音声機能の設定

この章では、Cisco Catalyst 8000 Edge プラットフォームでの音声機能の設定について説明します。

この章の内容は、次のとおりです。

コール ウェイティング

コール待機機能を使用すると、別のコールでの通話中に、別のコールを受信できます。別のコールが着信すると、コール ウェイティング トーン（300 ms 間のトーン）が聞こえます。発信者 ID がサポートされる電話機には、発信者 ID が表示されます。フックフラッシュを使用して、待ち状態のコールに応答し、アクティブだったコールを保留状態にできます。フックフラッシュを使用すると、アクティブ コールと保留中のコールとの間を入れ替えることができます。コール ウェイティング機能がディセーブルの場合に、現在のコールを終了した場合、2 つ目のコールではビジー トーンが聞こえます。コールウェイティングの詳細については、https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/sip/configuration/15-mt/sip-config-15-mt-book/voi-sip-hookflash.html を参照してください。

着信転送

コール転送は、2 つ目のコールが 2 人のユーザ間で確立される間に、アクティブ コールが保留状態にされることです。2 つ目のコールを確立して、アクティブ コールを終了した後に、保留中のコールでは、リングバックが聞こえます。コール転送機能によって、ブラインド、準在席、在席の、コール転送の 3 つのタイプすべてがサポートされます。

機能グループ D の設定

機能グループ D シグナリングを設定するには、次の手順を実行します。

始める前に

機能グループ D サービスは、電話の顧客が長距離ネットワークを選択し、使用するキャリアに関係なく同じ桁数の番号を使用できるトランク側接続です。ルータは、キャリア環境内の音声トラフィックをサポートするために、機能グループ D を使用して長距離通信事業者とインターフェイス接続します。

この設定を開始する前に、次の前提条件が満たされていることを確認してください。

- プラットフォームでは、デジタル T1/E1 パケット音声トランク ネットワーク モジュールが使用されている必要があります。
- デジタル T1/E1 パケット音声トランク ネットワーク モジュールには、音声/WAN インターフェイス ネットワーク モジュール（NIM）用のスロットを 1 つまたは 2 つ搭載できます。NIM は 1 ー 8 個のポートをサポートします。デジタル E1 パケット音声トランク ネットワーク モジュールでは、デュアルモード（音声/WAN）マルチトランクカードのみがサポートされ、古い VIC はサポートされません。
- ドロップアンドインサート機能は、複数の同じカード上の 2 つのポート間でのみサポートされます。

手順の概要

1. **configure terminal** {*ip-address* | *interface-type interface-number* [*ip-address*]}
2. **voice-card slot/subslot**
3. **controller T1/E1 slot/subslot/port**
4. **framing** {*sf* | *esf* }
5. **linecode** {*b8zs* | *ami*}
6. **ds0-group** *ds0-group-no***timeslots** *timeslot-list type*{*e&m-fgd* | *fgd-eana*}
7. **no shutdown**
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** {*ip-address* | *interface-type interface-number* [*ip-address*]} 例： `Router(config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**voice-card slot/subslot** 例： `Router(config)# voice-card slot/subslot`	音声カードインターフェイス コンフィギュレーション モードを開始し、使用中のルータに応じて 0 ー 5 の値を使用してスロットの場所を指定します。
ステップ 3	**controller T1/E1 slot/subslot/port** 例： `Router(config)# controller T1 slot/subslot/port`	指定されたスロット/ポートの場所で、T1 コントローラのコントローラ コンフィギュレーション モードを開始します。スロットとポートの有効な値は 0 と 1 です。
ステップ 4	**framing** {*sf* | *esf* } 例： `Router(config)# framing {sf | esf}`	サービスプロバイダーの指示に従って、フレーミングを設定します。Extended Superframe（ESF）形式または Superframe（SF）形式を選択します。
ステップ 5	**linecode** {*b8zs* | *ami*}	サービスプロバイダーの指示に従って、回線エンコーディングを設定します。Bipolar-8 Zero Substitution（B8ZS）では、回線コーディング違反を検出するために、連続した 8 つの 0 を一意のバイナリシーケンスにエンコードします。Alternate Mark Inversion（AMI）では、各ビットセルで 01 を使用してゼロを表し、各ビットセルで 11 または 00 を交互に使用して 1 を表します。AMI では、送信側デバイスが ones density を維持する必要があります。ones density がデータストリームと無関係に維持されることはありません。
ステップ 6	**ds0-group** *ds0-group-no* **timeslots** *timeslot-list type*{*e&m-fgd* | *fgd-eana*}	圧縮音声コールで使用される T1 チャネルと、ルータが PBX または CO に接続するために使用するシグナリング方法を定義します。ds0-group-no は、DS0 グループを特定する 0 ～ 23 の値です。（注）ds0-group コマンドは、slot/port:ds0-group-no の形式で番号が付けられた論理音声ポートを自動的に作成します。作成される音声ポートは 1 つだけですが、該当するコールはグループ内の任意のチャネルにルーティングされます。timeslot-list は、単一の数字、カンマで区切られた複数の数字、またはタイムスロットの範囲を示すハイフンで区切られた数字のペアです。T1 に指定できる値は 1 ー 24 です。個々の DS0 タイムスロットをマッピングするには、追加のグループを定義します。システムは、定義された各グループに追加の音声ポートをマッピングします。タイプに応じたシグナリング方式の選択は、構築する接続によって異なります。e&m-fgd 設定では、

	コマンドまたはアクション	目的
		PBX トランク回線（タイ回線）および電話機器の E&M インターフェイス接続で、機能グループ D のスイッチアクセスサービスを使用できます。fgd-eana 設定では、Exchange Access North American（EANA）シグナリングがサポートされます。
ステップ 7	**no shutdown**	コントローラをアクティブにします。
ステップ 8	**exit**	コントローラ コンフィギュレーション モードを終了します。ドロップアンドインサートを設定しない場合は、次の手順をスキップします。

メディア認証およびシグナリング認証と暗号化

Cisco IOS MGCP ゲートウェイのメディアおよびシグナリング認証および暗号化機能により、MGCP ゲートウェイでのメディアおよびシグナリング暗号化に加えて、シグナリング認証を含む音声セキュリティ機能が導入されます。メディアおよびシグナリング認証および暗号化機能の詳細については、http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/mgcp/configuration/15-mt/vm-15-mt-book/vm-gw-med-sig.html を参照してください。

マルチキャスト保留音

保留音（MOH）機能を使用すると、Cisco IOS MGCP 音声ゲートウェイを使用しているときに、音楽ストリーミングサービスに登録できます。MOH サーバーから、保留になっているオンネットおよびオフネットの発信者の音声インターフェイスに音楽がストリーミングされます。Cisco Communications Manager は、ストリーミング マルチキャスト MOH サーバーから提供される音楽を保留中のコールの発信者に再生する機能をサポートしています。

Cisco Unified Communications Manager またはゲートウェイに事前設定されたマルチキャストアドレスを使用することで、ゲートウェイは、ネットワークのデフォルトルータからブロードキャストされる Real-Time Transport Protocol（RTP）パケットを「リッスン」し、ネットワーク内の指定された音声インターフェイスにパケットをリレーできます。保留中のコールを開始できます。ただし、MGCP 制御アナログ電話機で保留音を開始することはできません。着信側が発信側を保留にするたびに、Cisco Communications Manager は、事前設定されたマルチキャストアドレスを介して RTP パケットを「保留」になっているインターフェイスにストリーミングするように MOHサーバーに要求します。このようにして、RTP パケットは、適切に設定された保留状態の音声インターフェイスにリレーされます。ゲートウェイでマルチキャストアドレスを設定すると、ゲートウェイは、デフォルトルータにインターネットゲートウェイ管理プロトコル（IGMP）「join」メッセージを送信し、RTP マルチキャストパケットを受信する準備ができたことを示します。

複数の MOH サーバーが同じネットワークに存在する可能性がありますが、各サーバーには異なるクラス D IPアドレスが必要であり、そのアドレスは Cisco Communications Manager と MGCP

音声ゲートウェイで設定する必要があります。MOH の設定の詳細については、http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cminterop/configuration/15-0m/vc-15-0m-book/vc-ucm-mgcp-gw.html#GUID-A3461142-2F05-4420-AEE6-032FCA3B7952 を参照してください。

SCCP ゲートウェイでの TLS 1.2 のサポート

「SCCP ゲートウェイでの TLS 1.2 サポート」では、ユニキャスト会議ブリッジを含むデジタルシグナルプロセッサ（DSP）ファームの SCCP プロトコルでの TLS 1.2 設定について詳しく説明します。

（CFB）、メディア ターミネーション ポイント（MTP）、および SCCP テレフォニー制御（STC）アプリケーション（STCAPP）。

ゲートウェイ上の DSP は、変換またはトランスコーディングのメディアリソースとして使用できます。各メディアリソースは、Secure Skinny Client Control Protocol（SCCP）を使用して Cisco Unified Communications Manager と通信します。現在、TLS 1.0 と同等の SSL 3.1 がセキュアな信号の送信に使用されています。この機能により、TLS 1.2 のサポートが強化されます。Cisco IOS XE Cupertino 17.7.1a 以降、TLS 1.2 が拡張され、次世代暗号化（NGE）暗号スイートをサポートするようになりました。

（注） Cisco Unified Communications Manager（CUCM）バージョン 14SU2 は、AA:22:BB:44:55 または AA22BB4455 のように、コロン付きまたはコロンなしのサブジェクト名フィールド（CN 名）を持つセキュアな SCCP ゲートウェイをサポートするように拡張されました。

CUCM は、SCCP ゲートウェイからの着信証明書の CN フィールドを確認し、このゲートウェイの CUCM に設定された DeviceName と照合して確認します。DeviceName には、ゲートウェイの MAC アドレスが含まれています。CUCM は、DeviceName の MAC アドレスをコロン付きの MAC アドレスに変換し（AA:22:BB:44:55 など）、ゲートウェイの証明書の CN 名で検証します。したがって、CUCM では、ゲートウェイが証明書内の CN フィールド、つまりサブジェクト名にコロン付きの MAC アドレスの使用が求められています。

国防情報システム局（DISA）の新しいガイドラインにより、サブジェクト名フィールド CN にはコロンを使用しないことが要件となっています。たとえば、AA22BB4455 です。

SCCP TLS 接続

CiscoSSL は OpenSSL に基づいています。SCCP は CiscoSSL を使用して通信信号を保護します。

リソースがセキュアモードで設定されている場合、SCCP アプリケーションは、Transport Layer Security（TLS）ハンドシェイクを完了するプロセスを開始します。ハンドシェイクの際、サーバーは、サポートされている TLS バージョンと暗号スイートに関する情報を CiscoSSL に送信します。以前は、SCCP セキュアシグナリングでは SSL 3.1 のみがサポートされていました。SSL 3.1 は TLS 1.0 と同等です。TLS 1.2 サポート機能は、SCCP セキュアシグナリングに TLS 1.2 サポートを導入します。

TLS ハンドシェイクが完了すると、SCCP に通知され、SCCP はプロセスを強制終了します。

ハンドシェイクが正常に完了すると、REGISTER メッセージがセキュアトンネル経由で Cisco Unified Communications Manager に送信されます。ハンドシェイクが失敗し、再試行が必要な場合は、新しいプロセスが開始されます。

（注） SCCP ベースのシグナリングでは、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートのみがサポートされます。

暗号スイート

SCCP ベースのシグナリングでは、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートがサポートされます。

Cisco IOS XE Cupertino 17.7.1a 以降、次の NGE 暗号スイートもサポートされます。

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384

これらの暗号スイートにより、STCAPP アナログ電話と SCCP DSPFarm 会議サービスの両方でセキュアな音声シグナリングが可能になります。暗号スイートの選択は、ゲートウェイと CUCM の間でネゴシエートされます。

NGE 暗号スイートを使用するには、次の前提条件が適用されます。

- TLS 1.2 を設定します。詳細については、STC アプリケーションの TLS バージョンの設定（7 ページ）を参照してください。
- CUCM リリース 14.1 SU1 以降、および TLS 1.2 をサポートする音声ゲートウェイまたはプラットフォームを使用します。
- CUCM Web UI から、[Cipher Management] に移動し、[CIPHER switch] を [NGE] として設定します。詳細については、「暗号管理」を参照してください。

暗号スイートの確認の詳細については、TLS バージョンと暗号スイートの確認 （7 ページ）を参照してください。

SRTP で暗号化されたメディアの場合、より高度な暗号スイート（AEAD-AES-128-GCM または AEAD-AES-256-GCM）を使用できます。これらの暗号スイートの選択は、セキュアなアナログ音声とハードウェア会議ブリッジ音声メディアの両方について、GW と CUCM との間で自動的にネゴシエートされます。Authenticated Encryption with Associated Data（AEAD）暗号は、メッセージの完全性を検証する組み込みの SHA アルゴリズムを使用せずに機密性、完全性、および信頼性を同時に実現します。

サポートされるプラットフォーム

SCCP ゲートウェイ機能での TLS 1.2 サポートは、次のプラットフォームで使用できます。

- Cisco Catalyst 8200 および 8300 シリーズ エッジ プラットフォーム

STC アプリケーションの TLS バージョンの設定

STC アプリケーションの TLS バージョンを設定するには、次のタスクを実行します。

```
enable
configure terminal
stcapp security tls-version v1.2
exit
```

（注） stcapp security tls コマンドは、TLS バージョンをv.1.0、v1.1、または v1.2 のみに設定します。明示的に設定されない場合は、デフォルトで TLS v1.0 が選択されます。

DSP ファームプロファイルに対するセキュアモードでの TLS バージョンの設定

DSP ファームプロファイルの TLS バージョンをセキュアモードで設定するには、次のタスクを実行します。

```
enable
configure terminal
dspfarm profile 7 conference security
  tls-version v1.2
  exit
```

（注） 注意： **tls** コマンドは、セキュリティモードでのみ設定できます。

TLS バージョンと暗号スイートの確認

TLS バージョンと暗号スイートを確認するには、次のタスクを実行します。

```
# show dspfarm profile 100
Dspfarm Profile Configuration

 Profile ID = 100, Service = CONFERENCING, Resource ID = 2
 Profile Service Mode : secure
 Trustpoint : Overlord_DSPFarm_GW
 TLS Version  : v1.2
 TLS Cipher   : ECDHE-RSA-AES256-GCM-SHA384
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : UP
 Total Number of Resources Configured : 10
 Total Number of Resources Available : 10
 Total Number of Resources Out of Service : 0
 Total Number of Resources Active : 0
 Maximum conference participants : 8
 Codec Configuration: num_of_codecs:6
 Codec : g711ulaw, Maximum Packetization Period : 30 , Transcoder: Not Required
 Codec : g711alaw, Maximum Packetization Period : 30 , Transcoder: Not Required
 Codec : g729ar8, Maximum Packetization Period : 60 , Transcoder: Not Required
 Codec : g729abr8, Maximum Packetization Period : 60 , Transcoder: Not Required
 Codec : g729r8, Maximum Packetization Period : 60 , Transcoder: Not Required
 Codec : g729br8, Maximum Packetization Period : 60 , Transcoder: Not Required
```

STCAPP アプリケーションの TLS バージョンの確認

STCAPP アプリケーションの TLS バージョンを確認するには、次のタスクを実行します。

```
Device# show call application voice stcapp
App Status: Active
CCM Status: UP
CCM Group: 120
Registration Mode: CCM
Total Devices: 0
Total Calls in Progress: 0
Total Call Legs in Use: 0
ROH Timeout: 45
TLS Version: v1.2

# show stcapp dev voice 0/1/0
Port Identifier:  0/1/0
Device Type:      ALG
Device Id:        585
Device Name:      ANB3176C85F0080
Device Security Mode : Encrypted
  TLS version        : TLS version 1.2
  TLS cipher         : ECDHE-RSA-AES256-GCM-SHA384
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 80010
Dial Peer(s):     100
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:       STCAPP_CC_EV_CALL_MODIFY_DONE
Line State:       ACTIVE
Line Mode:        CALL_CONF
Hook State:       OFFHOOK
mwi:              DISABLE
vmwi:             OFF
mwi config:       Both
Privacy:          Not configured
HG Status:        Unknown
PLAR:             DISABLE
Callback State:   DISABLED
CWT Repetition Interval: 0 second(s) (no repetition)
Number of CCBs:   1
Global call info:
    Total CCB count      = 3
    Total call leg count = 6

Call State for Connection 2 (ACTIVE): TsConnected
Connected Call Info:
   Call Reference: 33535871
   Call ID (DSP):  187
   Local IP Addr:  198.51.100.2
   Local IP Port:  8234
   Remote IP Addr: 198.51.100.20
   Remote IP Port: 8154
   Calling Number: 80010
   Called Number:
   Codec:          g711ulaw
   SRTP:           on
   RX Cipher:      AEAD_AES_256_GCM
   TX Cipher:      AEAD_AES_256_GCM
```

DSPfarm 接続の sRTP 暗号スイートを確認するには、次のタスクを実行します。

```
# show sccp connection detail

bridge-info(bid, cid) - Normal bridge information(Bridge id, Calleg id)
mmbridge-info(bid, cid) - Mixed mode bridge information(Bridge id, Calleg id)

sess_id    conn_id    call-id    codec   pkt-period dtmf_method    type
bridge-info(bid, cid)   mmbridge-info(bid, cid) srtp_cryptosuite          dscp
                        call_ref   spid       conn_id_tx

16778224   -          125        N/A     N/A        rfc2833_pthru     confmsp   All
RTPSPI Callegs      All MM-MSP Callegs      N/A                       N/A
                        -          -          -

16778224   16777232   126        g711u   20         rfc2833_pthru  s- rtpspi    (101,125)
                N/A                        AEAD_AES_256_GCM          184
                        30751576   16777219   -

16778224   16777231   124        g711u   20         rfc2833_pthru  s- rtpspi    (100,125)
                N/A                        AEAD_AES_256_GCM          184
                        30751576   16777219   -


Total number of active session(s) 1, connection(s) 2, and callegs 3
```

コール情報の確認

フォワーディング プレーン インターフェイス（FPI）に保存されている TDM コールと IVR コールのコール情報を表示するには、**showvoipfpi calls** コマンドを使用します。コール ID を選択し、**show voip fpi calls confID** *call_id_number* コマンドを使用して暗号スイートを確認できます。次の例では、暗号スイート 6 は AES_256_GCM です。

```
#show voip fpi calls
Number of Calls : 2
---------- ---------- ---------- ---------- --------------- ---------------
    confID correlator    AcallID     BcallID           state           event
---------- ---------- ---------- ---------- --------------- ---------------
         1          1         87         88       ALLOCATED DETAIL_STAT_RSP
        21         21         89         90       ALLOCATED DETAIL_STAT_RSP

#show voip fpi calls confID 1
--------------------------------------------------------------------------------
VoIP-FPI call entry details:
--------------------------------------------------------------------------------
Call Type        :           TDM_IP     confID           :                1
correlator       :                1     call_state       :        ALLOCATED
last_event       :  DETAIL_STAT_RSP     alloc_start_time :       1796860810
modify_start_time:                0     delete_start_time:                0
Media Type(SideA):             SRTP     cipher suite     :                6
--------------------------------------------------------------------------------
FPI State Machine Stats:
------------------------
create_req_call_entry_inserted              :         1
……
```

表 *1 : SCCP* ゲートウェイでの *TLS 1.2* サポートの機能情報

機能名	リリース	機能情報
NGE 暗号スイートのサポート	Cisco IOS XE Cupertino 17.7.1a	この機能は、セキュアな音声シグナリングとセキュアなメディアでのNGE暗号スイートをサポートします。これらの暗号スイートは、STCAPP アナログ電話と SCCP DSPFarm 会議サービスの両方に適用できます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。