Configuring SIP, SPCP, and NAT

The Cisco SPA IP phones use the following protocols:

- Session Initiation Protocol (SIP)—Cisco SPA300 Series, Cisco SPA500 Series, Cisco WIP310
- Cisco Smart Phone Control Protocol (SPCP)—Cisco SPA300 Series, Cisco SPA500 Series

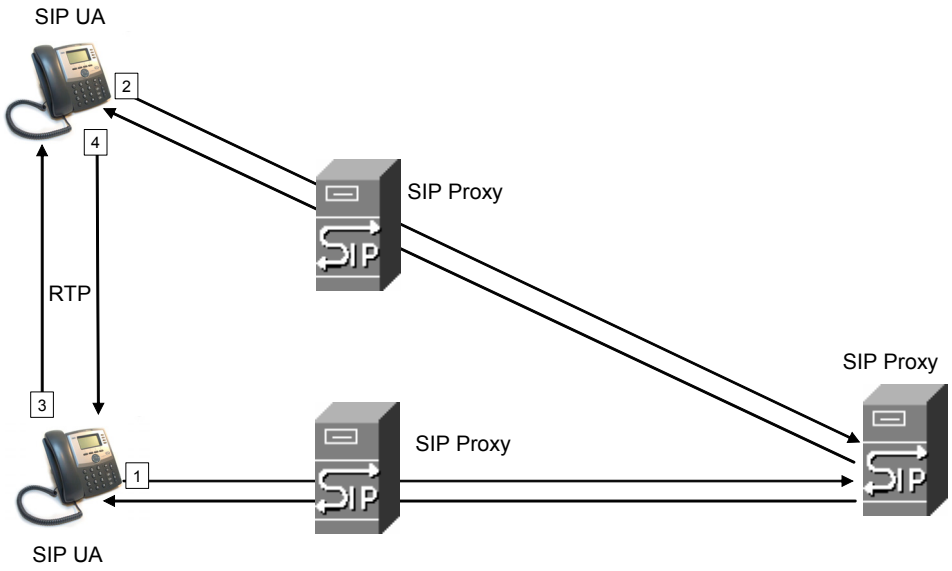
This chapter describes how to configure the phone protocols:

SIP and Cisco IP Phones

Cisco IP phones use Session Initiation Protocol (SIP), allowing interoperation with all IT service providers supporting SIP.

SIP handles signaling and session management within a packet telephony network. *Signaling* allows call information to be carried across network boundaries. *Session management* controls the attributes of an end-to-end call.

The diagram shows a SIP request for connection to another subscriber in the network.



In typical commercial IP telephony deployments, all calls go through a SIP proxy server. The requesting phone is called the SIP user agent server (UAS), while the receiving phone is called the user agent client (UAC).

SIP message routing is dynamic. If a SIP proxy receives a request from a UAS for a connection but cannot locate the UAC, the proxy forwards the message to another SIP proxy in the network. When the UAC is located, the response is routed back to the UAS, and a direct peer-to-peer session is established between the two UAs. Voice traffic is transmitted between UAs over dynamically-assigned ports using Real-time Protocol (RTP).

RTP transmits real-time data such as audio and video; it does not guarantee real-time delivery of data. RTP provides mechanisms for the sending and receiving applications to support streaming data. Typically, RTP runs on top of UDP. See NAT Mapping with STUN.

SIP Over TCP

To guarantee state-oriented communications, Cisco IP phones can use TCP as the transport protocol for SIP. This protocol provides *guaranteed delivery* that assures that lost packets are retransmitted. TCP also guarantees that the SIP packages are received in the same order that they were sent.

TCP overcomes the problem UDP ports have of being blocked by corporate firewalls. With TCP, new ports do not need to be opened or packets dropped, because TCP is already in use for basic activities, such as Internet browsing or e-commerce.

SIP Proxy Redundancy

An average SIP proxy server can handle tens of thousands of subscribers. A backup server allows an active server to be temporarily switched out for maintenance. Cisco phones support the use of backup SIP proxy servers to minimize or eliminate service disruption.

A static list of proxy servers is not always adequate. If your user agents are served by different domains, for example, you would not want to configure a static list of proxy servers for each domain into every Cisco IP phone.

A simple way to support proxy redundancy is to configure a SIP proxy server in the Cisco IP phone configuration profile. The DNS SRV records instruct the phones to contact a SIP proxy server in a domain named in SIP messages. The phone consults the DNS server. If configured, the DNS server returns an SRV record that contains a list of SIP proxy servers for the domain, with their host names, priority, listening ports, and so forth. The Cisco IP phone tries to contact the hosts in the order of their priority.

If the Cisco IP phone currently uses a lower-priority proxy server, the phone periodically probes the higher-priority proxy and switches to the higher-priority proxy when available.

Configuring Survivable Remote Site Telephony (SRST) Support

The *proxy* and *outbound proxy* fields in the **Ext** tab can be configured with an extension that includes a statically-configured DNS SRV record or DNS A record. This allows for failover and fallback functionality with a secondary proxy server. The format for the parameter value is:

```
FQDN format: hostname[:port][:SRV=host-list OR :A=ip-list]
host-list:  srv[|srv[|srv…]]
srv: hostname[:port][:p=priority][:w=weight][:A=ip-list]
ip-list: ip-addr[,ip-addr[,ip-addr…]]
```

The default priority is 0 and default weight is 1. The default port is 0, and the application substitutes the proper port value (for example, port 5060 for SIP).

Dual Registration

The phone always registers to both primary (or primary outbound) and alternate (or alternate outbound) proxies. After registration, the phone sends out Invite and Non-Invite SIP messages via primary proxy first. If there is no response for the new INVITE from the primary proxy, after timeout, the phone should attempt with the alternate proxy.

Dual registration is supported per line basis. Three new parameters are added which can be configured via Web GUI and remote provisioning:

- Alternate Proxy—Default is empty
- Alternate Outbound Proxy—Default is empty
- Dual Registration—Default is NO (turned off)

Upon configuring the parameters, reboot the phone for the feature to take effect.

Note The administrator should specify a value for primary proxy (or primary outbound proxy) and alternate proxy (or alternate outbound proxy) for the feature to function properly.

Limitations for Dual Registration and DNS SRV Redundancy

Beginning from this release (7.5.6) the limitations for Dual Registration and DNS SRV redundancy are as follows:

- When Dual Registration is enabled, DNS SRV Proxy Fallback/Recovery must be disabled.
- Do not use Dual Registration in conjunction with other Fallback/Recovery mechanisms. For example: Broadsoft mechanism.
- When Dual Registration is enabled, the parameter Auto Register when Failover must be disabled.

- There is no recovery mechanism for feature request. However, the administrator can adjust the re-registration time for a prompt update of the registration state for primary and alternate proxy.

Alternate Proxy and Dual Registration

When the parameter, Dual Register is set to no alternate proxy is ignored.

Register Upon Failover/Recovery

- Failover—SPA phone performs a failover to secondary proxy when the SIP request gets no response from primary proxy.
- Recovery—The phone attempts to re-register with the primary proxy while registered or actively connected to the secondary proxy.

Note In the 7.5.5 and early releases, to control the Re-registration upon failover or recovery, "BT" was set in the parameter <Try Backup RSC>. From 7.5.6, this is replaced with another new parameter <Auto Register When Failover>.

Old Behavior (7.5.5 and prior):

In the failover/recovery scenario, the phone remains registered to the primary proxy, but makes and receives calls on the alternate proxy. The SPA IP phone re-registers upon failover or recovery with "BT" configured in <Try Backup RSC> field under the "Response Status Code Handling" section of SIP tab.

Note The <Try Backup RSC> parameter is used to invoke failover upon receiving specified response codes.

New Behavior (7.5.6):

When the new parameter <Auto register when failover> is set to **yes**, the phone unregisters and registers like the previous behavior (when a special value "BT" is set in the parameter <Try Backup RSC>.

The solution is to remove the "BT" definition and add the new parameter, <Auto Register When Failover> to control the phone to auto-register to fail-over proxy when fail-over action is executed. After re-register successfully the INVITE message will be resend to new proxy

Fallback Behavior

When the parameter Auto Register When Failover is set to no, the fallback happens immediately and automatically. If the Proxy Fallback Intvl exceeds, all the new SIP messages go to primary proxy.

When the parameter, Auto Register When Failover is set to yes, the fallback happens only when current registration expires, which means only REGISTER message can trigger fallback.

For example, when the value for Register Expires is 3600 seconds and Proxy Fallback Intvl is 600 seconds, the fallback is triggered 3600 seconds later and not 600 seconds later.

When the value for Register Expires is 600 seconds and Proxy Fallback Intvl is 1000 seconds, the fallback is triggered at 1200 seconds.

After successfully registering back to primary server, all the SIP messages go to primary server.

RFC3311 Support

The Cisco SPA525G or Cisco SPA525G2 support RFC-3311, the SIP UPDATE Method.

Support for SIP NOTIFY XML-Service

The Cisco SPA300 Series and Cisco SPA500 Series IP phones support the SIP NOTIFY XML-Service event. On receipt of a SIP NOTIFY message with an XML-Service event, the IP phone challenges the NOTIFY with a 401 response if the message does not contain correct credentials. The client must be furnish the correct credentials using MD5 digest with the SIP account password for the corresponding line of the IP phone.

The body of the message can contain the XML event Message. For example:

```
<CiscoIPPhoneExecute>
  <ExecuteItem Priority="0" URL="http://xmlserver.com/event.xml"/>
</CiscoIPPhoneExecute>
```

Authentication:

```
challenge  = MD5( MD5(A1) ":" nonce ":" nc-value ":" cnonce ":" qop-value
":" MD5(A2) )
where A1 = username ":" realm ":" passwd
and A2 = Method ":" digest-uri
```

Configuring SIP

SIP settings for the Cisco SPA IP phones are configured for the phone in general and for individual extensions.

Configuring Basic SIP Parameters

To configure general SIP parameters, navigate to **Admin Login > advanced > Voice > SIP.** Under **SIP Parameters**, make these changes:

Parameter	Description
Max Forward	The number of proxies or gateways that can forward the request to the next downstream server. The Max-Forwards value is an integer in the range of 0 to 255 indicating the remaining number of times the request message is allowed to be forwarded. This count is decremented by each server that forwards the request. The initial value is 70.
Max Redirection	Number of times an invite can be redirected to avoid an infinite loop. The default is 5.
Max Auth	Maximum number of times (from 0 to 255) a request might be challenged. The default is 2.
SIP User Agent Name	User-Agent header used in outbound requests. The default is $VERSION. If empty, the header is not included. Macro expansion of $A to $D corresponding to GPP_A to GPP_D allowed.

Parameter	Description
SIP Server Name	Server header used in responses to inbound responses. The default is **$VERSION**.
SIP Reg User Agent Name	User-Agent name used in a REGISTER request. If not specified, the SIP User Agent Name is used for the REGISTER request.
SIP Accept Language	The preferred languages for reason phrases, session descriptions, or status responses carried as message bodies in the response. If blank, the header is not included and the server assumes that all languages are acceptable to the client. Defaults to blank.
DTMF Relay MIME Type	MIME Type used in a SIP INFO message to signal a DTMF event. This parameter must match that of the service provider. Defaults to application/dtmf-relay.
Hook Flash MIME Type	MIME Type used in a SIPINFO message to signal a hook flash event.
Remove Last Reg	If set to **yes**, removes the previous registration before re-registering (if the value is different). Defaults to no.
Use Compact Header	If set to **yes**, the Cisco IP phone uses compact SIP headers in outbound SIP messages. If inbound SIP requests contain normal (non-compact) headers, the phone substitutes incoming headers with compact headers. If set to **no**, Cisco SPA IP phones use normal SIP headers. If inbound SIP requests contain compact headers, the phones reuse the same compact headers when generating the response, regardless of this setting. Defaults to no.
Escape Display Name	If set to **yes**, encloses the configured Display Name string in a pair of double quotes for outbound SIP messages. Any occurrences of or \ in the string is escaped with \ and \\ inside the pair of double quotes. Defaults to yes.
SIP-B Enable	If set to **yes**, enables SIP for Business (supports Sylantro call flows) call features. See www.broadsoft.com for more information. Defaults to no.
Talk Package	If set to **yes**, enables support for the BroadSoft Talk Package that lets users answer or resume a call by clicking a button in an external application. Defaults to no.
Hold Package	If set to **yes**, enables support for the BroadSoft Hold Package, which lets users place a call on hold by clicking a button in an external application. Defaults to no.
Conference Package	If set to **yes**, enables support for the BroadSoft Conference Package that enables users to start a conference call by clicking a button in an external application. Defaults to no.
Notify Conference	If set to **yes**, Cisco SPA IP phones send out a NOTIFY with event=conference when starting a conference call (with the BroadSoft Conference Package). Defaults to no.

Parameter	Description
RFC 2543 Call Hold	If set to **yes**, Cisco SPA IP phones include Session Description Protocol (SDP) syntax c=0.0.0.0 when sending a SIP re-INVITE to a peer to hold the call. If set to no, Cisco SPA IP phones do not include the c=0.0.0.0 syntax in the SDP. With either setting, the phone includes a=sendonly syntax in the SDP. Defaults to yes.
Random REG CID On Reboot	If set to **yes**, Cisco SPA IP phones use a different random call-ID for registration after the next software reboot. If set to no, the phone tries to use the same call-ID for registration after the next software reboot. With either setting the phone uses a new random call-ID for registration after a power-cycle. Defaults to no. Not applicable to the Cisco WIP310.
Mark All AVT packets	If set to **yes**, all audio video transport (AVT) tone packets (encoded for redundancy) have the marker bit set. If set to no, only the first packet has the marker bit set for each DTMF event. Defaults to yes.
SIP TCP Port Min	Lowest TCP port number that can be used for SIP sessions. Defaults to 5060.
SIP TCP Port Max	Highest TCP port number that can be used for SIP sessions. Defaults to 5080.
Keep Referee When REFER Failed	When set to **yes**, the phone immediately handles NOTIFY sipfrag messages.
CTI Enable	If set to **yes**, enables the computer telephony integration (CTI), where a computer can act as a call center handling all sorts of incoming and outgoing communications., including phone calls, faxes, and text messages. The CTI interface allows a third-party application to control and monitor the state of a Cisco IP phone and, for example, initiate or answer a call by clicking a mouse on a PC, CTI must be enabled on the Cisco SPA300 Series or Cisco SPA500 Series IP phones for an attached Cisco Attendant Console to properly monitor the IP phone line status. Defaults to no.
Caller ID Header	Select from where the IP phone gets the caller ID: PAID-RPID-FROM P-ASSERTED-IDENTITY REMOTE-PARTY-ID FROM header Defaults to PAID-RPID-FROM. Not applicable to the Cisco WIP310.
SRTP Method	The method to use for Secure Real-time Transport Protocol (SRTP): x-sipura—legacy SRPT method s-descriptor—compliant with RFC-3711 and RFC-4568 The default value is **x-sipura**. Not applicable to Cisco WIP310.

Parameter	Description
Hold Target Before REFER	Controls whether to hold call leg with transfer target before sending REFER to the transferee when initiating a fully-attended call transfer (where the transfer target has answered). Default value is "no," where the call leg is not held. Not applicable to Cisco WIP310.
Dialog SDP Enable	When enabled and the Notify message body is too big causing fragmentation, the Notify message xml dialog is simplified; Session Description Protocol (SDP) is not included in the dialog xml content.
Display Diversion Info	Parses Diversion Header information in an incoming SIP Invite and displays it as the Caller ID.
Disable Local Name To Header	The options are No and Yes: • If No is selected, no changes are made. The default value is No. • If Yes is selected, the following happens: – Disables the display name in "Directory" and "Call History" in the "To" header during an outgoing call. – Ignores the CLID in the "UPDATE" message. – Redial list is populated based on 18x or 200 OK PAID header with or without Display Name. **Note** This field is supported in Firmware Release 7.6.2 and later.

Configuring SIP Timer Values

All SIP timer values are in seconds. To configure SIP timer values, navigate to **Admin Login > advanced > Voice > SIP.** Under **SIP Timer Values (sec)**, make these changes:

Parameter	Description
SIP T1	RFC-3261 T1 value (RTT estimate). Ranges from 0 to 64 seconds. Defaults to .5 seconds.
SIP T2	RFC-3261 T2 value, the maximum retransmit interval for non-INVITE requests and INVITE responses. Ranges from 0 to 64 seconds. Defaults to 4 seconds.
SIP T4	RFC-3261 T4 value, which is the maximum duration a message remains in the network. Ranges from 0 to 64 seconds. Defaults to 5 seconds.
SIP Timer B	RFC-3261 INVITE transaction time-out value. Ranges from 0 to 64 seconds. Defaults to 16 seconds.
SIP Timer F	RFC-3261 Non-INVITE transaction time-out value. Ranges from 0 to 64 seconds. Defaults to 16 seconds.
SIP Timer H	RFC-3261 INVITE final response time-out value for ACK receipt. Ranges from 0 to 64 seconds. Defaults to 16 seconds.
SIP Timer D	RFC-3261 wait time for response retransmits. Ranges from 0 to 64 seconds. Defaults to 16 seconds.

Parameter	Description
SIP Timer J	RFC-3261 Wait time for Non-INVITE request retransmits. Ranges from 0 to 64 seconds. Defaults to 16 seconds.
INVITE Expires	The length of time the INVITE is valid. If you enter 0, the Expires header is not included in the request. Ranges from 0 to 19999999999999999999999999999999. Defaults to 240 seconds.
ReINVITE Expires	ReINVITE request Expires header value. If you enter 0, the Expires header is not included in the request. Ranges from 0 to 19999999999999999999999999999999. Defaults to 30
Reg Min Expires	Minimum registration expiration time allowed from the proxy in the Expires header or as a Contact header parameter. If the proxy returns a value less than this setting, the smallest of the two values is used. Defaults to 1 second.
Reg Max Expires	Maximum registration expiration time allowed from the proxy in the Min-Expires header. If the value is greater than this setting, the largest of the two values is used. Defaults to 7200 seconds.
Reg Retry Intvl[1]	Interval to wait before the Cisco IP phone retries registration after failing during the previous registration. The range is from 1 to 268435455. Do not enter 0. Defaults to 30 seconds.
Reg Retry Long Intvl[1]	When registration fails with a SIP response code that does not match the Retry Reg response status code (RSC) value (see next table), the IP phone waits for this length of time before retrying. If this interval is 0, the Cisco IP phone stops trying. This value should be much larger than the Reg Retry Intvl value. The range is from 0 to 268435455. Defaults to 1200 seconds.
Reg Retry Random Delay	Random delay added to the Register Retry Intvl value when retrying REGISTER after a failure. Minimum and maximum random delay to be added to the short timer. The range is from 0 to 268435455. Defaults to 0, which disables this feature.
Reg Retry Long Random Delay	Random delay added to Register Retry Long Intvl value when retrying REGISTER after a failure. Minimum and maximum random delay to be added to the long timer. Random delay range (in seconds) to add to the Register Retry Long Intvl when retrying REGISTER after a failure. Defaults to 0, which disables this feature. Not applicable to Cisco WIP310.
Reg Retry Intvl Cap	Reg_Retry_Intvl_Cap—Maximum value of the exponential delay. The maximum value to cap the exponential backoff retry delay (which starts at the Register Retry Intvl and doubles every retry). Defaults to 0, which disables the exponential backoff (that is, the error retry interval is always at the Register Retry Intvl). When this feature is enabled, the Reg Retry Random Delay is added to the exponential backoff delay value. The range is from 0 to 268435455. Not applicable to Cisco WIP310.
Sub Min Expires	Lower limit of the REGISTER (subscribe) expires value returned from the proxy server. The range is from 0 to 268435455. Defaults to 10 seconds.

Parameter	Description
Sub Max Expires	Upper limit of the REGISTER (subscribe) min-expires value returned from the proxy server in the Min-Expires header. The range is from 0 to 268435455. Defaults to 7200 seconds.
Sub Retry Intvl	The retry interval when the last Subscribe request fails. The range is from 0 to 268435455. Defaults to 10 seconds.

1. Cisco IP phones can use a RETRY-AFTER value when it is received from a SIP proxy server that is too busy to process a request (503 Service Unavailable message). If the response message includes a RETRY-AFTER header, the phone waits for the specified length of time before to REGISTER again. If a RETRY-AFTER header is not present, the phone waits for the value specified in the Reg Retry Interval or the Reg Retry Long Interval.

Configuring Response Status Code Handling

To configure response status code handling , under **Response Status Code Handling** make these changes:

- **SIT1 through SIT4 RSC**—SIP response status code for the appropriate Special Information Tone (SIT). If you set the SIT1 RSC to 404, when the user makes a call and a failure code of 404 is returned, the SIT1 tone is played. The Reorder or Busy tone is played by default for all unsuccessful response status code for SIT 1 RSC through SIT 4 RSC. Defaults to blank.
- **Try Backup RSC**—SIP response code that retries a backup server for the current request. Defaults to blank.
- **Retry Reg RSC**—Interval the device waits before re-trying registration after a failed registration. Defaults to blank.

Configuring RTP Parameters

To configure Real-time Transport Protocol (RTP), navigate to **Admin Login > advanced > Voice > SIP.** Under **RTP Parameters**, configure these fields:

- **RTP Port Min**—Minimum port number for RTP transmission and reception. <RTP Port Min> and <RTP Port Max> defines a range that contains at least 10 even number ports (twice the number of lines); for example, 100–106. Defaults to 16384.
- **RTP Port Max**—Maximum port number for RTP transmission and reception. <RTP Port Min> and <RTP Port Max> should define a range that contains at least 10 even number ports (twice the number of lines); for example, 100–106. Defaults to 16482.
- **RTP Packet Size**—Packet size in seconds. The range is from 0.01 to 0.16. Valid values must be a multiple of 0.01 seconds. Defaults to 0.030.
- **Max RTP ICMP Err**—Number of successive ICMP errors allowed when transmitting RTP packets to the peer before the Cisco IP phone terminates the call. If the value is set to 0 (the default), the Cisco IP phone ignores the limit on ICMP errors, disabling the feature.
- **RTCP Tx Interval—**Interval for sending out Real-Time Transport Control Protocol (RTCP) sender reports on an active connection. During an active connection, the Cisco SPA IP phones send out compound RTCP packets. Each compound RTP packet, except the last one, contains a sender report (SR) and a source description (SDES). The last RTCP packet contains an additional BYE packet. Each SR, except the last one, contains one receiver report (RR); the last SR carries no RR.

  The SDES contains CNAME, NAME, and TOOL identifiers:

  - **CNAME**—*User ID@Proxy*
  - **NAME**—*Display Name* (or *Anonymous* if user blocks caller ID)
  - **TOOL**—Vendor/Hardware-platform-software-version (such as Cisco SPA9000-5.2.2(SCb)).

  The NTP timestamp used in the SR is a snapshot of the Cisco IP phone local time, not the time reported by an NTP server.

  If the Cisco IP phone receives a RR from a peer, it tries to compute the round trip delay and show it as the *Call Round Trip Delay* value in the Info section of the phone web user interface administration page. The range is from 0 to 255 seconds. Defaults to 0.

- **No UDP Checksum**—Select **yes** to enable the Cisco IP phone to calculate the UDP header checksum for SIP messages. Since this adds to the computation load, we recommend the default value, no (disabled).
- **Symmetric RTP**—Select **yes** to enable Symmetric RTP operation. When enabled, it sends RTP packets to the source address and the port of the last received valid inbound RTP packet. If disabled (or before the first RTP packet arrives) it sends RTP to the destination as indicated in the inbound SDP. Defaults to no.
- **Stats in BYE**—Select **yes** to send the P-RTP-Stat header in response to a BYE message. The header contains the RTP statistics on the current call. Defaults to no.

  The format of the P-RTP-Stat header is:

```
P-RTP-State: PS=<packets sent>,OS=<octets sent>,PR=<packets received>,OR=<octets
received>,PL=<packets lost>,JI=<jitter in ms>,LA=<delay in ms>,DU=<call duration
in s>,EN=<encoder>,DE=<decoder>
```

Configuring SDP Payload Types

Configured dynamic payloads are used for outbound calls only when the Cisco IP phone presents a Session Description Protocol (SDP) offer. For inbound calls with a SDP offer, the phone follows the caller's assigned dynamic payload type.

Cisco IP phones use the configured codec names in outbound SDP. For incoming SDP with standard payload types of 0-95, the Cisco IP phone ignores the codec names. For dynamic payload types, the Cisco IP phone identifies the codec by the configured codec names (comparison is case-sensitive).

To configure SDP payload types, navigate to **Admin Login > advanced > Voice > SIP.** Under **SDP Payload Types**, configure these parameters:

Parameter	Description
AVT Dynamic Payload	Any non-standard data. Both sender and receiver must agree on a number. Ranges from 96 to 127. Defaults to 101.
INFOREQ Dynamic Payload	Codec number used in the SIP messaging for the Dynamic Payload size mechanism. This number should match the number configured in the network/other party to enable the use of Dynamic Payload. The best range is 96 to 27 for any dynamic payload type. Defaults to blank.

Parameter	Description
G726r16 Dynamic Payload	RTP Payload Type Number that indicates the transmitted packet is using the G.726 codec. Other codecs have preassigned payload numbers that you do not have to be set, but G.726 does not.. Ranges from 96 to 127. Defaults to 98. Not applicable to Cisco SPA525G or Cisco SPA525G2.
G726r24 Dynamic Payload	RTP Payload Type Number that indicates the transmitted packet is using the G.726-24 codec. Ranges from 96 to 127. Defaults to 97. Not applicable to Cisco SPA525G or Cisco SPA525G2.
G726r32 Dynamic Payload	RTP Payload Type Number that indicates the transmitted packet is using the G726r32 codec. The range is from 0 to 268435455. Defaults to 2.
G726r40 Dynamic Payload	RTP Payload Type Number that indicates the transmitted packet is using the G.726-40 codec Ranges from 96 to 27. Defaults to 96. Not applicable to Cisco SPA525G or Cisco SPA525G2.
G729b Dynamic Payload	RTP Payload Type Number that indicates the transmitted packet is using the G729b codec. The range is from 0 to 268435455. Defaults to 99.
EncapRTP Dynamic Payload	EncapRTP Dynamic Payload type. The range is from 0 to 268435455. Defaults to 112.
RTP-Start-Loopback Dynamic	RTP-Start-Loopback Dynamic Payload. Defaults to 113.
RTP-Start-Loopback Codec	RTP-Start-Loopback codec. Select one of following: G711u, G711a, G726-16, G726-24, G726-32, G726-40, G729a, or G723. Defaults to G711u.
AVT Codec Name	AVT codec name used in SDP. Defaults to `telephone-event`.
G711u Codec Name	G.711u codec name used in SDP. Defaults to Pulse Code Modulation mu-law (PCMU).
G711a Codec Name	G.711a codec name used in SDP. Defaults to Pulse Code Modulation A-Law (PCMA).
G726r16 Codec Name	G.726-16 codec name used in SDP. Defaults to G726-16. Not applicable to Cisco SPA525G or Cisco SPA525G2.
G726r24 Codec Name	G.726-24 codec name used in SDP. Defaults to G726-24. Not applicable to Cisco SPA525G or Cisco SPA525G2.
G726r32 Codec Name	G.726-32 codec name used in SDP. Defaults to G726-32.
G726r40 Codec Name	G.726-40 codec name used in SDP. Defaults to G726-40. Not applicable to Cisco SPA525G or Cisco SPA525G2.
G729a Codec Name	G.729a codec name used in SDP. Defaults to G729a.
G729b Codec Name	G.729b codec name used in SDP. Defaults to G729ab.

Parameter	Description
G723 Codec Name	G.723 codec name used in SDP. Defaults to G723. Not applicable to the Cisco WIP310, Cisco SPA525G or Cisco SPA525G2.
EncapRTP Codec Name	EncapRTP codec name used in SDP. Defaults to encaprtp.

Configuring SIP Settings for Extensions

To configure the network settings for SIP extensions, navigate to **Admin Login > advanced > Voice > Ext_n.** Under **Network Settings**, configure the following fields:

Parameter	Description
SIP ToS/DiffServ Value	Time of service (ToS)/differentiated services (DiffServ) field value in UDP IP packets carrying a SIP message. Defaults to 0x68.
SIP CoS Value [0-7]	Class of service (CoS) value for SIP messages. Ranges from 0 to 7. Defaults to 3.
RTP ToS/DiffServ Value	ToS/DiffServ field value in UDP IP packets carrying RTP data. Defaults to 0xb8.
RTP CoS Value [0-7]	CoS value for RTP data. Ranges from 0 to 7. Defaults to 6.
Network Jitter Level	The jitter buffer size as it is adjusted by a device. Jitter buffer size is adjusted dynamically. The minimum jitter buffer size is 30 milliseconds or (10 milliseconds plus the current RTP frame size), whichever is larger, for all jitter level settings. However, the starting jitter buffer size value is larger for higher jitter levels. This setting controls the rate at which the jitter buffer size is adjusted to reach the minimum milliseconds. Select: **low (30 ms)**, **medium (40 ms)**, **high (60 ms)**, **very high** (80 ms), or **extremely high (180 ms)**. Defaults to high.
Jitter Buffer Adjustment	How the jitter buffer is adjusted. Select: **up and down**, **up only**, **down only**, or **disable**. Defaults to up and down.

To configure SIP settings, navigate to **Admin Login > advanced > Voice > Ext_n.** Under **SIP Settings**, configure the following fields:

Parameter	Description
SIP Transport	Select from **UDP**, **TCP** or **TLS**. Defaults to UDP.
SIP Port	Port number of the SIP message listening and transmission port. Defaults to 5060.
SIP 100REL Enable	Support of 100REL SIP extension for reliable transmission of provisional responses (18x) and use of PRACK requests. Select **yes** to enable. Otherwise, select **no**. Defaults to no.
EXT SIP Port	The external SIP port number substituted for the actual SIP port in all outgoing SIP messages. If 0 is specified, no SIP port substitution is performed. Defaults to blank. The range is from 0 to 65535.

Parameter	Description
Auth Resync-Reboot	The Cisco IP phone authenticates the sender when it receives a NOTIFY message with the following requests: resync reboot report restart XML-service Select **yes** to enable. Otherwise, select **no**. Defaults to yes.
SIP Proxy-Require	SIP proxy for each extension or behavior when an extension sees this header from the user agent. If this field is configured and the proxy does not support it, it responds with the message, unsupported. Enter the appropriate header in the field provided. For example, `com.nortel.networks.firewall`.
SIP Remote-Party-ID	The Remote-Party-ID header to use instead of the From header. Select **yes** to enable. Otherwise, select **no**. Defaults to yes.
Referor Bye Delay	Time when the Cisco IP phone sends BYE to terminate stale call legs upon completion of call transfers. Multiple delay settings (Referor, Refer Target, Referee, and Refer-To Target). Enter the appropriate period of time in seconds. Defaults to 4.
Refer-To Target Contact	Indicates the refer-to target. Select **yes** to send the **SIP Refer** to the contact. Otherwise, select **no**. Defaults to no.
Referee Bye Delay	Delay time for the Referee Bye Delay. Enter the appropriate period of time in seconds. Defaults to 0.

Parameter	Description
SIP Debug Option	How SIP messages are received at or sent from the proxy listen port to the log. Select: • none—No logging. • 1-line—Logs the start-line only for all messages. • 1-line excl. OPT—Logs the start-line only for all messages except OPTIONS requests/responses. • 1-line excl. NTFY—Logs the start-line only for all messages except NOTIFY requests/responses. • 1-line excl. REG—Logs the start-line only for all messages except REGISTER requests/responses. • 1-line excl. OPT|NTFY|REG—Logs the start-line only for all messages except OPTIONS, NOTIFY, and REGISTER requests/responses. • full—Logs all SIP messages in full text. • full excl. OPT—Logs all SIP messages in full text except OPTIONS requests/responses. • full excl. NTFY—Logs all SIP messages in full text except NOTIFY requests/responses. • full excl. REG—Logs all SIP messages in full text except REGISTER requests/responses. • full excl. OPT|NTFY|REG—Logs all SIP messages in full text except for OPTIONS, NOTIFY, and REGISTER requests/responses. Defaults to none.
Refer Target Bye Delay	Delay time for the Refer Target Bye Delay. Enter the appropriate period of time in seconds. Defaults to 0.
Sticky 183	When enabled, the IP telephony ignores further 180 SIP responses after receiving the first 183 SIP response for an outbound INVITE. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to no.
Auth INVITE	When enabled, authorization is required for initial incoming INVITE requests from the SIP proxy. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to no. Not applicable to the Cisco WIP310.
Ntfy Refer On 1xx-To-Inv	When enabled as a transferee, the phone sends a NOTIFY with Event:Refer to the transferor for any 1xx response returned by the transfer target, on the transfer call leg. To enable this feature, select **yes**. If set to **no**, the phone only sends a NOTIFY for final responses (200 and higher). Not applicable to the Cisco WIP310.

Parameter	Description
Use Anonymous with RPID	When enabled and the caller blocks his caller-id, the FROM header display-name and user-id fields are set to **anonymous**. This parameter applies only if <SIP Remote-Party-ID> is set to yes; otherwise, it is ignored. When disabled, the FROM header display-name and user-id are not masked. The Remote-Party-ID header indicates privacy=full when the caller tries to block his caller-id. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to yes. Not applicable to the Cisco WIP310.
Set G729 annexb	G.729 Annex B (G.729b) that provides silence compression by enabling a voice activity detection (VAD) module. It uses 2-byte Silence Insertion Descriptor (SID) frames transmitted to initiate comfort noise generation (CNG). If transmission is stopped and the link goes quiet because of there is no speech transmitted, the receiving side might assume that the link has been cut. By inserting comfort noise, analog hiss is simulated digitally during the silence to assure the receiver that the link is active and operational. **none**—do not enable. **no**—turn on but do not silence the VAD. **yes**—enable. Not applicable to the Cisco SPA525G or Cisco SPA525G2.

Parameter	Description

Voice Quality Report Address	The name of the collector that collects the statistics from SIP PUBLISH events. For example, **collector@*fully-qualified-domain-name*** (collector@reports.cisco.com) or ***collector@IP-address*** (collector@192.168.5.1). The SIP event package, SIP PUBLISH, enables the collection and reporting of metrics that measure the quality for VoIP sessions. Voice call quality information derived from RTCP-XR and call information from SIP is conveyed from a User Agent in a session to the third party in SIP PUBLISH method.
	
	RTCP-XR must be configured first (see Configuring RTP Parameters). After RTCP-XR is enabled, the call status information is updated on the **Voice > Info** page during an active call. Additionally, RTCP-XR packets containing a voice metrics block report are sent with the interval specified in the RTCP Tx Interval. When the call session is ended, a SIP PUBLISH with voice metrics info is sent to the collector endpoint.
	
	This parameter supports a full SIP URI. Examples of valid addresses:
	• collector@domain.com
	• 123.collect@123.123.123.123:5555
	• 5678@domain.com:5656
	
	For example if extension 1 was configured by using the phone profile:
	`<Voice_Quality_Report_Address_1_ ua="na">`
	`collector@domain.com`
	`</Voice_Quality_Report_Address_1_>`
	
	or
	
	`<Voice_Quality_Report_Address_1_ ua="na">`
	`123.collect@123.123.123.123:5555`
	`</Voice_Quality_Report_Address_1_>`
	
	or
	
	`<Voice_Quality_Report_Address_1_ ua="na">`
	`5678@domain.com:5656`
	`</Voice_Quality_Report_Address_1_>`

Configuring a SIP Proxy Server

To configure SIP proxy and registration parameters:

Step 1 Navigate to **Admin Login > advanced > Voice > Ext_n.**

Step 2 Under **Proxy and Registration**, configure the following fields:

Parameter	Description
Proxy	SIP proxy server and port number set by the service provider for all outbound requests. For example: 192.168.2.100:6060. The port number is optional. The default is port 5060.

Use Outbound Proxy	The outbound proxy (for example, 172.20.2.1:5060—port is optional) or a domain name, such as *sip.server.com*, as long as this name is a fully-qualified domain name. When set to **no**, the **Outbound Proxy** and **Use OB Proxy in Dialog** parameters are ignored. Defaults to no.
	Optionally, the proxy can be configured (Cisco SPA300 or Cisco SPA500 Series only) for Survivable Remote Site Telephony (SRST) support. The proxy is configured with an extension that includes a statically-configured DNS SRV record or DNS A record. Configuring the proxy allows for failover and fallback functionality with a secondary proxy server. For example:
	For SRV Record:
	`sip.server.com:SRV=node1.sip.server.com:5060:p=1:w=50|node2.sip.server.com:5060:p=2:w=50`
	For A Record:
	`sip.server.com:A=172.20.2.1,172.20.2.2`
	In both examples **Use DNS SRV** to **no** and **DNS SRV Auto Prefix** are set to **no**.

Outbound Proxy	All outbound requests are sent as the first hop. Enter an IP address or domain name.
Use OB Proxy In Dialog	SIP requests are sent to the outbound proxy within a dialog. This field is ignored if **Use Outbound Proxy** is set to **no**, or **Outbound Proxy** is blank. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to yes.
Register	Enables periodic registration with the proxy. This parameter is ignored if a proxy is not specified. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to yes.
Make Call Without Reg	Enables making outbound calls without successful (dynamic) registration by the phone. If set to no, the dial tone plays only when registration is successful. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to no.
Register Expires	Defines how often the phone renews registration with the proxy. If the proxy responds to a REGISTER with a lower expires value, the phone renews registration based on that lower value instead of the configured value. If registration fails with an “Expires too brief” error response, the phone retries with the value specified in the Min-Expires header of the error. The range is from 0 to 268435455. Defaults to 3600 seconds.

Parameter	Description
Ans Call Without Reg	The user does not have to be registered with the proxy to answer calls. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to no.
Use DNS SRV	Enables DNS SRV lookup for the proxy and outbound proxy. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to no.
DNS SRV Auto Prefix	The phone automatically prepends the proxy or outbound proxy name with _sip._udp when performing a DNS SRV lookup on that name. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to no.
Proxy Fallback Intvl	Sets the delay after which the phone retries from the highest priority proxy (or outbound proxy) after it has failed over to a lower priority server. The phone should have the primary and backup proxy server list from a DNS SRV record lookup on the server name. It needs to know the proxy priority; otherwise, it does not retry. The range is from 0 to 65535. Defaults to 3600 seconds.
Proxy Redundancy Method	The phone creates an internal list of proxies returned in the DNS SRV records. Select **Normal** to create a list that contains proxies ranked by weight and priority. Select **Based on SRV** and the phone creates a Normal list, then inspects the port numbers based on the first-listed proxy port. When the weight and priority match, the device selects the first port in the list. Defaults to Normal.

Step 3 Click **Submit All Changes**.

Configuring Subscriber Information Parameters

To configure subscriber information parameters for each extension, navigate to **Admin Login > advanced > Voice > Ext_n.** Under **Subscriber Information**, configure the following fields:

Parameter	Description
Display Name	Name displayed as the caller ID.
User ID	Extension number for this line.
Password	Password for this line. Defaults to blank (no password required).
Use Auth ID	Enables the authentication ID and password for SIP authentication. To enable this feature, select **yes**. Otherwise, select **no**. Defaults to no.
Auth ID	Authentication ID for SIP authentication. Defaults to blank.
Mini Certificate	Base64 encoding of a mini-certificate concatenated with the 1024-bit public key of the certificate authority (CA) signing the mini-certificate of all subscribers in the group. Defaults to blank.

Parameter	Description
SRTP Private Key	Base64 encoding of the 512-bit private key per subscriber for establishment of a secure call. Defaults to blank.
Reversed Authentication Realm	The IP address for an authentication realm other than the proxy IP address. The default value is blank; the proxy IP address is used as the authentication realm. The parameter for extension 1 appears as follows in the phone configuration file: <Reversed_Auth_Realm_1_ ua="na"> </Reversed_Auth_Realm_1_>

Configuring the IP Phone Communications Protocol

By default, the phone automatically detects the protocol and the Unified Communications device.

Cisco SPA500 Series IP Phones can be used as part of a Cisco Unified Communications System that uses Smart Phone Control Protocol (SPCP), also known as Skinny Call Control Protocol (SCCP), to manage a voice network. Or the phones can be configured to use Session Initiation Protocol (SIP), an IETF-defined signaling protocol that controls voice communication sessions in an IP network.

Configuring the Protocol on a Cisco SPA525G or Cisco SPA525G2

To configure the protocol on the Cisco SPA525G or Cisco SPA525G2, navigate to **Admin Login > advanced > Voice > System.** Under **System Configuration** in the **SPA525-protocol** field, choose **SCCP or SIP**.

To configure the phone to automatically detect the protocol being used on the network that it is connected to, in the **SPA525-auto-detect-sccp** field, choose **yes**.

Configuring the Protocol on a Cisco SPA300 Series or Cisco SPA500 Series IP Phone

To configure the protocol on a Cisco SPA300 Series or Cisco SPA500 Series IP phone, navigate to **Admin Login > advanced > Voice > System.** Under **System Configuration** in the **Signaling Protocol** field, choose **SCCP or SIP**.

To configure the phone to automatically detect the protocol being used on the network that it is connected to, in the **SPCP Auto-detect** field, choose **yes**. The phone defaults to SIP unless it detects a Cisco Unified Communications device. When set to no, the phone uses the protocol set in the **Signaling Protocol** field.

The Cisco SPA301 or the Cisco SPA501G can be configured by using the IVR. See Using IVR on IP Phones Without Screens for more information.

Managing NAT Transversal with Cisco IP Phones

Network Address Translation (NAT) allows multiple devices to share a single, public, routable, IP address to establish connections over the Internet. NAT is present in many broadband access devices to translate public and private IP addresses. For VoIP to co-exist with NAT, NAT traversal is required.

Not all service providers provide NAT traversal. If your service provider does not provide NAT traversal, you have several options:

- NAT Mapping with Session Border Controller
- NAT Mapping with SIP-ALG Router
- NAT Mapping with a Static IP Address
- NAT Mapping with STUN

NAT Mapping with Session Border Controller

We recommend that you choose an service provider that supports NAT mapping through a Session Border Controller. With NAT mapping provided by the service provider, you have more choices in selecting a router.

NAT Mapping with SIP-ALG Router

NAT mapping can be achieved by using a router that has a SIP Application Layer Gateway (ALG). By using a SIP-ALG router, you have more choices in selecting an service provider.

NAT Mapping with a Static IP Address

You can configure NAT mapping on the phone to ensure interoperability with the service provider.

- You must have an external (public) IP address that is static.
- The NAT mechanism used in the router must be symmetric. See Determining Whether the Router Uses Symmetric or Asymmetric NAT.

Use NAT mapping only if the service provider network does not provide a Session Border Controller functionality. To configure NAT mapping on the phone:

Step 1 Click **Voice > SIP** and navigate to **NAT Support Parameters**.

Step 2 Set the following parameters to **yes**:

- **Handle VIA received**
- **Insert VIA received**,
- **Substitute VIA Addr**
- **Handle VIA rport**
- **Insert VIA rport**
- **Send Resp To Src Port**

Step 3 Enter the public IP address for your router **EXT IP** field.

Step 4 Click the **Ext_n** tab and navigate to **NAT Settings**.

Step 5 Set **NAT Mapping Enable** to **yes**.

Step 6 (Optional) Set **NAT Keep Alive Enable** to **yes**.

The service provider might require the phone to send NAT keep alive messages to keep the NAT ports open. Check with your service provider to determine the requirements.

Step 7 Click **Submit All Changes**.

Step 8 Configure the firewall settings on your router to allow SIP traffic. See Configuring SIP.

NAT Mapping with STUN

If the service provider network does not provide a Session Border Controller functionality and if the other requirements are met, it is possible to use Session Traversal Utilities for NAT (STUN) to discover the NAT mapping. The STUN protocol allows applications operating behind a network address translator (NAT) to discover the presence of the network address translator and to obtain the mapped (public) IP address (NAT addresses) and the port number that the NAT has allocated for the User Datagram Protocol (UDP) connections to remote hosts. The protocol requires assistance from a third-party network server (STUN server) located on the opposing (public) side of the NAT, usually the public Internet. This option is considered a last resort and should be used only if the other methods are not available. To use STUN

- The router must use asymmetric NAT. See Determining Whether the Router Uses Symmetric or Asymmetric NAT.
- A computer running STUN server software is available on the network. You can also use a public STUN server or set up your own STUN server.

Step 1 Click **Voice > SIP** and navigate to **NAT Support Parameters**.

Step 2 Set the following parameters to **yes**:

- **Handle VIA received**
- **Insert VIA received**,
- **Substitute VIA Addr**
- **Handle VIA rport**
- **Insert VIA rport**
- **Send Resp To Src Port**
- **STUN Enable**

Step 3 Enter the IP address for your STUN server in the **STUN Server** field.

Step 4 Click **Ext_n.**

Step 5 Set **NAT Mapping Enable** to **yes**.

Step 6 (Optional) Set **NAT Keep Alive Enable** to **yes**.

The service provider might require the phone to send NAT keep alive messages to keep the NAT ports open. Check with your service provider to determine the requirements.

Step 7 Click **Submit All Changes**.

Step 8 Configure the firewall settings on your router to allow SIP traffic. See Configuring SIP.

Determining Whether the Router Uses Symmetric or Asymmetric NAT

STUN does not work on routers with symmetric NAT. With symmetric NAT, IP addresses are mapped from one internal IP address and port to one external, routable destination IP address and port. If another packet is sent from the same source IP address and port to a different destination, a different IP address and port number combination is used. This method is restrictive because an external host can send a packet to a particular port on the internal host *only if* the internal host first sent a packet from that port to the external host.

This procedure assumes that a syslog server is configured and is ready to receive syslog messages.

To Determine Whether the Router Uses Symmetric or Asymmetric NAT:

Step 1 Verify that the firewall is not running on your PC. (It can block the syslog port.) By default, the syslog port is 514.)

Step 2 Click **Voice > System** and navigate to **Optional Network Configuration**.

Step 3 Enter the IP address for the **Debug Server** and port number of your syslog server, if the port number is anything other than the default, 514. It is not necessary to include the port number if it is the default.

The address and port number must be reachable from the Cisco IP phone. The port number appears on the output log file name. The default output file is `syslog.514.log` (if port number was not specified).

Step 4 Set the **Debug Level** to **3.**

Step 5 To capture SIP signaling messages, click the **Ext** tab and navigate to SIP Settings. Set the **SIP Debug Option** to **Full**.

Step 6 To collect information about what type of NAT your router uses click the **SIP** tab and navigate to NAT Support Parameters.

Step 7 Click **Voice > SIP** and navigate to NAT Support Parameters.

Step 8 Set **STUN Test Enable** to **yes**.

Step 9 Determine the type of NAT by viewing the debug messages in the log file. If the messages indicate that the device is using symmetric NAT, you cannot use STUN.

Step 10 Click **Submit All Changes**.