CHAPTER 20

H.323 Support

In addition to Session Initiation Protocol (SIP), the Session Border Controller (SBC) now supports H.323, enabling multimedia products and applications from multiple vendors to interoperate, and allowing users to communicate without concern for compatibility.

H.323 is the international standard for multimedia communication over packet-switched networks, including local area networks (LANs), wide area networks (WANs), and the Internet. It was first defined by the International Communications Union (ITU) in 1996. The most recent version is H.323 version 5 (2003).

Note For ACE SBC Release 3.0.00 and later, this feature is supported in the unified model only.

Caution In progress H.323 calls will be disconnected during an SBC switchover from one service card to a standby card.

Feature History for H.323 Support

Release	Modification
ACE SBC Release 3.1.00	Added support for H.323 performance improvement.
ACE SBC Release 3.0.00	This feature was introduced on the Cisco 7600 series router along with support for the SBC unified model.

Contents

This module contains the following sections:

Prerequisites for H.323 Support

This feature requires basic understanding of H.323-related ITU standards, gatekeepers, and gateways. Gateways are responsible for edge routing decisions between the Public Switched Telephone Network (PSTN) and the H.323 network. Gatekeepers are used to group gateways into logical zones and perform call routing between them.

Restrictions for H.323 Support

The restrictions for H.323 support are listed per feature in this chapter and other H.323-related chapters in the guide.

Information About H.323 Support

H.323 is a suite of protocols and documents that includes the ITU-T standards H.323, H.225.0, H.245, the H.450-series, and the H.460-series. It supports T.120 for data collaboration and file transfer. Not all components of H.323 are mandatory as part of a standard H.323 system. For example, H.460.2, which describes number portability, is generally not used in enterprise video conferencing systems.

H.323 is used in Voice over Internet Protocol (VoIP), and IP-based video conferencing and serves a similar purpose to that of the Session Initiation Protocol (SIP). It was designed from the outset to operate over IP networks, primarily, though H.323 may also operate over other packet-switched networks. H.323 was designed with multipoint voice and video conferencing capabilities, though most users do not take advantage of the multipoint capabilities specified in the protocol.

H.323 is more mature than SIP, but lacks the flexibility of SIP. SIP is currently less defined, but has greater scalability which could ease the Internet application integration. Like SIP, H.323 is one of the world market leaders for transporting voice and video over networks around the world, with billions of minutes of voice traffic every month. The SBC supports both SIP and H.323, enabling multimedia products and applications from multiple vendors to interoperate, and allowing users to communicate without concern for compatibility.

The following supported H.323 features are documented separately in this guide or represent part of standard Q.931/H.225 protocols:

- H.323/SIP Interworking—Interworking of a defined subset of SIP/H.323 call and media signaling.
- Domain name server (DNS) configuration of signaling peer—This feature enables you to use the domain name instead of the IP address in an adjacency-signal-peer configuration.
- Hunting—Enables the SBC to hunt for other routes or destination adjacencies in case of a failure. Hunting means the route is retried.
- Basic conferencing passthrough (this feature is part of Q.931/H.225 passthrough)—Passthrough of conferenceID and conferenceGoal. Conference is controlled by the third party equipment, such as call manager. The SBC enables the conference to pass through all the conference-related information.
- H.450 passthrough (this feature is part of Q.931/H.225 passthrough)—Passthrough of H.450 elements between call legs.

The following supported H.323 features are documented in this chapter:

- Separate H.245 Control Channel

- H.245 Passthrough
- Slow Start Media Relay
- Codec Mappings
- DTMF Interworking
- Transcoding
- RAS Tech Prefix
- User Protocol Timer Control
- T.38 Fax Relay
- Q.931/H.225 Passthrough
- H.323 Privacy

Separate H.245 Control Channel

The H.323 procedures require that the SBC sets up a separate H.245 control channel over TCP. This feature complements tunneled H.245 support, enabling the user to control whether to use tunneling or not.

The new feature enables the SBC to carry out an H.323-H.323 call, where two call legs can negotiate different H.245 transport mechanisms. Each call leg decides independently whether to use a separate H.245 control channel.

The SBC sets up separate H.245 control channels only when required in one of the following cases:

- The SBC has received a startH245 Facility
- The SBC needs to send out an H.245 message and tunneling is not available

The SBC never requests separate H.245 control channel while tunneling is available unless the "disable tunneling" command line interface (CLI) command is set (see "Configuring Separate H.245 Control Channel" section on page 20-17). The SBC does not connect to an H.245 address simply because the peer offered an h245Address.

The SBC does not offer an H.245 address until it needs to, performing the following:

- Where possible, the SBC connects to the peer instead.
- Where impossible, the SBC offers its own H.245 address in a startH245 Facility and waits for 10 seconds for the peer to connect. This timeout is not configurable.

Since H.323 v2 onwards has support for Facility reason startH245, support for this feature is assumed in all peer devices. If the peer requires an H.245 connection and one does not exist, the partner must use a startH245 Facility to induce the SBC to connect to it.

If there is no H.245 transport possible (tunneled or separate), and H.245 messages must be sent by the SBC, then the call is terminated.

On receipt of provisionalRespToH245Tunnelling, the SBC waits to determine the final tunneling outcome before attempting separate H.245. H.245 messages are queued at this point and sent as soon as an H.245 transport becomes available.

In the event of an H.245 connection race, the SBC only disconnects if it looses. The partner must disconnect if it loses. Races are resolved by comparing the listen address/port (not the connection address/port).

Back-pressure is exerted at call scope, or connection scope when multiple calls share a connection. So, if call leg B cannot forward H.245 messages for some reason, call leg A's connection may exert TCP back pressure on the peer. If call leg A is doing H.245 tunneling, and sharing a Q.931 TCP connection with other calls, then the peer will experience back pressure on the other calls too.

The SBC tears down separate H.245 connections at the same point as their call by closing the relevant socket.

Restrictions for Separate H.245 Control Channel

The restrictions for the H.245 control channel are:

- The SBC does not support a model, in which it induces the peers in an H.323-H.323 call to set up the H.245 TCP connection directly between themselves or to the data border element (DBE).
- No show command is provided to list the H.245 transport status on a per-adjacency or per-call basis.
- The H.245 security is not supported.

H.245 Passthrough

In media bypass, H.245 content is passed unmodified between two H.323 call legs (for more information about media bypass see section "How Adjacencies Affect Media Routing" in the Implementing SBC Adjacencies chapter). Passthrough happens irrespective of whether an H.245 message is received over tunneled H.245 transport or a separate H.245 control channel, and does not require that both H.323 call legs use the same H.245 transport mechanism. This feature permits inserting an SBC between two H.323 devices without any change to the passing H.245 content.

This is achieved by passing through H.245 messages opaquely between the endpoints. The Fast Start request and response is passed through in the same way as mainline H.245. The only messages inspected by the SBC are fast start and logical channel signaling. These are used to derive the bandwidth used for the call.

Restrictions for H.245 Passthrough

The restrictions for the H.245 passthrough are:

- Configuration to block passthrough of certain messages or message elements is not included in this feature and is covered separately.
- In a media bypass call, no Session Description Protocol (SDP) appears in the billing records.
- The SBC does not support rate limiting of passed-through H.245 traffic, other than generic rate limiting of all signaling traffic.

Slow Start Media Relay

The SBC supports media relay (which is media pass through the DBE) of unidirectional H.245 channels. H.245 codec types are converted to Session Description Protocol (SDP) for the purposes of the DBE programming, transcoder programming, and billing. This is done using a codec mapping table (see "T.38 Fax Relay" section on page 20-9). When dealing with codec types, for which no SDP mapping exists, the SBE makes a best-effort attempt, and tries to find the best possible SDP match.

Inserting an SBC between two H.323 devices does not impact H.245 function (see "H.245 Passthrough" section on page 20-4). For example, the SBC does not modify the logical channel numbers of H.245 channels in a media relay call. In a distributed DBE model, H.248 signals are used to establish the necessary media terminations on the DBE.

The SBC supports renegotiation of media, using H.245 procedures, such as:

- Fax upspeed: Where endpoints switch over from a low-bit-rate audio codec to ITU-T G.711
- TCS=0: Where one endpoint induces the other to temporarily close all of its channels

Switchover to T.38 fax is described below in "T.38 Fax Relay" section on page 20-9.

Restrictions for Slow Start Media Relay

The restrictions for slow start media relay are:

- The SBC does not support bidirectional H.245 channels in fast start or Open Logical Channel Close (OLCs).
- Dual tone multifrequency (DTMF) interworking is not supported between different types of UserInputIndication.
- No user configuration is provided to control DTMF interworking, which is triggered solely by capability negotiation.
- No means are provided to block setup of a particular codec, nor to ignore an unknown codec. The best-effort function mentioned above is always enabled.
- The SBC does not support multipoint capabilities.

Codec Mappings

The following codec mappings (Table 20-1) are used by the SBC to represent H.245 codecs as SDP for the purpose of:

- Billing records (media relay only)
- DBE programming (media relay only)
- Bandwidth allocation (media relay and media bypass). The bandwidth here is calculated based on the SDP, not directly from the H.245.

Table 20-1 Codec Mappings

H.245 codec	appears as:
g711Alaw64k	PCMA/8000
g711Ulaw64k	PCMU/8000
g722_64k	G722/8000
g7231	G723.1/80
g728	G728/8000
g729	G729/8000
g729AnnexA	G729/8000
g729wAnnexB	G729/8000

Table 20-1 Codec Mappings

H.245 codec	appears as:
g729AnnexAwAnnexB	G729/8000
gsmHalfRate	GSM-HR/8000
gsmFullRate	GSM/8000
All other audio codecs	PCMU/8000 (the default codec)
T.38	See "T.38 Fax Relay"

Note the following:

- H.245 video and data codecs other than T.38 are not supported by the SBC either for media relay or media bypass.
- The subset of codecs supported for H.323/SIP interworking is much smaller (for more information see the H.323-SIP Interworking chapter)

DTMF Interworking

Dual-tone multi-frequency (DTMF) tones are used to transfer user requests. Different systems may support different forms of DTMF. The SBC enables the DTMF interworking between these systems.

For example, some nonstandard H.323 devices do not support the lowest common denominator of alphanumeric UserInputIndication. Such devices can only signal DTMF through RFC2833 telephony events or as in-band media data. Other devices support UserInputIndication but not the RFC2833 telephony event.

If two such devices are deployed back to back, their only option is to send DTMF tones as it is done in-band media data. Deploying an SBC between them allows each side to send DTMF, using its supported signaled method, UserInputIndication on one side and RFC2833 on the other, with the SBC interworking between the two.

This function requires the SBE to program the DBE to enable interception and insertion of RFC2833 DTMF on a particular side of the call—the side facing the RFC2833-only device. The SBE and DBE then collaborate to transfer DTMF signaling between the H.245 control channel and the RTP steam.

DTMF interworking is negotiated through TerminalCapabilitySet. Therefore, the SBC must be capable of extending the TerminalCapabilitySet to advertise support for both alphanumeric and RFC2833 methods.

The feature described in this section replaces all previous H.323 DTMF interworking functions. H.323 calls must support DTMF interworking between alphanumeric UserInputIndication and RFC2833. In this case, the SBE coordinates with the DBE to carry out DTMF insertion and interception in the Real-Time Protocol (RTP).

DTMF interworking is negotiated through TerminalCapabilitySet, not manual configuration. Therefore, the SBC must always advertise support for both alphanumeric and RFC2833 methods, if necessary by extending the TerminalCapabilitySet on its way through. (The exception is a TCS=0.)

Restrictions for DTMF Interworking

The restrictions for DTMF internetworking are:

- Only the alphanumeric UserInputIndication method is supported for DTMF interworking.

- The SBE assumes that a peer, advertising any form of UserInputCapability is capable of sending and receiving alphanumeric DTMF.
- No manual configuration is provided to force DTMF interworking to occur.
- Detection or insertion of DTMF as in-band audio data is not supported.

Transcoding

The SBC supports transcoding of slow start calls, enabling communication between different endpoints with different codecs, which otherwise cannot communicate with each other. Two H.323 endpoints deployed back-to-back might fail to agree on a mutually acceptable codec.

A typical case might be where one side is insisting on a low-bandwidth codec (such as ITU-T G.729) because of bandwidth constraints or administrative policy, and the other side only supports G.711. For example, if the calling party uses g711alaw and the callee uses G.729 annex B, the SBC can convert G.711alaw codec to g729 annex B codec and enable communication between the two. When the SBC detects that codec negotiation is needed, it uses Cisco Voice Interworking Service Module (VXSM) in the Cisco MGX 8880 switch as its media gateway to perform the transcoding. Deploying the SBC between the endpoints, in conjunction with an MGX 8880 transcoder, allows such calls to succeed.

The previous releases supported a fast-start-only version of transcoding. This function is now replaced with an implementation of transcoding that is triggered off TerminalCapabilitySet.

Restrictions for Transcoding

The restrictions for transcoding are:

- The decision whether to use a transcoder is taken once per call, and is not modified if endpoints issue updated TerminalCapabilitySets (including TCS=0).
- When transcoding is required, the SBC enforces symmetric codecs for the call.
- Transcoding is never invoked in a fast start call. If no channels are suitable, endpoints must drop to slow start at which point transcoding may be invoked.
- The only codecs supported for transcoding are G.711 and G.729, and the only transcoder tested with them is the Cisco MGX 8880 switch.

RAS Tech Prefix

A technology prefix is an optional H.323 standard-based feature, supported by gateways and gatekeepers, that enables more flexibility in call routing within an H.323 VoIP network. The gatekeeper uses technology prefixes to group endpoints of the same type together. Technology prefixes can also be used to identify a type, class, or pool of gateways. This feature provides per-adjacency configuration of RAS Tech Prefix and registers this prefix with the gatekeeper.

An H.323 adjacency may now be optionally configured with a single tech prefix consisting of 1-32 dialed digits. It publishes the tech prefix to the gatekeeper in the following field of the RAS registration

request (RRQ):

```
terminalType.gateway.protocol.voice.supportedPrefixes.
```

As with existing adjacency configuration, this field may not be changed while the adjacency is attached. This feature works in conjunction with existing SBC support for adding or removing digits on dialed numbers (see section "Number Manipulation" in the Implementing SBC Policies chapter).

Restrictions for RAS Tech Prefix

- This feature does not support zone prefixes, for example, registration of prefix AliasAddresses with the gatekeeper.

User Protocol Timer Control

H.323 standards recommends timers, timeout, and retry counts for various messages. Their values are not fixed and represent a range. The ability to define these values facilitates interworking between different devices. H.323 timers and retry counts can be now configured by the user at a global and per-adjacency level. Timers are expressed in seconds.

The following Q.931/H.225 timers are configurable.

- Q.931/H.225 Setup Timer T303
- Q.931/H.225 Establishment Timer T301
- Q.931/H.225 Incoming Call Proceeding Timer T310

The following RAS timeout and retry counts are configurable.

- GRQ
- RRQ
- URQ
- ARQ
- BRQ
- DRQ

The RAS RRQ TTL and keepalive times (governing lightweight RRQ behavior) are configurable. These two settings are interrelated. If the user configures unsafe values for a given adjacency, the SBE reverts to the defaults.

The adjacency retry timer is configurable, and can be used to automatically reattempt adjacency attachment when an adjacency fails for any reason.

The following timers are hardcoded:

- TCP shutdown timeout—when gracefully closing a TCP connection, the time allowed for remote closure before closing it ungracefully. The hardcoded value is 1 second.
- TCP connect timeout—time allowed before giving up on a TCP connection attempt to a remote peer. The hardcoded value is 1 second.

Restrictions

User protocol timer control restrictions are:

- Changing timer values or retry counts while adjacencies are attached is allowed, but does not affect timers' or gatekeeper's transactions that are already in progress.
- No facility is provided to configure all RAS timeouts at once.
- H.245 timers are not included here since they only run in interworking scenarios.
- The SBC does not support the configuration of the following Q.931/H.225 timers:
  - Q.931/H.225 Overlap Sending Timer T302

  - Q.931/H.225 Overlap Receiving Timer T304
  - Q.931/H.225 Status Timer T322
- The SBC does not support the configuration of the following RAS timers:
  - IRQ
  - IRR
  - RAI
  - SCI

T.38 Fax Relay

This feature provides support for media relay of T.38 fax. The following features are supported:

- Both fax-only and fax-plus voice calls.
- Switchover from voice to T.38 fax.
- T.38 relay over unnumbered datagram protocol transport layer (UDPTL) only, and unidirectional H.245 channels only.

T.38 H.245 - SDP Mapping

The T.38 H.245—SDP mapping is shown below:

```
DataApplicationCapability
 application
  t38fax
   t38FaxProtocol              m=image 40000 {udptl | tcp} t38
   t38FaxProfile
    fillBitRemoval             a=T38FaxFillBitRemoval
    transcodingJBIG            a=T38FaxTranscodingJBIG
    transcodingMMR             a=T38FaxTranscodingMMR
    version                    a=T38FaxVersion:<digits>
    t38FaxRateManagement       a=T38FaxRateManagement:{localTCF | transferredTCF}
    t38FaxUdpOptions OPTIONAL
     t38FaxMaxBuffer           a=T38FaxMaxBuffer:<digits>
     t38FaxMaxDatagram         a=T38FaxMaxDatagram:<digits>
     t38FaxUdpEC               a=T38FaxUdpEC:{t38UDPFEC | t38UDPRedundancy}
    t38FaxTcpOptions OPTIONAL
     t38TCPBidirectionalMode   [no mapping]
  maxBitRate                   a=T38maxBitRate:<digits> (UDP only)
```

The only parameters needed for media relay function are the port and the peak-bit rate, which are highlighted in the example. Therefore, the presence of a T.38 fax function causes the following SDP to be transmitted to the DBE:

```
m=image <remote T.38 port> udptl t38
a=T38maxBitRate:14400
```

For interworking scenarios, a complete mapping needs to be carried out. However, this is not supported as of ACE SBC Release 3.0.00.

H.245 Mode Request

Switchover from a voice to fax call is handled by a RequestMode exchange. In an H.323-H.323 call this exchange is passed through transparently between call legs without DBE signaling. This allows endpoints to coordinate replacement of audio with T.38 channels.

RAS Maximum Bit Rate

In accordance with H.323v5 standards, the SBC counts UDP but not TCP towards the maximum bit rate agreed with the gatekeeper.

H.323 Annex D / T.38 Annex B Interoperability

T.38 Annex B is a fast start only (no H.245) version of H.323 Annex D. Interoperation with Annex B nodes is not supported by the SBC.

Restrictions

The restrictions are as follows:

- The SBC cannot be configured to advertise the t38FaxAnnexbOnly field of SupportedProtocols in RAS messages, and ignores this field on receipt.
- No support for TCP or Secure Real-Time Transport Protocol (SRTP) transport.
- No support for bidirectional H.245 channel signaling.

Q.931/H.225 Passthrough

This feature enables message elements from Q.931/H.225 to be passed through between two H.323 call legs. This section describes the "base passthrough profile" of the SBC, listing the parts of the Q.931/H.225 message that may be passed through.

The following conventions are used in the base passthrough profile:

- ASN.1 syntax for Q.931 / H.225 messages is reproduced in this document.
- The following tags are attached to ASN.1 subtrees, specifying the passthrough behavior.
  - P = "passthrough". This subtree is passed opaquely between call legs.
  - P* = "passthrough with privacy implications". Similar to "P", but passing through this subtree may reveal information about an endpoint or a remote telephone number.
  - B = "block". This subtree is unconditionally blocked by the SBC and any information contained in it is lost.
  - SBC. This subtree is manipulated by the SBC. Typically, values are replaced by those local to the SBC.

Call Proceeding Passthrough

A Call Proceeding message is never passed through. However, fields from it are extracted and put into a Progress or Facility in the upstream call log.

- A Progress is used if the Call Proceeding contains a progress indicator.

- A Facility is used otherwise.

Unsupported Messages

The following ITU-T Q.931 messages are not supported by the SBC either because they are forbidden in H.323 or because the SBC does not currently support their corresponding features.

- Status, Status Enquiry
- SetupAck
- Information
- Notify
- userInformation.

Privacy

Subtrees marked as "P*" - "passthrough with privacy implications" are automatically blocked if the outgoing call leg has privacy enabled in CAC policy. This automatic blocking cannot be overridden by configuration, therefore, the only way to have these fields pass through is to disable privacy.

Setting of Protocol Version

When passing through messages, the SBC sets the version of outgoing messages to the lower value of its own ASN.1 version from that received in the original protocol message.

Q.931 / H.225 Base Passthrough Profile

```
Q931Message
 protocolDiscriminator              SBC
 callReferenceValue                 SBC
 message
  setup
   sendingComplete                  P
   bearerCapability                 P
   facility                         P
   progressIndicator                P
   progressIndicator31              P
   notificationIndicator            P
   display                          P*
   keypadFacility                   P
   signal                           P
   callingPartyNumber               SBC
   callingPartySubaddress           B
   calledPartyNumber                SBC
   calledPartySubaddress            B
   redirectingNumber                P*
   userUser
    h323-uu-pdu
     h323-message-body
      setup
       protocolIdentifier           SBC
       h245Address                  SBC
       sourceAddress                SBC
       sourceInfo                   SBC
       destinationAddress           SBC
       destCallSignalAddress        SBC
```

```
      destExtraCallInfo             B
      destExtraCRV                  B
      activeMC                      P
      conferenceID                  P
      conferenceGoal                P
      callServices                  P
      callType                      B
      sourceCallSignalAddress       SBC
      remoteExtensionAddress        B
      callIdentifier                P
      h245SecurityCapability        B
      tokens                        B
      cryptoTokens                  B
      fastStart                     SBC
      mediaWaitForConnect           P
      canOverlapSend                B
      endpointIdentifier            P*
      multipleCalls                 SBC
      maintainConnection            SBC
      connectionParameters          P
      language                      P
      presentationIndicator         SBC
      screeningIndicator            SBC
      serviceControl                P
      symmetricOperationRequired    P
      capacity                      B
      circuitInfo                   SBC
      desiredProtocols              B
      neededFeatures                B
      desiredFeatures               B
      supportedFeatures             B
      parallelH245Control           B
      additionalSourceAddresses     B
    nonStandardData                 P
    h4501SupplementaryService       P
    h245Tunneling                   SBC
    h245Control                     SBC
    nonStandardControl              P
    callLinkage                     P
    tunnelledSignallingMessage      P
    provisionalRespToH245Tunneling  SBC
    stimulusControl                 P
    genericData                     P
   user-data                        P
callProceeding
 bearerCapability                   P
 facility                           P
 progressIndicator                  SBC
 progressIndicator31                SBC
 notificationIndicator              P
 display                            P
 userUser
  h323-uu-pdu
   h323-message-body
    callProceeding
     protocolIdentifier             SBC
     destinationInfo                P*
     h245Address                    SBC
     callIdentifier                 P
     h245SecurityMode               B
     tokens                         B
     cryptoTokens                   B
     fastStart                      SBC
     multipleCalls                  SBC
```

```
      maintainConnection            SBC
      fastConnectRefused            SBC
      featureSet                    B
    nonStandardData                 P
    h4501SupplementaryService       P
    h245Tunneling                   SBC
    h245Control                     SBC
    nonStandardControl              P
    callLinkage                     P
    tunnelledSignallingMessage      P
    provisionalRespToH245Tunneling  SBC
    stimulusControl                 P
    genericData                     P
   user-data                        P
alerting
 bearerCapability                   P
 facility                           P
 progressIndicator                  SBC
 progressIndicator31                SBC
 notificationIndicator              P
 display                            P*
 signal                             P
 userUser
  h323-uu-pdu
   h323-message-body
    alerting
     protocolIdentifier             SBC
     destinationInfo                P*
     h245Address                    SBC
     callIdentifier                 P
     h245SecurityMode               B
     tokens                         B
     cryptoTokens                   B
     fastStart                      SBC
     multipleCalls                  SBC
     maintainConnection             SBC
     alertingAddress                P*
     presentationIndicator          SBC
     screeningIndicator             SBC
     fastConnectRefused             SBC
     serviceControl                 P
     capacity                       B
     featureSet                     B
    nonStandardData                 P
    h4501SupplementaryService       P
    h245Tunneling                   SBC
    h245Control                     SBC
    nonStandardControl              P
    callLinkage                     P
    tunnelledSignallingMessage      P
    provisionalRespToH245Tunneling  SBC
    stimulusControl                 P
    genericData                     P
   user-data                        P
connect
 bearerCapability                   P
 facility                           P
 progressIndicator                  SBC
 progressIndicator31                SBC
 notificationIndicator              P
 display                            P*
 dateTime                           P
 connectedNumber                    P*
 connectedSubaddress                P*
```

```
 userUser
  h323-uu-pdu
   h323-message-body
    connect
     protocolIdentifier            SBC
     h245Address                   SBC
     destinationInfo               P*
     conferenceID                  P
     callIdentifier                P
     h245SecurityMode              B
     tokens                        B
     cryptoTokens                  B
     fastStart                     SBC
     multipleCalls                 SBC
     maintainConnection            SBC
     language                      P
     connectedAddress              P*
     presentationIndicator         SBC
     screeningIndicator            SBC
     fastConnectRefused            SBC
     serviceControl                P
     capacity                      B
     featureSet                    B
   nonStandardData                 P
   h4501SupplementaryService       P
   h245Tunneling                   SBC
   h245Control                     SBC
   nonStandardControl              P
   callLinkage                     P
   tunnelledSignallingMessage      P
   provisionalRespToH245Tunneling  SBC
   stimulusControl                 P
   genericData                     P
  user-data                        P
progress
 bearerCapability                  P
 cause                             P
 facility                          P
 progressIndicator                 SBC
 progressIndicator31               SBC
 notificationIndicator             P
 display                           P*
 userUser
  h323-uu-pdu
   h323-message-body
    progress
     protocolIdentifier            SBC
     destinationInfo               SBC
     h245Address                   SBC
     callIdentifier                P
     h245SecurityMode              B
     tokens                        B
     cryptoTokens                  B
     fastStart                     SBC
     multipleCalls                 SBC
     maintainConnection            SBC
     fastConnectRefused            SBC
   nonStandardData                 P
   h4501SupplementaryService       P
   h245Tunneling                   SBC
   h245Control                     SBC
   nonStandardControl              P
   callLinkage                     P
   tunnelledSignallingMessage      P
```

```
   provisionalRespToH245Tunneling  SBC
   stimulusControl                 P
   genericData                     P
  user-data                        P
releaseComplete
 cause                             SBC
 facility                          P
 notificationIndicator             P
 display                           P*
 signal                            P
 userUser
  h323-uu-pdu
   h323-message-body
    connect
     protocolIdentifier            SBC
     reason                        SBC
     callIdentifier                P
     tokens                        B
     cryptoTokens                  B
     busyAddress                   P*
     presentationIndicator         SBC
     screeningIndicator            SBC
     capacity                      B
     serviceControl                P
     featureSet                    B
   nonStandardData                 P
   h4501SupplementaryService       P
   h245Tunneling                   SBC
   h245Control                     SBC
   nonStandardControl              P
   callLinkage                     P
   tunnelledSignallingMessage      P
   provisionalRespToH245Tunneling  SBC
   stimulusControl                 P
   genericData                     P
  user-data
facility
 facility                          P
 notificationIndicator             P
 display                           P*
 callingPartyNumber                P*
 calledPartyNumber                 P*
 userUser
  h323-uu-pdu
   h323-message-body
    facility
     protocolIdentifier            SBC
     alternativeAddress            B
     alternativeAliasAddress       P
     conferenceID                  P
     reason                        P
     callIdentifier                P
     destExtraCallInfo             P
     remoteExtensionAddress        P
     tokens                        B
     cryptoTokens                  B
     conferences                   P
     h245Address                   SBC
     fastStart                     SBC
     multipleCalls                 SBC
     maintainConnection            SBC
     fastConnectRefused            SBC
     serviceControl                P
     circuitInfo                   B
```

```
    featureSet                    B
    destinationInfo               P*
    h245SecurityMode              B
   empty
  nonStandardData                 P
  h4501SupplementaryService       P
  h245Tunneling                   SBC
  h245Control                     SBC
  nonStandardControl              P
  callLinkage                     P
  tunnelledSignallingMessage      P
  provisionalRespToH245Tunneling  SBC
  stimulusControl                 P
  genericData                     P
 user-data                        P
```

Restrictions

- Any message elements from Q.931/H.225 that are not listed in this section cannot be passed through.
- Passthrough of security tokens is not supported.

H.323 Privacy

With the H.323 privacy feature, users can invoke identity hiding on Q.931/H.225 messages. When this feature is implemented, the SBC strips Q.931/H.225 message elements that reveal information about the remote caller or callee before passing them to the endpoints.

Note The Q.931/H.225 message elements that impact privacy are defined in the H.323 passthrough profile.

The SBC applies the privacy service to a message if it contains a privacy request submitted by a user, or if a Call Admission Control(CAC) policy on the SBC is configured to enable privacy on a caller or callee basis. If, however, the privacy configuration fields are set to default values, then the SBC forwards the message to the next call leg without applying the privacy service to the message. You can also configure the SBC to provide the H.323 privacy service on a per-adjacency basis.

The SBC applies the following rules when providing the H.323 privacy service:

- If an H.323 adjacency is configured to allow private information, then the SBC does not apply privacy service even if an incoming message requests it or the CAC policy is configured to enable privacy.
- If an H.323 adjacency is not configured to allow private information, but a CAC policy is configured to enable privacy, then the SBC applies the privacy service to outgoing messages.
- If an incoming message requests the privacy service, but a CAC policy has not been configured to enable privacy, then the SBC applies the service if the adjacency is configured to apply the privacy service.
- If an incoming message requests the privacy service when both the CAC policy and the adjacency have not been configured to apply the privacy service, then the SBC does not apply the privacy service and allows the private information to pass through.

Restrictions and Limitations

Restrictions and limitations are as follows:

- The SBC does not apply the H.323 privacy service to H.245 and RAS messages.
- Currently, the CAC policy for callee privacy is available for the H.323 signaling stack at "connect time", and only if a connectedNumber is present. As a result, the callee privacy service is not applied to the Q.931 protocol messages that pass through before or after a call is connected when a connectedNumber is not present. Due to this limitation, the SBC forwards the Q.931 Alerting, Q.931 Progress, and Q.931 Release Complete messages without applying the privacy service request to them.
- In an interworking call, the SBC only applies privacy requests based on the CAC policy.

Configuring H.323 Features

This section contains the following:

Configuring Separate H.245 Control Channel

This command disables tunneling on a per-adjacency basis, facilitating interoperability with existing devices that are confused by tunneling. The command controls both incoming and outgoing calls.

SUMMARY STEPS

1. **configure**
2. **sbc** *service-name*
3. **sbe**
4. **adjacency h323** *adjacency-name*
5. **h245 tunnel disable**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure** **Example:** `host1/Admin# configure`	Enables the global configuration mode.
Step 2	**sbc** *service-name* **Example:** `host1/Admin(config)# sbc mysbc`	Enters the mode of an SBC service. Use the *service-name* argument to define the name of the SBC.

	Command or Action	Purpose
Step 3	**sbe** **Example:** `host1/Admin(config-sbc)# sbe`	Enters the mode of the SBE function of the SBC.
Step 4	**adjacency h323** *adjacency-name* **Example:** `host1/Admin(config-sbc-sbe)# adjacency h323 2651XM-5`	Enters the mode of an SBE H.323 adjacency. Use the *adjacency-name* argument to define the name of the H.323 adjacency.
Step 5	**h245 tunnel disable** **Example:** `host1/Admin(config-sbc-sbe-adj-h323)# h245 tunnel disable`	Disables tunneling on a per-adjacency basis, facilitating interoperability with existing devices that are confused by tunneling. The command controls both incoming and outgoing calls. The default is tunneling enabled.
Step 6	**exit** **Example:** `host1/Admin(config-sbc-sbe-adj-h323)# exit`	Exits the media address mode to the DBE mode.

Configuring RAS Tech Prefix

This feature provides per-adjacency configuration of RAS Tech Prefix and registers this prefix with the gatekeeper. RAS tech prefix may consist of 1-32 dialed digits.

SUMMARY STEPS

1. **configure**
2. **sbc** *service-name*
3. **sbe**
4. **adjacency h323** *adjacency-name*
5. **tech-prefix** *tech-prefix*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure** **Example:** `host1/Admin# configure`	Enables the global configuration mode.
Step 2	**sbc** *service-name* **Example:** `host1/Admin(config)# sbc mysbc`	Enters the mode of an SBC service. Use the *service-name* argument to define the name of the SBC.

	Command or Action	Purpose
Step 3	**sbe** **Example:** `host1/Admin(config-sbc)# sbe`	Enters the mode of the signaling border element (SBE) function of the SBC.
Step 4	**adjacency h323** *adjacency-name* **Example:** `host1/Admin(config-sbc-sbe)# adjacency h323 2651XM-5`	Enters the mode of an SBE H.323 adjacency. Use the *adjacency-name* argument to define the name of the H.323 adjacency.
Step 5	**tech-prefix** *tech-prefix* **Example:** `host1/Admin(config-sbc-sbe-adj-h323)# tech-prefix 32#`	Provides per-adjacency configuration of RAS Tech Prefix and registers this prefix with the gatekeeper. RAS tech prefix may consist of 1-32 dialed digits followed by a # sign. The default is no tech prefix.
Step 6	**exit** **Example:** `host1/Admin(config-sbc-sbe-adj-h323)# exit`	Exits the media address mode to the DBE mode.

Configuring User Protocol Timer Control

SUMMARY STEPS

1. **configure**
2. **sbc** *service-name*
3. **sbe**
4. **h323 | adjacency h323** *adjacency-name*
5. **adjacency timeout** *value*
6. **h225 timeout**
7. **ras retry**
8. **ras rrq ttl** *value*
9. **ras rrq keepalive** *value*
10. **ras timeout**
11. **exit**
12. **show services sbc** *sbc-name* **sbe h323 timers**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure** **Example:** `host1/Admin# configure`	Enables the global configuration mode.
Step 2	**sbc** *service-name* **Example:** `host1/Admin(config)# sbc mysbc`	Enters the mode of an SBC service. Use the *service-name* argument to define the name of the SBC.
Step 3	**sbe** **Example:** `host1/Admin(config-sbc)# sbe`	Enters the mode of the SBE function of the SBC.
Step 4	**h323 | adjacency h323** *adjacency-name* **Example:** `host1/Admin(config-sbc-sbe)# adjacency h323 2651XM-5`	Enters the mode of either all H.323 adjacencies or a specified H.323 adjacency. Use the *adjacency-name* argument to define the name of the H.323 adjacency.
Step 5	**adjacency timeout** *value* **Example:** `host1/Admin(config-sbc-sbe-adj-h323)# adjacency timeout 10000`	Defines the time in milliseconds, during which in case of failure to connect, the SBC keeps trying to reconnect to the remote signaling peer and receive keep-alive messages from it. The value range is 10000—30000.
Step 6	**h225 timeout [establishment** *timeout-value* **| proceeding** *timeout-value* **| setup** *timeout-value* **|** **Example:** `host1/Admin(config-sbc-sbe-adj-h323)# h225 timeout establishment 250000`	Defines the time for waiting to receive H.225 messages. • **establishment** *timeout-value*—h225 establishment state timeout value in milliseconds. The default is 180000. The value range is 30000-300000. • **proceeding** *timeout-value*—h225 proceeding state timeout value in milliseconds. 10000. The value range is 1000-30000. • **setup** *timeout-value*—h225 setup timeout value in milliseconds. The default is 4000. The value range is 1000-30000.

	Command or Action	Purpose

Step 7	**ras retry [arq | brq | drq | grq | rrq | urq]** *retry count*
	
	Example:
	`host1/Admin(config-sbc-sbe-adj-h323)#`
	`ras retry arq 2`
	`ras retry brq 2`
	`ras retry drq 2`
	`ras retry rrq 2`
	`ras retry urq 2`
		Defines the number of times the system trys to re-send RAS messages in case of failure to send the messages.
		• arq retry count—Number of times to retry an ARQ transaction.
		• brq retry count—Number of times to retry a BRQ transaction.
		• drq retry count—Number of times to retry a DRQ transaction.
		• grq retry count—Number of times to retry a GRQ transaction.
		• rrq retry count—Number of times to retry an RRQ transaction.
		• urq retry count—Number of times to retry a URQ transaction.
		The value range is 0-30.

Step 8	**ras rrq ttl** *value* **Example:** `host1/Admin(config-sbc-sbe-adj-h323)# ras rrq ttl 100`	Defines the time to live messages (TTL) in seconds for registration request (RRQ). The default is 60. The value range is 16—300.
Step 9	**ras rrq keepalive** *value* **Example:** `host1/Admin(config-sbc-sbe-adj-h323)# ras rrq keepalive 100000`	Defines the time in milliseconds for registration request (RRQ) keep-alive messages. The default is 45000. The value range is 15000—150000.

Step 10	**ras timeout [arq | brq | drq | grq | rrq | urq]** *timeout*
	
	Example:
	`host1/Admin(config-sbc-sbe-adj-h323)#`
	`ras timeout arq 1000`
	`ras timeout brq 1000`
	`ras timeout drq 1000`
	`ras timeout grq 1000`
	`ras timeout rrq 1000`
	`ras timeout urq 1000`
		Defines the common timeout in milliseconds for all RAS messages.
		• arq timeout—Timeout value for an ARQ transaction.
		• brq timeout—Timeout value for an BRQ transaction.
		• drq timeout—Timeout value for an DRQ transaction.
		• grq timeout—Timeout value for an GRQ transaction.
		• rrq timeout—Timeout value for an RRQ transaction.
		• urq timeout—Timeout value for an URQ transaction.
		The default is 5000. The value range is 1000-45000. The default is 5000.

	Command or Action	Purpose
Step 11	**exit** **Example:** `host1/Admin(config-sbc-sbe-adj-h323)# exit`	Exits the H.323 global or specified adjacency mode.
Step 12	**show services sbc** *service-name* **sbe h323 timers** **Example:** `host1/Admin# show services sbc mysbc sbe h323 timers`	Displays the values of all H.323 timers.

Configuring H.323 Privacy

This feature allows the SBC to apply the H.323 privacy service on outbound messages.

SUMMARY STEPS

1. **configure**
2. **sbc** *service-name*
3. **sbe**
4. **adjacency h323** *adjacency-name*
5. **allow private info**
6. **privacy restrict outbound**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure** **Example:** `host1/Admin# configure`	Enables the global configuration mode.
Step 2	**sbc** *service-name* **Example:** `host1/Admin(config)# sbc mysbc`	Enters the mode of an SBC service. Use the *service-name* argument to define the name of the SBC.
Step 3	**sbe** **Example:** `host1/Admin(config-sbc)# sbe`	Enters the mode of the SBE function of the SBC.
Step 4	**adjacency h323** *adjacency-name* **Example:** `host1/Admin(config-sbc-sbe)# adjacency h323 2651XM-5`	Enters the mode of an SBE H.323 adjacency. Use the *adjacency-name* argument to define the name of the H.323 adjacency.

	Command or Action	Purpose
Step 5	**allow private info** **Example:** `host1/Admin(config-sbc-sbe-adj-h323)# allow private info`	Configures the H.323 adjacency to allow private information on messages sent out by the adjacency even if the CAC policy is configured to apply privacy service or the user requests privacy service. The **no** version of this command configures the H.323 adjacency to stop allowing private information from being sent out by the adjacency.
Step 6	**privacy restrict outbound** **Example:** `host1/Admin(config-sbc-sbe-adj-h323)# privacy restrict outbound`	Configures the H.323 adjacency to apply privacy restriction on outbound messages if the user requests the privacy service. The **no** version of this command configures the H.323 adjacency to allow private information messages sent out by the adjacency.
Step 7	**exit** **Example:** `host1/Admin(config-sbc-sbe-adj-h323)# exit`	Exits an SBE H.323 global or specified adjacency mode.

Configuring Separate H.245 Control Channel and RAS Tech Prefix: Example

```
configure
sbc mysbc
sbe
adjacency h323 h323-fxs-1b
signaling-address ipv4 88.110.128.13
signaling-port 1720
remote-address ipv4 10.0.0.0/8
signaling-peer 10.124.2.2
signaling-peer-port 1720
account h323-fxs-1b
tech-prefix 2#
h245-tunnel disable
attach
exit
```

Configuring User Protocol Timer Controls: Example

```
configure
sbc mysbc
sbe
adjacency h323 abcd
adjacency timeout 10000
h225 timeout establishment 40000
adjacency timeout 10000?
h225 timeout ?
  establishment  h225 establishment state timeout value.
  proceeding     h225 proceeding state timeout value.
  setup          h225 setup timeout value.
h225 timeout proceeding 30000
```

```
h225 timeout setup 30000
ras ?
  retry    RAS retry configuration.
  rrq      RRQ (Registration Request) configuration.
  timeout  RAS timeout configuration.
ras retry ?
  arq  Retry count for an ARQ transaction.
  brq  Retry count for an BRQ transaction.
  drq  Retry count for an DRQ transaction.
  grq  Retry count for an GRQ transaction.
  rrq  Retry count for an RRQ transaction.
  urq  Retry count for an URQ transaction.
ras retry arq 2
ras retry brq 2
ras retry drq 2
ras retry rrq 2
ras retry rrq 2
ras rrq ?
  keepalive  Rate for keepalive msgs to refresh an H323 adjacency registration.
  ttl        TTL (time to live) value for an RRQ request.
ras rrq keepalive ?
  <15000-150000>  Keepalive refresh time in milliseconds - default: 45000 ras rrq
keepalive 15000
ras rrq ttl ?
  <16-300>  TTL value in seconds - default: 60
ras rrq ttl 30
adjacency timeout 30000
ras timeout ?
  arq  Timeout value for an ARQ transaction.
  brq  Timeout value for an BRQ transaction.
  drq  Timeout value for an DRQ transaction.
  grq  Timeout value for an GRQ transaction.
  rrq  Timeout value for an RRQ transaction.
  urq  Timeout value for an URQ transaction.
ras timeout arq ?
  <1000-45000>  Timeout value in milliseconds - default: 5000
ras timeout arq 1000
ras timeout brq 1000
ras timeout drq 1000
ras timeout grq 1000
ras timeout rrq 1000
ras timeout urq 1000
```