Service Advertisement Framework コンフィギュレーション ガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください 1

SAF の設定 3

機能情報の確認 3

Cisco SAF の前提条件 4

Cisco SAF の制限事項 4

Cisco SAF に関する情報 4

Cisco SAF の概要 4

Cisco SAF Forwarder の概要 5

Cisco SAF Client の概要 5

XMCP の概要を使用する外部 Cisco SAF クライアント 7

Cisco SAF サービス ID 番号のフォーマット 7

Cisco SAF とネットワークにおけるドメインの役割 8

Cisco SAF 仮想ルータ 9

Cisco SAF ネイバー関係 10

Cisco SAF のメリット 10

Cisco SAF Forwarder の設定方法 12

Cisco SAF の有効化 12

Cisco SAF のインターフェイス固有コマンドの設定 13

マルチトポロジ ネットワーク用の Cisco SAF の設定 14

Cisco SAF の静的ネイバー関係の設定 16

Cisco SAF のスタブ ルーティングの設定 17

Cisco SAF のルート認証の設定 18

ネイバー変更と警告のログの設定 21

Cisco SAF に使用されるリンク帯域幅の割合の設定 23

Cisco SAF インターフェイスのメトリック ダンプニング インターバルの設定 24

変更ベースのダンプニング設定 25

インターバル ベースのダンプニング設定 27

hello パケット間のインターバルとホールド タイムの調整 28
スプリット ホライズンの無効化 30
メトリック最大ホップ カウントの設定 32
Cisco SAF External Client の設定方法 33
前提条件 34
Cisco SAF External Client の設定 34
Cisco SAF の統計情報の表示方法 37
Cisco SAF 設定から情報を削除する方法 42
Cisco SAF の設定例 43
例：Cisco SAF の有効化 43
例：Cisco SAF インターフェイスの設定 43
例：Cisco SAF トポロジの設定 44
例：Cisco SAF スタブ ルーティングの設定 44
例：IP-RIP を使用する Cisco SAF の設定 45
例：OSPF を使用する Cisco SAF の設定 45
例：EIGRP を使用する Cisco SAF の設定 45
例：別々の LAN 上に配置された Cisco SAF Forwarder の設定 45
集中型 Cisco SAF Forwarder の設定例 46
例：Cisco SAF Client の設定 46
その他の参考資料 48
Cisco SAF の機能情報 49
Extensible Messaging Control Protocol の設定 53
機能情報の確認 54
XMCP の前提条件 54
XMCP に関する情報 54
XMCP の設定方法 55
基本的な XMCP サーバの設定 55
高度な XMCP サーバの設定 57
XMCP クライアントおよびサーバ情報の表示 60
XMCP の設定例 61
例：XMCP サーバと Cisco SAF Forwarder の設定 61
その他の参考資料 61

XMCP に関する機能情報 63
動的ネイバーの設定 65
機能情報の確認 66
動的ネイバーの前提条件 66
動的ネイバーの制約事項 66
動的ネイバーに関する情報 67
リモート ネイバー セッション ポリシー 67
ネイバー フィルタ リスト 67
最大リモート ネイバー 68
ネイバーのフィルタ リスト、および最大リモート ネイバーの設定の変更 68
ネイバー タイプ 68
リモート ユニキャスト リッスン（ポイントツーポイント）ネイバー 69
リモート マルチキャスト グループ（マルチポイントツーマルチポイント）ネイバー 69
リモート ネイバー設定の継承と優先度 70
動的ネイバーの設定方法 70
動的ネイバーの設定例 72
例：Cisco SAF の動的ネイバーの設定 72
その他の参考資料 73
動的ネイバーの機能情報 74
機能マネージャの設定 75
機能情報の確認 75
機能マネージャの設定の前提条件 75
機能マネージャに関する情報 76
機能の検出 76
SAF Forwarder との相互運用性 76
機能情報 76
機能グループ 77
ハードウェア グループ情報 77
ソフトウェア グループ情報 77
機能データの XML スキーマ 78
機能マネージャの設定方法 80

機能マネージャの有効化および無効化 **80**

機能マネージャ情報の表示 **81**

登録済み機能情報の削除 **83**

その他の参考資料 **84**

機能マネージャの機能情報 **85**

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

Cisco IOS XE Release 3.7.0E（Catalyst スイッチ用）および Cisco IOS XE Release 3.17S（Access および Edge ルーティング用）より、この 2 つのリリースは集約されたリリース Cisco IOS XE 16 の 1 つのバージョンに進化（マージ）します。1 つのリリースでスイッチおよびルーティング ポートフォリオ内の Access や Edge 製品を幅広くカバーします。

（注） テクノロジーの設定ガイドの機能情報の表には、機能が導入された時期についても記載されています。その機能が他のプラットフォームでサポートされた時期については、記載されている場合とされていない場合があります。特定の機能がお使いのプラットフォームでサポートされているかどうかを確認するには、該当製品のランディング ページに掲載されているテクノロジー コンフィギュレーション ガイドをご覧ください。テクノロジー コンフィギュレーション ガイドがご使用の製品のランディング ページに表示された場合は、その機能がそのプラットフォームでサポートされていることを意味します。

第 2 章

SAF の設定

- 機能情報の確認，3 ページ
- Cisco SAF の前提条件，4 ページ
- Cisco SAF の制限事項，4 ページ
- Cisco SAF に関する情報，4 ページ
- Cisco SAF Forwarder の設定方法，12 ページ
- Cisco SAF External Client の設定方法，33 ページ
- Cisco SAF の統計情報の表示方法，37 ページ
- Cisco SAF 設定から情報を削除する方法，42 ページ
- Cisco SAF の設定例，43 ページ
- その他の参考資料，48 ページ
- Cisco SAF の機能情報，49 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Cisco SAF の前提条件

- Cisco SAF を設定する前に、このマニュアルに記載された概念を理解しておく必要があります。
- 別の LAN 上に配置された Cisco SAF Forwarder のネイバー関係を設定する前に、各 Cisco SAF Forwarder 間の IP ルーティングが設定されていることを確認してください。

Cisco SAF の制限事項

- Cisco SAF は、Cisco EIGRP ルーティングとは無関係に動作します。

Cisco SAF に関する情報

Cisco SAF の概要

Cisco SAF は、ネットワークに接続されたリソースの存在、位置、および設定をアプリケーションで検出可能にするフレームワークを提供します。Cisco SAF を使用すれば、アプリケーションでネットワーク上のサービスをアドバタイズまたは検出することによって、ネットワーク上のサービスのタイムリーで信頼できる認識が可能になります。サービス情報は、サービスの内容を効率的に配信してその検出を促進する特定の機能を担う Cisco SAF 共同ノードのネットワークを通して配信されます。

非 SAF ノードとは、SAF を認識しないネットワーク上のノードのことです。非 SAF ノードは、「ダーク ネット」と呼ばれており、ISP を通過するために必要です。Cisco SAF メッセージは IP ベースのため、ダーク ネットの影響を受けません。

これらの Cisco SAF 共同ネットワーク ノードは、次の 2 つの機能的役割に分類されます。

- Cisco SAF Forwarder：サービス情報をネットワーク上で配布し、これらのサービスをネットワークでクライアントによって検出可能にします
- Cisco SAF Client：サービスがアドバタイズされ、検出できます

有効な Cisco SAF ネットワークでは両方の役割が設定されている必要があります。

ここでは、次の情報を提供します。

Cisco SAF Forwarder の概要

Cisco SAF Forwarder は、Cisco SAF Client がアドバタイズしたサービスを受信して、そのサービスをネットワークを通して安全に配信し、他の Cisco SAF Client がそのサービスを利用できるようにします。Cisco SAF Forwarder の特徴：

- サービス アドバタイズメントの信頼できる配信を保証します。
- パスの冗長性に関する情報を保持します。
- スケーラブルです。
- ターゲットを絞ったマルチキャストおよびユニキャスト メッセージを使用することによって、ネットワーク帯域幅の使用を最小限に抑えます。

Cisco SAF Forwarder は、サービス アドバタイズメントを他の Cisco SAF Forwarder に伝搬させたり、LAN、構内ネットワーク、WAN、または ISP を通して伝搬させたりすることができます。

基本 Cisco SAF Forwarder は、Cisco SAF Client 間の関係とフレームワークを提供します。Cisco SAF Forwarder の多くは、ネットワークの端または境界に配置されます。Cisco SAF Forwarder は、サービスアドバタイズメントを受信して、そのコピーを保存してから、ネイバー SAF ノードに転送します。クライアントとフォワーダの関係は、アドバタイズメントを維持することです。クライアントがサービスを削除したり、フォワーダ ノードから切断したりした場合は、そのノードから使用できなくなったサービスに関するフレームワークが通知されます。あるフォワーダ ノードで別のフォワーダ ノードからのアドバタイズメントが受信された場合は、その全体（ヘッダーと不明瞭なデータ）のコピーが保存され、他の SAF ピアに転送されます。

有効なすべてのインターフェイスに対してサービスの動的検出を自動的に許可するように LAN 上の Cisco SAF Forwarder を設定すると同時に、他のインターフェイスがサービスを検出するのをブロックするインターフェイス（静的設定）を指定できます。

Cisco SAF Forwarder は、SAF ネイバー ノードにサービス メタデータを送信できます。メタデータは XML 情報であり、サービス データは、サーバが自分自身についてクライアントと通信する情報です。サービス メタデータは EIGRP/SAF のバージョンがアップグレードされるまで、混在環境では伝播されません。

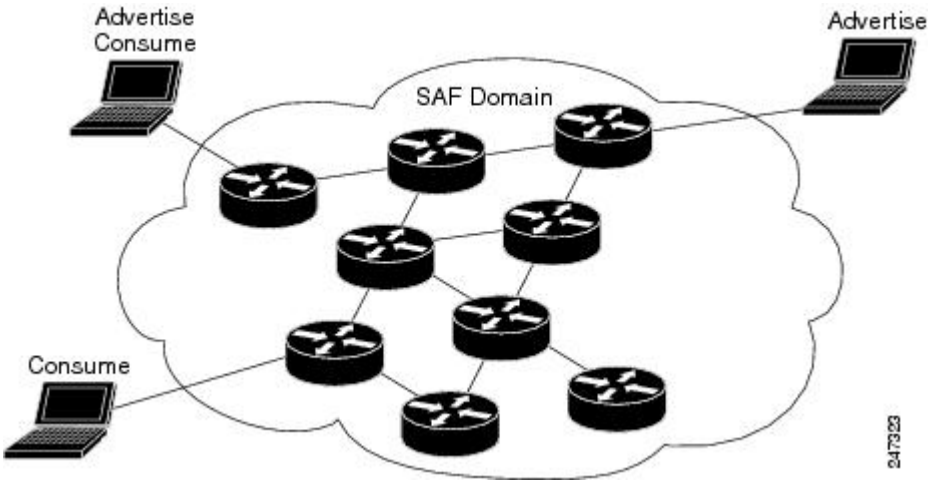
サービスの動的検出を自動的に許可するように非 SAF ノード上の Cisco SAF Forwarder を設定できます。たとえば、Cisco SAF Forwarder は共通のピア グループに属しています。Cisco SAF Forwarder のペア間の静的設定（ユニキャスト）を作成することもできます。

（注） サービスの動的検出を許可するには、マルチキャスト ルーティングが必要です。

Cisco SAF Client の概要

Cisco SAF Client は、サービスの製作者（ネットワークにアドバタイズする）と消費者（ネットワークにサービスを要求する）のどちらかまたはその両方です。Cisco SAF Client から Cisco SAF Forwarder に登録メッセージが送信されると、Cisco SAF Forwarder との関係が確率されます。Cisco

SAF Forwarder は、この登録メッセージを使用して、その Cisco SAF Client を同じフォワーダに接続されている他のクライアントから区別する一意のハンドルを取得します。Cisco SAF Client は、登録しなければ、サービスをアドバタイズ（パブリッシュ）または要求（サブスクライブ）することができません。次の図は、一般的な Cisco SAF ネットワークを示します。



サービスをアドバタイズするときに、Cisco SAF Client は、提供するサービスに関する情報を含むアドバタイズメントを Cisco SAF Forwarder にパブリッシュ（送信）します。サービスは、一意のサービス ID、サブサービス ID、およびインスタンス ID によって識別され、サービス データによって記述されます。サービスの識別子の詳細については、「Cisco SAF サービス ID 番号のフォーマット」を参照してください。Cisco SAF Client は、新しいサービスのアドバタイズごとにパブリッシュ要求を送信できます。Cisco SAF Forwarder は、Cisco SAF Client がパブリッシュしたすべてのサービスをアドバタイズします。Cisco SAF Client は同じサービスの新規発行要求を送信することで、既存のサービスのアドバタイズメントを更新できます。また、クライアントは、既存のサービス アドバタイズメントのいずれかを削除する非公開の要求を生成することもできます。

サービスを要求するときに、Cisco SAF Client は、サブスクライブ要求を使用してサービスの要求通知を送信します。サブスクライブ要求には、Cisco SAF Client に必要なサービス セットが記述されたフィルタが含まれています。この要求に応答して、Cisco SAF Forwarder は、一連の通知要求で、フィルタと一致する最新のサービス セットを Cisco SAF Client に送信します。パブリッシュ要求と同様に、Cisco SAF Client は、新しいフィルタを使用するたびにサブスクライブ要求を生成する必要があります。Cisco SAF Client は、既存のサブスクリプションのいずれかを削除するサブスクライブ解除要求も生成できます。

Cisco SAF Client は内部（Cisco SAF Forwarder に常駐している）または外部（他のデバイスに存在し、XMCP プロトコルを使用して Cisco SAF フォワーダと通信する）のいずれかです。内部 Cisco SAF Client には、機能マネージャ（「機能マネージャの設定」を参照）および Cisco Unified Communications Manager Express（Cisco Unified CME）が含まれます。XMCP を使用する外部 Cisco SAF Client には、Cisco Unified Communications Manager が含まれます。

XMCP の概要を使用する外部 Cisco SAF クライアント

外部 Cisco SAF クライアントは XMCP サーバとして設定された Cisco SAF Forwarder への TCP 接続を開始します。TCP 接続が確立されると、クライアントは Cisco SAF Forwarder へ XMCP 登録メッセージを送信することにより、この接続上で XMCP セッションを開始します。

XMCP セッションはセキュリティのためにユーザ名とパスワードを使用します。

- ユーザ名は XMCP サーバ（Cisco SAF Forwarder）への XMCP クライアント（Cisco SAF クライアント）からの要求に含まれます。
- パスワードは要求で送信されないが、クライアントが要求に付加されるメッセージ整合性値を計算するために使用される共有秘密です。

XMCP サーバが要求を受信すると、要求内でユーザ名属性を検索し、それをパスワードのローカル コピーにアクセスするために使用し、要求に対する独自のメッセージ整合性値を計算します。計算が一致すると、パスワードが一致するはずで、要求が認証されて、XMCP クライアントが Cisco SAF クライアントとして機能することが許可されます。一致しないと、パスワードが正しくなく、要求は拒否されます。

XMCP のセッションが正常に確立されると、XMCP クライアントは XMCP パブリッシュ、非パブリッシュ、登録、および登録解除要求を送信できます。サーバがこのような要求を受信し、正常に認証すると、同等の Cisco SAF クライアント要求に変換し、Cisco SAF Forwarder に送信します。同様に、フォワーダからの Cisco SAF Client 通知要求は XMCP 通知要求に変換され、XMCP クライアントに送信されます。

外部 Cisco SAF クライアントがネットワーク停止時に Cisco SAF ネットワークへの接続を失う可能性があるため、Cisco SAF Forwarder は、Cisco SAF クライアントの有効性に関する定期的な検証を要求し、Cisco SAF ネットワークにサービスをアドバタイズします。XMCP では、これは登録時にクライアントとサーバ間で有効性タイマーを交換することによって実現されます。XMCP クライアントは要求の間隔がこの値を超えないようにする責任があります。XMCP クライアントには送信するデータ（パブリッシュまたは登録）がないので、サーバのタイマーを更新するために、小さなキープアライブ メッセージを生成します。

Cisco SAF Forwarder は、有効性タイマーと同じ時間内にクライアントから XMCP 要求が送信されなかった場合に、外部 Cisco SAF Client を故障中と見なします。Cisco SAF Forwarder が Cisco SAF Client の故障を検出すると、そのクライアントの代わりに、アドバタイズされたサービスをネットワークから削除して、そのクライアントが設定したすべてのサブスクリプションを抹消します。有効性タイマーの期限切れを待つ代替として、Cisco SAF クライアントは手動で登録を解除（XMCP のセッションを終了する登録解除要求を送信）して、正常に Cisco SAF Forwarder にすべてのサービスとサブスクリプションを終了させることができます。

Cisco SAF サービス ID 番号のフォーマット

サービスとは、ある Cisco SAF Client アプリケーションでアドバタイズすることによって、他の Cisco SAF Client アプリケーションで使用可能になる情報のことです。サービス アドバタイズメントはサービス データで構成されます。また、サービス アドバタイズメントはヘッダー データを

使用してフォワーダ間で伝搬されます。サービスの受信を希望する Cisco SAF Client は、サービスヘッダーとサービス データを調査することができます。

サービス ID 番号がネットワーク上のサービスを一意に識別します。次の例は、サービス ID 番号のフォーマットを示しています。

```
service:sub-service:instance.instance.instance.instance
```

サービス ID は、アドバタイズするメジャー サービスの 16 ビットの 10 進識別番号です。メジャーサービスとは、Cisco Unified Communications（UC）などの特定のテクノロジー領域を意味します。サービス ID は、SAF クライアントが必要なさまざまなお客様にシスコから割り当てられます。

次の例は、IP Everywhere と Cisco Unified Communications のサービス ID 値を示しています。

```
Cisco Defined Numbers
    SAF_SERVICE_ID_IPE              = 100   ! IP Everywhere
    SAF_SERVICE_ID_UC               = 101   ! Unified Communications
```

サブサービス ID は、アドバタイズするマイナー サービスの 16 ビットの 10 進識別番号です。サブサービス（マイナーサービスとも呼ばれる）とは、テクノロジー内部のサービスタイプを意味します。たとえば、UC 内部には次のようなサブサービスがあります。

- サブサービス 1 は TDM ゲートウェイです。
- サブサービス 2 はホステッド DN です。
- インスタンスが、この種のサービスのサービス アドバタイズメントを識別します。たとえば、サービス ID が「101:1:abcd.1234.ef.678」の場合は、特定の場所（インスタンス abcd.1234.ef.678）にある Communications Manager クラスタによって通知された UC（サービス 101）TDM ゲートウェイ（サブサービス 1）のアドバタイズメントを意味します。

インスタンス ID は、アドバタイズされた特定のサービスを識別する一意の 128 ビット値です。

クライアント チームがサブサービスの使用方法とアプリケーションのインスタンス値を定義します。クライアントは、Cisco SAF ドメインにおけるインスタンスの一意性を保証する必要があります。

Cisco SAF とネットワークにおけるドメインの役割

ネットワーク サービスの種類と数が増えるほど、これらのサービスのタイムリーで信頼できる認識の実現が、生産性と効率性の向上に大きく貢献することになります。WAN 上でサービス可用性の認識を伝搬させる場合の最重要課題の 1 つがスケーラビリティです。ネットワークの成長に合わせて、ネットワーク上のデバイスから提供されるサービスも増加します。サービス アドバタイズメントに関与するプロトコルは、この増加した負荷を処理するためにスケールする必要があります。このようなプロトコルは、変化に迅速に対応し、新しい情報をタイムリーに生成する必要もあります。

Cisco SAF は、企業のサービス拠点向けのスケーラブルなソリューションとして設計されており、LAN および WAN のインターネット セグメントをカバーすることができます。企業向けソリューションの Cisco SAF は、ドメインを使用して大規模ネットワークにスケールするように設定できます。Cisco Enhanced Interior Gateway Routing Protocol（EIGRP）では、ルートを階層的に検索可能

な自律システムの概念が定義されていますが、Cisco SAF でも、ドメインとサブドメインの同様の概念を採用しています。

Cisco SAF は、IP マルチキャストと呼ばれる動的なピア検出およびサービス アドバタイズメント伝搬技術を提供します。IP マルチキャストでは、IP Cisco SAF Forwarder（IP サブネット同士を接続してイントラネットを形成するデバイス）同士が協力する必要があります。ただし、IP マルチキャストがイントラネット全体に実装されない場合があります。IP マルチキャストが存在しない場合は、Cisco SAF が、設定されたサブネット内または IP マルチキャストがサポートされているサブネット グループ内で動作します。

Cisco SAF Forwarder が、ドメインとサブドメインの 2 つのプライマリ タイプ管理ドメイン（AD）を提供します。ドメインとサブドメインは、1 つの注目すべき例外を除いて、同様に機能します。サブドメインでは、一意のネイバー関係が構築されない代わりに、シングル ピアリングが使用されます。

ネットワーク上には、すべてのサービスをアドバタイズするためのドメインが 1 つだけ存在するのが理想的です。ただし、スケーリングやポリシーの問題を考えると、ネットワークによって複数ドメインが必要な場合があります。単一ドメインの使用をお勧めします。次のような場合は、複数ドメインの使用を検討してください。

- 30,000 を超えるサービスが 1 つのドメインに登録されている。
- サービスの伝搬を制限するためにサービスを論理的にグループ分けする必要がある。

アクセスが許可されていないユーザによるサービスの閲覧を防止するには、閉じたグループが必要です。

サービスの再分配によって、複数のドメイン間でサービス情報を交換することができます。サービスをネットワークの特定の領域に限定したり、特定のネットワーク上のサービス数を制限したりしなければならない場合があります。複数ドメインを使用する必要がある場合は、サービス アドバタイズメントの再分配が解決策になる可能性があります。

ネットワーク上の各ドメインは、1 つずつの管理ドメイン（AD）に分けられています。同じ AD 内のすべての Cisco SAF Forwarder（同じドメインを実行している）は、AS 全体の情報を把握しています。2 つ以上の管理ドメインを接続している Cisco Forwarder は、境界フォワーダと呼ばれています。境界フォワーダが、AS 間でサービス情報をアドバタイズします。複数の境界フォワーダを使用してループ（ある AD から入手された情報がその AD に戻される）を回避する場合は、設計を慎重に検討する必要があります。

Cisco SAF 仮想ルータ

Cisco EIGRP Service-Family Support は、独立して動作する複数のインスタンスの設定を可能にする名前付き設定を拡張したものです。基本の Cisco EIGRP パケット エンコードに仮想ルータ ID（VRID）が追加されたことによって、複数インスタンスが可能になります。

仮想ルータが作成されるたびに、VRID が、トップ レベル ルータに割り当てられ、その下に設定されたアドレス ファミリとサービス ファミリで共有されます。

Cisco SAF ネイバー関係

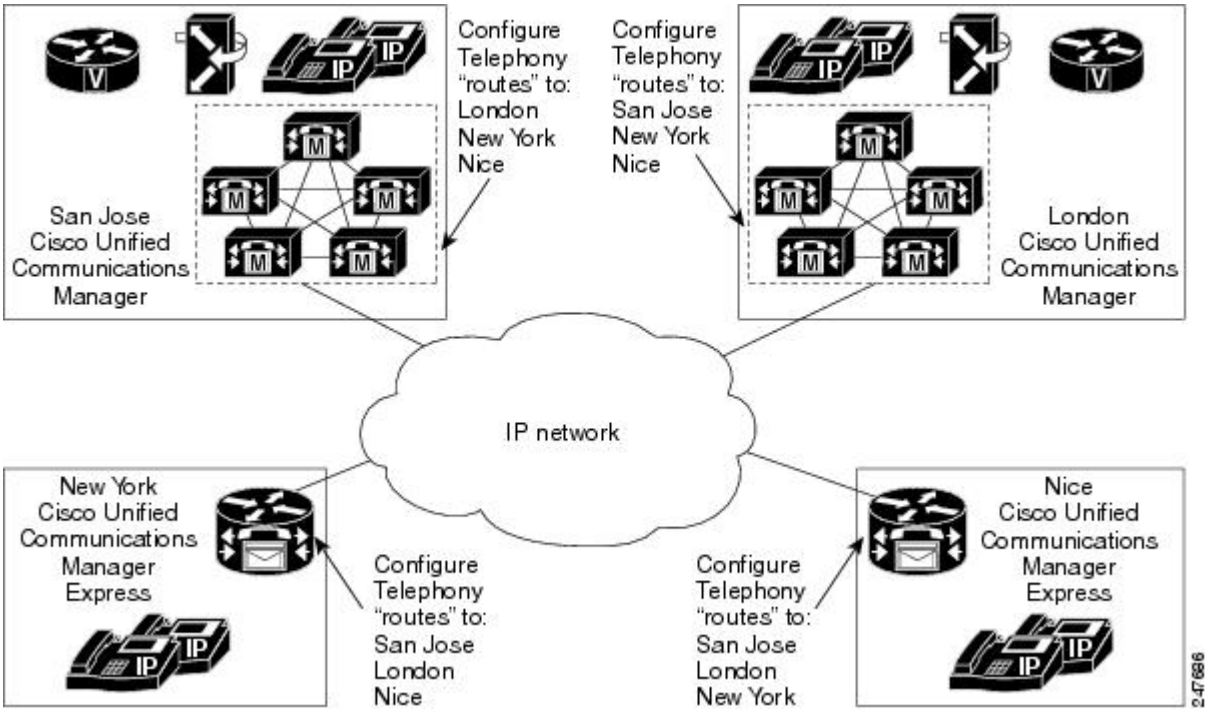
Cisco SAF Forwarder は、Cisco SAF Forwarder プロトコルをサポートするルータが存在しないネットワーク上で動作できます。このようなネットワークは「ダーク ネット」と呼ばれています。Cisco SAF（IP クラウド）をサポートしていない IP ネットワーク上で Cisco SAF Forwarder を設定する方法が 2 つあります。1 つはユニキャスト Cisco SAF ネイバーで、もう 1 つはマルチキャスト Cisco SAF ネイバーです。

ユニキャスト設定を使用すれば、ネイバーとの信頼できるポイントツーポイント隣接関係を構築することができます。Cisco SAF Forwarder の数が増えた場合は、マルチキャストを使用して、複数の Cisco SAF ネイバー間の効率的な転送を実現することができます。1 つの IP マルチキャスト グループ アドレスを使用して、複数の Cisco SAF ネイバーが 1 つのピアグループ内で SAF 情報を交換することができます。

Cisco SAF のメリット

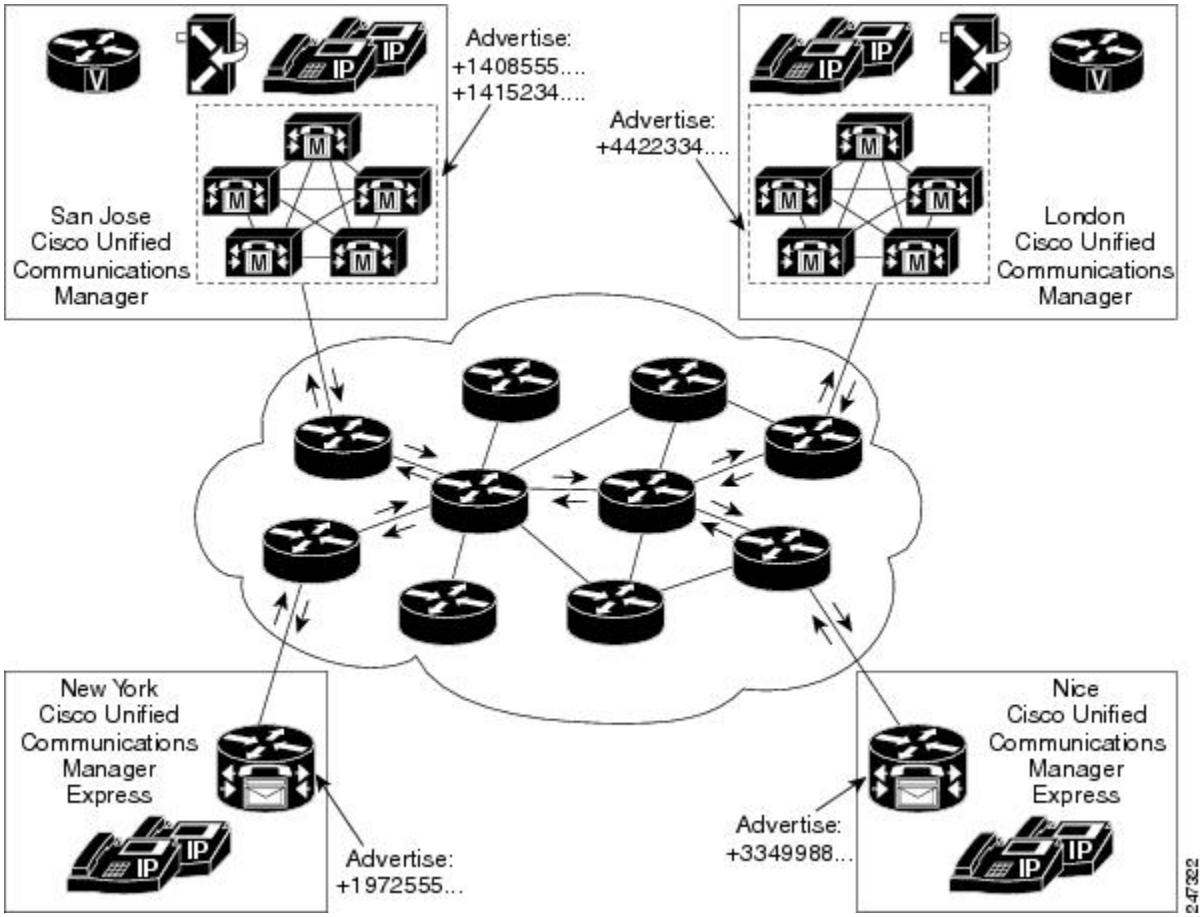
従来、ネットワーク上のサービスを特定するには、ネットワーク アプリケーションに必要なサービスのホスト名とネットワーク アドレスを設定するか、ネットワーク アプリケーションで DNS などのオーバーレイ メカニズムを使用する必要がありました。サービスアドバタイズメントをサポートする既存のプロトコルでは、リソース使用の定期的な通知が提供されます。このようなネットワーク サービスの多くは LAN ベースです。

次の図 に、従来の設定方法が必要な Cisco Unified Communications Manager ネットワークを示します。



Cisco SAF は、ネットワークに接続されたサービスの存在、位置、および設定をネットワーク アプリケーションで自動的に検出可能にするフレームワークを提供します。このサービスの自動検出によって、頻繁に設定を変更しなければならないダイヤル プランなどの複雑な設定を手動で入力する必要がなくなります。また、Cisco SAF を使用すれば、アプリケーションでサービスをアドバタイズしたり、検出したりできます。さらに、1 つの設定を作成すれば、情報が必要なすべてのデバイスにその設定を伝搬させることができます。

次の図に、Cisco SAF を使用した Cisco Unified Communications Manager ネットワークを示します。



Cisco SAF Client は、Cisco SAF Forwarder と同じルータ上に設定することも、外部ルータ上に設定することもできます。

Cisco SAF Forwarder の設定方法

Cisco SAF の有効化

Cisco SAF を有効にして Cisco SAF サービス検出プロセスを作成するには、次のコマンドを使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routereigrp***virtual-instance-name*
4. **service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number*
5. **exit-service-family**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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。
ステップ 3	**routereigrp***virtual-instance-name* 例： `Router(config)# router eigrp saf`	グローバル コンフィギュレーション モードで EIGRP 仮想インスタンスを有効にします。
ステップ 4	**service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number* 例： `Router(config-router)# service-family ipv4 autonomous-system 4453`	ルータ上で指定された自律システム用の Cisco SAF サービス ファミリを有効にします。

	コマンドまたはアクション	目的
ステップ 5	**exit-service-family** 例： `Router(config-router-sf)# exit-service-family`	サービス ファミリ コンフィギュレーション モードを終了します。

Cisco SAF のインターフェイス固有コマンドの設定

Cisco SAF は、インターフェイス固有コマンドの継承優先を提供します。sf-interface コンフィギュレーション モードで実施された設定は、特定の sf-interface 設定や工場出荷時のデフォルト設定よりも優先されます。Cisco SAF のサービス ファミリの下でインターフェイス固有コマンドを設定するには、次のコマンドを使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routereigrp***virtual-instance-name*
4. **service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number*
5. **sf-interface***interface-nameinterface-number*
6. **sf-interface**
7. **exit-sf-interface**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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 3	**routereigrp***virtual-instance-name* 例： `Router(config)# router eigrp saf`	グローバルコンフィギュレーションモードで EIGRP 仮想インスタンスを有効にします。
ステップ 4	**service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number* 例： `Router(config-router)# service-family ipv4 autonomous-system 4453`	デフォルトで有効になっている、ルータ上で指定された自律システム用の Cisco SAF サービス ファミリを作成します。
ステップ 5	**sf-interface***interface-nameinterface-number* 例： `Router(config-router-sf)# sf-interface ethernet 0/0`	ルータ上で指定されたインターフェイスのサービス ファミリ インターフェイス コンフィギュレーション モードを有効にします。
ステップ 6	**sf-interface** 例： `Router(config-router-sf-interface)# sf-interface hello-interval 10`	設定に必要な適切な **interface** コマンドを入力します。
ステップ 7	**exit-sf-interface** 例： `Router(config-router-sf-interface)# exit-sf-interface`	サービス ファミリ インターフェイス コンフィギュレーション モードを終了します。

マルチトポロジ ネットワーク用の Cisco SAF の設定

次の設定を使用して、クライアントを登録し、名前付きトポロジにサービスをパブリッシュまたはサブスクライブします。既存のトポロジ名を使用して 2 つ目のトポロジを別の ID に設定した場合は、同じトポロジの 2 つの ID が作成されるのではなく、既存のトポロジが置き換えられます。

マルチトポロジ ネットワーク用の Cisco SAF を設定するには、次のコマンドを使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routereigrp***virtual-instance-name*
4. **service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number*
5. **topologybase**
6. **exit-sf-topology**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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。
ステップ 3	**routereigrp***virtual-instance-name* 例： `Router(config)# router eigrp saf`	グローバル コンフィギュレーション モードで EIGRP 仮想インスタンスを有効にします。
ステップ 4	**service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number* 例： `Router(config-router)# service-family ipv4 autonomous-system 4453`	ルータ上で指定された自律システム用の Cisco SAF サービス ファミリを有効にします。
ステップ 5	**topologybase** 例： `Router(config-router-sf)# topology base`	サービス ファミリ インターフェイス トポロジコンフィギュレーションモードを有効にして、ルータ上で指定されたインターフェイス用のトポロジベースを作成します。

	コマンドまたはアクション	目的
ステップ 6	**exit-sf-topology** 例： `Router(config-router-sf-topology)# exit-sf-topology`	サービス ファミリ インターフェイス トポロジ コンフィギュレーション モードを終了します。

Cisco SAF の静的ネイバー関係の設定

次のコマンドを使用して、Cisco SAF Forwarder 間の静的ネイバー隣接関係を設定します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routereigrp***virtual-instance-name*
4. **service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number*
5. **neighbor**{*ip-address* {*interface-typeinterface-number}*|**description***word*|**maximum-service}** | **maximum-service***number[threshold-value]* [**dampened** | **reset-time** | **restart***interval* | **restart-count** | **warning-only**]}
6. **exit-service-family**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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。
ステップ 3	**routereigrp***virtual-instance-name* 例： `Router(config)# router eigrp saf`	グローバル コンフィギュレーション モードで EIGRP 仮想インスタンスを有効にします。

	コマンドまたはアクション	目的
ステップ 4	**service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number* 例： `Router(config-router)# service-family ipv4 autonomous-system 4453`	ルータ上で指定された自律システム用の Cisco SAF サービス ファミリを有効にします。
ステップ 5	**neighbor**{*ip-address* {*interface-typeinterface-number}*|**description***word*|**maximum-service**} | **maximum-service***number[threshold-value]* [**dampened** | **reset-time** | **restart***interval* | **restart-count** | **warning-only**]} 例： `Router(config-router-sf)# neighbor 10.10.10.1 Ethernet 0/0`	ルータ上で指定されたインターフェイスの Cisco SAF ネイバー関係を有効にします。
ステップ 6	**exit-service-family** 例： `Router(config-router-sf)# exit-service-family`	サービス ファミリ コンフィギュレーション モードを終了します。

Cisco SAF のスタブ ルーティングの設定

Cisco SAF Forwarder をスタブ ルータとして設定できます。Cisco EIGRP スタブ ルーティングの詳細については、『*Cisco IOS IP Routing: EIGRP Configuration Guide*』の「Configuring EIGRP」モジュールを参照してください。

Cisco SAF スタブ ルータを作成するには、次のコマンドを使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routereigrp***virtual-instance-name*
4. **service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***number*
5. **eigrpstub** [**receive-only**|**connected**]
6. **exit-service-family**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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。
ステップ 3	**routereigrp***virtual-instance-name* 例： `Router(config)# router eigrp saf`	グローバル コンフィギュレーション モードで EIGRP 仮想インスタンスを有効にします。
ステップ 4	**service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***number* 例： `Router(config-router)# service-family ipv4 autonomous-system 4453`	ルータ上で指定された自律システム用の Cisco SAF サービス ファミリを有効にします。
ステップ 5	**eigrpstub** [**receive-only**|**connected**] 例： `Router(config-router-sf)# eigrp stub connected`	Cisco SAF のスタブ ルータを設定します。
ステップ 6	**exit-service-family** 例： `Router(config-router-sf)# exit-service-family`	サービス ファミリ コンフィギュレーション モードを終了します。

Cisco SAF のルート認証の設定

Cisco SAF ルート認証では、ルーティング プロトコルからのルーティング更新のメッセージ ダイジェスト 5（MD5）認証が提供されます。各パケット内の MD5 キー付きダイジェストによって、

未承認ソースからの不正なまたは偽のルーティング メッセージの導入が阻止されます。Cisco SAF のルート認証を設定するには、次のコマンドを使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routereigrp***virtual-instance-name*
4. **service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number*
5. **sf-interface***interface-nameinterface-number*
6. **authenticationkey-chain***name-of-chain*
7. **authenticationmode** {**hmac-sha-256** {**0** | **7**}*password*| **md5**}
8. **exit-sf-interface**
9. **exit-service-family**
10. **exit**
11. **key-chain***name-of-chain*
12. **key***key-id*
13. **key-string***text*
14. **accept-lifetime***start-time* [**local** {**duration***seconds* | **end-time** | **infinite**}]
15. **send-lifetime***start-time* [**local** {**duration***seconds* | **end-time** | **infinite**}]
16. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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。
ステップ 3	**routereigrp***virtual-instance-name* 例： `Router(config)# router eigrp saf`	グローバル コンフィギュレーション モードで EIGRP 仮想インスタンスを有効にします。

	コマンドまたはアクション	目的
ステップ 4	**service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number* 例： `Router(config-router)# service-family ipv4 autonomous-system 4453`	ルータ上で指定された自律システム用の Cisco SAF サービス ファミリを有効にします。
ステップ 5	**sf-interface***interface-nameinterface-number* 例： `Router(config-router-sf)# sf-interface ethernet 0/0`	ルータ上で指定されたインターフェイスの IPv4 サービス ファミリ インターフェイス コンフィギュレーション モードを有効にします。
ステップ 6	**authenticationkey-chain***name-of-chain* 例： `Router(config-router-sf-interface)# authentication key-chain example`	EIGRP の認証キー チェーンを指定します。
ステップ 7	**authenticationmode** {**hmac-sha-256** {**0** | **7**}*password*| **md5**} 例： `Router(config-router-sf-interface)# authentication mode md5`	ルータ上で指定されたインターフェイスの IPv4 サービス ファミリ認証モード HMAC-SHA-256 または MD5 を有効にします。
ステップ 8	**exit-sf-interface** 例： `Router(config-router-sf-interface)# exit-sf-interface`	サービス ファミリ インターフェイス コンフィギュレーション モードを終了します。
ステップ 9	**exit-service-family** 例： `Router(config-router-sf)# exit-service-family`	サービス ファミリ コンフィギュレーション モードを終了します。
ステップ 10	**exit** 例： `Router(config-router)# exit`	ルータ コンフィギュレーション モードを終了します。
ステップ 11	**key-chain***name-of-chain* 例： `Router(config)# key-chain example`	ルーティング プロトコルの認証を有効にするために必要な認証キーチェーンを定義して、キーチェーン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 12	**key***key-id* 例： `Router(config-keychain)# key example`	キーの認証文字列を特定します。
ステップ 13	**key-string***text* 例： `Router(config-keychain-key)# key-string example`	キーの認証文字列を指定します。
ステップ 14	**accept-lifetime***start-time* [**local** {**duration***seconds* | **end-time** | **infinite**}] 例： `Router(config-router-sf-interface)# accept-lifetime example`	キーチェーン内の認証キーが有効として受信される期間を設定します。
ステップ 15	**send-lifetime***start-time* [**local** {**duration***seconds* | **end-time** | **infinite**}] 例： `Router(config-router-sf-interface)# send-lifetime example`	キーチェーン上の認証キーが送信可能な期間を設定します。
ステップ 16	**exit** 例： `Router(config-router-sf-interface)# exit`	サービス ファミリ インターフェイス コンフィギュレーション モードを終了します。

ネイバー変更と警告のログの設定

デフォルトで、ルーティング システムの安定性を監視して問題を特定できるように、ネイバー隣接関係の変更がシステム ログに記録されます。無効にしたこのような変更のロギングを再度有効にする場合は、次のコマンドを使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routereigrp***virtual-instance-name*
4. **service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number*
5. **eigrplog-neighbor-changes**
6. **eigrplog-neighbor-warnings***seconds*
7. **exit-service-family**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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。
ステップ 3	**routereigrp***virtual-instance-name* 例： `Router(config)# router eigrp saf`	グローバル コンフィギュレーション モードで EIGRP 仮想インスタンスを有効にします。
ステップ 4	**service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number* 例： `Router(config-router)# service-family ipv4 autonomous-system 4453`	ルータ上で指定された自律システム用の Cisco SAF サービス ファミリを有効にします。
ステップ 5	**eigrplog-neighbor-changes** 例： `Router(config-router-sf)# eigrp log-neighbor-changes`	EIGRP サービス ファミリ ネイバー隣接関係の変更のロギングを有効にします。

	コマンドまたはアクション	目的
ステップ 6	**eigrplog-neighbor-warnings***seconds* 例： `Router(config-router-sf)# eigrp log-neighbor-warnings 60`	サービス ファミリ警告メッセージの変更のロギングを有効にします。
ステップ 7	**exit-service-family** 例： `Router(config-router)# exit-service-family`	サービス ファミリ コンフィギュレーション モードを終了します。

Cisco SAF に使用されるリンク帯域幅の割合の設定

デフォルトで、**bandwidthinterface** コンフィギュレーション コマンドで設定されたように、リンク帯域幅の最大 50% がパケットに消費されます。別のレベルのリンク使用が必要な場合、または、設定された帯域幅が実際のリンク帯域幅に適合しない（ルート メトリックの計算に影響を与えるように設定されている）場合は、この値を変更できます。次のコマンドを使用して、Cisco SAF に使用されるリンク帯域幅の割合を設定します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routereigrp***virtual-instance-name*
4. **service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number*
5. **sf-interface***interface-nameinterface-number*
6. **bandwidth-percent***maximum-bandwidth-percentage*
7. **exit-sf-interface**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# 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。
ステップ 3	**routereigrp***virtual-instance-name* 例： `Router(config)# router eigrp saf`	グローバルコンフィギュレーションモードで EIGRP 仮想インスタンスを有効にします。
ステップ 4	**service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number* 例： `Router(config-router)# service-family ipv4 autonomous-system 4453`	ルータ上で指定された自律システム用の Cisco SAF サービス ファミリを有効にします。
ステップ 5	**sf-interface***interface-nameinterface-number* 例： `Router(config-router-sf)# sf-interface ethernet0/0`	ルータ上で指定されたインターフェイスのサービス ファミリ インターフェイス コンフィギュレーションモードを有効にします。
ステップ 6	**bandwidth-percent***maximum-bandwidth-percentage* 例： `Router(config-router-sf-interface)# bandwidth-percent 75`	Cisco SAF のリンクに使用される帯域幅の最大割合を設定します。
ステップ 7	**exit-sf-interface** 例： `Router(config-router-sf-interface)# exit-sf-interface`	サービス ファミリ インターフェイス コンフィギュレーションモードを終了します。

Cisco SAF インターフェイスのメトリック ダンプニング インターバルの設定

メトリック コンポーネントは頻繁に変更される可能性があるため、その変更頻度がネットワークに影響を与える可能性があります。頻繁に変更するためには、SAF インターフェイス経由で取得したプレフィックスを更新して、すべての隣接ルータに送信する必要があります。この更新がさらなる更新を産み、最悪の場合、ネットワーク規模のチャーンを引き起こす可能性があります。

このような影響を回避するために、ダンプニングしきい値を下回っている変更は無視できるように、メトリックを下げるか、しきい値を設定することができます。

即時更新を引き起こすネットワーク変更には、新しい nexthop またはダウン インターフェイスかダウン ルータがルータ上で選択されるメトリックの変更が含まれます。

メトリック変更のダンプニングは変更またはタイム インターバルに基づいて設定できます。

ダンプニング方法によって次のように動作が異なります。

- 変更ベースの場合は、特定のインターフェイス経由で取得されたルートの変更または特定のインターフェイス メトリックの変更が、最後にアドバタイズされた値から計算されたメトリックの変更が非常に重要で更新を送信しなけらばならなくなるまで、隣接ルータにアドバタイズされません。
- インターバルベースの場合は、特定のインターフェイス経由で取得されたルートの変更または特定のインターフェイス メトリックの変更が、指定されたインターバルが経過するまで、または、その変更によって新しいルート パスが選択されなければ、隣接ルータにアドバタイズされません。タイマーが切れると、レポートに対する変更が未処理のルートが送信されます。ルートが変更され、そのルートの最終メトリックが最後に更新されたメトリックと一致する場合は、更新されたルータが送信されません。

変更ベースとインターバル ベースのメトリック ダンプニング パラメータの詳細については、次のセクションを参照してください。

変更ベースのダンプニング設定

次のコマンドを使用して、Cisco SAF インターフェイスの変更ベースの最大ダンプニング割合を設定します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routereigrp***virtual-instance-name*
4. **service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number*
5. **sf-interface***interface-nameinterface-number*
6. **dampening-change** [*change-percentage*]
7. **exit-sf-interface**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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。
ステップ 3	**routereigrp***virtual-instance-name* 例： `Router(config)# router eigrp saf`	グローバル コンフィギュレーション モードで EIGRP 仮想インスタンスを有効にします。
ステップ 4	**service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number* 例： `Router(config-router)# service-family ipv4 autonomous-system 4453`	ルータ上で指定された自律システム用の Cisco SAF サービス ファミリを有効にします。
ステップ 5	**sf-interface***interface-nameinterface-number* 例： `Router(config-router-sf)# sf-interface ethernet0/0`	ルータ上で指定されたインターフェイスのサービス ファミリ インターフェイス コンフィギュレーション モードを有効にします。
ステップ 6	**dampening-change** [*change-percentage*] 例： `Router(config-router-sf-interface)# dampening-change 50`	隣接ピアに更新がアドバタイズされる、EIGRP サービス ファミリ インターフェイス経由で取得されたルート変更の割合を設定します。
ステップ 7	**exit-sf-interface** 例： `Router(config-router-sf-interface)# exit-sf-interface`	サービス ファミリ インターフェイス コンフィギュレーション モードを終了します。

インターバル ベースのダンプニング設定

次のコマンドを使用して、Cisco SAF インターフェイスのインターバル ベースのダンプニングを設定します。設定した値によって、Cisco SAF インターフェイスとピアに影響を与えるトポロジ変更による更新が発生するインターバルが設定されます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routereigrp***virtual-instance-name*
4. **service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number*
5. **sf-interface***interface-nameinterface-number*
6. **dampening-interval***[interval]*
7. **exit-sf-interface**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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。
ステップ 3	**routereigrp***virtual-instance-name* 例： `Router(config)# router eigrp saf`	グローバル コンフィギュレーション モードで EIGRP 仮想インスタンスを有効にします。
ステップ 4	**service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number* 例： `Router(config-router)# service-family ipv4 autonomous-system 4453`	ルータ上で指定された自律システム用の Cisco SAF サービス ファミリを有効にします。

	コマンドまたはアクション	目的
ステップ 5	**sf-interface***interface-nameinterface-number* 例： `Router(config-router-sf)# sf-interface ethernet0/0`	ルータ上で指定されたインターフェイスのサービス ファミリ インターフェイス コンフィギュレーションモードを有効にします。
ステップ 6	**dampening-interval***[interval]* 例： `Router(config-router-sf-interface)# dampening-interval 30`	EIGRP インターバル ベースのダンプニング インターバルを設定します。
ステップ 7	**exit-sf-interface** 例： `Router(config-router-sf-interface)# exit-sf-interface`	サービス ファミリ インターフェイス コンフィギュレーションモードを終了します。

hello パケット間のインターバルとホールド タイムの調整

ルーティングデバイスは、定期的にhelloパケットを相互に送信して、直接接続されたネットワーク上の他のルータをダイナミックに学習します。この情報は、ネイバーを検出したり、ネイバーが到達不能または動作不能になったことを学習したりするために使用されます。

デフォルトでは、helloパケットは5秒間隔で送信されます。例外は、デフォルトのhelloインターバルが 60 秒の低速非ブロードキャスト マルチアクセス（NBMA）メディアの場合です。低速とは、**bandwidthinterface** コンフィギュレーション コマンドで指定されているように、T1 以下のレートを指します。高速 NBMA ネットワークのデフォルトの hello インターバルは 5 秒です。フレーム リレーやスイッチドマルチメガビットデータ サービス（SMDS）に使用されるネットワークは、NBMA と見なされる場合と見なされない場合があることに注意してください。このようなネットワークは、インターフェイスが物理マルチキャストを使用するように設定されていない場合は NBMA と見なされ、それ以外の場合は NBMA と見なされません。

保留時間は、hello パケットでアドバタイズされ、送信元を有効と見なす時間の長さをネイバーに示します。デフォルトの保留時間は、hello 間隔の 3 倍（15 秒）です。低速 NBMA ネットワークのデフォルトのホールド タイムは 180 秒です。混雑したネットワークや大規模なネットワーク上では、デフォルトのホールド タイムでは、すべてのルータがネイバーから hello パケットを受信するのに不十分な場合があります。この場合、ホールド タイムを増やすこともできます。ホールド タイムを調整する場合は、テクニカルサポート担当者に相談してください。自律システム番号で指定された特別なルーティングプロセス用のインターフェイスに関するホールドタイムを変更するには、**holdtime** コマンドを使用します。

hello パケットの間隔と保留時間は調整することができます。hello パケット間のインターバルとホールド タイムを変更するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routereigrp***virtual-instance-name*
4. **service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number*
5. **sf-interface***interface-nameinterface-number*
6. **hello-interval***seconds*
7. **hold-time***seconds*
8. **exit-sf-interface**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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。
ステップ 3	**routereigrp***virtual-instance-name* 例： `Router(config)# router eigrp saf`	グローバル コンフィギュレーション モードで EIGRP 仮想インスタンスを有効にします。
ステップ 4	**service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number* 例： `Router(config-router)# service-family ipv4 autonomous-system 4453`	ルータ上で指定された自律システム用の Cisco SAF サービス ファミリを有効にします。

	コマンドまたはアクション	目的
ステップ 5	**sf-interface***interface-nameinterface-number* 例： `Router(config-router-sf)# sf-interface ethernet0/0`	ルータ上で指定されたインターフェイスのサービス ファミリ インターフェイス コンフィギュレーション モードを有効にします。
ステップ 6	**hello-interval***seconds* 例： `Router(config-router-sf-interface)# hello-interval 50`	EIGRP サービス ファミリ プロセスの期間を設定します。
ステップ 7	**hold-time***seconds* 例： `Router(config-router-sf-interface)# hello-interval 50`	自律システム番号で指定された EIGRP サービス ファミリ ルーティング プロセスの期間を設定します。
ステップ 8	**exit-sf-interface** 例： `Router(config-router-sf-interface)# exit-sf-interface`	サービス ファミリ インターフェイス コンフィギュレーション モードを終了します。

スプリット ホライズンの無効化

インターフェイス上でスプリット ホライズンが有効になっている場合は、ルート情報（更新パケットや照会パケットなど）の発信元であるインターフェイス以外のルータによるその情報のアドバタイズがブロックされます。この方法でアップデートパケットとクエリーパケットを制御すると、ルーティング ループが発生する可能性が低くなります。

通常、特にリンクが切断された場合には、この動作によって複数のルーティング デバイス間の通信が最適化されます。ただし、非ブロードキャスト ネットワーク（フレーム リレーや SMDS など）を使用している場合は、この動作では不十分な状況が発生する可能性があります。その場合は、Cisco SAF を設定したネットワークを含めて、スプリット ホライズンを無効にすることができます。

デフォルトでは、スプリット ホライズンはすべてのインターフェイスでイネーブルになっています。スプリット ホライズンを無効にするには、インターフェイス コンフィギュレーション モードで、**nosplit-horizon** コマンドを使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routereigrp***virtual-instance-name*
4. **service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number*
5. **sf-interface***interface-nameinterface-number*
6. **nosplit-horizon**
7. **exit-sf-interface**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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。
ステップ 3	**routereigrp***virtual-instance-name* 例： `Router(config)# router eigrp saf`	グローバル コンフィギュレーション モードで EIGRP 仮想インスタンスを有効にします。
ステップ 4	**service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number* 例： `Router(config-router)# service-family ipv4 autonomous-system 4453`	ルータ上で指定された自律システム用の Cisco SAF サービス ファミリを有効にします。
ステップ 5	**sf-interface***interface-nameinterface-number* 例： `Router(config-router-sf)# sf-interface ethernet0/0`	ルータ上で指定されたインターフェイスのサービス ファミリ インターフェイス コンフィギュレーション モードを有効にします。

	コマンドまたはアクション	目的
ステップ 6	**nosplit-horizon** 例： `Router(config-router-sf-interface)# no split-horizon`	スプリットホライズンを無効にします。
ステップ 7	**exit-sf-interface** 例： `Router(config-router-sf-interface)# exit-sf-interface`	サービス ファミリ インターフェイス コンフィギュレーション モードを終了します。

メトリック最大ホップ カウントの設定

最大ホップカウントによって、サービスをアドバタイズする目的で伝搬可能なホップカウントが制限されます。デフォルトの最大ホップ カウントは 100 です。

サービスのアドバタイズに使用されるホップ カウントを制限するには、次のコマンドを使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routereigrp***virtual-instance-name*
4. **service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number*
5. **sf-interface***interface-nameinterface-number*
6. **metricmaximum-hops**
7. **exit-sf-interface**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# 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。
ステップ 3	**routereigrp***virtual-instance-name* 例： `Router(config)# router eigrp saf`	グローバル コンフィギュレーション モードで EIGRP 仮想インスタンスを有効にします。
ステップ 4	**service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number* 例： `Router(config-router)# service-family ipv4 autonomous-system 4453`	ルータ上で指定された自律システム用の Cisco SAF サービス ファミリを有効にします。
ステップ 5	**sf-interface***interface-nameinterface-number* 例： `Router(config-router-sf)# sf-interface ethernet 0/0`	ルータ上で指定されたインターフェイスのサービス ファミリ インターフェイス コンフィギュレーション モードを有効にします。
ステップ 6	**metricmaximum-hops** 例： `Router(config-router-sf-interface)# metric maximum-hops 5`	IP ルーティング ソフトウェアを到達不能ルートとしてアドバタイズするためのホップ カウントを指定します。
ステップ 7	**exit-sf-interface** 例： `Router(config-router-sf-interface)# exit-sf-interface`	サービス ファミリ インターフェイス コンフィギュレーション モードを終了します。

Cisco SAF External Client の設定方法

ここでは、Cisco SAF External Client を設定するタスクについて説明します。

Cisco SAF Client は、次のいずれかの方法で Cisco SAF ネットワークに接続します。

- 内部 API を使用して Cisco SAF Forwarder に接続する場合は、Cisco SAF Forwarder と同じルータ上に存在します。詳細については、「機能マネージャの設定」の項を参照してください。

- Cisco SAF Forwarder の外部に存在します。この設定では、SAF Client は Cisco SAF External Client と呼ばれ、Cisco SAF Forwarder に接続するためのプロトコル インターフェイスが必要になります。

前提条件

事前に必要な作業：

- Cisco SAF Client では、「Cisco SAF Client の概要」に記載された概念を理解しておく必要があります。
- 別々の LAN 上に配置された Cisco SAF External Client のネイバー関係を設定する前に、各 Cisco External Client 間の IP ルーティングが設定されていることを確認してください。

Cisco SAF External Client の設定

Cisco SAF External Client を設定するには、次のコマンドを使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routereigrp***virtual-instance-name*
4. **service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number*
5. **topologybase**
6. **external-client***client-label*
7. **exit-sf-topology**
8. **exit-service-family**
9. **exit**
10. **service-familyexternal-clientlisten**{**ipv4** | **ipv6**} tcp_port_number
11. **external-client***client-label***basename**
12. **username***user-name*
13. **password***password-name*
14. **keepalive***number*
15. **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	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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。
ステップ 3	**routereigrp***virtual-instance-name* 例： `Router(config)# router eigrp saf`	グローバル コンフィギュレーション モードで EIGRP 仮想インスタンスを有効にします。
ステップ 4	**service-family**{**ipv4** | **ipv6**}[**vrf***vrf-name*]**autonomous-system***autonomous-system-number* 例： `Router(config-router)# service-family ipv4 autonomous-system 4453`	ルータ上で指定された自律システム用の Cisco SAF サービス ファミリを有効にします。
ステップ 5	**topologybase** 例： `Router(config-router-sf)# topology base`	ルータ上で指定されたインターフェイスのサービス ファミリ インターフェイス トポロジ コンフィギュレーション モードを有効にします。
ステップ 6	**external-client***client-label* 例： `Router(config-router-topology)# external-client example`	指定されたクライアント ラベルで Cisco SAF External Client を設定します。
ステップ 7	**exit-sf-topology** 例： `Router(config-router-sf-topology)# exit-sf-topology`	サービス ファミリ トポロジ コンフィギュレーション モードを終了します。
ステップ 8	**exit-service-family** 例： `Router(config-router-sf)# exit-service-family`	サービス ファミリ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Router(config-router)# exit`	ルータ コンフィギュレーション モードを終了します。
ステップ 10	**service-familyexternal-clientlisten**{**ipv4** | **ipv6**} tcp_port_number 例： `Router(config)# service-family external-client listen ipv4 5050`	Cisco SAF Forwarder との通信に使用される Cisco SAF External Client の TCP ポートを設定します。ポートの有効範囲は 1024 ～ 65536 です。
ステップ 11	**external-client***client-label***basename** 例： `Router(config-external-client)# external-client example basename`	指定したクライアントラベルと任意でベース名を使用して Cisco SAF External Client を設定します。 **basename** キーワードを指定すると、SAF External Client がクライアント ラベルに基づいて命名規則を使用できるようになります。命名規則は、*client-label* @[1-1024] の形式で、最大で 1024 の SAF External Client を指定できます。たとえば、**external-client** コマンドが *example* というクライアントラベルを指定すると、SAF External Client のベース名は *example@1* になります。別の SAF External Client は *example@2* となり、最大 1024 まで同様のベース名となります（*@1024*）。
ステップ 12	**username***user-name* 例： `Router(config-external-client)# username example`	外部クライアント ラベル コンフィギュレーション モードを有効にして、指定されたユーザ名で Cisco SAF External Client を設定します。
ステップ 13	**password***password-name* 例： `Router(config-external-client-mode)# password examplepass`	Cisco SAF External Client のパスワードを設定します。最小パスワード長は 11 文字です。
ステップ 14	**keepalive***number* 例： `Router(config-external-client-mode)# keepalive 360000`	（任意）Cisco SAF External Client のキープアライブ タイマーを指定します。キープアライブ値はミリ秒単位です。デフォルトは 9600 ミリ秒です。

	コマンドまたはアクション	目的
ステップ 15	**exit** 例： `Router(config-external-client-mode)# exit`	外部クライアント ラベル コンフィギュレーション モードを終了します。

Cisco SAF の統計情報の表示方法

Cisco SAF の統計情報を表示するには、特権 EXEC モードで次のコマンドを使用します。

手順の概要

1. **show service-routing xmcp clients** [*ip_address* | *handle*] [**detail**]
2. **show service-routing xmcp server**
3. **showeigrpservice-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **accounting**
4. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **clients** [**detail**]
5. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **events** [*starting-event-number ending-event-number*]
6. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **interfaces** [*interface-type interface-number*] [**detail**]
7. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **subscriptions**
8. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **timers**
9. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **summary**
10. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **zero successors**
11. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology**
12. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology active**
13. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology all-links**
14. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology base** *service-instance-number* | **clients** [**detail**]
15. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology** [**detail-links**]
16. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology events**[*starting-event-number ending-event-number*]
17. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology pending**
18. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology** [**service-typeconnected** | **external** | **internal** | **local** | **redistributed** | **summary**]
19. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology sia-events** *starting-event-number ending-event-number*
20. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology sia-statistics** [*ip-address*]
21. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology summary**
22. **show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology zero-successors**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show service-routing xmcp clients** [*ip_address*	*handle*] [**detail**] 例： `Router> show service-routing clients detail`	接続された XMCP クライアントに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 2	**show service-routing xmcp server** 例： `Router> show service-routing xmcp server`	Cisco SAF 用に設定されたクライアント、外部クライアント、またはサブスクリプションに関する情報を表示します。
ステップ 3	**showeigrpservice-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **accounting** 例： `Router# show eigrp service-family ipv4 4453 accounting`	Cisco SAF に関するアカウンティング情報を表示します。
ステップ 4	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **clients** [**detail**] 例： `Router# show eigrp service-family ipv4 4453 clients`	Cisco SAF Client に関する情報を表示します。
ステップ 5	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **events** [*starting-event-number ending-event-number*] 例： `Router# show eigrp service-family ipv4 4453 events`	Cisco SAF イベントに関する情報を表示します。
ステップ 6	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **interfaces** [*interface-type interface-number*] [**detail**] 例： `Router# show eigrp service-family ipv4 4453 interfaces`	Cisco SAF インターフェイスに関する情報を表示します。
ステップ 7	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **subscriptions** 例： `Router# show eigrp service-family ipv4 4453 subscriptions`	Cisco SAF サブスクリプションに関する情報を表示します。
ステップ 8	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **timers** 例： `Router# show eigrp service-family ipv4 4453 timers`	Cisco SAF タイマーに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 9	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **summary** 例： `Router# show eigrp service-family ipv4 4453 summary`	Cisco SAF に関するサマリー情報を表示します。
ステップ 10	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **zero successors** 例： `Router# show eigrp service-family ipv4 4453 zero successors`	Cisco SAF ゼロ サクセサに関する情報を表示します。
ステップ 11	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology** 例： `Router# show eigrp service-family ipv4 4453 topology`	Cisco SAF トポロジ テーブルに関する情報を表示します。
ステップ 12	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology active** 例： `Router# show eigrp service-family ipv4 4453 topology active`	Cisco SAF トポロジ テーブルのアクティブ エントリのみを表示します。
ステップ 13	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology all-links** 例： `Router# show eigrp service-family ipv4 4453 topology all-links`	Cisco SAF トポロジ テーブルのすべてのアクティブ リンク エントリを表示します。
ステップ 14	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology base** *service-instance-number* | **clients** [**detail**] 例： `Router# show eigrp service-family ipv4 4453 topology base clients`	Cisco SAF トポロジ ベースのすべてのアクティブ リンクエントリを表示します。
ステップ 15	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology** [**detail-links**]	Cisco SAF に関する情報を表示します。

	コマンドまたはアクション	目的
	例： `Router# show eigrp service-family ipv4 4453 topology detail-links`	
ステップ 16	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology events**[*starting-event-number ending-event-number*] 例： `Router# show eigrp service-family ipv4 4453 topology`	Cisco SAF に関する情報を表示します。
ステップ 17	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology pending** 例： `Router# show eigrp service-family ipv4 4453 topology pending`	Cisco SAF に関する情報を表示します。
ステップ 18	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology** [**service-typeconnected** | **external** | **internal** | **local** | **redistributed** | **summary**] 例： `Router# show eigrp service-family ipv4 4453 topology service-type connected`	Cisco SAF トポロジテーブルの指定されたサービスタイプに関する情報を表示します。
ステップ 19	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology sia-events** *starting-event-number ending-event-number* 例： `Router# show eigrp service-family ipv4 4453 topology sia-events`	Cisco SAF トポロジテーブル内の Stuck in Active（SIA）イベントを表示します。
ステップ 20	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology sia-statistics** [*ip-address*] 例： `Router# show eigrp service-family ipv4 4453 topology sia-statistics 10.10.10.1`	Cisco SAF トポロジテーブルに関する Stuck in Active（SIA）イベントを表示します。

	コマンドまたはアクション	目的
ステップ 21	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology summary** 例： `Router# show eigrp service-family ipv4 4453 topology summary`	Cisco SAF トポロジ テーブルのサマリーを表示します。
ステップ 22	**show eigrp service-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] *autonomous-system-number* **topology zero-successors** 例： `Router# show eigrp service-family ipv4 4453 topology zero-successors`	Cisco SAF トポロジ テーブル内にゼロ サクセサが存在する利用可能なサービスに関する情報を表示します。

Cisco SAF 設定から情報を削除する方法

Cisco SAF 設定からサービス ファミリ情報を削除するには、EXEC モードで次のコマンドを使用します。

手順の概要

1. **clear service-family xmcp client** {*address* | *handle*}
2. **clear eigrp service-family** {**ipv4** | **ipv6**} **ipv6** [**vrf** *vrf-name*] *autonomous-system-number*
3. **clear eigrp service-family neighbors** *neighbor-address* | *interface-type interface-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear service-family xmcp client** {*address* | *handle*} 例： `Router> clear service-family xmcp client 1.1.1.1`	接続された XMCP クライアントを切断します。

	コマンドまたはアクション	目的
ステップ 2	**clear eigrp service-family** {**ipv4** | **ipv6**} **ipv6** [**vrf** *vrf-name*] *autonomous-system-number* 例： `Router# clear eigrp service-family ipv4 4453`	指定された自律システムの IPv4 または IPv6 プロトコル ファミリを使用して構成されたネイバーを削除します。オプションで、すべての Virtual Routing Forwarding（VRF）インスタンス テーブルまたは IP アドレスに関する特定の VRF テーブルを削除できます。 （注） **clear eigrp service-family ipv6** コマンドを使用する場合は、現在は存在しない IPv6 対応の SAF クライアントが必要です。
ステップ 3	**clear eigrp service-family neighbors** *neighbor-address* | *interface-type interface-number* 例： `Router> clear eigrp service-family neighbors Ethernet 0/0`	ネイバーテーブルから IPv4 プロトコル ファミリを使用して構成されたネイバーを削除します。オプションで、隣接関係をリセット（ソフト）せずにピアと再同期化できます。必要に応じて、このインターフェイスから学習したすべてのエントリを含むネイバー テーブルからインターフェイスのタイプと番号を削除できます。

Cisco SAF の設定例

例：Cisco SAF の有効化

次の例では、ルータ コンフィギュレーション モードを開始して、Cisco SAF Forwarder を設定し、サービス ファミリ フォワーダ プロセスを有効にして、4533 という名前の自律システムを設定します。

```
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 4533
```

例：Cisco SAF インターフェイスの設定

次の例では、ルータをサービス ファミリ コンフィギュレーション モードにして、すべてのインターフェイスを有効にします。

```
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# sf-interface default
Router(config-router-sf-interface)# no shutdown
```

次の例では、ルータをサービス ファミリ コンフィギュレーション モードにして、イーサネット インターフェイス 0/0 を有効にします。

```
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# sf-interface ethernet0/0
```

次の例では、ルータをサービス ファミリ コンフィギュレーション モードにして、イーサネット 0/0 インターフェイスを除くすべてのインターフェイス上の SAF を有効にします。

```
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 3
Router(config-router-sf)# interface default
Router(config-router-sf)# sf-interface ethernet0/0
Router(config-router-sf-interface)# shutdown
Router(config-router-sf-interface)# end
```

次の例では、ルータをサービス ファミリ コンフィギュレーション モードにして、イーサネット 2/0 インターフェイスとイーサネット 2/1 インターフェイス上の SAF を有効にし、他のすべてのインターフェイスを無効にします。

```
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 2
Router(config-router-sf)# sf-interface default
Router(config-router-sf-interface)# shutdown
Router(config-router-sf-interface)# sf-interface ethernet2/0
Router(config-router-sf-interface)# no
 shutdown
Router(config-router-sf-interface)# sf-interface ethernet2/1
Router(config-router-sf-interface)# no
 shutdown
Router(config-router-sf-interface)# end
```

例：Cisco SAF トポロジの設定

次の例では、Cisco SAF トポロジ ベースを設定します。

```
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# sf-interface default
Router(config-router-sf-interface)# no shutdown
Router(config-router-sf-interface)# topology
 base
```

例：Cisco SAF スタブ ルーティングの設定

次の例では、Cisco SAF Forwarder をスタブ ルータとして設定します。

```
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# eigrp stub connected
```

例：IP-RIP を使用する Cisco SAF の設定

次の例では、ネットワーク 10.0.0.0 上で IP-RIP ルーティングを使用して Cisco SAF を有効にします。

```
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# topology base
Router(config-router-sf-topology)# exit-sf-topology
Router(config-router-sf)# exit service-family
Router(config-router)# router rip
Router(config-router)# network 10.0.0.0
```

例：OSPF を使用する Cisco SAF の設定

次の例では、ネットワーク 10.0.0.0、領域 0 上で OSPF ルーティングを使用して Cisco SAF を有効にします。

```
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# topology base
Router(config-router-sf-topology)# exit-sf-topology
Router(config-router-sf)# exit service-family
Router(config-router)# router ospf 787
Router(config-router)# network 10.0.0.0  0.0.0.255 area 0
```

例：EIGRP を使用する Cisco SAF の設定

次の例では、ネットワーク 10.0.0.0 上で EIGRP ルーティングを使用して Cisco SAF を有効にします。

```
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 6476
Router(config-router-sf)# network 10.0.0.0  0.0.0.255
Router(config-router-sf)# topology base
Router(config-router-sf-topology)# exit-af-topology
Router(config-router-sf)# exit-service-family
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# topology base
```

（注） サービスが配信されるインターフェイスまたはネットワーク上でルーティングを実行する場合の要件は特にありませんが、到達可能性が保証されない領域にサービスが配信される可能性があります。

例：別々の LAN 上に配置された Cisco SAF Forwarder の設定

次の例では、別々の LAN 上に配置された 2 台の Cisco SAF Forwarder を設定します。

（注） ループバック モードを使用して、リモート ネイバーを設定します。

Cisco SAF Forwarder 1：

```
Router(config)# interface loopback1
Router(config-if)# ip address 10.1.1.1 255.255.255.255
Router(config-if)# exit
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 1
Router(config-router-sf)# neighbor 10.2.2.2 loopback1 remote 10
```

Cisco SAF Forwarder 2：

```
Router(config)# interface loopback1
Router(config-if)# ip address 10.2.2.2 255.255.255.255
Router(config-if)# exit
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 1
Router(config-router-sf)# neighbor 10.1.1.1 loopback1 remote 10
```

（注） 次の例では、2台のルータ間にIPルーティングが設定されており、ルータが両方のループバックを ping できるものとします。

集中型 Cisco SAF Forwarder の設定例

次の例では、すべてのサービス アドバタイズメントを IP アドレスが 10.4.15.5 と 10.4.15.1 のネイバーに送信する集中型 Cisco SAF Forwarder を設定します。

```
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# sf-interface loopback0
Router(config-router-sf-interface)# no split-horizon
Router(config-router-sf-interface)# exit-sf-interface
Router(config-router-sf)# topology base
Router(config-router-sf-topology)# exit-sf-topology
Router(config-router-sf)# neighbor 10.4.15.5 Loopback0 remote 20
Router(config-router-sf)# neighbor 10.4.15.1 Loopback0 remote 20
Router(config-router-sf)# exit-service-family
```

例：Cisco SAF Client の設定

次の例では、名前が *example*、ユーザ名が *username_example*、パスワードが *password_example*、キープアライブ設定が 360000 秒の Cisco SAF External Client を設定します。

```
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# topology base
Router(config-router-sf-topology)# external-client example
Router(config-router-sf-topology)# exit-sf-topology
```

```
Router(config-router-sf)# exit-service-family
Router(config-router)# exit
Router(config)# service-family external-client listen ipv4 3444
Router(config-external-client)# external-client example
Router(config-external-client-mode)# username
 username_example
Router(config-external-client-mode)# password
 password_example
Router(config-external-client-mode)# keepalive
 360000
```

次の例では、名前が *example1* ～ *example5*、ユーザ名が *username_example1* ～ *username_example5*、パスワードが *password_example1* ～ *password_example5*、キープアライブ設定が 360000 秒の 5 台の Cisco SAF External Client を設定します。

```
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 4533
Router(config-router-sf)# topology base
Router(config-router-sf-topology)# external-client example1
Router(config-router-sf-topology)# external-client example2
Router(config-router-sf-topology)# external-client example3
Router(config-router-sf-topology)# external-client example4
Router(config-router-sf-topology)# external-client example5
Router(config-router-sf-topology)# exit-sf-topology
Router(config-router-sf)# exit-service-family
Router(config-router)# exit
Router(config)# service-family external-client listen ipv4 3444
Router(config-external-client)# external-client example1
Router(config-external-client-mode)# username
 username_example1
Router(config-external-client-mode)# password
 password_example1
Router(config-external-client-mode)# keepalive
 360000
Router(config-external-client-mode)# external-client example2
Router(config-external-client-mode)# username
 username_example2
Router(config-external-client-mode)# password
 password_example2
Router(config-external-client-mode)# keepalive
 360000
Router(config-external-client-mode)# external-client example3
Router(config-external-client-mode)# username
 username_example3
Router(config-external-client-mode)# password
 password_example3
Router(config-external-client-mode)# keepalive
 360000
Router(config-external-client-mode)# external-client example4
Router(config-external-client-mode)# username
 username_example4
Router(config-external-client-mode)# password
 password_example4
Router(config-external-client-mode)# keepalive
 360000
Router(config-external-client-mode)# external-client example5
Router(config-external-client-mode)# username
 username_example5
Router(config-external-client-mode)# password
 password_example5
Router(config-external-client-mode)# keepalive
 360000
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Service Advertisement Framework コマンド	『Cisco IOS Service Advertisement Framework Technology Command Reference』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco SAF の機能情報

表 *1*：*Cisco Service Advertisement Framework* に関する機能情報

機能名	ソフトウェア リリース	機能の設定情報
Cisco Service Advertisement Framework	15.0M、12.2(33)SRE、12.2(33)XNE、15.1T、12.2(33)SXI4、15.0(1)S、15.1(2)S、12.2(50)SY、15.2(1)T、15.2(3)T、15.2(2)S、15.1(1)SG Cisco IOS XE 2.5、Cisco IOS XE 3S、Cisco IOS XE 3.3SG	

機能名	ソフトウェア リリース	機能の設定情報
		この機能を使用すれば、アプリケーションで、ネットワークに接続されたリソースの存在、位置、および設定を検出して、ネットワーク上のアプリケーション アドバタイズおよび検出サービスとして、タイムリーで信頼できるネットワーク上のサービス認識を実現できます。 この機能は、Cisco IOS リリース 15.0M で導入されました。 Cisco IOS XE 2.5 で、この機能は、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 Cisco IOS XE 3.3 SG では、Cisco Catalyst 4000 シリーズ スイッチのサポートが追加されました。 次のコマンドがこの機能で導入されました。 • **authentication(service-family)** • **bandwidth-percent** • **clear eigrpservice-family** • **dampening-change** • **dampening-interval** • **defaultexternal-client** • **default(SAF)** • **debugeigrpservice-family** • **default-metric(EIGRP)** • **eigrpstub(service-family)** • **exit-service-family** • **exit-sf-interface** • **exit-sf-topology** • **external-client** • **keepalive(SAF)** • **maximum-service(EIGRP)**

機能名	ソフトウェア リリース	機能の設定情報
		• **neighbors(service-family)** • **password(SAF)** • **service-family** • **service-familyexternal-clientlisten** • **sf-interface** • **showeigrpservice-family** • **showeigrpservice-familyipv4topology** • **showeigrpservice-familyipv6topology** • **showeigrptech-support** • シャットダウン • トポロジ • **username(SAF)**
Cisco Service Advertisement Framework	15.0M、12.2(33)SRE、12.2(33)XNE、15.0(1)S、15.1(2)S、15.2(3)T、15.2(2)S Cisco IOS XE リリース 2.5、Cisco IOS XE リリース 3S、Cisco IOS XE リリース 3.4S、Cisco IOS XE リリース 3.6S	次のコマンドがこの機能で変更されました。 • **accept-lifetime** • **eigrplog-neighbor-changes** • **eigrp-log-neighbor-warnings** • **eigrprouter-id** • **hello-interval** • **hold-time** • キー • **keychain** • **key-string(authentication)** • **metricweights(EIGRP)** • **next-hop-self** • **send-lifetime** • **split-horizon** • **timers**

機能名	ソフトウェア リリース	機能の設定情報
動的ネイバー	15.1(2)S、15.2(3)T、15.2(2)S、XE 3.6S	次のコマンドが導入または変更されました。 • **authenticationmode** • **remote-neighborssource** • **showeigrpservice-familyexternal-client**
機能マネージャ	15.0(1)SY、15.2(3)T、15.2(2)S、XE 3.6S	次のコマンドが導入または変更されました。 • **clear service-routingcapabilities-manager** • **service-routingcapabilities-manager** • **show service-routingplugins capman** • **showservicerouingcapabilitismanagerinternal** • **showservice-routingcapabilitis-manager group**
XMCP（Extensible Messaging Client Protocol）	15.2(2)T、15.2(1)S、15.2(3)T、15.2(2)S、XE 3.6S	次のコマンドが導入または変更されました。 • **allow-list** • **clearservice-routingxmcp client** • **client (XMCP)** • **domain** • **keepalive (XMCP)** • **max-clients** • **nonce** • **service-routingxmcp clients** • **service-routingxmcp server**

第 3 章

Extensible Messaging Control Protocol の設定

クライアントがサービスのルーティング対応のネットワークに接続するには次の2つの方法があります。

- Cisco IOS ソフトウェアに実装されているクライアントでのみ使用可能な、サービス ルーティング用の Cisco IOS 内部 API による
- プラットフォームのネットワーク内のあらゆるところで動作しているクライアントで使用可能な、External Client プロトコルとも呼ばれる、Extensible Messaging Client Protocol（XMCP）による

Cisco SAF Client は、次のいずれかの方法で Cisco SAF ネットワークに接続します。

- 内部 API を使用して Cisco SAF Forwarder に接続する場合は、Cisco SAF Forwarder と同じルータ上に存在します。
- Cisco SAF Forwarder の外部に存在します。この設定では、SAF Client は Cisco SAF External Client と呼ばれ、Cisco SAF Forwarder に接続するためのプロトコル インターフェイスが必要になります。

- 機能情報の確認，54 ページ
- XMCP の前提条件，54 ページ
- XMCP に関する情報，54 ページ
- XMCP の設定方法，55 ページ
- XMCP の設定例，61 ページ
- その他の参考資料，61 ページ
- XMCP に関する機能情報，63 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

XMCP の前提条件

- XMCP を設定する前に、「Cisco SAF の概要」のセクション、特に「Cisco SAF Client の概要」と「外部 Cisco SAF Client（XMCP）の概要」の概念を理解する必要があります。
- このセクションでは、Cisco IOS ソフトウェアの XMCP サーバ機能の設定について説明します。XMCP クライアントとして特定のデバイスやソフトウェア（たとえば、Cisco Unified Communications Manager）を設定するには、そのデバイスまたはソフトウェアのマニュアルを参照してください。クライアントのドキュメントが client-label の設定を参照する可能性があることに注意してください。client-label は、ユーザ名と同じ ID が設定されている必要があります。
- XMCP クライアントを XMCP サーバとして設定された Cisco ルータに接続するよう設定する前に、クライアント デバイスと Cisco ルータ間の IP ルーティングを設定したことを確認します。
- XMCP サーバとして設定されているどのデバイスも、Cisco SAF Forwarder として設定する必要があります。（「Cisco SAF Forwarder の設定」を参照してください）。XMCP を設定する前後に Cisco SAF Forwarder を設定できます。

XMCP に関する情報

XMCP のセッションが正常に確立されると、XMCP クライアントは XMCP パブリッシュ、非パブリッシュ、登録、および登録解除要求を送信できます。サーバがこのような要求を受信し、正常に認証すると、同等の Cisco SAF クライアント要求に変換し、Cisco SAF Forwarder に送信します。同様に、フォワーダからの Cisco SAF Client 通知要求は XMCP 通知要求に変換され、XMCP クライアントに送信されます。

XMCP の設定方法

クライアントがサービスのルーティング対応のネットワークに接続するには次の 2 つの方法があります。

- Cisco IOS ソフトウェアに実装されたクライアントでのみ使用可能な、サービス ルーティング用の内部 Cisco IOS API による。
- プラットフォームのネットワーク内のあらゆるところで動作しているクライアントで使用可能な、External Client プロトコルとも呼ばれる、Extensible Messaging Client Protocol（XMCP）による。

基本的な XMCP サーバの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **service-routing xmcp listen**
4. **client username** *username* **password** *password*
5. **domain** *domain-number* {**default** | **only**}
6. **end**
7. **show service-routing xmcp server**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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 3	**service-routing xmcp listen** 例： `Router(config)# service-routing xmcp listen`	XMCP サーバをイネーブルにし、XMCP 設定モードを開始します。XMCP サーバは次のことを行います。 • デフォルト ポート（4788）でリッスンします • すべての VRF（Virtual Route Forwarding）インスタンスの接続を受け入れます
ステップ 4	**client username** *username* **password** *password* 例： `Router(config-xmcp)# client username exampleuser password examplepassword`	XMCP クライアントがこのサーバの認証に使用できるユーザ名とパスワードのペアを定義し、XMCP クライアント コンフィギュレーション モードを開始します。 • デフォルトでは、ユーザ名またはパスワードが定義されていません。XMCP サーバを機能させるには、少なくとも 1 つの **client** コマンドを設定する必要があります。 • パスワードの範囲は 11 ～ 62 文字です。
ステップ 5	**domain** *domain-number* {**default** | **only**} 例： `Router(config-xmcp-client)# domain 100 only`	（オプション）指定したユーザ名とパスワードの組み合わせを使用するすべてのクライアントが関連付けられているサービス ルーティング ドメインを定義します。 • このペアは SAF の自律システムに対応します。したがって、SAF Forwarder としてこのルータを設定した場合（「Cisco SAF Forwarder の設定」セクションを参照）、ここで使用したドメインの数と同じ SAF Forwarder の自律システム番号を使用する必要があります。 • このコマンドを設定しないと、クライアントはドメイン 7177 をデフォルトに設定します。
ステップ 6	**end** 例： `Router(config-xmcp-client)# end`	XMCP クライアント コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show service-routing xmcp server** 例： `Router# show service-routing xmcp server`	XMCP サーバの設定のサマリーと接続されたクライアントの数が表示されます。

高度な XMCP サーバの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **service-routing xmcp listen** [**ipv4** | **ipv6**] [**port***port-number*] [**vrf***vrf-name*]
4. **allow-list** [**ipv4** *acl-name* | **ipv6** *acl-name*]
5. **max-clients** {**unauthenticated** *number* [**total** *number*] | **total** *number* [**unauthenticated** *number*]
6. **client unauthenticated**
7. **client username***username* {**password***password* | *encryption-typeencrypted-password*}
8. **domain***domain-number* {**default** | **only**}
9. **nonce** {**lifetime***seconds* | **none**}
10. **keepalive***seconds*
11. **exit**
12. **show service-routing xmcp server**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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。
ステップ 3	**service-routing xmcp listen** [**ipv4**	**ipv6**] [**port***port-number*] [**vrf***vrf-name*] 例： `Router(config)# service-routing xmcp listen ipv4 vrf vrf1 port 2000`	XMCP サーバをイネーブルにし、XMCP 設定モードを開始します。 • クライアント接続を制限するのに IPv4 と IPv6 のどちらも指定しないと、両方が許可されます。 • クライアント接続を指定した VRF に制限するには **vrf** キーワードを使用します。このキーワードを使用しないと、クライアントはすべての VRF の各インターフェイスから接続できます。 • クライアントが接続するポート番号を変更するには **port** キーワードを使用します。このキーワードを使用しないと、ポート番号は 4788 にデフォルト設定されます。

	コマンドまたはアクション	目的
ステップ 4	**allow-list** [**ipv4** *acl-name* | **ipv6** *acl-name*] 例： `Router(config-xmcp)# allow-list ipv4 XMCPClientListIPv4`	（オプション）指定したアクセス リストと一致するクライアントのみに続を許可します。他のすべてのクライアントは拒否されます。許可リストを指定しないと、クライアントはどのアクセス リストによってもフィルタリングされません。

ステップ 5	**max-clients** {**unauthenticated** *number* [**total** *number*] | **total** *number* [**unauthenticated** *number*]
	
	例：
	
	`Router(config-xmcp)# max-clients total 100`
	`Router(config-xmcp)# max-clients unauthenticated 5`
	`Router(config-xmcp)# max-clients unauthenticated 10 total 100`
		（オプション）認証されていないクライアントの最大数とすべてのタイプのクライアントの最大数を制限します。
		• 接続されたクライアントの最大数に達すると、それ以上のクライアントは拒否されます。
		• クライアントの数を指定しないと、最大で 1024 のクライアントが、使用可能な帯域幅およびメモリに応じて接続できます。

ステップ 6	**client unauthenticated** 例： `Router(config-xmcp)# client unauthenticated`	認証クレデンシャルを使用しない接続をクライアントに許可します。 • このコマンドを実行すると、XMCP クライアント設定モードに入り、次のように接続するクライアントに適用される追加の属性を提供します。 • デフォルトでは、認証されていないクライアントは許可されず、ユーザ名またはパスワード クレデンシャルは有効であるとみなされません。 • クライアントが XMCP サーバにより受け入れられるには、少なくとも 1 つの **client** コマンドを設定する必要があります。
ステップ 7	**client username***username* {**password***password* | *encryption-typeencrypted-password*} 例： `Router(config-xmcp-client)# client username example-user password example-password`	XMCP（Extensible Messaging Client Protocol）のクライアント接続に対し受け入れられるユーザ名とパスワードを設定します。 • 特定の認証クレデンシャルを使用したクライアントの接続を許可するには、1 つ以上の **client** コマンドを設定します。 • デフォルトでは、認証されていないクライアントは許可されず、ユーザ名またはパスワード クレデンシャルは有効であるとみなされません。 • クライアントが XMCP サーバにより受け入れられるには、少なくとも 1 つの **client** コマンドを設定する必要があります。

	コマンドまたはアクション	目的
ステップ 8	**domain***domain-number* {**default** | **only**} 例： `Router(config-xmcp-client)# domain 100 default`	（オプション）特定の認証クレデンシャルを使用するクライアントがデフォルトで割り当てられているドメイン、およびクライアントに別のドメインへの割り当ての要求が許可されているかどうかを定義します。ドメインの番号は、SAF Forwarder の自律システム番号に対応します。デフォルトでは、クライアントはドメイン 7177 に割り当てられますが、別のドメインへの割り当てを要求できます。 • デフォルト ドメインを選択し、クライアントが別のドメインを要求できるようにするには、**default** キーワードを使用します。 • デフォルト ドメインを選択し、クライアントが別のドメインを要求できないようにするには、**only** キーワードを使用します。
ステップ 9	**nonce** {**lifetime***seconds* | **none**} 例： `Router(config-xmcp-client)# nonce lifetime 600`	（オプション）ナンスはサーバのパケット スプーフィングおよびリプレイ アタックに対する追加のセッション セキュリティを（この機能をサポートするクライアントに対し）提供します。この機能は、追加の帯域幅と CPU リソースを必要とします。そのため、セキュリティのニーズに合わせて、有効または無効にすることができます。デフォルトでは、ナンスはこの機能をサポートするクライアントに使用されます。ナンスは 800 秒ごとに有効期限が切れ、クライアントは新しいナンスへの移行が必要です。ナンスを無効にするには、**nonce none** コマンドを使用します。 • セキュリティを高めるためには（ただし、さらに広い帯域幅と高い CPU 使用率を伴います）、ナンスの有効期間を最低 5 秒に短縮して設定します。 • セキュリティを低くするには（狭いクライアントの帯域幅と低い CPU 使用率を伴います）、ナンスの有効期間をより長く（最大 3600 秒）設定します。 ナンスは認証されていないクライアントには使用されません。したがって、このコマンドは **client unauthenticated** コマンドとともに使用することはできません。
ステップ 10	**keepalive***seconds* 例： `Router(config-xmcp-client)# keepalive 100`	（オプション）特定の認証クレデンシャルを使用してクライアントのキープアライブ間隔を調整します。 • クライアントが指定した間隔でメッセージを送信しない場合、XMCP サーバはクライアントに障害が発生したとみなし、XMCP セッションを終了し、このクライアントに関連するサービスやサブスクリプションを終了します。 • デフォルトでは、クライアントのキープアライブ間隔は30秒間です。

	コマンドまたはアクション	目的
ステップ 11	**exit** 例： `Router(config-xmcp-client)# exit`	XMCP クライアント コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 12	**show service-routing xmcp server** 例： `Router> show service-routing xmcp server`	XMCP サーバの設定のサマリーと接続されたクライアントの数が表示されます。

XMCP クライアントおよびサーバ情報の表示

接続されている XMCP クライアントおよびサーバに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで次のコマンドを使用します。コマンドはどの順序で入力してもかまいません。

手順の概要

1. **show service-routing xmcp clients** [*ip-address* | *handle*] [**detail**]
2. **show service-routing xmcp server**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show service-routing xmcp clients** [*ip-address* | *handle*] [**detail**] 例： `Router> show service-routing xmcp clients detail`	XMCP クライアントに関する情報を表示します。
ステップ 2	**show service-routing xmcp server** 例： `Router> show service-routing xmcp server`	XMCP サーバのステータス情報を表示します。

XMCP の設定例

例：XMCP サーバと Cisco SAF Forwarder の設定

次の例で、グローバル コンフィギュレーション モードで開始し、IPV4 XMCP サーバと IPv4 Cisco SAF Forwarder の両方としてルータを設定する方法を示します。また、すべての XMCP クライアントを正しい SAF の自律システムにマッピングします。

```
Router(config)# service-routing xmcp listen ipv4
Router(config-xmcp)# client unauthenticated
Router(config-xmcp-client)# client unauthenticated
Router(config-xmcp-client)# domain 1228 only
Router(config-xmcp-client)# client username example password passwordexample
Router(config-xmcp-client)# domain 1228 only
Router(config-xmcp-client)# exit
Router(config-xmcp)# exit
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 1228
Router(config-router-sf)# end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Service Advertisement Framework コマンド	『Cisco IOS Service Advertisement Framework Technology Command Reference』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

XMCP に関する機能情報

表 *2*：*XMCP* に関する機能情報

機能名	リリース	機能情報
XMCP（Extensible Messaging Client Protocol）	15.2(2)T、15.2(1)S、15.2(3)T、15.2(2)S Cisco IOS XE リリース 3.6S、Cisco IOS XE リリース 3.3SG 15.2(1)E	XMCP クライアントは、XMCP パブリッシュ、アンパブリッシュ、登録、および登録解除要求をサーバに送信します。サーバがこのような要求を受信し、正常に認証すると、同等の Cisco SAF クライアント要求に変換し、Cisco SAF Forwarder に送信します。 Cisco IOS XE 3.3 SG では、Cisco Catalyst 4000 シリーズ スイッチのサポートが追加されました。 次のコマンドが導入または変更されました。 • **allow-list** • **clearservice-routingxmcp client** • **client (XMCP)** • **domain** • **keepalive (XMCP)** • **max-clients** • **nonce** • **service-routingxmcp clients** • **service-routingxmcp server**

第 4 章

動的ネイバーの設定

ネイバーが隣接していない場合、通常の Cisco SAF のピアリング機能を使用して、ネットワーク クラウド経由で SAF 情報を交換することはできません。ネイバーは通常、複数のホップ先であり、ダーク ネット（SAF を実行しないルータ）で区切られます。

SAF はこのタイプのネットワークをサポートするために、**neighbor** コマンドを提供します。これにより、リモート ネイバーが設定され、ユニキャスト パケット伝送によりセッションが確立されます。ただし、ネットワーク クラウド経由で SAF 情報を交換する必要があるフォワーダの数が増えると、ユニキャスト SAF ネイバーの定義は管理しにくくなることがあります。各ネイバーは手動で設定される必要があるので、運用コストが増加します。

これらのトポロジの展開、設定管理の容易化、運用コストの削減を促進するために、動的ネイバー機能は、リモート ユニキャストおよびマルチキャスト ネイバー（「リモート ネイバー」と呼ばれる）の動的な検出をサポートします。リモート ネイバーがサポートされているため、Cisco SAF を 1 つ以上のリモート ネイバーとピアリングさせることができます。この情報はルータを設定する時点では認識されている必要がないため、設定管理が軽減されます。

ここでは、次の内容について説明します。

- 機能情報の確認，66 ページ
- 動的ネイバーの前提条件，66 ページ
- 動的ネイバーの制約事項，66 ページ
- 動的ネイバーに関する情報，67 ページ
- 動的ネイバーの設定方法，70 ページ
- 動的ネイバーの設定例，72 ページ
- その他の参考資料，73 ページ
- 動的ネイバーの機能情報，74 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

動的ネイバーの前提条件

SAF 動的ネイバーを設定する前に、使用時の次のことを確認します。

- ユニキャスト リッスン モード：IP 接続（到達可能性）が、動的なピアリングに必要なルータ間に存在すること。
- マルチキャスト グループ モード：マルチキャストがネットワークで稼働していること。
- **allow-list**

  キーワード：EIGRP ネイバー接続が受け入れられる可能性のあるリモート IP アドレスを指定する設定済みアクセス コントロール リスト。

動的ネイバーの制約事項

- **remote-neighbors** コマンドは、送信インターフェイスとしてループバックが必要です。
- 名前付き ACL（アクセス コントロール リスト）のみが **allow-list** キーワードで許可されています。設定済みの番号付き ACL は許可されません。

サービス ファミリ内では、次の制限事項が適用されます。

- 1 つの **remote-neighbors unicast-listen** コマンドと 1 つの **remote-neighbors multicast-group** コマンドがインターフェイスごとに設定されることがあります。たとえば、**remote-neighbors source Loopback1 multicast-group 224.1.1.1** および **remote-neighbors source Loopback1 multicast-group 224.1.1.2** は設定できません。複数の異なるマルチキャスト グループ アドレスを同じサービス ファミリに設定するには、複数の送信元インターフェイスを使用する必要があります。
- マルチキャスト グループ アドレスは単一の送信元インターフェイスにのみ関連付けることができます。たとえば、**remote-neighbors source Loopback1 multicast-group 224.1.1.1** および **remote-neighbors source Loopback2 multicast-group 224.1.1.1** は設定できません。

動的ネイバーに関する情報

ネイバーが隣接していない場合、通常の Cisco SAF のピアリング機能を使用して、ネットワーク クラウド経由で SAF 情報を交換することはできません。ネイバーは通常、複数のホップ先であり、ダーク ネット（SAF を実行しないルータ）で区切られます。

SAF はこのタイプのネットワークをサポートするために、**neighbor** コマンドを提供します。これにより、リモート ネイバーが設定され、ユニキャスト パケット伝送によりセッションが確立されます。ただし、ネットワーク クラウド経由で SAF 情報を交換する必要があるフォワーダの数が増えると、ユニキャスト SAF ネイバーの定義は管理しにくくなることがあります。各ネイバーは手動で設定される必要があるので、運用コストが増加します。

これらのトポロジの展開、設定管理の容易化、運用コストの削減を促進するために、動的ネイバー機能は、リモート ユニキャストおよびマルチキャスト ネイバー（「リモート ネイバー」と呼ばれる）の動的な検出をサポートします。リモート ネイバーがサポートされているため、Cisco SAF を 1 つ以上のリモート ネイバーとピアリングさせることができます。この情報はルータを設定する時点では認識されている必要がないため、設定管理が軽減されます。

リモート ネイバー セッション ポリシー

リモート ユニキャスト リッスンまたはリモート マルチキャスト グループ ネイバー設定を使用しているときは、SAF ネイバーの IP アドレスが定義されておらず、ネイバーは何ホップも離れた場所にある可能性があります。この設定のルータは有効な HELLO パケットを送信するルータとピア関係を確立できます。セキュリティ上の理由から、このオープンな側面はポリシー機能を有効なルータへのピアリングに限定し、リソース消費を最小限に抑えるため、ネイバー数を制限する必要があります。この機能は、次の手動で設定されたパラメータを使用して実行され、即座に有効になります。

ネイバー フィルタ リスト

remote-neighbors コマンドで使用できる、オプションの **allow-list** キーワードにより、アクセス リスト（アクセス コントロール リスト）を使用して、Cisco SAF ネイバー接続が受け入れられる可能性のあるリモート IP アドレスを指定できます。**allow-list** キーワードを使用しないと、すべての IP アドレス（permit any）が受け入れられます。

アクセス コントロール リスト（ACL）は、次の条件の IPv4 または IPv6 IP アドレスの範囲を定義します。

- アクセス リストの IP アドレスに一致する送信元 IP アドレスを持つネイバーは、ユーザ設定に基づいて許可（または拒否）されます。
- **allow-list** キーワードが指定されないと、どの IP アドレスも許可されます（permit any）。
- **allow-list** キーワードは、リモート マルチキャスト グループおよびユニキャスト リッスン ネイバーに対してのみサポートされます。静的、リモート静的、またはローカル ネイバーでは使用できません。

- 指定したアクセス リストに一致しない Cisco SAF 入力パケットは拒否されます。

最大リモート ネイバー

remote-neighbors コマンドで使用可能な、オプションの **max-neighbors** キーワードにより、Cisco SAF がリモート ネイバー設定を使用して作成できるリモート ネイバーの最大数を指定できます。設定に対しリモート ネイバーの最大数が作成されたら、Cisco SAF はその構成のすべての後続の接続試行を拒否します。このオプションは、ルータのリソースに負荷をかけようとして多くのリモート ネイバーを作成しようとする DoS 攻撃からの保護を支援します。

max-neighbors 設定オプションには、次の条件があります。

- このオプションは、マルチキャスト グループまたはユニキャスト リッスン ネイバー に対してのみサポートされます。ローカル、静的、またはリモート静的ネイバーでは使用できません。
- デフォルトの最大値はありません。リモート ネイバーの最大数を指定しないと、リモート ネイバーの数は、使用可能なメモリと帯域幅により制限されます。
- リモート ネイバーの最大数を現在のセッション数以下に減らすと、ネイバー数が新しい制限に達するまで、ネイバーは廃棄されます（順不同）。

ネイバーのフィルタ リスト、および最大リモート ネイバーの設定の変更

allow-list または **max-neighbors** 設定が変更されたときに、新しい設定では許可されていないすべての既存のリモート Cisco SAF セッションは自動的かつ即座に削除されます。新しい設定によって引き続き許可されている既存のネイバーは影響を受けません。

ネイバー タイプ

ネイバー タイプについて説明する際には、次の用語が使用されます。

- ローカル ネイバー：共有サブネット（または共通サブネット）に隣接し、パケット交換用のリンクローカル マルチキャスト アドレスを使用するネイバー。これは、Cisco SAF のネイバーのデフォルト タイプです。
- 静的ネイバー：通信にユニキャストを使用し、1 つのホップ先で、共通サブネット上にあり、IP アドレスが **neighbor***ip-address* コマンドを使用して指定されたネイバー。
- リモート ネイバー：リモート静的ネイバーを含む、複数のホップ先のネイバー。
- リモート静的ネイバー：通信にユニキャストを使用し、複数のホップ先で、IP アドレスが **neighbor***ip-address* コマンドを使用して指定されたネイバー。
- リモート マルチキャスト グループ：複数のホップ先ですが、**neighbor***ip-address* コマンドを使用して手動で設定された IP アドレスを持たず、パケット交換用に設定されているマルチキャスト グループ アドレスを使用するネイバー。

- リモート ユニキャスト リッスン（または単にユニキャスト リッスン）：通信にユニキャストを使用し、複数のホップ先で、IP アドレスが **neighbor***ip-address* コマンドを使用して設定されていないネイバー。

リモート ユニキャスト リッスン（ポイントツーポイント）ネイバー

複数のリモート ネイバーが 1 つのハブとピアリングする設定（ポイントツーポイント）の場合、**remote-neighbors** コマンドを使用して、ハブをリモート ユニキャスト リッスン ピアリング用に設定でき、ハブのリモート ネイバーの IP アドレスを手動で設定する必要なく、リモート ネイバーはハブとピアリングできます。

このコマンドを使用して設定すると、ハブ ルータは次のことを実行します。

- すべてのユニキャスト伝送の送信元の IP アドレスとしてインターフェイス IP アドレスを使用します。この IP アドレスはルーティング可能なものでなければなりません。
- ハブとピアリングするネイバーは、**neighbor***ip-address* **loopback** *loopback-interface-number* **remote***maximum-hops* コマンドを使用して設定する必要があります。この *ip-address* はローカル ルータ インタフェースの IP アドレスのユニキャスト アドレスです。
- **remote-neighbor** コマンドで指定されたインターフェイスのユニキャスト HELLO パケットをリッスンします。
- ユニキャスト HELLO パケットが **allow-list** キーワードを使用して設定された IP アドレス範囲にある場合は受け入れ、または許可リストが定義されていなければ、すべてのユニキャスト HELLO パケットを受け入れます。
- ユニキャスト HELLO パケットも送信していて、ユニキャスト許可リストにより許可されている（または許可リストが定義されていなければ、すべてのネイバー）、すべてのネイバーからのマルチキャスト HELLO パケットを拒否します。
- ネイバー関係が確立されると、パケット転送のためのリモート ネイバーの IP アドレスを使用して、通常のネイバーの確立を開始します。

リモート マルチキャスト グループ（マルチポイントツーマルチポイント）ネイバー

マルチキャストは、複数の Cisco SAF ネイバー間の効率的な転送を実現するために使用できます。1 つのマルチキャスト グループ アドレスを使用して、複数の Cisco SAF ネイバーが同じマルチキャスト グループ内で情報の交換をすることができます。マルチポイントツーマルチポイントを設定するには、**remote neighbors** コマンドで使用可能な **multicast-group** キーワードを使用します。

このコマンドを使用して設定すると、ルータは次のことを実行します。

- すべてのユニキャスト伝送の送信元の IP アドレスとしてインターフェイス IP アドレスを使用します。この IP アドレスはルーティング可能なものでなければなりません。

- 送受信されたすべてのマルチキャスト パケット用に設定されたマルチキャスト グループ アドレスを使用します。
- マルチポイントツーマルチポイントのネイバー関係を形成する、すべてのフォワーダおよびルータは、同じマルチキャストグループIPアドレスを使用して設定される必要があります。
- 定義されたマルチキャストグループアドレスのマルチキャストフォワーディングは、パケット配信のために設定され、機能することが必要です。

リモート ネイバー設定の継承と優先度

neighbor*ip-address* または **neighbor***ip address***remote** コマンドを使用して設定した静的ネイバーは、**remote-neighbors** コマンドの結果として作成されたリモート ネイバーよりも優先されます。着信ユニキャスト Cisco SAF 接続のリモート IP アドレスが、静的ネイバーと、リモート ユニキャスト リッスン ネイバーのアクセス リストの両方に一致する場合、静的ネイバーが使用され、リモート ユニキャスト リッスン ネイバーは作成されません。同じリモートIPアドレスのリモートネイバーがすでに存在する間に新しいスタティック ネイバーを設定すると、Cisco SAF は自動的にリモート ユニキャスト リッスン ネイバーを削除します。

リモート ユニキャスト リッスン ネイバーはリモート マルチキャスト グループ ネイバーよりも優先されます。Cisco SAF が同じローカル インターフェイスを対象とする同じリモート IP アドレスからユニキャストとマルチキャストの両方の HELLO を受信すると、パケット交換に対し、ネイバーはマルチキャスト（マルチキャストグループ）ではなくユニキャスト（ユニキャストリッスン）として処理されます。

動的ネイバーの設定方法

Cisco SAF 動的ネイバーを設定するには、次のコマンドを使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routereigrp***virtual-instance-name*
4. **service-family**{**ipv4** | **ipv6**} [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
5. **remote-neighborssource***interface* {**unicast-listen** | **multicast-group** *group-address* } [**allow-list** *access-list-name*] [**max-neighbors** *max-remote-peers*]
6. **exit-service-family**

手順の詳細

	コマンドまたはアクション	目的
ステップ **1**	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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。
ステップ 3	**routereigrp***virtual-instance-name* 例： `Router(config)# router eigrp saf`	グローバル コンフィギュレーション モードで EIGRP 仮想インスタンスを有効にします。
ステップ 4	**service-family**{**ipv4** | **ipv6**} [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* 例： `Router(config-router)# service-family ipv4 autonomous-system 4453`	ルータ上で指定された自律システム用の Cisco SAF サービス ファミリを有効にします。
ステップ 5	**remote-neighborssource***interface* {**unicast-listen** | **multicast-group** *group-address* } [**allow-list** *access-list-name*] [**max-neighbors** *max-remote-peers*] 例： `Router(config-router-sf)# remote-neighbors source Loopback1 unicast-listen allow-list myNeighborList`	リモート ネイバーがすべてのリモート IP アドレスからの着信接続を受け入れるようにする SAF プロセスを設定します。 以下を使用します。 • Cisco SAF ネイバー接続が受け入れられる可能性のあるリモート IP アドレスを指定するアクセス リスト（アクセス コントロール リスト）を使用するための **allow-list** キーワード。allow-list キーワードを使用しないと、すべての IP アドレス（permit any）が受け入れられます。 • リモート ネイバーの最大数を指定する **max-neighbors** キーワード。数を指定しないと、リモート ネイバーの最大数は、使用可能なメモリと帯域幅により制限されます。
ステップ 6	**exit-service-family** 例： `Router(config-router-sf)# exit-service-family`	サービス ファミリ コンフィギュレーション モードを終了します。

動的ネイバーの設定例

例：Cisco SAF の動的ネイバーの設定

次の例は、ネイバー関係に関与する両方のルータを設定する方法を説明します。

この例では、**unicast-listen** キーワードを使用して、アクセス リスト myNeighborList に一致する IP アドレスからの着信接続を受け入れるリモート ネバーを設定します。

```
Router1(config)# interface Loopback1
Router1(config-if)# ip address 10.1.1.1 255.255.255.255
Router1(config-if)# exit
Router1(config)# ip access-list standard myNeighborList
Router1(config-std-nacl)# permit 10.0.0.0 0.255.255.255
Router1(config-std-nacl)# exit
Router1(config)# router eigrp virtual-name
Router1(config-router)# service-family ipv4 autonomous-system 4453
Router1(config-router-sf)# remote-neighbors source Loopback1 unicast-listen allow-list
myNeighborList
Router2(config)# interface Loopback2
Router2(config-if)# ip address 10.2.2.2 255.255.255.255
Router2(config-if)# exit
Router2(config)# router eigrp virtual-name
Router2(config-router)# service-family ipv4 autonomous-system 4453
Router2(config-router-sf)# neighbor 10.1.1.1 Loopback2 remote 20
```

この例では、**multicast-group** キーワードを使用して、リモート ネイバーを検出し、リモート ネイバー関係を形成するために IP マルチキャストを使用します。また、マルチキャスト グループのメンバーが受け入れる可能性のあるリモート ネイバーからの着信接続の最大数を 30 に指定します。

```
Router1(config)# interface Loopback1
Router1(config-if)# ip address 10.1.1.1 255.255.255.255
Router1(config-if)# ip pim sparse-mode
Router1(config-if)# exit
Router1(config)# router eigrp virtual-name
Router1(config-router)# service-family ipv4 autonomous-system 4453
Router1(config-router-sf)# remote-neighbors source Loopback1 multicast-group 224.44.56.1
max-neighbors 30
Router2(config)# interface Loopback2
Router2(config-if)# ip address 10.2.2.2 255.255.255.255
Router2(config-if)# ip pim sparse-mode
Router2(config-if)# exit
Router2(config)# router eigrp virtual-name
Router2(config-router)# service-family ipv4 autonomous-system 4453
Router2(config-router-sf)# remote-neighbors source Loopback2 multicast-group 224.44.56.1
max-neighbors 30
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Service Advertisement Framework コマンド	『Cisco IOS Service Advertisement Framework Technology Command Reference』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

動的ネイバーの機能情報

表 *3* : 動的ネイバーの機能情報

機能名	リリース	機能情報
動的ネイバー	15.1(2)S、15.2(3)T、15.2(2)S、15.1(1)SG Cisco IOS XE 3.6S、Cisco IOS XE 3.3SG	動的ネイバー機能は、リモートユニキャストおよびマルチキャスト ネイバー（「リモート ネイバー」と呼ばれる）の動的な検出をサポートします。リモート ネイバーがサポートされているため、Cisco SAF を 1 つ以上のリモート ネイバーとピアリングさせることができます。 Cisco IOS XE 3.3 SG では、Cisco Catalyst 4000 シリーズ スイッチのサポートが追加されました。 次のコマンドが導入または変更されました。 • **authenticationmode** • **remote-neighborssource** • **showeigrpservice-familyexternal-client**

第 5 章

機能マネージャの設定

- 機能情報の確認，75 ページ
- 機能マネージャの設定の前提条件，75 ページ
- 機能マネージャに関する情報，76 ページ
- 機能マネージャの設定方法，80 ページ
- その他の参考資料，84 ページ
- 機能マネージャの機能情報，85 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

機能マネージャの設定の前提条件

- ルータで機能マネージャが使用可能なことを確認するには、**showservice-routingplugincapman** コマンドを入力します。ルータが機能情報を配信するためには、ルータの SAF Forwarder を設定します。
- ネットワーク内の他のルータの機能情報を表示するには、SAF Forwarder を設定します。

機能マネージャに関する情報

機能マネージャはデフォルトでシステムの起動時に有効化されます。起動時に、サービス ルーティング クライアントとして登録され、ハードウェアおよびソフトウェアプラットフォームのさまざまな機能の検出を開始します。

機能の検出

機能マネージャは機能がローカル システムでサポートされているかどうかだけを検出します。機能が設定されているかまたは有効かどうかは検出せず、またネットワーク内の他のルータの機能に関するその他の情報も検出しません。

機能情報は、サービス ルーティング データとしてローカルのネットワーク情報ベース（NIB）にインストールされ、サービス ルーティング ネットワークへのすべての SAF フォワーダによるアドバタイズメントに使用可能になりました。機能情報は XML 形式でサービス ルーティング インフラストラクチャに渡され、ローカルの NIB に保存されます。

SAF Forwarder との相互運用性

機能マネージャはサービス ルーティング ネットワークに機能情報をアドバタイズしません。SAF Forwarder は機能情報を配布する機能を実行します。ただし、SAF Forwarder は、機能マネージャが動作するのに必要ではありません。SAF Forwarder を設定しない場合、機能情報はローカル ルータにバインドされており、ネットワーク内の他のルータに配布されません。SAF Forwarder を設定すると、デフォルトですべての機能の情報を配布します。

機能情報

機能情報は、サービス ルーティング データとしてネットワーク情報ベース（NIB）にインストールされます。これは、次の形式の SAF アドレスで識別されます。

- サービス ID：機能マネージャはサービス ID 100 を使用します。
- サブサービス ID：機能グループ ID。サブサービス ID は機能のデータ タイプのグループ ID を示します。
- インスタンス番号：ローカル ルータの一意の識別子。これはハードウェアのシリアル番号、デフォルトの MAC アドレス、IPv4 ルータ ID、または IPv6 ルータ ID の順番で割り当てられます。

機能グループ

機能マネージャはクエリと取得を促進するためにグループによって機能を分類し、グループごとに一意の ID を割り当てます。機能マネージャは次の機能グループを提供します。

- 1（ハードウェア）
- 2（ソフトウェア）

ハードウェア グループ情報

ハードウェア情報は、グループ ID 1 として指定されます。使用可能な場合は、グループ 1 は次の機能情報を提供します。すべてのハードウェア情報が、機能マネージャをサポートする各プラットフォームで使用できるとは限りません。

- Host Name
- Platform
- 共有メモリ サイズ
- IO メモリ サイズ

ソフトウェア グループ情報

ソフトウェア情報は、グループ ID 2 として指定されます。使用可能な場合は、グループ 2 は次の機能情報を提供します。すべてのソフトウェア情報が、機能マネージャをサポートする各プラットフォームで使用できるとは限りません。

- Host Name
- Software
- Image
- Version
- ソフトウェア サブシステム：
  - IP Multicast：IP マルチキャスト
  - eigrp_ipv4
  - eigrp_ipv6
  - fh_fd_ipsla
  - ospf
  - ospfv3
  - isis
  - isis_ipv6

- bgp_ipv4
- bgp_ipv6
- service_routing

機能データの XML スキーマ

SAF Forwarder に接続されている Extensible Messaging Client Protocol（XMCP）クライアント（外部クライアント）がある場合、サービス ID 100 である機能マネージャに登録できます。データは次の XML スキーマを使用して解釈できます。

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs='http://www.w3.org/2001/XMLSchema'>
<xs:element name="Capabilities" type="CapabilitiesType" />
<xs:complexType name="CapabilitiesType">
<xs:sequence>
<xs:element ref="Group" minOccurs="1" maxOccurs="unbounded" />
</xs:sequence>
</xs:complexType>
<xs:element name="Group" type="GroupType" />
<xs:complexType name="GroupType">
<xs:sequence>
<xs:element ref="Capability" minOccurs="1" maxOccurs="unbounded" />
</xs:sequence>
<xs:attribute name="Name" type="xs:normalizedString" use="required" />
</xs:complexType>
<xs:element name="Capability" type="CapabilityType" />
<xs:complexType name="CapabilityType">
<xs:sequence>
<xs:element name="Value" type="xs:normalizedString" />
</xs:sequence>
<xs:attribute name="Name" type="xs:normalizedString" use="required" />
</xs:complexType>
</xs:schema>
```

例：

```
<Capabilities>
<Group Name="HARDWARE">
<Capability Name="HostName">
```

```
<Value>R100</Value>
</Capability>
<Capability Name="Platform">
<Value>Solaris Unix (Sparc) processor</Value>
</Capability>
<Capability Name="MainMemorySize">
<Value>63683Kbytes</Value>
</Capability>
</Group>
<Group Name="SOFTWARE">
<Capability Name="HostName">
<Value>R100</Value>
</Capability>
<Capability Name="Software">
<Value>Cisco IOS Software</Value>
</Capability>
<Capability Name="Image">
<Value>Solaris Software (UNIX-ADVENTERPRISE-M)</Value>
</Capability>
<Capability Name="Version">
<Value>Experimental Version 15.1(20110323:093227)</Value>
</Capability>
<Capability Name="ipmulticast">
<Value>Subsystem loaded</Value>
</Capability>
<Capability Name="eigrp_ipv4">
<Value>Subsystem loaded</Value>
</Capability>
</Group>
</Capabilities>
```

機能マネージャの設定方法

機能マネージャの有効化および無効化

機能マネージャはデフォルトで有効になっています。機能マネージャはいつでも無効にしたり再度有効にすることができます。

- 機能マネージャを無効にすると、ローカルのネットワーク情報ベース（NIB）にインストールされている機能情報は削除され、その情報はサービス ルーティングから登録解除されます。
- 機能マネージャを再度有効にすると、機能が再検出され、ローカルの NIB およびサービス ルーティングに情報が提供されます。

次の作業を実行して、機能マネージャを無効にして再度有効にします。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **no service-routingcapabilities-manager**
4. **service-routing capabilities-manager**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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。
ステップ 3	**no service-routingcapabilities-manager** 例： `Router(config)# no service-routing capabilities-manager`	機能マネージャを無効にします。

	コマンドまたはアクション	目的
ステップ 4	**service-routing capabilities-manager** 例： `Router(config)# service-routing capabilities-manager`	機能マネージャを有効にします。

機能マネージャ情報の表示

機能マネージャに関する情報を表示するには、特権 EXEC モードで次のコマンドを使用します。

手順の概要

1. **show service-routing plugins** *plugin-name*
2. **show service-routing plugins capabilities-manager internal**
3. **show service-routing capabilities-manager**
4. **show service-routing capabilities-manager** [**group** *group-id*] [**local**]

手順の詳細

ステップ 1 **show service-routing plugins** *plugin-name*

例：

```
Device> show service-routing plugins capman

Service Routing plugins:::
    capman             :   1.00.00 : Cisco Capability Manager
```

機能マネージャ プラグインに関する情報が表示されます。

ステップ 2 **show service-routing plugins capabilities-manager internal**

例：

```
Device> show service-routing capabilities-manager internal

Service-Routing Capabilities Manager
====================================

Major Version: 1  Minor Version: 0  Edit Version: 0
Reachability: 5.12.20.13:0
Local Instance GUID: 53504531-3233-3830-3136-390000000000
```

機能マネージャに関する内部情報を表示します。

ステップ 3 **show service-routing capabilities-manager**

例：

```
Device> show service-routing capabilities-manager

Service-Routing Capabilities Manager
====================================

Registered Capabilities
=======================

Group/ID: HARDWARE/1
Service: 100:1:53504531-3233-3830-3136-390000000000
Originator: 5.12.20.13
Capability Data:
<Capabilities>
<Group Name="HARDWARE">
  <Capability Name="HostName">
    <Value>Router</Value>
  </Capability>
  <Capability Name="Platform">
    <Value>cisco WS-C4503-E (MPC8572) processor</Value>
  </Capability>
  <Capability Name="MainMemorySize">
    <Value>786516Kbytes</Value>
  </Capability>
  <Capability Name="IOMemorySize">
    <Value>20480Kbytes</Value>
  </Capability>
</Group>
</Capabilities>


Group/ID: SOFTWARE/2
Service: 100:2:53504531-3233-3830-3136-390000000000
Originator: 5.12.20.13
Capability Data:
<Capabilities>
<Group Name="SOFTWARE">
  <Capability Name="HostName">
    <Value>Router</Value>
  </Capability>
  <Capability Name="Software">
    <Value>Cisco IOS Software</Value>
  </Capability>
  <Capability Name="Image">
    <Value> Catalyst 4500 L3 Switch Software (cat4500e-UNIVERSALK9-M)</Value>
  </Capability>
  <Capability Name="Version">
    <Value> Version 15.2(1.1.69)E</Value>
  </Capability>
  <Capability Name="ipmulticast">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="eigrp_ipv4">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="eigrp_ipv6">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="ospf">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="ospfv3">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="isis">
    <Value>Subsystem Loaded</Value>
```

```
  </Capability>
  <Capability Name="isis_ipv6">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="bgp_ipv4">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="bgp_ipv6">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="fh_fd_ipsla">
    <Value>Subsystem Loaded</Value>
  </Capability>
  <Capability Name="service_routing">
    <Value>Subsystem Loaded</Value>
  </Capability>
</Group>
</Capabilities>
```

機能マネージャに関する情報を表示します。

ステップ 4 **show service-routing capabilities-manager** [**group** *group-id*] [**local**]

例：

```
Device# show service-routing capabilities-manager group 1 local

Service-Routing Capabilities Manager
====================================

Registered Capabilities
=======================

Group/ID: HARDWARE/1
Service: 100:1:53504531-3233-3830-3136-390000000000
Originator: 5.12.20.13
Capability Data:
<Capabilities>
<Group Name="HARDWARE">
  <Capability Name="HostName">
    <Value>Router</Value>
  </Capability>
  <Capability Name="Platform">
    <Value>cisco WS-C4503-E (MPC8572) processor</Value>
  </Capability>
  <Capability Name="MainMemorySize">
    <Value>786516Kbytes</Value>
  </Capability>
  <Capability Name="IOMemorySize">
    <Value>20480Kbytes</Value>
  </Capability>
</Group>
</Capabilities>
```

登録された機能に関する情報を表示します。

登録済み機能情報の削除

NIB から現在の機能情報を削除するには、次の作業を実行します。NIB が削除されると、機能マネージャは自動的に新しい機能を再検出します。

手順の概要

1. イネーブル化
2. **clear service-routingcapabilities-manager**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear service-routingcapabilities-manager** 例： `Device# clear service-routing capabilities-manager`	NIB データベースの現在の機能情報を削除します。機能マネージャが自動的に新しい機能を再検出します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Service Advertisement Framework コマンド	『Cisco IOS Service Advertisement Framework Technology Command Reference』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

機能マネージャの機能情報

表 *4*：機能マネージャの機能情報

機能名	リリース	機能情報
機能マネージャ	15.0(1)SY、15.2(3)T、15.2(2)S Cisco IOS XE 3.6S、Cisco IOS XE 3.3SG 15.2(1)E	機能マネージャはデフォルトでシステムの起動時に有効化されます。起動時に、サービスルーティング クライアントとして登録され、ハードウェアおよびソフトウェア プラットフォームのさまざまな機能の検出を開始します。 Cisco IOS XE 3.3 SG では、Cisco Catalyst 4000 シリーズ スイッチのサポートが追加されました。 次のコマンドが導入または変更されました。 • **clear service-routingcapabilities-manager** • **service-routingcapabilities-manager** • **show service-routingplugins capman** • **showservice-routingcapabilities-managerinternal** • **showservice-routingcapabilities-manager group**