Protocols

- About H.323, on page 1
- Configuring H.323, on page 2
- About SIP, on page 4
- Configuring SIP, on page 7
- Configuring Domains, on page 13
- Configuring SIP and H.323 Interworking, on page 15

About H.323

The Expressway supports the H.323 protocol. It's an H.323 gatekeeper.

The Expressway can also provide Configuring SIP and H.323 Interworking between H.323 and SIP. It translates between the two protocols to enable endpoints that only support one of these protocols to call each other. To support H.323, the **H.323 mode** must be enabled.

Using the Expressway as an H.323 Gatekeeper

As an H.323 gatekeeper, the Expressway accepts registrations from H.323 endpoints and provides call control functions such as address translation and admission control.

To enable the Expressway as an H.323 gatekeeper, ensure that **H.323 mode** is set to *On* (**Configuration** > **Protocols** > **H.323**).

H.323 Endpoint Registration

H.323 endpoints in your network must register with the Expressway in order to use it as their gatekeeper.

There are two ways an H.323 endpoint can locate an Expressway with which to register:

- Manual
- Automatically

The option is configured on the endpoint itself under the Gatekeeper Discovery setting (consult your endpoint manual for how to access this setting).

- If the mode is set to automatic, the endpoint will try to register with any Expressway it can find. It does this by sending out a Gatekeeper Discovery Request, to which eligible Expressways will respond.
- If the mode is set to manual, you must specify the IP address of the Expressway with which you want your endpoint to register, and the endpoint will attempt to register with that Expressway only.

Preventing Automatic H.323 Registrations

You can prevent H.323 endpoints being able to register automatically with the Expressway by disabling **Auto Discovery** on the Expressway (**Configuration** > **Protocols** > **H.323**).

Registration Refresh

The H.323 Time to live setting controls the frequency of H.323 endpoint registration refresh. The refresh frequency increases when the time to live is decreased. When you have many H.323 endpoints, be careful not to set the TTL too low, because a flood of registration requests will unnecessarily impact the Expressway performance.

Configuring H.323

Go to **Configuration** > **Protocols** > **H.323** to configure the About H.323 settings on the Expressway.

The configurable options are:

Field	Description	Usage tips
H.323 mode	Enables or disables H.323 on the Expressway. H.323 support is *Off* by default.	You must enable H.323 mode if you are clustering the Expressway, even if there are no H.323 endpoints in your deployment.
Registration UDP port	The listening port for H.323 UDP registrations.	The default Expressway configuration uses standard port numbers so you can use H.323 services out of the box without having to first set these up.

Field	Description	Usage tips
Registration conflict mode	Determines how the system behaves if an endpoint attempts to register an alias currently registered from another IP address. *Reject*: Denies the new registration. This is the default. *Overwrite*: Deletes the original registration and replaces it with the new registration.	An H.323 endpoint may attempt to register with the Expressway using an alias that has already been registered on the Expressway from another IP address. The reasons for this could include: • Two endpoints at different IP addresses are attempting to register using the same alias. • A single endpoint has previously registered using a particular alias. The IP address allocated to the endpoint then changes, and the endpoint attempts to re-register using the same alias. *Reject* is useful if your priority is to prevent two users registering with the same alias. *Overwrite* is useful if your network is such that endpoints are often allocated new IP addresses, because it will prevent unwanted registration rejections. **Note** In a cluster a registration conflict is only detected if the registration requests are received by the same peer.
Call signaling TCP port	The listening port for H.323 call signaling.	
Call signaling port range start and end	Specifies the port range used by H.323 calls after they are established.	The call signaling port range must be great enough to support all the required concurrent calls.
Time to live	The interval (in seconds) at which an H.323 endpoint must re-register with the Expressway in order to confirm that it is still functioning. Default is 1800.	Some older endpoints do not support the ability to periodically re-register with the system. In this case, and in any other situation where the system has not had a confirmation from the endpoint within the specified period, it will send an IRQ to the endpoint to verify that it is still functioning. **Note** By reducing the registration time to live too much, you risk flooding the Expressway with registration requests, which will severely impact performance. This impact is proportional to the number of endpoints, so you should balance the need for occasional quick failover against the need for continuous good performance.

Field	Description	Usage tips
Call time to live	The interval (in seconds) at which the Expressway polls the endpoints in a call to verify that they are still in the call. Default is 120.	If the endpoint does not respond, the call is disconnected. The system polls endpoints in a call, whether the call type is traversal or non-traversal.
Auto discover	Determines whether it will respond to About H.323 sent out by endpoints. The default is *On*.	To prevent H.323 endpoints being able to register automatically with the Expressway, set **Auto discover** to *Off*. This means that endpoints can only register with the Expressway if their **Gatekeeper Discovery** setting is *Manual* and they have been configured with the Expressway's IP address.
Caller ID	Specifies whether the prefix of the ISDN gateway is inserted into the caller's E.164 number presented on the destination endpoint.	Including the prefix allows the recipient to directly return the call.

About SIP

The Expressway supports the SIP protocol. It can act as a SIP registrar, SIP proxy and as a SIP Presence Server. Expressway can provide interworking between SIP and H.323, translating between the two protocols to enable endpoints that only support one of the protocols to call each other.

To support SIP:

- Configuring SIP must be enabled.
- At least one of the SIP transport protocols (UDP, TCP or TLS) must be active.

Note Use of UDP is not recommended for video as SIP message sizes are frequently larger than a single UDP packet.

Any dialog-forming requests, such as INVITE and SUBSCRIBE, that contain Route Sets are rejected. Requests that do not have Route Sets are proxied as normal in accordance with existing call processing rules.

Expressway as a SIP Registrar

For a SIP endpoint to be contactable via its alias, it must register its Address of Record (AOR) and its location with a SIP registrar. The SIP registrar maintains a record of the endpoint's details against the endpoint's AOR. The AOR is the alias through which the endpoint can be contacted; it is a SIP URI and always takes the form **username@domain**.

When a call is received for that AOR, the SIP registrar refers to the record to find its corresponding endpoint.

Note The same AOR can be used by more than one SIP endpoint at the same time, although to ensure that all endpoints are found they must all register with the same Expressway or Expressway cluster.

A SIP registrar only accepts registrations for domains for which it is authoritative. The Expressway can act as a SIP registrar for up to 200 domains. To make the Expressway act as a SIP registrar, you must configure it with the Configuring Domains for which it will be authoritative . It will then handle registration requests for any endpoints attempting to register against that domain.

Note Expressway will also accept registration requests where the domain portion of the AOR is either the FQDN or the IP address of the Expressway. Whether or not the Expressway accepts a registration request depends on its registration control settings.

In a Unified Communications deployment, endpoint registration for SIP devices may be provided by Unified CM. In this scenario, the Expressway provides secure firewall traversal and line-side support for Unified CM registrations. When configuring a domain, you can select whether Cisco Unified Communications Manager or Expressway provides registration and provisioning services for the domain.

SIP endpoint registration

There are two ways a SIP endpoint can locate a registrar with which to register: manually or automatically. The option is configured on the endpoint itself under the SIP **Server Discovery** option (consult your endpoint user guide for how to access this setting; it may also be referred to as **Proxy Discovery**).

- If the **Server Discovery** mode is set to automatic, the endpoint will send a REGISTER message to the SIP server that is authoritative for the domain with which the endpoint is attempting to register. For example, if an endpoint is attempting to register with a URI of **john.smith@example.com**, the request will be sent to the registrar authoritative for the domain **example.com**. The endpoint can discover the appropriate server through a variety of methods including DHCP, DNS or provisioning, depending upon how the video communications network has been implemented.
- If the **Server Discovery** mode is set to manual, the user must specify the IP address or FQDN of the registrar (Expressway or Expressway cluster) with which they want to register, and the endpoint will attempt to register with that registrar only.

The Expressway is a SIP server and a SIP registrar.

- If an endpoint is registered to the Expressway, the Expressway will be able to forward inbound calls to that endpoint.
- If the Expressway is not configured with any SIP domains, the Expressway will act as a SIP server. It may proxy registration requests to another registrar, depending upon the **SIP registration proxy** mode setting.

Registration refresh intervals

Depending on the typical level of active registrations on your system, you may want to configure the **Standard registration refresh strategy** to *Variable* and set the refresh intervals as follows:

Active registrations	Minimum refresh interval	Minimum refresh interval
1–100	45	60
101–500	150	200
501–1000	300	400
1000–1500	450	800
1500+	750	1000

Note If you have a mix of H.323 and SIP endpoints, be aware that H.323 registration requests and SIP registration requests can both impair performance of the Expressway if it receives too many. See Configuring H.323.

If you want to ensure registration resiliency, use SIP outbound registrations as described below.

SIP registration resiliency

The Expressway supports multiple client-initiated connections (also referred to as "SIP Outbound") as outlined in RFC 5626.

This allows SIP endpoints that support *RFC 5626* to be simultaneously registered to multiple Expressway cluster peers. This provides extra resiliency: if the endpoint loses its connection to one cluster peer it will still be able to receive calls via one of its other registration connections.

Expressway as a SIP Proxy Server

The Expressway acts as a SIP proxy server when **SIP mode** is enabled. The role of a proxy server is to forward requests (such as REGISTER and INVITE) from endpoints or other proxy servers on to further proxy servers or to the destination endpoint.

Expressway's behavior as a SIP proxy server is determined by:

- SIP registration proxy mode setting
- Presence of Route Set information in the request header
- Whether the proxy server from which the request was received is a neighbor of the Expressway

A Route Set specifies the path to take when requests are proxied between an endpoint and its registrar. For example, when a REGISTER request is proxied by the Expressway, it adds a path header component to the request. This signals that calls to that endpoint should be routed through the Expressway. This is usually required in situations where firewalls exist and the signaling must follow a specified path to successfully traverse the firewall. For more information about path headers, see RFC 3327.

When the Expressway proxies a request that contains Route Set information, it forwards it directly to the URI specified in the path. Any call processing rules configured on the Expressway are bypassed. This may present a security risk if the information in the Route Set cannot be trusted. For this reason, you can configure how the Expressway proxies requests that contain Route Sets by setting the **SIP registration proxy mode** as follows:

- *Off*: Requests containing Route Sets are rejected. This setting provides the highest level of security.

- *Proxy to known only*: Requests containing Route Sets are proxied only if the request was received from a known zone.
- *Proxy to any*: Requests containing Route Sets are always proxied.

In all cases, requests that do not have Route Sets are proxied as normal in accordance with existing call processing rules. This setting only applies to dialog-forming requests, such as INVITE and SUBSCRIBE. Other requests, such as NOTIFY, are always proxied regardless of this setting.

Proxying Registration Requests

If the Expressway receives a registration request for a domain for which it is not acting as a Registrar (the Expressway does not have that SIP domain configured), then the Expressway may proxy the registration request onwards. This depends on the **SIP registration proxy mode** setting, as follows:

- *Off*: The Expressway does not proxy any registration requests. They are rejected with a "403 Forbidden" message.
- *Proxy to known only*: The Expressway proxies the request in accordance with existing call processing rules, but only to known neighbor, traversal client and traversal server zones.
- *Proxy to any*: This is the same as *Proxy to known only* but for all zone types i.e. it also includes ENUM and DNS zones.

Accepting proxied registration requests

If the Expressway receives a proxied registration request, in addition to the Expressway's standard registration controls, you can also control whether the Expressway accepts the registration depending upon the zone through which the request was received. You do this through the **Accept proxied registrations** setting when configuring a zone.

Proxied registrations are classified as belonging to the zone they were last proxied from. This is different from non-proxied registration requests which are assigned to a subzone within the Expressway.

Expressway as a SIP Presence Server

The Expressway supports the SIP-based SIMPLE protocol. It can act as a Presence Server and Presence User Agent for any of the SIP domains for which it is authoritative. For details on how to enable and use Expressway as a SIP Presence server, see the Presence section.

Configuring SIP

The **SIP** page (**Configuration** > **Protocols** > **SIP**) is used to configure SIP settings on the Expressway, including:

- SIP functionality and SIP-specific transport modes and ports.
- Certificate revocation checking modes for TLS connections.
- Registration controls for standard and outbound registrations.

Note The value of "SIP Registration" will be changed to OFF due to enabling Smart Licensing. The administrator must manually change this field to ON to enable SIP registrations to Expressway.

SIP Functionality and SIP-Specific Transport Modes and Ports

This section contains the basic settings for enabling SIP functionality and for configuring the various SIP-specific transport modes and ports. The configurable options are:

Field	Description	Usage tips
SIP mode	Enables and disables SIP functionality (SIP registrar and SIP proxy services) on the Expressway. Default is *Off*.	This mode must be enabled to use either the Presence Server or the Presence User Agent.
SIP protocols and ports	The Expressway supports SIP over **UDP**, **TCP**, and **TLS** transport protocols. Use the **Mode** and **Port** settings for each protocol to configure whether or not incoming and outgoing connections using that protocol are supported. And if so, the ports on which the Expressway listens for such connections. The default modes are: • UDP mode *Off* • TCP mode *Off* • TLS mode *On* • Mutual TLS mode *Off*	At least one of the transport protocol modes must be *On* to enable SIP functionality. If you use both TLS and MTLS, we recommend that you enable them on different ports. If you must use port 5061 for MTLS, you should avoid engaging the B2BUA - by switching **Media encryption mode** to *Auto* on all zones in the call path.
TCP outbound port start / end	The range of ports the Expressway uses when TCP and TLS connections are established.	The range must be sufficient to support all required concurrent connections.
Session refresh interval	The maximum time allowed between session refresh requests for SIP calls. Default is 1800 seconds.	For further information see the definition of *Session-Expires* in *RFC 4028*.
Minimum session refresh interval	The minimum value the Expressway will negotiate for the session refresh interval for SIP calls. Default is 500 seconds.	For further information see the definition of *Min-SE header* in *RFC 4028*.

Field	Description	Usage tips
TLS handshake timeout	The timeout period for TLS socket handshake. Default is 5 seconds.	You may want to increase this value if TLS server certificate validation is slow (e.g. if OCSP servers do not provide timely responses) and thus cause connection attempts to timeout.

Certificate Revocation Checking Modes

This section controls the certificate revocation checking modes for SIP TLS connections. The configurable options are:

Field	Description	Usage tips
Certificate revocation checking mode	Controls whether revocation checking is performed for certificates exchanged during SIP TLS connection establishment.	We recommend that revocation checking is enabled.
Use OCSP	Controls whether the Online Certificate Status Protocol (OCSP) may be used to perform certificate revocation checking.	To use OCSP: • The X.509 certificate to be checked must contain an OCSP responder URI. • The OCSP responder must support the SHA-256 hash algorithm. If it is not supported, the OCSP revocation check and the certificate validation will fail.
Use CRLs	Controls whether Certificate Revocation Lists (CRLs) are used to perform certificate revocation checking.	CRLs can be used if the certificate does not support OCSP. CRLs can be loaded manually onto the Expressway, downloaded automatically from preconfigured URIs (see Managing Certificate Revocation Lists (CRLs)), or downloaded automatically from a CRL distribution point (CDP) URI contained in the X.509 certificate.
Allow CRL downloads from CDPs	Controls whether the download of CRLs from the CDP URIs contained in X.509 certificates is allowed.	

Field	Description	Usage tips
Fallback behavior	Controls the revocation checking behavior if the revocation status cannot be established, for example if the revocation source cannot be contacted. *Treat as revoked*: Treat the certificate as revoked (and thus do not allow the TLS connection). *Treat as not revoked*: Treat the certificate as not revoked. Default: *Treat as not revoked*.	*Treat as not revoked* ensures that your system continues to operate in a normal manner if the revocation source cannot be contacted, however it does potentially mean that revoked certificates will be accepted.

Registration Controls

This section contains the registration controls for standard and outbound SIP registrations. The configurable options are:

Field	Description	Usage tips
Standard registration refresh strategy	The method used to generate the SIP registration expiry period (the period within which a SIP endpoint must re-register to prevent its registration expiring) for standard registrations. *Maximum*: Uses the lesser of the configured **Maximum** refresh value and the value requested in the registration. *Variable*: Generates a random value between the configured **Minimum** refresh value and the lesser of the configured **Maximum** refresh value and the value requested in the registration. The default is *Maximum*.	The *Maximum* setting uses the requested value providing it is within the specified maximum and minimum ranges. The *Variable* setting calculates a random refresh period for each registration (and re-registration) request in an attempt to continually spread the load. The Expressway never returns a value higher than what was requested. This applies only to endpoints registered with the Expressway. It does not apply to endpoints whose registrations are proxied through the Expressway.
Standard registration refresh minimum	The minimum allowed value for a SIP registration refresh period for standard registrations. Requests for a value lower than this will result in the registration being rejected with a 423 Interval Too Brief response. The default is 45 seconds.	See Registration refresh intervals.

Field	Description	Usage tips
Standard registration refresh maximum	The maximum allowed value for a SIP registration refresh period for standard registrations. Requests for a value greater than this will result in a lower value being returned (calculated according to the **Standard registration refresh strategy**). The default is 60 seconds.	
Outbound registration refresh strategy	The method used to generate the SIP registration expiry period for outbound registrations. *Maximum*: Uses the lesser of the configured **Maximum** refresh value and the value requested in the registration. *Variable*: Generates a random value between the configured **Minimum** refresh value and the lesser of the configured **Maximum** refresh value and the value requested in the registration. The default is *Variable*.	These options work in the same manner as for the **Standard registration refresh strategy**. However, outbound registrations allow a much higher maximum value than standard registrations. This is because standard registrations use the re-registration mechanism to keep their connection to the server alive. With outbound registrations the keep-alive process is handled by a separate, less resource intensive process, meaning that re-registrations (which are more resource-intensive) can be less frequent.
Outbound registration refresh minimum	The minimum allowed value for a SIP registration refresh period for outbound registrations. Requests for a value lower than this will result in the registration being rejected with a 423 Interval Too Brief response. The default is 300 seconds.	
Outbound registration refresh maximum	The maximum allowed value for a SIP registration refresh period for an outbound registration. Requests for a value greater than this will result in a lower value being returned (calculated according to the **Outbound registration refresh strategy**). The default is 3600 seconds.	

Field	Description	Usage tips
SIP registration proxy mode	Specifies how proxied registrations and requests containing Route Sets are handled when the Expressway receives a registration request for a domain for which it is not acting as a Registrar. *Off*: Registration requests are not proxied (but are still permitted locally if the Expressway is authoritative as a Registrar for that domain). Requests with existing Route Sets are rejected. *Proxy to known only*: Registration requests are proxied in accordance with existing call processing rules, but only to known neighbor, traversal client and traversal server zones. Requests containing Route Sets are proxied only if they were received from a known zone. *Proxy to any*: Registration requests are proxied in accordance with existing call processing rules to all known zones. Requests containing Route Sets are always proxied. The default is *Off*.	See Proxying Registration Requests for more information.

Authentication Controls

This section contains the device authentication controls for enabling delegated credential checking. The configurable options are:

Field	Description	Usage tips
Delegated credential checking	Controls whether the credential checking of SIP messages is delegated, via a traversal zone, to another Expressway. *Off:* Use the relevant credential checking mechanisms (local database, Active Directory Service or H.350 directory via LDAP) on the Expressway performing the authentication challenge. *On:* Delegate the credential checking to a traversal client. The default is *Off*.	**Note** Delegated credential checking must be enabled on both the traversal server and the traversal client. See delegated credential checking for more information.

Advanced SIP Settings

Field	Description	Usage tips
SIP max size	Specifies the maximum SIP message size that can be handled by the Expressway (in bytes). Default is 32768 bytes.	If you use Microsoft interop with dual-homed conferencing through Expressway and Meeting Server with an AVMCU invoked on the Microsoft side, we recommend 32768 or greater.
SIP TCP connect timeout	Specifies the maximum number of seconds to wait for an outgoing SIP TCP connection to be established. Default is 10 seconds.	You can reduce this to speed up the time between attempting a broken route (like an unavailable onward SIP proxy peer) and failing over to a good one. Be careful in high latency networks that you leave enough time for the connection to establish.

Retain Connection for Corrupt/Malformed SIP Message (CLI)

From X8.11, a CLI command (not the web user interface) is available to optionally configure the Expressway to keep a connection open even if it receives malformed or corrupt SIP messages. You can specify this for non-mandatory headers only, or for mandatory headers too. See Zones Zone [1..1000] Neighbor RetainConnectionOnParseErrorMode: <mode>.

Configuring Domains

The **Domains** page (**Configuration** > **Domains**) lists the SIP domains managed by this Expressway.

A domain name can comprise multiple levels. Each level's name can only contain letters, digits and hyphens, with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter. An example valid domain name is **100.example-name.com**.

Note Values shown in the **Index** column correspond to the numeric elements of the **%localdomain1%, %localdomain2%, . . . %localdomain200%** pattern matching variables.

You can configure up to 200 domains.

Note You cannot configure domains on an Expressway-E.

Configuring the Supported Services for Unified Communications (Expressway-C Only)

When the Expressway-C has been enabled for Unified Communications mobile and remote access, you must select the services that each domain will support. The options are:

- **SIP registrations and provisioning on Expressway:** The Expressway is authoritative for this SIP domain. The Expressway acts as a SIP registrar for the domain (and Presence Server in the case of VCS systems), and accepts registration requests for any SIP endpoints attempting to register with an alias that includes this domain. The default is *On*.
- **SIP registrations and provisioning on Unified CM:** Endpoint registration, call control and provisioning for this SIP domain is serviced by Unified CM. The Expressway acts as a Unified Communications gateway to provide secure firewall traversal and line-side support for Unified CM registrations. The default is *Off*.
- **IM and Presence Service:** Instant messaging and presence services for this SIP domain are provided by the Unified CM IM and Presence service. The default is *Off*.
- **XMPP federation:** Enables XMPP federation between this domain and partner domains. The default is *Off*.
- **Deployment:** Associates the domain with the selected deployment, if there are multiple deployments. This setting is absent if there is only one deployment (there is always at least one).

Any domain configuration changes, when one or more existing domains are configured for *IM and Presence services on Unified CM* or *XMPP Federation* will result in an automatic restart of the XCP router on both Expressway-C and Expressway-E.

The end-user impact is temporary loss of federation and any Jabber clients using mobile and remote access will be temporarily disconnected. The clients will automatically reconnect after a short period.

Configuring Delegated Credential Checking (Expressway-E Only)

If you have enabled delegated credential checking (**Configuration** > **Protocols** > **SIP**), you need to specify the traversal zone to use when delegating credential checks for SIP messages for this domain. This only applies to the SIP domains for which Expressway is acting as the service provider and SIP registrar.

You can specify a different zone for each SIP domain, if required.

Choose *Do not delegate* if you want to continue to use this Expressway-E to perform the credential checking.

Testing the credential checking service

To verify whether the Expressway to which credential checking has been delegated is able to receive messages and perform the relevant authentication checks:

Procedure

Step 1 Go to **Configuration** > **Domains**.

Step 2 Select the relevant domains.

Step 3 Click **Test credential checking service**.

The system displays a **Results** section and reports whether the receiving Expressway can be reached over the traversal zone and, additionally, if it is able to perform credential checking for both NTLM and SIP digest type challenges.

If you are not using NTLM authentication in your video network, and thus the receiving Expressway is not configured with a connection to an Active Directory Service, then the NTLM check will be expected to fail.

Configuring SIP and H.323 Interworking

The **Interworking** page (**Configuration** > **Protocols** > **Interworking**) lets you configure whether or not the Expressway acts as a gateway between SIP and H.323 calls. The translation of calls from one protocol to the other is known as “interworking”.

By default, the Expressway acts as a SIP–H.323 and H.323–SIP gateway but only if at least one of the endpoints that are involved in the call is locally registered. You can change this setting so that the Expressway acts as a SIP–H.323 gateway regardless of whether the endpoints involved are locally registered. You also have the option to disable interworking completely.

The options for the **H.323 <-> SIP interworking mode** are:

- *Off*: The Expressway does not act as a SIP–H.323 gateway.
- *Registered only*: The Expressway acts as a SIP–H.323 gateway but only if at least one of the endpoints is locally registered.
- *On*: The Expressway acts as a SIP–H.323 gateway regardless of whether the endpoints are locally registered.

Note We recommend that you leave this setting as *Registered only*. Unless your network is correctly configured, setting it to *On* (where all calls can be interworked) may result in unnecessary interworking, for example where a call between two H.323 endpoints is made over SIP, or vice versa.

Calls for which the Expressway acts as a SIP to H.323 gateway are RMS calls except when both the endpoints are registered to the Cisco infrastructure. The Expressway always takes the media for SIP–H.323 interworked calls so that it can independently negotiate payload types on the SIP and H.323 sides and Expressway will re-write these as the media passes.

Also in a SIP SDP negotiation, multiple codec capabilities can be agreed (more than one video codec can be accepted) and the SIP device is at liberty to change the codec it uses at any time within the call. If this happens, because Expressway is in the media path it will close and open logical channels to the H.323 device as the media changes (as required) so that media is passed correctly.

Configuring DH key length

X12.6 introduced support for 2048-bit Diffie-Hellman keys for H.323 call encryption, as part of the ongoing security enhancements for Expressway, so Expressway offers both 1024-bit and 2048-bit encryption key length as default behavior.

This may cause unexpected H.323 call failures if the deployed firewall's ALG function or endpoints are unable to handle both 1024-bit and 2048-bit for the Diffie-Hellman key exchange. In this case, from X12.6.4

administrators can optionally revert to 1024-bit encryption by using the CLI command `xConfiguration Interworking Encryption KeySize2048: <On/Off>`.

Changes to the interworking encryption key size do not need a restart to take effect. Changes to the primary node in a cluster are automatically replicated to its subsidiary nodes.

Searching by protocol

When searching a zone, the Expressway first performs the search using the protocol of the incoming call. If the search is unsuccessful the Expressway may then search the zone again using the alternative protocol, depending on where the search came from and the **Interworking mode**.

Note The zone must also be configured with the relevant protocols enabled (SIP and H.323 are enabled on a zone by default).

- If the request has come from a neighboring system and **Interworking mode** is set to *Registered only*, the Expressway searches the Local Zone using both protocols, and all other zones using the native protocol only (because it will interwork the call only if one of the endpoints is locally registered).
- If **Interworking mode** is set to *On*, or the request has come from a locally registered endpoint, the Expressway searches the Local Zone and all external zones using both protocols.

Enabling SIP endpoints to dial H.323 numbers

SIP endpoints can only make calls in the form of URIs — such as **name@domain**. If the caller does not specify a domain when placing the call, the SIP endpoint automatically appends its own domain to the number that is dialed.

So if you dial **123** from a SIP endpoint, the search will be placed for **123@domain**. If the H.323 endpoint being dialed is just registered as **123**, the Expressway will not be able to locate the alias **123@domain** and the call will fail. The solutions are to either:

- Ensure all your endpoints, both H.323 and SIP, register with an alias in the form **name@domain**.
- Create a pre-search transform on the Expressway that strips the **@domain** portion of the alias for those URIs that are in the form of **number@domain**.

  See the pre-search transforms section for information about how to configure pre-search transforms, and the stripping @domain for dialing to H.323 numbers section for an example of how to do this.

Interworking DTMF signals

For SIP calls, the Expressway implements RFC 2833 for DTMF signaling in RTP payloads.

For H.323 calls, the Expressway implements H.245 UserInputIndication for DTMF signaling. **dtmf** is the only supported **UserInputCapability**. Expressway does not support any other H.245 user input capabilities (for example, **basicString, generalString**)

When the Expressway is interworking a call between SIP and H.323, it also interworks the DTMF signaling, but only between RFC 2833 DTMF, and the H.245 user input indicators “dtmf” and “basicString”.