Session Initiation Protocol (SIP) Configuration on a WRP400

Objective

Session Initiation Protocol (SIP) is a signaling protocol used to create, manage and terminate sessions in an IP based network. SIP is a mechanism for call management. It allows for the establishment of user locations. It provides for feature negotiation so that all of the participants in a session can agree on the features to be supported among them. It also allows for changes to be made to features of a session while a session is in progress.

The objective of this document is to guide you on how to configure the SIP Settings on a WRP400.

Applicable Device

• WRP400

Software Version

• 2.00.30

Session Initiation Protocol Configuration

SIP Parameters

Step 1. Log in to the web configuration utility and choose Voice > Admin Login > SIP. The SIP page opens:

Step 2. In the Max Forward field, enter the SIP Maximum Forward value (an integer in the range 0 to 255) to limit the number of proxies or gateways that can forward the request to the next downstream server. The default Max Forward is 70.

Step 3. In the Max Redirection field, enter the maximum number of times that an invite can be redirected to avoid infinite loop in a network. The default Max Redirections is 5.

Step 4. In the Max Auth field, enter the maximum authorization in numbers that a request
may be challenged. The Max Auth value can range from 0 to 255.

Step 5. In the SIP User Agent Name field, enter the User-Agent header used in outbound requests. The default User Agent Name is $VERSION. If this field is left empty, then the header will not include any value.

Step 6. In the SIP Server Name field, enter the server head used in responses to inbound responses. The default Server Name is $VERSION.

Step 7. In the SIP Reg User Agent Name field, enter the User-Agent name to be used in a register request.

Step 8. In the SIP Accept Language field, enter the preferred language header to be used. This field is used in requests to indicate the preferred languages for reason phrases, or status responses carried as message bodies in the response. If no Accept Language header field is present, the server should assume all languages are acceptable to the client.

Step 9. In the Dual Tone Multi Frequency (DTMF) Relay Multipurpose Internet Mail Extensions (MIME) Type field, enter the MIME type used in a SIP info message to signal a DTMF event. The default is application/dtmf-relay.

Step 10. From the Remove Last Reg drop-down list, choose yes to remove the last registration used before registering a new one, if the value is different. The default is yes.

Step 11. From the Use Compact Header drop-down list, choose yes to use compact SIP headers in outbound SIP messages instead of normal SIP headers. The default is yes.

Step 12. From the Escape Display Name drop-down list, choose yes to keep your display name private. The default is yes.

Step 13. From the RFC 2543 Call Hold drop-down list, choose yes to configure the type of call hold. The default is yes.

Step 14. If you choose yes from the Mark All AVT Packets drop-down list, then all AVT tone packets have a marker bit set. If you choose No, then only the first packet has a marker bit set for each DTMF event. The default is Yes.

Step 15. In the SIP TCP Port Min field, enter the lowest TCP port number that can be used for SIP sessions.

Step 16. In the SIP TCP Port Max field, enter the highest TCP port number that can be used for SIP sessions.

Step 17. From the Enable Voice Over USB Network drop down list choose yes to enable.

Step 18. Click Submit All Changes to save the settings.

SIP Timer Values
Step 1. Enter a RFC-3261 T1 value in the SIP T1 field. The range is 0 to 64 seconds. The default is 0.5 seconds.

Step 2. Enter a RFC-3261 T2 value in the SIP T2 field. It is the maximum retransmit interval for non-INVITE requests and INVITE responses. The range is from 0 to 64 seconds. Default is 4 seconds.

Step 3. Enter a RFC-3261 T4 value in the SIP T4 field. It is the maximum duration a message remains in the network. The range is from 0 to 64 seconds. Default is 5 seconds.

Step 4. Enter a RFC-3261 INVITE transaction time-out value in the SIP Timer B field. The range is from 0 to 64 seconds. Default is 16 seconds.

Step 5. Enter a RFC-3261 Non-INVITE transaction time-out value in the SIP Timer F field. The range is from 0 to 64 seconds. Default is 16 seconds.

Step 6. Enter a RFC-3261 INVITE final response time-out value for ACK receipt in the SIP Timer H field. The range is from 0 to 64 seconds. Default is 16 seconds.

Step 7. Enter a RFC-3261 wait time for retransmits in the SIP Timer D field. The range is from 0 to 64 seconds. Default is 16 seconds.

Step 8. Enter a RFC-3261 wait time for Non-INVITE request retransmits in the SIP Timer J field. The range is from 0 to 64 seconds. Default is 16 seconds.

Step 9. Enter the INVITE request Expire header value in the INVITE Expires field. If you enter 0 in this field, then the expire header is not included in the request.

Step 10. Enter a ReINVITE request Expires header value in the ReINVITE Expires field. The range is from 0 to 19999999999999999999999999999999 seconds. If you enter 0, the Expires header is not included in the request. Default is 30 seconds.

Step 11. Enter the minimum registration expiration time allowed from the proxy in the Reg Min Expires field. If the proxy returns a value less than this setting, the smallest of the two values is used. Default is 1 second.

Step 12. Enter the maximum registration expiration time allowed from the proxy in the Reg Max Expires field. If the value is greater than this setting, the largest of the two values is used. Default is 7200 seconds.

Step 13. Enter the retry interval in the Reg Retry Intvl field. It is the interval to wait before the Cisco IP phone retries registration after failing during the previous registration. The range is from 1 to 268435455 seconds. Default is 30 seconds.
Step 14. Enter the retry long interval in the Reg Retry Long Intvl field. When registration fails with a SIP response code that does not match the Retry Reg response status code (RSC) value, the IP phone waits for this length of time before retrying. This value should be much larger than the Reg Retry Intvl value. The range is from 0 to 268435455 seconds. Defaults is 1200 seconds.

Step 15. Click **Submit All Changes** to save the settings.

**Response Status Code Handling**

<table>
<thead>
<tr>
<th>SIT1 RSC:</th>
<th>401</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIT3 RSC:</td>
<td>403</td>
</tr>
<tr>
<td>Try Backup RSC:</td>
<td>500</td>
</tr>
<tr>
<td>SIT2 RSC:</td>
<td>402</td>
</tr>
<tr>
<td>SIT4 RSC:</td>
<td>404</td>
</tr>
<tr>
<td>Retry Reg RSC:</td>
<td>501</td>
</tr>
</tbody>
</table>

Step 1. Enter a SIP response status code for the appropriate Special Information Tone (SIT) in the SIT1 RSC field. It is an alternative to the recorder tone which is played when an error occurs as a caller makes an unbound call. The default is blank.

Step 2. Enter a SIP response status code that will result in the SIT2 Tone being played in the SIT2 RSC field. It is an alternative to the recorder tone which is played when an error occurs as a caller makes an unbound call. The default is blank.

Step 3. Enter a SIP response status code that will result in the SIT3 Tone being played in the SIT3 RSC field. It is an alternative to the recorder tone which is played when an error occurs as a caller makes an unbound call. The default is blank.

Step 4. Enter a SIP response status code that will result in the SIT4 Tone being played in the SIT4 RSC field. It is an alternative to the recorder tone which is played when an error occurs as a caller makes an unbound call. The default is blank.

Step 5. Enter a SIP response code that retries a backup server for the current request in the Try Backup RSC field. The default is blank.

Step 6. Enter the interval to wait (in seconds) before the device retries registration after the failure for the duration of the last registration in the Retry Reg RSC field. The default is 30.

Step 7. Click **Submit All Changes** to save the settings.

**RTP Parameters**

<table>
<thead>
<tr>
<th>RTP Port Min:</th>
<th>16384</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP Packet Size:</td>
<td>0.030</td>
</tr>
<tr>
<td>RTCP Tx Interval:</td>
<td>0</td>
</tr>
<tr>
<td>Stats In BYE:</td>
<td>yes</td>
</tr>
</tbody>
</table>

| RTP Port Max: | 16482 |
| Max RTP ICMP Err: | 0 |
| No UDP Checksum: | no |

Step 1. Enter the desired value in the RTP Port Min field. The RTP Port Min value is the minimum port number you can use for RTP transmission and reception. The default value is set to 16384.

Step 2. Enter the desired value in the RTP Port Max field. The RTP Port Max value is the maximum port number you can use for transmission and reception. The default value is set
Step 3. Enter the desired value in the RTP Packet Size field. The RTP Packet Size is the packet size in a transmission per second. The default value is set to 0.030.

Step 4. Enter the desired value in the Max RTP ICMP Err field. The Max RTP ICMP Err value is the number of successive ICMP errors allowed when transmitting RTP packets before the call is terminated. The default value is set to 0.

Step 5. Enter the desired value in the RTCP Tx Interval field. The RTCP Tx Interval is the interval in seconds (range from 0 to 255) for sending out RTCP sender reports on an active connection. The default value is set to 0.

Step 6. From the No UDP Checksum drop-down menu choose yes or no to calculate the UDP checksum. Choose yes if you want the SPA to do this calculation. The default value is set to no.

Step 7. From the Stats in Bye drop-down list, choose yes or no. This field determines whether the SPA includes in its header the P-RTP stat in a BYE message.

Step 8. Click **Submit All Changes** to save the settings.

**SDP Payload Types**

<table>
<thead>
<tr>
<th>NSE Dynamic Payload:</th>
<th>AVT Dynamic Payload:</th>
<th>G726r32 Dynamic Payload:</th>
<th>EncapRTP Dynamic Payload:</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFORMEQ Dynamic Payload:</td>
<td>100</td>
<td>G726r32 Dynamic Payload:</td>
<td>RTP-Start-Loopback Codec:</td>
</tr>
<tr>
<td>G729b Dynamic Payload:</td>
<td>5</td>
<td>EncapRTP Dynamic Payload:</td>
<td>RTP-Start-Loopback Codec:</td>
</tr>
<tr>
<td>RTP-Start-Loopback Dynamic Payload:</td>
<td>99</td>
<td>AVT Codec Name:</td>
<td>AVT Codec Name:</td>
</tr>
<tr>
<td>NSE Codec Name:</td>
<td>113</td>
<td>PCMU</td>
<td>telephone-event</td>
</tr>
<tr>
<td>G711a Codec Name:</td>
<td></td>
<td>G729a Codec Name:</td>
<td>G729a Codec Name:</td>
</tr>
<tr>
<td>G726r32 Codec Name:</td>
<td></td>
<td>G726r32 Codec Name:</td>
<td>EncapRTP Codec Name:</td>
</tr>
<tr>
<td>G729ab Codec Name:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Step 1. Enter the NSE Dynamic Payload value in the NSE Dynamic Payload field. This field specifies the payload for named signal events (NSE) for the WRP400 adapter. This payload is useful when there are no audio waveforms that are used in network. The valid range is 96-127. The default value is 100.

Step 2. Enter the number on which the sender and receiver must agree for the session event in the AVT Dynamic Payload field. The range is from 96 to 127. The default is 101.

Step 3. Enter the codec number which is used to send an SIP message in the INFORMEQ Dynamic Payload field. The best range is from 96 to 27. The default is blank.

**Note:** The INFORMEQ Dynamic Payload number should match with the network or other party number which is configured to enable the Dynamic Payload.

Step 4. Enter the RTP Payload Type Number in the G726r32 Dynamic Payload field. This is the number which represents the G.726r32 codec transmitted packet. The range is from 0 to 268435455. The default is 2.

Step 5. Enter the RTP Payload Type Number in the G729b Dynamic Payload field. This is
the number which represents the G.729b codec transmitted packet. The range is from 0 to 268435455. The default is 99.

Step 6. Enter the Encapsulated RTP Dynamic Payload Type in the EncapRTP Dynamic Payload field. The range is from 0 to 268435455. The default is 112.

Step 7. Enter the value which indicates the RTP-Start-Loopback in the RTP-Start-Loopback Dynamic field. In RTP-Start-Loopback, a network element blocks the media of the loopback-source until the loopback-mirror starts the transmission of the packet. The default is 113.

Step 8. Choose the appropriate RTP-Start-Loopback Codec to convert an analog voice signal to digital encoded voice signal from the RTP-Start-Loopback Codec drop-down list. The default is G711u.

• G711u — It is a Pulse Code Modulation (PCM) scheme. It uses mu-law codec which improves signal-to-noise-ratio without the requirement of more additional data. It is used in the United States and Japan.

• G711a — It is a Pulse Code Modulation (PCM) scheme. It uses A-law codec. It is used in most of the countries of the world.

• G726-32 — It is an Adaptive Different Pulse Code Modulation (ADPM) scheme. It uses both a-law and mu-law. It helps to reduce the bandwidth.

• G729a — It is an extension of G729 which uses Algebric Code Excited Linear Prediction (ACELP) to simplify the complexity and cut the high cost of G729. It requires less computational power than G729.

• G722 — It is a Sub-Band Adaptive Different Pulse Code Modulation (SB-ADPCM) scheme which provides 7kHz wide band audio data rates to improve the speech quality.

Step 9. Enter the name of the NSE codec in the NSE Codec Name field. The default is NSE.

Step 10. Enter the name of the Audio Video Transport (AVT) codec in the AVT Codec Name field. The default is telephone-event.

Step 11. Enter the name of the G711u codec in the G711u Codec Name field. It is a Pulse Code Modulation (PCM) scheme which uses mu-law codec to improve signal-to-noise-ratio without the requirement of more additional data. It is used in the United States and Japan. The default is Pulse Code Modulation mu-law (PCMU).

Step 12. Enter the name of the G711a codec in the G711a Codec Name field. It is a Pulse Code Modulation (PCM) scheme which uses A-law codec. It is used in most of the countries of the world. The default is Pulse Code Modulation A-law (PCMA).

Step 13. Enter the name of the G726r32 code in the G726r32 Codec Name field. It is a Adaptive Differential Pulse Code Modulation (ADPCM) scheme which uses 32 kbit per second. The default is G726-32.

Step 14. Enter the name of the G729a codec in the G729a Codec Name field. It is an extension of G729 which uses Algebric Code Excited Linear Prediction (ACELP) to simplify the complexity and cut the high cost of G729. It requires less computational power than G729. The default is G729a.

Step 15. Enter the name of the G729b codec in the G729b Codec Name field. It is an
extension of G729 to provide support to wideband speech and audio. The default is G729ab.

Step 16. Enter the name of the EncapRTP codec in the EncapRTP Codec name field. It is the encapsulated Real-Time Protocol name. The default is encaprtp.

Step 17. Click **Submit All Changes** to save the settings.

**NAT Support Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Handle VIA received</td>
<td>no</td>
</tr>
<tr>
<td>Insert VIA received</td>
<td>no</td>
</tr>
<tr>
<td>Substitute VIA Addr</td>
<td>no</td>
</tr>
<tr>
<td>STUN Enable</td>
<td>no</td>
</tr>
<tr>
<td>STUN Server</td>
<td></td>
</tr>
<tr>
<td>EXT RTP Port Min</td>
<td></td>
</tr>
<tr>
<td>Handle VIA rport</td>
<td>no</td>
</tr>
<tr>
<td>Insert VIA rport</td>
<td>no</td>
</tr>
<tr>
<td>Send Resp To Src Port</td>
<td>no</td>
</tr>
<tr>
<td>STUN Test Enable</td>
<td>no</td>
</tr>
<tr>
<td>EXT IP</td>
<td></td>
</tr>
<tr>
<td>NAT Keep Alive Intvl</td>
<td>15</td>
</tr>
</tbody>
</table>

Step 1. From the Handle VIA Received drop-down list choose **yes** to enable the adapter process the received parameter in the VIA header. If set to **no** then the parameter would be ignored. The default value is no.

Step 2. From the Handle VIA rport drop-down list choose **yes** to enable the adapter process the received parameter in the VIA header. If set to **no** then the parameter would be ignored. The default value is no.

Step 3. From the Insert VIA received drop-down list choose **yes** to enable the adapter insert the received parameter into the VIA header of SIP responses, if the received-from IP and VIA sent-by IP values differ. The default is no.

Step 4. From the Insert VIA rport drop-down list choose **yes** to enable the adapter insert the received parameter into the VIA header of SIP responses, if the received-from IP and VIA sent-by IP values differ. The default is no.

Step 5. From the Substitute VIA Addr drop-down list choose **yes** to make use of NAT-mapped IP port values in the VIA header. The default value is no.

Step 6. From Send Resp To Src Port drop-down list choose **yes**. This would send responses to the request source port instead of the VIA sent-by port. The default value is no.

Step 7. From the STUN Enable drop-down list choose **yes** to discover NAT mappings. The default is **no**.

Step 8. From the STUN Test Enable drop-down list choose **yes** to enable the STUN feature. If STUN Enable feature is enabled and a valid STUN server is available, the adapter could perform a NAT-type discovery operation when it would power on. It would contact the configured stun server and the result of the discovery would be reported in a warning header in all subsequent REGISTER requests. If the adapter would detect a symmetric NAT or a symmetric firewall, NAT mapping would be disabled. The default value of this field is no.

Step 9. Enter the IP Address or the Fully Qualified Domain Name of the STUN server in STUN Server field. This would help in NAT mapping discovery.

Step 10. In the EXT IP field, enter the External IP Address that would substitute the actual IP
address of the adapter in all outgoing SIP messages. The default value is 0.0.0.0. If no value were entered then no substitution would be performed.

Step 11. In EXT RTP Port Min, enter the external port mapping number of the RTP Port Min. The default value for this field is zero. If it were not zero, then the RTP port number in all outgoing SIP messages would be substituted for the corresponding port value in the external RTP port range.

Step 12. The value in NAT Keep Alive Intvl field is the interval between NAT-mapping keep alive messages. The default value is 15 seconds.

Step 13. Click **Submit All Changes** to save the settings.