorsell
Customer Number:	20995
Filer:	Raimond J Salenieks/Nino Lopez
Filer Authorized By:	Raimond J Salenieks
Attorney Docket Number:	SMARB19.004APC
Receipt Date:	10-SEP-2012
Filing Date:	27-JAN-2011
Time Stamp:	18:23:39
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		SMARB19004APC_IDS.pdf	73102 3714726defee508b18e91b13ba013b03397a9d2d	yes	2

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	1
	Information Disclosure Statement (IDS) Form (SB08)	2	2

Warnings:					
Information:					
2	Non Patent Literature	Supplementary_European_SR.pdf	64795 c399f75eb631044ea69c18b9ec7dcbabaa0b8aa3	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	137897		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

INFORMATION DISCLOSURE STATEMENT

Applicant	:	Johan Emil Viktor Bjorsell, et al.
App. No.	:	13/056,277
Filed	:	January 27, 2011
For	:	MOBILE GATEWAY
Examiner	:	Yao, Kwang Bin
Art Unit	:	2473
Conf. No.	:	2403

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

References and Listing

Submitted herewith in the above-identified application is an Information Disclosure Statement listing references for consideration. Copies of any listed foreign and non-patent literature references are being submitted.

Timing of Disclosure

This Information Disclosure Statement is being filed before the receipt of a first Office Action on the merits, and presumably no fee is required. If a first Office Action on the merits was mailed before the mailing date of this Statement, the Commissioner is authorized to charge the fee set forth in 37 CFR 1.17(p) to Deposit Account No. 11-1410.

Respectfully submitted,
KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 9-10-2012 By: _____

Raimond J. Salenieks
Registration No. 37,924
Agent of Record
Customer No. 20995
(858) 707-4000

13928002-sjw 090712

PLUS Search Results for S/N 13056277, Searched Tue Nov 20 15:47:31 EST 2012

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

4998272 99
5606699 99
5625884 99
5878261 99
6125400 99
6243668 99
6397379 99
6457023 99
6788769 99
7647629 99
20010031631 99
20050172286 99
20060135137 99
20080139186 99
20110122827 99
20120151184 99
20120151461 99
5010584 71
5187735 71
5276442 71
5373289 71
5436963 71
5479491 71
5564031 71
5590128 71
5675632 71
5734828 71
5818931 71
5835845 71
5859999 71
5884037 71
5973614 71
5974453 71
5978455 71
6055300 71
6091945 71
6102965 71
6128382 71
6154660 71
6185519 71
6192044 71
6446127 71
6496691 71
6574599 71
6671508 71
6792094 71
6829231 71
6956843 71
6996216 71
7016675 71

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/056,277
	Filing Date	January 27, 2011
	First Named Inventor	Johan Emil Viktor Bjorsell et al.
	Art Unit	2473
(Multiple sheets used when necessary)	Examiner	Kwang Bin Yao
SHEET 1 OF 1	Attorney Docket No.	SMARB19.004APC

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	1	7,055,174 B1	05-30-2006	Cope et al.	
	2	2003/0200311 A1	10-23-2003	Baum	
	3	2004/0240439 A1	12-02-2004	Castleberry et al.	
	4	2006/0072550 A1	04-06-2006	Davis et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T^1
	5	WO 01/89145 A2	11-22-2001	Telefonaktiebolaget LM Ericsson		

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T^1
	6	EPO, Supplementary European Search Report, dated November 2, 2012, Application No. 07855436.7, corresponds to U.S. Application No. 12/517,026, Attorney Docket No. SMARB19.002APC.	

14649429:djl
011113

Examiner Signature	Date Considered
***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

T^1 - Place a check mark in this area when an English language Translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	14693053
Application Number:	13056277
International Application Number:	
Confirmation Number:	2403
Title of Invention:	MOBILE GATEWAY
First Named Inventor/Applicant Name:	Johan Emil Viktor Bjorsell
Customer Number:	20995
Filer:	John M Carson/ThuyQuyen Nguyen
Filer Authorized By:	John M Carson
Attorney Docket Number:	SMARB19.004APC
Receipt Date:	14-JAN-2013
Filing Date:	27-JAN-2011
Time Stamp:	19:21:22
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	WO0189145A2.PDF	1074842 e642b7efbe177a86fa7f74fc0a134c462c07b460	no	24

Warnings:

Information:

2	Non Patent Literature	EPOextendedsdearchteport.PDF	363464 23f4a2bbe8a8d9ce8b78411429b42933a8e1ae59	no	8
Warnings:					
Information:					
3		SMARB19004APCids.pdf	92197 453830d7da03ccc4b4cde81f8a89039eea555422	yes	2

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	1
	Information Disclosure Statement (IDS) Form (SB08)	2	2

Warnings:	
Information:	
Total Files Size (in bytes):	1530503

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 November 2001 (22.11.2001)

PCT

(10) International Publication Number
WO 01/89145 A2

(51) International Patent Classification[7]: H04L 12/00

(21) International Application Number: PCT/SE01/00972

(22) International Filing Date: 4 May 2001 (04.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/570,997 15 May 2000 (15.05.2000) US

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventor: **FOTI, Georges**; 163 Mozart, Dollard des Ormeaux, Quebec H9G 2Z8 (CA).

(74) Agent: **MAGNUSSON, Monica**; Ericsson Radio Systems AB, Patent Unit Radio Access, S-164 80 Stockholm (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/89145 A2

(54) Title: METHOD OF MONITORING CALLS IN AN INTERNET PROTOCOL (IP)-BASED NETWORK

(57) Abstract: A method of monitoring a call with a mobile terminal (MT) (11) in an Internet Protocol (IP)-based network (10) having a Gatekeeper (17) that controls the network, a plurality of access routers (12, 14) that provide access to the network, and a Monitoring Station (18) having monitoring facilities and a database of MTs to be monitored. When the MT sends an Admission Request message (21) to the Gatekeeper, the Gatekeeper sends a query (23) to the Monitoring Station asking whether the MT is to be monitored. The Monitoring Station sends a reply (25) to the Gatekeeper indicating that the MT is to be monitored and providing an IP address where monitored packets are to be sent. The Gatekeeper then sends a monitoring request message (28) to the access router (12) associated with the MT. The request identifies the MT to be monitored, instructs the access router to monitor the MT, and provides a unique call identification (Call ID) and the IP address where monitored packets are to be sent. When the access router detects a packet associated with the MT, the router sends all packets associated with the MT to the Monitoring Station. The method also controls monitoring during intra-domain and inter-domain handoffs of the MT.

T-Mobile Exhibit 1002
Part 5 of 6

METHOD OF MONITORING CALLS IN AN INTERNET PROTOCOL (IP)-BASED NETWORK

BACKGROUND OF THE INVENTION

Technical Field of the Invention

This invention relates to telecommunication systems and, more particularly, to a method of monitoring calls in an Internet Protocol (IP)-based network.

Description of Related Art

In existing circuit-switched telecommunications networks such as the Public Switched Telephone Network (PSTN) and the legacy Public Land Mobile Network (PLMN), law enforcement agencies are able to easily monitor telephone calls because the calls, once established, are routed over a dedicated path from one subscriber to another. In an IP-based telecommunications network, this is not the case.

For IP calls that originate in a circuit-switched network, a gateway provides an interface between the circuit-switched network and the packet-switched IP network. The gateway takes bits of digitized voice, packetizes them, puts on a header, and ships them over the IP network. The packetized call may enter the core IP network at any access (edge) router near the originating subscriber. Thereafter, the individual packets follow any available route to the destination address. At that point, all of the packets exit the core network through a single access router near the destination subscriber. The same principle applies if both the calling terminal and the called terminal are IP-based. Since one or both of the subscribers involved in the call may be mobile, calls between the same subscribers may enter and leave the IP network through different access routers at different times. As a result of the changing access routers and the independent routing of the packets in the IP network, law enforcement agencies are not able to monitor real-time IP applications such as Voice-over-IP (VoIP) calls.

It would be advantageous to have a method of monitoring calls in an Internet Protocol (IP)-based network. The present invention provides such a method.

T-Mobile Exhibit 1002
Part 5 of 6

SUMMARY OF THE INVENTION

In one aspect, the present invention is a method of monitoring a call from a mobile terminal (MT) in an IP-based network having a Gatekeeper that controls the network, a plurality of access routers that provide access to the network, and a Monitoring Station having monitoring facilities and a database of MTs to be monitored. The method includes the steps of sending an access request from the MT to the Gatekeeper, sending a query from the Gatekeeper to the Monitoring Station asking whether the MT is to be monitored, and sending a reply from the Monitoring Station to the Gatekeeper indicating that the MT is to be monitored and providing an IP address where monitored packets are to be sent. This is followed by sending a monitoring request from the Gatekeeper to the access router associated with the monitored MT, the request identifying the MT to be monitored, instructing the access router to monitor the MT, and providing the IP address where monitored packets are to be sent. When the access router detects a packet associated with the MT, the router sends all packets associated with the MT to the Monitoring Station.

When the monitored MT is handed off from a first base station to a second base station, and each of the base stations is controlled by a single Radio Network Controller (RNC), the RNC sends a monitoring request to the second base station. The monitoring request identifies the MT to be monitored, instructs the second base station to monitor the MT, and provides a unique call identification (Call ID) and the IP address where monitored packets are to be sent. The unique Call ID is assigned by the Gatekeeper. The RNC also sends a notification to the Gatekeeper that the MT is being served by the second base station, and includes the unique Call ID and a new transport address for the MT, if any.

When the monitored MT is handed off from a first base station controlled by a first RNC to a second base station controlled by a second RNC, and both RNCs are in a single Gatekeeper domain, the method performs the steps of sending identifying information regarding the MT being monitored from the first RNC to the second RNC, and sending a monitoring request from the second RNC to the second base station, the request identifying the MT to be monitored, instructing the second base station to monitor the MT, and providing the unique Call ID and the IP address where monitored

packets are to be sent. The second RNC also sends a notification to the Gatekeeper that the MT is being served by the second base station, and includes the Call ID and the new transport address for the MT. Whenever there is a change to the transport address of the MT, the Gatekeeper forwards the Call ID and the new transport address to the Monitoring Station.

When the monitored MT is handed off from a first base station controlled by a first RNC in a first Gatekeeper domain, to a second base station controlled by a second RNC in a second Gatekeeper domain, the method performs the steps of sending a notification from the first RNC to the second RNC that the MT is being monitored, and sending a monitoring request from the second RNC to the second base station. The monitoring request identifies the MT to be monitored, instructs the base station to monitor the MT, and provides the unique Call ID and the IP address of a Monitoring Station where monitored packets are to be sent. The second base station then begins sending media packets having the MT address as a source address or destination address to the Monitoring Station. Then, the second RNC sends the unique Call ID it received and a new transport address for the MT to the second Gatekeeper. The second Gatekeeper forwards this information to the Monitoring Station. This is followed by sending an access request from the MT to the second Gatekeeper, and allocating bandwidth to the MT by the Gatekeeper.

In another aspect, the present invention is a method performed within a Gatekeeper in an IP-based network. The method monitors a call from an MT and routes the monitored call to a Monitoring Station having monitoring facilities and a database of MTs to be monitored. The method includes the steps of receiving in the Gatekeeper, a network access request from the MT, sending a query from the Gatekeeper to the Monitoring Station asking whether the MT is to be monitored, and receiving in the Gatekeeper, a reply from the Monitoring Station indicating that the MT is to be monitored and providing an IP address where monitored packets are to be sent. This is followed by sending a monitoring request from the Gatekeeper to the access router that is associated with the monitored MT and is providing access to the network. The request identifies the MT to be monitored, instructs the access router

to send any packets associated with the MT to the Monitoring Station, and provides the unique Call ID and the IP address where monitored packets are to be sent.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be better understood and its numerous objects and advantages will become more apparent to those skilled in the art by reference to the following drawings, in conjunction with the accompanying specification, in which:

FIG. 1 is an illustrative drawing of an IP network modified in accordance with the teachings of the present invention to monitor a call between two IP terminals;

FIG. 2 is a message flow diagram illustrating the flow of messages when setting up a call for monitoring in the IP network of FIG. 1 in accordance with the teachings of the present invention;

FIG. 3 is an illustrative drawing of an IP network modified in accordance with the teachings of the present invention to monitor a call between an IP terminal and a terminal in the Public Switched Telephone Network (PSTN);

FIG. 4 is a message flow diagram illustrating the flow of messages when a monitored mobile terminal is handed off from an old base station to a new base station controlled by the same Radio Network Controller (RNC) as the old base station;

FIG. 5 is a message flow diagram illustrating the flow of messages when a monitored mobile terminal roams into a new subnet within the same domain, and acquires a new RNC, a new base station, and a new transport address; and

FIG. 6 is a message flow diagram illustrating the flow of messages when the mobile terminal roams into a new domain and acquires a new Gatekeeper, a new RNC, a new base station, and a new transport address.

DETAILED DESCRIPTION OF EMBODIMENTS

The present invention is described herein primarily in terms of the International Telecommunications Union (ITU) H.323 protocol, but is equally applicable to both H.323 and the Session Initiation Protocol (SIP) developed by the Internet Engineering Task Force (IETF). In particular, the term "Gatekeeper" which

is used herein refers to both an H.323 Gatekeeper and a SIP proxy server and registry. In addition, reference to an H.245 address herein also refers to a SIP address.

In a typical IP network, PC clients or IP telephony terminals (fixed or mobile) are identified and addressed by an e-mail address (proxy/alias), or an IP address, or both. Prior to making any calls, such terminals register with a Gatekeeper in an H.323 network, or with a SIP proxy server in a SIP network. If the registration is accepted by the Gatekeeper, the Gatekeeper handles incoming calls to the terminal as well as outgoing calls from the terminal. The Gatekeeper maintains a subscriber profile that includes, among other things, the services to which the subscriber is entitled. For simplicity, the term "mobile terminal (MT)" is used herein to refer generically to IP clients, both fixed and mobile since the most challenging monitoring tasks involve intra-domain and inter-domain handoff of MTs.

FIG. 1 is an illustrative drawing of an IP network 10 modified in accordance with the teachings of the present invention to monitor a call between two IP terminals. IP Terminal-1 11, which may be originating a call, is connected to the IP network through Access Router-1 12. Media traffic (i.e., data) 13 is carried by independent paths through the network to Access Router-2 14 through which IP Terminal-2 15 has accessed the network. IP Terminal-2 may be the terminating (destination) terminal. Control signaling between the two subscribers is carried in a control plane 16 which passes through a Gatekeeper 17, and from the Gatekeeper to a Monitoring Station 18 which may be operated by a law enforcement agency.

In order for the two IP subscribers 11 and 15 to communicate over the IP-based network 10, they have to go through the Gatekeeper 17 which can be likened to a mobile switching center (MSC) in a circuit-switched network. The Gatekeeper is the brain of the network regarding the routing of calls. The Gatekeeper manages the bandwidth (with the help of other network entities), generates the accounting data, etc.

In a first scenario, the calling and called subscribers are within the same domain. In that case, when a subscriber wants to make or receive a call, an Admission Request (ARQ) message (when using H.323) is sent to the Gatekeeper. In response to the ARQ message, the Gatekeeper allocates the bandwidth for the call or, if none is available, the Gatekeeper denies the call. The present invention extends the

procedure performed by the Gatekeeper when a bandwidth allocation request (i.e., ARQ) is received from a device that is originating or receiving a call. Additionally, new mandatory parameters are introduced in the ARQ message.

The Gatekeeper does not know which subscribers need to be monitored. Only the law enforcement Monitoring Station has this information. The Monitoring Station includes a database of all subscribers who should be monitored for security reasons. So for each call that is originated by or terminated to a subscriber in its domain, the Gatekeeper queries the Monitoring Station to determine whether the subscriber should be monitored.

FIG. 2 is a message flow diagram illustrating the flow of messages when setting up a call for monitoring in the IP network of FIG. 1 in accordance with the teachings of the present invention. In the illustrated example, IP Terminal-1 11 is the subscriber to be monitored. After Terminal-1 sends an ARQ message 21 to the Gatekeeper 17, the Gatekeeper performs the bandwidth allocation function at 22, and then sends a monitor query message 23 to the Monitoring Station 18. The monitor query message includes the H.245 source address and the H.245 destination address for the call, if available, as well as subscriber addressing information (e-mail/proxy) and the unique Call ID that it generates for the call. The Monitoring Station checks the database at 24 and returns a monitor reply message 25 to the Gatekeeper indicating whether any of the parties in the call should be monitored, as well as the IP address of the Monitoring Station to which the monitored conversation should be sent. In the illustrated example, the message indicates that Terminal-1 is to be monitored. If none of the terminals is being monitored, the Gatekeeper then returns an Admission Confirm (ACF) message 26 to Terminal-1. If any of the subscribers is being monitored, the Gatekeeper sets a flag in the subscriber record at 27 indicating that fact.

The Gatekeeper finds, through normal IP routing protocols, the path for the media to follow. The Gatekeeper obtains this information in the course of allocating bandwidth since the policy related to the QoS of the call must be downloaded to all of the routers in the media path. The routers, in this case, act as policy enforcement points to ensure that the subscribers are respecting the QoS agreements. However, for

the sake of monitoring, it suffices that the Gatekeeper identifies only the access router associated with IP Terminal-1.

Hence, the Gatekeeper is able to identify the access router for this call. The Gatekeeper then sends a Monitoring Request message 28 to the access router associated with the subscriber (for example, Access Router-1), and includes the Monitoring Station IP address and the unique Call ID for that call. Access Router-1 sends back an Acknowledgment message 29. Once the Gatekeeper receives the Acknowledgment message from the Access Router, the Gatekeeper sends an ACF message 31 to Terminal-1.

It should also be noted that in IP networks, addressing is different in each media direction. Therefore, the IP address to be monitored is the source address in the IP header while the monitored subscriber is initiating the conversation, and is the destination field in the IP header while the monitored subscriber is listening. Thus, while the Access Router performs its normal routing functions, it has to monitor both the source and the destination addresses in the IP headers that it handles in order to identify addresses that match the monitored address. Media packets then begin to flow from the IP Terminal to Access Router-1 at 32, and Access Router-1 sends the packets to the Monitoring Station at 33.

To send media packets to the Monitoring Station, the Access Router encapsulates every identified packet with a new header that includes the router's address as the source address, and the Monitoring Station's address as the destination address. The unique Call ID is also included in the IP header. This enables the Monitoring Station to correlate packets belonging to the same conversation. Other parameters may be included in the header as well. Upon receipt, the Monitoring Station strips away the header and recovers the original packets. When the call is cleared, the connection from the access router to the Monitoring Station is also cleared.

In another scenario, the calling and called subscribers are in different domains. In that case, two different Gatekeepers must deal with the calling and called subscribers. Additional information must be exchanged between the Gatekeepers as

part of the call setup for the management and coordination of monitoring a call. Otherwise, both Gatekeepers may end up monitoring the same call.

In this scenario, the originating Gatekeeper will likely not know the IP address of the destination. Thus, the originating Gatekeeper follows the same procedure previously described. However, the query that the originating Gatekeeper sends to the Monitoring Station includes only the calling subscriber identity. If the calling subscriber is not the one being monitored, then the originating Gatekeeper returns an ACF message and proceeds with normal call setup. During the setup, the originating Gatekeeper forwards to the Gatekeeper that deals with the destination terminal, a special flag informing the destination Gatekeeper that the calling subscriber is not the one being monitored. The destination Gatekeeper follows the previously described procedure, including the monitoring procedure, when the called terminal sends an ARQ message to accept the incoming call.

On the other hand, if the calling subscriber is the one being monitored, the originating Gatekeeper follows the same procedure described previously when it receives an ARQ message from the calling subscriber. The originating Gatekeeper then sends a flag to the destination Gatekeeper identifying the calling subscriber as a subscriber to be monitored. The destination Gatekeeper follows the same procedure previously described when the called terminal sends an ARQ message to accept the call, but bypasses the monitoring procedure.

It should also be noted that in this scenario, the originating Gatekeeper receives only the destination IP address as part of the call setup procedure. Therefore, the originating Gatekeeper must send a second Monitoring Request Message to the Access Router to convey the destination IP address.

FIG. 3 is an illustrative drawing of an IP network 20 modified in accordance with the teachings of the present invention to monitor a call between an IP terminal (IP Terminal-3) 41 and a terminal in a circuit-switched network (PSTN Terminal) 42 such as the Public Switched Telephone Network (PSTN) 43. If the subscriber to be monitored is in a circuit-switched network such as the PSTN, the call goes through a Gateway 44 to the IP subscriber in the IP network. If the subscriber to be monitored is on the PSTN side, then existing procedures in the PSTN ensure that monitoring

takes place. However, if the subscriber to be monitored is on the IP side, the procedure described previously is invoked when the called subscriber (to be monitored) sends an ARQ message to the Gatekeeper to accept an incoming call.

Again in this case, coordination is needed to ensure that no double monitoring occurs when both subscribers are to be monitored. Therefore, for an H.323 endpoint of the gateway type (as opposed to a terminal type of endpoint), the ARQ message sent to the Gatekeeper from the Gateway 44 includes a flag to indicate whether an incoming call is already being monitored from the PSTN side. The Gatekeeper then bypasses the monitoring procedure. The PSTN, of course, must convey this information to the Gateway so that it can be passed to the Gatekeeper. In one embodiment, Integrated Services User Part (ISUP) signaling is extended to carry this information. Optionally, specialized control messages can convey the information to the Gateway from the entity that is coordinating the monitoring in the PSTN. In all cases, the globally unique Call ID must be transferred to uniquely identify the impacted call.

Mobility/Handoff Scenarios

Mobility adds another level of complexity to the task of IP monitoring due to the potential changing of the point of attachment of the MT to the network. In this case, the base stations serve as Access Routers since they are the closest point of attachment to the subscriber. However, Gatekeepers do not communicate directly with base stations since base stations belong to the Radio Access Network (RAN). Therefore, the Gatekeepers must go through the Radio Network Controller/Base Station Controller (RNC/BSC) that controls these base stations for all requests to the base stations regarding the monitoring of subscribers.

Therefore, the same procedures described above for monitoring fixed subscribers still apply for mobile subscribers except that all Gatekeeper requests that are sent directly to the Access Routers for fixed subscribers, are sent instead to the RNC. The RNC, in turn, sends them to the base stations.

FIG. 4 is a message flow diagram illustrating the flow of messages when the monitored mobile terminal (MT) is handed off from an old base station (BS-1) 51 to a new base station (BS-2) 52 controlled by the same RNC 53 as the old base station.

When the MT does not change its transport address, but roams in a new base station, the link layer in the base station ensures delivery of the call to the MT. After handoff occurs at 54, the RNC instructs BS-2 to monitor the subscriber at 55 and includes the address of the Monitoring Station and the unique Call ID. The RNC then informs the Gatekeeper 17 of the new base station at 56, and includes the unique Call ID to identify the impacted call. If there is a change in the transport address of the mobile terminal as a result of the handoff, the new address is also sent to the Gatekeeper by the RNC. The RNC learns the new address during the handoff procedure. In the preferred embodiment, this information is passed only for monitored subscribers in order to minimize the signaling load. At 57, the Gatekeeper forwards the Call ID and the new transport address, if any, to the Monitoring Station 18. At 58, media is passed from BS-2 to the Monitoring Station.

FIG. 5 is a message flow diagram illustrating the flow of messages when the monitored MT is handed off from an old base station (BS-1) 61 controlled by an old RNC (RNC-1) 62 to a new base station (BS-3) 63 controlled by a new RNC (RNC-2) 64 within the same Gatekeeper domain. Thus, in this scenario, the MT roams into a new subnet within the same domain, and acquires a new RNC, a new base station, and a new transport address. At 65, the MT is handed off from BS-1 to BS-3. At 66, RNC-1 forwards to RNC-2 all of the pertinent information regarding the subscriber being monitored, including the unique Call ID for the call being monitored. At 67, the new RNC (RNC-2) instructs the new base station (BS-3) to monitor the subscriber, and includes the unique Call ID and the address of the Monitoring Station.

Since the mobile terminal changed transport addresses, it is required to register its new transport address with the Gatekeeper 17. Therefore, at 68, RNC-2 informs the Gatekeeper of the new base station and the new transport address assigned to the mobile terminal. The unique Call ID is also included. At 69, the new transport address and the Call ID are passed by the Gatekeeper to the Monitoring Station 18 so that all the packets belonging to the same monitored call can be correlated. Thereafter, media packets are forwarded from BS-3 to the Monitoring Station at 70.

FIG. 6 is a message flow diagram illustrating the flow of messages when the mobile terminal roams into a new domain and acquires a new Gatekeeper, a new RNC,

a new base station, and a new transport address. The monitored MT 71 is initially operating in IP Network-1 which includes Gatekeeper-1 72. RNC-1 73 and BS-1 74 are in RAN-1 which provides radio access for IP Network-1. At handoff 75, the monitored MT is handed off from BS-1 to a new base station (BS-2) 76 controlled by a new RNC (RNC-2) 77. RNC-2 and BS-2 are in RAN-2 which provides radio access for IP Network-2 which includes Gatekeeper-2 78. Monitoring Station 18 is monitoring the call with the MT.

At 79, the new RNC (RNC-2) is informed by RNC-1 that the MT is being monitored. At 81, the RNC-2 instructs the new base station (BS-2) to monitor the subscriber, and includes the unique Call ID and the address of the Monitoring Station. Media then begins to flow from BS-2 to the Monitoring Station at 82. RNC-2 then informs Gatekeeper-2 at 83 that a new subscriber is now roaming in its service area, and that the new subscriber needs to be monitored. RNC-2 includes the IMSI for the MT, the unique Call ID, and the MT's new transport address in the message to Gatekeeper-2. Every time there is a change in the transport address of a monitored mobile terminal, the controlling Gatekeeper must inform the Monitoring Station of the new transport address. Thus, at 84, the new transport address and the Call ID are passed to the Monitoring Station. The unique Call ID is used by the Monitoring Station to track all packets belonging to the same conversation. In addition, the Call ID is used by any Gatekeeper that handles a portion of the call (other than the original Gatekeeper) to report the same call to the Monitoring Station. Thus, during a handoff scenario, the RNC passes the Call ID to the same Gatekeeper if there is no change of domain, and to the new Gatekeeper when there is a change of domain.

At 85, Gatekeeper-2 sets a flag in the subscriber record for MT 71 indicating that the MT is in its area and is being monitored. The flag also indicates that a subscriber will soon have to register with his transport address. Since the MT changed its transport address, the MT is required to register with the new Gatekeeper and report its new transport address. A registration timer is started when the flag is set in case the registration never arrives (registration is lost, subscriber hangs up, etc.).

At 86, an ARQ message is sent from the MT to Gatekeeper-2. When the ARQ arrives, the registration timer in Gatekeeper-2 is stopped at 87, and bandwidth is

allocated. Gatekeeper-2 then returns an ACF message 88 to the MT. Gatekeeper-2 knows that the MT is being monitored because Gatekeeper-2 was informed by RNC-2. Therefore, Gatekeeper-2 does not perform the monitoring procedure associated with the new registration. Thus, double monitoring of the conversation is avoided.

Whenever any monitored subscriber hangs up, a De-Admission Request is sent to the Gatekeeper. The Gatekeeper clears the flag for monitoring the subscriber and sends a message to the Monitoring Station to stop the monitoring of the call. This message is also propagated to the Access Router performing the monitoring.

It is thus believed that the operation and construction of the present invention will be apparent from the foregoing description. While the method shown and described has been characterized as being preferred, it will be readily apparent that various changes and modifications could be made therein without departing from the scope of the invention as defined in the following claims.

WHAT IS CLAIMED IS:

1. A method of monitoring a call with an Internet Protocol (IP) client in an IP-based network having a Gatekeeper that controls the network, a plurality of access routers that provide access to the network, and a Monitoring Station having monitoring facilities and a database of IP clients to be monitored, said method comprising:

sending an access request from the IP client to the Gatekeeper;

sending a query from the Gatekeeper to the Monitoring Station asking whether the IP client is to be monitored;

sending a reply from the Monitoring Station to the Gatekeeper indicating that the IP client is to be monitored and providing an IP address where monitored packets are to be sent;

sending a monitoring request from the Gatekeeper to an access router associated with the IP client, said request identifying the IP client to be monitored, instructing the access router to monitor the IP client, and providing the IP address where monitored packets are to be sent;

detecting by the access router, a packet associated with the IP client; and

routing by the access router, all packets associated with the IP client to the Monitoring Station.

2. The method of monitoring a call with an IP client in an IP-based network of claim 1 further comprising, before the step of sending a query from the Gatekeeper to the Monitoring Station asking whether the IP client is to be monitored, the step of performing bandwidth allocation functions by the Gatekeeper to determine whether network access can be granted to the IP client.

3. The method of monitoring a call with an IP client in an IP-based network of claim 2 further comprising, after the step of sending a reply from the Monitoring Station to the Gatekeeper indicating that the IP client is to be monitored,

the step of setting a flag in the Gatekeeper identifying the IP client as a monitored IP client.

4. The method of monitoring a call with an IP client in an IP-based network of claim 3 further comprising, after the step of sending a monitoring request from the Gatekeeper to the access router, the steps of:

sending an acknowledgment message from the access router to the Gatekeeper; and

sending an admission confirm message from the Gatekeeper to the IP client when the acknowledgment message has been received from the access router.

5. The method of monitoring a call with an IP client in an IP-based network of claim 4 wherein the step of detecting a packet associated with the IP client includes detecting a packet that has the IP client as its source address.

6. The method of monitoring a call with an IP client in an IP-based network of claim 4 wherein the step of detecting a packet associated with the IP client includes detecting a packet that has the IP client as its destination address.

7. The method of monitoring a call with an IP client in an IP-based network of claim 3 further comprising the steps of:

sending a de-admission request from the IP client to the Gatekeeper;

clearing the flag in the Gatekeeper that identifies the IP client as a monitored IP client;

sending a message from the Gatekeeper to the Monitoring Station to stop the monitoring of the call; and

sending a message from the Gatekeeper to the access router to stop the routing of packets to the Monitoring Station.

8. The method of monitoring a call with an IP client in an IP-based network of claim 1 wherein the IP client is a mobile terminal (MT), and the method further comprises the steps of:

handing off the MT from a first base station to a second base station, each of said base stations being controlled by a single radio network controller (RNC);

sending a monitoring request from the RNC to the second base station, said request identifying the MT to be monitored, instructing the second base station to monitor the MT, and providing a unique call identification (Call ID) and the IP address where monitored packets are to be sent; and

sending a notification from the RNC to the Gatekeeper that the MT is being served by the second base station, said notification including the unique Call ID and a new transport address for the MT.

9. The method of monitoring a call with an IP client in an IP-based network of claim 8 further comprising sending the Call ID and the new transport address from the Gatekeeper to the Monitoring Station.

10. The method of monitoring a call with an IP client in an IP-based network of claim 1 wherein the IP client is a mobile terminal (MT), and the method further comprises the steps of:

handing off the MT from a first base station to a second base station, the first base station being controlled by a first radio network controller (RNC), and the second base station being controlled by a second RNC, and both RNCs being in a single Gatekeeper domain;

sending identifying information regarding the MT being monitored from the first RNC to the second RNC, said information including a unique call identification (Call ID);

sending a monitoring request from the second RNC to the second base station, said request identifying the MT to be monitored, instructing the second base station to monitor the MT, and providing the unique Call ID and the IP address where monitored packets are to be sent;

sending a notification from the second RNC to the Gatekeeper that the MT is being served by the second base station, said notification including the unique Call ID and a new transport address for the MT; and

sending the Call ID and the new transport address from the Gatekeeper to the Monitoring Station.

11. The method of monitoring a call with an IP client in an IP-based network of claim 1 wherein the step of detecting a packet associated with the IP client includes detecting a media having the IP client address as either a source address or destination address.

12. The method of monitoring a call with an IP client of claim 11 wherein the step of routing all packets associated with the IP client to the Monitoring Station includes encapsulating each packet associated with the IP client with a new header that includes the router's address as a source address, and the Monitoring Station's address as a destination address.

13. A method of handing off a monitored mobile terminal (MT) in an Internet Protocol (IP)-based network, said method comprising:

handing off the MT from a first base station to a second base station, the first base station being controlled by a first radio network controller (RNC) in a first Gatekeeper domain, and the second base station being controlled by a second RNC in a second Gatekeeper domain,

sending a notification from the first RNC to the second RNC that the MT is being monitored, said notification including a unique call identification (Call ID) and an IP address of a Monitoring Station where monitored packets are to be sent;

sending a monitoring request from the second RNC to the second base station, said request identifying the MT to be monitored, instructing the base station to monitor the MT, and providing the Call ID and the IP address of the Monitoring Station;

sending by the second base station, media packets having the MT address as a source address or destination address to the Monitoring Station;

sending the unique Call ID and a new transport address for the MT from the second RNC to the second Gatekeeper;

sending the unique Call ID and the new transport address for the MT from the second Gatekeeper to the Monitoring Station;

sending an access request from the MT to the second Gatekeeper; and

allocating bandwidth to the MT by the Gatekeeper.

14. The method of handing off a monitored MT in an IP-based network of claim 13 further comprising, after the step of sending a unique Call ID and a new transport address for the MT from the second RNC to the second Gatekeeper and to the Monitoring Station, the steps of:

setting a flag in the second Gatekeeper indicating that a monitored MT is in the second Gatekeeper's area, and that the MT will soon register with the second Gatekeeper; and

starting a registration timer in the second Gatekeeper.

15. The method of handing off a monitored MT in an IP-based network of claim 14 further comprising the steps of:

sending a de-admission request from the monitored MT to the second Gatekeeper;

clearing the flag in the second Gatekeeper that identifies the MT as a monitored MT;

sending a message from the second Gatekeeper to the Monitoring Station to stop the monitoring of the call; and

sending a message from the second Gatekeeper to the second base station to stop the routing of packets to the Monitoring Station.

16. The method of handing off a monitored MT in an IP-based network of claim 13 further comprising, after the step of sending an access request from the MT to the second Gatekeeper, the step of stopping the registration timer.

17. The method of handing off a monitored MT in an IP-based network of claim 13 wherein the step of sending media packets having the MT address as a source address or destination address to the Monitoring Station includes encapsulating each packet associated with the MT with a new header that includes the second base station's address as a source address, and the Monitoring Station's address as a destination address.

18. A method of monitoring a call with a mobile terminal (MT) and routing the monitored call to a Monitoring Station having monitoring facilities and a database of MTs to be monitored, said method being performed within a Gatekeeper in an Internet Protocol (IP)-based network, and comprising the steps of:

receiving in the Gatekeeper, a network access request from the MT;

sending a query from the Gatekeeper to the Monitoring Station asking whether the MT is to be monitored;

receiving in the Gatekeeper, a reply from the Monitoring Station indicating that the MT is to be monitored and providing an IP address where monitored packets are to be sent; and

sending a monitoring request from the Gatekeeper to an access router providing the MT with access to the network, said request identifying the MT to be monitored, instructing the access router to send any packets associated with the MT to the Monitoring Station, and providing a unique call identification (Call ID) and the IP address where monitored packets are to be sent.

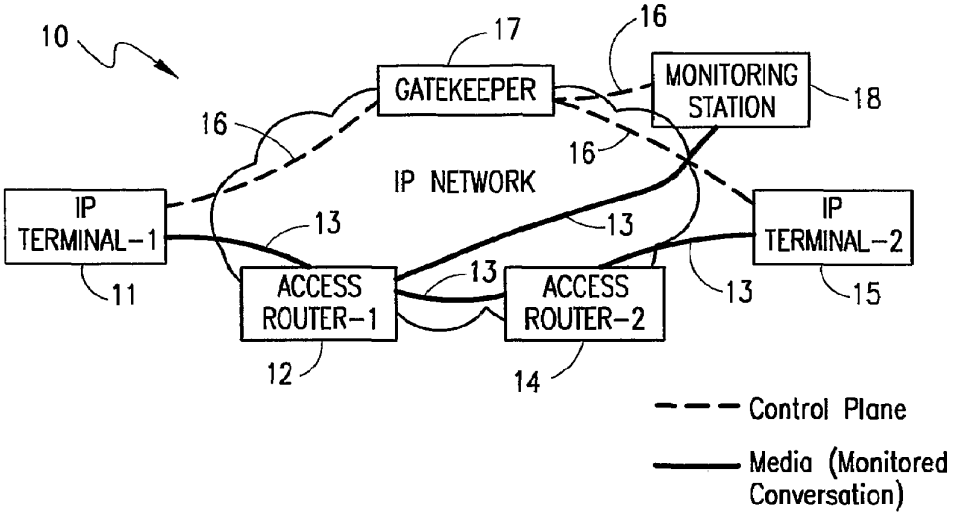

10
17
16
GATEKEEPER
MONITORING STATION
18
16
16
IP NETWORK
IP TERMINAL-1
13
13
IP TERMINAL-2
13
13
ACCESS ROUTER-1
ACCESS ROUTER-2
11
12
14
15
Control Plane
Media (Monitored Conversation)

FIG. 1

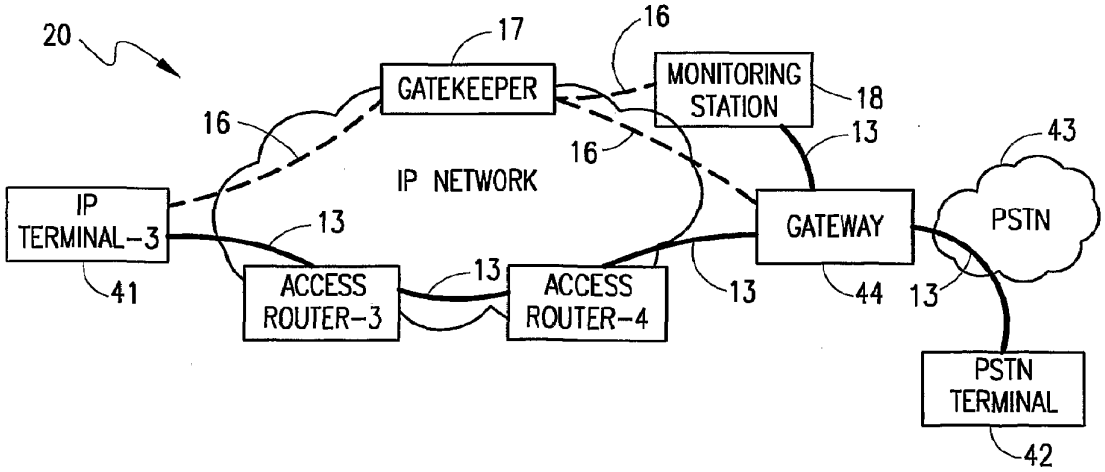

20
17
16
GATEKEEPER
MONITORING STATION
18
16
16
13
43
IP NETWORK
IP TERMINAL-3
13
GATEWAY
PSTN
ACCESS ROUTER-3
13
ACCESS ROUTER-4
13
13
41
44
PSTN TERMINAL
42
Control Plane
Media (Monitored Conversation)

FIG. 3

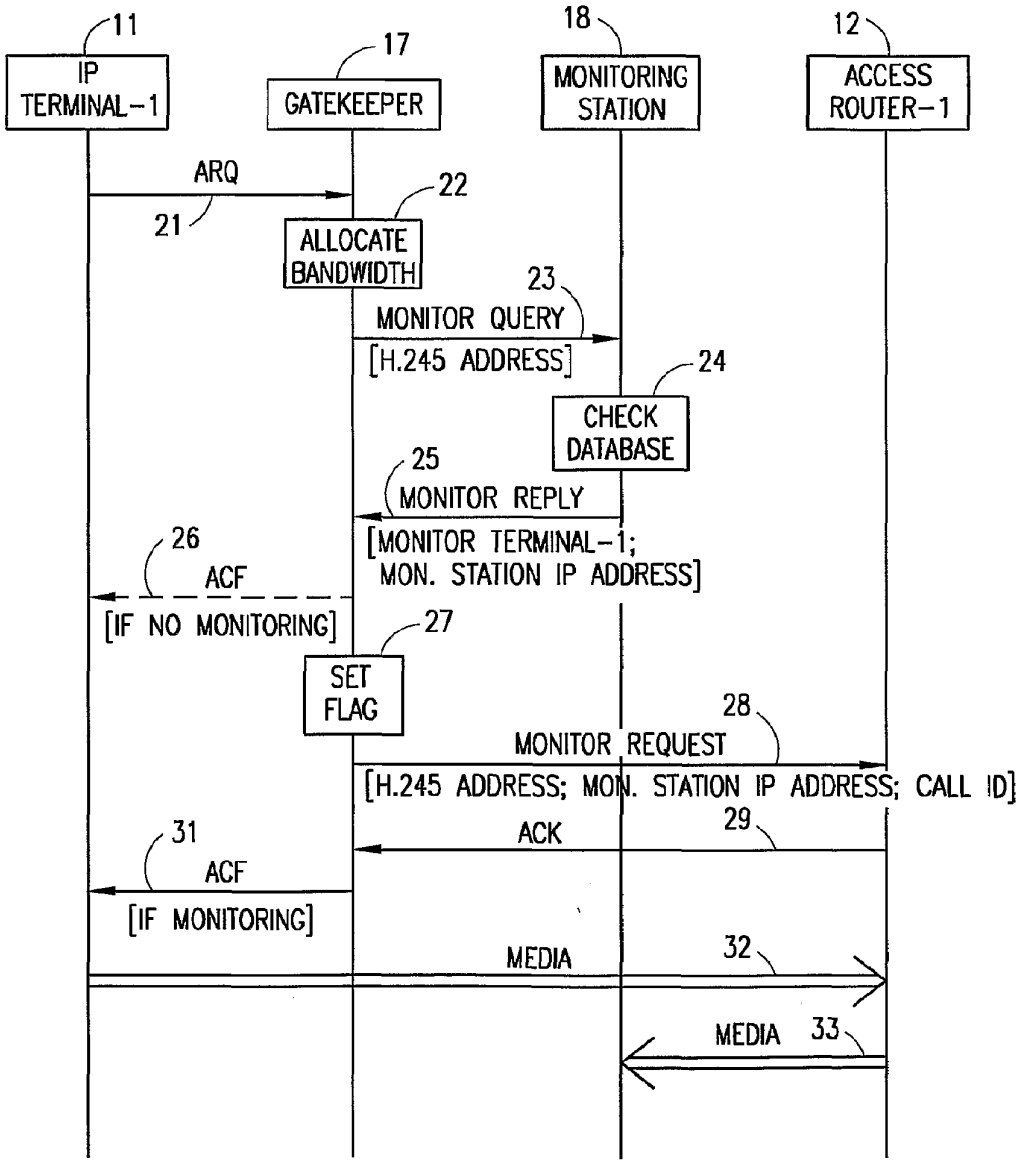

11
IP TERMINAL-1
17
GATEKEEPER
18
MONITORING STATION
12
ACCESS ROUTER-1
ARQ
21
22
ALLOCATE BANDWIDTH
23
MONITOR QUERY
[H.245 ADDRESS]
24
CHECK DATABASE
25
MONITOR REPLY
[MONITOR TERMINAL-1; MON. STATION IP ADDRESS]
26
ACF
[IF NO MONITORING]
27
SET FLAG
28
MONITOR REQUEST
[H.245 ADDRESS; MON. STATION IP ADDRESS; CALL ID]
ACK
29
31
ACF
[IF MONITORING]
MEDIA
32
MEDIA
33

FIG. 2

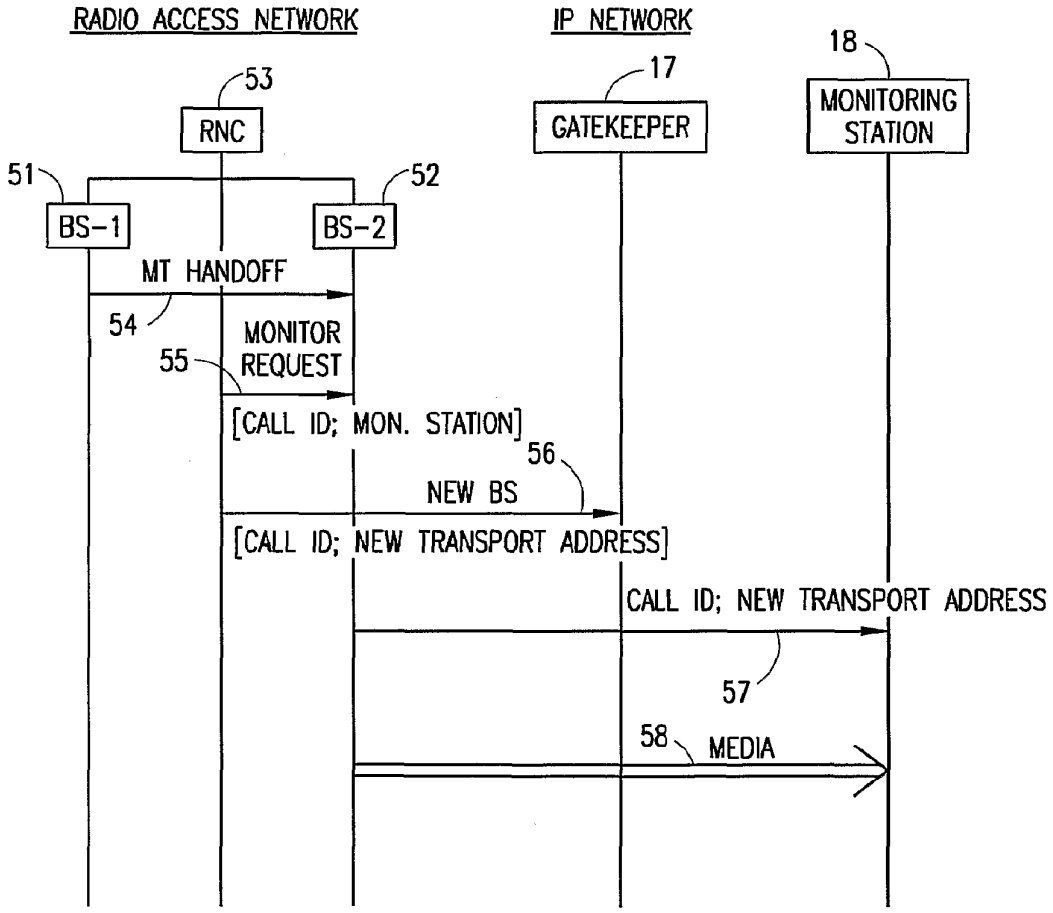

RADIO ACCESS NETWORK
IP NETWORK
18
17
53
MONITORING STATION
GATEKEEPER
RNC
51
52
BS-1
BS-2
MT HANDOFF
54
MONITOR REQUEST
55
[CALL ID; MON. STATION]
56
NEW BS
[CALL ID; NEW TRANSPORT ADDRESS]
CALL ID; NEW TRANSPORT ADDRESS
57
58
MEDIA

FIG. 4

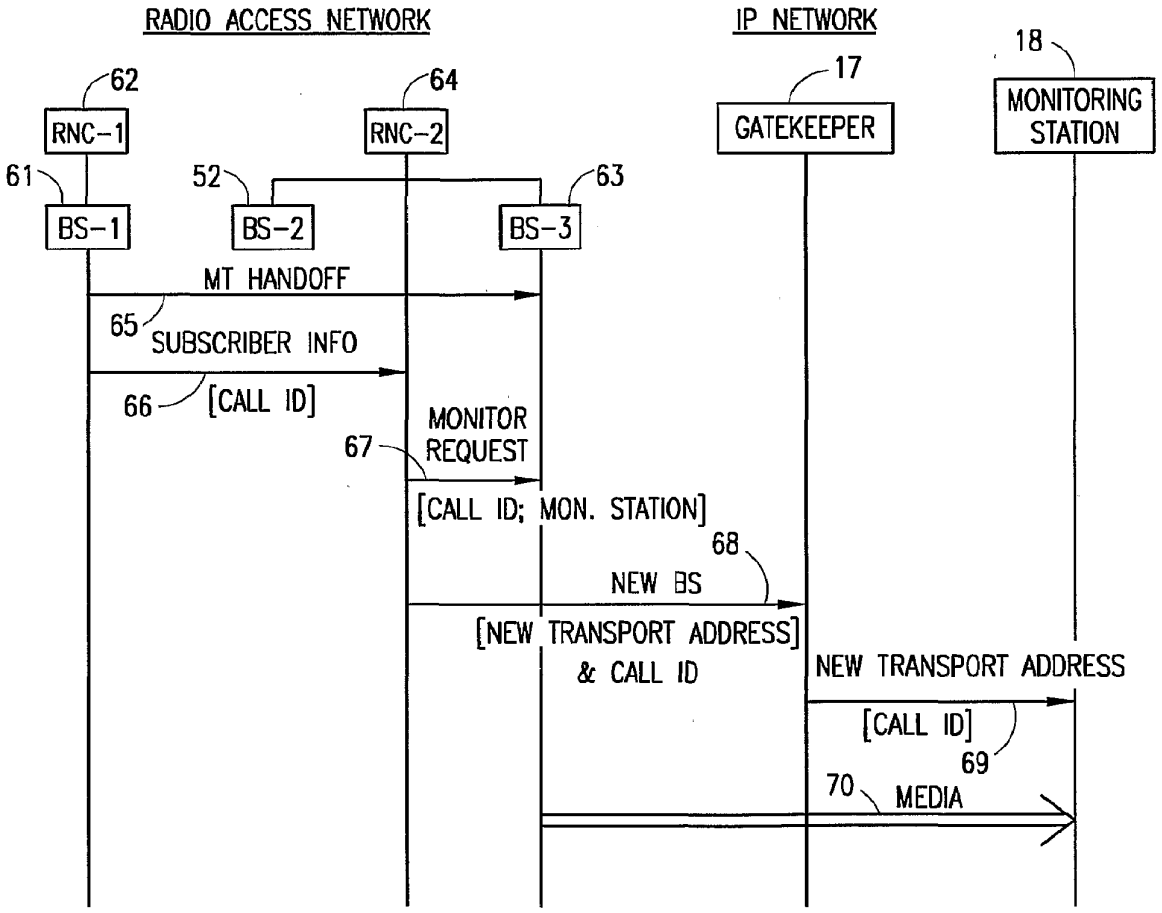

RADIO ACCESS NETWORK
IP NETWORK
18
62
64
17
RNC-1
RNC-2
GATEKEEPER
MONITORING STATION
61
52
63
BS-1
BS-2
BS-3
MT HANDOFF
65
SUBSCRIBER INFO
66
[CALL ID]
MONITOR REQUEST
67
[CALL ID; MON. STATION]
68
NEW BS
[NEW TRANSPORT ADDRESS] & CALL ID
NEW TRANSPORT ADDRESS
[CALL ID]
69
70
MEDIA

FIG. 5

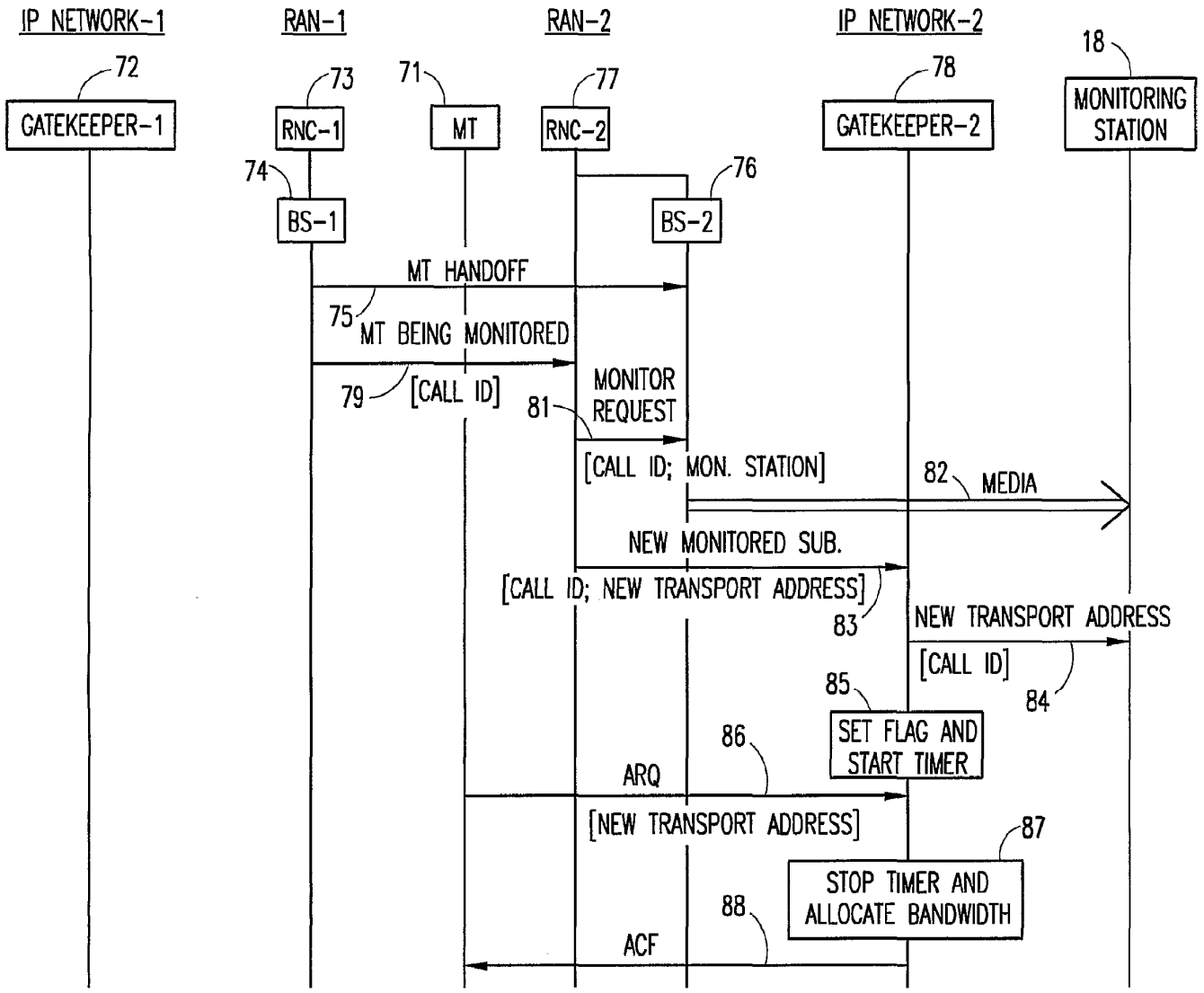

IP NETWORK-1
RAN-1
RAN-2
IP NETWORK-2
72
GATEKEEPER-1
73
RNC-1
71
MT
77
RNC-2
78
GATEKEEPER-2
18
MONITORING STATION
74
BS-1
76
BS-2
MT HANDOFF
75
MT BEING MONITORED
79
[CALL ID]
MONITOR REQUEST
81
[CALL ID; MON. STATION]
82
MEDIA
NEW MONITORED SUB.
[CALL ID; NEW TRANSPORT ADDRESS]
83
NEW TRANSPORT ADDRESS
[CALL ID]
84
85
SET FLAG AND START TIMER
86
ARQ
[NEW TRANSPORT ADDRESS]
87
STOP TIMER AND ALLOCATE BANDWIDTH
88
ACF

FIG. 6

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
80298 MUNICH
GERMANY
Tel. +49 (0)89 2399 - 0
Fax +49 (0)89 2399 - 4465

For any questions about this communication:
Tel.:+31 (0)70 340 45 00

Butler, Michael John
Dehns
St Bride's House
10 Salisbury Square
London
EC4Y 8JD
ROYAUME UNI

File 406.99
02 NOV 2012
RECEIVED
ANSD

Date
02.11.12

Reference	Application No./Patent No.
406.102658	07855436.7 - 2414 / 2090024 PCT/CA2007002150
Applicant/Proprietor	
Digifonica (International) Limited	

Communication

The extended European search report is enclosed.

The extended European search report includes, pursuant to Rule 62 EPC, the supplementary European search report (Art. 153(7) EPC) and the European search opinion.

Copies of documents cited in the European search report are attached.

☑ 0 additional set(s) of copies of such documents is (are) enclosed as well.

Refund of the search fee
If applicable under Article 9 Rules relating to fees, a separate communication from the Receiving Section on the refund of the search fee will be sent later.

Should you wish to further prosecute this application in the examination phase, your attention is drawn to the provisions of Rule 70a EPC. An invitation to respond to the extended European search report will be issued shortly (R. 70(2) EPC).

Europäisches Patentamt • European Patent Office • Office européen des brevets

EPO Form 1507S 06.12

T-Mobile Exhibit 1002
Part 5 of 6

Europäisches Patentamt
European Patent Office
Office européen des brevets

SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application Number
EP 07 85 5436

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 2006/072550 A1 (DAVIS THOMAS C [US] ET AL) 6 April 2006 (2006-04-06) * paragraphs [0004], [0009] - [0011]; claims 1-3; figure 1 * -----	1-15	INV. H04L12/26 H04L12/66 H04M11/06 H04M3/22
X	US 2004/240439 A1 (CASTLEBERRY MICHAEL RAY [US] ET AL) 2 December 2004 (2004-12-02) * paragraphs [0029] - [0032]; claim 1; figures 2,3,4 * -----	1-15	
X	WO 01/89145 A2 (ERICSSON TELEFON AB L M [SE]) 22 November 2001 (2001-11-22) * abstract; claim 1; figures 2-6 * -----	1-15	
X	US 7 055 174 B1 (COPE WARREN B [US] ET AL) 30 May 2006 (2006-05-30) * paragraphs [0007] - [0009] * * abstract * -----	1-15	
A	US 2003/200311 A1 (BAUM ROBERT T [US]) 23 October 2003 (2003-10-23) * paragraphs [0038], [0040], [0041] * -----	1-15	

TECHNICAL FIELDS SEARCHED (IPC)
H04L H04M

The supplementary search report has been based on the last set of claims valid and available at the start of the search

1

Place of search	Date of completion of the search	Examiner
Munich	23 October 2012	Domingos, Luis

CATEGORY OF CITED DOCUMENTS

X particularly relevant if taken alone
Y particularly relevant if combined with another document of the same category
A technological background
O non-written disclosure
P intermediate document

T theory or principle underlying the invention
E earlier patent document, but published on, or after the filing date
D document cited in the application
L document cited for other reasons

& member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C04)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 07 85 5436

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information

23-10-2012

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006072550 A1	06-04-2006	NONE	
US 2004240439 A1	02-12-2004	NONE	
WO 0189145 A2	22-11-2001	AT 343896 T	15-11-2006
		AU 5690501 A	26-11-2001
		DE 60124087 T2	31-05-2007
		EP 1282977 A2	12-02-2003
		US 6839323 B1	04-01-2005
		WO 0189145 A2	22-11-2001
US 7055174 B1	30-05-2006	NONE	
US 2003200311 A1	23-10-2003	NONE	

EPO FORM P0459

For more details about this annex see Official Journal of the European Patent Office, No 12/82

The examination is being carried out on the **following application documents**

Description, Pages

2-23, 26-62	as published
1, 24, 25	filed with entry into the regional phase before the EPO

Claims, Numbers

1-16	filed with entry into the regional phase before the EPO

Drawings, Sheets

1/29-5/29, 10/29-12/29, 14/29, 17/29, 19/29-22/29, 24/29, 27/29, 29/29	as published
6/29-9/29, 13/29, 15/29, 16/29, 18/29, 23/29, 25/29, 26/29, 28/29	filed with entry into the regional phase before the EPO

The following document has been cited in the international search report; the numbering will be adhered to in the rest of the procedure.

D1 US 2004/181599 A1

additionally, reference is made to the following documents; the numbering will be adhered to in the rest of the procedure.

D2 US 2006/072550 A1 (DAVIS THOMAS C [US] ET AL) 6 April 2006 (2006-04-06)

D3 US 2004/240439 A1 (CASTLEBERRY MICHAEL RAY [US] ET AL) 2 December 2004 (2004-12-02)

D4 WO 01/89145 A2 (ERICSSON TELEFON AB L M [SE]) 22 November 2001 (2001-11-22)

D5 US 7 055 174 B1 (COPE WARREN B [US] ET AL) 30 May 2006 (2006-05-30)

1 In the originally filed application, no basis could be found for the feature "... *through a media relay to which the subscriber and the another party address their communications destined for each other*", found in claim 1.

Indeed, why should the caller or the callee address communications to a media relay of which they should not even be aware, rather than to the person they want to reach? In fact, not only does this feature contradict the originally filed description, it also contradicts common sense.

Consequently, the amendments fail to comply with the requirements of Article 123(2) EPC for introduction of subject-matter which extends beyond the content of the application as filed.

2 Additionally, and concerning Article 84 EPC, the application contains below described deficiencies:

2.1 It is clear from the opening part of the description (e. g., in page 2, line 18: "*in contrast to circuit-switched networks. IP-based networks are "connectionless" by design ... which establish a **plurality of paths** ...*", in page 3, line 7, "*while the plurality of available paths and out-of-order arrivals present no problems to IP-based applications ... , **the same factors present formidable problems** for the lawful intercept ... VoIP calls*", further on, in line 20, "*... these packets may take **any available path** across the IP network ... . Even if a service provider could place an interception device **at every point** ... (it) would have to reassemble all of the intercepted packets at a single device and only then pass the result to the law enforcement agency*") that the objective problem to be solved by the present invention is how to implement lawful interception **in a multipath IP network**.

However, independent claims 1 and 14 fail to provide the corresponding solution to that problem. Instead, the starting conditions of both claims are IP networks having, by some sort of magic trick, a media relay between the caller and the called parties.

It is only in dependent claims 5, 7, 8 and 9 that the "magic trick" actually solving the problem underlying the present application is described as a technical solution.

Consequently, independent claims 1 and 14 fail to meet the requirement following from Article 84 EPC taken in combination with Rules 43(1) and (3) EPC that any independent claim must contain all the technical features essential to the definition of the invention.

2.2 Notwithstanding the above, from the wording of method claims 1-13 alone, it is not clear which device implements each method step (namely, the Call controller (CC, 14), the Routing Controller (RC, 16), the database (DB, 18), etc).

Not only does this incomplete definition of the method fail to provide the skilled person with the means to clearly and unambiguously assess the subject-matter sought for protection (Article 84 EPC), it also has as consequence that the scope of protection sought is rendered broader than that allowed by the description and the embodiments contained therein (Article 84 EPC).

3 Notwithstanding the above, the present application does not meet the requirements of Article 52(1) EPC, because the subject-matter of claim 1 is not novel in the sense of Article 54(1) and (2) EPC.

3.1 This can be seen with respect to document D1 (references to D1 are provided between brackets) that discloses according to all the features of claim 1, a method for intercepting communications in an Internet Protocol, IP, network system (abstract) in which communications between a subscriber of the system and another party occur through a media relay (figure 1, signs PRO and LIS) which relays the communications between both subscribers (paragraph 55), the method comprising:

determining whether determination information associated with a subscriber dialing profile associated with the subscriber meets intercept criteria (paragraphs 19 and 20);

when said determination information meets intercept criteria, causing the same media relay to produce a copy of the communications between the parties while relaying the communication (e. g., paragraph 55);

causing the media relay to send the copy to a mediation device (figure 1, sign ASW) specified by destination information associated with the subscriber dialing profile (figures 2A and 2B and paragraphs 12, 16, 19, 20 and 67 where the monitoring designation UWD is implicitly (because there's no other data available) converted into an identifying designation IDK comprising an identification of the authorized agency identifier LID).

3.2 The attention of the applicant is drawn to the fact that documents D2-D5 (reference is made to the passages cited in the search report) also disclose methods of implementing lawful interception in IP networks of such similarity to that of the present application that they render the subject-matter of claim 1 obvious for the skilled person.

4 The subject-matter of independent apparatus claim 14 corresponds to that of claim 1. Therefore, an analogous argumentation to the one above provided for claim 1 would lead to the same novelty objection (Article 52(1), 54 EPC) for claim 14.

5 Dependent claims 2-13 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the EPC in respect of novelty (Article 54(2) EPC) or inventive step (Article 56 EPC) as their subject-matter is either contained in the disclosure of D1 (see passages above referred) or immediately derivable from the combined disclosure of documents D1-D5 (reference is made to the passages cited in the search report).

6 It is not at present apparent which part of the application could serve as a basis for a new, allowable claim. Should the applicant nevertheless regard some particular matter as patentable, an independent claim should be filed taking account of Rule 43(1) EPC. The applicant should also indicate in the letter of reply the difference of the subject-matter of the new claim vis-à-vis the state of the art and the significance thereof. The following comments should also be taken into consideration:

6.1 Documents D1-D5 appear to represent the most relevant prior art. They should therefore be acknowledged in the description, and differences distinguishing the present application from the disclosed content should be pointed out (Rule 42(1)(b) EPC).

6.2 The features of the claims should be provided with reference signs placed in parentheses to increase the intelligibility of the claims (Rule 43(7) EPC). This applies to both the preamble and characterizing portion (see the guidelines, F-IV.4.19).

6.3 When filing amended claims the applicant should at the same time bring the description into conformity with the amended claims (Rule 42(1)(c) EPC). Care should be taken during revision not to add subject-matter which extends beyond the content of the application as originally filed (Article 123(2) EPC). In order to facilitate the examination of the conformity of the amended application with the requirements of Article 123(2) EPC, the applicant should comply with the provisions of Rule 137(4) EPC by clearly identifying the

amendments carried out, irrespective of whether they concern amendments by addition, replacement or deletion, and to indicate the passages of the application as filed on which the amendments are based.

INFORMATION DISCLOSURE STATEMENT

Inventor	:	Johan Emil Viktor Bjorsell et al.
App. No.	:	13/056,277
Filed	:	January 27, 2011
For	:	MOBILE GATEWAY
Examiner	:	Kwang Bin Yao
Art Unit	:	2473
Conf. No.	:	2403

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

References and Listing

Submitted herewith in the above-identified application is an Information Disclosure Statement listing references for consideration. Copies of any listed foreign and non-patent literature references are being submitted.

Timing of Disclosure

This Information Disclosure Statement is being filed before the receipt of a first Office Action on the merits, and presumably no fee is required. If a first Office Action on the merits was mailed before the mailing date of this Statement, the Commissioner is authorized to charge the fee set forth in 37 CFR 1.17(p) to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 1/14/13

By: _____

John M. Carson
Registration No. 34,303
Attorney of Record
Customer No. 20995
(858) 707-4000

14649385:djl
011113

PATENT ASSIGNMENT

Electronic Version v1.1
Stylesheet Version v1.1

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	Correction by Declaration of the Reel and Frame 029995/0668 and the Patent Application numbers 12513147, 12517026, 12532989, 13056277 and 13496864.

CONVEYING PARTY DATA

Name	Execution Date
Digifonica (International) Limited	04/01/2013

RECEIVING PARTY DATA

Name:	Digifonica (International) Limited
Street Address:	773 Hornby St
City:	Vancouver
State/Country:	CANADA
Postal Code:	V6Z1S4

PROPERTY NUMBERS Total: 5

Property Type	Number
Application Number:	12513147
Application Number:	12517026
Application Number:	12532989
Application Number:	13056277
Application Number:	13496864

OP $200.00 12513147

CORRESPONDENCE DATA

Fax Number:
Correspondence will be sent via US Mail when the fax attempt is unsuccessful.
Phone: 7788779434
Email: konstantin@telus.net
Correspondent Name: Emil Malak
Address Line 1: 773 Hornby St
Address Line 4: Vancouver, CANADA V6Z1S4

NAME OF SUBMITTER:	Emil Malak

	This document serves as an Oath/Declaration (37 CFR 1.63).

Total Attachments: 2
source=Digifonica Gibraltar 3300#page1.tif
source=Digifonica Affidavit2#page1.tif

Subject: FW: Digifonica (International) Limited

Subject: Digifonica (International) Limited
Date: Mon, 25 Mar 2013 09:41:20 +0000
From: Karen.Shiels@stanleydavis.co.uk
To: emil_malak@hotmail.com

Dear Emil

Further to our discussion, I can confirm that the officers and shareholders of the above named Gibraltar registered company are as follows:

Director:

Sole director is Emil Malak

Shareholder:

Sole shareholder holding 10,000,000 of Gib£0.01 shares is Emil Malak

Please note that there have been no changes to the above and in the went that a 3rd party requested any changes to the company, we would require your authorisation as you are our client of record. We would further not action any changes to the directors or shareholders without full due diligence on the proposed companies/individuals.

Kind regards

Karen

Karen Shiels
Offshore and Technical Department
Stanley Davis Group Limited, 41 Chalton Street, London NW1 1JD
Direct tel: +44 (207) 554 2252
email: karen.shiels@stanleydavis.co.uk

Affidavit of Ownership

Date: April 1, 2013

To: USPTO Assignment Department

From: Emil Malak, President

Digifonica (International) Limited

These five (5) Patent Application #s 12513147, 12517026, 12532989, 13056277 and 13496864 belong to Digifonica (International) Limited and Digifonica (International) Limited is the rightful owner. These patent applications should have never been recorded by these particular parties. Digifonica (International) Limited has never assigned these patent applications to anyone.

I, Emil Malak, President of Digifonica (International) Limited, hereby affirm that these statements are true and accurate.

BY: _____

Emil Malak, President

WITNESS BY: _____

Print Name: Ric Chin

773 Hornby Street

Vancouver, BC V6Z 1S4

604 889 0516

emil_malak@hotmail.com

2090 Comox Street

Vancouver BC V6G 1R8

778 989 3872

ric_chin@hotmail.com

PATENT ASSIGNMENT

Electronic Version v1.1
Stylesheet Version v1.1

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	Correction by Declaration of the Reel and Frame 029995/0777 and the Patent Application numbers 12513147, 12517026, 12532989, 13056277 and 13496864.

CONVEYING PARTY DATA

Name	Execution Date
Digifonica (International) Limited	04/01/2013

RECEIVING PARTY DATA

Name:	Digifonica (International) Limited
Street Address:	773 Hornby St
City:	Vancouver
State/Country:	CANADA
Postal Code:	V6Z1S4

PROPERTY NUMBERS Total: 5

Property Type	Number
Application Number:	12513147
Application Number:	12517026
Application Number:	12532989
Application Number:	13056277
Application Number:	13496864

OP $200.00 12513147

CORRESPONDENCE DATA

Fax Number:
Correspondence will be sent via US Mail when the fax attempt is unsuccessful.
Phone: 7788779434
Email: konstantin@telus.net
Correspondent Name: Emil Malak
Address Line 1: 773 Hornby St
Address Line 4: Vancouver, CANADA V6Z1S4

NAME OF SUBMITTER:	Emil Malak

	This document serves as an Oath/Declaration (37 CFR 1.63).

Total Attachments: 2
source=Digifonica Gibraltar 3300#page1.tif
source=Digifonica Affidavit2#page1.tif

Subject: FW: Digifonica (International) Limited

Subject: Digifonica (International) Limited
Date: Mon, 25 Mar 2013 09:41:20 +0000
From: Karen.Shiels@stanleydavis.co.uk
To: emil_malak@hotmail.com

Dear Emil

Further to our discussion, I can confirm that the officers and shareholders of the above named Gibraltar registered company are as follows:

Director:

Sole director is Emil Malak

Shareholder:

Sole shareholder holding 10,000,000 of Gib£0.01 shares is Emil Malak

Please note that there have been no changes to the above and in the went that a 3rd party requested any changes to the company, we would require your authorisation as you are our client of record. We would further not action any changes to the directors or shareholders without full due diligence on the proposed companies/individuals.

Kind regards

Karen

Karen Shiels
Offshore and Technical Department
Stanley Davis Group Limited, 41 Chalton Street, London NW1 1JD
Direct tel: +44 (207) 554 2252
email: karen.shiels@stanleydavis.co.uk

Affidavit of Ownership

Date: April 1, 2013

To: USPTO Assignment Department

From: Emil Malak, President

Digifonica (International) Limited

These five (5) Patent Application #s 12513147, 12517026, 12532989, 13056277 and 13496864 belong to Digifonica (International) Limited and Digifonica (International) Limited is the rightful owner. These patent applications should have never been recorded by these particular parties. Digifonica (International) Limited has never assigned these patent applications to anyone.

I, Emil Malak, President of Digifonica (International) Limited, hereby affirm that these statements are true and accurate.

BY: _____

Emil Malak, President

WITNESS BY: _____

Print Name: Ric Chin

773 Hornby Street

Vancouver, BC V6Z 1S4

604 889 0516

emil_malak@hotmail.com

2090 Comox Street

Vancouver BC V6G 1R8

778 989 3872

ric_chin@hotmail.com

PATENT ASSIGNMENT

Electronic Version v1.1
Stylesheet Version v1.1

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	Correction by Declaration of the Reel and Frame 029942/0905 and the Patent Application numbers 12513147, 12517026, 12532989, 13056277 and 13496864.

CONVEYING PARTY DATA

Name	Execution Date
Digifonica (International) Limited	04/01/2013

RECEIVING PARTY DATA

Name:	Digifonica (International) Limited
Street Address:	773 Hornby St
City:	Vancouver
State/Country:	CANADA
Postal Code:	V6Z1S4

PROPERTY NUMBERS Total: 5

Property Type	Number
Application Number:	12513147
Application Number:	12517026
Application Number:	12532989
Application Number:	13056277
Application Number:	13496864

OP $200.00 12513147

CORRESPONDENCE DATA

Fax Number:
Correspondence will be sent via US Mail when the fax attempt is unsuccessful.
Phone: 7788779434
Email: konstantin@telus.net
Correspondent Name: Emil Malak
Address Line 1: 773 Hornby St
Address Line 4: Vancouver, CANADA V6Z1S4

NAME OF SUBMITTER:	Emil Malak

	This document serves as an Oath/Declaration (37 CFR 1.63).

Total Attachments: 2
source=Digifonica Gibraltar 3300#page1.tif
source=Digifonica Affidavit2#page1.tif

Subject: FW: Digifonica (International) Limited

Subject: Digifonica (International) Limited
Date: Mon, 25 Mar 2013 09:41:20 +0000
From: Karen.Shiels@stanleydavis.co.uk
To: emil_malak@hotmail.com

Dear Emil

Further to our discussion, I can confirm that the officers and shareholders of the above named Gibraltar registered company are as follows:

Director:

Sole director is Emil Malak

Shareholder:

Sole shareholder holding 10,000,000 of Gib£0.01 shares is Emil Malak

Please note that there have been no changes to the above and in the went that a 3rd party requested any changes to the company, we would require your authorisation as you are our client of record. We would further not action any changes to the directors or shareholders without full due diligence on the proposed companies/individuals.

Kind regards

Karen

Karen Shiels
Offshore and Technical Department
Stanley Davis Group Limited, 41 Chalton Street, London NW1 1JD
Direct tel: +44 (207) 554 2252
email: karen.shiels@stanleydavis.co.uk

Affidavit of Ownership

Date: April 1, 2013

To: USPTO Assignment Department

From: Emil Malak, President

Digifonica (International) Limited

These five (5) Patent Application #s 12513147, 12517026, 12532989, 13056277 and 13496864 belong to Digifonica (International) Limited and Digifonica (International) Limited is the rightful owner. These patent applications should have never been recorded by these particular parties. Digifonica (International) Limited has never assigned these patent applications to anyone.

I, Emil Malak, President of Digifonica (International) Limited, hereby affirm that these statements are true and accurate.

BY: _____

Emil Malak, President

WITNESS BY: _____

Print Name: Ric Chin

773 Hornby Street

Vancouver, BC V6Z 1S4

604 889 0516

emil_malak@hotmail.com

2090 Comox Street

Vancouver BC V6G 1R8

778 989 3872

ric_chin@hotmail.com

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/056,277	01/27/2011	Johan Emil Viktor Bjorsell	SMARB19.004APC	2403

20995 7590 04/11/2013

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER	
RAHMAN, MOSTAZIR M	

ART UNIT	PAPER NUMBER
2413	

NOTIFICATION DATE	DELIVERY MODE
04/11/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

jayna.cartee@knobbe.com
efiling@knobbe.com

PTOL-90A (Rev. 04/07)

Office Action Summary	Application No.	Applicant(s)	
	13/056,277	BJORSELL ET AL.	
	Examiner	Art Unit	
	M MOSTAZIR RAHMAN	2413	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01/27/2011*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-90* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-90* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *01/27/2011* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date 1/27/2011,05/06/2011,6/21/2012,8/2/2012,9/6/2012,9/10/2012,1/14/2013

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

4) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

The information disclosure statements (IDS) submitted on 01/27/2011, 05/26/2011, 06/21/2012, 08/03/2012, 09/06/2012, 09/10/2012 and 01/14/2013 have been placed in record and considered by the examiner.

Priority

Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Claim Objections

Claims 52, 71 and 90 are objected to because of the following informalities: Specifically,

a. Claim 52 line 5: replace first occurrence of "**said routing controller**" -- "**a routing controller**" -- instead.

b. Claim 71 line 9: replace first occurrence of "**said routing controller**" into -- "**a routing controller**" -- instead.

c. Claim 90 line 6: replace first occurrence of "**said routing controller**" into -- "**a routing controller**" -- instead.

Appropriate corrections are required.

T-Mobile Exhibit 1002
Part 5 of 6

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 32 and 90 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The claims are drawn to a "**computer readable medium**". Thus, applying the broadest reasonable interpretation in light of the specification and taking into account the meaning of the words in their ordinary usage they would be understood by one of ordinary skill in the art (MPEP §2111) , the claim as a whole covers both transitory and not transitory media. A transitory medium does not fall into any of the 4 categories of invention (Process, Machine, Manufacture, or composition of matter). The applicants are respectfully suggested to amend the claims to read as "A **non-transitory computer readable medium** ..." to overcome the 35 USC § 101 rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious

> at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1-3, 5-7, 8- 14, 16- 24, 26-35, 52-54, 71-73 and **90** are rejected under 35 U.S.C. 103(a) as being unpatentable over **ELLIOTT** et al. (US Pub No. **2004/0022237 A1**; hereinafter as "**ELLIOTT**") in view of **ALBINA** et al. (US Pub No. **2008/0056235 A1**; hereinafter as "**ALBINA**").

1. **Elliott teaches** a method of initiating a call to a callee using, *a telephone*, the method comprising ***(Elliott; Fig. 1: initiate a call from caller 102 to callee 120)***:

receiving, from a user of *the telephone*, a callee identifier associated with the callee ***(Elliott, [0035] lines 20-22; user of calling party dials phone number of the called party)***;

transmitting an access code request message to an access server, said access code request message including said callee identifier ***(Elliott, [0035] lines 24-37: soft switch takes request from calling party with dialed number to set up contact with called party)***;

receiving an access code reply message from the access server in response to said access code request message, said access code reply message including an access code different from said callee identifier and associated with said callee identifier (***[0487]: soft switch sends IPDC protocol command back to gateway (reply) which is connected to the calling party so that the call termination to called party 120***); and

initiating a call with *the telephone* using said access code to identify the callee (***[0487]: the connection between origination and termination is established***).

However, Elliott does not explicitly teach that caller is a mobile phone.

In an analogous art, **Albina** teaches functionality of:

a mobile phone is calling a callee ***(Albina, Fig. 1 mobile device 102 is calling device 104).***

Therefore, it would have been obvious to one of the ordinary skill in the art at the time the invention was made to provide the technique of **Albina** to the system of **Elliott** in order to establish a VoIP media session between the originating cellular telephone and the VoIP destination device ***(Albina, [0007]).***

2. **Elliott and Albina, specifically, Elliott teach** the method of claim 1 wherein transmitting comprises transmitting said access code request message to said access server on a non-voice network ***(Elliott,[0485]: dialed number; (Fig. 4A: 408: [0582]:408 is a TCP/IP (i.e. non-voice) connection)***.

3. **Elliott and Albina, specifically, Albina teach** the method of claim 1.

wherein transmitting comprises transmitting a location identifier of a location associated with the mobile telephone to said access server ***(Albina [0105]; mobile station 1202 register with Registrar/Location server 1210 to give the location of mobile station; Fig. 12)***.

5. **Elliott and Albina, specifically, Albina teach** the method of claim 3 wherein transmitting said location identifier comprises transmitting an identifier of a wireless

voice signal station in wireless communication with the mobile telephone ***(Albina; Fig. 2: [0033] lines 1-18: mobile device 102 sends a data message (i.e. identifier) which is carried via mobile data network 106 which is deliver to application server 110).***

6. **Elliott and Albina, specifically, Albina teach** the method of claim 3 wherein transmitting said location identifier comprises transmitting a user-configured identifier of a location associated with the mobile telephone ***(Albina; Fig. 12: mobile station 1202 registers with register/location server 1210. [0104] lines 8-14: Client's application (i.e. user-configured identifier) resides on mobile station 1202 for enabling the user to select a call. Application is configured (i.e. user-configured identifier) such that requests arrive at the IP address of IWF 1208)***.

7. **Elliott and Albina, specifically, Albina teaches** the method of claim 1 wherein receiving said access code reply message comprises receiving said access code reply message from said access server on a non-voice network ***(Elliott , Fig. 1: mobile phone 102 is communicating with soft switch using data network 112 which is a non-voice network.; [0863]: ServerProxy 426)***.

8. **Elliott and Albina, specifically, Albina teach** the method of claim 1.

wherein receiving said access code reply message comprises receiving, in said access code reply message, said access code temporarily associated with said

callee identifier (***Albina; [0053]: destination phone number (the assigned local temporary number) to the SIP application server***).

9. **Elliott and Albina, specifically, Elliott teach** the method of claim 1 wherein receiving said access code reply message comprises receiving, in said access code reply message, a telephone number identifying a channel operably configured to cooperate with an IP network to cause a call involving the mobile telephone and the callee to be routed through the IP network ***(Elliott, Fig. 1: Device 102 makes a call to callee 120 which is routing through IP data network 112).***

10 **Elliott and Albina, specifically, Elliott teach** the method of claim 1 wherein initiating said call comprises engaging a routing controller to route said call on said IP network to the callee ***(*Elliott *Fig. 1: device 102 engaging gateway site 108 (a routing controller) to route the call through IP data network 118 to callee 120).***

11. **Elliott and Albina, specifically, Elliott teach** the method of claim 1 further comprising:

receiving from the mobile telephone said access code request message ***(Elliott ,[0485]: dialed number)***;

communicating with a routing controller to obtain from the routing controller said access code wherein said access code identifies a channel and is useable by the

mobile telephone to cause the routing controller to establish a call to the callee using the channel ***(Elliott, Fig. 22A: 2226: [0487]: gateway setup call from caller to callee using IPDC protocol commands)***;

and transmitting said access code reply message to the mobile telephone ***(Elliott ,[0487]: soft switch sends IPDC protocol command back to gateway (reply) which is connected to the calling party so that the call termination to called party 120 and the connection between origination and termination is established)***.

12. **Elliott teaches** *a* telephone apparatus comprising:

means for receiving, from a user of the telephone, a callee identifier associated with the callee ***(Elliott, [0035] lines 20-22; user of calling party dials phone number of the called party)***;

transmitting means for transmitting an access code request message to an access server, said access code request message including said callee identifier ***(Elliott, [0035] lines 24-37: soft switch takes request from calling party with dialed number to set up contact with called party)***;

means for receiving an access code reply message from the access server in response to said access code request message, said access code reply message

including an access code different from said callee identifier and associated with said callee identifier (***[0487]: soft switch sends IPDC protocol command back to gateway (reply) which is connected to the calling party so that the call termination to called party 120***);

and means for initiating a call using said access code to identify the callee (***[0487]: the connection between origination and termination is established***).

However, Elliott does not teach that apparatus is a **mobile phone**.

In an analogous art, **Albina** teaches functionality of:

a mobile apparatus is calling a callee ***(Albina, Fig. 1 mobile device 102 is calling device 104).***

Therefore, it would have been obvious to one of the ordinary skill in the art at the time the invention was made to provide the technique of **Albina** to the system of **Elliott** in order to establish a VoIP media session between the originating cellular telephone and the VoIP destination device ***(Albina, [0007]).***

21. **Elliott and Albina, specifically, Elliott teach** a system for initiating a call to a callee, the system comprising the mobile telephone apparatus of claim 12, and further comprising:

a routing controller ***(Elliott: Fig. 1: Gateway site 108)***; and

an access server comprising ***(Elliott: Fig 1: Soft switch 106):***

means for receiving from the mobile telephone said access code request message ***(Elliott,[0485]: dialed number)***;

means for communicating with said routing controller to obtain from said routing controller said access code wherein said access code identifies a channel and is useable by the mobile telephone to cause the routing controller to establish a call to the callee using the channel ***(Elliott ,Fig. 22A: 2226: [0487]: gateway setup call from caller to callee using IPDC protocol commands)***; and

means for transmitting said access code reply message including said access code to the mobile telephone ***(Elliott ,[0487]: soft switch sends IPDC protocol command back to gateway (reply) which is connected to the calling party so that the call termination to called party 120 and the connection between origination and termination is established)***.

22. **Elliott teach** a telephone apparatus comprising:

a processor circuit ***(Fig. 1: a phone stations (102 and 122) must have a processor)***;

T-Mobile Exhibit 1002
Part 5 of 6

a network interface in communication with said processor circuit ***(Fig. 1: phone stations (102 and 122) must have a network interface to connect to other devices)***; and

a computer readable medium in communication with said processor circuit and encoded with codes for directing said processor circuit ***(stations (102 and 122) must have computer code to operate)*** to:

receive, from a user of the telephone, a callee identifier associated with the callee ***(Elliott, [0035] lines 20-22; user of calling party dials phone number of the called party)***;

cause an access code request message to be transmitted to an access server, said access code request message including said callee identifier ***(Elliott, [0035] lines 24-37: soft switch takes request from calling party with dialed number to set up contact with called party);***

receive an access code reply message from the access server in response to said access code request message, said access code reply message including an access code different from said callee identifier and associated with said callee identifier (***Elliott ,[0487]: soft switch sends IPDC protocol command back to gateway (reply) which is connected to the calling party so that the call termination to called party 120***); and

initiate a call using said access code to identify the callee (***[0487]: the connection between origination and termination is established***).

However, Elliott does not teach that apparatus is a **mobile phone**.

In an analogous art, **Albina** teaches functionality of:

a mobile apparatus is calling a callee ***(Albina, Fig. 1 mobile device 102 is calling device 104).***

Therefore, it would have been obvious to one of the ordinary skill in the art at the time the invention was made to provide the technique of **Albina** to the system of **Elliott** in order to establish a VoIP media session between the originating cellular telephone and the VoIP destination device ***(Albina, [0007]).***

23. **Elliott and Albina, specifically, Elliott teach** the mobile telephone apparatus of claim 22 wherein said network interface comprises a non-voice network interface, and wherein said codes for directing said processor circuit to cause said access code request message to be transmitted include codes for directing said processor circuit to cause said access code request message to be transmitted to said access server using said non-voice network interface on a non-voice network ***(Elliott, Fig.1: phone 102 calls callee 120 which is routing through gateway site 108 using data network (i.e. non-voice network) through another gateway***

site 110 and reach to destination callee 120).

24. **Elliott and Albina, specifically, Albina teaches** the mobile telephone apparatus of claim 22.

wherein said access code request message further includes a location identifier of a location associated with the mobile telephone server ***(Albina [0105]; mobile station 1202 register with Registrar/Location server 1210 to give the location of mobile station; Fig. 12)***.

26. **Elliott and Albina, specifically, Albina teach** the mobile telephone apparatus of claim 24 wherein said location identifier comprises an identifier of a wireless voice signal station in wireless communication with the mobile telephone ***(Albina; Fig. 2: [0033] lines 1-18: mobile device 102 sends a data message (i.e. identifier) which is carried via mobile data network 106 which is deliver to application server 110).***

27. **Elliott and Albina, specifically, Albina teach** the mobile telephone apparatus of claim 24 wherein said location identifier comprises a user-configured identifier of a location associated with the mobile telephone ***(Albina; Fig. 12: mobile station 1202 registers with register/location server 1210. [0104] lines 8-14: Client's application (i.e. user-configured identifier) resides on mobile station 1202 for enabling the user to select a call. Application is configured (i.e. user-***

configured identifier) such that requests arrive at the IP address of IWF 1208).

28. **Elliott and Albina, specifically, Albina teach** the mobile telephone apparatus of claim 22 as applied above and

wherein said network interface comprises a non-voice network interface, and

wherein said codes for directing said processor circuit to receive an access code reply message include codes for directing said processor circuit to cause said access code reply message to be received from said access server using said non-voice network interface on a non-voice network ***(Albina, Fig. 11: Mobile phone 1102 to communicate with wireless data network 1106 and application server 1108. It must have a data interface (i.e. non-voice interface) to communicate with wireless data network 1106; [0007]; mobile phone sends data message to wireless data network (i.e. non-voice network; [0011]: cellular-to-VoIP call establishment module)).***

29. **Elliott and Albina, specifically, Elliott teaches** the mobile telephone apparatus of claim 22 wherein said access code includes a telephone number identifying a channel operably configured to cooperate with an IP network to cause a call involving the mobile telephone and the callee to be routed through the IP network ***(Elliott, Fig. 1: phone 102 engaging gateway site 108 (a routing controller) to route the call through IP data network 118 to callee 120)***.

30. **Elliott and Albina, specifically, Elliott teaches** the mobile telephone apparatus of claim 22 as applied above, wherein said network interface comprises a mobile telephone network interface, and wherein said codes for directing said processor circuit to initiate include codes for directing said processor circuit to cause a call to be initiated using said mobile telephone network interface on a mobile telephone network ***(Albina, Fig. 1: Mobile communication device 102 which must have mobile telephone network interface communicate with mobile wireless service provider 116***).

31. **Elliott and Albina, specifically, Elliott teaches** a system for initiating a call to a callee, the system comprising the mobile telephone of claim 22, and further comprising:

a routing controller ***(Elliott, Fig. 1: Gateway 108)***; and

an access server comprising a processor circuit and a computer readable medium in communication with the processor circuit, the computer readable medium encoded with codes for directing said processor circuit to ***(Elliott, Fig. 1: Soft switch 104, 106 must have a process, must have a computer readable medium and computer code to operate)***:

receive from the mobile telephone said access code request message ***(Elliott, [0035] lines 20-22; user of calling party dials phone number of the called party***

on mobile phone);

communicate with said routing controller to obtain from said routing controller said access code wherein said access code identifies a channel and is useable by the mobile telephone to cause the routing controller to establish a call to the callee using the channel ***(Elliott, Fig. 22A: 2226: [0487]: gateway setup call from caller to callee using IPDC protocol commands***;

and transmit said access code reply message to the mobile telephone ***(Elliott ,[0487]: soft switch sends IPDC protocol command back to gateway (reply) which is connected to the calling party so that the call termination to called party 120 and the connection between origination and termination is established)***.

Regarding claim 13, the claim is interpreted and rejected for the same reason as set forth in claim 2.

Regarding claim 18, the claim is interpreted and rejected for the same reason as set forth in claim 7.

Regarding claim 20, the claim is interpreted and rejected for the same reason as set forth in claim 9.

Regarding claim 32, the claim is interpreted and rejected for the same reason as set forth in claim **1**.

T-Mobile Exhibit 1002
Part 5 of 6

Regarding claims 14, 16, 17, 19, the claim are interpreted and rejected for the same reason as set forth in claims **3, 5, 6, 8** respectively**.**

71. **Elliott teaches** a system for enabling a telephone to initiate a call to a callee through a channel ***(Fig. 1: 102 to 120)***, the system comprising:

a processor circuit ***(Fig. 1: soft switch (104 and 106) must have a processor)***; a network interface in communication with said processor circuit ***(Fig. 1: soft switch (104 and 106) must have a network interface to connect to other devices)***; and

a computer readable medium in communication with said processor circuit and encoded with codes for directing said processor circuit to ***(soft switch, 104, 106 must have computer code to operate)***:

receive from the mobile telephone an access code request message including a callee identifier associated with the callee ***([0485]: dialed number);***

communicate with said routing controller to obtain from said routing controller an access code identifying the channel, said access code being different from the callee identifier and useable by the telephone to initiate a call to the callee using the channel ***(Fig. 22A: 2226: [0487]: gateway setup call from caller to callee using***

IPDC protocol commands); and

cause an access code reply message including said access code to be transmitted to the telephone ***([0487]: soft switch sends IPDC protocol command back to gateway (reply) which is connected to the calling party so that the call termination to called party 120 and the connection between origination and termination is established).***

However, Elliott does not teach that caller is a mobile phone.

In an analogous art, **Albina** teaches functionality of:

a mobile phone is calling a callee ***(Albina, Fig. 1 mobile device 102 is calling device 104).***

Therefore, it would have been obvious to one of the ordinary skill in the art at the time the invention was made to provide the technique of **Albina** to the system of **Elliott** in order to establish a VoIP media session between the originating cellular telephone and the VoIP destination device ***(Albina, [0007]).***

72. **Elliott and Albina, specifically, Elliott teach** the system of claim 71 wherein said network interface comprises a non- voice network interface ***(Elliott ,Fig. 4A: 408: [0582]:408 is a TCP/IP (i.e. non-voice) connection)***, and wherein said codes for directing said processor circuit to receive include codes for directing said

processor circuit to cause said access code request message to be received using said non-voice network interface on a non-voice network ***(Elliott ,Fig. 4B: Codes to interface with Route ServerProxy 426; [0860]; [0863];)***.

73. **Elliott and Albina, specifically, Elliott teach** the system of claim 71 wherein said computer readable medium is further encoded with codes for directing said processor circuit to cause said access code to be produced ***(Elliott ,Fig. 22: 2226; [0515] soft switch sites 104,106 can send messages (i.e. encoded with codes) through data network 112 (e.g. using IPDC protocol commands) (i.e. access code) to gateway sites 108,101 to instruct the gateway sites to make the necessary connecting for setting up the call from origination and termination)***.

Regarding claims 33-35, the claims are interpreted and rejected for the same reason as set forth in claims **71-73** respectively.

Regarding claims 52-54, the claims are interpreted and rejected for the same reason as set forth in claims **71-73** respectively.

Regarding claim 90, the claim is interpreted and rejected for the same reason as

set forth in claim **71**.

Claims 4, 15, 25, 36-42, 43-48, 55-67, 74-80, and 81-86 are rejected under 35 U.S.C. 103(a) as being unpatentable over **ELLIOTT** et al. (US Pub No. **2004/0022237 A1**; hereinafter as "**ELLIOTT**") in view of **ALBINA** et al. (US Pub No. **2008/0056235 A1**; hereinafter as "**ALBINA**") and further in view of **SCHUSTER** et al. (US Pat No. **6,674,745 B1**; hereinafter as "**SCHUSTER**").

4. **Elliott and Albina teach** the method of claim 3.

However the **combination of Elliott and Albina** do not explicitly teach wherein transmitting said location identifier comprises transmitting an IP address of the mobile telephone in a wireless IP network.

In an analogous art, **Schuster** teaches functionality of:
wherein transmitting said location identifier comprises transmitting an IP address of the mobile telephone in a wireless IP network ***(Schuster col.6 lines 58-62: setup up a call, originating gateway needs some mechanism to determine the IP address of the appropriate terminating gateway 20 based on the telephone number supplied by the calling party)***.

Therefore, it would have been obvious to one of the ordinary skill in the art at the time the invention was made to provide the technique of ***Schuster*** to the combine system of **Elliott and Albina** in order to provide IP telephone mapping **(Schuster, abstract)**.

25. **Elliott and Albina teach** the mobile telephone apparatus of claim 24 as applied above.

However the **combination of Elliott and Albina** do not explicitly teach wherein said location identifier comprises an IP address of the mobile telephone in a wireless IP network.

In an analogous art, ***Schuster*** teaches functionality of:

wherein said location identifier comprises an IP address of the mobile telephone in a wireless IP network ***(Schuster col.6 lines 58-62: setup up a call, originating gateway needs some mechanism to determine the IP address of the appropriate terminating gateway 20 based on the telephone number supplied by the calling party)***.

Therefore, it would have been obvious to one of the ordinary skill in the art at the time the invention was made to provide the technique of ***Schuster*** to the combine system of **Elliott and Albina** in order to provide IP telephone mapping **(Schuster, abstract)**.

Regarding claims 15, the claim is interpreted and rejected for the same reason as set forth in claims 4**.**

74. **Elliott and Albina teach** the system of claim 73.

However **Elliott and Albina** do not explicitly teach

wherein said codes for directing said processor circuit to cause said access code to be produced cause said access code to be selected from a pool of access codes, where each access code in said pool of access codes identifies a respective telephone number.

In an analogous art, **Schuster** teaches functionality of:

wherein said codes for directing said processor circuit to cause said access code to be produced cause said access code to be selected from a pool of access codes, where each access code in said pool of access codes identifies a respective telephone number ***(Schuster, col. 11 lines 1-5: For instance, if the SRITG serves wireless (e.g., cellular, PCS, etc.) customers, then the AMS may refer to an appropriate reference database (i.e. pool) to associate the IP address of the SRITG with the wireless phone numbers that the SRITG serves).***

Therefore, it would have been obvious to one of the ordinary skill in the art at the

time the invention was made to provide the technique of ***Schuster*** to the system of **Elliott and Albina** in order to provide IP telephone mapping **(Schuster, abstract)**.

81. **Elliott and Albina and Schuster, specifically, Schuster teaches** the system of claim 74 wherein each access code in said pool of access codes further identifies a respective channel operably configured to cooperate with an IP network to cause a call involving the mobile telephone and the callee to be routed through the IP network ***(Schuster, abstract, Fig. 1: ITG routes the call with an IP network (19)).***

82. **Elliott and Albina and Schuster, specifically, Elliott teaches** the system of claim 81 wherein said computer readable medium is further encoded with codes for directing said processor circuit to cause communication through said IP network to be established in response to a call received on said channel ***(Elliott;[0026]: establish new call through data network and tear down exiting call in SS7 network; Also [0915]; Fig. 8F: soft switch has code to establish connected with Route Server (RS) for a particular call in a particular channel after they establish connection for the call).***

83. **Elliott and Albina and Schuster, specifically, Elliott teaches** the system of claim 82 wherein said codes for directing said processor circuit to cause said access code to be produced cause a caller identifier associated with the mobile

telephone to be stored in association with said access code (**Elliott; soft switch has code**).

84. **Elliott and Albina and Schuster, specifically, Elliott teaches** the system of claim 83 wherein said codes for directing said processor circuit to cause communication to be established cause communication to be established only if said caller identifier associated with said access code identifies the mobile telephone ***(Elliott, [0735]-[0736] and [0738]: when phone number matches table entry, call is routed and therefore communication is established).***

85. **Elliott and Albina and Schuster, specifically, Elliott teaches** the system of claim 74 wherein said codes for directing said processor circuit to cause said access code to be produced cause said callee identifier to be stored in association with said access code ***(Elliott, [0738]: callee identifier (i.e. dialed number) is stored in table entry; table 14)***.

86. **Elliott and Albina and Schuster, specifically, Elliott teaches** the system of claim 85 wherein said codes for directing said processor circuit to cause said access code to be produced cause said pool of access codes to be searched for an access code associated with said callee identifier to identify the channel usable by the mobile telephone to initiate a call to the callee (**Elliott, *Table 14: circuit group contains channels for identifying callee)***.

Regarding claims 36 and 55, the claims are interpreted and rejected for the same

reason as set forth in claim **74.**

Regarding claims 43-48, the claims are interpreted and rejected for the same reason as set forth in claims **81-86** respectively.

Regarding claims 62-67, the claims are interpreted and rejected for the same reason as set forth in claims **81-86** respectively.

75. **Elliott, Albina and SCHUSTER, specifically, Albina teaches** the system of claim 74.

wherein said computer readable medium is further encoded with codes for directing said processor circuit to cause to be determined a local calling area associated with the mobile telephone ***(Albina; [0053]: destination phone number (the assigned local temporary number) to the SIP application server).***

Therefore, it would have been obvious to one of the ordinary skill in the art at the time the invention was made to provide the technique of **Albina** to the combine system of **Elliott and Schuster** in order to establish a VoIP media session between the originating cellular telephone and the VoIP destination device ***(Albina, [0007]).***

76. **Elliott, Schuster and Albina, specifically, Albina teaches** the system of claim 75. wherein said codes for directing said processor circuit to cause to be determined cause a dialing profile associated with the caller to be accessed, said dialing profile including a location field having contents identifying at least a default location of the caller ***(Albina [0105]; mobile station 1202 register with Registrar/Location server 1210 to give the location of mobile station; Fig. 12)***.

77. **Elliott, Schuster and Albina, specifically, Schuster teaches** the system of claim 75 wherein said codes for directing said processor circuit to cause to be determined cause to be received an IP address of the mobile telephone in a wireless IP network ***(Schuster col.6 lines 58-62: setup up a call, originating gateway needs some mechanism to determine the IP address of the appropriate terminating gateway 20 based on the telephone number supplied by the calling party).***

78. **Elliott, Schuster and Albina, specifically, Albina teaches** the system of claim 75 wherein said codes for directing said processor circuit to cause to be determined cause to be received an identifier of a wireless voice signal station in wireless communication with the mobile telephone ***(Albina; Fig. 2: [0033] lines 1-18: mobile device 102 sends a data message (i.e. identifier) which is carried via mobile data network 106 which is deliver to application server 110).***

79. **Elliott, Schuster and Albina, specifically, Albina teaches** the system of

claim 75 wherein said codes for directing said processor circuit to cause to be determined cause to be received a user-configured identifier of a location associated with the mobile telephone ***(Albina; Fig. 12: mobile station 1202 registers with register/location server 1210. [0104] lines 8-14: Client's application (i.e. user-configured identifier) resides on mobile station 1202 for enabling the user to select a call. Application is configured (i.e. user-configured identifier) such that requests arrive at the IP address of IWF 1208).***

80. **Elliott, Schuster and Albina, specifically, Albina teaches** the system of claim 75 wherein said codes for directing said processor circuit to cause said access code to be produced further cause to be selected an access code in said local calling area associated with the mobile telephone (***(Albina; [0053]: destination phone number (the assigned local temporary number) to the SIP application server***).

Regarding claims 37-42, the claims are interpreted and rejected for the same reason as set forth in claims **75-80** respectively.

Regarding claims 56-61, the claims are interpreted and rejected for the same reason as set forth in claims **75-80** respectively.

Claims 49-50, 68-69, 87-88 are rejected under 35 U.S.C. 103(a) as being unpatentable over **ELLIOTT and Albina** as applied above and further in view of **SHALIT**. (US Pub No.**2002/012391 A1**; hereinafter as "**SHALIT**").

87. **Elliott and Albina teach** the system of claim 73.

However, Elliott and Albina do not explicitly teach

wherein said codes for directing said processor circuit to cause said access code to be produced cause a timestamp for use in determining when the usability of said access code to initiate a call to the callee will expire, to be stored in association with said access code.

In an analogous art**, Shalit** teaches the functionality of:

wherein said codes for directing said processor circuit to cause said access code to be produced cause a timestamp for use in determining when the usability of said access code to initiate a call to the callee will expire, to be stored in association with said access code ***(Shalit; [0044]: Resource manager 15 also deallocates the session access code after the session has expired due to time constraints (i.e., the host will only pay for a 30 minute chat) or physical call breaks (i.e., hang-ups)).***

Therefore, it would have been obvious to one of the ordinary skill in the art at the time the invention was made to provide the technique of **Shalit** to the system of

Elliott and Albina in order to provide audio conferencing services to users of an on-line text messaging service ***(*Shalit, *[abstract]).***

88. **Elliott, Albina and Shalit, specifically Shalit teaches** the system of claim 87 wherein said codes for directing said processor circuit to cause communication to be established cause communication to be established only if the usability of said access code to initiate a call to the callee has not expired ***(Shalit; [0044]: Resource manager 15 also deallocates the session access code after the session has expired due to time constraints (i.e., the host will only pay for a 30 minute chat) or physical call breaks (i.e., hang-ups).***

Regarding claims 49-50, the claims are interpreted and rejected for the same reason as set forth in claims **87-88** respectively.

Regarding claims 68-69, the claims are interpreted and rejected for the same reason as set forth in claims **87-88** respectively.

Claims 51, 70, 89 are rejected under 35 U.S.C. 103(a) as being unpatentable over **ELLIOTT and Albina** as applied above and further in view of **de Oliveira et al.** (US Pat No.**5, 454,030**; hereinafter as "**de Oliveira**").

T-Mobile Exhibit 1002
Part 5 of 6

89. **Elliott and Albina teach** the system of claim 71.

However, **Elliott and Albina teach** do not explicitly teach

wherein said network interface comprises a non- voice network interface, and wherein codes for directing said processor circuit to transmit include codes for directing said processor circuit to cause said access code reply message to be transmitted using said non-voice network interface on a non-voice network.

In an analogous art**, De Oliveira** teaches the functionality of:

wherein said network interface comprises a non- voice network interface, and wherein codes for directing said processor circuit to transmit include codes for directing said processor circuit to cause said access code reply message to be transmitted using said non-voice network interface on a non-voice network ***(Col. 8 lines 42-48: transmitting a reply message from the further system (VMS2) via the network interface (FDDI) and the message path (NW) to said one system (VMS1) having transmitted the broadcast message, said reply message containing all control data identifying the home mailbox, including an associated personal access code and a directory).***

Therefore, it would have been obvious to one of the ordinary skill in the art at the time the invention was made to provide the technique of **De Oliveira** to the system of **Elliott and Albina** in order to provide and voice and fax system over the Fiber

Distributed Data Interface ***(De Oliveira, [Abstract]).***

Regarding claims 51 and 70, the claims are interpreted and rejected for the same reason as set forth in claim **89.**

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. **Guedalia** et. al, US Pub **2007/0112964 A1**: Caller-Callee association of a plurality of networked devices.

2. **Wipliez** et al. US Pat **7,079,526 B1**: caller is calling callee (fig. 2 and abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to M MOSTAZIR RAHMAN whose telephone number is (571)272-4717. The examiner can normally be reached on M-F: 8:00AM-4:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, UN C. CHO can be reached on 571-272-7919. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M MOSTAZIR RAHMAN/
Examiner, Art Unit 2413

/UN C. CHO/
Supervisory Patent Examiner, Art Unit 2413

Notice of References Cited	Application/Control No. 13/056,277	Applicant(s)/Patent Under Reexamination BJORSELL ET AL.	
	Examiner M MOSTAZIR RAHMAN	Art Unit 2413	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,454,030 A	09-1995	de Oliveira et al.	379/100.08
*	B	US-2002/0122391 A1	09-2002	Shalit, Andrew L.	370/260
*	C	US-6,674,745 B1	01-2004	Schuster et al.	370/352
*	D	US-2004/0022237 A1	02-2004	Elliott et al.	370/356
*	E	US-7,079,526 B1	07-2006	Wipliez et al.	370/352
*	F	US-2007/0112964 A1	05-2007	Guedalia et al.	709/227
*	G	US-2008/0056235 A1	03-2008	Albina et al.	370/352
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13056277	BJORSELL ET AL.
	Examiner	Art Unit
	M MOSTAZIR RAHMAN	2413

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
370	310-338	03/13/2013	MR

SEARCH NOTES		
Search Notes	Date	Examiner
EAST Search: 1)keyword search in USPAT, US-PGPUB, DERWENT, EPO, JPO, IBM_TDB; 2) class/subclasses, inventors, assignee	03/13/2013	MR
Inventor and assignee search in eDAN and PALM.	03/13/2013	MR
Google Patent Search	03/13/2013	MR
IP.COM Search	03/13/2013	MR
Consulted with primary examiner, Xavier Wong.	03/13/2013	MR

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/M MOSTAZIR RAHMAN/ Examiner, Art Unit 2413	

ip.com
866.473.6826
Home About Search Publish Research & Analytics Solutions Innovation2

[morelike:patapp.US20110122827]

(*searching selected collections; filters have been applied*)

More-Like-This on the following document

Mobile gateway
US20110122827 -- US Applications -- 26-May-2011 -- DIGIFONICA (INTERNATIONAL) LIMITED
A method of initiating a call to a callee using a mobile telephone involves: receiving, from a user of the mobile telephone, a callee identifier associated with the callee; transmitting an access code request message to an access server, said access code request message including said callee identifier; receiving an...

Showing top twenty-five English Language results for each content group.Results per group: 25

All Content Groups
Focus on
- All Content Groups
- Prior Art Database
- Non-Patent Literature
- Patents and Applications

Filter by
Publication Date:
to
ex: 2004 or 2004-02 or 2004-02-27
Content Groups: view details
- Prior Art Database
- Non-Patent Literature
- Patents and Applications

Clear All Check All

Prior Art Database (25 of 20306) more

Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping (RFC3398)
This document describes a way to perform the mapping between two signaling protocols: the Session Initiation Protocol (SIP) and the Integrated Services Digital Network (ISDN) User Part... 01-Nov-2002

SIP: Session Initiation Protocol (RFC2543)
The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants. These sessions... 01-Mar-1999

A SIP portal system for globalized SIP addressing and efficient call routing
A system is disclosed in which users are provided with temporary SIP endpoint-ID. Their access to VOIP is mediated via the dynamically assigned SIP endpoint ID (consists of an end point... 03-Apr-2006

Telephone Message Reply-By Mechanism
Current mail systems provide a multiplicity of means for conveying and automating Reply-by fields for electronic distributions. Often within an office environment users utilize telephone... 01-Jan-1994

Method for Phone Call Interception of Calls Deemed Important
Provided to a user is the ability to set up criteria for messages which are deemed important. Message content may be configured with voice prints or content by string specification... 01-May-1993

A Phone Message Pad
Disclosed is a graphical expression of an on-screen memo, under a computer-telephony integrated environment, which automatically displays information about the originating caller, the... 28-Jul-2005

Method of Direct to Hold for Mobile Phones
Disclosed is a method of informing callers to cell phones that the callee is repositioning to answer the call. A method of indicating how long the expected wait is also disclosed. 23-Aug-2007

Toward the PSTN/Internet Inter-Networking--Pre-PINT implementations (RFC2458)
This document contains the information relevant to the development of the inter-networking interfaces underway in the Public Switched Telephone Network (PSTN)/Internet Inter-Networking... 01-Nov-1998

A Method for Accepting or Rejecting Phone Calls Based on Caller's Voice Imprint
Currently telephone stalking victims have limited options when trying to avoid their stalker. Typically, caller id is used to screen unwanted calls. However, the stalker may use a friend's... 01-Feb-2007

RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals (RFC2833)
This memo describes how to carry dual-tone multifrequency (DTMF) signaling, other tone signals and telephony events in RTP packets. 01-May-2000

Method for Informing Callers of Forwarded Telephone
Provided is an option to a user for setting a telephone apparatus mode of automatically indicating to a caller that the telephone is forwarded and optionally provide forwarded number... 01-Oct-1993

Dial Tone Modulation Frequency Action Mechanism
This article describes a mechanism for managing touch-tone signals from an incoming phone call so that the touch-

tone signals can be used directly by the recipient of the call in subsequent... 01-Jun-1992

Voice Based Automatic Call Screening
There are existing techniques to block unwanted phone calls. For example, systems that detect that the call was made by a computer or detect the caller id of the call and block these calls.... 14-May-2004

Extended MRET service
Recently, more and more mobile operators launch their 3G services. Most of them are running a hybrid 2G/3G network and their users in 2G (GSM) network are much more than those in 3G (UMTS).... 17-Oct-2006

Method for Automatic Directory Update upon Encounter of Specific Callee Messages
Provided is an automatic update of a Rolodex or Address Book (AB) application, as a result of an auto-dialed phone number, using a phone number received in an encountered message. 01-Jan-1994

Display and user on cellular telephone (Radio)
Although Caller ID is currently implemented on digital cellular phones as well as land-line phones, it is sometimes easier to recognize a person's face than to recognize his/her voice. 01-Jun-1999

Authorized Access to In-Progress Telephone Calls
When a telephone user places a call and receives a busy signal, the caller often needs to know who the callee is talking to, and how long the conversation has been in progress, but there is... 01-Feb-1994

Prank Call Deterent Means
Prank telephone calls will be deterred when prank callers realize that their calling locations will be apparent to the receivers of their calls. This is accomplished when the method... 01-Dec-1982

Enhanced Inbound Call Blocking
Disclosed is a Personal Identification Number (PIN) pass-through telephony mechanism based on a many-to-many mapping of a caller PIN and a callee code using a temporary ID that can be... 09-Mar-2006

Automatic contact number selection based on user location, availability, and message type
Proposed is a method and apparatus enabling a caller to dial once and reach the callee's nearest/best receiving device the first time. 29-Oct-2007

Accounting System for Rolm 244 PC Adapter using Caller Voice Recognition
A set of programs is described which intercepts incoming calls, ensures the caller is known by source phone number or voice match and allows automatic management of billing information for... 01-Mar-1993

Method for Automatically Leaving Messages on Answer Machines Depending on the Outgoing Message
Provided to a user is the ability to define one or more outgoing messages which may automatically be left on a person's answer machine or answering phone mail system. 01-May-1993

Return Receipt by consent for phone calls and e-mail
In current technology, one cannot know if a call, and an SMS, or an e-mail was not answered because it was not seen, or despite its having been seen. For example, a phone call can occur... 18-Jun-2008

Method for Dialing Automated Rolodex Topic Entry
Provided is an automated method for calling rolodex entries which are filed by topic. 01-Feb-1994

Multiple Threads to Implement Dual-Mode Operation for Person-to-Person Communication
Disclosed is a scheme for implementing Person-to-Person communications over communication links of different types (e.g., LAN, Async, ISDN), in which only point-to-point connection is... 01-Jun-1993

Patents and Applications (25 of 1838127) next

Caller-callee association of a plurality of networked devices caller-callee association of a plurality of networked devices
The present disclosure generally relates to systems and methods for establishing and maintaining communication between two or more communication devices coupled to communication networks.... 11-Jan-2007

Caller-callee association of a plurality of networked devices
The present disclosure generally relates to systems and methods for establishing and maintaining communication between two or more communication devices coupled to communication networks.... 17-May-2007

Caller-Callee Association of a Plurality of Networked Devices with Direct Dial Through Thin Client
The present disclosure generally relates to systems and methods for establishing and maintaining communication between two or more communication devices coupled to communication networks.... 21-Jun-2007

Caller-callee association of a plurality of networked devices

System and method for advertising using data network telephone connections
A system and method for providing advertising and advertising services using a telephone system. A data network telephony system includes a commercial message server that communicates with a... 30-Aug-2005

Time based regulation of access to callees
A method, system, and program for time based regulation of access to callees are provided. An authenticated

identity of a caller placing a call is preferably detected. Then, a communication... 21-Aug-2003

System and method for providing call-handling services on a data network telephone system
A system and method for providing call handling services on a data network telephony system. A portable information device, such as a PDA, associated with a user contains the user's address... 24-Jun-2003

Identifying relevant scheduling events for a call
A method, system, and program for identifying relevant scheduling events for a call. When a call is received at a service provider, the service provider initiates a call context request. A... 19-Jun-2003

Just-in-time call registration for mobile call to voip device
A method for establishing a hybrid voice session between a mobile device and a VoIP device is disclosed. A caller using a mobile device in a mobile network initiates a request for a voice... 24-Jul-2008

Associating a telephone call with a dialog associating a telephone call with a dialog based on a computer protocol such as sip
Providing non-voice capabilities relating to a phone call at a computing device includes receiving a request to begin a telephone call from a first telephone to a second telephone, wherein... 22-Feb-2007

Identifying a context for a call
A method, system, and program for identifying a context for a call are provided. Multiple context clues for a call are detected from a line number, a line subscriber profile, a caller... 19-Jun-2003

Identifying a call made or received on behalf of another
A system, system, and program for identifying a call made or received on behalf of another are provided. In particular, a call request for a call is detected. A context for the call is... 19-Jun-2003

Producing routing messages for voice over ip communications producing routing messages for voice over ip communications
A process and apparatus to facilitate communication between callers and callees in a system comprising a plurality of nodes with which callers and callees are associated is disclosed. In... 08-May-2008

Compensating recipients of calls
A method, system, and program for compensating recipients of calls are provided. A request to bill a caller a tariff for a call is initiated, wherein the caller originates the call. The... 19-Jun-2003

System and method for providing user mobility services on a telephony network
A system and method for providing user mobility services on a data network telephony system. User attributes may be transmitted from a portable information device, such as a personal digital... 03-Sep-2002

Intermediary device based callee identification
A method, system, and program for intermediary device initiated callee identification are provided. A trusted telephone network detects a call receipt connection from a destination device.... 23-Jan-2007

Time based regulation of use of a telephone line
A method, system, and program for time based regulation of use of a telephone line are provided. An identity of a first caller requesting use of a telephone line is detected. Use of the... 28-Aug-2003

Systems and Methods for Providing Communications Services Using Assigned Codes
A communications service (and components thereof) have one or more communication addresses (e.g. short codes, telephone numbers, IM names/domains, IP addresses, etc.) for receiving... 24-Apr-2008

Distributing billing for a call between a caller and a callee
A method, system, and program for distributing billing for a call between a caller and a callee are provided. Responsive to receiving a call request, a caller billing plan for an... 19-Jun-2003

Destination device billing according to call recipient
A method, system, and program for billing for service provided to destination device according to the calling plan of the individual receiving the call. An authenticated identity for a... 19-Jun-2003

Associating a telephone call with a dialog based on a computer protocol such as SIP
Providing non-voice capabilities relating to a phone call at a computing device includes receiving a request to begin a telephone call from a first telephone to a second telephone, wherein... 15-Feb-2007

System and method for controlling telephone service using a wireless personal information device
A system and method for accessing a data network telephony account using a wireless personal information device (PID). The user may connect over the wireless cellular infrastructure to a... 21-Mar-2006

Destination device order billing according to call recipient
A method, system, and program for billing for orders placed from a destination device according to the calling plan of the individual receiving the call. An authenticated identity for a... 27-Oct-2005

Origin device order billing according to caller
A method, system, and program for billing for order places from an origin device according to the current caller billing plan are provided. A billing plan associated with an authenticated... 27-Oct-2005

Intermediary Device Based Callee Identification

Methods, systems, and products for informing a caller of a callee identity are disclosed that include: detecting a call receipt condition from a destination device at a trusted telephone... 11-Oct-2007

ip.com

866.473.6826

Home About Search Publish Research & Analytics Solutions InnovationIQ

Method for facilitating communication between remote services and applications installed on e.g. personal computer, involves transmitting multiple application-specific messages from data management system (DMS) server to DMS client

(*searching selected collections*)

Semantic Gist Search on the provided text

Method for facilitating communication between remote services and applications installed on e.g. personal computer, involves transmitting multiple application-specific messages from data management system (DMS) server to DMS client

Please note that your query includes some special characters (such as * ? ( )) or a term that starts with http://. For these results any special characters have been ignored and all the terms have been treated as keywords.

All Content Groups

Focus on

- All Content Groups
- Prior Art Database
- Non-Patent Literature
- Patents and Applications

Filter by

Publication Date:

to

ex: 2004 or 2004-02 or 2004-02-05

Content Groups: View details

- Prior Art Database
- Non-Patent Literature
- Patents and Applications

Clear All Check All

Shared heartbeat service for managed devices

US20110296011 — US Applications — 01-Dec-2011 — OpenPeak Inc.

Systems, methods, and apparatuses for facilitating communication between remote services and applications installed on a device are described. In accordance with embodiments, each of a plurality of remote services generates an application-specific message intended for processing by a corresponding application installed...

Shared heartbeat service for managed devices shared heartbeat service for managed devices

WO2011150234A1 — WIPO Applications — 01-Dec-2011

Systems and methods for facilitating communication between remote services and applications installed on a device are described. Each remote service generates an application-specific message intended for processing by a corresponding application installed on a device and transmits the message to a device management...

Apparatus and methods for use of access tokens in an internet document management system

US6314425 — US Patents — 06-Nov-2001 — Critical Path, Inc.

An Internet-based document management system and methods are provided wherein access to the system and its services may be controlled through use of access tokens. The Internet-based document management system allows an electronic document to be stored on an Internet-accessible server and accessed using a previously...

Internet document management system and methods

US6584488 — US Patents — 24-Jun-2003 — Critical Path, Inc.

An Internet-based document management system and methods are provided wherein an electronic document may be stored on an Internet-accessible server and accessed using a previously known web browser, downloaded for review or manipulation, and then returned to the server for access by further users. The server is...

Multi-network monitoring architecture

US20050225936 — US Applications — 20-Oct-2005 — CARTER CLAUDIU

A network monitoring architecture for multiple computer network systems is disclosed. In particular, the network monitoring architecture includes an agent system installed within each computer network and a remote central management unit in communication with the agent system of each computer network. The agent systems...

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 2403

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/056,277	01/27/2011	370	2413	SMARB19.004APC

APPLICANTS

Johan Emil Viktor Bjorsell, Vancouver, BC, CANADA;
Maksym Sobolyev, New Westminster, BC, CANADA;
Pentti Kalevi Huttunen, Vancouver, BC, CANADA;

**** CONTINUING DATA ***************************

This application is a 371 of PCT/CA2009/001062 07/28/2009
which claims benefit of 61/129,898 07/28/2008

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
02/16/2011

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /M MOSTAZIR RAHMAN/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		BC	17	90	8

ADDRESS

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614
UNITED STATES

TITLE

MOBILE GATEWAY

FILING FEE RECEIVED		
2860	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/056,277
	Filing Date	January 27, 2011
	First Named Inventor	Johan Emil Viktor Bjorsell et al.
	Art Unit	~~2473~~ 2413
(Multiple sheets used when necessary)	Examiner	~~Kwang Bin Yao~~ Rahman, M Mostazir
SHEET 1 OF 1	Attorney Docket No.	SMARB19.004APC

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	1	7,055,174 B1	05-30-2006	Cope et al.	
	2	2003/0200311 A1	10-23-2003	Baum	
	3	2004/0240439 A1	12-02-2004	Castleberry et al.	
	4	2006/0072550 A1	04-06-2006	Davis et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T[1]
	5	WO 01/89145 A2	11-22-2001	Telefonaktiebolaget LM Ericsson		

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[1]
	6	EPO, Supplementary European Search Report, dated November 2, 2012, Application No. 07855436.7, corresponds to U.S. Application No. 12/517,026, Attorney Docket No. SMARB19.002APC.	

14649429:djl
011113

Examiner Signature	/M MOSTAZIR RAHMAN/	Date Considered	03/22/2013

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

T[1] - Place a check mark in this area when an English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT		
	Application No.	~~Unknown~~ 13/056,277
	Filing Date	~~Herewith~~
	First Named Inventor	Johan Emil Viktor Bjorsell
	Art Unit	~~Unassigned~~ 2413
(Multiple sheets used when necessary)	Examiner	~~Unassigned~~ Rahman, M Mostazir
SHEET 1 OF 1	Attorney Docket No.	SMARB19.004APC

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	1	2007/0112964 A1	05-17-2007	Guedalia et al.	
	2	2004/0022237 A1	02-05-2004	Elliot et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T[1]

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[1]
	3	A copy of the International Search Report and Written Opinion mailed on March 12, 2010 for corresponding PCT Application No. PCT/CA2009/001062.	

10416667\cey
012711

Examiner Signature	/M MOSTAZIR RAHMAN/	Date Considered	03/22/2013

***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

T[1] - Place a check mark in this area when an English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT		
	Application No.	13/056277
	Filing Date	01-27-2011
	First Named Inventor	Johan Emil Viktor Björsell et al
	Art Unit	~~2472~~ 2413
(Multiple sheets used when necessary)	Examiner	~~Unassigned~~ Rahman, M Mostazir
SHEET 1 OF 5	Attorney Docket No.	SMARB19.004APC

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	1	4,916,491	04-10-1990	Katoh	
	2	5,146,491	09-08-1992	Silver et al.	
	3	5,247,571	09-21-1993	Kay et al .	
	4	5,303,297	04-12-1994	Hillis	
	5	5,359,642	10-25-1994	Castro	
	6	5,425,085	06-13-1995	Weinberger et al.	
	7	5,440,621	08-08-1995	Castro	
	8	5,469,497	11-21-1995	Pierce et al.	
	9	5,506,893	04-09-1996	Buscher et al.	
	10	5,519,769	05-21-1996	Weinberger et al.	
	11	5,559,871	09-24-1996	Smith	
	12	5,590,133	12-31-1996	Billstrom et al.	
	13	5,608,786	05-04-1997	Gordon	
	14	5,621,787	04-15-1997	McKoy et al.	
	15	5,661,790	08-26-1997	Hsu	
	16	5,712,907	01-27-1998	Wegner et al.	
	17	5,724,355	05-03-1998	Bruno et al.	
	18	5,726,984	05-10-1998	Kubler et al.	
	19	5,737,414	04-07-1998	Walker et al.	
	20	5,751,961	05-12-1998	Smyk	
	21	5,793,762	08-11-1998	Penners et al.	
	22	5,799,072	08-25-1998	Vulcan et al.	
	23	5,802,502	09-01-1998	Gell et al.	
	24	5,825,863	10-20-1998	Walker	
	25	5,828,740	10-27-1998	Khuc et al.	
	26	5,838,682	11-17-1998	Dekelbaum et al.	
	27	5,845,267	12-01-1998	Ronen	
	28	5,850,433	12-15-1998	Rondeau	
	29	5,864,610	01-26-1999	Ronen	

Examiner Signature	Date Considered
***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

T[1] - Place a check mark in this area when an English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT		
	Application No.	13/056277
	Filing Date	01-27-2011
	First Named Inventor	Johan Emil Viktor Björsell et al
	Art Unit	~~2473~~ 2413
(Multiple sheets used when necessary)	Examiner	~~Unassigned~~ Rahman, M Mostazir
SHEET 2 OF 5	Attorney Docket No.	SMARB19.004APC

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	30	5,867,495	02-02-1999	Elliott et al.	
	31	5,883,891	05-16-1999	Williams et al.	
	32	5,889,774	05-30-1999	Mirashrafi et al.	
	33	5,905,736	05-18-1999	Ronen et al.	
	34	5,907,547	05-25-1999	Foladare et al.	
	35	5,910,946	06-08-1999	Csapo	
	36	5,915,005	06-22-1999	He	
	37	5,923,659	01-30-2001	Curry et al.	
	38	5,930,343	07-27-1999	Vasquez	
	39	5,937,045	08-10-1999	Yaoya et al.	
	40	5,940,598	08-17-1999	Strauss et al.	
	41	5,953,504	09-14-1999	Sokal et al.	
	42	5,956,391	09-21-1999	Melen et al.	
	43	5,970,477	10-19-1999	Roden	
	44	5,974,043	10-26-1999	Solomon	
	45	5,991,291	11-23-1999	Asai et al .	
	46	6,005,926	12-21-1999	Mashinsky	
	47	6,014,379	01-11-2000	White et al.	
	48	6,021,126	02-01-2000	White et al.	
	49	6,052,445	10-28-2003	Bashoura et al.	
	50	6,058,300	05-02-2000	Hanson	
	51	6,069,890	05-30-2000	White et al.	
	52	6,073,013	06-06-2000	Agre et al.	
	53	6,104,704	08-15-2000	Buhler et al.	
	54	6,104,711	08-15-2000	Voit	
	55	6,115,737	09-05-2000	Ely et al.	
	56	6,128,304	10-03-2000	Gardell et al.	
	57	6,137,869	10-24-2000	Voit, Eric A., et al.	
	58	6,141,404	10-31-2000	Westerlage et al.	

Examiner Signature	/M MOSTAZIR RAHMAN/	Date Considered	03/22/2013

***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

T[1] - Place a check mark in this area when an English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT		
	Application No.	13/056277
	Filing Date	01-27-2011
	First Named Inventor	Johan Emil Viktor Björsell et al
	Art Unit	~~2473~~ 2413
(Multiple sheets used when necessary)	Examiner	~~Unassigned~~ Rahman, M Mostazir
SHEET 3 OF 5	Attorney Docket No.	SMARB19.004APC

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	59	6,188,752	02-13-2001	Lesley	
	60	6,282,574	08-28-2001	Voit	
	61	6,298,062	10-02-2001	Gardell et al.	
	62	6,351,464	02-26-2002	Galvin et al.	
	63	6,359,880	05-19-2002	Curry et al.	
	64	6,430,275	08-06-2002	Voit et al	
	65	6,507,644	01-14-2003	Henderson et al.	
	66	6,766,159	07-20-2004	Lindholm	
	67	6,819,929	11-16-2004	Antonucci et al.	
	68	6,954,453	10-11-2005	Schindler	
	69	7,068,772	06-27-2006	Widger et al.	
	70	7,120,682	10-10-2006	Salama	
	71	7,212,522	05-01-2007	Shankar et al.	
	72	7,454,510	11-18-2008	Kleyman et al.	
	73	2002/0051518 A1	05-02-2002	Bondy et al.	
	74	2002/0116464 A1	08-22-2002	Mak	
	75	2003/0219103 A1	11-27-2003	Rao et al.	
	76	2004/0157629 A1	08-12-2004	Kallio et al.	
	77	2004/0165709 A1	08-26-2004	Pence et al.	
	78	2004/0181599 A1	09-16-2004	Kreusch et al.	
	79	2004/0202295 A1	10-14-2004	Shen et al.	
	80	2004/0255126 A1	12-16-2004	Reith	
	81	2005/0083911 A1	04-21-2005	Grabelsky et al.	
	82	2005/0094651 A1	05-05-2005	Lutz et al.	
	83	2005/0169248 A1	08-04-2005	Truesdale et al.	
	84	2005/0174937 A1	08-11-2005	Scoggins et al.	
	85	2005/0177843 A1	08-11-2005	Williams	
	86	2006/0072547 A1	04-06-2006	Florkey et al.	
	87	2006/0111116 A1	05-25-2006	Palmer et al.	

Examiner Signature	/M MOSTAZIR RAHMAN/	Date Considered	03/22/2013

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

T[1] - Place a check mark if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT		
	Application No.	13/056277
	Filing Date	01-27-2011
	First Named Inventor	Johan Emil Viktor Björsell et al
	Art Unit	~~2473~~ 2413
(Multiple sheets used when necessary)	Examiner	~~Unassigned~~ Rahman, M Mostazir
SHEET 4 OF 5	Attorney Docket No.	SMARB19.004APC

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	88	2006/0160565 A1	07-20-2006	Singh et al.	
	89	2006/0177035 A1	08-10-2006	Cope et al.	
	90	2006/0209768 A1	09-21-2006	Yan et al.	
	91	2007/0036143 A1	02-15-2007	Alt et al.	
	92	2007/0253418	11-01-2007	Shiri et al.	
	93	2008/0037715 A1	02-14-2008	Prozeniuk et al.	
	94	2008/0063153 A1	03-13-2008	Krivorot et al.	
	95	2009/0028146 A1	01-29-2009	Kleyman et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T[1]
	96	CA 2,249,668	04-07-1999	Bruno et al.		
	97	EP 1 389 862 A1	02-18-2004	Shen et al.		
	98	WO 2007/044454 A2	04-19-2007	Croy et al.		
	99	WO 2008/052340 A1	05-08-2008	Perreault et al.		
	100	WO 2008/064481 A1	06-05-2008	Bjorsell et al.		
	101	WO 2008/116296 A1	10-02-2008	Bjorsell et al.		

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[1]
	102	A copy of the International Preliminary Report on Patentability and Written Opinion of the International Searching Authority mailed February 10, 2011 for related PCT Application No. PCT/CA2009/001062., February 10, 2011.	
	103	A copy of the International Preliminary Report on Patentability mailed February 13, 2009 for corresponding PCT/CA2007/002150.	
	104	A copy of the International Preliminary Report on Patentability mailed May 14, 2009 for related PCT/CA2007/001956.	
	105	A copy of the International Search Report and Written Opinion of the International Searching Authority completed February 6, 2008 for corresponding PCT/CA2007/001956.	
	106	A copy of the International Search Report and Written Opinion of the International Searching Authority completed June 6, 2008 for corresponding PCT/CA2008/000545.	

Examiner Signature	/M MOSTAZIR RAHMAN/	Date Considered	03/22/2013

***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] - Place a check mark if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/056277
	Filing Date	01-27-2011
	First Named Inventor	Johan Emil Viktor Björsell et al
	Art Unit	~~2473~~ 2413
(Multiple sheets used when necessary)	Examiner	~~Unassigned~~ Rahman, M Mostazir
SHEET 5 OF 5	Attorney Docket No.	SMARB19.004APC

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[1]
	107	A copy of the International Search Report completed on March 3, 2008 for corresponding PCT/CA2007/002150.	
	108	A copy of the Written Opinion and International Search Report completed on June 17, 2010 for related PCT Application No. PCT/CA2009/001317.	
	109	Cisco. "Lawful Intercept Requirements Summary." http://www.faqs.org/rfcs/rfc3924.html. November 8, 2006.	
	110	ETSI Technical Specification. "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services." Apr 2008, 25 pgs, v.2.3.1, France.	
	111	F. Baker et al. "RFC 3924 - Cisco Architecture for Lawful Intercept in IP Networks." October 2004.	
	112	M. Handley et al. "RFC 2543 - SIP: Session Initiation Protocol." March 1999.	
	113	Sippy SIP B2BUA. "About Sippy RTPproxy." http://www.rtpproxy.org. July 15, 2009.	

11179724
050411

Examiner Signature	/M MOSTAZIR RAHMAN/	Date Considered	03/22/2013

***Examiner**: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

T[1] - Place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/056,277
	Filing Date	January 27, 2011
	First Named Inventor	Johan Emil Viktor Bjorsell et al.
	Art Unit	~~2473~~ 2413
(Multiple sheets used when necessary)	Examiner	~~Kwang Bin Yao~~ Rahman, M Mostazir
SHEET 1 OF 1	Attorney Docket No.	SMARB19.004APC

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T[1]
	1	EP 1 389 862 B1	11/3/2004	Shen et al.		

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[1]
	2	A copy of the International Preliminary Report on Patentability issued on September 29, 2009 for PCT/CA2008/000545.	
	3	A copy of the International Preliminary Report on Patentability issued on March 20, 2012 for PCT/CA2009/001317.	
	4	Townsley, et al.; "RFC 2661 - Layer Two Tunneling Protocol 'L2TP' ", August 1999.	
	5	IP2Location, http://www.ip2location.com/; printed June 20, 2012.	
	6	DOTS IP Address Validation, "Overview", http://www.serviceobjects.com/products/dots_ipgeo.asp; printed June 21, 2012.	
	7	List of North American Numbering Plan area codes, http://en.wikipedia.org/wiki/List_of_NANP_area_codes; printed June 20, 2012.	
	8	DOTS Phone Exchange, "Overview", http://www.serviceobjects.com/demos/PhoneExchangeDemo.asp (URL no longer valid, current URL is http://www.serviceobjects.com/products/phone/phone-exchange); printed June 21, 2012.	
	9	Rosenberg, et al.; "RFC 3261 - SIP: Session Initiation Protocol", June 2002.	

13465299-sjw 061512

Examiner Signature	/M MOSTAZIR RAHMAN/	Date Considered	03/22/2013

***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

T[1] - Place a check mark in this area when an English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R./

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT		
	Application No.	13/056,277
	Filing Date	January 27, 2011
	First Named Inventor	Johan Emil Viktor Bjorsell et al.
	Art Unit	~~2473~~ 2413
(Multiple sheets used when necessary)	Examiner	~~Kwang-Bin Yao~~ Rahman, M Mostazir
SHEET 1 OF 1	Attorney Docket No.	SMARB19.004APC

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	1	8,116,307	2/14/2012	Thesayi et al.	
	2	2006/0093135 A1	5/4/2006	Fiatal et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T[1]

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[1]

13685123-sjw 072612

Examiner Signature	/M MOSTAZIR RAHMAN/	Date Considered	03/22/2013

***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

T[1] - Place a check mark in this area when an English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT		
	Application No.	13/056,277
	Filing Date	January 27, 2011
	First Named Inventor	Johan Emil Viktor Bjorsell et al.
	Art Unit	~~2473~~ 2413
(Multiple sheets used when necessary)	Examiner	~~Kwang Bin Yao~~ Rahman, M Mostazir
SHEET 1 OF 1	Attorney Docket No.	SMARB19.004APC

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	1	6,151,385	11/21/2000	Reich et al.	
	2	6,597,686	7/22/2003	Darek A Smyk	
	3	6,724,860	4/20/2004	Stumer et al.	
	4	6,744,858	6/1/2004	Ryan et al.	
	5	6,963,557	11/8/2005	Mark Clinton Knox	
	6	7,046,658	5/16/2006	Vinay Kundaje	
	7	2005/025043 A1	2/3/2005	Mussman et al	
	8	2006/0153342 A1	7/13/2006	Syouichi Sasaki	
	9	2006/0258328 A1	11/16/2006	Mario Francisco Godoy	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T[1]

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[1]
	10	Lind AT&T S: "ENUM Call Flows for VoIP Interworking; draft-lind-enum-callflows-03.txt", 20020201, no. 3, 1 February 2002, pages 1-17.	
	11	IETF ENUM WG R STASTNY OEFEG INFORMATIONAL NUMBERING FOR VOIP AND OTHER IP COMMUNICATIONS: "Numbering for VoIP and other IP Communications, draft-stastny-enum-numbering-voip-00.txt", 20031001, 1 October 2003, pages 1-43.	

13893588-sjw 083112

Examiner Signature	/M MOSTAZIR RAHMAN/	Date Considered	03/22/2013

***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] - Place a check mark in this area when an English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13056277	BJORSELL ET AL.
	Examiner	Art Unit
	M MOSTAZIR RAHMAN	2413

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	03/22/2013								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	✓								
	30	✓								
	31	✓								
	32	✓								
	33	✓								
	34	✓								
	35	✓								
	36	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13056277	BJORSELL ET AL.
	Examiner	Art Unit
	M MOSTAZIR RAHMAN	2413

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	03/22/2013								
	37	✓								
	38	✓								
	39	✓								
	40	✓								
	41	✓								
	42	✓								
	43	✓								
	44	✓								
	45	✓								
	46	✓								
	47	✓								
	48	✓								
	49	✓								
	50	✓								
	51	✓								
	52	✓								
	53	✓								
	54	✓								
	55	✓								
	56	✓								
	57	✓								
	58	✓								
	59	✓								
	60	✓								
	61	✓								
	62	✓								
	63	✓								
	64	✓								
	65	✓								
	66	✓								
	67	✓								
	68	✓								
	69	✓								
	70	✓								
	71	✓								
	72	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13056277	BJORSELL ET AL.
	Examiner	Art Unit
	M MOSTAZIR RAHMAN	2413

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	03/22/2013								
	73	✓								
	74	✓								
	75	✓								
	76	✓								
	77	✓								
	78	✓								
	79	✓								
	80	✓								
	81	✓								
	82	✓								
	83	✓								
	84	✓								
	85	✓								
	86	✓								
	87	✓								
	88	✓								
	89	✓								
	90	✓								

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/056,277
	Filing Date	January 27, 2011
	First Named Inventor	Johan Emil Viktor Bjorsell et al.
	Art Unit	~~2473~~ 2413
(Multiple sheets used when necessary)	Examiner	~~Kwang Bin Yao~~ Rahman, M Mostazir
SHEET 1 OF 1	Attorney Docket No.	SMARB19.004APC

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T[1]

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[1]
	1	Supplementary European Search Report for European Application No. 07816106 dated June 18, 2012.	

13927989-sjw 090712

Examiner Signature	/M MOSTAZIR RAHMAN/	Date Considered	03/22/2013

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] - Place a check mark in this area when an English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	2	"13056277"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/02/25 16:48
S2	34	("20060093135" | "20040022237" | "7055174" | "20060153342" | "20060258328" | "6724860" | "20070112964" | "7046658" | "20030200311" | "8116307" | "6151385" | "6597686" | "6744858" | "20060072550" | "20050025043" | "6963557" | "20040240439").PN.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/02/25 18:09
S6	4	((JOHAN) near2 (BJORSELL)).INV.	US-PGPUB; USPAT	OR	ON	2013/03/13 16:16
S7	3	((MAKSYM) near2 (SOBOLYEV)).INV.	US-PGPUB; USPAT	OR	ON	2013/03/13 16:16
S8	2	((PENTTI) near2 (HUTTUNEN)).INV.	US-PGPUB; USPAT	OR	ON	2013/03/13 16:17
S10	5	(digifonica).as.	US-PGPUB; USPAT	OR	ON	2013/03/13 16:21
S11	5	S6 or S7 or S8 or S10	US-PGPUB; USPAT	OR	ON	2013/03/13 16:21
S12	288340	(370/310-338,395.$.ccls. "379".clas. "709".clas. "455".clas.) and (@ad <"20080728" @rlad <"20080728")	US-PGPUB; USPAT	OR	ON	2013/03/13 16:29
S13	1195	((caller 'calling party')same (callee 'called party') same access same code same request same call$4)	US-PGPUB; USPAT	OR	ON	2013/03/13 16:33
S14	701	S12 and ((caller 'calling party')same (callee 'called party') same access same code same request same call$4)	US-PGPUB; USPAT	OR	ON	2013/03/13 16:33
S15	40	S12 and ((caller 'calling party')same (callee 'called party') same access same code same request same call$4 same server same rout$5)	US-PGPUB; USPAT	OR	ON	2013/03/13 16:34
S16	23	S12 and ((caller 'calling party')same (callee 'called party') same access same code same request same call$4 same server same rout$5 same (channel or (ID identifier identificat$5)))	US-PGPUB; USPAT	OR	ON	2013/03/13 16:36
S18	2	us-20070112964-$.did. us-20040022237-$.did.	US-PGPUB; USPAT	OR	ON	2013/03/13 16:49
S19	4	us-20070112964-$.did. us-20040022237-$.did.	US-PGPUB; USPAT; FPRS;	OR	ON	2013/03/13 16:49

			EPO; JPO; DERWENT; IBM_TDB			
S20	245256	(370/310-338,395.$.ccls. "709".clas. "455".clas.) and (@ad <"20080728" @rlad <"20080728")	US-PGPUB; USPAT	OR	ON	2013/03/13 16:52
S21	1	S20 and ((access adj code) same (channel adj (identifier ID identification) same request))	US-PGPUB; USPAT	OR	ON	2013/03/13 16:53
S22	366030	("370".clas. "709".clas. "455".clas.) and (@ad <"20080728" @rlad <"20080728")	US-PGPUB; USPAT	OR	ON	2013/03/13 16:54
S24	354	S22 and ((access adj code) same (channel ID identification) same request)	US-PGPUB; USPAT	OR	ON	2013/03/13 16:55
S25	8	S22 and ((access adj code) same (channel with (ID identification)) same request)	US-PGPUB; USPAT	OR	ON	2013/03/13 16:56
S26	10	S22 and ((access adj2 code) same caller same callee)	US-PGPUB; USPAT	OR	ON	2013/03/13 16:59
S27	58	S22 and ((phone caller callee 'calling party') same server same router same (initiat$4 or setup or sett$4)same channel)	US-PGPUB; USPAT	OR	ON	2013/03/13 17:05
S28	10	S22 and ((phone caller callee "calling party" "called party" "called terminal" "calling party") same server same rout$5 same (call near5 (initiat$4 or setup)) same channel same request same (ID identif$7))	US-PGPUB; USPAT	OR	ON	2013/03/13 17:19
S29	257	S22 and (caller callee "calling party" "called party" "called terminal" "calling party") same (call$3 near server) same (router gateway rout$3 adj control$5)	US-PGPUB; USPAT	OR	ON	2013/03/13 17:27
S30	72	S22 and (caller callee "calling party" "called party" "called terminal" "calling party") same (call$3 near server) same (router gateway rout$3 adj control$5) same access$5	US-PGPUB; USPAT	OR	ON	2013/03/13 17:28
S31	11	(US-20070281705-$ or US-20130028251-$ or US-20090252159-$ or US-20080049732-$ or US-20070121590-$ or US-20040042607-$ or US-20040022237-$ or US-20030114139-$ or US-20030095542-$).did. or (US-7068684-$ or US-6963635-$).did.	US-PGPUB; USPAT	OR	ON	2013/03/13 19:13
S32	9	S31 and ((caller callee "calling party" "called party" "called terminal" "calling party") same (call$3 near server) same (router gateway rout$3 adj control$5))	US-PGPUB; USPAT	OR	ON	2013/03/13 19:13
S33	3	S31 and ((caller callee "calling party" "called party" "called terminal" "calling party") same (call$3 near server) same (router gateway rout$3 adj control$5) and processor and interface and identification)	US-PGPUB; USPAT	OR	ON	2013/03/13 19:16
S34	7	S31 and ((caller callee "calling party" "called party" "called terminal" "calling	US-PGPUB; USPAT	OR	ON	2013/03/13 19:18

		party") same (call$3 near server) same (router gateway rout$3 adj control$5) and channel and (initiat$5 setup) and (identi$7 ID))				
S36	2	S31 and ((caller callee "calling party" "called party" "called terminal" "calling party") same (call$3 near server) same (router gateway rout$3 adj control$5) and channel and (initiat$5 setup) and (identi$7 ID) and voice and (location local$3 geograph$5 area) and number and expir$5)	US-PGPUB; USPAT	OR	ON	2013/03/13 19:22
S37	2	S31 and ((caller callee "calling party" "called party" "called terminal" "calling party") same (call$3 near server) same (router gateway rout$3 adj control$5) and channel and (initiat$5 setup) and (identi$7 ID) and voice and (location local$3 geograph$5 area) and number and expir$5 and (access adj code))	US-PGPUB; USPAT	OR	ON	2013/03/13 19:54
S39	3	"7079526".pn. us-20030114145-$.did. "6016319".pn.	US-PGPUB; USPAT	OR	ON	2013/03/14 11:27
S40	409041	("370".clas. "709".clas. "455".clas.) and (@ad <"20080728" @rlad <"20080728")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 11:17
S43	21100	S40 and (initiat$4 adj3 call)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 11:21
S44	128	S40 and ((initiat$4 adj2 call) same (access adj2 code))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 11:22
S45	101	S40 and ((initiat$4 adj2 call) same (access adj2 code) and (channel ID))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 11:23
S46	38	S40 and ((initiat$4 adj2 call) same (access adj2 code) and (channel ID) and ((voice data) adj2 network))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 11:23
S47	33	S40 and ((initiat$4 adj2 call) same (access adj2 code) and (channel ID) and ((non$voice data) adj2 network$5))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 11:25
S48	11	S40 and ((initiat$4 adj2 call) same (access adj2 code) and (channel ID)	US-PGPUB; USPAT;	OR	ON	2013/03/15 11:26

		and ((non$voice data) adj2 network$5) and (indentifier ID indentification))	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S49	35	("2006/0189337").URPN.	USPAT	OR	ON	2013/03/15 11:34
S52	409041	("370".clas. "709".clas. "455".clas.) and (@ad <"20080728" @rlad <"20080728")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 11:52
S53	0	S52 and ((initiat$4 adj2 call) same (access adj2 code) same (data adj2 network$5))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 11:52
S54	213	S52 and ((initiat$4 with call) same (access adj5 code) and (data with network$5))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 11:53
S55	159	S52 and ((initiat$4 with call) same (access adj5 code) and (data with network$5) and (wirless mobile handfree))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 11:54
S56	22	S52 and ((initiat$4 with call) same (access adj5 code) and (data with network$5) and (wirless mobile handfree) adj5 (IP or (internet adj2 protocol)))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 11:54
S57	20	S52 and ((initiat$4 with call) same (access adj5 code) and (data adj5 network$5) and (wirless mobile handfree) adj5 (IP or (internet adj2 protocol)))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 11:55
S58	17	(US-20070281705-$ or US-20130028251-$ or US-20090252159-$ or US-20080049732-$ or US-20070121590-$ or US-20040042607-$ or US-20040022237-$ or US-20030114139-$ or US-20030095542-$ or US-20030114145-$ or US-20070112964-$ or US-20060189337-$).did. or (US-7068684-$ or US-6963635-$ or US-7079526-$ or US-6016319-$).did. or (WO-2010012090-$).did.	US-PGPUB; USPAT; DERWENT	OR	ON	2013/03/15 12:01
S62	17	S58 and (server)	US-PGPUB; USPAT; DERWENT	OR	ON	2013/03/15 12:02
S64	181	S52 and (channel same (ID indentifier indentification) same request same server same (router rout$5 gateway	US-PGPUB; USPAT; FPRS;	OR	ON	2013/03/15 12:32

		adj control$5))	EPO; JPO; DERWENT; IBM_TDB			
S65	27	S52 and (channel same (ID indentifier indentification) same request same (call$5 near5 server) same (router rout$5 gateway adj control$5))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 12:33
S67	154	S64 not S65	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 12:34
S68	32	S52 and (channel same (ID indentifier indentification) same request same (call$5 near5 server) same (router rout$5 gateway))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 12:34
S69	2	S52 and (channel same (ID indentifier indentification) same request same (call$5 near5 server) same (router rout$5 gateway) and (wireless adj2 ip adj4 network$5))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 12:35
S73	5	S52 and (channel same (ID indentifier indentification) same request same (call$5 near5 server) same (router rout$5 gateway) AND (wireless with (ip or (internet adj2 protocol))))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 12:46
S74	12	S52 and (channel same (ID indentifier indentification) same request same (call$5 near5 server) same (router rout$5 gateway) AND ((wireless mobile) with (ip or (internet adj2 protocol))))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 12:48
S76	7	S74 not S73	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 12:49
S98	20	(US-20070281705-$ or US-20130028251-$ or US-20090252159-$ or US-20080049732-$ or US-20070121590-$ or US-20040042607-$ or US-20040022237-$ or US-20030114139-$ or US-20030095542-$ or US-20030114145-$ or US-20070112964-$ or US-20060189337-$ or US-20080056235-$ or US-20040205211-$).did. or (US-7068684-$ or US-6963635-$ or US-7079526-$ or US-6016319-$ or US-6674745-$).did. or (WO-2010012090-$).did.	US-PGPUB; USPAT; DERWENT	OR	ON	2013/03/15 16:13
S99	11	S98 and (local with number)	US-PGPUB; USPAT; DERWENT	OR	ON	2013/03/15 16:17

S100	9	S98 and (local near7 number)	US-PGPUB; USPAT; DERWENT	OR	ON	2013/03/15 16:19
S102	3	(US-20040022237-$ or US-20080056235-$).did. or (US-6674745-$).did.	US-PGPUB; USPAT	OR	ON	2013/03/15 16:49
S103	3	S102 AND (ip adj2 address)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 16:49
S105	2	S102 AND (ip adj2 address with (receiv$5 reception))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 16:50
S106	3	S102 AND (ip adj2 address with server)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/15 16:52

3/22/2013 10:50:51 AM
C:\Users\mrahman6\Documents\EAST\Workspaces\10010_Application_13_056277_MobileGate.wsp

Prior Art Finder

Top 10 | Scholar | Patents | Web | Books | People | Print

Search Terms

Add your own

- [x] mobile gateway
- [x] callee
- [x] callee identifier
- [x] mobile telephone
- [x] access code
- [ ] access server
- [ ] processor circuit
- [ ] routing controller
- [ ] codes
- [ ] code request message

Custom Date Range

Start date: MM/DD/YYYY

End date: 07/28/2008

Patents US20110122827 Related Results

Filing date › Any time–Jul 28, 2008

System and method for mobile telephone as audio gateway



www.google.com/patents/EP2030417B1?cl=en

Grant - Filed Nov 20, 2006 - Issued Jul 25, 2012 - L. Scott Shoebaum - Sony Ericsson Mobile Communications Ab

In one embodiment, a **mobile telephone** (12) requests: **access** to a wireless network (100), ... The **mobile telephone** (12) assigns a subnet internet protocol (IP) address to a ... The **mobile telephone** acts as a **gateway** or proxy for routing multimedia .... The processing device 32 executes **code** stored in a memory (not shown) ...

System and method for roaming for prepaid mobile telephone service



www.google.com/patents/EP1680590A4?cl=en

App. - Filed Mar 16, 2005 - Published Jun 7, 2006 - Cry Biran - Star Home Gmbh

The home intelligent **gateway** (102) and the visited intelligent **gateway** (106) are ... The present invention relates to **mobile telephone** networks, in general, and to providing ... A prepaid user pays in advance for airtime and is given **access** to the ... The SICAP platform in the home **mobile** network receives the USSD **code** and ...

Wireless wide area network (wwan) mobile gateway with ...



www.google.com/patents/EP2090026B1?cl=en

Grant - Filed Nov 9, 2007 - Issued May 2, 2012 - Michael D. Johnson - Kyocera Corporation

A wireless wide area network 'WWAN' **mobile gateway** (102) is configured to execute a ... **identifier** to the WWAN modem card (120) and to execute, in response to ... connected to a public switching system such as a public switched **telephone** .... system 104 operates in accordance **Code** Division Multiple **Access** (CDMA) ...

Mobile telephone gateway apparatus, communication system, and ...



www.google.com/patents/EP1708963A1?cl=en

App. - Filed Nov 2, 2003 - Published Oct 4, 2006 - Yoshy Sata - Sata, Yoshy

A **mobile telephone gateway** and call routing device (MPG) (121) disclosed by the present invention is physically coupled with **mobile** phone (100) which is ...

Caching transformed content in a mobile gateway

www.google.com/patents/EP1227637A2?cl=en

App. - Filed Jan 21, 2002 - Published Jul 31, 2002 - Brent Curtis - Microsoft Corporation

Application US20110122827



MOBILE GATEWAY

Show Claims

Inventors: Johan Emil Viktor BJORSELL, Maksym SOBOLYEV, Pentti Kalevi HUTTUNEN

Assignees: DIGIFONICA (INTERNATIONAL) LIMITED

Publication number: US20110122827

Application number: 13/058,277

Filing date: Jul 28, 2009

Find Prior Art Similar to This



A **mobile gateway** receives content from a content source and customizes the content ... a transform **identifier** are cached at the **mobile gateway** so that subsequent requests ... However, as the demand for constant **mobile access** to information has ... and PDAs are supporting **telephone**- and pager-like communication links.

Mobile gateway device



www.google.com/patents/EP2014061A2?cl=en

App. - Filed Apr 13, 2007 - Published Jan 14, 2009 - Brian Mcbride - Alcatel Lucent

The WS-**Mobile Gateway** is the interworking **gateway** between users of a **mobile** ... The **mobile gateway** of claim 2, wherein said **access** tunnel termination unit is an .... [0010] Web services applications are built with pieces of **code** and data that ...

Method and apparatus in a gateway for registering mobile routers ...



www.google.com/patents/EP1540915B1?cl=en

Grant - Filed Sep 17, 2003 - Issued Aug 29, 2012 - Marco Molteni - Cisco Technology, Inc.

identifying, by the **gateway** (12), a plurality of **mobile** routers (16) within the **mobile** ... initiating, by the **gateway** (12) and on behalf of each identified **mobile** router .... that enables **mobile** ad hoc network nodes to **access** a wide area network without .... in Figures 3A and 3B can be implemented as executable **code** stored on a ...

Mobile communication system, base station device, access gateway ...



www.google.com/patents/EP2129148A1?cl=en

App. - Filed Jan 30, 2008 - Published Dec 2, 2009 - Yuri Andamawanti Hapsari - NTT DoCoMo, Inc.

Mobile communication system, base station device, **access gateway** device, and tracking ... a newly-installed base station configured to send an **identifier** of the ...

Connector gateway



www.google.com/patents/EP1523152A2?cl=en

App. - Filed Oct 7, 2004 - Published Apr 13, 2005 - Kevin R. Corneille - Accenture Global Services GmbH

A connector **gateway** system that provides **mobile** devices with **access** to ... The connector **gateway** system comprises a **mobile** device that includes an ... a **code** segment that generates a connection request for a connector type for an ... the serial number and **telephone** number of the **mobile telephone** (if applicable), and/ or ...

Method and system for enabling personalized shared mobile phone usage



www.google.com/patents/US8611532



Grant - Filed Mar 4, 2008 - Issued Nov 13, 2012 - Nigel Waller - Movirtu Limited

Disclosed is a system and method for enabling personalized shared **mobile** ... short **code** followed by his account number on a borrowed handset to **access** a ...

See Patent Reports

Google Home - Sitemap - USPTO Bulk Downloads - Privacy Policy - Terms of Service - About Google Patents - Google Patents Help - Send Feedback

©2012 Google

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	:	Johan Emil Viktor Bjorsell, et al.
App. No.	:	13/056,277
Filed	:	January 27, 2011
For	:	MOBILE GATEWAY
Examiner	:	Rahman, Mostazir M.
Art Unit	:	2413
Conf No.	:	2403

REPLY TO NON-FINAL OFFICE ACTION WITH AMENDMENT

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In reply to the non-final Office Action dated April 11, 2013, Applicant presents the following amendments and remarks.

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks begin on page 21 of this paper.

AMENDMENTS TO THE CLAIMS

1. (**Currently Amended**) A method of ~~initiating a call to a callee using~~ roaming with a mobile telephone, the method comprising:

receiving, from a user of the mobile telephone, a callee identifier associated with the callee;

transmitting an access code request message to an access server, said access code request message including said callee identifier and a location identifier identifying a location of the mobile telephone;

receiving an access code reply message from the access server in response to said access code request message, said access code reply message including an access code different from said callee identifier and associated with said ~~callee~~ location identifier; and

initiating a call with the mobile telephone using said access code to identify the callee.

2. (**Original**) The method of claim **1** wherein transmitting comprises transmitting said access code request message to said access server on a non-voice network.

3. (**Cancelled**)

4. (**Currently Amended**) The method of claim ~~3~~ **1** wherein transmitting said location identifier comprises transmitting an IP address of the mobile telephone in a wireless IP network.

5. (**Currently Amended**) The method of claim ~~3~~ **1** wherein transmitting said location identifier comprises transmitting an identifier of a wireless voice signal station in wireless communication with the mobile telephone.

6. (**Currently Amended**) The method of claim ~~3~~ **1** wherein transmitting said location identifier comprises transmitting a user-configured identifier of a location associated with the mobile telephone.

7. (**Original**) The method of claim **1** wherein receiving said access code reply message comprises receiving said access code reply message from said access server on a non-voice network.

8. (**Original**) The method of claim **1** wherein receiving said access code reply message comprises receiving, in said access code reply message, said access code temporarily associated with said callee identifier.

9. (**Original**) The method of claim **1** wherein receiving said access code reply message comprises receiving, in said access code reply message, a telephone number identifying a channel operably configured to cooperate with an IP network to cause a call involving the mobile telephone and the callee to be routed through the IP network.

10. (**Original**) The method of claim **9** wherein initiating said call comprises engaging a routing controller to route said call on said IP network to the callee.

11. (**Currently amended**) The method of claim **1** further comprising:

receiving from the mobile telephone said access code request message;

communicating with a routing controller to obtain from the routing controller said access code wherein said access code identifies a communications channel associated with said location identifier and wherein said access code is useable by the mobile telephone to cause the routing controller to establish a call to the callee using the channel; and

transmitting said access code reply message to the mobile telephone.

12. (**Currently Amended**) A mobile telephone apparatus comprising:

means for receiving, from a user of the mobile telephone, a callee identifier associated with the callee;

transmitting means for transmitting an access code request message to an access server, said access code request message including said callee identifier and a location identifier identifying a location of the mobile telephone;

means for receiving an access code reply message from the access server in response to said access code request message, said access code reply message including an access code different from said callee identifier and associated with said ~~callee~~ location identifier; and

means for initiating a call using said access code to identify the callee.

13. (**Original**) The mobile telephone apparatus of claim **12** wherein said transmitting means comprises a non-voice network interface for transmitting said access code request message to said access server on a non-voice network.

14. (**Cancelled**)

15. (**Currently Amended**) The mobile telephone apparatus of claim ~~14~~ 12 wherein said location identifier comprises an IP address of the mobile telephone in a wireless IP network.

16. (**Currently Amended**) The mobile telephone apparatus of claim ~~14~~ 12 wherein said location identifier comprises an identifier of a wireless voice signal station in wireless communication with the mobile telephone.

17. (**Currently Amended**) The mobile telephone apparatus of claim ~~14~~ 12 wherein said location identifier comprises a user-configured identifier of a location associated with the mobile telephone.

18. (**Original**) The mobile telephone apparatus of claim **12** wherein said means for receiving an access code reply message comprises a non-voice network interface for receiving said access code reply message on a non-voice network.

19. (**Original**) The mobile telephone apparatus of claim **12** wherein said access code includes a telephone number.

20. (**Original**) The mobile telephone apparatus of claim **12** wherein said means for initiating comprises a mobile telephone network interface.

21. (**Currently amended**) A system for ~~initiating a call to a callee~~enabling roaming by a mobile telephone, the system comprising the mobile telephone apparatus of claim **12** and further comprising:

a routing controller; and

an access server comprising:

means for receiving from the mobile telephone said access code request message;

means for communicating with said routing controller to obtain from said routing controller said access code wherein said access code identifies a channel associated with said location identifier and wherein said access code is useable by the mobile telephone to cause the routing controller to establish a call to the callee using the channel; and

means for transmitting said access code reply message including said access code to the mobile telephone.

22. (**Currently Amended**) A mobile telephone apparatus comprising:

a processor circuit;

a network interface in communication with said processor circuit; and

a computer readable medium in communication with said processor circuit and encoded with codes for directing said processor circuit to:

receive, from a user of the mobile telephone, a callee identifier associated with the callee;

cause an access code request message to be transmitted to an access server, said access code request message including said callee identifier and a location identifier identifying a location of the mobile telephone;

receive an access code reply message from the access server in response to said access code request message, said access code reply message including an access code different from said callee identifier and associated with said ~~callee~~ location identifier; and

initiate a call using said access code to identify the callee.

23. (**Original**) The mobile telephone apparatus of claim **22** wherein said network interface comprises a non-voice network interface, and wherein said codes for directing said processor circuit to cause said access code request message to be transmitted include codes for directing said processor circuit to cause said access code request message to be transmitted to said access server using said non-voice network interface on a non-voice network.

24. (**Cancelled**)

25. (**Currently Amended**) The mobile telephone apparatus of claim ~~24~~ **22** wherein said location identifier comprises an IP address of the mobile telephone in a wireless IP network.

26. (**Currently Amended**) The mobile telephone apparatus of claim ~~24~~ **22** wherein said location identifier comprises an identifier of a wireless voice signal station in wireless communication with the mobile telephone.

27. (**Currently Amended**) The mobile telephone apparatus of claim ~~24~~ **22** wherein said location identifier comprises a user-configured identifier of a location associated with the mobile telephone.

28. (**Original**) The mobile telephone apparatus of claim **22** wherein said network interface comprises a non-voice network interface, and wherein said codes for directing said processor circuit to receive an access code reply message include codes for directing said processor circuit to cause said access code reply message to be received from said access server using said non-voice network interface on a non-voice network.

29. (**Original**) The mobile telephone apparatus of claim **22** wherein said access code includes a telephone number identifying a channel operably configured to cooperate with an IP network to cause a call involving the mobile telephone and the callee to be routed through the IP network.

30. (**Original**) The mobile telephone apparatus of claim **22** wherein said network interface comprises a mobile telephone network interface, and wherein said codes for directing said processor circuit to initiate include codes for directing said processor circuit to cause a call to be initiated using said mobile telephone network interface on a mobile telephone network.

31. (**Currently amended**) A system for ~~initiating a call to a callee~~enabling roaming by a mobile telephone, the system comprising the mobile telephone of claim **22** and further comprising:

a routing controller; and

an access server comprising a processor circuit and a computer readable medium in communication with the processor circuit, the computer readable medium encoded with codes for directing said processor circuit to:

receive from the mobile telephone said access code request message;

communicate with said routing controller to obtain from said routing controller said access code wherein said access code identifies a channel associated with said location identifier and wherein said access code is useable by the mobile telephone to cause the routing controller to establish a call to the callee using the channel; and

transmit said access code reply message to the mobile telephone.

32. (**Currently amended**) A computer readable medium encoded with codes for directing a processor circuit to ~~initiate a call to a callee using~~enable ~~a~~ mobile telephone roaming, said codes being operable to direct the processor circuit to:

receive, from a user of a mobile telephone, a callee identifier associated with a callee;

transmit an access code request message to an access server, said access code request message including said callee identifier and a location identifier identifying a location of the mobile telephone;

receive an access code reply message from the access server in response to said access code request message, said access code reply message including an access code different from said callee identifier and associated with said callee identifier; and

initiate a call using said access code to identify the callee.

33. **(Currently Amended)** A method for enabling ~~a~~ mobile telephone ~~to initiate a call to a callee through a channel~~roaming, the method comprising:

receiving from the mobile telephone an access code request message including a callee identifier associated with the callee and a location identifier identifying a location of the mobile telephone;

~~communicating with a routing controller to obtain from the routing controller~~ producing an access code identifying ~~the~~ a communication channel based on said location identifier, said access code being different from the callee identifier and useable by the mobile telephone to initiate a call to the callee using the channel; and

transmitting an access code reply message including said access code, to the mobile telephone.

34. **(Original)** The method of claim **33** wherein receiving comprises receiving said access code request message on a non-voice network.

35. **(Currently Amended)** The method of claim **33** wherein producing said access code comprises causing a ~~further comprising causing the~~ routing controller operably configured to route a call between said caller and said callee to produce said access code.

36. **(Currently Amended)** The method of claim ~~35~~ 33 wherein producing ~~comprises selecting~~ said access code comprises selecting said access code from a pool of access codes,

~~where~~wherein each access code in said pool of access codes identifies a respective telephone number or Internet Protocol (IP) network address.

37. (**Currently Amended**) The method of claim **36** further comprising determining from said location identifier ~~determining~~ a local calling area associated with the mobile telephone and selecting an access code associated with a calling area matching said local calling area associated with the mobile telephone.

38. (**Currently Amended**) The method of claim ~~**37**~~ **36** ~~wherein determining comprises accessing a dialing profile associated with the caller, said dialing profile including a location field having contents identifying at least a default location of the caller~~further comprising accessing a location field of a dialing profile associated with the caller when a local calling area cannot be determined from the contents of said location identifier and determining a local calling area associated with the mobile telephone from the contents of said location field and selecting an access code associated with a calling area matching the local calling area associated with the mobile telephone.

39. (**Currently Amended**) The method of claim ~~**37**~~ **33** wherein said location identifier ~~determining~~ comprises ~~receiving~~ an IP address of the mobile telephone in a wireless IP network.

40. (**Currently Amended**) The method of claim ~~**37**~~ **33** wherein said location identifier ~~determining~~ comprises ~~receiving~~ an identifier of a wireless voice signal station in wireless communication with the mobile telephone.

41. (**Currently Amended**) The method of claim ~~**37**~~ **33** wherein said location identifier ~~determining~~ comprises ~~receiving~~ a user-configured identifier of a location associated with the mobile telephone.

42. (**Cancelled**)

43. (**Currently Amended**) The method of claim **36** wherein at least one of said ~~each~~ access ~~code~~ codes in said pool of access codes ~~further~~ identifies ~~a respective channel operably configured to cooperate with~~ an IP network address as a possible channel through which said call can be conducted.~~to cause a call involving the mobile telephone and the callee to be routed through the IP network.~~

44. (**Currently Amended**) The method of claim **43** further comprising enabling ~~causing said routing controller to establish~~ ~~communication~~ communications between said caller and said callee to be established through an ~~said~~ IP network in response to a call received at said IP network address~~on said channel~~.

45. (**Currently Amended**) The method of claim **~~44~~ 36** ~~wherein producing~~wherein said access code request message includes a caller identifier and wherein the method further comprises associating ~~storing a~~ said caller identifier included in said access code request message ~~associated with the mobile telephone in association~~ with the selected ~~said~~ access code.

46. (**Cancelled**)

47. (**Currently Amended**) The method of claim **~~36~~45** ~~wherein producing~~ further ~~comprises~~ comprising associating ~~storing~~ said callee identifier included in said access code request message ~~in association~~ with ~~said~~ the selected access code.

48. (**Currently Amended**) The method of claim **47** wherein said associating said caller identifier and said callee identifier with the selected access code occurs only when:

a) the access code is not already associated with a callee id; or

b) the access code is already associated with a callee id, and a timeout value associated with that callee id has expired.~~producing further comprises searching said pool of access codes for an access code associated with said callee identifier to identify the channel usable by the mobile telephone to initiate a call to the callee.~~

49. (**Currently Amended**) The method of claim ~~35~~ 33 wherein producing further comprises ~~storing, in association~~ associating a timestamp with said access code, ~~a timestamp~~ for use in determining when the usability of said access code to initiate a call to the callee will expire, and causing said timestamp to be included in said access code reply message transmitted to the mobile telephone.

50. (**Currently Amended**) The method of claim **49** further comprising enabling communications to be established between said caller and said callee when the mobile telephone seeks to establish a call to said callee using the access code transmitted in the access code reply message when said timestamp associated with said access code indicates the usability of said access code has not expired and not enabling said communications to be established when said timestamp indicates the usability of said access code has expired.
~~wherein causing said routing controller to establish communication comprises causing said routing controller to establish communication only if the usability of said access code to initiate a call to the callee has not expired.~~

51. (**Original**) The method of claim **33** wherein transmitting comprises transmitting said access code reply message on a non-voice network.

52. (**Currently Amended**) A system for enabling ~~a~~ mobile telephone ~~to initiate a call to a callee through a channel~~ roaming, the system comprising:

means for receiving from the mobile telephone an access code request message including a callee identifier associated with the callee and a location identifier identifying a location of the mobile telephone;

means for ~~communicating with said routing controller to obtain from said routing controller~~ producing an access code identifying ~~the~~ a communication channel based on said location identifier, said access code being different from the callee identifier and useable by the mobile telephone to initiate a call to the callee using the channel; and

means for transmitting an access code reply message including said access code to the mobile telephone.

53. (**Original**) The system of claim **52** wherein said means for receiving comprises a non-voice network interface for receiving said access code request message on a non-voice network.

54. (**Currently Amended**) The system of claim **52** ~~further comprising~~ wherein said means for producing said access code comprises a routing controller operably configured to route a call between said caller and said callee.

55. (**Currently Amended**) The system of claim **54** wherein said means for producing said access code comprises a processor circuit operably configured to select said access code from a pool of access codes, where each access code in said pool of access codes identifies a respective telephone number or Internet Protocol (IP) network address.

56. (**Currently Amended**) The system of claim **55** wherein said processor circuit is operably configured to determine a local calling area associated with the mobile telephone from said location identifier and to select an access code associated with a calling area matching said local calling area associated with the mobile telephone.

57. (**Currently Amended**) The system of claim **56** further comprising:

a dialing profile associated with the caller, said dialing profile including a location field; and

wherein said processor circuit is operably configured to determine a local calling area associated with the mobile telephone from the contents of said location field and to select an access code associated with a calling area matching the local calling area associated with the mobile telephone, when a local calling area associated with the mobile telephone cannot be determined from said location identifier.

~~using a dialing profile associated with the caller, said dialing profile including a location field having contents identifying at least a default location of the caller.~~

58. (**Currently Amended**) The system of claim **56** wherein said location identifier includes ~~processor circuit is operably configured to determine a local calling area associated with the mobile telephone using~~ an IP address of the mobile telephone in a wireless IP network.

59. (**Currently Amended**) The system of claim **56** wherein said location identifier includes ~~processor circuit is operably configured to determine a local calling area associated with the mobile telephone using~~ an identifier of a wireless voice signal station in wireless communication with the mobile telephone.

60. (**Currently Amended**) The system of claim **56** wherein said location identifier includes ~~processor circuit is operably configured to determine a local calling area associated with the mobile telephone using~~ a user-configured identifier of a location associated with the mobile telephone.

61. (**Cancelled**)

62. (**Currently Amended**) The system of claim **55** wherein ~~each~~ at least one of said access ~~code~~ codes in said pool of access codes ~~further~~ identifies ~~a respective channel operably configured to cooperate with~~ an IP network ~~to cause a call involving the mobile telephone and the callee to be routed through the IP network~~address as a possible channel through which said call can be conducted.

63. (**Currently Amended**) The system of claim ~~62~~ **55** wherein said processor circuit is operably configured to ~~establish~~ enable communications between said caller and said callee to be established through ~~said~~ an IP network in response to a call received at said IP network address~~on said channel~~.

64. (**Currently Amended**) The system of claim **63** wherein said access code request message includes a caller identifier and wherein said processor circuit is operably configured to associate ~~store a~~ said caller identifier ~~associated~~ with the ~~mobile telephone in association with said~~ selected access code.

65. (**Cancelled**)

66. (**Currently Amended**) The system of claim ~~55~~ **64** wherein said processor circuit is operably configured to associate ~~store~~ said callee identifier included in said access code request message with ~~in association with said~~ the selected access code.

67. (**Currently Amended**) The system of claim **66** wherein said processor circuit is operably configured to associate said caller identifier and said callee identifier with the selected access code only when:

a) the access code is not already associated with a callee id; or

b) the access code is already associated with a callee id, and a timeout value associated with that callee id has expired.~~search said pool of access codes for an access code associated with said callee identifier to identify the channel usable by the mobile telephone to initiate a call to the callee.~~

68. (**Currently Amended**) The system of claim ~~54~~ **55** wherein said processor circuit is operably configured to associate a timestamp with said access code, for use in determining when the usability of said access code to initiate a call to the callee will expire, and to cause said timestamp to be included in said access code reply message transmitted to the mobile telephone~~store, in association with said access code, a timestamp for use in determining when the usability of said access code to initiate a call to the callee will expire~~.

69. (**Currently Amended**) The system of claim **68** wherein said processor circuit is operably configured to enable communications to be established between said caller and said callee when the mobile telephone seeks to establish a call to said callee using the access code

transmitted in the access code reply message when said timestamp associated with said access code indicates the usability of said access code has not expired and to prevent said communications from being established when said timestamp indicates the usability of said access code has expired~~establish communication only if the usability of said access code to initiate a call to the callee has not expired~~.

70. (**Original**) The system of claim **52** wherein said means for transmitting comprises a non-voice network interface for transmitting said access code reply message on a non-voice network.

71. (**Currently Amended**) A system for enabling ~~a~~ mobile telephone ~~to initiate a call to a callee through a channel~~roaming, the system comprising:

a processor circuit;

a network interface in communication with said processor circuit; and

a computer readable medium in communication with said processor circuit and encoded with codes for directing said processor circuit to:

receive from the mobile telephone an access code request message including a callee identifier associated with the callee and a location identifier identifying a location of the mobile telephone;

communicate with ~~said~~ a routing controller to obtain from said routing controller an access code identifying ~~the~~ a communication channel, said access code being determined from said location identifier and said access code being different from the callee identifier and useable by the mobile telephone to initiate a call to the callee using the channel; and

cause an access code reply message including said access code to be transmitted to the mobile telephone.

72. (**Original**) The system of claim **71** wherein said network interface comprises a non-voice network interface, and wherein said codes for directing said processor circuit to

receive include codes for directing said processor circuit to cause said access code request message to be received using said non-voice network interface on a non-voice network.

73. (**Currently Amended**) The system of claim **71** wherein said ~~computer-readable medium is further encoded with~~ codes for directing said processor circuit include codes for directing said processor circuit to cause a routing controller to produce said access code ~~to be produced~~.

74. (**Currently Amended**) The system of claim **73** wherein said codes for directing said processor circuit to cause said access code to be produced include codes that cause said processor circuit to ~~access code to be selected~~ select said access code from a pool of access codes, ~~where~~ wherein each access code in said pool of access codes identifies a respective telephone number or Internet Protocol (IP) network address.

75. (**Currently Amended**) The system of claim **74** wherein said codes for directing said processor circuit include ~~computer-readable medium is further encoded with~~ codes for directing said processor circuit to determine from said location identifier a local calling area associated with the mobile telephone and to select an access code associated with a calling area matching said local calling area associated with the mobile telephone.

~~cause to be determined a local calling area associated with the mobile telephone.~~

76. (**Currently Amended**) The system of claim **75** wherein said codes for directing said processor circuit include codes for directing said processor circuit to accessing a location field of a dialing profile associated with the caller when a local calling area cannot be determined from the contents of said location identifier and determining a local calling area associated with the mobile telephone from the contents of said location field and selecting an access code associated with a calling area matching the local calling area associated with the mobile telephone.

~~to cause to be determined cause a dialing profile associated with the caller to be accessed, said dialing profile including a location field having contents identifying at least a default location of the caller.~~

77. **(Currently Amended)** The system of claim **75** wherein said location identifier comprises ~~wherein said codes for directing said processor circuit to cause to be determined cause to be received~~ an IP address of the mobile telephone in a wireless IP network.

78. **(Currently Amended)** The system of claim **75** wherein said location identifier comprises ~~wherein said codes for directing said processor circuit to cause to be determined cause to be received~~ an identifier of a wireless voice signal station in wireless communication with the mobile telephone.

79. **(Currently Amended)** The system of claim **75** wherein said location identifier comprises ~~wherein said codes for directing said processor circuit to cause to be determined cause to be received~~ a user-configured identifier of a location associated with the mobile telephone.

80. **(Cancelled)**

81. **(Currently Amended)** The system of claim **74** wherein at least one of said access codes ~~each access code~~ in said pool of access codes ~~further~~ identifies ~~a respective channel operably configured to cooperate with~~ an IP network address as a possible channel through which said call can be conducted.~~to cause a call involving the mobile telephone and the callee to be routed through the IP network.~~

82. **(Currently Amended)** The system of claim **81** wherein said codes for directing said processor circuit include ~~computer readable medium is further encoded with~~ codes for directing said processor circuit to enable communications between said caller and said callee to be established through an IP network in response to a call received at said IP network address.

~~cause communication through said IP network to be established in response to a call received on said channel.~~

83. (**Currently Amended**) The system of claim **82** wherein said access code request message includes a caller identifier and wherein said codes for directing said processor circuit include codes for directing said processor circuit to ~~cause~~ associate said caller identifier included in said access code request message with the selected access code.

~~said access code to be produced cause a caller identifier associated with the mobile telephone to be stored in association with said access code.~~

84. (**Cancelled**)

85. (**Currently Amended**) The system of claim ~~74~~ **83** wherein said codes for directing said processor circuit include codes for directing said processor circuit to associate said callee identifier included in said access code request message with the selected access code.

~~to cause said access code to be produced cause said callee identifier to be stored in association with said access code.~~

86. (**Currently Amended**) The system of claim **85** wherein said codes for directing said processor circuit include codes for directing said processor circuit to associate said caller identifier and said callee identifier with the selected access code only when:

a) the access code is not already associated with a callee id; or

b) the access code is already associated with a callee id, and a timeout value associated with that callee id has expired.

~~to cause said access code to be produced cause said pool of access codes to be searched for an access code associated with said callee identifier to identify the channel usable by the mobile telephone to initiate a call to the callee.~~

87. (**Currently Amended**) The system of claim ~~73~~ **71** wherein said codes for directing said processor circuit include codes for directing said processor circuit to associate a

timestamp with said access code, for use in determining when the usability of said access code to initiate a call to the callee will expire, and to cause said timestamp to be included in ~~to cause said access code to be produced cause a timestamp for use in determining when the usability of said access code to initiate a call to the callee will expire, to be stored in association with~~ said access code reply message.

88. (**Currently Amended**) The system of claim **87** wherein said codes for directing said processor circuit include codes for directing said processor circuit to enable communications to be established between said caller and said callee when the mobile telephone seeks to establish a call to said callee using the access code transmitted in the access code reply message when said timestamp associated with said access code indicates the usability of said access code has not expired and to prevent said communications from being established when said timestamp indicates the usability of said access code has expired.
~~to cause communication to be established cause communication to be established only if the usability of said access code to initiate a call to the callee has not expired.~~

89. (**Original**) The system of claim **71** wherein said network interface comprises a non-voice network interface, and wherein codes for directing said processor circuit to transmit include codes for directing said processor circuit to cause said access code reply message to be transmitted using said non-voice network interface on a non-voice network.

90. (**Currently Amended**) A computer readable medium encoded with codes for directing a processor circuit to enable ~~a~~ mobile telephone ~~to initiate a call to a callee through a channel~~roaming, the codes being operable to direct the processor circuit to:

receive from the mobile telephone an access code request message including a callee identifier associated with the callee and a location identifier identifying a location of the mobile telephone;

communicate with ~~said~~ a routing controller to obtain from said routing controller an access code identifying ~~the~~ a communication channel, based on said location identifier,

said access code being different from the callee identifier and useable by the mobile telephone to initiate a call to the callee using the channel; and

cause an access code reply message including said access code to be transmitted to the mobile telephone.

REMARKS

Claim 3, 14, 24, 42, 46, 61, 65, 80 and 84 have been canceled. Claims 1, 4-6, 11, 12,15-17, 21, 22, 25-27, 31, 32, 33, 35-41, 43-45, 47-50, 52, 54-60, 62-64, 66-69, 71, 73-79, 81-83, 85-88 and 90 have been amended. Claims 2, 7-10, 13, 18-20, 23, 28-30, 34, 51, 53, 70, 72 and 89 are unchanged. The amendments are supported by the original claims, and at least in part by p. 3, ll. 24-25, p. 24, ll. 16-20, p. 25, ll. 24-29, p. 37, ll. 1-16, and p. 38, ll. 1-17 of PCT Publication WO 2010/012090. No new subject matter has been added. Applicant respectfully requests reconsideration of the rejections in light of the amendments and the following remarks.

Discussion of Claim Objections

Claims 52, 71 and 90 have been objected to because of informalities regarding the first occurrence of the phrase "said routing controller". Claim 52 has been amended to delete the phrase "said routing controller". Claims 71 and 92 have been amended to change the phrase "said routing controller" to be "a routing controller" as suggested by the Examiner.

Discussion of Claim Rejections Under 35 U.S.C. § 101

Claims 32 and 90 have been rejected under 35 U.S.C. § 101 for being directed to non-statutory subject matter. Claims 32 and 90 have been amended to refer to a non-transitory computer readable medium as suggested by the Examiner. Claims 22, 31 and 71 have been voluntarily amended to change the reference to computer readable medium to also recite a non-transitory computer readable medium.

Discussion of Claim Rejections Under 35 U.S.C. § 103(a)

The Examiner has rejected Claims 1-3, 5-7, 8-14, 16-24, 26-35, 52-54, 71-73 and 90 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Application Publication No. 2004/0022237 A1 (Elliott) and U.S. Application Publication No. 2008/0056235 A1 (Albina). Claims 4, 15, 25, 36-42, 43-48, 55-67, 74-80, 81-86 are rejected under 35 U.S.C. § 103(a) as unpatentable over Elliott in view of Albina and U.S. Patent No. 6,674,745 (Schuster). Claims 49-50, 68-69 and 87-88 are rejected under 35 U.S.C. § 103(a) as unpatentable over Elliott in

view of Albina and U.S. Application Publication No. 2002/012391 A1 (Shalit). Claims 51, 70 and 89 are rejected under 35 U.S.C. § 103(a) as unpatentable over Elliott in view of Albina and U.S. Patent No. 5,454,030 (de Oliveira). Applicant respectfully submits that all pending claims are patentable over the prior art of record as discussed below.

Standard of *Prima facie* Obviousness

The Patent and Trademark Office has the burden under section 103 to establish a *prima facie* case of obviousness. The rationale to support a conclusion that the claim would have been obvious is that **all the claimed elements** were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination yielded nothing more than predictable results to one of ordinary skill in the art. It can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does. If any of these findings cannot be made, then this rationale cannot be used to support a conclusion that the claim would have been obvious to one of ordinary skill in the art. M.P.E.P. § 2143.

Discussion of Patentability of Pending Claims

Rejection of Claims 1-3, 5-7, 8-14, 16-24, 26-35, 52-54, 71-73 and 90 over Elliott in view of Albina

All of the independent Claims 1, 12, 22, 32, 33, 52, 71 and 90 and certain ones of the dependent claims have been rejected over the combination of Elliott and Albina. Claims 3, 14, and 24 have been cancelled and therefore the rejection as it pertains to these claims is moot.

Independent Claims **1, 12, 22** and **32** all recite a common feature in various forms of language, this common feature being represented by the following language of amended Claim 1:

> *...transmitting an access code request message to an access server, said access code request message including said callee identifier and a location identifier identifying a location of the mobile telephone; and*
> *receiving an access code reply message from the access server in response to said access code request message, said access code reply message including an access code different from said callee identifier and associated with said location identifier;...*

Neither Elliott nor Albina disclose or suggest including a location identifier in an access code request message or an access code associated with a location identifier provided in an access code request message. Cancelled Claim 3 recited "transmitting a location identifier" with the access code request message but the Examiner regarded paragraph 105 of Albina as teaching a mobile station 1202 registers with registrar/location server 1210 to give the location of mobile station and referred to Figure 12. However, it appears that in the indicated paragraph and in Figure 12, the term "registrar/location server 1210" is merely a label. There is nothing in Albina to suggest any location information pertaining to the location of the mobile telephone should or could be used; or that if such location information were available it should or could be transmitted in an access code request message sent from a mobile telephone; or if it were transmitted in an access code request message that it should or could be associated with the access code provided back to the mobile telephone in an access code reply message.

Therefore, there is nothing to suggest the above indicated language that now appears in each of amended independent Claims 1, 12, 22 or 32 herewith is disclosed or suggested in Elliott, Albina or their combination. Therefore, the amended independent Claims 1, 12, 22 and 32 are not obvious in view of the cited references and the rejection of these independent claims under 35 USC 103 is overcome and these claims are allowable over Elliott and Albina.

In addition, the rejection of the claims that ultimately depend from independent Claims 1, 12, 22 or 32 is also overcome due to their ultimate dependence on one of these claims and due to the additional subject matter they add to these claims.

Regarding Claims **5, 16 and 26**, these claims have been amended to recite language to the effect that:

> *transmitting said location identifier comprises transmitting an identifier of a wireless voice signal station in wireless communication with the mobile telephone*

The Examiner has referred to Figure 3 and paragraph 33, lines 1-18 of Albina, which the Examiner has paraphrased as "mobile device 102 sends a data message (i.e. identifier) which is carried via mobile data network 106 which is deliver to application server 110."

In Applicant's system, the location identifier recited by Applicant is in a field of the access code request message which is sent to an access server. The Examiner has not referred to

any part of Elliott that is alleged to describe this and there is nothing to suggest the data message described by Albina should contain an identification of the wireless voice station in communication with the mobile telephone from which the access code request message is sent. In the very passages of Albina mentioned by the Examiner, Albina recites: "The data message from mobile communication device 102 comprises information associated with VoIP destination device 104. The data message may include a unique identifier or other information sufficient to identify VoIP destination device 104" (emphasis added). Albina appears to be focusing on information associated with VoIP destination device 104 and appears to have no regard to the identification of a wireless voice station in communication with the mobile telephone. There no disclosure or suggestion to provide in the access code request message an identification of the wireless voice station in communication with the mobile telephone from which the access code request message is sent. This is a further reason why Claims 5, 16 and 26 are not obvious in view of the cited references and overcome the rejection under 35 USC 103(a).

In addition, regarding Claims **6, 17** and **27**, these claims refer to a:

user configured identifier of a location associated with the mobile telephone.

The Examiner refers to lines 8-14 of paragraph 104 of Albina, and appears to equate the client application on the mobile phone of Albina with the term "user-configured identifier" used by Applicant in Claims 6, 17 and 27.

Applicant respectfully submits that the Examiner ignores the following underlined language of the term claimed by Applicant: user configured identifier of a location associated with the mobile telephone. Even if the client application referred to by Albina could be characterized as a user configured identifier, there is nothing to suggest that such application is a user configured identifier of a location associated with the mobile telephone. This is a further reason why Claims 6, 17 and 27 are not obvious in view of the cited references and overcome the rejection under 35 USC 103(a).

Claims **9, 19** and **29** have been amended to recite:

the access code comprises a telephone number or an IP network address useable by the mobile telephone to establish communications between the mobile telephone and the callee.

The Examiner refers to Elliott, Fig 1: Device 102 makes a call to callee 120 which is routing through IP data network 112. Albina refers to a temporary directory number (TDN) but not an IP network address being an access code and provides no disclosure to suggest that a temporary directory number could be a network address. This is a further reason why Claims 9, 19 and 29 are not obvious in view of the cited references and overcome the rejection under 35 USC 103(a).

Regarding independent Claims **33, 52, 71** and **90**, these claims all recite in various forms the following exemplary language of Claim 33:

> ...receiving from the mobile telephone an access code request message including a callee identifier associated with the callee and a location identifier identifying a location of the mobile telephone; and
>
> *producing an access code identifying the channel based on said location identifier, said access code being different from the callee identifier and useable by the mobile telephone to initiate a call to the callee using the channel...*

The Examiner cites paragraph 487 of Elliott which reads:

> [0487] In step 2226, soft switch sites 104, 106 instruct the gateway sites to make connections to set up the call. Soft switch sites 104, 106 can send messages through data network 112 (e.g. using IPDC protocol commands) to gateway sites 108, 110, to instruct the gateway sites to make the necessary connections for setting up the call origination from calling party 102, the call termination to called party 120, and the connection between origination and termination.

Applicant respectfully submits that the cited passage of Elliott refers to a soft switch instructing gateway sites by sending IPDC protocol commands to instruct the gateway sites to set up call origination, termination and connections. There is nothing that would be considered to be an access code reply message that is transmitted back to the mobile telephone wherein the access code reply message includes an access code that is useable by the mobile telephone to call the callee. Rather the soft switch receives an incoming signaling message at the onset of a call and then determines an appropriate route to route the call and then contacts a suitable gateway to configure it to be part of the route and then the soft switch routes the call through the gateway. The routing and configuration of the gateway is independent of the originating telephone (which is not a mobile telephone, as noted by the Examiner) and the soft switch receives nothing like the

claimed access code request message with a location identifier from the telephone. In addition, the soft switch makes no use of location information to produce an access code that can be subsequently used by the telephone to make a call and the soft switch does not send an access code reply message bearing such an access code back to the originating telephone. As a result there is nothing in Elliott to suggest *receiving from the mobile telephone an access code request message including a callee identifier associated with the callee and a location identifier identifying a location of the mobile telephone; and producing an access code identifying the channel based on said location identifier, said access code being different from the callee identifier and useable by the mobile telephone to initiate a call to the callee using the channel.*

Regarding Albina, as stated above, there is nothing in Albina to suggest any location information pertaining to the location of the mobile telephone should or could be used; or that if such location information were available it should or could be transmitted in an access code request message sent from a mobile telephone; or if it were transmitted in an access code request message that it should or could be associated with the access code provided back to the mobile telephone in an access code reply message. Albina merely provides a temporary directory number (TDN) without regard to any location information about the mobile telephone. Neither Elliott nor Albina discloses or suggests receiving location information from a mobile telephone or producing an access code based on said location information. Therefore, amended independent Claims 33, 52, 71 and 90 are not obvious in view of the cited references and the rejection under 35 USC 103 as it pertains to Claims 33, 52, 71 and 90 is overcome.

The claims that ultimately depend from amended independent Claims 33, 52, 71 and 90 are also not obvious and therefore the rejection of such claims is also overcome, due to their dependence on one of the indicated independent claims and due to the additional subject matter they add to one of the independent claims. Therefore, the rejection of Claims 1-3, 5-7, 8-14, 16-24, 26-35, 52-54, 71-73 and 90 under 35 USC 103 having regard to Elliott and Albina is overcome.

Rejection of Claims 4, 15, 25, 36-42, 43-48, 55-67, 74-80, 81-86 over Elliott in view of Albina and Schuster

Regarding Claims **4, 15** and **25**, these claims are dependent on amended Claims 1, 12 and 22 respectively, which have been shown above to distinguish over Elliott and Albina. Claims 4, 15 and 25 recite:

> *transmitting said location identifier comprises transmitting an IP address of the mobile telephone in a wireless IP network*

The Examiner has correctly noted that the combination of Elliott and Albina does not teach transmitting an IP address of the mobile telephone in a wireless IP network. The Examiner has referred to col. 6, lines 58-62 of Schuster which state:

> Therefore, to properly set up an internet telephony call, the originating gateway needs some mechanism to determine the IP address of the appropriate terminating gateway 20 based on the telephone number supplied by the calling party.

Applicant respectfully submits that the indicated portion of Shuster refers to an IP address of a terminating gateway, not an IP address of a telephone. Furthermore, the context in which the IP address is recited in Applicant's Claims 4, 15 and 25 is one in which the IP address is part of a location identifier, the existence or use of which is not disclosed in Elliott, Albina or Schuster. There is no suggestion in Elliott, Albina or Schuster that would lead one skilled in the art to modify the use of the IP address of a terminating gateway to cause such an IP address to act as a location identifier of a access request message sent from a mobile telephone and to cause an access code reply message containing an access code associated with the location identifier to be sent back to the mobile telephone for use by the mobile telephone to initiate a call using a channel identified by the access code. Therefore Claims 4, 15 and 25 are not obvious in view of the cited references and the rejection of Claims 4, 15 and 25 under 35 USC 103(a) is overcome by the amendment to the independent claims from which they depend.

Regarding Claims **36, 55** and **74**, these claims have been amended to generally recite:

> *...producing said access code comprises selecting said access code from a pool of access codes, wherein each access code in said pool of access codes identifies a respective telephone number or IP network address.*

The Examiner has referred to col. 11, lines 1-5 of Schuster which recite:

> For instance, if the SRITG serves wireless (e.g., cellular, PCS, etc.) customers, then the AMS may refer to an appropriate reference database to associate the IP address of the SRITG with the wireless phone numbers that the SRITG serves....

Applicant respectfully submits that Schuster describes relating wireless phone numbers to IP addresses (see the title of Schuster). The database referred to by Schuster relates only IP addresses to wireless phone numbers. The pool claimed by Applicant relates location information to telephone numbers or IP addresses. There is nothing in Schuster to suggest that the database should be used as a pool that relates location information and telephone numbers or IP addresses, in the context of selecting an access code based on a location identifier received from the mobile telephone. Therefore Claims 36, 55 and 74 are not obvious in view of the cited references and the rejection under 35 USC 103(a) is overcome.

Regarding Claims **37, 56** and **75**, these claims have generally been amended to recite:

determining from said location identifier a local calling area associated with the mobile telephone and selecting an access code associated with a calling area matching said local calling area associated with the mobile telephone.

The Examiner has referred to Albina, paragraph 53, which recites:

> [0053] A media gateway receives the call and routes the SIP signaling associated with the destination phone number (the assigned local temporary number) to the SIP application server.

Applicant respectfully submits that the indicated passage and the context provided by Albina provide no disclosure or suggestion to "determine from said location identifier a local calling area associated with the mobile telephone and selecting an access code associated with a calling area matching said local calling area associated with the mobile telephone," as recited in

amended Claims 37, 57 and 75. Therefore, these claims are not obvious in view of the cited references and the rejection of Claims 37, 56 and 75 under 35 USC 103(a) is overcome.

Regarding Claims **38, 57** and **76** these claims have been amended to recite:

> *accessing a location field of a dialing profile associated with the caller when a local calling area cannot be determined from the contents of said location identifier and determining a local calling area associated with the mobile telephone from the contents of said location field and selecting an access code associated with a calling area matching the local calling area associated with the mobile telephone.*

The Examiner refers to Albina, paragraph 105, which recites:

> [0105] A. Mobile station 1202 registers with registrar/location server 1210 through PDSN/SGSN (e.g., PDSN 1204). This occurs on application start and reoccurs every "Expires" (see c. below) seconds.

The Examiner also referred to Figure 12. Applicant respectfully submits that as stated above, it appears that in the indicated paragraph and in Figure 12, the term "registrar/location server 1210" is merely a label. There is nothing in Albina to suggest any location information pertaining to the location of the mobile telephone should or could be used to determine an access code, or more particularly that a local calling area should be determined from a location field of a dialing profile associated with the caller or that the access code should be selected by matching a local calling area associated therewith to a local calling area indicated in the location field of a dialing profile associated with the caller. Therefore amended Claims 38, 57, and 76 are not obvious in view of the cited references and the rejection under 35 USC 103(a) is overcome.

Regarding Claims **39, 58** and **77**, these claims have been amended to recite:

> *said location identifier comprises an IP address of the mobile telephone in a wireless IP network.*

The Examiner refers to Schuster, col. 6, lines 58-62 which recite:

> Therefore, to properly set up an internet telephony call, the originating gateway needs some mechanism to determine the IP address of the appropriate terminating gateway 20 based on the telephone number supplied by the calling party.

Applicant respectfully submits that this portion of Schuster refer to determining an IP address of a terminating gateway based on a (callee) telephone number supplied by the calling party (by caller). Applicant's Claims 39, 58 and 77 refer to a location identifier identifying a location of the mobile telephone in an access code request message from the mobile telephone. The cited portion of Schuster provide no suggestion to provide an access code request message having a location identifier comprising an IP address of the mobile telephone in a wireless IP network. Therefore amended Claims 39, 58 and 77 are not obvious in view of the cited references and the rejection under 35 USC 103(a) is overcome.

Regarding Claims **40, 59** and **78**, these claims recite:

said location identifier comprises an identifier of a wireless voice signal station in wireless communication with the mobile telephone.

The Examiner refers to Albina, Figure 2, and paragraph 33 which recite:

> [0033] Having generally described the supporting infrastructure of communication system 100, the operation of various embodiments of the cellular-to-VoIP call establishment process will be described. In the embodiment illustrated in FIG. 2, the cellular-to-VoIP call establishment process begins, at reference A, with mobile communication device 102 providing a data message to mobile data network 106, which is delivered to application server 110. While the data message is initially carried via mobile data network 106, it should be appreciated that the data message may be routed to other communication networks (wireless or wired) before arriving at application server 110.

Applicant respectfully submits that in Applicant's system, the location identifier recited by Applicant is in a field of the access code request message which is sent to an access server. There is nothing to suggest the data message described by Albina should contain an identification of the wireless voice station in communication with the mobile telephone from which the access code request message is sent. In the very passages of Albina mentioned by the Examiner, Albina recites that "The data message from mobile communication device 102 comprises information associated with VoIP destination device 104. The data message may include a unique identifier or other information sufficient to identify VoIP destination device 104." There no disclosure or suggestion to provide in the access code request message an identification of the wireless voice

station in communication with the mobile telephone from which the access code request message is sent. Therefore Claims 40, 59, and 78 are not obvious in view of the cited references and the rejection under 35 USC 103(a) is overcome.

Regarding Claims **41, 60** and **79**, these claims recite:

said location identifier comprises a user-configured identifier of a location associated with the mobile telephone.

The Examiner cites Albina, Figure 12, as indicating the mobile station 1202 registers with register/location server 1210 and refers to paragraph 104, lines 8-12 which recite:

> [0104] FIG. 12 illustrates yet another embodiment of a cellular-to-VoIP call establishment process, which occurs across the following system components: a mobile station 1202, PDSN 1204, a mobile switching center 1206, an internetworking function 1208, a registrar/location server 1210, an SIP proxy 1212, an IP service provider proxy server 1214, a PSTN gateway 1216, and a VoIP SIP proxy. In this example, it assumed that a client application resides on mobile station 1202 for enabling the user to select a party to call by name (e.g., voip@prov.com). The application is configured such that requests arrive at the IP address of internetworking function (IWF) 1208.

Applicant respectfully submits that Applicant's claims refer to a user configured identifier of a location associated with the mobile telephone. The Examiner appears to equate the client application on the mobile phone of Albina with the term "user-configured identifier" used by Applicant in Claims 41, 60 and 79, but this ignores the following underlined language of the term used by Applicant: user configured identifier <u>of a location associated with the mobile telephone.</u> In the context of Applicant's claim, of course the user is the user of the mobile telephone. Even if the client application referred to by Albina could be characterized as a user configured identifier, there is nothing to suggest that such application is a user configured identifier <u>of a location associated with the mobile telephone</u>. Therefore Claims 41, 60 and 79 are not obvious in view of the cited references and the rejection under 35 USC 103(a) is overcome.

Regarding Claims **42, 61** and **80**, these claims have been cancelled and therefore the rejection of these claims is moot.

Regarding Claims **43, 62** and **81**, these claims have been amended to recite:

at least one of said access codes in said pool of access codes identifies an IP network address as a possible channel through which said call can be conducted.

The Examiner refers to Schuster, Abstract and Figure 1 and indicates that ITG routes the call with an IP network.

Applicant respectively submits that of course, Schuster describes a method and system for mapping phone numbers to IP addresses and thus refers to IP addresses, but they are not referred to in the context of a system in which an access code is selected from a pool of access codes.

Schuster describes relating wireless phone numbers to IP addresses (see the title of Schuster). The database referred to by Schuster relates only IP addresses to wireless phone numbers. The pool claimed by the present application relates location information to telephone numbers or IP addresses. There is nothing in Schuster to suggest that the database should be used as a pool that relates location information and telephone numbers or IP addresses, in the context of selecting an access code based on a location identifier received from the mobile telephone. Therefore, Schuster fails to describe or suggest *at least one of said access codes in said pool of access codes identifies an IP network address as a possible channel through which said call can be conducted,* as recited in Applicant's Claims 43, 62 and 81. Therefore, Claims 43, 62, 81 are not obvious in view of the cited references and the rejection under 35 USC 103(a) is overcome.

Claims **46, 65** and **84** have been cancelled and therefore the rejection of these claims is moot.

Claims **47, 66** and **85** recite:

associating said callee identifier included in said access code request message with the selected access code.

The Examiner indicates Elliott describes at paragraph 738 the callee identifier (i.e., dialed number) is stored in table entry, table 14.

Applicant respectfully submits that table 14 has four columns identified as Number, Terminating Circuit Group, Priority and Load. The table thus associates these entities with each other. While the "Number" column appears to hold a dialed number, none of the other columns appears to relate to a selected access code, and therefore, there is nothing that discloses or suggests the dialed number acting as a callee identifier should be associated with a selected

access code, especially since none of the columns in the table holds an access code of the type claimed by Applicant. Therefore Claims 47, 66 and 85 are not obvious in view of the cited references and the rejection under 35 USC 103(a) is overcome.

Claims **48, 67** and **86** have been amended to recite:

associating said caller identifier and said callee identifier with the selected access code occurs only when:
a) the access code is not already associated with a callee id; or
b) the access code is already associated with a callee id, and a timeout value associated with that callee id has expired.

The Examiner refers to Elliott table 14: circuit group contains channels for identifying callee.

Applicant respectfully submits that as stated above, none of the columns of table 14 appears to relate to a selected access code and therefore there is nothing that discloses or suggests the dialed number acting as a callee identifier should be associated with a selected access code. Furthermore, none of the columns appear to hold a timeout value and therefore there is nothing to suggest that a timeout value is associated with a callee id. Therefore Claims 48, 67 and 86 are not obvious in view of the cited references and the rejection under 35 USC 103(a) is overcome.

Rejection of Claims 49-50, 68-69 and 87-88 over Elliott in view of Albina and Shalit

Claims 49, 68 and 87 are similar, and Claims 50, 69 and 88 are similar.

Claims **49, 68** and **87** have been amended to recite:

associating a timestamp with said access code, for use in determining when the usability of said access code to initiate a call to the callee will expire, and causing said timestamp to be included in said access code reply message transmitted to the mobile telephone.

The Examiner states Shalit at paragraph 44 recites:

> Resource manager 15 also deallocates the session access code after the session has expired due to time constraints (i.e., the host will only pay for a 30 minute chat) or physical call breaks (i.e., hang-ups).

Applicant respectfully submits that the access code referred to by Shalit is an audio conferencing access code that is manually entered into a telephone by a participant in an audio conference. This is quite different from the claimed access code that is produced based on a location identifier received from a mobile telephone, identifying the location of the mobile telephone. None of the cited references provides anything to suggest that a timestamp could or should be included in a reply message transmitted to the mobile telephone in response to a request by the mobile telephone for such a message. Shalit provides no mention of the use of a message of this type. Therefore Claims 49, 68 and 87 are not obvious in view of the cited references and the rejection under 35 USC 103(a) is overcome.

Regarding Claims **50, 69** and **88**, these claims have been amended to recite:

> *enabling communications to be established between said caller and said callee when the mobile telephone seeks to establish a call to said callee using the access code transmitted in the access code reply message when said timestamp associated with said access code indicates the usability of said access code has not expired and not enabling said communications to be established when said timestamp indicates the usability of said access code has expired.*

Applicant respectfully submits that the Examiner has repeated the same comments made with respect to Claims 49, 68 and 87. Therefore, Applicant reiterates the comments above with regard to these claims and further submits that Shalit does not describe a timestamp and the access code of Shalit is not comparable to the access code recited in Applicant's claims for the reasons given above. Therefore Claims 50, 69 and 88 are not obvious in view of the cited references and the rejection under 35 USC 103(a) is overcome.

Rejection of Claims 51, 70 and 89 over Elliott in view of Albina and de Oliveira

Claims **51, 70** and **89** recite:

transmitting comprises transmitting said access code reply message on a non-voice network.

The Examiner refers to de Oliveira, col. 8, lines 42-48 (i.e., Claim 6) which recite:

transmitting a reply message from the further system (VMS2) via the network interface (FDDI) and the message path (NW) to said one system (VMS1) having transmitted the broadcast message, said reply message containing all control data identifying the home mailbox, including an associated personal access code and a directory;

Applicant respectfully submits that de Oliveira describes the use of a network interface (FDDI) that appears to be used for all communications, including voice and non-voice communications. Applicant's claims recite transmitting an access code reply message on a non-voice network. In the context of Applicant's system, the non-voice network is different from the conventional PSTN network and different from a conventional cellular network, where voice is carried. See Figure 1 item 16 of Applicant's application, for example. The non-voice network may be a WiFi, GPRS, WiMAX or other similar type of network, for example. The use of this type of network results in less cost compared to using a conventional cellular network for receiving the access code reply message.

Because de Oliveira appears to suggest the use of the same network for all communications, it appears de Oliveira has failed to recognize the benefits that can be achieved by using a separate network for communications involving receiving an access code request message and transmitting an access code reply message of the type claimed by Applicant. It appears de Oliveira fails to disclose or suggest the use of a separate non-voice network for communications involving the access code request message and the access code reply message. Therefore it is respectfully submitted that Claims 51, 70 and 89 are not obvious in view of the cited references and the rejection under 35 USC 103(a) is overcome.

Final Comments

Applicant wishes to refer the Examiner to page 24, lines 16-20 of Applicant's specification (PCT Publication WO 2010/012090) which recites:

> *It will be appreciated that use of the access code facilitates avoidance of long distance or roaming charges that a mobile telephone service provider would charge for a call placed directly using the callee identifier using conventional calling processes, for example.*

In essence, the user of a mobile telephone can initiate a telephone call by operating his or her phone in the usual manner, e.g., selecting a contact to call. Using the process claimed in Claims 1-32, for example, the mobile telephone can automatically send an access code request message, including the location identifier identifying the location of the mobile telephone, to an access server. The access server uses the location identifier to find a suitable access code identifying a suitable channel, on the basis of the location identifier, and sends that access code back to the mobile telephone. The access code may be a telephone number or an IP address. Assuming the access code is a telephone number, the mobile phone automatically dials the access code, which connects the telephone to a communications channel which could be a telephone line associated with a geographical location near the mobile telephone. All this occurs transparently to the user and the user may have no idea the mobile telephone is actually calling a different number than the one associated with the contact in the contact list. The system thus provides for efficiency in that long distance routing is generally avoided and a geographically nearest telephone line can be used to conduct the call. This avoids excessive long distance charges and can result in a better quality telephone line being used to conduct the call. Furthermore, the methods and systems claimed easily facilitate "roaming" of the mobile telephone in a manner that is transparent to the user of the mobile telephone. If the service provider to which the mobile telephone user normally subscribes operates or is associated with the access server that provides access codes based on location as recited in Claims 33-90, subscribers are bound to the same service provider, which avoids engaging other mobile telephone service providers directly with the subscriber as in conventional roaming and avoids the associated loss of revenue by the home service provider. In effect to the subscriber, the

service appears to be continuous and local at all times and is under closer control of the home service provider.

Discussion of Dependent Claims

Although Applicant has not addressed all the issues of the dependent claims, Applicant respectfully submits that Applicant does not necessarily agree with the characterization and assessments of the dependent claims made by the Examiner, and Applicant believes that each claim is patentable on its own merits. The dependent claims are dependent either directly or indirectly on the above-discussed independent claims. Applicant respectfully submits that pursuant to 35 U.S.C. § 112, ¶ 4, the dependent claims incorporate by reference all the features of the claim to which they refer and include their own patentable features, and are therefore in condition for allowance. Therefore, Applicant respectfully requests the withdrawal of all claim rejections and prompt allowance of the claims.

No Disclaimers or Disavowals

Although the present communication may include alterations to the application or claims, or characterizations of claim scope or referenced art, Applicant is not conceding in this application that previously pending claims are not patentable over the cited references. Rather, any alterations or characterizations are being made to facilitate expeditious prosecution of this application. Applicant reserves the right to pursue at a later date any previously pending or other broader or narrower claims that capture any subject matter supported by the present disclosure, including subject matter found to be specifically disclaimed herein or by any prior prosecution. Accordingly, reviewers of this or any parent, child or related prosecution history shall not reasonably infer that Applicant has made any disclaimers or disavowals of any subject matter supported by the present application.

Co-Pending Applications of Assignee

Applicant wishes to draw the Examiner's attention to the following co-pending applications of the present application's assignee.

Docket No.	Serial No.	Title	Filed
SMARB19.001APC	12/513147	Producing Routing Messages for Voice Over IP Communications	03/01/10
SMARB19.002C1	13/863306	Intercepting Voice Over IP Communications and Other Data Communications	04/15/13
SMARB19.003APC	12/532989	Emergency Assistance Calling for Voice Over IP Communications Systems	03/05/10
SMARB19.005APC	13/496864	Uninterrupted Transmission of Internet Protocol Transmissions During Endpoint Changes	03/16/12

Conclusion

Applicant has endeavored to address all of the Examiner's concerns as expressed in the outstanding Office Action. In light of the above remarks, reconsideration and withdrawal of the outstanding rejections is respectfully requested. If the Examiner has any questions which may be answered by telephone, the Examiner is invited to call the undersigned directly.

Any remarks in support of patentability of one claim should not be imputed to any other claim in this or a related application, even if similar terminology is used. Any remarks referring to only a portion of a claim should not be understood to base patentability on solely that portion; rather, patentability must rest on each claim taken as a whole.

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 5/24/13

By: _____

John M. Carson
Registration No. 34,303
Attorney of Record
Customer No. 20995
(858) 707-4000

15435052
051713

Electronic Acknowledgement Receipt

EFS ID:	15870956
Application Number:	13056277
International Application Number:	
Confirmation Number:	2403
Title of Invention:	MOBILE GATEWAY
First Named Inventor/Applicant Name:	Johan Emil Viktor Bjorsell
Customer Number:	20995
Filer:	John M Carson/Daniela Lopez
Filer Authorized By:	John M Carson
Attorney Docket Number:	SMARB19.004APC
Receipt Date:	24-MAY-2013
Filing Date:	27-JAN-2011
Time Stamp:	19:13:49
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		SMARB19-004APC.pdf	2149648 73459e9dae45af84baa9d5fa57a922b2faf9bc1e	yes	39

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	20
	Applicant Arguments/Remarks Made in an Amendment	21	39
Warnings:			
Information:			
	Total Files Size (in bytes):	2149648	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/056,277	Filing Date 01/27/2011	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **05/24/2013**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 81	Minus	** 90	= 0	X $40 =	0
Independent (37 CFR 1.16(h))	* 8	Minus	***8	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/JACQUELINE COUPLIN/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/056,277
	Filing Date	January 27, 2011
	First Named Inventor	Björsell, Johan Emil Viktor
	Art Unit	2413
(Multiple sheets used when necessary)	Examiner	Rahman, Mostazir M.
SHEET 1 OF 1	Attorney Docket No.	SMARB19.004APC

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	1	6,798,767	9/29/2004	Alexander et al.	
	2	7,950,046	5/24/2011	Kropivny, Alexander	
	3	2006/0264200 A1	11/23/2006	Laiho et al.	
	4	2008/0056235 A1	3/6/2008	Albina et al.	
	5	2009/0292539 A1	11/26/2009	Jaroker, Jon	
	6	2009/0325558 A1	12/31/2009	Pridmore et al.	
	7	2010/0086119 A1	4/8/2010	De Luca et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name of Patentee or Applicant	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T^1

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T^1

15491498
052913

Examiner Signature	Date Considered
***Examiner**: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

T^1 - Place a check mark in this area when an English language Translation is attached.

Electronic Patent Application Fee Transmittal	
Application Number:	13056277
Filing Date:	27-Jan-2011
Title of Invention:	MOBILE GATEWAY
First Named Inventor/Applicant Name:	Johan Emil Viktor Bjorsell
Filer:	John M Carson/Norman Green
Attorney Docket Number:	SMARB19.004APC
Filed as Small Entity	

U.S. National Stage under 35 USC 371 Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt	
EFS ID:	15924792
Application Number:	13056277
International Application Number:	
Confirmation Number:	2403
Title of Invention:	MOBILE GATEWAY
First Named Inventor/Applicant Name:	Johan Emil Viktor Bjorsell
Customer Number:	20995
Filer:	John M Carson/Norman Green
Filer Authorized By:	John M Carson
Attorney Docket Number:	SMARB19.004APC
Receipt Date:	31-MAY-2013
Filing Date:	27-JAN-2011
Time Stamp:	20:14:36
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$90
RAM confirmation Number	7273
Deposit Account	111410
Authorized User	KNOBBE MARTENS OLSON AND BEAR
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		IDS_SMARB19_004APC_05_31_2013.pdf	82652 29f34a64fa7e7a4a710890c51bb55a184ba6edc3	yes	2

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	1
	Information Disclosure Statement (IDS) Form (SB08)	2	2

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	30604 a1a1f6a42b709351625019ebae350930607df278	no	2

Warnings:

Information:

Total Files Size (in bytes):	113256

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

INFORMATION DISCLOSURE STATEMENT

Inventor	:	Björsell, et al.
App. No.	:	13/056,277
Filed	:	January 27, 2011
For	:	MOBILE GATEWAY
Examiner	:	Rahman, Mostazir M.
Art Unit	:	2413
Conf. No.	:	2403

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

References and Listing

Submitted herewith in the above-identified application is an Information Disclosure Statement listing references for consideration. Copies of any listed foreign and non-patent literature references are being submitted.

Timing of Disclosure

This Information Disclosure Statement is being filed after receipt of a First Office Action, but before the mailing date of a Final Action and before the mailing date of a Notice of Allowance. This Statement is accompanied by the fees set forth in 37 C.F.R. § 1.17(p). The Commissioner is hereby authorized to charge any additional fees which may be required or to credit any overpayment to Account No. 11-1410.

Respectfully submitted,
KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 5/31/13

By: _____
John M. Carson
Registration No. 34,303
Attorney of Record
Customer No. 20995
(858) 707-4000

IDS
15491763
052913

Please Direct All Correspondence to Customer Number 20995

REQUEST TO CORRECT INVENTORSHIP

Inventor	:	Johan Emil Viktor Bjorsell, et al.
App. No	:	13/056277
Filed	:	January 27, 2011
For	:	MOBILE GATEWAY
Examiner	:	Rahman, Mostazir M.
Conf. No.	:	2403

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Pursuant to 37 CFR 1.48(c), this Request is being made to have Emil Malak added as an inventor to the present application. Applicant submits that the omission of the inventor Emil Malak was an error that occurred without deceptive intent.

The inventors of U.S. Patent Application No. 13/056,277 should be listed as follows:

Johan Emil Viktor Bjorsell

Maksym Sobolyev

Pentti Kalevi Huttunen

Emil Malak

This Request is accompanied by:

1. A statement by Emil Malak indicating that the error in inventorship in the above-referenced application occurred without deceptive intent, and was necessitated by amendment of the claims pursuant to 37 C.F.R. § 1.48(c)(2
2. An oath or declaration by the actual inventors as required by 37 C.F.R. §1.63;
3. Written Consent of the Assignee, Digifonica (International) Limited; and

Please Direct All Correspondence to Customer Number **20995**

4. The fee set forth in §1.17(i).

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE MARTENS OLSON & BEAR LLP

Dated: 8/5/13

By: _____

John M. Carson
Registration No. 34,303
Attorney of Record
Customer No. 20995
(858) 707-4000

15836629

Please Direct All Correspondence to Customer Number 20995

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	:	Johan Emil Viktor Bjorsell, et al.
App. No	:	13/056277
Filed	:	January 27, 2013
For	:	MOBILE GATEWAY
Examiner	:	Rahman, Mostazir M.
Art Unit	:	2403

WRITTEN CONSENT OF ASSIGNEE TO CORRECTION OF INVENTORSHIP UNDER 37 C.F.R. § 1.48(c)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The undersigned is an empowered representative of the Assignee. On behalf of the Assignee, Digifonica (International) Limited, and in accordance with 37 C.F.R. § 1.48(c)(5), the undersigned hereby consents to the addition of the following inventor:

Emil Malak
1005-1288 Alberni Street
Vancouver B.C. V6E 4N5

Date: August 2nd 2013 Signature: E Malak

Name: EMIL MALAK

Title: Director

Digifonica (International) Limited

Please Direct All Correspondence to Customer Number 20995

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	:	Johan Emil Viktor Bjorsell, et al.
App. No	:	13/056277
Filed	:	January 27, 2013
For	:	MOBILE GATEWAY
Examiner	:	Rahman, Mostazir M.
Art Unit	:	2403

STATEMENT UNDER 37 C.F.R. § 1.48(c)

Commissioner for Patents – Mail Stop PCT
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

I, Emil Malak, declare as follows:

1. I should be listed as an inventor of the above-referenced application.

2. My listing as an inventor was necessitated by amendment of the claims and the inventorship error occurred without deceptive intention on my part.

3. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful, false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States codes and that such willful, false statements may jeopardize the validity of the application or patent issuing therefrom.

Dated: 2nd August 2013 By: _____
Emil Malak

ASSIGNMENT

WHEREAS, Emil Malak, a CA citizen, residing at Canada (hereinafter referred to as "ASSIGNOR") invented certain new and useful improvements, technology, inventions, developments, ideas or discoveries related to MOBILE GATEWAY (collectively hereinafter referred to as the "Work") for which an application for Letters Patent in the United States has been filed with the United States Patent and Trademark Office and designated U.S. Patent App. No. 13/056277 (hereinafter the "Application");

AND WHEREAS, DIGIFONICA (INTERNATIONAL) LIMITED, an entity organized under the Companies Act of Gibraltar and having a Canadian Address of 773 Hornby Street Vancouver British Columbia, V6Z 1S4 Canada, (formerly 1401, 4710 Kingsway, Burnaby, British Columbia, V5H 4M2 Canada (hereinafter the "ASSIGNEE"), desires to acquire the entire right, title, and interest in and to the Application and the Work:

NOW, THEREFORE, for good and valuable consideration, the receipt of which is hereby acknowledged, ASSIGNOR hereby acknowledges that ASSIGNOR has sold, assigned, transferred and set over, and by these presents does hereby sell, assign, transfer and set over, unto said ASSIGNEE, its successors, legal representatives and assigns, the entire right, title, and interest throughout the world in the Application and the Work, including all provisional applications relating thereto (including but not limited to U.S. Provisional Application No. 61/129,898, filed July 28, 2008), and all nonprovisional applications claiming priority thereto, including, all divisions, continuations, continuations-in-part, reissues, and reexaminations thereof, and all Letters Patent of the United States which may be granted thereon and all reissues and extensions thereof, and all rights of priority under International Conventions and any related Letters Patent which may hereafter be granted or filed in any country or countries foreign to the United States, all extensions, renewals and reissues thereof; and ASSIGNOR hereby authorizes and requests the Commissioner of Patents of the United States, and any Official of any country or countries foreign to the United States, whose duty it is to issue patents on applications as aforesaid, to issue all related Letters Patent to the ASSIGNEE, its successors, legal representatives and assigns, in accordance with the terms of this instrument.

AND ASSIGNOR DOES HEREBY sell, assign, transfer, and convey to ASSIGNEE, its successors, legal representatives, and assigns all claims for damages and all remedies arising out of any violation of the rights assigned hereby that may have accrued prior to the date of assignment to ASSIGNEE, or may accrue hereafter, including, but not limited to, the right to sue for, collect, and retain damages for past infringements of said Letters Patent before or after issuance.

AND ASSIGNOR DOES HEREBY covenant and agree that ASSIGNOR will communicate to said ASSIGNEE, its successors, legal representatives and assigns, any facts known to ASSIGNOR respecting the Work, and testify in any legal proceeding, assist in the preparation of any other provisional or non-provisional applications relating to the Application and the Work or any improvements made thereto, sign all lawful papers, execute and make all rightful oaths and/or declarations in connection with the Application and the Work including any improvements made thereto, any patent applications filed therefrom, and any continuing application filed from any of the aforementioned applications, and generally do everything possible to aid the ASSIGNEE, its successors, legal representatives and assigns, to obtain and enforce proper patent protection for the Work in all countries.

This 2nd day of August, 2013.

Emil Malak

Witnessed by:

Printed Name: Erica Nath

DECLARATION FOR UTILITY OR DESIGN APPLICATION UNDER 37 CFR 1.63

Docket No.: SMARB19.004APC

Title: MOBILE GATEWAY

Inventors: Johan Emil Viktor Bjorsell, Maksym Sobolyev, Pentti Kalevi Huttunen, Emil Malak

Please Direct All Correspondence to Customer Number 20995

This Declaration is directed to the invention described and claimed the application that was filed on July 28, 2009, was assigned International App. No. PCT/CA2009/001062, entered the national phase on January 27, 2011, and was further assigned U.S. Patent App. No. 13/056277.

As a below named inventor:

I believe the inventors named below to be the original and first inventors of the subject matter which is described and claimed and for which a patent is sought;

I have reviewed and understand the contents of the above-identified application, including the claims; and

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

The application was originally filed with an Application Data Sheet (ADS). The ADS sets forth any applicable Foreign Priority Claims under 35 USC § 119, and sets forth the full mailing address and residence of each inventor whose signature appears below as allowed under 37 CFR 1.63(c). The ADS also sets forth any Domestic Priority Claims under 35 USC §§ 119(e), 120, 121, and 365.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful, false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first inventor: Johan Emil Viktor Bjorsell

Signature: _____ Date: August 2nd 2013

Citizenship: ~~SIS~~ CA EB

DECLARATION FOR UTILITY OR DESIGN APPLICATION UNDER 37 CFR 1.63

Title: MOBILE GATEWAY

Inventors: Johan Emil Viktor Bjorsell, Maksym Sobolyev, Pentti Kalevi Huttunen, Emil Malak

Please Direct All Correspondence to Customer Number 20995

Full name of **second** inventor: Maksym Sobolyev

Signature: _____ Date: August 2nd, 2013

Citizenship: ~~UA~~ CA

Full name of **third** inventor: Pentti Kalevi Huttunen

Signature: _____ Date: _____

Citizenship: CA

Full name of **fourth** inventor: Emil Malak

Signature: _____ Date: _____

Citizenship: CA

Send Correspondence To:
KNOBBE, MARTENS, OLSON & BEAR, LLP
Customer No. 20995

15836998
071913

DECLARATION FOR UTILITY OR DESIGN APPLICATION UNDER 37 CFR 1.63

Docket No.: SMARB19.004APC

Title: MOBILE GATEWAY

Inventors: Johan Emil Viktor Bjorsell, Maksym Sobolyev, Pentti Kalevi Huttunen, Emil Malak

Please Direct All Correspondence to Customer Number 20995

This Declaration is directed to the invention described and claimed the application that was filed on July 28, 2009, was assigned International App. No. PCT/CA2009/001062, entered the national phase on January 27, 2011, and was further assigned U.S. Patent App. No. 13/056277.

As a below named inventor:

I believe the inventors named below to be the original and first inventors of the subject matter which is described and claimed and for which a patent is sought;

I have reviewed and understand the contents of the above-identified application, including the claims; and

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

The application was originally filed with an Application Data Sheet (ADS). The ADS sets forth any applicable Foreign Priority Claims under 35 USC § 119, and sets forth the full mailing address and residence of each inventor whose signature appears below as allowed under 37 CFR 1.63(c). The ADS also sets forth any Domestic Priority Claims under 35 USC §§ 119(e), 120, 121, and 365.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful, false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first inventor: Johan Emil Viktor Bjorsell

Signature: _____ Date: August 2nd 2013

Citizenship: ~~SIS~~ CA EB

DECLARATION FOR UTILITY OR DESIGN APPLICATION UNDER 37 CFR 1.63

Docket No.: SMARB19.004APC Page 2 of 2

Title: MOBILE GATEWAY

Inventors: Johan Emil Viktor Bjorsell, Maksym Sobolyev, Pentti Kalevi Huttunen, Emil Malak

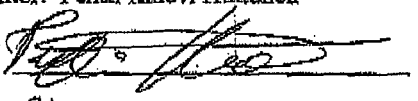
Please Direct All Correspondence to Customer Number 20995

Full name of **second** inventor: Maksym Sobolyev

Signature: _____ Date: _____

Citizenship: UA

Full name of **third** inventor: Pentti Kalevi Huttunen

Signature:  Date: Aug 02, 2013.

Citizenship: CA

Full name of **fourth** inventor: Emil Malak

Signature: _____ Date: _____

Citizenship: CA

Send Correspondence To:
KNOBBE, MARTENS, OLSON & BEAR, LLP
Customer No. 20995

15836998
071913

DECLARATION FOR UTILITY OR DESIGN APPLICATION UNDER 37 CFR 1.63

Docket No.: SMARB19.004APC

Title: MOBILE GATEWAY

Inventors: Johan Emil Viktor Bjorsell, Maksym Sobolyev, Pentti Kalevi Huttunen, Emil Malak

Please Direct All Correspondence to Customer Number 20995

This Declaration is directed to the invention described and claimed the application that was filed on July 28, 2009, was assigned International App. No. PCT/CA2009/001062, entered the national phase on January 27, 2011, and was further assigned U.S. Patent App. No. 13/056277.

As a below named inventor:

I believe the inventors named below to be the original and first inventors of the subject matter which is described and claimed and for which a patent is sought;

I have reviewed and understand the contents of the above-identified application, including the claims; and

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

The application was originally filed with an Application Data Sheet (ADS). The ADS sets forth any applicable Foreign Priority Claims under 35 USC § 119, and sets forth the full mailing address and residence of each inventor whose signature appears below as allowed under 37 CFR 1.63(c). The ADS also sets forth any Domestic Priority Claims under 35 USC §§ 119(e), 120, 121, and 365.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful, false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first inventor: Johan Emil Viktor Bjorsell

Signature: _____ Date: August 2nd 2013

Citizenship: ~~SIS~~ CA EB

DECLARATION FOR UTILITY OR DESIGN APPLICATION UNDER 37 CFR 1.63

Docket No.: SMARB19.004APC

Title: MOBILE GATEWAY

Inventors: Johan Emil Viktor Bjorsell, Maksym Sobolyev, Pentti Kalevi Huttunen, Emil Malak

Please Direct All Correspondence to Customer Number 20995

Full name of **second** inventor: Maksym Sobolyev

Signature: _____ Date: _____

Citizenship: UA

Full name of **third** inventor: Pentti Kalevi Huttunen

Signature: _____ Date: _____

Citizenship: CA

Full name of **fourth** inventor: Emil Malak

Signature: _____ Date: 2nd August 2013

Citizenship: CA

Send Correspondence To:
KNOBBE, MARTENS, OLSON & BEAR, LLP
Customer No. 20995

15836998
071913

Electronic Patent Application Fee Transmittal	
Application Number:	13056277
Filing Date:	27-Jan-2011
Title of Invention:	MOBILE GATEWAY
First Named Inventor/Applicant Name:	Johan Emil Viktor Bjorsell
Filer:	John M Carson/Catherine Tolo
Attorney Docket Number:	SMARB19.004APC
Filed as Small Entity	

U.S. National Stage under 35 USC 371 Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Correction of Inventorship on Merits	2819	1	300	300
		Total in USD ($)		**300**

Electronic Acknowledgement Receipt

EFS ID:	16504925
Application Number:	13056277
International Application Number:	
Confirmation Number:	2403
Title of Invention:	MOBILE GATEWAY
First Named Inventor/Applicant Name:	Johan Emil Viktor Bjorsell
Customer Number:	20995
Filer:	John M Carson/Gustavo Lopez
Filer Authorized By:	John M Carson
Attorney Docket Number:	SMARB19.004APC
Receipt Date:	05-AUG-2013
Filing Date:	27-JAN-2011
Time Stamp:	19:13:36
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$300
RAM confirmation Number	6355
Deposit Account	111410
Authorized User	KNOBBE MARTENS OLSON AND BEAR

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request under Rule 48 correcting inventorship	SMARB19_004APC_request.pdf	213453 90dd96df689e7f8fc5ba4da82e49ed3ce546f8e2	no	6
Warnings:					
Information:					
2	Oath or Declaration filed	SMARB19_004APC_declaration.pdf	210561 53168ae4db210875f8dcae5328f9fd2b6c512274	no	6
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30292 420b1f90614622a5de1d19f9bd86c835964c5183	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	454306		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/056,277	01/27/2011	Johan Emil Viktor Bjorsell	SMARB19.004APC

CONFIRMATION NO. 2403

IMPROPER CFR REQUEST

20995
KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

OC000000063143041

Date Mailed: 08/12/2013

RESPONSE TO REQUEST FOR CORRECTED FILING RECEIPT

Power of Attorney, Claims, Fees, System Limitations, and Miscellaneous

In response to your request for a corrected Filing Receipt, the Office is unable to comply with your request because:

- The request to correct inventorship under 37 CFR 1.48(a) is deficient because a new or corrected application data sheet has not been submitted.

/ydemisse/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Please Direct All Correspondence to Customer Number 20995

CORRECTED REQUEST TO CORRECT INVENTORSHIP

Inventor	:	Johan Emil Viktor Bjorsell, et al.
App. No	:	13/056277
Filed	:	January 27, 2011
For	:	MOBILE GATEWAY
Examiner	:	Rahman, Mostazir M.
Conf. No.	:	2403

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Pursuant to 37 CFR 1.48(c), this Request is being made to have Emil Malak added as an inventor to the present application. Applicant submits that the omission of the inventor Emil Malak was an error that occurred without deceptive intent.

The inventors of U.S. Patent Application No. 13/056,277 should be listed as follows:

Johan Emil Viktor Bjorsell

Maksym Sobolyev

Pentti Kalevi Huttunen

Emil Malak

This Request is accompanied by:

1. A statement by Emil Malak indicating that the error in inventorship in the above-referenced application occurred without deceptive intent, and was necessitated by amendment of the claims pursuant to 37 C.F.R. § 1.48(c)(2
2. An oath or declaration by the actual inventors as required by 37 C.F.R. §1.63;
3. Written Consent of the Assignee, Digifonica (International) Limited; and
4. A Supplemental Application Data Sheet.

Please Direct All Correspondence to Customer Number **20995**

The fee set forth in §1.17(i) was previously paid on August 5, 2013. Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE MARTENS OLSON & BEAR LLP

Dated: 8/19/13

By: _____

John M. Carson
Registration No. 34,303
Attorney of Record
Customer No. 20995
(858) 707-4000

16038677
081613

Please Direct All Correspondence to Customer Number 20995

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	:	Johan Emil Viktor Bjorsell, et al.
App. No	:	13/056277
Filed	:	January 27, 2013
For	:	MOBILE GATEWAY
Examiner	:	Rahman, Mostazir M.
Art Unit	:	2403

WRITTEN CONSENT OF ASSIGNEE TO CORRECTION OF INVENTORSHIP UNDER 37 C.F.R. § 1.48(c)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The undersigned is an empowered representative of the Assignee. On behalf of the Assignee, Digifonica (International) Limited, and in accordance with 37 C.F.R. § 1.48(c)(5), the undersigned hereby consents to the addition of the following inventor:

Emil Malak
1005-1288 Alberni Street
Vancouver B.C. V6E 4N5

Date: August 2nd/2013 Signature: E Malak

Name: EMIL MALAK

Title: Director

Digifonica (International) Limited

Please Direct All Correspondence to Customer Number 20995

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	:	Johan Emil Viktor Bjorsell, et al.
App. No	:	13/056277
Filed	:	January 27, 2013
For	:	MOBILE GATEWAY
Examiner	:	Rahman, Mostazir M.
Art Unit	:	2403

STATEMENT UNDER 37 C.F.R. § 1.48(c)

Commissioner for Patents – Mail Stop PCT
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

I, Emil Malak, declare as follows:

1. I should be listed as an inventor of the above-referenced application.

2. My listing as an inventor was necessitated by amendment of the claims and the inventorship error occurred without deceptive intention on my part.

3. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful, false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States codes and that such willful, false statements may jeopardize the validity of the application or patent issuing therefrom.

Dated: 2nd August 2013 By: _____
Emil Malak

ASSIGNMENT

WHEREAS, Emil Malak, a CA citizen, residing at Canada (hereinafter referred to as "ASSIGNOR") invented certain new and useful improvements, technology, inventions, developments, ideas or discoveries related to MOBILE GATEWAY (collectively hereinafter referred to as the "Work") for which an application for Letters Patent in the United States has been filed with the United States Patent and Trademark Office and designated U.S. Patent App. No. 13/056277 (hereinafter the "Application");

AND WHEREAS, DIGIFONICA (INTERNATIONAL) LIMITED, an entity organized under the Companies Act of Gibraltar and having a Canadian Address of 773 Hornby Street Vancouver British Columbia, V6Z 1S4 Canada, (formerly 1401, 4710 Kingsway, Burnaby, British Columbia, V5H 4M2 Canada (hereinafter the "ASSIGNEE"), desires to acquire the entire right, title, and interest in and to the Application and the Work:

NOW, THEREFORE, for good and valuable consideration, the receipt of which is hereby acknowledged, ASSIGNOR hereby acknowledges that ASSIGNOR has sold, assigned, transferred and set over, and by these presents does hereby sell, assign, transfer and set over, unto said ASSIGNEE, its successors, legal representatives and assigns, the entire right, title, and interest throughout the world in the Application and the Work, including all provisional applications relating thereto (including but not limited to U.S. Provisional Application No. 61/129,898, filed July 28, 2008), and all nonprovisional applications claiming priority thereto, including, all divisions, continuations, continuations-in-part, reissues, and reexaminations thereof, and all Letters Patent of the United States which may be granted thereon and all reissues and extensions thereof, and all rights of priority under International Conventions and any related Letters Patent which may hereafter be granted or filed in any country or countries foreign to the United States, all extensions, renewals and reissues thereof; and ASSIGNOR hereby authorizes and requests the Commissioner of Patents of the United States, and any Official of any country or countries foreign to the United States, whose duty it is to issue patents on applications as aforesaid, to issue all related Letters Patent to the ASSIGNEE, its successors, legal representatives and assigns, in accordance with the terms of this instrument:

AND ASSIGNOR DOES HEREBY sell, assign, transfer, and convey to ASSIGNEE, its successors, legal representatives, and assigns all claims for damages and all remedies arising out of any violation of the rights assigned hereby that may have accrued prior to the date of assignment to ASSIGNEE, or may accrue hereafter, including, but not limited to, the right to sue for, collect, and retain damages for past infringements of said Letters Patent before or after issuance.

AND ASSIGNOR DOES HEREBY covenant and agree that ASSIGNOR will communicate to said ASSIGNEE, its successors, legal representatives and assigns, any facts known to ASSIGNOR respecting the Work, and testify in any legal proceeding, assist in the preparation of any other provisional or non-provisional applications relating to the Application and the Work or any improvements made thereto, sign all lawful papers, execute and make all rightful oaths and/or declarations in connection with the Application and the Work including any improvements made thereto, any patent applications filed therefrom, and any continuing application filed from any of the aforementioned applications, and generally do everything possible to aid the ASSIGNEE, its successors, legal representatives and assigns, to obtain and enforce proper patent protection for the Work in all countries.

This 2nd day of August, 2013.

Emil Malak

Witnessed by:

Printed Name: Erica Nath

DECLARATION FOR UTILITY OR DESIGN APPLICATION UNDER 37 CFR 1.63

Docket No.: SMARB19.004APC

Title: MOBILE GATEWAY

Inventors: Johan Emil Viktor Bjorsell, Maksym Sobolyev, Pentti Kalevi Hummen, Emil Malak

Please Direct All Correspondence to Customer Number 20995

This Declaration is directed to the invention described and claimed the application that was filed on July 28, 2009, was assigned International App. No. PCT/CA2009/001062, entered the national phase on January 27, 2011, and was further assigned U.S. Patent App. No. 13/056277.

As a below named inventor:

I believe the inventors named below to be the original and first inventors of the subject matter which is described and claimed and for which a patent is sought;

I have reviewed and understand the contents of the above-identified application, including the claims; and

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

The application was originally filed with an Application Data Sheet (ADS). The ADS sets forth any applicable Foreign Priority Claims under 35 USC § 119, and sets forth the full mailing address and residence of each inventor whose signature appears below as allowed under 37 CFR 1.63(c). The ADS also sets forth any Domestic Priority Claims under 35 USC §§ 119(e), 120, 121, and 365.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful, false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first inventor: Johan Emil Viktor Bjorsell

Signature: _____ Date: August 2nd 2013

Citizenship: ~~SE~~ CA

DECLARATION FOR UTILITY OR DESIGN APPLICATION UNDER 37 CFR 1.63

Docket No.: SMARB19.004APC

Title: MOBILE GATEWAY

Inventors: Johan Emil Viktor Bjorsell, Maksym Sobolyev, Pentti Kalevi Huttunen, Emil Malak

Please Direct All Correspondence to Customer Number 20995

Full name of second inventor: Maksym Sobolyev

Signature: _____ Date: August 2nd, 2013

Citizenship: ~~UA~~ CA

Full name of third inventor: Pentti Kalevi Huttunen

Signature: _____ Date: _____

Citizenship: CA

Full name of fourth inventor: Emil Malak

Signature: _____ Date: _____

Citizenship: CA

Send Correspondence To:
KNOBBE, MARTENS, OLSON & BEAR, LLP
Customer No. 20995

15836998
071913

DECLARATION FOR UTILITY OR DESIGN APPLICATION UNDER 37 CFR 1.63

Docket No.: SMARB19.004APC

Title: MOBILE GATEWAY

Inventors: Johan Emil Viktor Bjorsell, Maksym Sobolyev, Pentti Kalevi Huttunen, Emil Malak

Please Direct All Correspondence to Customer Number 20995

This Declaration is directed to the invention described and claimed the application that was filed on July 28, 2009, was assigned International App. No. PCT/CA2009/001062, entered the national phase on January 27, 2011, and was further assigned U.S. Patent App. No. 13/056277.

As a below named inventor:

I believe the inventors named below to be the original and first inventors of the subject matter which is described and claimed and for which a patent is sought;

I have reviewed and understand the contents of the above-identified application, including the claims; and

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

The application was originally filed with an Application Data Sheet (ADS). The ADS sets forth any applicable Foreign Priority Claims under 35 USC § 119, and sets forth the full mailing address and residence of each inventor whose signature appears below as allowed under 37 CFR 1.63(c). The ADS also sets forth any Domestic Priority Claims under 35 USC §§ 119(e), 120, 121, and 365.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful, false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first inventor: Johan Emil Viktor Bjorsell

Signature: _____ Date: August 2nd 2013

Citizenship: ~~SE~~ CA EB

DECLARATION FOR UTILITY OR DESIGN APPLICATION UNDER 37 CFR 1.63

Docket No.: SMARB19.004APC Page 2 of 2

Title: MOBILE GATEWAY

Inventors: Johan Emil Viktor Bjorsell, Maksym Sobolyev, Pentti Kalevi Huttunen, Emil Malak

Please Direct All Correspondence to Customer Number 20995

Full name of **second** inventor: Maksym Sobolyev

Signature: _____ Date: _____

Citizenship: UA

Full name of **third** inventor: Pentti Kalevi Huttunen

Signature: _____ Date: Aug 02, 2013.

Citizenship: CA

Full name of **fourth** inventor: Emil Malak

Signature: _____ Date: _____

Citizenship: CA

Send Correspondence To:
KNOBBE, MARTENS, OLSON & BEAR, LLP
Customer No. 20995

15836998
071913

DECLARATION FOR UTILITY OR DESIGN APPLICATION UNDER 37 CFR 1.63

Docket No.: SMARB19.004APC

Title: MOBILE GATEWAY

Inventors: Johan Emil Viktor Bjorsell, Maksym Sobolyev, Pentti Kalevi Huttunen, Emil Malak

Please Direct All Correspondence to Customer Number 20995

This Declaration is directed to the invention described and claimed the application that was filed on July 28, 2009, was assigned International App. No. PCT/CA2009/001062, entered the national phase on January 27, 2011, and was further assigned U.S. Patent App. No. 13/056277.

As a below named inventor:

I believe the inventors named below to be the original and first inventors of the subject matter which is described and claimed and for which a patent is sought;

I have reviewed and understand the contents of the above-identified application, including the claims; and

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

The application was originally filed with an Application Data Sheet (ADS). The ADS sets forth any applicable Foreign Priority Claims under 35 USC § 119, and sets forth the full mailing address and residence of each inventor whose signature appears below as allowed under 37 CFR 1.63(c). The ADS also sets forth any Domestic Priority Claims under 35 USC §§ 119(e), 120, 121, and 365.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful, false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first inventor: Johan Emil Viktor Bjorsell

Signature: _____ Date: August 2nd 2013

Citizenship: ~~SE~~ CA EB

DECLARATION FOR UTILITY OR DESIGN APPLICATION UNDER 37 CFR 1.63

Docket No.: SMARB19.004APC

Title: MOBILE GATEWAY

Inventors: Johan Emil Viktor Bjorsell, Maksym Sobolyev, Pentti Kalevi Huttunen, Emil Malak

Please Direct All Correspondence to Customer Number 20995

Full name of second inventor: Maksym Sobolyev

Signature: _____ Date: _____

Citizenship: UA

Full name of third inventor: Pentti Kalevi Huttunen

Signature: _____ Date: _____

Citizenship: CA

Full name of fourth inventor: Emil Malak

Signature: _____ Date: 2nd August 2013

Citizenship: CA

Send Correspondence To:
KNOBBE, MARTENS, OLSON & BEAR, LLP
Customer No. 20995

15836998
071913

SUPPLEMENTAL APPLICATION DATA SHEET

Application Information

Application Number::	13/056,277
Filing Date::	January 27, 2011
Application Type::	Nonprovisional
Subject Matter::	Utility
Title::	MOBILE GATEWAY
Attorney Docket Number::	SMARB19.004APC
Total Drawing Sheets::	17
Small Entity?::	Yes

Applicant Information

Applicant Authority Type::	Inventor
Primary Citizenship Country::	SE
Given Name::	Johan
Middle Name::	Emil Viktor
Family Name::	Bjorsell
City of Residence::	Vancouver
State or Prov. of Residence::	BC
Country of Residence::	CA
Street::	PO Box 29164, RPO South Granville Post
City::	Vancouver
State or Province::	BC
Country::	CA
Postal or Zip Code::	V6J 0A6

Applicant Authority Type::	Inventor
Primary Citizenship Country::	UA
Given Name::	Maksym
Family Name::	Sobolyev

City of Residence::	New Westminster
State or Prov. of Residence::	BC
Country of Residence::	CA
Street::	506-210 Eleventh Street
City::	New Westminster
State or Province::	BC
Country::	CA
Postal or Zip Code::	V3M 4C9

Applicant Authority Type::	Inventor
Primary Citizenship Country::	CA
Given Name::	Pentti
Middle Name::	Kalevi
Family Name::	Huttunen
City of Residence::	Vancouver
State or Prov. of Residence::	BC
Country of Residence::	CA
Street::	76-3180 East 58th Avenue
City::	Vancouver
State or Province::	BC
Country::	CA
Postal or Zip Code::	V5S 3S8

Applicant Authority Type::	Inventor
Primary Citizenship Country::	CA
Given Name::	Emil
Family Name::	Malak
City of Residence::	Vancouver
State or Prov. of Residence::	BC
Country of Residence::	CA
Street::	1005-1288 Alberni Street

City:: Vancouver
State or Province:: BC
Country:: CA
Postal or Zip Code:: V6E 4N5

Correspondence Information

Correspondence Customer Number:: 20995
E-Mail Address:: efiling@knobbe.com

Representative Information

Representative Customer Number:: 20995

Domestic Priority Information

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
	a 371 of international	PCT/CA2009/001062	2009-07-28
PCT/CA2009/001062	non provisional of	61/129898	2008-07-28

Assignment Information

Assignee Name:: DIGIFONICA (INTERNATIONAL) LIMITED
Street:: ~~Suite #890, 999 West Hastings Street~~ 773 Hornby Street
City:: Vancouver
State or Province:: BC
Country:: CA
Postal or Zip Code:: ~~V6C 2W2~~ V6Z 1S4



Dated: August 19, 2013

By:

John M. Carson
Registration No. 34,303
Attorney of Record
Customer No. 20995
(858) 707-4000

16037787
081613

Electronic Acknowledgement Receipt

EFS ID:	16625827
Application Number:	13056277
International Application Number:	
Confirmation Number:	2403
Title of Invention:	MOBILE GATEWAY
First Named Inventor/Applicant Name:	Johan Emil Viktor Bjorsell
Customer Number:	20995
Filer:	John M Carson/Erica Van Sciver
Filer Authorized By:	John M Carson
Attorney Docket Number:	SMARB19.004APC
Receipt Date:	19-AUG-2013
Filing Date:	27-JAN-2011
Time Stamp:	19:03:02
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request under Rule 48 correcting inventorship	SMARB19004APC_CORRFR.pdf	217969 165c740f3b8ced4d281d30c4b0ed33c15d0096b1	no	6

Warnings:	
Information:	

2	Oath or Declaration filed	SMARB19004APC_DEC.pdf	205933 76b1c21f5e51b5db67c4e85819afce82989eda92	no	6
Warnings:					
Information:					
3	Application Data Sheet	SMARB19004APC_SUPPADS.pdf	81071 de99a4e4dda37d20f6266e618336ae1396a4870e	no	4
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
		Total Files Size (in bytes):	504973		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 08/28/2013

ASAHLE SALE #00000024 Mailroom Dt: 08/19/2013 111410 13056277
01 FC : 2830 70.00 DA

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	:	Johan Emil Viktor Bjorsell, et al.
App. No.	:	13/056,277
Filed	:	January 27, 2011
For	:	MOBILE GATEWAY
Examiner	:	Rahman, Mostazir M.
Art Unit	:	2413
Conf. No.	:	2403

SUPPLEMENTAL AMENDMENT

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Supplemental to the Reply to Non-final Office Action with Amendment filed on May 24, 2013, and responsive to the Examiner Interviews conducted on August 14, 2013 and August 20, 2013, Applicant presents the following amendments and remarks.

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Summary of Interview begins on page 20 of this paper.

Remarks begin on page 21 of this paper.

AMENDMENTS TO THE CLAIMS

1. (**Currently Amended**) A method of roaming with a mobile telephone, the method comprising:

receiving, from a user of the mobile telephone, a callee identifier associated with the callee;

transmitting an access code request message to an access server~~,~~ to seek an access code from a pool of access codes wherein each access code in said pool of access codes identifies a respective telephone number or Internal Protocol (IP) network address that enables a local call to be made to call the callee identified by the callee identifier, said access code request message including said callee identifier and a location identifier separate and distinctive from said callee identifier, said location identifier identifying a location of the mobile telephone;

receiving an access code reply message from the access server in response to said access code request message, said access code reply message including an access code different from said callee identifier and associated with said location identifier and/or associated with a location pre-associated with the mobile telephone and wherein said access code expires after a period of time; and

initiating a call with the mobile telephone using said access code to identify the callee.

2. (**Original**) The method of claim **1** wherein transmitting comprises transmitting said access code request message to said access server on a non-voice network.

3. (**Cancelled**)

4. (**Previously Presented**) The method of claim **1** wherein transmitting said location identifier comprises transmitting an IP address of the mobile telephone in a wireless IP network.

5. (**Previously Presented**) The method of claim **1** wherein transmitting said location identifier comprises transmitting an identifier of a wireless voice signal station in wireless communication with the mobile telephone.

6. (**Previously Presented**) The method of claim **1** wherein transmitting said location identifier comprises transmitting a user-configured identifier of a location associated with the mobile telephone.

7. (**Original**) The method of claim **1** wherein receiving said access code reply message comprises receiving said access code reply message from said access server on a non-voice network.

8. (**Currently Amended**) The method of claim **1** wherein receiving said access code reply message comprises receiving, in said access code reply message, ~~said~~ an access code temporarily associated with said callee identifier.

9. (**Original**) The method of claim **1** wherein receiving said access code reply message comprises receiving, in said access code reply message, a telephone number identifying a channel operably configured to cooperate with an IP network to cause a call involving the mobile telephone and the callee to be routed through the IP network.

10. (**Original**) The method of claim **9** wherein initiating said call comprises engaging a routing controller to route said call on said IP network to the callee.

11. (**Previously Presented**) The method of claim **1** further comprising:

receiving from the mobile telephone said access code request message;

communicating with a routing controller to obtain from the routing controller said access code wherein said access code identifies a communications channel associated with said location identifier and wherein said access code is useable by the mobile

telephone to cause the routing controller to establish a call to the callee using the channel; and

transmitting said access code reply message to the mobile telephone.

12. (**Currently Amended**) A mobile telephone apparatus comprising:

means for receiving, from a user of the mobile telephone, a callee identifier associated with the callee;

transmitting means for transmitting an access code request message to an access server~~,~~ to seek an access code from a pool of access codes wherein each access code in said pool of access codes identifies a respective telephone number or Internal Protocol (IP) network address that enables a local call to be made to call the callee identified by the callee identifier, said access code request message including said callee identifier and a location identifier separate and distinctive from said callee identifier, said location identifier identifying a location of the mobile telephone;

means for receiving an access code reply message from the access server in response to said access code request message, said access code reply message including an access code different from said callee identifier and associated with said location identifier and/or associated with a location pre-associated with the mobile telephone and wherein said access code expires after a period of time; and

means for initiating a call using said access code to identify the callee.

13. (**Original**) The mobile telephone apparatus of claim **12** wherein said transmitting means comprises a non-voice network interface for transmitting said access code request message to said access server on a non-voice network.

14. (**Cancelled**)

15. (**Previously Presented**) The mobile telephone apparatus of claim **12** wherein said location identifier comprises an IP address of the mobile telephone in a wireless IP network.

16. (**Previously Presented**) The mobile telephone apparatus of claim **12** wherein said location identifier comprises an identifier of a wireless voice signal station in wireless communication with the mobile telephone.

17. (**Previously Presented**) The mobile telephone apparatus of claim **12** wherein said location identifier comprises a user-configured identifier of a location associated with the mobile telephone.

18. (**Original**) The mobile telephone apparatus of claim **12** wherein said means for receiving an access code reply message comprises a non-voice network interface for receiving said access code reply message on a non-voice network.

19. (**Original**) The mobile telephone apparatus of claim **12** wherein said access code includes a telephone number.

20. (**Original**) The mobile telephone apparatus of claim **12** wherein said means for initiating comprises a mobile telephone network interface.

21. (**Previously Presented**) A system for enabling roaming by a mobile telephone, the system comprising the mobile telephone apparatus of claim **12** and further comprising:

a routing controller; and

an access server comprising:

means for receiving from the mobile telephone said access code request message;

means for communicating with said routing controller to obtain from said routing controller said access code wherein said access code identifies a channel associated with said location identifier and wherein said access code is useable by the mobile telephone to cause the routing controller to establish a call to the callee using the channel; and

means for transmitting said access code reply message including said access code to the mobile telephone.

22. (**Currently Amended**) A mobile telephone apparatus comprising:

a processor circuit;

a network interface in communication with said processor circuit; and

a computer readable medium in communication with said processor circuit and encoded with codes for directing said processor circuit to:

receive, from a user of the mobile telephone, a callee identifier associated with the callee;

cause an access code request message to be transmitted to an access server to seek an access code from a pool of access codes wherein each access code in said pool of access codes identifies a respective telephone number or Internal Protocol (IP) network address that enables a local call to be made to call the callee identified by the callee identifier, said access code request message including said callee identifier and a location identifier separate and distinctive from said callee identifier, said location identifier identifying a location of the mobile telephone;

receive an access code reply message from the access server in response to said access code request message, said access code reply message including an access code different from said callee identifier and associated with said location identifier and/or associated with a location pre-associated with the mobile telephone and wherein said access code expires after a period of time; and

initiate a call using said access code to identify the callee.

23. (**Original**) The mobile telephone apparatus of claim **22** wherein said network interface comprises a non-voice network interface, and wherein said codes for directing said processor circuit to cause said access code request message to be transmitted include codes for directing said processor circuit to cause said access code request message to be transmitted to said access server using said non-voice network interface on a non-voice network.

24. (**Cancelled**)

25. (**Previously Presented**) The mobile telephone apparatus of claim **22** wherein said location identifier comprises an IP address of the mobile telephone in a wireless IP network.

26. (**Previously Presented**) The mobile telephone apparatus of claim **22** wherein said location identifier comprises an identifier of a wireless voice signal station in wireless communication with the mobile telephone.

27. (**Previously Presented**) The mobile telephone apparatus of claim **22** wherein said location identifier comprises a user-configured identifier of a location associated with the mobile telephone.

28. (**Original**) The mobile telephone apparatus of claim **22** wherein said network interface comprises a non-voice network interface, and wherein said codes for directing said processor circuit to receive an access code reply message include codes for directing said processor circuit to cause said access code reply message to be received from said access server using said non-voice network interface on a non-voice network.

29. (**Original**) The mobile telephone apparatus of claim **22** wherein said access code includes a telephone number identifying a channel operably configured to cooperate with an IP network to cause a call involving the mobile telephone and the callee to be routed through the IP network.

30. (**Original**) The mobile telephone apparatus of claim **22** wherein said network interface comprises a mobile telephone network interface, and wherein said codes for directing said processor circuit to initiate include codes for directing said processor circuit to cause a call to be initiated using said mobile telephone network interface on a mobile telephone network.

31. (**Previously Presented**) A system for enabling roaming by a mobile telephone, the system comprising the mobile telephone of claim **22** and further comprising:

a routing controller; and

an access server comprising a processor circuit and a computer readable medium in communication with the processor circuit, the computer readable medium encoded with codes for directing said processor circuit to:

receive from the mobile telephone said access code request message;

communicate with said routing controller to obtain from said routing controller said access code wherein said access code identifies a channel associated with said location identifier and wherein said access code is useable by the mobile telephone to cause the routing controller to establish a call to the callee using the channel; and

transmit said access code reply message to the mobile telephone.

32. (**Currently amended**) A non-transitory computer readable medium encoded with codes for directing a processor circuit to enable mobile telephone roaming, said codes being operable to direct the processor circuit to:

receive, from a user of a mobile telephone, a callee identifier associated with a callee;

transmit an access code request message to an access server to seek an access code from a pool of access codes telephone wherein each access code in said pool of access codes identifies a respective telephone number or Internal Protocol (IP) network address to enable a local call to be made to call the callee identified by the callee identifier, said access code request message including said callee identifier and a location identifier separate and distinctive from said callee identifier, said location identifier identifying a location of the mobile telephone;

receive an access code reply message from the access server in response to said access code request message, said access code reply message including an access code different from said callee identifier and associated with said ~~callee~~ location identifier and/or associated with a location pre-associated with the mobile telephone and wherein said access code expires after a period of time; and

initiate a call using said access code to identify the callee.

33. (**Currently Amended**) A method for enabling mobile telephone roaming, the method comprising:

receiving from the mobile telephone an access code request message including a callee identifier associated with the callee and a location identifier separate and distinctive from said callee identifier, identifying a location of the mobile telephone;

producing an access code identifying a communication channel based on said location identifier and/or based on a location pre-associated with the mobile telephone, said access code being different from the callee identifier and useable by the mobile telephone to initiate a call to the callee using the channel, and wherein said access code expires after a period of time and wherein producing said access code comprises selecting said access code from a pool of access codes, wherein each access code in said pool of access codes identifies a respective telephone number or Internet Protocol (IP) network address; and

transmitting an access code reply message including said access code, to the mobile telephone.

34. (**Original**) The method of claim **33** wherein receiving comprises receiving said access code request message on a non-voice network.

35. (**Previously Presented**) The method of claim **33** wherein producing said access code comprises causing a routing controller operably configured to route a call between said caller and said callee to produce said access code.

36. (**Cancelled**)

37. (**Currently Amended**) The method of claim ~~36~~ **33** further comprising determining from said location identifier a local calling area associated with the mobile telephone and selecting an access code associated with a calling area matching said local calling area associated with the mobile telephone.

38. (**Currently Amended**) The method of claim ~~36~~ 37 further comprising accessing a location field of a dialing profile associated with the caller when a local calling area cannot be determined from the contents of said location identifier and determining a local calling area associated with the mobile telephone from the contents of said location field and selecting an access code associated with a calling area matching the local calling area associated with the mobile telephone.

39. (**Previously Presented**) The method of claim **33** wherein said location identifier comprises an IP address of the mobile telephone in a wireless IP network.

40. (**Previously Presented**) The method of claim **33** wherein said location identifier comprises an identifier of a wireless voice signal station in wireless communication with the mobile telephone.

41. (**Previously Presented**) The method of claim **33** wherein said location identifier comprises a user-configured identifier of a location associated with the mobile telephone.

42. (**Cancelled**)

43. (**Currently Amended**) The method of claim ~~36~~ 33 wherein at least one of said access codes in said pool of access codes identifies an IP network address as a possible channel through which said call can be conducted.

44. (**Previously Presented**) The method of claim **43** further comprising enabling communications between said caller and said callee to be established through an IP network in response to a call received at said IP network address.

45. (**Currently Amended**) The method of claim ~~36~~ 33 wherein said access code request message includes a caller identifier and wherein the method further comprises associating said caller identifier included in said access code request message with the selected access code.

46. (**Cancelled**)

47. (**Previously Presented**) The method of claim **45** further comprising associating said callee identifier included in said access code request message with the selected access code.

48. (**Previously Presented**) The method of claim **47** wherein said associating said caller identifier and said callee identifier with the selected access code occurs only when:

a) the access code is not already associated with a callee id; or

b) the access code is already associated with a callee id, and a timeout value associated with that callee id has expired.

49. (**Previously Presented**) The method of claim **33** wherein producing further comprises associating a timestamp with said access code, for use in determining when the usability of said access code to initiate a call to the callee will expire, and causing said timestamp to be included in said access code reply message transmitted to the mobile telephone.

50. (**Previously Presented**) The method of claim **49** further comprising enabling communications to be established between said caller and said callee when the mobile telephone seeks to establish a call to said callee using the access code transmitted in the access code reply message when said timestamp associated with said access code indicates the usability of said access code has not expired and not enabling said communications to be established when said timestamp indicates the usability of said access code has expired.

51. (**Original**) The method of claim **33** wherein transmitting comprises transmitting said access code reply message on a non-voice network.

52. (**Currently Amended**) A system for enabling mobile telephone roaming, the system comprising:

means for receiving from the mobile telephone an access code request message including a callee identifier associated with the callee and a location identifier separate and distinctive from said callee identifier, identifying a location of the mobile telephone;

means for producing an access code identifying a communication channel based on said location identifier and/or based on a location pre-associated with the mobile telephone, said access code being different from the callee identifier and useable by the mobile telephone to initiate a call to the callee using the channel and wherein said access code expires after a period of time and wherein said means for producing said access code comprises means for selecting said access code from a pool of access codes wherein each access code in said pool of access codes identifies a respective telephone number or Internet Protocol (IP) network address; and

means for transmitting an access code reply message including said access code to the mobile telephone.

53. (**Original**) The system of claim **52** wherein said means for receiving comprises a non-voice network interface for receiving said access code request message on a non-voice network.

54. (**Previously Presented**) The system of claim **52** wherein said means for producing said access code comprises a routing controller operably configured to route a call between said caller and said callee.

55. (**Cancelled**)

56. (**Currently Amended**) The system of claim ~~55~~ **52** wherein said processor circuit is operably configured to determine a local calling area associated with the mobile telephone from said location identifier and to select an access code associated with a calling area matching said local calling area associated with the mobile telephone.

57. (**Previously Presented**) The system of claim **56** further comprising:

a dialing profile associated with the caller, said dialing profile including a location field; and

wherein said processor circuit is operably configured to determine a local calling area associated with the mobile telephone from the contents of said location field and to select an access code associated with a calling area matching the local calling area associated with the mobile telephone, when a local calling area associated with the mobile telephone cannot be determined from said location identifier.

58. (**Currently Amended**) The system of claim ~~56~~ 52 wherein said location identifier includes an IP address of the mobile telephone in a wireless IP network.

59. (**Currently Amended**) The system of claim ~~56~~ 52 wherein said location identifier includes an identifier of a wireless voice signal station in wireless communication with the mobile telephone.

60. (**Currently Amended**) The system of claim ~~56~~ 52 wherein said location identifier includes a user-configured identifier of a location associated with the mobile telephone.

61. (**Cancelled**)

62. (**Currently Amended**) The system of claim ~~55~~ 52 wherein at least one of said access codes in said pool of access codes identifies an IP network address as a possible channel through which said call can be conducted.

63. (**Currently Amended**) The system of claim ~~55~~ 52 wherein said processor circuit is operably configured to enable communications between said caller and said callee to be established through an IP network in response to a call received at said IP network address.

64. (**Currently Amended**) The system of claim ~~63~~ 52 wherein said access code request message includes a caller identifier and wherein said processor circuit is operably configured to associate said caller identifier with the selected access code.

65. (**Cancelled**)

66. (**Previously Presented**) The system of claim **64** wherein said processor circuit is operably configured to associate said callee identifier included in said access code request message with the selected access code.

67. (**Previously Presented**) The system of claim **66** wherein said processor circuit is operably configured to associate said caller identifier and said callee identifier with the selected access code only when:

a) the access code is not already associated with a callee id; or

b) the access code is already associated with a callee id, and a timeout value associated with that callee id has expired.

68. (**Currently Amended**) The system of claim ~~55~~ 52 wherein said processor circuit is operably configured to associate a timestamp with said access code, for use in determining when the usability of said access code to initiate a call to the callee will expire, and to cause said timestamp to be included in said access code reply message transmitted to the mobile telephone.

69. (**Previously Presented**) The system of claim **68** wherein said processor circuit is operably configured to enable communications to be established between said caller and said callee when the mobile telephone seeks to establish a call to said callee using the access code transmitted in the access code reply message when said timestamp associated with said access code indicates the usability of said access code has not expired and to prevent said communications from being established when said timestamp indicates the usability of said access code has expired.

70. (**Original**) The system of claim **52** wherein said means for transmitting comprises a non-voice network interface for transmitting said access code reply message on a non-voice network.

71. (**Currently Amended**) A system for enabling mobile telephone roaming, the system comprising:

a processor circuit;

a network interface in communication with said processor circuit; and

a computer readable medium in communication with said processor circuit and encoded with codes for directing said processor circuit to:

receive from the mobile telephone an access code request message including a callee identifier associated with the callee and a location identifier separate and distinctive from said callee identifier, identifying a location of the mobile telephone;

communicate with a routing controller to obtain from said routing controller an access code identifying a communication channel, said access code being determined from said location identifier and/or based on a location pre-associated with the mobile telephone and said access code being different from the callee identifier and useable by the mobile telephone to initiate a call to the callee using the channel, and wherein said access code expires after a period of time and wherein said access code is selected from a pool of access codes and wherein each access code in said pool of access codes identifies a respective telephone number or Internet Protocol (IP) network address; and

cause an access code reply message including said access code to be transmitted to the mobile telephone.

72. (**Original**) The system of claim **71** wherein said network interface comprises a non-voice network interface, and wherein said codes for directing said processor circuit to receive include codes for directing said processor circuit to cause said access code request message to be received using said non-voice network interface on a non-voice network.

73. (**Previously Presented**) The system of claim **71** wherein said codes for directing said processor circuit include codes for directing said processor circuit to cause a routing controller to produce said access code.

74. (**Cancelled**)

75. (**Currently Amended**) The system of claim ~~74~~ 71 wherein said codes for directing said processor circuit include codes for directing said processor circuit to determine from said location identifier a local calling area associated with the mobile telephone and to select an access code associated with a calling area matching said local calling area associated with the mobile telephone.

76. (**Currently Amended**) The system of claim **75** wherein said codes for directing said processor circuit include codes for directing said processor circuit to ~~accessing~~access a location field of a dialing profile associated with the caller when a local calling area cannot be determined from the contents of said location identifier and ~~determining~~determine a local calling area associated with the mobile telephone from the contents of said location field and ~~selecting~~select an access code associated with a calling area matching the local calling area associated with the mobile telephone.

77. (**Currently Amended**) The system of claim ~~75~~ 71 wherein said location identifier comprises an IP address of the mobile telephone in a wireless IP network.

78. (**Currently Amended**) The system of claim ~~75~~ 71 wherein said location identifier comprises an identifier of a wireless voice signal station in wireless communication with the mobile telephone.

79. (**Currently Amended**) The system of claim ~~75~~ 71 wherein said location identifier comprises a user-configured identifier of a location associated with the mobile telephone.

80. (**Cancelled**)

81. (**Currently Amended**) The system of claim ~~74~~ 71 wherein at least one of said access codes in said pool of access codes identifies an IP network address as a possible channel through which said call can be conducted.

82. (**Previously Presented**) The system of claim **81** wherein said codes for directing said processor circuit include codes for directing said processor circuit to enable communications between said caller and said callee to be established through an IP network in response to a call received at said IP network address.

83. (**Currently Amended**) The system of claim ~~82~~ 71 wherein said access code request message includes a caller identifier and wherein said codes for directing said processor circuit include codes for directing said processor circuit to associate said caller identifier included in said access code request message with the selected access code.

84. (**Cancelled**)

85. (**Previously Presented**) The system of claim **83** wherein said codes for directing said processor circuit include codes for directing said processor circuit to associate said callee identifier included in said access code request message with the selected access code.

86. (**Previously Presented**) The system of claim **85** wherein said codes for directing said processor circuit include codes for directing said processor circuit to associate said caller identifier and said callee identifier with the selected access code only when:

a) the access code is not already associated with a callee id; or

b) the access code is already associated with a callee id, and a timeout value associated with that callee id has expired.

87. (**Previously Presented**) The system of claim **71** wherein said codes for directing said processor circuit include codes for directing said processor circuit to associate a timestamp

with said access code, for use in determining when the usability of said access code to initiate a call to the callee will expire, and to cause said timestamp to be included in said access code reply message.

88. (**Previously Presented**) The system of claim **87** wherein said codes for directing said processor circuit include codes for directing said processor circuit to enable communications to be established between said caller and said callee when the mobile telephone seeks to establish a call to said callee using the access code transmitted in the access code reply message when said timestamp associated with said access code indicates the usability of said access code has not expired and to prevent said communications from being established when said timestamp indicates the usability of said access code has expired.

89. (**Original**) The system of claim **71** wherein said network interface comprises a non-voice network interface, and wherein codes for directing said processor circuit to transmit include codes for directing said processor circuit to cause said access code reply message to be transmitted using said non-voice network interface on a non-voice network.

90. (**Currently Amended**) A non-transitory computer readable medium encoded with codes for directing a processor circuit to enable mobile telephone roaming, the codes being operable to direct the processor circuit to:

receive from the mobile telephone an access code request message including a callee identifier associated with the callee and a location identifier separate and distinctive from said callee identifier, identifying a location of the mobile telephone;

communicate with a routing controller to obtain from said routing controller an access code identifying a communication channel, based on said location identifier and/or based on a location pre-associated with the mobile telephone, said access code being different from the callee identifier and useable by the mobile telephone to initiate a call to the callee using the channel, and wherein said access code expires after a period of time and wherein said access code is selected from a pool of access codes, wherein each access

code in said pool of access codes identifies a respective telephone number or Internet Protocol (IP) network address; and

cause an access code reply message including said access code to be transmitted to the mobile telephone.

SUMMARY OF INTERVIEW

Attendees, Date and Type of Interview

The telephonic interviews were conducted on August 14, 2013, attended by Examiner Mostazir M. Rahman, Supervisor Xavier Wong, and Applicant's representatives Andrew E. Morrell, John Knox and Raimond Salenieks and on August 20, 2013 and attended by supervisor Xavier Wong and Applicant's representative, Raimond Salenieks.

Identification of Claims Discussed

Independent Claims 1, 32, 33 and 90 were discussed.

Identification of Prior Art Discussed

No prior art was specifically discussed during the interview.

Proposed Amendments

Proposed amendments were discussed with the Examiners.

Principal Arguments and Other Matters

The cited references do not disclose all the features of the claims.

Results of Interview

Examiner Wong agreed that the proposed amendments overcome the cited references. Applicant to file a supplemental amendment with the proposed claim amendments.

REMARKS

Claims 1, 8, 12, 22, 32, 33, 37, 38, 43, 45, 52, 56, 58, 59, 60, 62, 63, 64, 68, 71, 75, 76, 77, 78, 79, 81, 83 and 90 have been amended. Claims 36, 55 and 74 are hereby cancelled. The amendments are supported by at least the original claims, and the PCT Publication WO 2010/012090. Independent Claims 1, 12, 22, 32, 33, 52, 71 and 90 have been amended as suggested by the Examiner, including independent Claims 32 and 90 that have been amended to refer to a non-transitory computer readable medium. Claims 8, 32, 38, and 76 have been amended to include minor editorial amendments. Claims 37, 38, 43, 45, 56, 58, 59, 60, 62, 63, 64, 68, 75, 77, 78, 79, 81, and 83 have been amended to change their dependencies, as necessitated by the cancellation of Claims 36, 55 and 74, and to change the chain of dependency where necessary. No new subject matter has been added. Applicant respectfully requests reconsideration of the application in light of the amendments.

Examiner Interviews

Applicant wishes to thank Examiner Mostazir M. Rahman and Supervisor Xavier Wong for the telephonic interview on August 14, 2013, and the follow-up telephonic interview with Supervisor Xavier Wong on August 20, 2013. The claims have been amended based on the helpful discussions with the Examiners. Supervisor Wong agreed that the proposed amendments will overcome the cited references.

No Disclaimers or Disavowals

Although the present communication may include alterations to the application or claims, or characterizations of claim scope or referenced art, Applicant is not conceding in this application that previously pending claims are not patentable over the cited references. Rather, any alterations or characterizations are being made to facilitate expeditious prosecution of this application. Applicant reserves the right to pursue at a later date any previously pending or other broader or narrower claims that capture any subject matter supported by the present disclosure, including subject matter found to be specifically disclaimed herein or by any prior prosecution. Accordingly, reviewers of this or any parent, child or related prosecution history shall not

reasonably infer that Applicant has made any disclaimers or disavowals of any subject matter supported by the present application.

Conclusion

Applicant has endeavored to address all of the Examiner's concerns as expressed in the telephonic interview on August 20, 2013. In light of the above amendments withdrawal of the outstanding rejections and a notice of allowance is respectfully requested. If the Examiner has any questions which may be answered by telephone, the Examiner is invited to call the undersigned directly.

Any remarks in support of patentability of one claim should not be imputed to any other claim in this or a related application, even if similar terminology is used. Any remarks referring to only a portion of a claim should not be understood to base patentability on solely that portion; rather, patentability must rest on each claim taken as a whole.

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 8/22/13

By: _____

John M. Carson
Registration No. 34,303
Attorney of Record
Customer No. 20995
(858) 707-4000

16065512
082113

Electronic Acknowledgement Receipt

EFS ID:	16664915
Application Number:	13056277
International Application Number:	
Confirmation Number:	2403
Title of Invention:	MOBILE GATEWAY
First Named Inventor/Applicant Name:	Johan Emil Viktor Bjorsell
Customer Number:	20995
Filer:	John M Carson/Daniela Lopez
Filer Authorized By:	John M Carson
Attorney Docket Number:	SMARB19.004APC
Receipt Date:	22-AUG-2013
Filing Date:	27-JAN-2011
Time Stamp:	19:58:27
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		SMARB19004APCsupplemental amend.pdf	955485 b42b45216111627ab933baac893079a33000ce5f	yes	22

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Supplemental Response or Supplemental Amendment	1	1
	Claims	2	19
	Applicant summary of interview with examiner	20	20
	Applicant Arguments/Remarks Made in an Amendment	21	22
Warnings:			
Information:			
	Total Files Size (in bytes):	955485	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.