

基本 VSAN間のルーティング構成

この章では、VSAN 間ルーティング（IVR）機能について説明し、IVR 管理インターフェイスを使用して VSAN 間で技術情報を共有するための基本的な手順を示します。基本的な IVR 構成を設定した後、高度な IVR 構成を設定する必要がある場合は、 高度 VSAN間のルーティング構成 を参照してください。

- VSAN 間ルーティングについて, on page 1
- 基本 IVR 構成タスク リスト, on page 5
- 基本 IVR 構成, on page 6
- IVR 仮想ドメイン, on page 14
- IVR ゾーンと IVR ゾーン セット, on page 17
- IVR ロギング, on page 25
- データベース マージの注意事項, on page 26
- IVR 自動トポロジ モードの構成例, on page 29
- デフォルト設定 , on page 32

VSAN 間ルーティングについて

仮想 SAN（VSAN）は、複数のファイバ チャネル SAN がスイッチと ISL の共通の物理インフラストラクチャを共有できるようにすることで、ストレージ エリア ネットワーク（SAN）の拡張性、可用性、およびセキュリティを向上させます。これらの利点は、各VSANでのファイバチャネルサービスの分離と、VSAN間のトラフィックの分離から得られます。また、VSAN 間のデータ トラフィックの分離により、VSAN に接続されているリソース（ロボット テープ ライブラリなど）の共有も本質的に防止されます。IVRを使用すると、他のVSANの利点を損なうことなく、VSAN 全体のリソースにアクセスできます。

IVR 機能

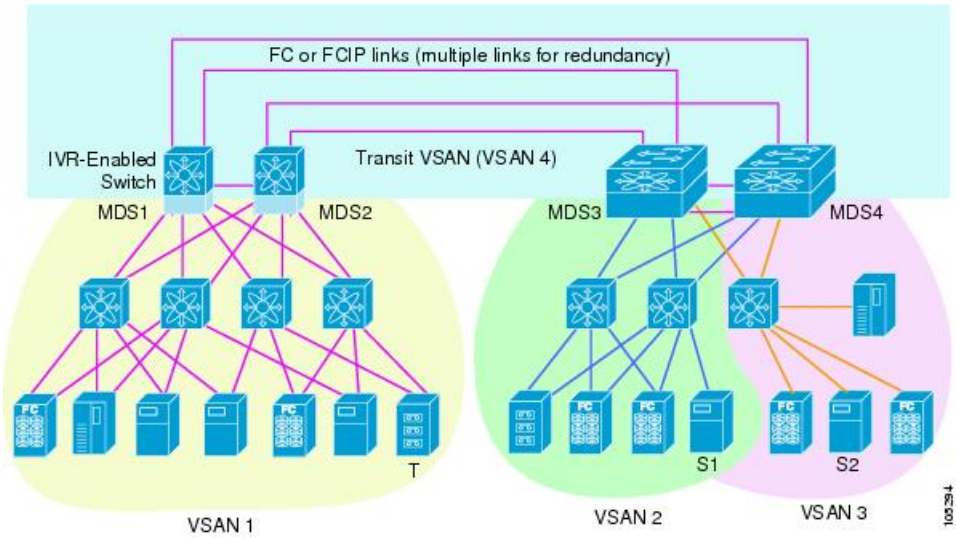
IVR は次の機能をサポートしています：

- 他の VSAN の利点を損なうことなく、VSAN 全体の技術情報にアクセスします。

- VSANを単一の論理ファブリックにマージすることなく、異なるVSAN上の特定のイニシエータとターゲットの間でデータ トラフィックを転送します。
- 複数のスイッチ間で 1 つ以上の VSAN を移動する適切な相互接続ルートを確立します。IVR は、共通のスイッチ上に存在する VSAN に限定されません。
- 貴重な技術情報（テープライブラリなど）を VSAN 間で妥協することなく共有します。ファイバ チャネル トラフィックは VSAN 間を流れることはなく、発信側は指定された VSAN 以外の VSAN 間でリソースにアクセスすることもできません。
- FCIP と組み合わせて使用すると、効率的なビジネス継続性またはディザスタ リカバリ ソリューションを提供します。図 「IVR および FCIP を使用したトラフィックの継続性」を参照してください。
- ファイバ チャネル標準に準拠しています。
- サード パーティ製スイッチが組み込まれていますが、IVR 対応 VSAN はいずれかの相互運用モードで構成する必要がある場合があります。

Note 次の図に示すサンプルシナリオを構成するには、「IVR 自動トポロジモードの構成例」の手順に従います。

***Figure 1: IVR* および *FCIP* を使用したトラフィックの継続性**



IVR 用語

次の IVR 関連用語は、IVR ドキュメントで使用されています。

- ネイティブ VSAN：エンド デバイスがログ オンする VSAN は、そのエンド デバイスのネイティブ VSAN です。
- [現在のVSAN（Current VSAN）]：現在 IVR 用に構成されている VSAN。

- VSAN 間ルーティング ゾーン（IVR ゾーン）：相互接続された SAN ファブリック内の VSAN 間で通信できるエンド デバイスのセット。この定義は、ポートのワールド ワイド 名（pWWN）とネイティブ VSAN の関連付けに基づいています。Cisco SAN-OS リリース 3.0（3）より前は、ネットワーク内のスイッチで最大 2000 の IVR ゾーンと 10,000 の IVR ゾーンメンバーを構成できました。Cisco SAN-OS リリース 3.0（3）では、ネットワーク内のスイッチに最大 8000 の IVR ゾーンと 20,000 の IVR ゾーンメンバーを構成できます。
- VSAN 間ルーティング ゾーン セット（IVR ゾーン セット）：1 つ以上の IVR ゾーンが IVR ゾーン セットを構成します。Cisco MDS 9000 シリーズのスイッチには、最大 32 の IVR ゾーン セットを構成できます。アクティブにできる IVR ゾーン セットは常に 1 つだけです。
- IVR パス：IVR パスは、ある VSAN 内のエンド デバイスからのフレームが別の VSAN 内の別のエンドデバイスに到達できるようにするためのスイッチとスイッチ間リンク（ISL）のセットです。このような 2 つのエンド デバイス間には、複数のパスが存在できます。
- IVR 対応スイッチ：IVR 機能が有効になっているスイッチ。
- エッジ VSAN：IVR パスを開始（送信元エッジ VSAN）または終了（宛先エッジ VSAN）する VSAN。エッジ VSAN は、相互に隣接している場合もあれば、1 つ以上の中継 VSAN によって接続されている場合もあります。VSAN 1、2、および 3（Figure 1: IVR および FCIP を使用したトラフィックの継続性, on page 2を参照）は、エッジ VSAN です。

Note 1 つの IVR パスのエッジ VSAN を、別の IVR パスの中継 VSAN にすることができます。

- 中継 VSAN：そのパスの送信元エッジ VSAN からそのパスの宛先エッジ VSAN への IVR パスに沿って存在する VSAN。VSAN 4 は中継 VSANです（Figure 1: IVR および FCIP を使用したトラフィックの継続性, on page 2を参照）。

Note 送信元エッジVSANと宛先エッジVSANが相互に隣接している場合、それらの間に中継VSANは必要ありません。

- ボーダー スイッチ：2 つ以上の VSAN のメンバーである IVR 対応スイッチ。VSAN 1 と VSAN 4 間の IVR 対応スイッチ（Figure 1: IVR および FCIP を使用したトラフィックの継続性, on page 2を参照）などのボーダースイッチは、色分けされた 2 つ以上の VSAN にまたがります。
- エッジ スイッチ：IVR ゾーンのメンバーがログインしているスイッチ。エッジ スイッチは、ボーダー スイッチの IVR 構成を認識しません。エッジスイッチは IVR 対応である必要はありません。
- 自律ファブリック識別子（AFID）：同じ VSAN ID を使用してネットワーク内に複数の VSAN を構成でき、同じ ID を持つ VSAN を含むファブリック間で IVR を構成する際のダウンタイムを回避できます。
- サービス グループ：IVR 対応 VSAN へのトラフィックを制限する 1 つ以上のサービス グループを構成することで、IVR 非対応 VSAN への IVR トラフィックの量を減らすことができます。

IVR 構成の制限

IVR 構成の制限の詳細については、Cisco MDS NX-OS の構成の制限、リリース 8.x を参照してください。

ファイバ チャネル ヘッダーの変更

IVR は、仮想ドメインを使用してネイティブ VSAN 内のリモート エンド デバイスを仮想化します。2 つの異なる VSAN 内のエンド デバイスをリンクするように IVR が構成されている場合、IVR ボーダー スイッチは、エンド デバイス間のすべての通信のファイバ チャネル ヘッダーを変更します。変更されるファイバ チャネル フレーム ヘッダーのセクションは次のとおりです：

- VSAN 番号
- 送信元 FCID
- 宛先 FCID

フレームがイニシエータからターゲットに移動すると、ファイバ チャネル フレーム ヘッダーが変更され、イニシエータ VSAN 番号がターゲット VSAN 番号に変更されます。IVR ネットワーク アドレス変換（NAT）がイネーブルの場合、送信元および宛先の FCID もエッジ ボーダー スイッチで変換されます。IVR NAT が有効になっていない場合は、IVR パスに関連するすべてのスイッチに一意のドメイン ID を構成する必要があります。

IVR ネットワーク アドレス変換

IVR NAT を使用するには、ファブリック内のすべての IVR 対応スイッチで IVR NAT を有効にする必要があります。CFS を使用した IVR 構成の配布については、「CFS を使用した IVR 構成の配布, on page 7」を参照してください。デフォルトでは、IVR NAT および IVR 構成の配信は、Cisco MDS 9000 ファミリのすべてのスイッチで無効になっています。

IVR の要件とガイドライン、および構成情報については、IVR NAT および IVR 自動トポロジ モードについて, on page 9 を参照してください。

IVR VSAN トポロジ

IVR は、構成された IVR VSAN トポロジを使用して、ファブリックを介したイニシエータとターゲット間のトラフィックのルーティング方法を決定します。

IVR 自動トポロジモードは、ファブリックの再構成が発生したときに、IVR VSAN トポロジを自動的に構築し、トポロジデータベースを維持します。また、IVR 自動トポロジモードでは、CFS を使用して IVR VSAN トポロジを IVR 対応スイッチに配信します。

IVR 自動トポロジ モードを使用すると、ファブリックで再構成が発生したときに IVR VSAN トポロジを手動で更新する必要がなくなります。IVR 手動トポロジデータベースが存在する場合、IVR 自動トポロジ モードは最初にそのトポロジ情報を使用します。自動更新では、ユーザー指定のトポロジ データベースから自動的に学習されたトポロジ データベースに徐々に移

行することで、ネットワークの中断が軽減されます。ネットワークの一部ではないユーザーの構成したのトポロジエントリは、約3分で期限切れになります。ユーザが構成したデータベースの一部ではない新しいエントリは、ネットワークで検出されると追加されます。

IVR 自動トポロジ モードを有効にすると、以前にアクティブだった IVR 手動トポロジが存在する場合はそのトポロジで開始され、ディスカバリ プロセスが開始されます。新しいパス、代替パス、またはより適切なパスを検出できます。トラフィックが代替パスまたはより適切なパスに切り替えられると、通常はスイッチングパスに関連する一時的なトラフィックの中断が発生する可能性があります。

Note IVR 自動トポロジ モードの IVR トポロジには、Cisco MDS SAN-OS リリース 2.1（1a）以降が必要であり、ファブリック内のすべてのスイッチで IVR に対して CFS を有効にする必要があります。

IVR 相互運用性

IVR機能を使用する場合、ファブリック内のすべての境界スイッチはCisco MDS スイッチである必要があります。ただし、ファブリック内の他のスイッチは非 MDS スイッチである場合があります。たとえば、アクティブ IVR ゾーン セットのメンバーであるエンド デバイスは、非 MDS スイッチに接続できます。相互運用モードの 1 つが有効になっている場合は、非 MDS スイッチがトランジット VSAN またはエッジ VSAN に存在することもあります。

スイッチの相互運用性の詳細については、『 *Cisco Data Center Interoperability Support Matrix*』を参照してください。

基本 IVR 構成タスク リスト

IVR 構成するには、次の手順に従います：

Procedure

ステップ 1 「IVR NAT を有効にします, on page 12」を参照してください。

IVR NAT を有効にします。

ステップ 2 「IVR を有効化 , on page 6」を参照してください。

すべての境界スイッチで IVR を有効にします。

ステップ 3 「CFS を使用した IVR 構成の配布, on page 7」を参照してください。

IVR 配信を有効にします。

ステップ 4 IVR NAT および IVR 自動トポロジ モードについて, on page 9を参照してください。

IVR 自動トポロジ モードを有効にします。

ステップ 5 IVR 仮想ドメインを構成します。

ステップ 6 「IVR ゾーンと IVR ゾーン セットの構成, on page 19」を参照してください。

ゾーン セットを構成し、アクティブにします。

ステップ 7 「変更のコミット, on page 8」を参照してください。

IVR 構成をコミットします。

ステップ 8 「IVR ゾーンと IVR ゾーン設定構成の確認, on page 23」を参照してください。

IVR 構成を確認します。

基本 IVR 構成

ここでは、IVR の構成方法について説明します。このセクションの内容は次のとおりです：

IVR を有効化

IVR機能は、IVRに参加するファブリック内のすべてのボーダースイッチで有効にする必要があります。デフォルトでは、この機能は全てのCisco MDS 9000シリーズスイッチで無効になっています。ファブリック内の必要なすべてのスイッチでIVRを手動で有効にするか、IVR設定のファブリック全体への配信を構成できます。「CFS を使用した IVR 構成の配布, on page 7」を参照してください。

Note IVR機能の構成および確認コマンドを使用できるのは、スイッチ上でIVRが有効にされている場合だけです。この構成を無効にした場合、関連するすべての構成は自動的に廃棄されます。

参加させるスイッチの IVR を有効にするには、次のステップを実行します：

Procedure

ステップ 1 構成モードに入ります。

switch# **config t**

ステップ 2 スイッチで IVR NAT を有効にします。

switch(config)# **ivr nat**

ステップ 3 スイッチで IVR を有効にします。

switch(config)# **feature ivr**

ステップ 4 スイッチ上の IVR を無効にします（デフォルト）。

switch(config)# **no feature ivr**

CFS を使用した IVR 構成の配布

IVR 機能は、Cisco Fabric Services（CFS）インフラストラクチャを利用して効率的な構成管理を可能にし、VSAN内のファブリック全体に対するシングルポイントでの構成を提供します。CFSの詳細については、『*Cisco MDS 9000* ファミリ *NX-OS* システム管理構成ガイド』を参照してください。

次の設定が配信されます。

- IVR ゾーン
- IVR ゾーン セット
- IVR VSAN トポロジ
- IVRアクティブトポロジおよびゾーンセット（1つのスイッチでこれらの機能をアクティブにすると、ファブリック内の他のすべてのディストリビューション対応スイッチに構成が伝播されます）
- AFID データベース

Note IVR構成の配信は、デフォルトでは無効になっています。この機能を正しく機能させるには、ネットワーク内のすべての IVR 対応スイッチでこの機能を有効にする必要があります。

データベースを導入

IVR 機能は、これらのデータベースを使用して、構成を受け入れ、実装します。

- 構成済みデータベース：データベースはユーザが手動で設定します。
- アクティブ データベース：データベースは、ファブリックが現在実行されています。
- 保留中データベース：構成を修正した場合は、構成済みのデータベースの変更内容を保留中データベースにコミットするかまたは廃棄する必要があります。その間、ファブリックはロックされた状態になります。保留中のデータベースへの変更は、CFSに変更をコミットするまで現用系データベースに反映されません。

構成流通の有効化

IVR 構成の配信を有効にするには、次の手順を実行します：

Procedure

ステップ 1 構成モードに入ります。

switch# **config t**

ステップ 2 IVR 配信をイネーブルにします。

switch(config)# **ivr distribute**

ステップ 3 IVR の配布をディセーブル（デフォルト）にします。

switch(config)# **no ivr distribute**

ファブリックのロック

データベースを変更するときの最初のアクションによって、保留中のデータベースが作成され、VSAN内の機能がロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザーがこの機能の設定に変更を加えることができなくなります。
- コンフィギュレーションデータベースのコピーが、最初のアクティブ変更と同時に保留中のデータベースになります。

変更のコミット

アクティブデータベースに加えられた変更をコミットする場合、ファブリック内のすべてのスイッチに構成がコミットされます。コミットが正常に行われると、構成の変更がファブリック全体に適用され、ロックが解除されます。

IVR 構成変更をコミットするには、次のステップに従います：

Procedure

ステップ 1 構成モードに入ります。

switch# **config t**

ステップ 2 IVR の変更をコミットします。

switch(config)# **ivr commit**

変更の廃棄

保留中のデータベースに加えられた変更を廃棄（終了）する場合、構成データベースは影響を受けないまま、ロックが解除されます。

IVR 構成の変更を廃棄するには、次の手順を実行します：

Procedure

ステップ 1 構成モードに入ります。

switch# **config t**

ステップ 2 IVR の変更を廃棄し、保留中の構成データベースをクリアします。

switch(config)# **ivr abort**

ロック済みセッションのクリア

IVR タスクを実行し、変更の確定か破棄を行ってロックを解除していない場合、管理者はファブリックのスイッチからロックを解除できます。管理者がこの操作を行うと、ユーザーによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。



Tip 保留データベースは、一時的なディレクトリだけで使用可能であり、スイッチが再起動されると破棄されることがあります。

管理者の特権を使用して、ロックされた DPVM セッションを解除するには、EXEC モードで **clear ivr session** コマンドを使用します。

```
switch# clear ivr session
```

IVR NAT および IVR 自動トポロジ モードについて

IVR NAT および IVR 自動トポロジ モードを使用するように IVR SAN ファブリックを構成する前に、次の点を考慮してください：

- 関連するスイッチでのみ IVR を構成します。
- ファブリック内のすべてのスイッチで IVR の CFS を有効にします。
- ファブリック内の全てのスイッチは、Cisco MDS SAN-OS リリース 2.2（1a）以降が稼働していることを確認します。
- Cisco MDS SAN-OS リリース 2.1（1a）以降とこの機能用のアクティブな IPS カードがある場合は、必須のエンタープライズ ライセンス パッケージまたは SAN-EXTENSION ライセ

ンス パッケージを取得します。ライセンスの詳細については、『 *Cisco MDS 9000* シリーズ *NX-OS* ライセンス ガイド』を参照してください。

Note FCIP 上の IVR 機能は Cisco MDS 9216i スイッチにバンドルされており、スーパーバイザ モジュールの固定 IP ポート用の SAN Extension over IP パッケージは必要ありません。

Tip FSPF リンク コストを変更する場合は、IVR パスの FSPF パス ディスタンス（つまり、パス上のリンク コストの合計）が 30,000 未満になるようにしてください。

Note IVR 対応 VSAN は、interop モードが有効（任意の相互運用モード）または無効（非相互運用モード）の場合に設定できます。

IVR NAT の要件とガイドライン

IVR NAT を使用するための要件とガイドラインを次に示します：

- ホストから受信した IVR NAT ポート ログイン（PLOGI）要求は、FC ID アドレスの書き換えを実行するために数秒遅延します。ホストの PLOGI タイムアウト値が 5 秒未満の値に設定されている場合、PLOGI が不必要に終了し、ホストがターゲットにアクセスできなくなる可能性があります。ホスト バス アダプタのタイムアウトを 10 秒以上に構成することを推奨します（ほとんどの HBA のデフォルト値は 10 または 20 秒です）。
- IVR NAT には、ファブリック内のすべての IVR スイッチで Cisco MDS SAN-OS リリース 2.1（1a）以降が必要です。
- Cisco NX-OS リリース 5.2（x）以降から IVR 非 NAT モードがサポートされません。IVR 非 NAT モードが構成されている場合は、IVR NAT モードへ移行する方法について、IVR NAT への移行を参照してください。
- IVR NAT を使用すると、IVR パス内のすべてのスイッチで一意のドメイン ID を必要とせずに、ファブリック内に IVR を設定できます。IVR NAT は、ファイバ チャネル ヘッダーの宛先 ID にローカル VSAN を使用して、他の VSAN 内のスイッチを仮想化します。一部の拡張リンク サービス メッセージ タイプでは、宛先 ID がパケット データに含まれています。このような場合、IVR NAT は実際の宛先 ID を仮想化された宛先 ID に置き換えます。IVR NAT は、次の表に示す拡張リンクサービスメッセージの宛先 ID の置換をサポートします。

Table 1: IVR NAT でサポートされる拡張リンク サービス メッセージ

拡張リンク サービス メッセージ	リンク サービス コマンド（**LS_COMMAND**）	**Mnemonic**
Abort Exchange	0x06 00 00 00	ABTX
Discover Address	0x52 00 00 00	ADISC
Discover Address Accept	0x02 00 00 00	ADISC ACC
Fibre Channel Address Resolution Protocol Reply	0x55 00 00 00	FARP-REPLY
Fibre Channel Address Resolution Protocol Request	0x54 00 00 00	FARP-REQ
Logout	0x05 00 00 00	LOGO
Port Login	0x30 00 00 00	PLOGI
Read Exchange Concise	0x13 00 00 00	REC
Read Exchange Concise Accept	0x02 00 00 00	REC ACC
Read Exchange Status Block	0x08 00 00 00	RES
Read Exchange Status Block Accept	0x02 00 00 00	RES ACC
Read Link Error Status Block	0x0F 00 00 00	RLS
Read Sequence Status Block	0x09 00 00 00	RSS
Reinstate Recovery Qualifier	0x12 00 00 00	RRQ
Request Sequence Initiative	0x0A 00 00 00	RSI
Scan Remote Loop	0x7B 00 00 00	RSL
Third Party Process Logout	0x24 00 00 00	TPRLO
Third Party Process Logout Accept	0x02 00 00 00	TPRLO ACC

- IVR NAT によって認識されないメッセージがあり、パケット データに宛先 ID が含まれている場合、トポロジ内の NAT で IVR を使用することはできません。

Note IVR トポロジに FICON VSAN が含まれている場合は、IVR NAT を有効にしないでください。IVR NAT が FICON VSAN とともにイネーブルの場合、スイッチは **fcid-nat cannot be enabled if FICON enabled VSANs and topology VSANs overlap** エラーをスローします。

中継 VSAN ガイドライン

トランジット VSAN については、次のガイドラインを考慮してください：

- IVR ゾーン メンバーシップの定義に加えて、トランジット VSAN のセットを指定して、2 つのエッジ VSAN 間の接続を提供することもできます。
  - IVR ゾーン内で二つのエッジ VSAN で重なった場合、トランジット VSAN は接続を提供する必要はありません。
  - IVR ゾーン内で二つのエッジ VSAN で重ならない場合、接続を提供するために1 つ以上の中継 VSAN が必要な場合があります。送信元と接続先エッジ VSAN 両方のメンバーのスイッチ上で IVR が有効ではない場合、IVR ゾーン内の二つのエッジ VSAN は重なりません。
- エッジ VSAN の間のトラフィックは、最短 IVR パスのみ通過します。
- 中継 VSAN 情報は、全ての IVR ゾーン セットで共通です。時には中継 VSAN は、別の IVR ゾーンでエッジ VSAN として機能することができます。

ボーダー スイッチ ガイドライン

ボーダー スイッチを構成する前に、次のガイドラインを考慮してください：

- ボーダー スイッチには、Cisco MDS SAN-OS リリース 2.1（1a）以降が必要です。
- ボーダー スイッチは、2 つ以上の VSAN のメンバーである必要があります。
- IVR 通信を容易にする境界スイッチは、IVR 対応である必要があります。
- IVR は、アクティブな IVR ゾーン メンバー間に冗長パスを提供するために、追加のボーダー スイッチで（オプションで）有効にすることができます。
- VSAN トポロジ構成は、境界スイッチが追加または削除されると自動的に更新されます。

IVR NAT を有効にします

ここでは、IVR NAT を有効にする方法と、IVR 自動トポロジモードを有効にする方法について説明します。

IVR NAT を有効にするには、次の手順を実行します：

Procedure

ステップ 1 構成モードに入ります。

switch# **config t**

ステップ 2 スイッチで IVR NAT を有効にします。

switch(config)# **ivr nat**

ステップ 3 スイッチ上の IVR NAT を無効にします（デフォルト）。

switch(config)# **no ivr nat**

IVR 自動トポロジ モードの有効化

Note IVR 自動トポロジモードを構成する前に、IVR 構成の配信を有効にする必要があります（CFS を使用した IVR 構成の配布, on page 7 を参照）。IVR 自動トポロジ モードを有効にすると、IVR 構成の配信を無効にすることはできません。

IVR 自動トポロジ モードを有効にするには、次の手順を実行します：

Procedure

ステップ 1 構成モードに入ります。

switch# **config t**

ステップ 2 IVR 自動トポロジ モードを有効にします。

switch(config)# **ivr vsan-topology auto**

What to do next

自動的に検出された IVR トポロジを表示するには、 **show ivr vsan-topology** コマンドを使用します。

```
switch# show ivr vsan-topology

AFID  SWITCH WWN                Active   Cfg. VSANS
-------------------------------------------------------
   1  20:00:54:7f:ee:1b:0b:d0     yes      no  11,1109
   1  20:00:54:7f:ee:1c:0e:00 *   yes      no  2,11-12,28,1110


Total:   2 entries in active and configured IVR VSAN-Topology
```

Note アスタリスク（*）はローカル スイッチを示します。

IVR NAT モードへの移行

このタスクの目的は、Cisco Fabric Services（CFS）を使用してすべての IVR 対応スイッチに VSAN 間ルーティング（IVR）構成定を有効にして配布し、シームレスな VSAN 間通信のための一貫性のある効率的なファブリック全体の構成を保証することです。

このタスクは、自動音声応答（IVR）システムを構成して有効にするために実行します。このシステムにより、ネットワーク環境内での自動音声インタラクションとアナウンスが可能になり、依存するアプリケーションやサービスとの適切なセットアップと統合が保証されます。

手順

ステップ 1 構成モードを開始します。

例：

```
switch# config t
```

ステップ 2 IVR ゾーンセットを非アクティブ化します。

例：

```
switch(config)# no ivr zoneset activate name IVR_Zoneset force
```

ステップ 3 IVR NAT を有効にします。

例：

```
switch(config)# ivr nat
```

ステップ 4 IVR ゾーンセットをアクティブ化します。

例：

```
switch(config)# ivr zoneset activate name IVR_Zoneset force
```

ステップ 5 IVR ファブリック全体で変更をコミットします。

例：

```
switch(config)# ivr commit
```

IVR 非 NAT モードは廃止され、NX OS リリース 5.2(x) 以降ではサポートされていないため、IVR NAT モードへの適切な移行が必要となっていますが、このタスクにより保証されます。また、この更新には、依存するアプリケーションの停止と、スイッチ間での構成の一貫性のためのCFS配信の使用に関するガイダンスも含まれています。

IVR 仮想ドメイン

リモート VSAN では、IVR アプリケーションは、割り当て済みドメイン リストに仮想ドメインを自動的に追加しません。一部のスイッチ（Cisco SN5428 スイッチなど）は、ファブリック

内の割り当て済みドメイン リストにリモート ドメインが表示されるまで、リモート ネーム サーバーにクエリを実行しません。このような場合は、特定の VSAN 内の IVR 仮想ドメインを、そのVSAN内の割り当て済みドメインリストに追加します。IVRドメインを追加すると、ファブリックに現在存在するすべての IVR 仮想ドメイン（および今後作成される仮想ドメイン）が、その VSAN の割り当て済みドメイン リストに表示されます。

Tip Cisco SN5428 または MDS 9020 スイッチが VSAN に存在する場合は、IVR 仮想ドメインを追加してください。

IVR 仮想ドメインを有効にすると、仮想ドメイン ID の重複が原因でリンクがアップに失敗することがあります。この場合は、重複する仮想ドメインをそのVSANから一時的に取り消します。

Note IVR VSANから重複する仮想ドメインを取り消すと、そのドメインとの間のIVRトラフィックが中断されます。

EXEC モードで **ivr withdraw domain** コマンドを使用すると、影響を受ける VSAN から重複する仮想ドメイン インターフェイスを一時的に取り消すことができます。

Tip 中継 VSAN ではなく、エッジ VSAN にのみ IVR ドメインを追加します。

IVR 仮想ドメインの手動構成

指定した VSAN で IVR 仮想ドメインを手動で構成するには、次の手順を実行します：

Procedure

ステップ 1 構成モードに入ります。

switch# **config t**

ステップ 2 VSAN 1 に IVR 仮想ドメインを追加します。すべての IVR スイッチでこの手順を実行します。

switch(config)# **ivr virtual-fcdomain-add vsan-ranges 1-4093**

ステップ 3 IVR 仮想ドメインを追加しない工場出荷時のデフォルトに戻し、その VSAN の現在アクティブな仮想ドメインを fcdomain マネージャ リストから削除します。

switch(config)# no **ivr virtual-fcdomain-add vsan-ranges 1-4093**

ファブリック全体の IVR 仮想ドメインの手動構成



Note Cisco SAN-OS リリース 3.1（2）の時点で、Cisco ファブリック構成サービス（FCS）は仮想デバイスの検出をサポートしています。FCS 構成 サブモードで **fcs virtual-device-add vsan-ranges** コマンドを実行すると、特定の VSAN またはすべての VSAN で仮想デバイスを検出できます。このコマンドを使用して IVRのためにゾーンされたデバイスを検出する場合、デバイスはリクエスト domain_ID（RDI）を有効にする必要があります。FCS の使用の詳細については、『Cisco MDS 9000 ファミリ NX-OS システム管理構成ガイド』を参照してください。

指定した VSAN にファブリック全体の IVR 仮想ドメインを構成するには、次の手順を実行します：

Procedure

ステップ 1 構成モードに入ります。

switch# **config t**

ステップ 2 VSAN 1 に IVR 仮想ドメインを追加します。すべての IVR スイッチでこの手順を実行します。

switch(config)# **ivr virtual-fcdomain-add 2 vsan-ranges 1-4093**

ステップ 3 ファブリック全体の構成をコミットします。

switch(config)# **ivr commit**

ステップ 4 IVR 仮想ドメインを追加しない工場出荷時のデフォルトに戻し、その VSAN の現在アクティブな仮想ドメインを fcdomain マネージャ リストから削除します。

switch(config)# no **ivr virtual-fcdomain-add2 vsan-ranges 1-4093**

仮想ドメイン構成を確認

IVR 仮想ドメイン構成のステータスを表示するには、 **show ivr virtual-fcdomain-add-status** コマンドを使用します。

```
switch# show ivr virtual-fcdomain-add-status
IVR virtual domains are added to fcdomain list in VSANS: 1
(As well as to VSANs in interoperability mode 2 or 3)
```

IVR fcdomain データベースのクリア

IVR fcdomain データベースをクリアするには、次のコマンドを使用します：

```
switch# clear ivr fcdomain database
```

IVR ゾーンと IVR ゾーン セット

ここでは、IVR ゾーンおよび IVR ゾーン セットの構成について説明します。内容は次のとおりです：

IVR ゾーンについて

IVR 構成の一部として、1 つ以上の IVR ゾーンを構成して、VSAN 間通信を有効にする必要があります。この結果を得るには、各IVRゾーンを（pWWN、VSAN）エントリのセットとして指定する必要があります。ゾーンと同様に、複数の IVR ゾーン セットを 1 つの IVR ゾーンに属するように 構成できます。複数の IVR ゾーン セットを定義し、定義した IVR ゾーン セットの 1 つだけをアクティブにすることができます。

Note すべての IVR 対応スイッチで同じ IVR ゾーン セットをアクティブにする必要があります。

次の表は、IVR ゾーンとゾーンの主な違いを識別します。

***Table 2: IVR* ゾーンとゾーンの主な違い**

IVR ゾーン	ゾーン
IVR ゾーン メンバーシップは、VSAN と pWWN の組み合わせを使用して指定されます。	ゾーンメンバーシップは、pWWN、ファブリック WWN、sWWN、または AFID を使用して指定されます。
デフォルトのゾーン ポリシーは常に拒否（構成不可）です。	デフォルトのゾーン ポリシーは deny（構成可能）です。

IVR ゾーンの制限とイメージのダウングレードに関する考慮事項

次の表に、物理ファブリックごとの IVR ゾーン制限を示します。

***Table 3: IVR* ゾーン制限**

Cisco リリース	IVR ゾーン制限	IVR ゾーン メンバー制限	IVR ゾーン設定制限
SAN-OS リリース 3.0（3 以降）	8000	20,000	32
SAN-OS リリース 3.0（2b）以前	2000	10,000	32

Note 2 つのゾーンに存在する場合、ゾーン メンバーは、2 回数えられます。「データベース マージの注意事項, on page 26」を参照してください。

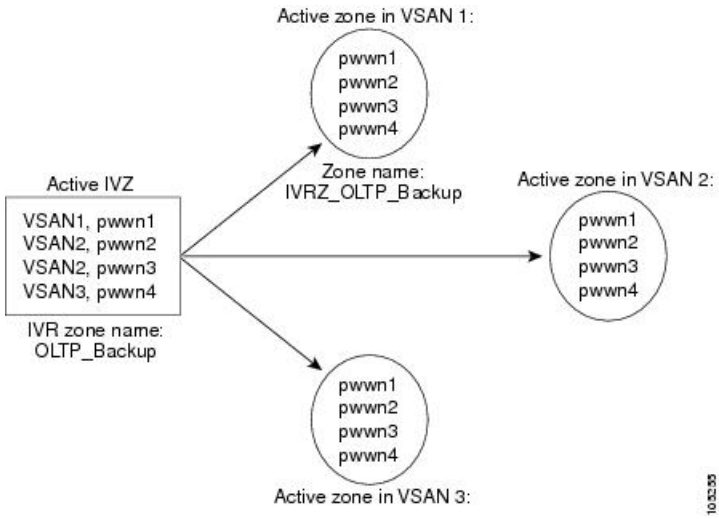
Caution Cisco SAN-OS リリース 3.0（3）より前のリリースにダウングレードする場合、IVR ゾーンの数は 2000 を超えることはできず、IVR ゾーン メンバーの数は 10,000 を超えることはできません。

自動 IVR ゾーン作成

次の図は、4 つのメンバーで構成される IVR ゾーンを示しています。pWWn1 が pWWn2 と通信できるようにするには、それらが VSAN 1 と VSAN 2 の同じゾーンに存在する必要があります。それらが同じゾーンにない場合、ハードゾーン分割 ACL エントリは、pWWn1 が pWWn2 と通信することを禁止します。

各アクティブ IVR ゾーンに対応するゾーンは、アクティブ IVR ゾーンで指定された各エッジ VSAN に自動的に作成されます。IVR ゾーン内のすべての pWWN は、各 VSAN 内のこれらのゾーンのメンバーです。

***Figure 2: IVR* ゾーンのアクティブ化時のゾーンの作成**



ゾーンは、IVR ゾーンセットがアクティブになると、IVR プロセスによって自動的に作成されます。これらはフル ゾーン セット データベースには保存されず、スイッチがリブートしたとき、または新しいゾーンセットがアクティブになったときに失われます。IVR 機能は、これらのイベントをモニターし、新しいゾーンセットがアクティブになると、アクティブな IVR ゾーン セット設定に対応するゾーンを追加します。ゾーン セットと同様に、IVR ゾーン セットも中断なしでアクティブ化されます。

Note pWWn1 と pWWn2 が現在の IVR ゾーン セットと新しい IVR ゾーン セットの IVR ゾーンにある場合、新しい IVR ゾーン セットをアクティブにしても、それらの間のトラフィックは中断されません。

IVR ゾーンおよび IVR ゾーン セット名は、64 文字の英数字に制限されています。

Caution Cisco SAN-OS リリース 3.0（3）より前では、ネットワーク内のスイッチには合計 2000 の IVR ゾーンと 32 の IVR ゾーン セットしか構成できません。Cisco SAN-OS リリース 3.0（3）では、ネットワーク内のスイッチに合計 8000 の IVR ゾーンと 32 の IVR ゾーン セットのみを構成できます。データベース マージの注意事項, on page 26を参照してください。

IVR ゾーンと IVR ゾーン セットの構成

IVR ゾーンおよび IVR ゾーン セットを作成するには、次の手順を実行します：

Procedure

ステップ 1 構成モードに入ります。

switch# **config t**

ステップ 2 sample_vsan2-3 という名前の IVR ゾーンを作成します。

switch(config)# **ivr zone name sample_vsan2-3**

ステップ 3 VSAN 3 の指定された pWWN を IVR ゾーン メンバーとして追加します。

switch(config-ivr-zone)# **member pwwn 21:00:00:e0:8b:02:ca:4a vsan 3**

ステップ 4 VSAN 2 の指定された pWWN を IVR ゾーン メンバーとして追加します。

switch(config-ivr-zone)# **member pwwn 21:00:00:20:37:c8:5c:6b vsan 2**

ステップ 5 コンフィギュレーション モードに戻ります。

switch(config-ivr-zone)# **exit**

ステップ 6 sample_vsan4-5 という名前の IVR ゾーンを作成します。

switch(config)# **ivr zone name sample_vsan4-5**

ステップ 7 VSAN 4 の指定された pWWN を IVR ゾーン メンバーとして追加します。

switch(config-ivr-zone)# **member pwwn 21:00:00:e0:8b:06:d9:1d vsan 4**

ステップ 8 VSAN 4 の指定された pWWN を IVR ゾーン メンバーとして追加します。

switch(config-ivr-zone)# **member pwwn 21:01:00:e0:8b:2e:80:93 vsan 4**

ステップ 9 VSAN 5 の指定された pWWN を IVR ゾーン メンバーとして追加します。

switch(config-ivr-zone)# **member pwwn 10:00:00:00:c9:2d:5a:dd vsan 5**

ステップ 10 コンフィギュレーション モードに戻ります。

switch(config-ivr-zone)# **exit**

ステップ 11 Ivr_zoneset1 という名前の IVR ゾーン セットを作成します。

switch(config)# **ivr zoneset name Ivr_zoneset1**

ステップ 12 sample_vsan2-3 IVR ゾーンを IVR ゾーン セット メンバーとして追加します。

switch(config-ivr-zoneset)# **member sample_vsan2-3**

ステップ 13 sample_vsan4-5 IVR ゾーンを IVR ゾーン セット メンバーとして追加します。

switch(config-ivr-zoneset)# **member sample_vsan4-5**

ステップ 14 コンフィギュレーション モードに戻ります。

switch(config-ivr-zoneset)# **exit**

ステップ 15 新しく作成された IVR ゾーン セットをアクティブにします。

switch(config)# **ivr zoneset activate name IVR_ZoneSet1**

ステップ 16 指定した IVR ゾーン セットを強制的にアクティブにします。

switch(config)# **ivr zoneset activate name IVR_ZoneSet1 force**

ステップ 17 指定された IVR ゾーン セットを非アクティブにします。

switch(config)# **no ivr zoneset activate name IVR_ZoneSet1**

ステップ 18 EXEC モードに戻ります。

switch(config)# **end**

ゾーン セットのアクティブ化と force オプションの使用について

ゾーンセットを作成して設定したら、ゾーンセットをアクティブにする必要があります。IVR ゾーン セットをアクティブにすると、IVR は各エッジ VSAN の通常のアクティブ ゾーン セットに IVR ゾーンを自動的に追加します。VSAN にアクティブ ゾーン セットがない場合、IVR は force オプションを使用して IVR ゾーン セットをアクティブにすることしかできません。これにより、IVR は「nozoneset」と呼ばれるアクティブ ゾーン セットを作成し、そのアクティブ ゾーン セットに IVR ゾーンを追加します。

Caution VSAN で通常のアクティブ ゾーン セットを非アクティブにすると、IVR ゾーン セットも非アクティブになります。これは、通常のアクティブ ゾーン セットの IVR ゾーンと、スイッチとの間で送受信されるすべての IVR トラフィックが停止するために発生します。IVR ゾーン セットを再アクティブ化するには、通常のゾーン セットを再アクティブ化する必要があります。

Note

- 同じファブリック内で IVR と iSLB がイネーブルになっている場合は、ファブリック内の少なくとも 1 つのスイッチで両方の機能をイネーブルにする必要があります。ゾーン分割関連の設定またはアクティブ化の操作（通常のゾーン、IVR ゾーン、または iSLB ゾーンに対して）は、このスイッチ上で実行する必要があります。そうしなければ、ファブリック内のトラフィックが中断される可能性があります。
- セグメント化された VSAN が IVR トポロジに存在する場合、IVR ゾーン セットはアクティブになりません。

force コマンド を使用して、IVR ゾーン セットをアクティブにすることもできます。次の表に、 **force command** オプションを使用する場合と使用しない場合のさまざまなシナリオを示します。

***Table 4: force* コマンドを使用する場合と使用しない場合の *IVR* シナリオ**

大文字/小文字	デフォルト ゾーン ポリシー	IVR ゾーンのアクティブ化前のアクティブ ゾーン セット	force command 使用されるオプション	IVR ゾーン セットのアクティブ化ステータス	アクティブな IVR ゾーンが作成されましたか?	起こりうる中断トラフィック
1	拒否	アクティブ ゾーン セットなし	非対応	エラー	非対応	非対応
2			はい	成功（Success）	はい	非対応
3[1]	拒否	アクティブ ゾーン セットが存在します	×/〇	成功（Success）	はい	非対応
4	許可	アクティブ ゾーン セットがないか、アクティブ ゾーン セットが存在しません	非対応	エラー	非対応	非対応
5			はい	成功（Success）	はい	対応

[1] ケース 3 のシナリオを使用することをお勧めします。

Caution IVR ゾーン セット アクティベーションの **force** コマンド を使用すると、IVR に関与していないデバイスであっても、トラフィックの中断が発生する可能性があります。たとえば、設定にアクティブなゾーン セットがなく、デフォルトのゾーン ポリシーが permit の場合、IVR ゾーン セットのアクティブ化は失敗します。ただし、 **force** コマンド を使用すると、IVR ゾーン セットのアクティブ化は成功します。ゾーンは各 IVR ゾーンに対応するエッジ VSAN で作成されるため、デフォルトのゾーン ポリシーが許可であるエッジ VSAN でトラフィックが中断される可能性があります。

IVR ゾーン セットのアクティブ化または非アクティブ化

既存の IVR ゾーン セットをアクティブまたは非アクティブにするには、次の手順を実行します。

Procedure

ステップ 1 構成モードに入ります。

switch# **config t**

ステップ 2 新しく作成された IVR ゾーン セットをアクティブにします。

switch(config)# **ivr zoneset activate name IVR_ZoneSet1**

ステップ 3 指定した IVR ゾーン セットを強制的にアクティブにします。

switch(config)# **ivr zoneset activate name IVR_ZoneSet1 force**

ステップ 4 指定された IVR ゾーン セットを非アクティブにします。

switch(config)# **no ivr zoneset activate name IVR_ZoneSet1**

What to do next

Note トラフィックを中断せずにアクティブな IVR ゾーン セットを新しい IVR ゾーン セットに置き換えるには、現在のアクティブな IVR ゾーン セットを非アクティブ化せずに、新しい IVR ゾーン セットをアクティブ化します。

IVR ゾーンと IVR ゾーン設定構成の確認

show ivr zone および **show ivr zoneset** コマンドを使用して、IVR ゾーンおよび IVR ゾーン セットの構成を確認します。

IVR ゾーン構成の表示

```
switch# show ivr zone
zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
zone name ivr_qa_z_all
    pwwn 21:00:00:e0:8b:06:d9:1d vsan 1
    pwwn 21:01:00:e0:8b:2e:80:93 vsan 4
    pwwn 10:00:00:00:c9:2d:5a:dd vsan 1
    pwwn 10:00:00:00:c9:2d:5a:de vsan 2
    pwwn 21:00:00:20:37:5b:ce:af vsan 6
    pwwn 21:00:00:20:37:39:6b:dd vsan 6
    pwwn 22:00:00:20:37:39:6b:dd vsan 3
    pwwn 22:00:00:20:37:5b:ce:af vsan 3
    pwwn 50:06:04:82:bc:01:c3:84 vsan 5
```

指定した IVR ゾーンの情報の表示

```
switch# show ivr zone name sample_vsan2-3
zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

アクティブ IVR ゾーン内の指定されたゾーンの表示

```
switch# show ivr zone name sample_vsan2-3 active
zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

IVR ゾーン セット構成の表示

```
switch# show ivr zoneset
zoneset name ivr_qa_zs_all
  zone name ivr_qa_z_all
    pwwn 21:00:00:e0:8b:06:d9:1d vsan 1
    pwwn 21:01:00:e0:8b:2e:80:93 vsan 4
    pwwn 10:00:00:00:c9:2d:5a:dd vsan 1
    pwwn 10:00:00:00:c9:2d:5a:de vsan 2
    pwwn 21:00:00:20:37:5b:ce:af vsan 6
    pwwn 21:00:00:20:37:39:6b:dd vsan 6
    pwwn 22:00:00:20:37:39:6b:dd vsan 3
    pwwn 22:00:00:20:37:5b:ce:af vsan 3
    pwwn 50:06:04:82:bc:01:c3:84 vsan 5
zoneset name IVR_ZoneSet1
  zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

アクティブな IVR ゾーン セット構成の表示

```
switch# show ivr zoneset active
zoneset name IVR_ZoneSet1
  zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

指定された IVR ゾーン セット構成の表示

```
switch# show ivr zoneset name IVR_ZoneSet1
zoneset name IVR_ZoneSet1
  zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

すべての IVR ゾーン セットの簡易情報の表示

```
switch# show ivr zoneset brief Active
zoneset name IVR_ZoneSet1
  zone name sample_vsan2-3
```

アクティブな IVR ゾーン セットの簡単な情報の表示

```
switch# show ivr zoneset brief Active
zoneset name IVR_ZoneSet1
  zone name sample_vsan2-3
```

IVR ゾーン セットのステータス情報の表示

```
switch# show ivr zoneset status
Zoneset Status
_______________
    name               : IVR_ZoneSet1
    state              : activation success
    last activate time : Sat Mar 22 21:38:46 1980
    force option       : off
status per vsan:
_________________
     vsan     status
      ____     ______
        1      active
        2      active
```

Tip IVR 構成に参加しているすべてのボーダー スイッチで、この構成を繰り返します。

Note Cisco ファブリック マネージャを使用して、相互接続された VSAN ネットワーク内のすべての IVR 対応スイッチに IVR ゾーン構成を配信できます。*Cisco* ファブリック マネージャ *VSAN* 間 ルーティング 構成ガイドを参照します。

IVR ゾーン データベースのクリア

ゾーンセットをクリアすると、構成済みゾーンデータベースのみが消去され、アクティブ ゾーン データベースは消去されません。

IVR ゾーン データベースをクリアするには、 **clear ivr zone database** コマンドを使用します。

```
switch# clear ivr zone database
```

このコマンドは、構成されているすべての IVR ゾーン情報をクリアします。

Note **clear ivr zone database**コマンドを実行した後に、明示的に**copy running-config startup-config** コマンドを実行して、スイッチの次の起動時に確実に実行構成が使用されるようにする必要があります。

IVR ロギング

IVR 機能の Telnet または SSH ロギングを構成できます。たとえば、IVR ロギング レベルをレベル 4（警告）に構成すると、重大度が 4 以上のメッセージが表示されます。このセクションの手順を使用して、ロギングレベルを構成および確認します：

IVR ロギング シビラティ レベルの構成

IVR 機能からのロギング メッセージのシビラティ レベルの構成をするには、次の手順を実行します：

Procedure

ステップ 1 構成モードに入ります。

switch# **config t**

ステップ 2 レベル 4（Warning（注意））で、IVR 機能に関する Telnet または SSH ロギングを構成します。その結果、重大度レベルが 4 以上のロギング メッセージが表示されます。

switch(config)# **logging level ivr 4**

ロギング レベル構成の確認

show logging level コマンドを使用して、IVR 機能に構成されているロギング レベルを表示します。

```
switch# show logging level
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
...
ivr                     5                       4
...
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

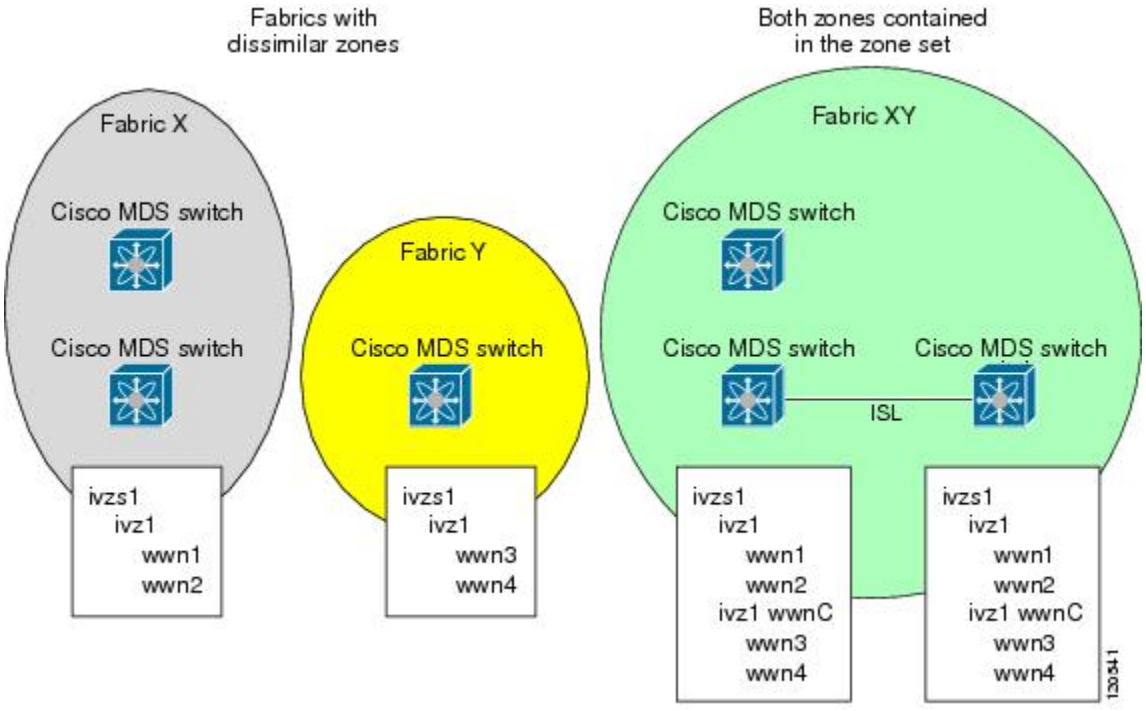
データベース マージの注意事項

データベースのマージとは、構成データベースとアクティブ データベース内のスタティック（学習されていない）エントリの統合を指します。CFS マージ サポートの詳細については、「*Cisco MDS 9000* シリーズ システム 管理構成ガイド」 または、 「*Cisco* ファブリックマネージャ管理構成ガイド」を参照してください。

2 つの IVR ファブリックをマージする場合は、次の点を考慮してください。

- 2 つのファブリックに異なる構成が含まれている場合でも、IVR 構成はマージされます。
- 2 つのマージされたファブリックに異なるゾーンが存在する場合、各ファブリックのゾーンは、適切な名前で分散ゾーン セットに複製されます。

Figure 3: ファブリック マージの結果



- Cisco MDS スイッチごとに異なる IVR 構成を構成できます。

- トラフィックの中断を回避するために、データベースのマージが完了した後の構成は、マージに関連する 2 つのスイッチに存在していた構成の組み合わせになります。
  - 両方のファブリックの構成が異なる場合でも、構成はマージされます。
  - ゾーンとゾーン セットの組み合わせを使用して、マージされたゾーンとゾーン セットを取得します。2 つのファブリックに異なるゾーンが存在する場合、異なるゾーンが適切な名前のゾーン セットに複製されるため、両方のゾーンが存在します。
  - マージされたトポロジには、両方のファブリックのトポロジエントリの組み合わせが含まれます。
  - マージされたデータベースに許容される最大数よりも多くのトポロジエントリが含まれている場合、マージは失敗します。
  - 2 つのファブリックの VSAN の合計数が 128 を超えることはできません。



Note VSAN ID が同じで AFID が異なる VSAN は、2 つの個別の VSAN としてカウントされます。

-
  - 2 つのファブリックの IVR 対応スイッチの合計数が 128 を超えることはできません。
  - 2 つのファブリックのゾーンメンバーの合計数が 10,000 を超えることはできません。Cisco SAN-OS リリース 3.0（3）では、2 つのファブリックのゾーン メンバーの合計数が 20,000 を超えることはできません。ゾーン メンバーは、2 つのゾーンに存在する場合、2 回カウントされます。



Note 1 つ以上のファブリック スイッチが Cisco SAN-OS リリース 3.0（3）以降を実行しており、ゾーン メンバーの数が 10,000 を超えている場合は、ファブリックのゾーン メンバーの数を減らすか、両方のファブリックのすべてのスイッチをアップグレードする必要があります。 Cisco SAN-OS リリース 3.0（3）以降。

-
  - 2 つのファブリックの合計ゾーン数が 2000 を超えることはできません。Cisco SAN-OS リリース 3.0（3）では、2 つのファブリックの合計ゾーン数が 8000 を超えることはできません。



Note ファブリック内の一部のスイッチのみが Cisco SAN-OS リリース 3.0（3）以降を実行しており、ゾーンの数が 2000 を超えている場合は、ファブリック内のゾーンの数を減らすか、両方のファブリックのすべてのスイッチをアップグレードする必要があります。 Cisco SAN-OS リリース 3.0（3）以降。

-
  - 2 つのファブリックの合計数またはゾーン セットが 32 を超えることはできません。

次の表に、さまざまな条件下での 2 つの IVR 対応ファブリックの CFS マージの結果を示します。

Table 5: 2 つの *IVR* 対応ファブリックのマージの結果

IVR ファブリック 1	IVR ファブリック 2	マージ後
NAT 有効	NAT 無効	マージが成功し、NAT が有効になります
自動モードが有効	自動モードが無効	マージが成功し、IVR 自動トポロジ モードが有効になります
競合する AFID データベース	マージに失敗する	
競合する IVR ゾーンセットデータベース	競合を解決するために作成された新しいゾーンでマージが成功する	
組み合わせた構成が制限（ゾーンまたは VSAN の最大数など）を超えている	マージに失敗する	
サービス グループ 1	サービス グループ 2	マージはサービス グループを組み合わせて成功します
ユーザ設定の VSAN トポロジ構成と競合	マージに失敗する	
競合のないユーザー構成の VSAN トポロジ構成	マージに成功しました	

Caution この条件に従わない場合は、マージに失敗します。次の配信がデータベースとファブリック内のアクティベーション ステートを強制的に同期化します。

データベース マージ失敗の解決

マージに失敗した場合は、次の CLI コマンドを使用してエラー状態を表示できます。

- **show ivr merge status**
- **show cfs merge status name ivr**
- **show logging last** *lines*（および MERGE の失敗を探します）

マージの失敗を解決するには、 **show** コマンドの出力に示されている失敗情報を確認し、このリストで失敗に関連するシナリオを見つけ、トラブル シューティングの手順に従います：

Note CFS コミットが成功すると、マージが成功します。

IVR 自動トポロジ モードの構成例

ここでは、IVR 自動トポロジ モードを有効にするための構成手順の例を示します。

Procedure

ステップ 1 ファブリック内のすべての境界スイッチで IVR を有効にします。

Example:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# feature ivr
switch(config)# exit
switch#
```

ステップ 2 すべての IVR 対応スイッチで IVR が有効になっていることを確認します。

Example:

```
switch# show ivr
Inter-VSAN Routing is enabled
Inter-VSAN enabled switches
---------------------------
No IVR-enabled VSAN is active. Check VSAN-Topology configuration.
Inter-VSAN topology status
--------------------------
Current Status: Inter-VSAN topology is INACTIVE
Inter-VSAN zoneset status
-------------------------
    name                :
    state               : idle
    last activate time :
Fabric distribution status
----------------------
fabric distribution disabled
Last Action                : None
Last Action Result         : None
Last Action Failure Reason : None
Inter-VSAN NAT mode status
--------------------------
FCID-NAT is disabled
License status
-----------------
IVR is running based on the following license(s)
ENTERPRISE_PKG
```

ステップ 3 ファブリック内のすべての IVR 対応スイッチで CFS 配信をイネーブルにします。

Example:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ivr distribution
```

ステップ 4 IVR 自動トポロジ モードを有効にします。

Example:

```
switch(config)# ivr vsan-topology auto
fabric is locked for configuration. Please commit after configuration is done.
```

ステップ 5 変更をファブリックにコミットします。

Example:

```
switch(config)# ivr commit
switch(config)# exit
switch#
```

ステップ 6 コミット要求のステータスを確認します。

Example:

```
switch# show ivr session status
Last Action                : Commit
Last Action Result         : Success
Last Action Failure Reason : None
```

ステップ 7 アクティブな IVR 自動トポロジを確認します。

Example:

```
switch# show ivr vsan-topology active
AFID  SWITCH WWN                Active   Cfg. VSANS
-------------------------------------------------------------
   1  20:00:00:0d:ec:08:6e:40 *  yes      no   1,336-338
   1  20:00:00:0d:ec:0c:99:40    yes      no   336,339
```

ステップ 8 IVR ゾーン セットとゾーンを構成します。次の 2 つのゾーンが必要です。

- 1 つのゾーンにはテープ T（pWWn 10:02:50:45:32:20:7a:52）とサーバー S1（pWWn 10:02:66:45:00:20:89:04）があります。
- 別のゾーンにはテープ T とサーバー S2（pWWn 10:00:ad:51:78:33:f9:86）があります。

Tip 2 つの IVR ゾーンを作成する代わりに、テープと両方のサーバーで 1 つの IVR ゾーンを作成することもできます。

Example:

```
mds(config)# ivr zoneset name tape_server1_server2
mds(config-ivr-zoneset)# zone name tape_server1
mds(config-ivr-zoneset-zone)# member pwwn 10:02:50:45:32:20:7a:52 vsan 1
mds(config-ivr-zoneset-zone)# member pwwn 10:02:66:45:00:20:89:04 vsan 2
mds(config-ivr-zoneset-zone)# exit
```

```
mds(config-ivr-zoneset)# zone name tape_server2
mds(config-ivr-zoneset-zone)# member pwwn 10:02:50:45:32:20:7a:52 vsan 1
mds(config-ivr-zoneset-zone)# member pwwn 10:00:ad:51:78:33:f9:86 vsan 3
mds(config-ivr-zoneset-zone)# exit
```

ステップ 9 IVR ゾーン構成を表示して、IVR ゾーン セットと IVR ゾーンが正しく構成されていることを確認します。

Example:

```
mds(config)# do show ivr zoneset
zoneset name tape_server1_server2
  zone name tape_server1
      pwwn 10:02:50:45:32:20:7a:52 vsan 1
      pwwn 10:02:66:45:00:20:89:04 vsan 2
  zone name tape_server2
      pwwn 10:02:50:45:32:20:7a:52 vsan 1
      pwwn 10:00:ad:51:78:33:f9:86 vsan 3
```

ステップ 10 IVR ゾーン セットをアクティブ化する前にゾーン セットを表示します。IVR ゾーン セットをアクティブにする前に、アクティブ ゾーン セットを表示します。VSAN 2 および 3 に対してこの手順を繰り返します。

Example:

```
mds(config)# do show zoneset active vsan 1
zoneset name finance_dept vsan 1
  zone name accounts_database vsan 1
    pwwn 10:00:23:11:ed:f6:23:12
    pwwn 10:00:56:43:11:56:fe:ee

  zone name $default_zone$ vsan 1
```

ステップ 11 設定された IVR ゾーン セットをアクティブにします。

Example:

```
mds(config)# ivr zoneset activate name tape_server1_server2
zoneset activation initiated. check inter-VSAN zoneset status
mds(config)# exit
mds#
```

ステップ 12 IVR ゾーン セットのアクティブ化を確認します。

Example:

```
mds# show ivr zoneset active
zoneset name tape_server1_server2
  zone name tape_server1
      pwwn 10:02:50:45:32:20:7a:52 vsan 1
      pwwn 10:02:66:45:00:20:89:04 vsan 2
  zone name tape_server2
      pwwn 10:02:50:45:32:20:7a:52 vsan 1
      pwwn 10:00:ad:51:78:33:f9:86 vsan 3
```

ステップ 13 ゾーン セットの更新を確認します。IVR ゾーン セットのアクティブ化が成功したら、適切なゾーンがアクティブ ゾーン セットに追加されていることを確認します。VSAN 2 および 3 に対してこの手順を繰り返します。

Example:

```
mds# show zoneset active vsan 1
zoneset name finance_dept vsan 1
  zone name accounts_database vsan 1
    pwwn 10:00:23:11:ed:f6:23:12
    pwwn 10:00:56:43:11:56:fe:ee

  zone name IVRZ_tape_server1 vsan 1
    pwwn 10:02:66:45:00:20:89:04
    pwwn 10:02:50:45:32:20:7a:52

  zone name IVRZ_tape_server2 vsan 1
    pwwn 10:02:50:45:32:20:7a:52
    pwwn 10:00:ad:51:78:33:f9:86

  zone name $default_zone$ vsan 1
mds# show ivr zoneset status
Zoneset Status
_______________
    name               : tape_server1_server2
    state              : activation success
    last activate time : Tue May 20 23:23:01 1980
    force option       : on
status per vsan:
__________________
     vsan     status
     ____     ______
     1        active
```

デフォルト設定

次の表に、IVR パラメータのデフォルト設定を示します。

Table 6: デフォルトの ***IVR*** パラメータ

パラメータ	デフォルト
IVR 機能	無効（Disabled）
IVR VSAN	仮想ドメインに追加されていません
IVR NAT	無効（Disabled）
IVR ゾーンの QoS	低
構成の配布	無効化

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。