Cisco Network Positioning System Cisco ASR 1000 ルータ リリース 1.0 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/

Text Part Number: OL-25794-01-J

【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。

目 次

はじめに v

目的 v

マニュアルの変更履歴 v

表記法 vi

関連資料 viii

マニュアルの入手方法およびテクニカル サポート viii

Network Positioning System の一般的な設定 1

PE での基本的なネットワーキングの設定 1

XMPP サーバの設定 3

XMPP サーバの設定 3

サービス配置の設定 5

サービス解決エンジンに関する情報 5

サービス解決エンジンのランキング要件 6

サービス解決エンジンの設定 6

サービス解決の設定例 8

show service-resolution dc コマンド：例 8

show service-resolution service-requests コマンド：例 9

機能ディレクトリの設定 11

機能ディレクトリの設定 11

サービスを選択するためのパフォーマンス メトリックの設定 13

パフォーマンス マネージャの前提条件 13

パフォーマンス マネージャの制限事項 13

パフォーマンス マネージャに関する情報 14

eXtensible Messaging and Presence Protocol クライアントの登録 15

パフォーマンス マネージャのメッセージ処理 16

パフォーマンス マネージャの設定方法 17

DC-Facing PE でのパフォーマンス マネージャの設定 17
CE-Facing PE でのパフォーマンス マネージャの設定 18
ネットワーク プロキシミティに使用するルーティング プロトコルの設定 23
ネットワーク ルーティング プロキシミティに関する情報 23
PXE のデータ要素 24
PXE のピアリングおよびランキング 25
ルーティング プロトコルの設定方法 25
プロキシミティの計算に向けた OSPF の設定 25
プロキシミティの計算に向けた BGP の設定 27
プロキシミティの計算に向けた IS-IS の設定 29
NPS の設定例 33
CE-Facing PE の設定例 33
DCE-Facing PE の設定例 34

はじめに

ここでは、『Cisco Network Positioning System Cisco ASR 1000 RouterCisco CRS RouterCisco ASR 9000 Router コンフィギュレーション ガイド』に関する情報を提供します。「はじめに」の内容は、次のとおりです。

- 目的，v ページ
- マニュアルの変更履歴，v ページ
- 表記法，vi ページ
- 関連資料，viii ページ
- マニュアルの入手方法およびテクニカル サポート，viii ページ

目的

『Cisco Network Positioning System Cisco ASR 1000 RouterCisco CRS RouterCisco ASR 9000 Router コンフィギュレーション ガイド』では、ルータで NPS を設定する方法について説明しています。

このマニュアルは、ルータ ベースのインターネットワーク設定に関する十分な知識および Cisco ルータとそれに関連するソフトウェアでの十分な経験を持つサービス プロバイダー カスタマーと Cisco インストール パートナーを対象としています。

マニュアルの変更履歴

初版後このマニュアルに加えられた技術的な変更の履歴をこの表に示します。

表 *1*：マニュアルの変更履歴

リビジョン	日付	変更点
OL-25811-01	2011 年 12 月	このマニュアルの初版

リビジョン	日付	変更点
OL-25794-01-J	2011 年 11 月	このマニュアルの初版

リビジョン	日付	変更点
OL-27948-01	2012 年 11 月	このマニュアルの初版

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control（Ctrl）キーを表します。 たとえば、**^D** または **Ctrl+D** というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します （ここではキーを大文字で表記していますが、小文字で入力してもかまいません）。
太字フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字**フォントで示しています。
イタリック体	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、イタリック体フォントで示しています。
`courier` フォント	システムが表示するターミナルセッションおよび情報は、`courier` フォントで示しています。
`太字の courier フォント`	太字の courier フォントは、ユーザが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。
...	構文要素の後の省略記号（3 つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。
|	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[x | y]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。

表記法	説明
{x | y}	いずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。 角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。 stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてstringとみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。

（注） 「注釈」です。 役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。 機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス 時間を節約する方法です。 ここに紹介している方法で作業を行うと、時間を短縮できます。

警告 **「警告」の意味です。 人身事故を予防するための注意事項が記述されています。**

関連資料

Cisco NPS の設定およびリファレンスの詳細については、以下のマニュアルを参照してください:

参照先	説明
『Cisco Network Positioning System Command Reference for the Cisco ASR 1000 RouterCisco CRS RouterCisco ASR 9000 Router』	サポートされているすべてのコマンドの構文について説明します。
『Cisco Network Positioning System Installation on Cisco ASR 1000 Routers』	Cisco ASR 1000 ルータで NPS をインストールする方法について説明します。
『Cisco Network Positioning System Installation on Cisco ASR 9000 Routers』	Cisco ASR 9000 ルータで NPS をインストールする方法について説明します。
『Cisco Network Positioning System Installation on Cisco CRS Routers』	Cisco CRS ルータで NPS をインストールする方法について説明します。
『Cisco Network Positioning System Overview』	NPS のサービス解決のコンポーネントについて説明します。
『Cisco Network Positioning System ITSM API Guide』	ITSM API および RESTful API を使用してプロキシミティやランキングに関する情報を要求し、取得する方法について説明します。
『Cisco Network Positioning System Capability Directory Messages Guide』	CD のアドバタイズ メッセージについて説明します。
『Release Notes for Cisco Network Positioning System on Cisco ASR 9000 Series Aggregation Services Routers』	Cisco ASR 9000 シリーズ ルータで Cisco NPS を実行する場合の警告事項および要件を示します。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 1 章

Network Positioning System の一般的な設定

Network Positioning System（NPS）の設定では次のタスクを実行します。

1. NPS と通信できるようにルータを設定する。 これには、ルータに対するホスト名の割り当てもあります。
2. データセンター（DC）に対向する 1 台のプロバイダーエッジルータ（PE）に対して eXtensible Messaging、Presence Protocol（XMPP）サーバを設定する。
3. 1 台の DC-Facing PE に対してサービス解決エンジン（SRE）を設定する。
4. SRE を設定したときと同じ DC-Faicng PE に対して機能ディレクトリ（CD）を設定する。
5. ルータ上で実行するパフォーマンス マネージャ（PFM）を設定する。 この設定は、DC-Facing PE を設定するか、カスタマー エッジ ルータ（CE）に対向する PE を設定するかによって異なります。
6. プロキシミティ エンジン（PXE）でのプロキシミティの計算にルーティング プロトコルを使用できるように、ルータに対してそれらのルーティング プロトコルを設定する。

このモジュールでは、ルータが NPS と通信できるようになるうえで必要となる基本的な設定について説明します。 その他の設定作業については、このマニュアルの以降のモジュールを参照してください。

- PE での基本的なネットワーキングの設定，1 ページ

PE での基本的なネットワーキングの設定

システムにある CE-Facing PE および DCE-Facing PE のそれぞれに XMPP サーバからアクセスできるようにするには、次の設定が必要です。

手順の概要

1. **hostname** *hostname*
2. **ip host** *hostname ip-address*
3. **ip name-server** *ip-address*
4. **interface** *interface-name*
5. **ip address** *ip-address mask*
6. **no shutdown**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**hostname** *hostname* 例： `server(config)# hostname ccnsr.com`	ルータのホスト名を設定します。
ステップ 2	**ip host** *hostname ip-address* 例： `server(config)# ip host ccnsr.com 172.16.0.2`	実行している XMPP サーバの IP アドレスを指定します。
ステップ 3	**ip name-server** *ip-address* 例： `server(config)# ip name-server`	ネーム サーバのアドレスを指定します。 **ip host** コマンドを使用しない場合にのみ、このコマンドが必要です。

ステップ 4	**interface** *interface-name*
	
	例：
	`server(config)# interface gigabitethernet 0eth0`
	`server(config-if)#`
		インターフェイス コンフィギュレーション モードを開始してインターフェイスをイネーブルにします。

ステップ 5	**ip address** *ip-address mask* 例： `server(config-if)# ip address 172.17.0.3 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 6	**no shutdown** 例： `server(config-if)# no shutdown`	インターフェイスをイネーブルにします。

次の作業

XMPP サーバを設定します。

第 2 章

XMPP サーバの設定

eXtensible Messaging and Presence Protocol（XMPP）は、ほぼリアルタイムの通信を実現するためのオープンな XML ベースの標準です。 XMPP は、情報の配信でさまざまなプラットフォームにわたってほぼリアルタイムの通信を提供できるので、NPS コンポーネント間で使用する主要な通信と転送のプロトコルとなっています。

Jabber は、NPS ソフトウェアと同時にインストールされる XMPP の実装です。 このモジュールでは、Jabber の設定について説明します。

NPS のインストールでは XMPP ソフトウェアはインストールされません。 NPS のさまざまなコンポーネント間でリアルタイム通信を容易にする XMPP ソフトウェアをインストールする必要があります。 あらゆるプラットフォームで動作する XCP の使用を推奨します。

- XMPP サーバの設定，3 ページ

XMPP サーバの設定

サービス解決を目的とした PE ルータ間の通信を容易にするために、Jabber を使用します。 次のタスクで、システムにある PE ルータのいずれかで Jabber サーバを設定します。 XMPP の pubsub プロトコルを使用してデバイスの機能を取得する際にも、機能ディレクトリ（CD）で Jabber を使用します。 一般的には、サービス解決エンジン（SRE）をインストールした DCE-Facing PE に Jabber サーバをインストールします。

手順の概要

1. **jabber server**
2. **domain** *domain-name*
3. **ipaddr ipv4** *ip-address*
4. **log-level** *level*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**jabber server** 例： `switch(config)# jabber server`	ルータで XMPP サーバを設定する Jabber コンフィギュレーション モードを開始します。
ステップ 2	**domain** *domain-name* 例： `switch(config-jabber)# domain ccnsr.com`	Jabber サーバのドメイン名を指定します。
ステップ 3	**ipaddr ipv4** *ip-address* 例： `switch(config-jabber)# ipaddr ipv4 172.16.0.2`	Jabber サーバに使用する IP アドレスを指定します。
ステップ 4	**log-level** *level* 例： `switch(config-jabber)# log-level info`	表示する通知を指定します。表示されるオプションには、次のものがあります。 • **debug** • **error** • **info** • **verbose** • **warn**

次の作業

SRE を設定します。

第 3 章

サービス配置の設定

Cisco NPS では、サービス解決エンジン（SRE）で推奨のサービス配置を指定します。 これは、要求されたサービスをサポートする多数のデータセンターからいずれかを選択する操作です。 SRE では、目的のサービスのパラメータが指定されたサービス要求を受け取ります。このようなサービスとして、たとえば仮想データセンター（vDC）でのデバイスのアクティブ化があります。 SRE からは、この要求に対応できる物理データセンターのリストを返します。このリストでは、サービス解決ポリシーで定義されているパラメータに従った順序でデータセンターが記述されています。

- サービス解決エンジンに関する情報，5 ページ
- サービス解決エンジンの設定，6 ページ

サービス解決エンジンに関する情報

SRE の主な機能は、ネットワークの中でサービスの配置に最適な場所を推奨することです。 SRE では、次のような所要のサービス パラメータを指定したサービス要求を取得します。

- 必要とするコンピューティング能力を備えた仮想データ センタ（vDC）リソース
- ストレージ容量
- ファイアウォールやロード バランサなどのネットワーク サービス
- サービスの論理トポロジ
- ポリシーのハンドル

SRE は、これらの要件を満足できるデータセンター（DCS）のリストを返します。このリストでは、該当のポリシーおよびユーザ指定の順序設定に従った順序でデータセンターが記述されています。 たとえば、サービスの起点と物理データセンター間のネットワーク プロキシミティや、サービスの起点と物理データセンター間のパフォーマンス メトリックに従って、データセンターを推奨される順に並べることができます。

SRE は、外部ポリシー サーバとのインターフェイスを通じて関連のポリシーを取得します。また、*NGN* 機能ディレクトリ（*NCD*）、パフォーマンス マネージャ（*PFM*）、プロキシミティ エンジン（*PXE*）などの内部コンポーネントとの対話を通じて、サービスの推奨事項を提示するために必要なデータを取得します。

サービス解決エンジンのランキング要件

SRE では、プロキシミティのランキングを求めるサービス要求があると、サービスの起点とデータセンター間のネットワーク プロキシミティに従ってデータセンターをランキングできます。

プロキシミティのランキング

Cisco NPS で扱うプロキシミティのランキングは、プロバイダー エッジ デバイスに対向するカスタマー エッジ デバイスとプロバイダー エッジ デバイスに対向するデータセンター エッジ デバイスとの間のネットワーク距離に基づきます。

パフォーマンスのランキング

SRE では、パフォーマンスのランキングを求めるサービス要求があると、パフォーマンスに従ってデータセンターをランキングできます。

Cisco NPS で扱うパフォーマンスのランキングは、プロバイダー エッジ デバイスに対向するカスタマー エッジ デバイスからプロバイダー エッジ デバイスに対向するデータセンター エッジ デバイスとの間で数値化したパフォーマンス属性値に基づきます。 ユーザは、パフォーマンス属性ごとに異なるランキングのプライオリティを割り当てることができます。 SRE でサポートしている属性は次のとおりです。

- トラフィックの遅延
- トラフィックの損失

ユーザはさまざまなパフォーマンス属性の組み合わせを選択し、それぞれに別々のランキング プライオリティを割り当てることができます。

サービス解決エンジンの設定

次の設定をプロバイダー エッジ ルータ（PE）で実行して、サービス解決エンジン（SRE）をイネーブルにします。 ネットワークの DCE-Facing PE で SRE を実行することを推奨します。

手順の概要

1. **service-resolution web-service address** *ip-address* [**port** *port*]
2. **service-resolution web-service username** *username* **password** *password*
3. **service-resolution dc** *id* **pe-address** *address*
4. **service-resolution exclude dc** *id*
5. **service-resolution service-request timeout** *timeout-interval*
6. **service-resolution web-service crypto certificate** *certificate*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**service-resolution web-service address** *ip-address* [**port** *port*] 例： `switch(config)# service-resolution web-service address 10.0.0.1 port 10000`	サービス解決 API Web サービスのホスト名（または IP アドレス）およびポートを設定します。アドレスは明示的に設定できます。 • *ip-address*：このサービス解決 API に外部から到達するために使用する IP アドレス。 • *port*：この API に外部から到達するために Web サーバアドレスの中で指定するポート。
ステップ 2	**service-resolution web-service username** *username* **password** *password* 例： `SR(config)# service-resolution web-service username foo password 1234`	サービス解決 API のユーザ認証で使用するユーザ名とパスワードを設定します。設定できるユーザ名とパスワードのペアは 1 つのみです。ユーザ名とパスワードを設定しないと、ユーザ認証がディセーブルになります。 • *username*：追加するサービス解決 API ユーザ名。 • *password*：このユーザ名に関連付けるパスワード。

ステップ 3	**service-resolution dc** *id* **pe-address** *address*
	
	例：
	`SR(config)# service-resolution dc att-west pe-address 5.5.5.5`
	`SR(config)# service-resolution dc DC1 pe-address 2.2.2.2`
	`SR(config)# service-resolution dc DC1 pe-address 3.3.3.3`
	`SR(config)# service-resolution dc DC2 pe-address 4.4.4.4`
	`SR(config)# service-resolution dc DC2 pe-address 1.1.1.1`
		データセンター（DC）と PE のペアを設定します。このコマンドで入力したデータセンターは、DC に接続した PE に関連付けられるほか、DC 候補のリストにも使用されます。
		• *id*：一意のデータセンター識別情報。
		• *address*：DC へのアクセスに使用する PE の IP アドレス。このアドレスは、さまざまなタイプのランキング（パフォーマンス、プロキシミティなど）でエンドポイントとして使用されます。

	コマンドまたはアクション	目的
ステップ 4	**service-resolution exclude dc** *id* 例： `switch(config)# service-resolution exclude dc att_west`	グローバルな除外リストにデータセンターを追加します。つまり、サービス配置として推奨する処理から除外するデータセンターのリストにデータセンターを追加します。一般的には、メンテナンスのためにデータセンターがダウンしている場合に、この除外処理を実行します。 • *id*：除外するデータセンターの識別情報。
ステップ 5	**service-resolution service-request timeout** *timeout-interval* 例： `switch(config)# service-resolution service-request timeout 90`	サービス要求のタイムアウト間隔を秒数で指定します。有効値の範囲は、1 ～ 3600 です。 デフォルトは 30 秒です。
ステップ 6	**service-resolution web-service crypto certificate** *certificate* 例： `switch(config)# service-resolution web-service crypto certificate lighttpd.pem`	HTTPS をサポートするために、サービス解決 Web サービスの暗号証明書を設定します。

サービス解決の設定例

show service-resolution dc コマンド：例

```
SR-1# show service-resolution dc

------------------------------------------------------------------------
DC
     PE-name                                    PE-address
------------------------------------------------------------------------
DC1
     PE1                                        1.1.1.1
     PE2                                        2.2.2.2
     PE3                                        3.3.3.3
DC2
     PE4                                        4.4.4.4
     PE1                                        1.1.1.1
my-data-center-14
     my-pe-22                                   22.22.22.22
     my-pe-28                                   111.111.111.111
```

show service-resolution service-requests コマンド：例

```
SR-1# show service-resolution service-requests

Service-Request:
  ID:          00000001
  vdc_id:      22222
  user_handle: my_handle_1
  URI:         https://sr.foobar.net/sr/serv_req_00000001

  state:       DONE
  Message:     Service-request '000000001' processing successfully completed.
  Detail:      n/a

  CE-address:     10.10.10.1
    PE-address:   10.10.10.2

  Ranked DC list:
    DC:           amazon_west
      PE-address: 30.30.30.2
      PE-address: 20.20.20.1
    DC:           att_west
      PE-address: 50.50.50.1
      PE-address: 60.60.60.1
      PE-address: 40.40.40.1

Service-Request:
  ID:          00000050
  vdc_id:      12345
  user_handle: h2
  URI:         https://sr.foobar.net/sr/serv_req_00000050

  state:       PENDING
  Message:     Waiting for ranking processing to complete
  Detail:      n/a

Service-Request:
  ID:          00001000
  vdc_id:      7890
  user_handle: handle3
  URI:         https://sr.foobar.net/sr/serv_req_00001000

  state:       ERROR
  Message:     Performance Manager Error
  Detail:      n/a
```

第 4 章

機能ディレクトリの設定

機能ディレクトリ（CD）は、各データセンターで利用できるサービスを追跡し、各要求の要件を満足するうえで十分な能力を持つ利用可能なデータセンターのリストを SRE に提供します。

- 機能ディレクトリの設定，11 ページ

機能ディレクトリの設定

SRE をインストールした DC-Faicng PE に対して機能ディレクトリ（CD）を設定します。

手順の概要

1. **cd xmpp username** *user* **password** *pass*
2. **xmpp server type cd host** *hostname*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**cd xmpp username** *user* **password** *pass* 例： `switch(config)# cd xmpp username user-xyz password pass`	CD のユーザ名とパスワードを設定します。
ステップ 2	**xmpp server type cd host** *hostname* 例： `switch(config)# xmpp server type cd host ccnsr.com`	CD のプロセスに対して XMPP サーバに接続する方法を指定します。

機能ディレクトリの設定

次の作業

PFM を設定します。

第 5 章

サービスを選択するためのパフォーマンス メトリックの設定

パフォーマンス マネージャ（PFM）はプラットフォームに依存しないサブコンポーネントであり、サービスの起点と候補とする各データセンターの間で得られたパフォーマンス データ（遅延、ジッター、および到達可能性）を提供します。

- パフォーマンス マネージャの前提条件，13 ページ
- パフォーマンス マネージャの制限事項，13 ページ
- パフォーマンス マネージャに関する情報，14 ページ
- パフォーマンス マネージャの設定方法，17 ページ

パフォーマンス マネージャの前提条件

PFM を正しく実装して使用できるようにするには、次の条件が必要です。

- 目的の PE デバイスで eXtensible Messaging and Presence Protocol（XMPP）がサポートされていること。
- Web Services Management Agent（WSMA）からパフォーマンス ルーティング（PfR）情報にアクセスできること。 Cisco CRS ルータでは PfR をサポートしていないので、CE 上またはマスター コントローラ（MC）として機能している Cisco ASR 1000 ルータ上で、該当の Cisco CSR ルータに隣接して PfR が動作するように設定する必要があります。

パフォーマンス マネージャの制限事項

パフォーマンス マネージャ（PFM）は、NPS 配置でプレフィックス マップおよびアクティブ プローブを使用して設定する必要があります。 このようなアクティブ プローブはジッター プローブとエコー プローブに制限されています。 エコー プローブの場合、PFM は損失統計情報を受け

取りません。 ジッター プローブの場合、DCE PE を IP SLA レスポンダとして設定する必要があります。

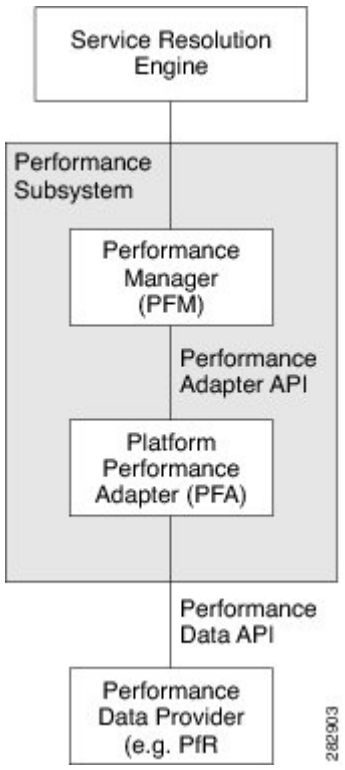
パフォーマンス マネージャに関する情報

パフォーマンス サブシステム（PFS）は Network Positioning System（NPS）のコンポーネントであり、データセンターのパフォーマンス データを評価して、サービス解決エンジン（SRE）にデータセンターのランキングを提示します。 PFS では次のようなパフォーマンス データを評価します。

- 遅延：一定期間内のエンドツーエンドのパケット遅延
- 損失：宛先へのパケット損失に関する統計情報
- 到達可能性：到達不能な宛先に送信されたパケットに関する統計情報

PFS ではパフォーマンス ルーティング（PfR）を使用してこのデータを取得します。 PFS は、SRE から受信した要求を解析し、その要求を満たすデータを PfR から導き出します。

図 *1*：パフォーマンス サブシステム



PFS には次の 2 つの主要コンポーネントがあります。

- パフォーマンス マネージャ（PFM）：プラットフォームに依存しないサブコンポーネントであり、サービスの起点と候補とする各データセンターの間で得られたパフォーマンス データ

（遅延、ジッター、および到達可能性）を提供します。 PFM は CE-Facing PE ルータと DCE-Facing PE ルータの両方で動作します。

- パフォーマンス アダプタ（PFA）：パフォーマンス データ プロバイダー（PDP）から PFM のパフォーマンスデータを取得するプラットフォーム依存サービス。PDP は、パフォーマンス サブシステムの外部に存在するプラットフォーム依存のアダプタです。 PFA および PDP は CE-Facing PE ルータでのみ動作します。

eXtensible Messaging and Presence Protocol クライアントの登録

さまざまな PE デバイス上に存在する各 PFM ピアは、eXtensible Messaging and Presence Protocol（XMPP）を使用して相互に通信します。 XMPP は要求応答メカニズムを使用します。 したがって、ピアどうしの接続を確立するには、それらのピアを XMPP サーバで認識できることが必要です（つまり、各ピアに Jabber ID（JID）が必要です）。

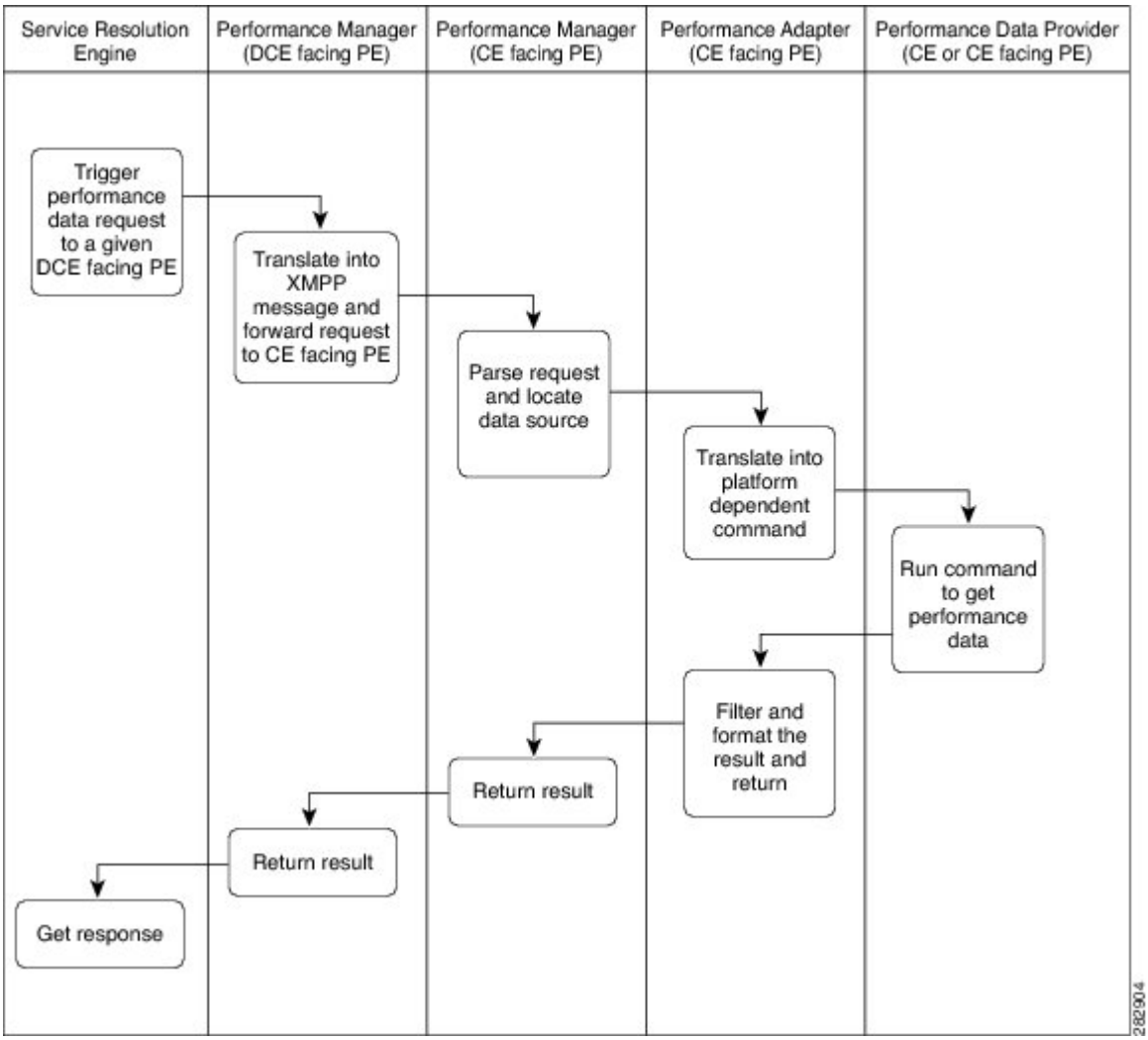
ピアの通知では次の情報を指定します。

- ホスト名：PE デバイスのホスト名または IP アドレス。
- PFMID：PFM エンティティの ID。
- PE のタイプ：CE デバイスまたは DCE デバイス。 ローカル CE テーブルで設定したデバイスは、PE デバイスに対向する CE デバイスであることが必要です。
- Jabber ID：XMPP クライアントの ID。

パフォーマンス マネージャのメッセージ処理

SRE は、Cisco NPS のメッセージ フローを開始します。 このメッセージ フローは、パフォーマンス サブシステム（PFM と PFA）および PDP によって順番に処理されます。

図 *2*：*PFM* メッセージ フロー



PFM プロセスは、10 秒ごとに PFA からパフォーマンス データを取得してキャッシュに保存します。 各 PFM エンティティは、キャッシュにあるテーブルを最新のデータ ソースとして共有します。

パフォーマンス マネージャの設定方法

DC-Facing PE でのパフォーマンス マネージャの設定

DC-Faicng PE 上のパフォーマンス サブシステム（PFS）では PFM のみを実行します。 これは、受信したすべての要求を CE-Facing PE に送信し、そこで処理できるようにします。 DC-Faicng PE 上の PFM は、次の処理を実行します。

- SRE から要求を受信する。
- 対応する CE-Facing PE を特定し、その PE から eXtensible Messaging and Presence Protocol（XMPP）を使用してパフォーマンス データを受け取る。
- 最終的なパフォーマンス データを SRE に送信する。

すべての DC-Faicng PE に対して PFM を設定します。

手順の概要

1. **xmpp server type pfm** *hostname*
2. **pfm local-host** *ip-address*
3. **pfm dce-facing**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**xmpp server type pfm** *hostname* 例： `xmpp server type pfm ccnsr.com`	PFM に XMPP サーバの名前を指定します。
ステップ 2	**pfm local-host** *ip-address* 例： `(config)# pfm local-host 10.4.1.1`	いずれかの DC に到達するための IP アドレスを任意に指定します。この値を使用して、XMPP 通信で使用する Jabber ID が生成されます。
ステップ 3	**pfm dce-facing** 例： `(config)# pfm dce-facing`	DCE-Facing PE で実行するパフォーマンス マネージャをイネーブルにします。

次の作業

すべての CE-Facing PE を設定します。

CE-Facing PE でのパフォーマンス マネージャの設定

CE-Facing PE 上のパフォーマンス サブシステム（PFS）は、パフォーマンス マネージャ（PFM）とパフォーマンス アダプタの両方を実行します。 これは次の処理を実行します。

- eXtensible Messaging and Presence Protocol（XMPP）を使用してリモートの PFM から要求を受信する。
- PFA API を使用して、CE デバイスが PDP からパフォーマンス データを取得できるようにする。
- PFA を使用して、CE デバイスのデータをフィルタリングおよびフォーマットする。

すべての CE-Faicng PE で PFM を設定します。

（注） DC-Facing PE 上で CE-Facing PFM を設定することもできます。 このシナリオでは、すべての DC-Faicng PE ルータで CE-Facing PE と DC-Faicng PE の両方を設定します。 したがって、どの CE-Facing PE ルータでも PFM は設定されません。

手順の概要

1. **xmpp server type pfm** *hostname*
2. **pfm local-host** *ip-address*
3. **ce-table** *name*
4. **ce-address ipv4** *ip-address* **pfr-mc**
5. **exit**
6. **pfm ce-facing**
7. **entity** *number*
8. **ce-table** *name*
9. **pfr-mc** {**enable** | **disable**}
10. **wsma agent**
11. **host** *ip-address* **username** *user* **password** *pass*
12. **do show pfm** *entity-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	**xmpp server type pfm** *hostname* 例： `switch(config)# xmpp server type pfm ccnsr.com`	PFM に XMPP サーバの名前を指定します。

	コマンドまたはアクション	目的
ステップ 2	**pfm local-host** *ip-address* 例： `switch(config)# pfm local-host 10.1.0.2`	外部からこの PFM に到達するために使用する IP アドレスを指定します。 この PE が MC 対応である場合、この IP アドレスは、この PE 上の WSMA サーバの有効な IP アドレスであることが必要です。 この PE が MC 対応でない場合は、DCE-Facing PE が XMPP を通じてこの PE と通信できるように、SRE の要求で指定されている PE アドレスと同じローカル ホストを指定する必要があります。
ステップ 3	**ce-table** *name* 例： `switch(config)# ce-table cet1`	PE 上に新しいローカル CE テーブルを作成し、CE テーブル コンフィギュレーション モードを開始します。 パフォーマンス ルーティング（PfR）マスターコントローラ（MC）対応ルータごとに CE テーブルを 1 つ設定する必要があります。 • *name*：CE テーブルの名前。 最大で 32 文字を使用できます。
ステップ 4	**ce-address ipv4** *ip-address* **pfr-mc** 例： `switch(config-ce-table)# ce-address ipv4 10.2.1.1 pfr-mc`	接続されている CE デバイスの IP アドレスを設定します。 1 つの CE テーブルには最大で 10 個の CE アドレスを入力できます。 • **pfr-mc**：接続された CE が PfR MC 対応であることを指定します。
ステップ 5	**exit** 例： `switch(config-ce-table)# exit (config)#`	CE テーブル コンフィギュレーション モードを終了します。
ステップ 6	**pfm ce-facing** 例： `switch(config)# pfm ce-facing (config-pfm-pece)#`	CE-Facing PE で実行するパフォーマンス マネージャをイネーブルにし、PFM コンフィギュレーション モードを開始します。
ステップ 7	**entity** *number* 例： `switch(config-pfm-pece)# entity 1 (config-pfm-pece-entity)#`	PFM エンティティを開始し、PFM エンティティ コンフィギュレーション モードを開始します。 1 つの PFM では最大で 10 個のエンティティを同時に実行できます。 • *number*：一意のエンティティ ID を生成するために使用するエンティティ番号。1 ～ 10 の範囲で指定します。 PFM エンティティ ID は、名前+ホスト名+エンティティ番号の形式で記述します。 たとえば、pfm-10.74.1.12-1 とします。
ステップ 8	**ce-table** *name* 例： `switch(config-pfm-pece-entity)# ce-table cet123`	ローカル CE テーブルとエンティティをバインドします。 • *name*：このエンティティとバインドする CE テーブルの名前。 ここで指定する CE テーブルを事前に設定しておく必要があります。

	コマンドまたはアクション	目的
ステップ 9	**pfr-mc** {**enable** | **disable**} 例： `switch(config-pfm-pece-entity)# pfr-mc enable`	エンティティが PfR MC 対応であるかどうかを指定します。
ステップ 10	**wsma agent** 例： `switch(config)# wsma agent`	Web Services Management Agent（WSMA）エージェントを設定する WSMA コンフィギュレーション モードを開始します。 PFA が MC からパフォーマンス データを取得できるようにするには、WSMA の設定が必要です。 この CE-Facing PE または任意の CE に MC を配置できます。
ステップ 11	**host** *ip-address* **username** *user* **password** *pass* 例： `switch(config-wsma)# host 10.1.0.2 username xyz password pass`	PFR とマスター コントローラをホストする CE ルータとの WSMA 接続で使用する IP アドレスを設定します。
ステップ 12	**do show pfm** *entity-number* 例： `switch# show pfm`	設定されたパフォーマンス管理情報を表示します。 • *entity-number*：特定のエンティティの情報を表示します。 これを指定しない場合は、設定されているすべてのエンティティの情報が表示されます。

CE-Facing PE での PFM の設定：例

この例で設定した CE-Facing PE には、PfR MC 非対応の CE が 1 つと PfR MC 対応の CE が 2 つあります。

```
pfm ce-facing
  entity 1
    ce-table table1
  entity 2
    pfr-mc disable
    ce-table table2
  entity 3
    pfr-mc disable
    ce-table table10
pfm local-host 10.1.1.2
ce-table table1
  ce-address ipv4 10.1.1.1
  ce-address ipv4 20.1.12.1
  ce-address ipv4 20.1.13.1
  ce-address ipv4 20.1.10.2
ce-table table2
  ce-address ipv4 50.1.1.1 pfr-mc
  ce-address ipv4 50.1.2.1
ce-table table10
  ce-address ipv4 60.1.1.1 pfr-mc
  ce-address ipv4 60.1.2.1
```

```
  ce-address ipv4 60.1.3.1
```

show pfm：例

次に、**show pfm** コマンドの出力例を示します。

```
switch# show pfm

Entity-ID  PFM-ID            Active-PDP-Address    CE-Table
  1        PFM-26.0.0.2-1    192.168.1.1            cet123
  5        PFM-26.0.0.2-5    10.74.5.32
```

次の作業

あらゆる DCE-Facing PE を設定します。

第 6 章

ネットワーク プロキシミティに使用するルーティング プロトコルの設定

NPS では、データセンターを選択するプロセスで IS-IS、OSPF、および BGP の各ルーティング プロトコルを使用してネットワーク プロキシミティを計算します。 このモジュールの説明に従って、これらのプロトコルが目的のルータで稼働している必要があります。

- ネットワーク ルーティング プロキシミティに関する情報，23 ページ
- ルーティング プロトコルの設定方法，25 ページ

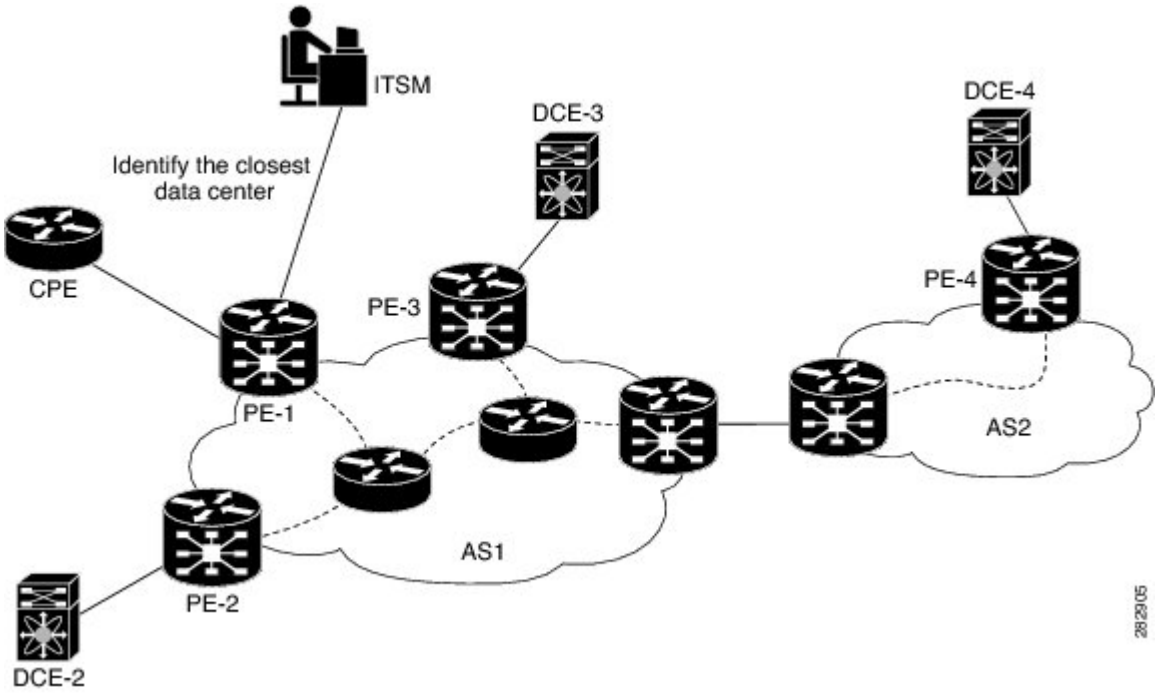
ネットワークルーティングプロキシミティに関する情報

Cisco NPS のプロキシミティ エンジン（PXE）では、ネットワーク ルーティング プロキシミティを使用し、クライアントからデータセンターまでのトポロジ距離とパス距離に基づいてデータセンターを選択します。 PXE は IGP（IS-IS、OSPF）と EGP（BGP）の両方からトポロジとパス情報を収集します。 次に、固定ソース（プロキシミティ ソース アドレス（PSA））からのトポロジ距離の順に、リスト（プロキシミティ ターゲット リスト（PTL））の中で宛先をランク付けします。 サービス解決エンジン（SRE）から、クライアント アドレス（PSA）とデータセンター候補リスト（PTL）が PXE に送信されます。 PXE は、そのリストをネットワーク プロキシミティによってランク付けして SRE に返します。 PXE は、PSA とプロキシミティ ターゲット アドレス（PTA）とのトポロジ距離を常時計算しています。PTA は、PTL に存在する単一の要素です。

次の図に、基本的なプロキシミティ機能を示します。 2 つの自律システム（AS）を持つこのネットワークには、それぞれ DCE-2、DCE-3、および DCE-4 でホストされている 3 つのデータセンターがあります。 PTL にはこれらの DCE が記述されます。 PE-1 の背後でホストされている CPE がサービス解決に要求を送信します。 サービス解決は、AS1 にあるどのプロバイダーエッジルータ（PE）上でも動作できます。 PE-1 は PSA を形成します。 PXE は IGP プロキシミティ アルゴ

リズムを実行し、DCE-2 を「最も近いデータセンター」として選択したうえで、ランキング リスト DCE-2、DCE-3、DCE-4 を返します。

図 *3*：ネットワーク プロキシミティによるデータセンターの選択



PXE のデータ要素

PXE の動作は、以下のデータ要素によって決まります。

- PSA：プロキシミティ ソース アドレス。 対象とするひと揃いのデータセンターの場所を得るためにプロキシミティの計算を要求しているエンドユーザまたはクライアントの送信元IP アドレスです。
- PTA：プロキシミティ ターゲット アドレス。 所定のデータ センタの場所を示す IP アドレスです。 所定の PSA と PAT のペアについてプロキシミティが計算されます。
- PTL：プロキシミティ ターゲット リスト。 PTA の集合です（ランク付けがある場合とない場合があります）。

PSA または PTA の従来の値は IP アドレスとマスクの組み合わせです。 Cisco NPS では、PXE で IP アドレスを扱うことを想定しているので、IP アドレスではない形式の識別情報はすべて、PXE の外部で IP アドレスとマスクの組み合わせに変換する必要があります。

PXE のピアリングおよびランキング

PXE は、ネットワーク上の他のルータとパッシブにピアリングします。つまり、PXE はルートのみを学習します。 PXE から何らかのルートがネットワークに追加されることはありません。 PXE は、適切な IGP/EGP コントロール プレーンの動作に全面的に参加します。 ただし、PXE は学習したルートをプロキシミティの計算にのみ使用し、メイン ルータ コントロール プレーンの Routing Information Base（RIB）には干渉しません。 この目的で、PXE は RIB のコピーを別途保持しています。

IGP のプロキシミティ

Cisco NPS は、IGP プロトコルとして OSPF と IS-IS をサポートしています。 そのアルゴリズムは、逆方向の Shortest Path First（SPF）の計算に依存しているので、たとえばリンク コストは PTA から PSA の方向に評価されます。

EGP のプロキシミティ

BGP は、事実上の EGP 標準であり、BGP のプロキシミティの基本アルゴリズムは AS PATH 属性に依存しています。 この計算は、IGP の場合に非常によく似ていますが、リンク コストの代わりにパス コストを使用する点が異なります。 Cisco NPS では、AS 間のトポロジでプロキシミティを計算できません。

プロキシミティ ソース アドレスのルート オリジン

PXE は、正しいプロキシミティ アルゴリズムを適用するために、PSA の学習で使用したものと同じルーティング プロトコルを選択します。 たとえば、PXE が OSPF を使用して PSA を学習している場合、プロキシミティの計算は IGP のプロキシミティに依存し、BGP から学習した PTA は自動的に低位にランクされます。 同じ OSPF エリアにある PTA が別の AS では PTA よりも優先するので、この手法は良好に機能します。 IGP のプロキシミティおよび BGP のプロキシミティは最も頻繁に適用されます。

ルーティング プロトコルの設定方法

プロキシミティの計算に向けた OSPF の設定

次のタスクで、プロキシミティ エンジンで実行するプロキシミティの計算に使用する Open Shortest Path First（OSPF）ルーティング プロセスを設定します。

はじめる前に

OSPF プロキシミティの計算機能を使用する場合は、使用しているルータの integrated-service インターフェイスに対し、インターフェイス コンフィギュレーション モードで **ip ospf priority** コマン

ドを設定することを推奨します。 このコマンドは、指定ルータ（DR）/バックアップ DR の選択を判断する上で効果的です。

```
Router# config
Router(config)# interface interface-service 0
Router(config-if)# ip ospf priority 1
```

手順の概要

1. **router ospf** *process-id*
2. **network** *ip-address wildcard-mask* **area** *area-id*
3. **area** *area-id* {**stub** | **nssa**}
4. **area** *area-id* **authentication** {**message-digest** | **cleartext**}
5. **log-adjacency-changes**
6. **router-id** *ip-address*
7. **interface eth0 priority** *priority*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**router ospf** *process-id* 例： `switch(config)# router ospf 123`	OSPF ルーティング プロセスを設定し、ルーティング コンフィギュレーション モードを開始します。 • *process-id*：OSPF ルーティング プロセスにローカルで割り当てて内部使用する識別情報。 任意の正の整数が使用できます。
ステップ 2	**network** *ip-address wildcard-mask* **area** *area-id* 例： `switch(config-router)# network 26.0.0.0 255.0.0.0 area 1`	OSPF を実行するインターフェイスと、そのインターフェイスのエリア識別情報を定義します。 • *ip-address*：OSPF に関連付けるエリアの IP アドレス。 • *wildcard-mask*：IP アドレスの範囲を定義するために IP アドレスに適用するワイルドカード マスク。 • *area-id*：OSPF アドレス範囲に関連付けるエリア。
ステップ 3	**area** *area-id* {**stub**	**nssa**} 例： `switch(config-router)# area 1 stub`	スタブ エリアまたは Not-So-Stubby Area として OSPF エリアを設定します。
ステップ 4	**area** *area-id* **authentication** {**message-digest**	**cleartext**} 例： `switch(config-router)# area 0 authentication message-digest`	OSPF エリアの認証をイネーブルにします。 • *area-id*：認証をイネーブルにするエリアの識別情報。 10 進数値で指定する必要があります。

	コマンドまたはアクション	目的
		• **message-digest**：指定のエリアに対して Message Digest 5（MD5）認証をイネーブルにします。 • **cleartext**：指定のエリアに対してクリア テキスト認証をイネーブルにします。
ステップ 5	**log-adjacency-changes** 例： `switch(config-router)# log-adjacency-changes`	OSPF ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。
ステップ 6	**router-id** *ip-address* 例： `switch(config-router)# router-id 26.0.0.2`	固定ルータ ID を使用することを指定します。 • *ip-address*：IP アドレス形式で記述したルータ ID。
ステップ 7	**interface eth0 priority** *priority* 例： `switch(config-router)# interface eth0 priority 2`	OSPF のプライオリティを指定します。 0 ～ 255 の範囲で値を指定できます。 デフォルトは 1 です。

プロキシミティの計算に向けた BGP の設定

次のタスクで、プロキシミティ エンジンでプロキシミティを計算できるようにボーダー ゲートウェイ プロトコル（BGP）のルーティング プロセスを設定します。

手順の概要

1. **router bgp** *as-no*
2. **location-community** *community-string* **weight** *weight*
3. **log-neighbor-changes**
4. **neighbor** *ip-address* **timers** *keepalives holdtime*
5. **neighbor** *ip-address* **ebgp-multihop**
6. **neighbor** *ip-address* **remote-as** *as-no*
7. **neighbor** *ip-address* **password** *string*
8. **ip urib bgp bestpath**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**router bgp** *as-no* 例： `switch(config)# router bgp 3`	BGP ルーティング プロセスを設定し、ルーティング コンフィギュレーション モードを開始します。 • *as-nc*：他の BGP ルータに対するルータを指定し、同時に渡されるルーティング情報のタギングをする、自律システムの番号。
ステップ 2	**location-community** *community-string* **weight** *weight* 例： `switch(config-router)# location-community 11:222 weight 100`	プロキシミティ エンジンに関連付けたコミュニティ値を設定します。 • *community-string*：プロキシミティ エンジンに関連付けた文字列。 • *weight*：コミュニティに関連付けた重み。
ステップ 3	**log-neighbor-changes** 例： `switch(config-router)# log-neighbor-changes`	BGP ネイバー リセットのロギングをイネーブルにします。
ステップ 4	**neighbor** *ip-address* **timers** *keepalives holdtime* 例： `switch(config-router)# neighbor 26.0.0.1 timers 30 100`	特定の BGP ピアまたは BGP ピア グループのタイマーを設定します。 • *ip-address*：BGP ピアまたは BGP ピア グループの IP アドレス。 • *keepalives*：BGP プロセスからそのピアにキープアライブ メッセージを送信する時間間隔（秒）。 デフォルトは 60 です。 有効な範囲は 0 ～ 65535 です。 • *holdtime*：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであるとプロセスで宣言するまでの時間（秒）。 デフォルト値は 180 です。 有効な範囲は 3 ～ 65535 です。 この保持時間は、キープアライブ メッセージの時間間隔の 2 倍より長くする必要があります。
ステップ 5	**neighbor** *ip-address* **ebgp-multihop** 例： `switch(config-router)# neighbor 26.0.0.1 ebgp-multihop`	直接接続されていないネットワークに存在する外部ピアとの BGP 接続を受け入れ、またその接続を試行するように BGP ルーティング プロセスを設定します。

	コマンドまたはアクション	目的
ステップ 6	**neighbor** *ip-address* **remote-as** *as-no* 例： `switch(config-router)# neighbor 26.0.0.1 remote-as 1`	BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバーテーブルにエントリを追加します。
ステップ 7	**neighbor** *ip-address* **password** *string* 例： `switch(config-router)# neighbor 26.0.0.1 password 123`	2 つの BGP ピア間の TCP 接続上で Message Digest 5（MD5）認証をイネーブルにします。 • *ip-address*：BGP スピーキング ネイバーの IP アドレス。 • *string*：大文字と小文字が区別される、最大 25 文字のパスワード。最初の文字を数値にはできません。この文字列には、スペースも含め、あらゆる英数字を使用できます。数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。
ステップ 8	**ip urib bgp bestpath** 例： `switch(config)# ip urib bgp bestpath`	BGP 自律システム（AS）のパスの長さに基づくプロキシミティを使用するプロキシミティ アルゴリズムをイネーブルにします。

プロキシミティの計算に向けた IS-IS の設定

次のタスクで、プロキシミティ エンジンで実行するプロキシミティの計算に使用する Intermediate System-to-Intermediate System（IS-IS）ルーティング プロセスを設定します。

手順の概要

1. **router isis** *process-name*
2. **net** *network-entity-title*
3. **lsp-mtu** *max-lsp-size*
4. **log-adjacency-changes**
5. **is-type** {**level-1** | **level-2** | **level -1-2**}
6. **authentication-check** {**level-1** | **level-2**}
7. **authentication-type** {**md5** | **text**} {**level-1** | **level-2**}
8. **authentication key-chain** *name-of-chain* {**level-1** | **level-2**}
9. **interface eth0 priority** *priority*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**router isis** *process-name* 例： `switch(config)# router isis 123`	IS-IS ルーティング プロセスを設定し、ルーティング コンフィギュレーション モードを開始します。 • *process-name*：ルーティング プロセスを表す名前。 この名前は、指定ルータでのすべての IP、またはコネクションレス型ネットワーク サービス（CLNS）ルータ プロセス内で一意でなければなりません。
ステップ 2	**net** *network-entity-title* 例： `switch(config-router)# net 26.0.0.0`	CLNS ルーティング プロセスの IS-IS Network Entity Title（NET）を設定します。 • *network-entity-title*：CLNS ルーティング プロセスのエリア アドレスおよびシステム ID。 この引数には、IP アドレスまたは名前を指定できます。
ステップ 3	**lsp-mtu** *max-lsp-size* 例： `switch(config-router)# lsp-mtu 1000`	IS-IS リンク ステート パケット（LSP）の最大伝送単位（MTU）サイズをバイトの単位で設定します。 指定できる値は 0 ～ 2147483647 です。
ステップ 4	**log-adjacency-changes** 例： `switch(config-router)# log-adjacency-changes`	IS-IS ネイバーが起動または停止したときに syslog メッセージを送信するようにルータを設定します。
ステップ 5	**is-type** {**level-1** | **level-2** | **level -1-2**} 例： `(config-router)# is-type level-1-2`	IS-IS ルーティング プロセスのインスタンスのルーティング レベルを設定します。 • **level-1**：レベル 1（エリア内）ルーティングのみの実行を指定します。 このルータが学習するのはそのエリア内の宛先だけです。 レベル 2（エリア間）ルーティングは、最も近いレベル 1 ～ 2 ルータによって実行されます。 • **level-2**：レベル 1 とレベル 2 の両方のルーティングを実行します。 このルータは、ルーティング プロセスのインスタンスを 2 つ実行します。 このルータは、エリア内（レベル 1 ルーティング）の宛先について 1 つのリンクステート パケット データベース（LSDB）を持っており、Shortest Path First（SPF）の計算を実行してエリア トポロジを検出します。 また、他のすべてのバックボーン（レベル 2）ルータの LSP による別の LSDB も備え、別の SPF 計算を実行してバックボーンのトポロジと他のすべてのエリアの存在を検出します。

	コマンドまたはアクション	目的
		• **level-1-2**：ルーティング プロセスはレベル 2（エリア間）ルータとしてのみ機能します。 このルータはバックボーンの一部であり、レベル 1 とは通信せずに、自身のエリアに存在するルータとのみ通信します。
ステップ 6	**authentication-check** {**level-1** | **level-2**} 例： `(config-router)# authentication-check level1`	該当のレベルで受信パケットのチェックをイネーブルにします。 • **level-1**：レベル 1 の LSP、CSNP、および PSNP の認証タイプ。 • **level-2**：レベル 2 の LSP、CSNP、および PSNP の認証タイプ。
ステップ 7	**authentication-type** {**md5** | **text**} {**level-1** | **level-2**} 例： `(config-router)# authentication-type md5 level-2`	IS-IS で使用する認証のタイプを指定します。 • **md5**：Message Digest 5 認証。 • **text**：クリア テキスト認証。 • **level-1**：レベル 1 パケットでのみ、指定の認証をイネーブルにします。 • **level-2**：レベル 2 パケットでのみ、指定の認証をイネーブルにします。
ステップ 8	**authentication key-chain** *name-of-chain* {**level-1** | **level-2**} 例： `(config-router)# authentication key-chain abc level-2`	IS-IS に対して認証をイネーブルにします。 • *name-of-chain*：有効なキーのグループを特定します。 • **level-1**：レベル 1 パケットでのみ認証をイネーブルにします。 • **level-2**：レベル 2 パケットでのみ認証をイネーブルにします。
ステップ 9	**interface eth0 priority** *priority* 例： `switch(config-router)# interface eth0 priority 2`	IS-IS プライオリティを指定します。 0 ～ 255 の範囲で値を指定できます。 デフォルトは 1 です。

第 7 章

NPS の設定例

このモジュールでは、Cisco Network Positioning System の設定例について説明します。

- CE-Facing PE の設定例，33 ページ
- DCE-Facing PE の設定例，34 ページ

CE-Facing PE の設定例

以下の例では、MC 対応のエンティティを 1 つおよび MC 非対応のエンティティを 2 つ定義した CE-Facing PE の設定を示しています。

```
hostname ccnsr1.com
ip host ccnsr.com 172.16.0.2
xmpp server type pfm ccnsr.com
xmpp server type cd ccnsr.com
interface eth0
  ip address 172.17.0.2 255.255.255.0
  no shutdown
router ospf 10
  network 172.17.0.0 0.0.255.255 area 0
pfm ce-facing
  entity 1
    ce-table table1
  entity 2
    pfr-mc disable
    ce-table table2
  entity 3
    pfr-mc disable
    ce-table table10
pfm local-host 10.1.0.2
ce-table table1
  ce-address ipv4 10.1.0.1
  ce-address ipv4 10.1.1.1
  ce-address ipv4 10.1.2.1
  ce-address ipv4 10.5.1.1
  ce-address ipv4 10.5.2.1
ce-table table2
  ce-address ipv4 10.2.1.1 pfr-mc
  ce-address ipv4 10.2.2.1
ce-table table10
  ce-address ipv4 10.3.1.1 pfr-mc
  ce-address ipv4 10.3.2.1
  ce-address ipv4 10.3.3.1
```

```
wsma agent
  host 10.1.0.2 username cisco password cisco
  host 10.2.1.1 username cisco password cisco
  host 10.3.1.1 username cisco password cisco
  host 10.5.1.2 username cisco password cisco
  reconnect-time 60
ip route 0.0.0.0 0.0.0.0 27.0.0.1


hostname ccnsr1.com
ip host ccnsr.com 172.16.0.2
xmpp server type pfm ccnsr.com
xmpp server type cd ccnsr.com
router ospf 10
  network 172.17.0.0 0.0.255.255 area 0
pfm ce-facing
  entity 1
    ce-table table1
  entity 2
    pfr-mc disable
    ce-table table2
  entity 3
    pfr-mc disable
    ce-table table10
pfm local-host 10.1.0.2
ce-table table1
  ce-address ipv4 10.1.0.1
  ce-address ipv4 10.1.1.1
  ce-address ipv4 10.1.2.1
  ce-address ipv4 10.5.1.1
  ce-address ipv4 10.5.2.1
ce-table table2
  ce-address ipv4 10.2.1.1 pfr-mc
  ce-address ipv4 10.2.2.1
ce-table table10
  ce-address ipv4 10.3.1.1 pfr-mc
  ce-address ipv4 10.3.2.1
  ce-address ipv4 10.3.3.1
wsma agent
  host 10.1.0.2 username cisco password cisco
  host 10.2.1.1 username cisco password cisco
  host 10.3.1.1 username cisco password cisco
  host 10.5.1.2 username cisco password cisco
  reconnect-time 60
```

DCE-Facing PE の設定例

以下の例では、サービス解決アプリケーションと Jabber サーバも実行している DCE-Facing PE の設定を示しています。

```
hostname ccnsr.com
ip host ccnsr.com 172.16.0.2
xmpp server type pfm ccnsr.com
xmpp server type cd ccnsr.com
interface eth0
  ip address 172.16.0.2 255.255.255.0
  no shutdown

router ospf 10
  network 172.16.0.0 0.0.255.255 area 0
pfm local-host 10.4.1.1
pfm dce-facing
ip route 0.0.0.0 0.0.0.0 172.16.0.1

jabber server
  domain ccnsr.com
  ipaddr ipv4 172.16.0.2
```

```
cd xmpp username test password test

service-resolution dc dc1 pe-addr 10.4.0.1
service-resolution dc dc2 pe-addr 10.4.1.1
service-resolution dc dc3 pe-addr 10.4.2.1
service-resolution dc dc4 pe-addr 10.4.3.1
service-resolution dc dc5 pe-addr 10.4.4.1
service-resolution dc dc6 pe-addr 10.4.5.1

service-resolution service-request timeout 3600


hostname ccnsr.com
ip host ccnsr.com 172.16.0.2
xmpp server type pfm ccnsr.com
xmpp server type cd ccnsr.com
router ospf 10
  network 172.16.0.0 0.0.255.255 area 0

pfm local-host 10.4.1.1
pfm dce-facing
ip route 0.0.0.0 0.0.0.0 172.16.0.1

cd xmpp username test password test
service-resolution dc dc1 pe-addr 10.4.0.1
service-resolution dc dc2 pe-addr 10.4.1.1
service-resolution dc dc3 pe-addr 10.4.2.1
service-resolution dc dc4 pe-addr 10.4.3.1
service-resolution dc dc5 pe-addr 10.4.4.1
service-resolution dc dc6 pe-addr 10.4.5.1

service-resolution service-request timeout 3600
```