CHAPTER **10**

SBC multi-VRF の実装

Session Border Controller（SBC; セッション ボーダ コントローラ）は、Customer Edge（CE; カスタマー エッジ）デバイスで multiple-VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）をサポートしています。この機能を使用すると、Provider Edge（PE; プロバイダー エッジ）がパケットを相互に再配布している場合に、PE チェックを抑制することによってループを防止できます。

（注） VRF は、Data Border Element（DBE）メディア アドレスおよび SBE AAA/H248 制御アドレスでだけサポートされます。DBE H248 制御アドレスは VRF をサポートしていません。

（注） ACE SBC Release 3.0.00 以降のリリースでは、この機能は統合モデルと分散モデルの両方でサポートされます。

この章で使用されているコマンドの詳細については、第 39 章「Cisco セッション ボーダ コントローラ コマンド」を参照してください。この章に記載されたその他のコマンドのマニュアルを特定するには、コマンド リファレンスのマスター インデックスを使用するか、またはオンラインで検索してください。

SBC multi-VRF の実装機能の履歴

リリース	変更内容
ACE SBC Release 3.0.1	VRF-Aware DNS 照会のサポートが追加されました。
ACE SBC Release 3.0.00	SBC 統合モデルのサポートが追加されました。 次のセクションが追加されました。 • multi-VRF の設定 • H.323 隣接への VRF の関連付け • SIP 隣接への VRF の関連付け
ACE SBC Release 2.0.00	Cisco 7600 シリーズ ルータにこの機能が追加されました。

この章の構成

この章で説明する内容は、次のとおりです。

- 「multi-VRF を実装するための設定例」（P.10-16）

前提条件 - multi-VRF の実装

次に、SBC multi-VRF を実装するための前提条件を示します。

- Application Control Engine（ACE）モジュールで SBC コマンドを入力するには、Admin ユーザである必要があります。詳細については、次の URL にある『*Application Control Engine Module Administration Guide*』を参照してください。
http://www.cisco.com/en/US/products/hw/modules/ps2706/products_configuration_guide_book09186a00806838f4.html
- multi-VRF を実装する前に、SBC を作成しておく必要があります。第 2 章「SBC の ACE を設定するための前提条件」に記載された手順に従ってください。

multi-VRF の実装について

カスタマー エッジ（CE）デバイス（つまりカスタマー側ルータ）で SBC の multi-VRF サポート機能を使用すると、PE がパケットを相互に再配布している場合に、PE チェックを抑制することによってループを防止できます。通常は複数のルータが実行するタスクを、1 台のルータだけで実行できます。multi-VRF は、MPLS および BGP の機器が搭載されていないネットワーク上で実行できます。

VRF を PE ではないルータで使用する場合は、VRF ルーティング テーブルに IP プレフィクスへのルートを正しく入力できるように、PE チェックをオフにすることができます。ローエンド システムでは Virtual Private Network（VPN; バーチャル プライベート ネットワーク）機能が完全にはサポートされていないため、multi-VRF は重要です。multi-VRF では、1 台のルータ内でルーティング インスタンス（および暗黙的にアドレス空間）を論理的に分割できます。

次に、multi-VRF の機能を示します。

- 単一の物理的なルータを複数の仮想ルータに分割できます。各仮想ルータには独自のインターフェイス、ルーティング テーブル、および転送テーブルが含まれます。SBC は、カスタマーごとに複数の（重複および独立した）ルーティング テーブル（アドレッシング）をサポートしています。単一のルータ内でルーティング ドメインを分割するには、仮想ルーティング コンテキストを使用します。
- multi-VRF は、複数のルータが必要であるものの、1 台のルータしか使用できない場所で使用できます。
- 1 つの物理インターフェイスを複数の仮想ルータに所属させるには、サブインターフェイス（フレームリレー、ATM、VLAN）を使用します。
- BGP および MPLS は使用しません。
- VRF 間に接続を確立しません（VRF 間で内部的にエクスポートおよびインポートを行うには、BGP を使用する必要があります）。
- 同じ VPN サイトの 2 つのエンドポイント間にコールを配置すると、SBC はそのエンドポイント間で直接メディアをルーティングして、ネットワーク使用率を削減できます。
- SBC で multi-VRF を実現すると、両方のエンドポイントが同じ VPN にある場合には、メディア バイパスを有効にして、最適化を図ることができます。

ACE SBC Release 3.0.00 の場合、デフォルトでは同じ VPN 上のすべての隣接でメディア バイパスが有効になっています。メディア バイパスをオフにするには、**media-bypass-forbid** コマンドを使用します（このコマンドは、CAC ポリシー専用に実装されます）。

（注）　隣接での VRF 名は、コンテキスト名に一致する必要があります。

VRF-Aware DNS 照会

この機能により、SBC は VRF ごとに DNS を照会できます。ACE SBC Release 3.0.1 以前の場合、すべての DNS 照会は Admin コンテキスト内で実行されていました。この機能を使用すると、コンテキストごとに DNS 照会を実行できます。

multi-VRF の実装

SBC multi-VRF の実装については、次の項を参照してください。

- 「multi-VRF の設定」（P.10-3）
- 「SIP 隣接への VRF の関連付け」（P.10-12）
- 「DBE への VRF の設定 - 分散モデル専用」（P.10-14）

multi-VRF の設定

このタスクでは、SBC が統合配置モードの multi-VRF モードで実行されるルータを設定します。インターフェイスと SBC の Service Virtual Interface（SVI）、隣接、および DBE メディア アドレスとの関係を必要に応じて書き留めておきます。

手順概要

1. **configure**
2. **context vrf**
3. **allocate-interface**
4. **exit**
5. **ft peer**
6. **heartbeat interval**
7. **heartbeat count**
8. **ft-interface vlan**
9. **exit**
10. **ft group**
11. **peer**
12. **priority**
13. **peer priority**
14. **associate-context**
15. **inservice**
16. **ft group**

17. **peer**
18. **priority**
19. **peer priority**
20. **associate-context**
21. **inservice**
22. **exit**
23. **exit**
24. **changeto**
25. **configure**
26. **interface vlan**
27. **ip address**
28. **alias**
29. **peer ip address**
30. **no shutdown**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** host1/Admin# configure host1/Admin(config)#	ACE モジュール コンフィギュレーション モードを開始します。
ステップ 2	**context** **例：** host1/Admin(config)# context my_vrf1	コンテキストを作成します。 **（注）** 隣接での VRF 名は、コンテキスト名に一致する必要があります。 例では、新しいコンテキスト my_vrf1 を作成します。
ステップ 3	**allocate-interface vlan** **例：** host1/Admin(config-context)# allocate-interface vlan 100	VLAN 100 をコンテキスト my_vrf1 に割り当て、VLAN 100 用に分類されたトラフィックをコンテキストが受信できるようにします。
ステップ 4	**exit** **例：** host1/Admin(config)# exit	config-context モードを終了します。
ステップ 5	**ft peer** **例：** host1/Admin(config)# **ft peer 1** host1/Admin(config-ft-peer)#	FT ピアを設定し、FT ピア コンフィギュレーション モードにアクセスします。

	コマンドまたはアクション	目的
ステップ 6	**heartbeat interval** frequency **例：** host1/Admin(config-ft-peer)# **heartbeat interval 100**	アクティブ FT ピアとスタンバイ FT ピア間での検証タイミング用にハートビート インターバルを設定します。
ステップ 7	**heartbeat count** number **例：** host1/Admin(config-ft-peer)# **heartbeat count 10**	アクティブ FT ピアとスタンバイ FT ピア間での検証タイミング用にハートビート カウントを設定します。
ステップ 8	**ft-interfac vlan** *vlan_id* **例：** host1/Admin(config-ft-peer)# **ft-interface vlan 99**	既存の FT VLAN をピアに関連付けます。
ステップ 9	**exit** **例：** host1/Admin(config)# exit	config-ft-peer モードを終了します。
ステップ 10	**ft group** **例：** host1/Admin(config)# ft group 1 host1/Admin(config-ft-group)#	デフォルト（Admin）コンテキストで FT グループ 1 を設定します。
ステップ 11	**peer** **例：** host1/Admin(config-ft-group)# peer 1	ピア ACE を FT グループに関連付けます。
ステップ 12	**priority** **例：** host1/Admin(config-ft-group)# priority 150	アクティブ グループ メンバーのプライオリティを設定します。
ステップ 13	**peer priority** **例：** host1/Admin(config-ft-group)# peer priority 50	リモート スタンバイ メンバー上の FT グループのプライオリティを設定します。
ステップ 14	**associate-context** **例：** host1/Admin(config-ft-group)# associate-context my_vrf1	コンテキストを FT グループに関連付けます。
ステップ 15	**inservice** **例：** host1/Admin(config-ft-group)# inservice	FT グループを稼動させます。

	コマンドまたはアクション	目的
ステップ 16	**ft group** **例：** host1/Admin(config)# ft group 2 host1/Admin(config-ft-group)#	Admin 以外のコンテキストで別の FT グループを設定します。
ステップ 17	**peer** **例：** host1/Admin(config-ft-group)# peer 1	ピア ACE を FT グループに関連付けます。
ステップ 18	**priority** **例：** host1/Admin(config-ft-group)# priority 150	アクティブ グループ メンバーのプライオリティを設定します。
ステップ 19	**peer priority** **例：** host1/Admin(config-ft-group)# peer priority 50	リモート スタンバイ メンバー上の FT グループのプライオリティを設定します。
ステップ 20	**associate-context** **例：** host1/Admin(config-ft-group)# associate-context my_vrf1	コンテキストを FT グループに関連付けます。
ステップ 21	**inservice** **例：** host1/Admin(config-ft-group)# inservice	FT グループを稼動させます。
ステップ 22	**exit** **例：** host1/Admin(config-ft-group)# exit	config-ft-group モードを終了します。
ステップ 23	**exit** **例：** host1/Admin(config)# exit	config モードを終了します。
ステップ 24	**changeto** **例：** host1/Admin# changeto my_vrf1 Router/vrf1#	ACE 上のあるコンテキストを別のコンテキストに移動します。
ステップ 25	**configure** **例：** host1/my_vrf1# configure host1/(config)#	コンテキスト *my_vrf1* の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 26	**interface vlan** **例：** `host1/vrf1(config)# interface vlan 100`	VLAN インターフェイスを作成します。 例では、VLAN 100 を使用して、SVI を作成します。VLAN は、ステップ 3 で Admin コンテキストからこのコンテキストに割り当てたものです。
ステップ 27	**ip address** **例：** `host1/vrf1(config-if)# ip address 77.101.1.2 255.255.255.0`	IP アドレスを VLAN インターフェイスに割り当てます。
ステップ 28	**alias** **例：** `host1/vrf1(config-if)# alias 77.101.1.100 255.255.255.0`	VLAN インターフェイスのアクティブ モジュールとスタンバイ モジュール間の IP アドレスを設定します。
ステップ 29	**peer ip address** **例：** `host1/vrf1(config-if)# peer ip address 77.101.1.3 255.255.255.0`	VLAN インターフェイス用のスタンバイ モジュールの IP アドレスを設定します。
ステップ 30	**no shutdown** **例：** `host1/my_vrf1(config-if)# no shutdown`	インターフェイスを使用できるようにイネーブルにします。

VRF-Aware DNS 照会の設定

このタスクでは、DNS 照会を VRF 用に設定します。

手順概要

1. **configure**
2. **context vrf**
3. **allocate-interface vlan**
4. **exit**
5. **sbc** *sbc-name*
6. **sbe**
7. **sip dns**
8. **cache-lifetime** *0-1879048*
9. **cache-limit** *0-4294967295*
10. **exit**
11. **adjacency sip** *adjacency-name*
12. **vrf** *vrf_name*
13. **exit**

14. **exit**
15. **exit**
16. **exit**
17. **changeto** *context_name*
18. **configure**
19. **ip domain-lookup**
20. **ip domain-name**
21. **ip name-server**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `host1/Admin# configure`	ACE モジュール コンフィギュレーション モードを開始します。
ステップ 2	**context** **例：** `host1/Admin(config)# context my_vrf1`	コンテキストを作成します。 **（注）** 隣接での VRF 名は、コンテキスト名に一致する必要があります。 例では、新しいコンテキスト my_vrf1 を作成します。
ステップ 3	**allocate-interface vlan** **例：** `host1/Admin(config-context)# allocate-interface vlan 100`	VLAN 100 をコンテキスト my_vrf1 に割り当て、VLAN 100 用に分類されたトラフィックをコンテキストが受信できるようにします。
ステップ 4	**exit** **例：** `host1/Admin(config)# exit`	現在のモードを終了します。
ステップ 5	**sbc** *sbc-name* **例：** `host1/Admin(config)# sbc mySbc`	SBC 上に SBC サービスを作成し、SBC コンフィギュレーション モードを開始します。
ステップ 6	**sbe** **例：** `host1/Admin(config-sbc)# sbe`	SBC 上に SBE サービスを作成し、SBC-SBE コンフィギュレーション モードを開始します。
ステップ 7	**sip dns** **例：** `host1/Admin(config-sbc-sbe)# sip dns`	SIP DNS 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 8	**cache-lifetime** *0-1879048* **例：** `host1/Admin(config-sbe-dns)# cache-lifetime 444`	DNS キャッシュ内の DNS エントリのライフタイムを設定します。
ステップ 9	**cache-limit** *0-4294967295* **例：** `host1/Admin(config-sbe-dns)# cache-limit 14`	DNS キャッシュの最大許容エントリ数を設定します。
ステップ 10	**exit** **例：** `host1/Admin(config-sbe-dns)# exit`	現在のモードを終了します。
ステップ 11	**adjacency sip** *adjacency-name* **例：** `host1/Admin(config-sbc-sbe)# vrf vpn3`	SBC サービスの隣接を設定します。
ステップ 12	**vrf** *vrf_name* **例：** `host1/Admin(config-sbc-sbe-adj-sip)# vrf vpn3`	特定の VPN に接続されている SIP 隣接を設定します。
ステップ 13	**exit** **例：** `host1/Admin(config-sbc-sbe-adj-sip)# exit`	現在のモードを終了します。
ステップ 14	**exit** **例：** `host1/Admin(config-sbc-sbe-adj)# exit`	現在のモードを終了します。
ステップ 15	**exit** **例：** `host1/Admin(config-sbe)# exit`	現在のモードを終了します。
ステップ 16	**exit** **例：** `host1/Admin(config)# exit`	現在のモードを終了します。
ステップ 17	**changeto** *context_name* **例：** `host1/Admin# changeto vrf120`	ACE 上のあるコンテキストを別のコンテキストに移動します。
ステップ 18	**configure** **例：** `host1/Admin# configure`	ACE モジュール 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 19	**ip domain-lookup** **例：** host1/Admin(config)# ip domain-lookup	ACE モジュールが DNS サーバを使用してドメイン検索（ホストとアドレスとの変換）を実行できるようにします。
ステップ 20	**ip domain-name** **例：** host1/Admin(config)# ip domain-name cisco.com	デフォルトのドメイン名を設定します。
ステップ 21	**ip name-server** **例：** host1/Admin(config)# ip name-server 192.168.12.15	ACE モジュール上で DNS ネーム サーバを設定します。最大 3 つの DNS ネーム サーバを設定できます。

H.323 隣接への VRF の関連付け

このタスクでは、H.323 隣接を VPN に関連付けます。

手順概要

1. **adjacency h323** *adjacency-name*
2. **vrf** *vrf_name*
3. **signaling-address ipv4** *local_signaling_IP_address*
4. **signaling-port** *port_num*
5. **remote-address ipv4** *remote_IP_address/prefix*
6. **signaling-peer** [**gk**] *peer_address*
7. **signaling-peer-port** *port_num*
8. **account** *account_name*
9. **media-bypass** (Optional command)
10. **media-bypass-forbid**
11. **attach**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**adjacency h323** *adjacency-name* **例：** host1/Admin(config-sbc-sbe)# adjacency h323 h323my_vrf1 host1/Admin(config-sbc-sbe-adj-h323)#	SBE H.323 隣接モードを開始します。 • サービス名を定義するには、*adjacency-name* 引数を使用します。

	コマンドまたはアクション	目的
ステップ 2	**vrf** *vrf_name* **例：** host1/Admin(config-sbc-sbe-adj-h323)# vrf my_vrf1	H.323 隣接を特定の VPN に接続します。 **（注）**　隣接での VRF 名は、コンテキスト名に一致する必要があります。
ステップ 3	**signaling-address ipv4** *local_signaling_IP_address* **例：** host1/Admin(config-sbc-sbe-adj-h323)# signaling-address ipv4 88.88.101.11	H.323 隣接のローカル IPv4 シグナリング アドレスを指定します。
ステップ 4	**signaling-port** *port_num* **例：** host1/Admin(config-sbc-sbe-adj-h323)# signaling-port 1720	H.323 隣接のローカル シグナリング ポートを指定します。
ステップ 5	**remote-address ipv4** *ipv4_IP_address/prefix* **例：** host1/Admin(config-sbc-sbe-adj-h323)# remote-address ipv4 10.10.101.4 255.255.255.255	隣接経由で通信するリモート シグナリング ピアのセットを、指定の IP アドレス プレフィクスを持つピアに制限します。
ステップ 6	**signaling-peer** [**gk**] *peer_address* **例：** host1/Admin(config-sbc-sbe-adj-h323)# signaling-peer gk 10.10.101.4	H.323 隣接が使用するリモート シグナリング ピアを指定します。
ステップ 7	**signaling-peer-port** *port_num* **例：** host1/Admin(config-sbc-sbe-adj-h323)# signaling-peer-port 1720	H.323 隣接が使用するリモート シグナリング ピア ポートを指定します。
ステップ 8	**account** *account_name* **例：** host1/Admin(config-sbc-sbe-adj-h323)# account h323-vrf1	SBE 上のアカウントに属するものとして H.323 隣接を定義します。
ステップ 9	**media-bypass** **例：** host1/Admin(config-sbc-sbe-adj-h323)# media-bypass	（任意）メディア トラフィックが DBE をバイパスできるように隣接を設定します。 このコマンドは任意であり、1 つの隣接でだけ機能します。
ステップ 10	**media-bypass-forbid** **例：** host1/Admin(config-sbc-sbe-adj-h323)# media-bypass-forbid	メディア トラフィックが DBE をバイパスできないように H.323 隣接を設定します。 これを設定していない場合、この隣接で発信および終了するコールのメディア トラフィックはエンドポイント間を直接流れます。両方の隣接が同じ VPN にない限り、DBE をパススルーしません。

	コマンドまたはアクション	目的
ステップ 11	**attach** **例：** `host1/Admin(config-sbc-sbe-adj-h323)# attach`	隣接を接続します。

SIP 隣接への VRF の関連付け

このタスクでは、SIP 隣接を VPN に関連付けます。

手順概要

1. **adjacency sip** *adjacency-name*
2. **vrf** *vrf_name*
3. **signaling-address ipv4** *local_signaling_IP_address*
4. **signaling-port** *port_num*
5. **remote-address ipv4** *local_signaling_IP_address/prefix*
6. **local-id host** *name*
7. **signaling-peer** [**gk**] *peer_address*
8. **signaling-peer-port** *port_num*
9. **account** *account-name*
10. **media-bypass** (optional)
11. **media-bypass-forbid**
12. **attach**

詳細手順

	コマンドまたはアクション	目的

ステップ 1	**adjacency sip** *adjacency-name*
	
	例：
	`host1/Admin(config-sbc-sbe)# adjacency sip sip_vrf1`
	`host1/Admin(config-sbc-sbe-adj-sip)#`
		SBE SIP 隣接モードを開始します。
		• サービス名を定義するには、*adjacency-name* 引数を使用します。

ステップ 2	**vrf** *vrf_name* **例：** `host1/Admin(config-sbc-sbe-adj-sip)# vrf my_vrf1`	H.323 隣接を特定の VPN に接続します。 **（注）**　隣接での VRF 名は、コンテキスト名に一致する必要があります。

ステップ 3	**signaling-address ipv4** *ipv4_IP_address*
	
	例：
	`host1/Admin(config-sbc-sbe-adj-sip)#`
	`signaling-address ipv4 88.88.88.88.101.11`
		SIP 隣接のローカル IPv4 シグナリング アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 4	**signaling-port** *port_num* **例：** host1/Admin(config-sbc-sbe-adj-sip)# signaling-port 5060	SIP 隣接のローカル シグナリング ポートを指定します。
ステップ 5	**remote-address ipv4** *remote_IP_address/prefix* **例：** host1/Admin(config-sbc-sbe-adj-sip)# remote-address ipv4 10.10.101.4 255.255.255.255	隣接経由で通信するリモート シグナリング ピアのセットを、指定の IP アドレス プレフィクスを持つピアに制限します。
ステップ 6	**local-id host** *address* **例：** host1/Admin(config-sbc-sbe-adj-sip)# local-id host 88.88.101.11	SIP 隣接のローカル識別名を設定します。
ステップ 7	**signaling-peer** [**gk**] *peer_address* **例：** host1/Admin(config-sbc-sbe-adj-sip)# signaling-peer 10.10.101.4	SIP 隣接が使用するリモート シグナリング ピアを指定します。
ステップ 8	**signaling-peer-port** *port_num* **例：** host1/Admin(config-sbc-sbe-adj-sip)# signaling-peer-port 5060	SIP 隣接が使用するリモート シグナリング ピア ポートを指定します。
ステップ 9	**account** *account_name* **例：** host1/Admin(config-sbc-sbe-adj-sip)# account sip-vrf1	SBE 上のアカウントに属するものとして SIP 隣接を定義します。
ステップ 10	**media-bypass** **例：** host1/Admin(config-sbc-sbe-adj-sip)# media-bypass	（任意）メディア トラフィックが DBE をバイパスできるように隣接を設定します。 このコマンドは任意であり、1 つの隣接でだけ機能します。
ステップ 11	**media-bypass-forbid** **例：** host1/Admin(config-sbc-sbe-adj-sip)# media-bypass-forbid	メディア トラフィックが DBE をバイパスできないように SIP 隣接を設定します。 これを設定していない場合、この隣接で発信および終了するコールのメディア トラフィックはエンドポイント間を直接流れます。両方の隣接が同じ VPN にない限り、DBE をパススルーしません。
ステップ 12	**attach** **例：** host1/Admin(config-sbc-sbe-adj-sip)# attach	隣接を接続します。

DBE への VRF の設定 - 分散モデル専用

このタスクでは、分散モデルの DBE に VRF を設定します。

手順概要

1. **configure**
2. **sbc** *sbc-name*
3. **dbe**
4. **vdbe** *global*
5. **unexpected-source-alerting**
6. **local-port** *abcd*
7. **control-address h248 ipv4** *A.B.C.D*
8. **controller h248** *controller-index*
9. **remote-address ipv4** *remote-address*
10. **remote-port** [*port-num*]
11. **transport** [**udp** | **tcp**]
12. **attach-controllers**
13. **media-address pool ipv4** *A.B.C.D E.F.G.H* **vrf** *vrfname*
14. **media-timeout** *timeout*
15. **overload-time-threshold** *time*
16. **deact-mode**
17. **activate**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `host1/Admin# configure`	コンフィギュレーション モードを開始します。
ステップ 2	**sbc** *sbc-name* **例：** `host1/Admin(config)# sbc mySbc`	SBC 上に SBC サービスを作成し、SBC コンフィギュレーション モードを開始します。
ステップ 3	**dbe** **例：** `host1/Admin(config-sbc)# dbe`	SBC 上に DBE サービスを作成し、SBC-DBE 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 4	**vdbe** [**global**] **例：** host1/Admin(config-sbc-dbe)# vdbe	VDBE コンフィギュレーション サブモードを開始します。 **（注）** 初期リリースでは、vDBE（グローバル vDBE）が 1 つだけサポートされています。vdbe 名は省略可能です。指定する場合は、global を指定する必要があります。
ステップ 5	**unexpected-source-alerting** **例：** host1/Admin(config-sbc-dbe-vdbe-global)# unexpected-source-alerting	予期せぬ送信元アドレスに対するアラートを設定します。 このコマンドの **no** 形式を使用すると、予期せぬ送信元アドレスが受信された場合に、アラートが生成されなくなります。
ステップ 6	**local-port** {*abcd*} **例：** host1/Admin(config-sbc-dbe)# local-port 5090	特定のローカル ポートを使用するように DBE を設定します。
ステップ 7	**control-address h248 ipv4** *A.B.C.D* **例：** host1/Admin(config-sbc-dbe)# control-address h248 ipv4 10.0.0.1	特定の IPv4 H.248 制御アドレスを使用するように DBE を設定します。
ステップ 8	**controller h248** *controller-index* **例：** host1/Admin(config-sbc-dbe)# controller h248 1	DBE の H.248 コントローラを識別し、Controller H.248 コンフィギュレーション モードを開始します。
ステップ 9	**remote-address ipv4** *remote-address* **例：** host1/Admin(config-sbc-dbe-vdbe-h248)# remote-address ipv4 1.1.1.1	H.248 コントローラの IPv4 リモート アドレスを設定します。
ステップ 10	**remote-port** [*port-num*] **例：** host1/Admin(config-sbc-dbe-h248)# remote-port 2094	H.248 コントローラに対応する、SBE の接続先ポートを定義します。
ステップ 11	**transport udp** **例：** host1/Admin(config-sbc-dbe-h248)# transport udp	H.248 制御シグナリングに User Datagram Protocol（UDP; ユーザ データグラム プロトコル）を使用するように、DBE を設定します。
ステップ 12	**attach-controllers** **例：** host1/Admin(config-sbc-dbe)# attach-controllers	H.248 コントローラに接続するように DBE を設定します。

	コマンドまたはアクション	目的
ステップ 13	**media-address pool ipv4** *A.B.C.D E.F.G.H* **vrf** *vrfname* **例：** host1/Admin(config-sbc-dbe)# media-address pool ipv4 10.10.10.1 10.10.10.20 vrf my_vrf1	特定の VRF インスタンスに関連付けられた IPv4 アドレス用に、連続した IPv4 メディア アドレスのプールを作成します。 **（注）** 隣接での VRF 名は、コンテキスト名に一致する必要があります。
ステップ 14	**media-timeout** *timeout* **例：** host1/Admin(config-sbc-dbe)# media-timeout 10	コールに関する最終メディア パケットを受信してから、コール リソースをクリーンアップするまでの DBE の最大待機時間を設定します。
ステップ 15	**overload-time-threshold** *time* **例：** host1/Admin(config-sbc-dbe)# overload-time-threshold 400	Media Gateway（MG; メディア ゲートウェイ）過負荷制御検出のしきい値を設定します。
ステップ 16	**deact-mode normal** **例：** host1/Admin(config-sbc-dbe)# deactivation-mode normal	SBC の DBE がサービス変更を通知し、DBE サービスが非アクティブになった時点ですべてのコールを終了するように指定します。
ステップ 17	**activate** **例：** host1/Admin(config-sbc-dbe)# activate	SBC サービスを開始します。

multi-VRF を実装するための設定例

ここでは、次の設定例を示します。

- 「multi-VRF の設定：例」（P.10-16）
- 「H.323 隣接への VRF の関連付け：例」（P.10-18）
- 「SIP 隣接への VRF の関連付け：例」（P.10-18）
- 「DBE への VRF の設定（分散モデル専用）：例」（P.10-21）

multi-VRF の設定：例

この設定例では、Service Virtual Interface（SVI）および隣接を追加して、それらに VPN を関連付ける方法を示します。

1. スーパーバイザ上の vrf my_vrf1 に関連付けられたラインカード インターフェイスを設定します。

```
vrf definition my_vrf1
rd 55:1111
!
address-family ipv4
exit-address-family
!
```

2. スーパーバイザ上の vrf my_vrf1 に関連付けられたラインカード インターフェイスを設定します。

```
interface GigabitEthernet1/3
description ''Connected to CAT-3550-101 Fa 0/13 vlan919''
vrf forwarding my_vrf1
ip address 10.122.3.3 255.255.255.0

interface Vlan 99
vrf forwarding my_vrf1
ip address 99.101.1.1 255.255.255.0
!
```

3. ACE カードのコンテキストを設定し、VLAN を割り当てます。

```
context my_vrf1
allocate-interface vlan 99
```

4. FT グループを設定します。

（注） デフォルト（Admin）コンテキストで（このインスタンス *my_vrf1* に）FT グループ 1 を設定する必要があります。

```
ft group 1
peer 1
priority 127
peer priority 126
associate-context my_vrf1
inservice
```

5. my_vrf1 コンテキストにインターフェイスを設定します。このインターフェイスを使用して、コンテキストを変更するための CLI に変更を加える必要があります。

```
ACE-101-UUT1-1/Admin# changeto my_vrf1
ACE-101-UUT1-1/my_vrf1#

interface vlan 99
ip address 99.101.1.2 255.255.255.0
alias 99.101.1.100 255.255.255.0
peer ip address 99.101.1.3 255.255.255.0
no shutdown

ip route 10.0.0.0 255.0.0.0 99.101.1.1
ip route 100.0.0.0 255.0.0.0 99.101.1.1
```

6. DBE を設定します。

```
dbe
    media-address pool ipv4 88.88.101.12  88.88.101.15 vrf my_vrf1
    activate
```

DNS 照会設定：例

この設定例では、DNS 照会を設定します。

```
context vrf110
  allocate-interface vlan 110
context vrf120
  allocate-interface vlan 120

sbc mysbc
  sbe
    sip dns
      cache-lifetime 6000
```

```
      cache-limit 100
    ...
    adjacency sip sip1
      vrf vrf110
      ...
    adjacency sip sip2
      vrf vrf120
      ...

host1/Admin# changeto vrf110
ip domain-lookup
ip domain-name test.com
ip name-server 192.168.110.2

host1/Admin# changeto vrf120
ip domain-lookup
ip domain-name test1.com
ip name-server 192.168.120.2
```

H.323 隣接への VRF の関連付け：例

この設定例では、VPN に関連付けられた H.323 隣接を作成します。

```
adjacency h323 h323my_vrf1
   vrf my_vrf1
   signaling-address ipv4 88.88.101.11
   signaling-port 1720
   remote-address ipv4 10.10.101.4 255.255.255.255
   signaling-peer 10.10.101.4
   signaling-peer-port 1720
   account h323-my_vrf1
   attach
```

SIP 隣接への VRF の関連付け：例

次の設定例では、VPN に関連付けられた SIP 隣接を作成します。コンテキストごとに FT グループが設定されていることに注意してください。

```
ft interface vlan 99
  ip address 10.10.10.15 255.255.255.0
  peer ip address 10.10.10.16 255.255.255.0
  no shutdown

ft peer 1
  heartbeat interval 100
  heartbeat count 10
  ft-interface vlan 99
ft group 1
  peer 1
  priority 127
  peer priority 126
  associate-context Admin
  inservice

ip route 10.10.0.0 255.255.0.0 101.101.101.100 ip route 20.20.20.0 255.255.255.0
101.101.101.4
```

```
context vlan100
  description vlan100
  allocate-interface vlan 100

ft group 2
  peer 1
  priority 127
  peer priority 126
  associate-context vlan100
  inservice
username admin password 5 $1$faXJEFBj$TJR1Nx7sLPTi5BZ97v08c/  role Admin domain
default-domain username www password 5 $1$UZIiwUk7$QMVYN1JASaycabrHkhGcS/  role Admin
domain default-domain

sbc mysbc
  sbe
    adjacency sip 7200-1
      vrf vlan100
      inherit profile preset-core
      preferred-transport udp
      redirect-mode pass-through
      authentication nonce timeout 300
      signaling-address ipv4 101.101.101.3
      signaling-port 5061
      remote-address ipv4 0.0.0.0 0.0.0.0
      signaling-peer 101.101.101.5
      signaling-peer-port 5060
      dbe-location-id 0
      account sip-core
      attach

    adjacency sip 7200-2
      vrf vlan100
      inherit profile preset-access
      preferred-transport udp
      redirect-mode pass-through
      authentication nonce timeout 300
      signaling-address ipv4 101.101.101.3
      signaling-port 5060
      remote-address ipv4 0.0.0.0 0.0.0.0
      signaling-peer 101.101.101.4
      signaling-peer-port 5060
      dbe-location-id 0
      account sip-core
      attach

    adjacency sip 7200-3
      vrf vlan100
      nat force-on
      inherit profile preset-core
      preferred-transport udp
      redirect-mode pass-through
      authentication nonce timeout 300
      signaling-address ipv4 101.101.101.3
      signaling-port 5063
      remote-address ipv4 0.0.0.0 0.0.0.0
      signaling-peer 101.101.101.5
      signaling-peer-port 5063
      dbe-location-id 0
      account sip-core
      reg-min-expiry 3000
      attach

    sip inherit profile preset-standard-non-ims
```

```
    retry-limit 3

    call-policy-set 1
      first-call-routing-table invite-table
      first-reg-routing-table start-table
      rtg-src-adjacency-table invite-table
        entry 1
          action complete
          dst-adjacency 7200-2
          match-adjacency 7200-3
        entry 2
          action complete
          dst-adjacency 7200-3
          match-adjacency 7200-2
      rtg-src-adjacency-table start-table
        entry 1
          action complete
          dst-adjacency 7200-1
          match-adjacency 7200-2
        entry 2
          action complete
          dst-adjacency 7200-2
          match-adjacency 7200-1
      complete

    active-call-policy-set 1

    network-id 2

    sip max-connections 2
    sip timer
      tcp-idle-timeout 120000
      tls-idle-timeout 3600000
      udp-response-linger-period 32000
      udp-first-retransmit-interval 500
      udp-max-retransmit-interval 4000
      invite-timeout 180

    blacklist
      global

    redirect-limit 2
    deact-mode normal
    activate

  dbe
    media-address ipv4 101.101.101.160 vrf vlan100 port-range 11000 20000 any
    location-id 0
    media-timeout 30
    deact-mode normal
    activate

newace4/Admin# changeto vlan100
newace4/vlan100# sh run
Generating configuration....

interface vlan 100
  ip address 101.101.101.1 255.255.255.0
  alias 101.101.101.3 255.255.255.0
  peer ip address 101.101.101.2 255.255.255.0
  no shutdown

ip route 0.0.0.0 0.0.0.0 101.101.101.100
```

DBE への VRF の設定（分散モデル専用）：例

この例では、コンテキスト my_vrf1 を作成し、my_vrf1 に VLAN を割り当てます。

```
context my_vrf1
allocate-interface vlan 97
```

フォールトトレラント グループが作成され、コンテキスト my_vrf1 が関連付けられます。

```
ft group 2
peer 1
priority 127
peer priority 126
associate-context my_vrf1
inservice
```

SBC に、コンテキスト my_vrf1 に関連付けられたメディア アドレスが設定されます。

```
sbc j
dbe
vdbe global
unexpected-source-alerting
local-port 2985
control-address h248 ipv4 87.87.29.100
controller h248 1
remote-address ipv4 200.200.200.123
remote-port 2985
transport udp
attach-controllers
media-address ipv4 97.97.29.100 vrf my_vrf1
media-address pool ipv4 87.87.29.100 87.87.29.101
media-timeout 3600
overload-time-threshold 100
deact-mode normal
activate
```

（新しく作成されたコンテキスト my_vrf1）

VLAN インターフェイスが作成されます。

```
interface vlan 97
ip address 97.97.29.2 255.255.255.0
alias 97.97.29.100 255.255.255.0
peer ip address 97.97.29.252 255.255.255.0
no shutdown

ip route 200.200.200.0 255.255.255.0 97.97.29.1
```

```
ip route 20.20.29.0 255.255.255.0 97.97.29.1
```

VLAN インターフェイスは、スーパーバイザ エンジン上の my_vrf1 に関連付けられます。

```
interface Vlan 97
vrf forwarding my_vrf1
ip address 97.97.29.1 255.255.255.0
```