IP ルーティング：OSPF 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

『Configuring OSPF』 3

機能情報の確認 3

OSPF に関する情報 4

シスコの OSPF 実装 4

OSPF のルータの調整 4

OSPF のルート配布 5

OSPF ネットワーク タイプ 5

エリア パラメータ 7

以前の LSA の動作 10

複数のタイマーを使用する LSA グループ ペーシング 11

OSPF の設定方法 13

OSPF のイネーブル化 14

OSPF インターフェイス パラメータの設定 15

さまざまな物理ネットワークでの OSPF の設定 17

ポイントツーマルチポイント ブロードキャスト ネットワーク用 OSPF の設定 17

非ブロードキャスト ネットワークの OSPF の設定 18

OSPF エリア パラメータの設定 20

OSPFv2 NSSA の設定 21

OSPFv2 NSSA エリアとそのパラメータの設定 21

強制 NSSA LSA トランスレータとしての NSSA ABR の設定 23

RFC 3101 互換性のディセーブル化と RFC 1587 互換性のイネーブル化 24

OSPF NSSA パラメータの設定 25

前提条件 25

OSPF エリア間のルート集約の設定 26

OSPF にルートを再配布する場合のルート集約の設定 26

仮想リンクの確立 26

デフォルト ルートの生成 27
DNS 名ルックアップの設定 28
ループバック インターフェイスによる強制的ルータ ID 選択 29
デフォルト メトリックの制御 29
OSPF アドミニストレーティブ ディスタンスの変更 30
シンプレックス イーサネット インターフェイスでの OSPF の設定 31
ルート計算タイマーの設定 32
OSPF over On-Demand 回路の設定 33
前提条件 33
ネイバーの起動と停止のロギング 34
LSA グループ ペーシング インターバルの変更 35
OSPF LSA フラッディングのブロック 36
LSA フラッディングの低減 36
MOSPF LSA パケットの無視 37
OSPF のモニタリングおよびメンテナンス 38
OSPF アップデート パケットのペーシングの表示 40
OSPF の制約事項 41
OSPF の設定例 41
例：OSPF ポイントツーマルチポイント 41
例：ブロードキャストを行う OSPF ポイントツーマルチポイント 43
例：非ブロードキャストの OSPF ポイントツーマルチポイント 44
例：可変長サブネット マスク 44
例：OSPF NSSA の設定 45
例：RFC 3101 がディセーブル、RFC 1587 がアクティブな OSPF NSSA 47
例：OSPF ルーティングおよびルート再配布 49
例：OSPF の基本設定 49
例：内部ルータ、ABR、および ASBR の OSPF の基本設定 49
例：複雑な内部ルータ、ABR、および ASBR 51
例：ABR の複雑な OSPF 設定 53
例：ルート マップ 55
例：OSPF アドミニストレーティブ ディスタンスの変更 57
例：OSPF over On-Demand ルーティング 58

例：LSA グループ ペーシング 59
例：OSPF LSA フラッディングのブロック 59
例：MOSPF LSA パケットの無視 59
OSPF Not-So-Stubby Areas（NSSA）に関する追加情報 59
OSPF 設定の機能情報 60
IPv6 ルーティング：OSPFv3 63
機能情報の確認 63
IPv6 ルーティング：OSPFv3 の前提条件 64
IPv6 ルーティング：OSPFv3 の制約事項 64
IPv6 ルーティングについて：OSPFv3 64
OSPFv3 の機能 64
OSPFv3 と OSPF バージョン 2 の比較 65
OSPFv3 の LSA タイプ 65
OSPFv3 でのロード バランシング 67
OSPFv3 にインポートされるアドレス 67
OSPFv3 のカスタマイゼーション 67
OSPFv3 の強制的な SPF 68
OSPFv3 でのロード バランシングの設定方法 68
OSPFv3 デバイス プロセスの設定 68
SPF 計算の強制実行 70
OSPFv3 の設定と動作の確認 71
OSPFv3 でのロード バランシングの設定例 74
例：OSPFv3 デバイス プロセスの設定 74
例：SPF 設定の強制実行 75
その他の参考資料 75
IPv6 ルーティング：OSPFv3 の機能情報 77
IPv6 ルーティング：IPsec を使用した OSPFv3 認証サポート 79
機能情報の確認 79
IPv6 ルーティング：IPsec を使用した OSPFv3 認証の前提条件 80
IPv6 ルーティングについて：IPsec を使用した OSPFv3 認証サポート 80
IPsec を使用した OSPFv3 認証サポート 80
IPv6 ルーティングの設定方法：IPsec を使用した OSPFv3 認証サポート 81

OSPFv3 での IPsec の設定 81
Defining Authentication on an Interface 82
OSPFv3 エリア内の認証の定義 83
IPv6 ルーティングの設定例：IPsec を使用した OSPFv3 認証サポート 84
例：インターフェイスでの認証の定義 84
例：OSPFv3 エリア内の認証の定義 84
IPv6 ルーティング：IPsec を使用した OSPFv3 認証サポートに関する追加情報 85
IPv6 ルーティング：IPsec を使用した OSPFv3 認証サポートの機能情報 86
OSPFv2 暗号化認証 87
機能情報の確認 87
OSPFv2 暗号化認証の前提条件 88
OSPFv2 暗号化認証について 88
OSPFv2 暗号化認証の設定 88
OSPFv2 暗号化認証の設定方法 89
キー チェーンの定義 89
Defining Authentication on an Interface 90
OSPFv2 暗号化認証の設定例 91
例：キー チェーンの定義 91
例：キー チェーンの確認 92
例：インターフェイスでの認証の定義 92
例：インターフェイスでの認証の確認 92
OSPFv2 暗号化認証に関する追加情報 94
OSPFv2 暗号化認証の機能情報 95
OSPFv3 外部パス プリファレンス オプション 97
機能情報の確認 97
OSPFv3 外部パス プリファレンス オプションについて 98
OSPFv3 外部パス プリファレンス オプション 98
OSPFv3 外部パス プリファレンス オプションの計算方法 98
RFC 5340 に従った OSPFv3 外部パス プリファレンスの計算 98
OSPFv3 外部パス プリファレンス オプションの設定例 99
例：RFC 5340 に従った OSPFv3 外部パス プリファレンスの計算 99
その他の参考資料 100
OSPFv3 外部パス プリファレンス オプションの機能情報 101

『OSPFv3 Graceful Restart』 103
機能情報の確認 103
OSPFv3 グレースフル リスタートに関する情報 104
『OSPFv3 Graceful Restart』 104
OSPFv3 グレースフル リスタートをイネーブルにする方法 104
グレースフル リスタート対応ルータでの OSPFv3 グレースフル リスタートのイネーブル化 104
グレースフル リスタート対応ルータでの OSPFv3 グレースフル リスタートのイネーブル化 105
グレースフル リスタート認識ルータでの OSPFv3 グレースフル リスタートのイネーブル化 106
グレースフル リスタート認識ルータでの OSPFv3 グレースフル リスタートのイネーブル化 107
OSPFv3 グレースフル リスタートの設定例 108
例：OSPFv3 グレースフル リスタートのイネーブル化 108
その他の参考資料 109
OSPFv3 グレースフル リスタートの機能情報 110
OSPFv3 のグレースフル シャットダウンのサポート 113
機能情報の確認 113
OSPFv3 グレースフル シャットダウン サポートについて 114
OSPFv3 グレースフル シャットダウン 114
OSPFv3 グレースフル シャットダウン サポートの設定方法 114
OSPFv3 プロセスのグレースフル シャットダウンの設定 114
アドレス ファミリ コンフィギュレーション モードでの OSPFv3 プロセス のグレースフル シャットダウンの設定 116
OSPFv3 インターフェイスの OSPFv3 グレースフル シャットダウンの設定 117
OSPFv3 グレースフル シャットダウン サポートの設定例 119
例：OSPFv3 プロセスのグレースフル シャットダウンの設定 119
例：OSPFv3 インターフェイスのグレースフル シャットダウンの設定 119
OSPFv3 グレースフル シャットダウン サポートに関する追加情報 120
OSPFv3 グレースフル シャットダウン サポートの機能情報 120
『OSPF Stub Router Advertisement』 123

機能情報の確認 123
OSPF スタブ ルータ アドバタイズメントに関する情報 124
OSPF スタブ ルータ アドバタイズメント機能 124
最大メトリックを使用したルーティング テーブルのコンバージ 124
最大メトリックを使用したルータのグレースフル シャットダウン 125
OSPF スタブ ルータ アドバタイズメントの利点 125
OSPF スタブ ルータ アドバタイズメントの設定方法 126
起動時アドバタイズメントの設定 126
ルーティング テーブル コンバージ中のアドバタイズメントの設定 126
グレースフル シャットダウンのためのアドバタイズメントの設定 127
最大メトリックのアドバタイズメントの確認 128
OSPF スタブ ルータ アドバタイズメントのモニタリングおよびメンテナンス 130
OSPF スタブ ルータ アドバタイズメントの設定例 130
例：起動時アドバタイズメント 130
例：ルーティング テーブルのコンバージまでのアドバタイズメント 130
例：グレースフル シャットダウン 131
その他の参考資料 131
OSPF スタブ ルータ アドバタイズメントの機能情報 132
OSPF アップデート パケット ペーシング タイマー設定 135
機能情報の確認 135
OSPF アップデート パケット ペーシング タイマー設定の制約事項 136
OSPF アップデート パケットペーシング タイマー設定について 136
OSPF アップデート パケットペーシング タイマーの機能 136
OSPF アップデート パケットペーシング タイマー設定の利点 137
OSPF パケットペーシング タイマーの設定方法 137
OSPF パケット ペーシング タイマーの設定 137
再送信パケット ペーシング タイマーの設定 138
グループ パケット ペーシング タイマーの設定 138
OSPF パケット ペーシング タイマーの確認 139
トラブルシューティングのヒント 139
OSPF パケットペーシング タイマーのモニタリングおよびメンテナンス 140
OSPF アップデート パケット ペーシングの設定例 140

例：LSA フラッド ペーシング 140
例：LSA 再送信ペーシング 140
例：LSA グループ ペーシング 140
その他の参考資料 141
OSPF アップデート パケット ペーシング タイマー設定の機能情報 142
MPLS VPN のための OSPF 模造リンクのサポート 145
機能情報の確認 145
MPLS VPN のための OSPF 模造リンクのサポートの前提条件 146
MPLS VPN のための OSPF 模造リンクのサポートの制約事項 146
MPLS VPN のための OSPF 模造リンクのサポートについて 146
MPLS VPN のための OSPF 模造リンクのサポートの利点 146
PE-CE 間ルータ接続での OSPF の使用 147
模造リンクを使用した OSPF バックドア ルーティングの修正方法 148
OSPF 模造リンクの設定方法 150
模造リンクの作成 150
作成した模造リンクの確認 153
模造リンクのモニタリングと維持 153
OSPF 模造リンクの設定例 153
例：模造リンクの設定 153
例：2 つの PE ルータ間の模造リンク 155
その他の参考資料 156
MPLS VPN の OSPF 模造リンク サポートの機能情報 157
用語集 158
CE ルータでの OSPF マルチ VRF サポート 161
機能情報の確認 161
CE ルータでの OSPF マルチ VRF サポートについて 162
CE ルータでの OSPF マルチ VRF サポートの設定方法 162
OSPF ルーティングのためのマルチ VRF 機能の設定 162
OSPF マルチ VRF 設定の確認 164
CE ルータでの OSPF マルチ VRF サポートの設定例 165
例：マルチ VRF 機能の設定 165
その他の参考資料 166

CE ルータでの OSPF マルチ VRF サポートの機能情報 167
用語集 168
OSPFv2 マルチエリア隣接関係 171
機能情報の確認 171
OSPFv2 マルチエリア隣接関係の前提条件 172
OSPFv2 マルチエリア隣接関係の制約事項 172
OSPFv2 マルチエリア隣接関係について 172
OSPFv2 マルチエリア隣接関係の概要 172
OSPFv2 マルチエリア隣接関係の設定方法 173
OSPFv2 マルチエリア隣接関係の設定 173
OSPFv2 マルチエリア隣接関係の設定例 175
例：OSPFv2 マルチエリア隣接関係の設定 175
OSPFv2 マルチエリア隣接関係に関する追加情報 176
OSPFv2 マルチエリア隣接関係の機能情報 177
OSPFv2 自動ルート除外 179
機能情報の確認 179
OSPFv2 自動ルート除外の前提条件 180
OSPFv2 自動ルート除外について 180
OSPFv2 自動ルート除外の概要 180
OSPFv2 自動ルート除外の設定方法 181
OSPFv2 自動ルート除外の設定 181
OSPFv2 自動ルート除外の設定例 182
例：OSPFv2 自動ルート除外の設定 182
OSPFv2 自動ルート除外に関する追加情報 182
OSPFv2 自動ルート除外の機能情報 183
OSPFv3 アドレス ファミリ 185
機能情報の確認 185
OSPFv3 アドレス ファミリの前提条件 186
OSPFv3 アドレス ファミリに関する情報 186
OSPFv3 アドレス ファミリ 186
OSPFv3 アドレス ファミリの設定方法 187
OSPFv3 ルータ プロセスの設定 187

OSPFv3 への IPv6 アドレス ファミリの設定 190
OSPFv3 への IPv4 アドレス ファミリの設定 193
OSPFv3 へのルート再配布の設定 196
インターフェイス上での OSPFv3 のイネーブル化 198
IPv6 または IPv4 アドレス ファミリに対する OSPFv3 エリア範囲の定義 199
OSPFv3 エリア範囲の定義 201
OSPFv3 アドレス ファミリの設定例 202
例：OSPFv3 アドレス ファミリの設定 202
その他の参考資料 202
OSPFv3 アドレス ファミリの機能情報 204
OSPFv3 認証トレーラ 209
機能情報の確認 209
OSPFv3 認証トレーラに関する情報 210
OSPFv3 認証トレーラの概要 210
OSPFv3 認証トレーラの設定方法 211
OSPFv3 認証トレーラの設定 211
OSPFv3 認証トレーラの設定例 213
例：OSPFv3 認証トレーラの設定 213
例：OSPFv3 認証トレーラの確認 213
OSPFv3 認証トレーラに関する追加情報 214
OSPFv3 認証トレーラの機能情報 215
OSPFv3 の自動ルート通知と Forwarding Adjacency（FA） 217
機能情報の確認 217
OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）の前提条件 218
OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）の制約事項 218
OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）について 218
OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）の概要 218
OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）の設定方法 220
OSPFv3 の自動ルート通知および Forwarding Adjacency の設定 220
OSPFv3 の自動ルート通知および Forwarding Adjacency の設定例 223
例：OSPFv3 の自動ルート通知および Forwarding Adjacency の設定 223
OSPFv3 の自動ルート通知および Forwarding Adjacency に関する追加情報 224

OSPFv3 の自動ルート通知および Forwarding Adjacency の機能情報 225

OSPFv3 自動ルート除外 227

機能情報の確認 227

OSPFv3 自動ルート除外の前提条件 228

OSPFv3 自動ルート除外について 228

OSPFv3 自動ルート除外の概要 228

OSPFv3 自動ルート除外の設定方法 229

OSPFv3 自動ルート除外の設定 229

OSPFv3 自動ルート除外の設定例 230

例：OSPFv3 自動ルート除外の設定 230

OSPFv3 自動ルート除外に関する追加情報 230

OSPFv3 自動ルート除外の機能情報 231

OSPFv2 IP FRR ローカル マイクロループ回避 233

機能情報の確認 233

OSPFv2 IP FRR ローカル マイクロループ回避について 234

OSPFv2 IP FRR ローカル マイクロループ回避の概要 234

OSPFv2 IP FRR ローカル マイクロループ回避の設定方法 235

OSPFv2 IP FRR ローカル マイクロループの設定 235

OSPFv2 IP FRR ローカル マイクロループ回避の設定例 236

例：OSPFv2 IP FRR ローカル マイクロループの設定 236

OSPFv2 IP FRR ローカル マイクロループ回避に関する追加情報 236

OSPFv2 IP FRR ローカル マイクロループ回避の機能情報 237

OSPFv2-OSPF Live-Live 239

機能情報の確認 239

OSPFv2-OSPF Live-Live に関する情報 240

OSPFv2-OSPF Live-Live の概要 240

OSPFv2-OSPF Live-Live の設定方法 241

OSPFv2-OSPF Live-Live の設定 241

OSPFv2-OSPF Live-Live の設定例 245

例：OSPFv2-OSPF Live-Live の設定 245

OSPFv2-OSPF Live-Live に関する追加情報 246

OSPFv2-OSPF Live-Live の機能情報 246

変換後のタイプ 5 LSA での OSPF フォワーディング アドレス抑制 249

機能情報の確認 **249**

OSPF フォワーディング アドレス抑制の前提条件 **250**

OSPF フォワーディング アドレス抑制に関する情報 **250**

OSPF フォワーディング アドレス抑制の利点 **250**

変換後のタイプ 5 LSA で OSPF フォワーディング アドレスを抑制する場合 **250**

OSPF フォワーディング アドレスを抑制する方法 **252**

変換後のタイプ 5 LSA での OSPF フォワーディング アドレスの抑制 **252**

OSPF フォワーディング アドレス抑制の設定例 **253**

変換後のタイプ 5 LSA での OSPF フォワーディング アドレスの抑制：例 **253**

その他の参考資料 **253**

OSPF フォワーディング アドレス抑制の機能情報 **255**

配布リスト付きのルート マップによる OSPF インバウンド フィルタリング 257

機能情報の確認 **257**

配布リスト付きのルート マップによる OSPF インバウンド フィルタリングの前提条件 **258**

配布リスト付きのルート マップによる OSPF インバウンド フィルタリングについて **258**

OSPF ルートマップベースフィルタリングの利点 **258**

ルート マップを使用した OSPF インバウンド フィルタリングの設定方法 **259**

ルート マップによる OSPF インバウンド フィルタリングの設定 **259**

配布リスト付きのルート マップによる OSPF インバウンド フィルタリングの設定例 **261**

例：OSPF ルート マップ ベースのフィルタリング **261**

その他の参考資料 **261**

配布リスト付きのルート マップによる OSPF インバウンド フィルタリングの機能情報 **263**

distribute-list を使用した OSPFv3 ルート フィルタリング 265

機能情報の確認 **265**

distribute-list を使用した OSPFv3 ルート フィルタリングの前提条件 **266**

distribute-list を使用した OSPFv3 ルート フィルタリングについて **266**

distribute-list を使用した OSPFv3 ルート フィルタリングの設定方法 **267**

OSPFv3（IPv4 アドレス ファミリ）の設定 **267**

インバウンド フィルタリング：ルート マップの設定 **267**

インバウンド フィルタリング：プレフィックス リスト/アクセス リストの設定 268
アウトバウンド フィルタリングの設定 269
OSPFv3（IPv6 アドレス ファミリ）の配布リストを使用したルート フィルタリングの設定 270
インバウンド フィルタリング：ルート マップの設定 270
インバウンド フィルタリング：プレフィックス リストの設定 271
アウトバウンド フィルタリングの設定 271
その他の参考資料 272
配布リストを使用した OSPFv3 ルート フィルタリングの機能情報 273
OSPF Shortest Path First スロットリング 275
機能情報の確認 275
OSPF SPF スロットリングについて 276
OSPF SPF スロットリングの設定方法 277
OSPF SPF スロットリングの設定 277
SPF スロットル値の確認 278
OSPF SPF スロットリングの設定例 278
例：スロットル タイマー 278
その他の参考資料 279
OSPF Shortest Path First スロットリングの機能情報 280
fast hello パケットに対する OSPF のサポート 283
機能情報の確認 283
fast hello パケットに対する OSPF のサポートの前提条件 284
fast hello パケットに対する OSPF のサポートについて 284
OSPF Hello インターバルおよび dead 間隔 284
OSPF fast hello パケット 284
OSPF fast hello パケットの利点 285
OSPF fast hello パケットの設定方法 285
OSPF fast hello パケットの設定 285
fast hello パケットに対する OSPF のサポートの設定例 287
例：OSPF fast hello パケット 287
その他の参考資料 287

fast hello パケットに対する OSPF のサポートの機能情報 288
OSPF のインクリメンタル SPF 291
機能情報の確認 291
OSPF のインクリメンタル SPF の前提条件 292
OSPF のインクリメンタル SPF について 292
OSPF のインクリメンタル SPF をイネーブルにする方法 292
インクリメンタル SPF のイネーブル化 292
OSPF のインクリメンタル SPF の設定例 293
例：インクリメンタル SPF 293
その他の参考資料 293
OSPF のインクリメンタル SPF の機能情報 295
OSPF のルート再配布数の制限 297
機能情報の確認 297
OSPF のルート再配布数制限の前提条件 298
OSPF のルート再配布数制限について 298
OSPF のルート再配布数を制限する方法 298
再配布されるルート数の制限 298
OSPF へのルートの再配布数に関する警告の要求 300
OSPF のルート再配布数制限の設定例 302
例：OSPF のルート再配布数の制限 302
例：ルートの再配布数に関する警告の要求 302
その他の参考資料 302
OSPF のルート再配布数制限の機能情報 304
OSPFv3 高速コンバージェンス：LSA および SPF スロットリング 305
機能情報の確認 305
OSPFv3 高速コンバージェンスについて：LSA および SPF スロットリング 306
高速コンバージェンス：LSA および SPF スロットリング 306
OSPFv3 高速コンバージェンスの設定方法：LSA および SPF スロットリング 306
OSPFv3 高速コンバージェンスに対する LSA および SPF タイマーの調整 306
OSPFv3 高速コンバージェンスに対する LSA および SPF スロットリングの設定 308
OSPFv3 高速コンバージェンスの設定例：LSA および SPF スロットリング 309
OSPFv3 高速コンバージェンスに対する LSA および SPF スロットリングの設定例 309

その他の参考資料 310
OSPFv3 高速コンバージェンス：LSA および SPF スロットリングの機能情報 311
OSPFv3 Max-Metric ルータ LSA 313
機能情報の確認 313
OSPFv3 Max-Metric ルータ LSA について 314
OSPFv3 Max-Metric ルータ LSA 314
OSPFv3 Max-Metric ルータ LSA の設定方法 314
OSPFv3 Max-Metric ルータ LSA の設定 314
OSPFv3 Max-Metric ルータ LSA の設定例 316
例：OSPFv3 Max-Metric ルータ LSA の確認 316
OSPF ノンストップ ルーティングに関する追加情報 316
OSPFv3 Max-Metric ルータ LSA の機能情報 317
OSPF リンクステート アドバタイズメント スロットリング 319
機能情報の確認 319
OSPF LSA スロットリングの前提条件 320
OSPF LSA スロットリングについて 320
OSPF LSA スロットリングの利点 320
OSPF LSA スロットリングの動作 320
OSPF LSA スロットリングのカスタマイズ方法 321
OSPF LSA スロットリングのカスタマイズ 321
OSPF LSA スロットリングの設定例 326
例：OSPF LSA スロットリング 326
その他の参考資料 326
OSPF リンクステート アドバタイズメント スロットリングの機能情報 327
PE ルータごとに無制限なソフトウェア VRF の OSPF サポート 329
機能情報の確認 329
PE ルータごとに無制限なソフトウェア VRF の OSPF サポートの前提条件 330
PE ルータごとに無制限なソフトウェア VRF の OSPF サポートの制約事項 330
PE ルータごとに無制限なソフトウェア VRF の OSPF サポートについて 330
PE ルータごとに無制限のソフトウェア VRF を OSPF がサポートする設定方法 331
PE ルータごとの無制限のソフトウェア VRF の設定 331
PE ルータごとの無制限のソフトウェア VRF に対する OSPF サポートの設定例 332

例：PE ルータごとの無制限のソフトウェア VRF に対する OSPF サポートの設定 332
例：PE ルータごとの無制限のソフトウェア VRF に対する OSPF サポートの確認 333
その他の参考資料 333
PE ルータごとの無制限のソフトウェア VRF に対する OSPF サポートの機能情報 335
OSPF エリア中継機能 337
機能情報の確認 337
OSPF エリア トランジット機能について 338
OSPF エリア トランジット機能の動作 338
OSPF エリア トランジット機能をディセーブルにする方法 338
エリア境界ルータでの OSPF エリア中継機能のディセーブル化 338
その他の参考資料 339
OSPF エリア中継機能の機能情報 340
OSPF インターフェイス単位リンクローカル シグナリング 343
機能情報の確認 343
OSPF インターフェイス単位リンクローカル シグナリングについて 344
OSPF インターフェイス単位リンクローカル シグナリングの設定方法 344
インターフェイス単位での LLS の停止 344
次の作業 346
OSPF インターフェイス単位リンクローカル シグナリングの設定例 346
例：OSPF インターフェイス単位リンクローカル シグナリングの設定と確認 346
その他の参考資料 347
OSPF インターフェイス単位リンクローカル シグナリングの機能情報 349
OSPF リンクステート データベース オーバーロードの防止 351
機能情報の確認 351
OSPF リンクステート データベース オーバーロード防止機能の前提条件 352
OSPF リンクステート データベース オーバーロード防止機能について 352
OSPF リンクステート データベース オーバーロード防止機能を使用する利点 352
OSPF リンクステート データベース オーバーロード防止機能の動作 352
OSPF リンクステート データベース オーバーロード防止の設定方法 353
OSPF プロセスの自己生成 LSA 数の制限 353
OSPF リンクステート データベース オーバーロード防止の設定例 355
LSA 生成制限の設定：例 355

その他の参考資料 356
OSPF リンクステート データベース オーバーロード防止の機能情報 358
RFC 1850 の OSPF MIB サポートおよび最新の拡張 359
機能情報の確認 359
RFC 1850 の OSPF MIB サポートおよび最新の拡張の前提条件 360
RFC 1850 の OSPF MIB サポートおよび最新の拡張について 360
RFC 1850 をサポートするための OSPF MIB の変更 360
OSPF MIB 360
OSPF トラップ MIB 362
CISCO OSPF MIB 363
CISCO OSPF トラップ MIB 364
OSPF MIB の利点 366
RFC 1850 の OSPF MIB サポートおよび最新の拡張をイネーブルにする方法 366
OSPF MIB サポートのイネーブル化 366
次の作業 368
特定の OSPF トラップのイネーブル化 368
ルータ上の OSPF MIB トラップの確認 370
RFC 1850 の OSPF MIB サポートおよび最新の拡張の設定例 371
例：OSPF MIB サポート トラップのイネーブル化と確認 371
次の作業 371
その他の参考資料 371
RFC 1850 の OSPF MIB サポートおよび最新の拡張の機能情報 373
OSPF 拡張トラフィックの統計情報 377
機能情報の確認 377
OSPF 拡張トラフィック統計情報の前提条件 378
OSPF 拡張トラフィック統計情報について 378
OSPF 拡張トラフィック統計情報を表示およびクリアする方法 378
OSPFv2 の OSPF トラフィック統計情報の表示とクリア 378
OSPFv3 の OSPF トラフィック統計情報の表示とクリア 379
OSPF 拡張トラフィック統計情報の設定例 380
例：OSPFv2 の拡張トラフィック統計情報の表示とクリア 380
例：OSPFv3 の拡張トラフィック統計情報の表示とクリア 382
その他の参考資料 384

OSPF 拡張トラフィック統計情報の機能情報 385

IPv6 での OSPFv3 の TTL セキュリティ サポート 387

機能情報の確認 387

IPv6 での OSPFv3 の TTL セキュリティ サポートの制約事項 388

IPv6 での OSPFv3 の TTL セキュリティ サポートの前提条件 388

IPv6 での OSPFv3 の TTL セキュリティ サポートについて 388

仮想および模造リンクの OSPFv3 TTL セキュリティ サポート 388

IPv6 での OSPFv3 の TTL セキュリティ サポートの設定方法 389

IPv6 での OSPFv3 の仮想リンクに対する TTL セキュリティ サポートの設定 389

IPv6 での OSPFv3 の模造リンクに対する TTL セキュリティ サポートの設定 391

IPv6 での OSPFv3 の TTL セキュリティ サポートの設定例 392

例：IPv6 での OSPFv3 の仮想リンクに対する TTL セキュリティ サポート 392

例：IPv6 での OSPFv3 の模造リンクに対する TTL セキュリティ サポート 392

その他の参考資料 393

IPv6 での OSPFv3 の TTL セキュリティ サポートの機能情報 394

OSPF TTL セキュリティ チェックと OSPF グレースフル シャットダウンの設定 395

機能情報の確認 395

OSPF TTL セキュリティ チェックと OSPF グレースフル シャットダウンについて 396

OSPF の TTL セキュリティ チェック 396

TTL セキュリティ チェックを使用するための既存ネットワークの移行 396

OSPF 仮想リンクおよび模造リンクの TTL セキュリティ チェック 396

TTL セキュリティ チェックに対する OSPF サポートの利点 397

OSPF グレースフル シャットダウン 397

OSPF TTL セキュリティ チェックと OSPF グレースフル シャットダウンの設定方法 398

すべての OSPF インターフェイスでの TTL セキュリティ チェックの設定 398

インターフェイス単位での TTL セキュリティ チェックの設定 399

インターフェイス単位での OSPF グレースフル シャットダウンの設定 401

OSPF TTL セキュリティ チェックおよび OSPF グレースフル シャットダウンの設定例 403

例：TTL セキュリティ チェックを使用するための既存ネットワークの移行 403

その他の参考資料 403

OSPF TTL セキュリティ チェックおよび OSPF グレースフル シャットダウンの機能情報 405

OSPF 模造リンク MIB サポート 407

機能情報の確認 407

OSPF 模造リンク MIB サポートの前提条件 408

OSPF 模造リンク MIB サポートの制約事項 408

OSPF 模造リンク MIB サポートに関する情報 408

PE-PE 間ルータ接続における OSPF 模造リンク 408

Cisco OSPF MIB および Cisco OSPF トラップ MIB の拡張機能 408

OSPF 模造リンク設定のサポート 409

OSPF 模造リンク ネイバーのサポート 409

OSPF 模造リンク インターフェイスの移行ステート変更のサポート 410

OSPF 模造リンク ネイバーの移行ステート変更のサポート 410

模造リンクのエラー 410

OSPF 模造リンク MIB サポートの設定方法 411

ルータによる SNMP 通知送信のイネーブル化の設定 411

OSPF 模造リンク エラー トラップ送信のイネーブル化 412

OSPF 模造リンクの再送信トラップのイネーブル化 414

OSPF 模造リンクのステート変更トラップのイネーブル化 415

ルータ上の OSPF 模造リンク MIB トラップの確認 417

OSPF 模造リンク MIB サポートの設定例 417

例：OSPF 模造リンク エラー トラップのイネーブル化と確認 417

例：OSPF ステート変更トラップのイネーブル化と確認 418

例：OSPF 模造リンク再送信トラップのイネーブル化と確認 418

次の作業 419

その他の参考資料 419

OSPF 模造リンク MIB サポートの機能情報 421

データ フィールドのインターフェイス ID の OSPF SNMP ifIndex 値 423

機能情報の確認 423

データ フィールドのインターフェイス ID の SNMP ifIndex 値の前提条件 424

データ フィールドのインターフェイス ID の SNMP ifIndex 値について 424

SNMP MIB-II ifIndex 値でインターフェイスを識別する利点 424

OSPFv2 および OSPFv3 での SNMP MIB-II ifIndex 値の使用方法 424

データ フィールドにインターフェイス ID として SNMP ifIndex 値を設定する方法 425

OSPF インターフェイスによる SNMP MIB-II ifIndex 番号の使用の設定 425
データ フィールドのインターフェイス ID としての SNMP ifIndex 値の設定例 427
例：OSPFv2 のインターフェイス ID としての SNMP ifIndex 値の設定 427
例：OSPFv3 のインターフェイス ID としての SNMP ifIndex 値の設定 427
その他の参考資料 431
インターフェイス ID としての OSPF SNMP ifIndex 値の機能情報 432
OSPFv2 ローカル RIB 435
機能情報の確認 435
OSPFv2 ローカル RIB の前提条件 436
OSPFv2 ローカル RIB の制約事項 436
OSPFv2 ローカル RIB について 436
OSPFv2 ローカル RIB の設定方法 437
デフォルトのローカル RIB 基準の変更 437
廃棄ルートのアドミニストレーティブ ディスタンスの変更 438
トラブルシューティングのヒント 440
OSPFv2 ローカル RIB の設定例 440
例：デフォルトのローカル RIB 基準の変更 440
例：廃棄ルートのアドミニストレーティブ ディスタンスの変更 440
その他の参考資料 441
OSPFv2 ローカル RIB の機能情報 442
MPLS TE トンネルを介した Forwarding Adjacency（FA）の OSPF サポート 445
機能情報の確認 446
OSPF Forwarding Adjacency（FA）の前提条件 446
OSPF Forwarding Adjacency（FA）について 446
OSPF Forwarding Adjacency（FA）の設定方法 447
OSPF Forwarding Adjacency の設定 447
OSPF Forwarding Adjacency の設定例 450
例：OSPF Forwarding Adjacency 450
その他の参考資料 451
インターフェイスごとの OSPFv2 のイネーブル化 453
機能情報の確認 453
インターフェイスごとに OSPFv2 をイネーブルにする前提条件 454

インターフェイスごとの OSPFv2 のイネーブル化の制約事項 454
インターフェイスごとの OSPFv2 のイネーブル化について 454
インターフェイスごとに OSPFv2 をイネーブルにする利点 454
ルータごとまたはインターフェイスごとの OSPFv2 の設定の影響 454
インターフェイスごとに OSPFv2 をイネーブルにする方法 456
インターフェイス上での OSPFv2 のイネーブル化 456
インターフェイス上での OSPFv2 のイネーブル化の設定例 457
例：インターフェイス上での OSPFv2 のイネーブル化 457
その他の参考資料 458
インターフェイス単位での OSPFv2 のイネーブル化の機能情報 459
OSPF ノンストップ ルーティング 461
機能情報の確認 461
OSPF NSR の前提条件 462
OSPF NSR の制約事項 462
OSPFv3 認証トレーラに関する情報 462
OSPF NSR 機能 462
OSPF ノンストップ ルーティングの設定方法 463
OSPF NSR の設定 463
トラブルシューティングのヒント 464
OSPF ノンストップ ルーティングの設定例 464
例：OSPF NSR の設定 464
その他の参考資料 465
OSPF NSR の機能情報 466
OSPFv3 NSR 467
機能情報の確認 467
OSPFv3 NSR について 468
OSPFv3 NSR 機能 468
OSPFv3 NSR の設定方法 468
OSPFv3 NSR の設定 468
アドレス ファミリに対する OSPFv3 NSR の設定 470
アドレス ファミリの OSPFv3 NSR の表示 470
トラブルシューティングのヒント 471

OSPFv3 NSR の設定例 472
例：OSPFv3 NSR の設定 472
例：OSPFv3 NSR の確認 473
その他の参考資料 474
OSPFv3 NSR の機能情報 475
OSPFv2 Loop-Free Alternate Fast Reroute 477
機能情報の確認 477
OSPFv2 Loop-Free Alternate Fast Reroute の前提条件 478
OSPFv2 Loop-Free Alternate Fast Reroute の制約事項 478
OSPFv2 Loop-Free Alternate Fast Reroute に関する情報 478
LFA 修復パス 478
LFA 修復パス属性 479
共有リスク リンク グループ 479
インターフェイスの保護 480
ブロードキャスト インターフェイス保護 480
ノード保護 480
ダウンストリーム パス 480
ラインカード Disjoint インターフェイス 480
メトリック 481
等コスト マルチパス プライマリ パス 481
修復パスの候補リスト 481
OSPFv2 Loop-Free Alternate Fast Reroute の設定方法 481
プレフィックスごとの OSPFv2 Loop-Free Alternate Fast Reroute のイネーブル化 481
LFA FRR によるプレフィックス保護の指定 482
修復パスの選択ポリシーの設定 484
考慮する修復パス リストの作成 485
インターフェイスのネクスト ホップとしての使用の禁止 486
OSPFv2 Loop-Free Alternate Fast Reroute の設定例 487
例：プレフィックスごとの LFA IP FRR のイネーブル化 487
例：プレフィックス保護優先度の指定 488
例：修復パスの選択ポリシーの設定 488
例：修復パスの選択の監視 488

例：インターフェイスの保護インターフェイス化の禁止 488
その他の参考資料 488
OSPFv2 Loop-Free Alternate Fast Reroute の機能情報 490
OSPFv3 MIB 493
機能情報の確認 493
OSPFv3 MIB の前提条件 494
OSPFv3 MIB サポートの制約事項 494
OSPFv3 MIB について 494
OSPFv3 MIB 494
OSPFv3 トラップ MIB 494
OSPFv3 MIB の設定方法 495
特定の OSPFv3 トラップのイネーブル化 495
デバイスでの OSPFv3 MIB トラップの確認 496
OSPFv3 MIB の設定例 497
例：OSPFv3 MIB トラップのイネーブル化と確認 497
OSPFv3 MIB に関する追加情報 498
OSPFv3 MIB の機能情報 499
OSPFv3 のプレフィックス抑制のサポート 501
機能情報の確認 501
OSPFv3 のプレフィックス抑制サポートの前提条件 502
OSPFv3 プレフィックス抑制サポートについて 502
OSPFv3 プレフィックス抑制サポート 502
OSPFv3 プロセスの設定による IPv4 および IPv6 プレフィックス アドバタイズメントのグローバルな抑制 502
インターフェイスごとの IPv4 および IPv6 プレフィックス アドバタイズメントの抑制 503
OSPFv3 プレフィックス抑制サポートの設定方法 503
OSPFv3 プロセスのプレフィックス抑制サポートの設定 503
アドレス ファミリ コンフィギュレーション モードでの OSPFv3 プレフィックス抑制サポートの設定 504
インターフェイス単位でのプレフィックス抑制サポートの設定 506
IPv4 および IPv6 プレフィックス抑制のトラブルシューティング 507
OSPFv3 プレフィックス抑制サポートの設定例 508

例：OSPFv3 プレフィックス抑制サポートの設定 508
OSPFv3 プレフィックス抑制サポートに関する追加情報 509
OSPFv3 プレフィックス抑制サポートの機能情報 509
OSPFv3 VRF-Lite/PE-CE 511
機能情報の確認 511
OSPFv3 VRF-Lite/PE-CE の制約事項 512
OSPFv3 VRF-Lite/PE-CE について 512
OSPFv3 VRF-Lite および PE-CE のサポート 512
VRF-Lite/PE-CE の設定方法 513
IPv6 アドレス ファミリでの VRF への OSPFv3 の設定 513
VRF インターフェイスでの OSPFv3 IPv6 アドレス ファミリのイネーブル化 515
OSPFv3 PE-CE への模造リンクの設定 516
OSPFv3 PE-CE へのドメイン ID の設定 519
OSPFv3 への VRF-Lite 機能の設定 520
OSPFv3 VRF-Lite/PE-CE の設定例 522
例： IPv4 および IPv6 ルーティングを提供するためのプロバイダー エッジ デバイスの設定 522
例：VRF-Lite に対するプロバイダー エッジ デバイスの設定 523
OSPFv3 VRF-Lite/PE-CE に関する追加情報 524
OSPFv3 VRF-Lite/PE-CE の機能情報 525
OSPFv3 ABR タイプ 3 LSA フィルタリング 527
機能情報の確認 527
OSPFv3 ABR タイプ 3 LSA フィルタリング 528
OSPFv3 ABR タイプ 3 LSA フィルタリングについて 528
エリア フィルタのサポート 528
OSPFv3 ABR タイプ 3 LSA フィルタリングの設定方法 528
OSPFv3 のエリア フィルタ サポートの設定 528
OSPFv3 ABR タイプ 3 LSA フィルタリングの設定例 529
例：OSPFv3 のエリア フィルタ サポート 529
OSPFv3 ABR タイプ 3 LSA フィルタリングに関する追加情報 530
OSPFv3 ABR タイプ 3 LSA フィルタリングの機能情報 531
OSPFv3 デマンド回路の無視 533

機能情報の確認 533
OSPFv3 デマンド回線無視について 534
デマンド回線の無視のサポート 534
OSPFv3 デマンド回線無視の設定方法 534
OSPFv3 デマンド回線無視の設定 534
OSPFv3 デマンド回線無視の設定例 536
例：OSPFv3 デマンド回線無視のサポート 536
OSPFv3 デマンド回線無視に関する追加情報 536
OSPFv3 デマンド回線無視の機能情報 537
OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute 539
機能情報の確認 539
OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute の前提条件 540
OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute の制約事項 540
OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute について 541
IP 高速再ルーティング 541
リング トポロジを含む OSPF IPv4 リモート IPFRR LFA 541
OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute の設定方法 542
リモート LFA トンネルの設定 542
トンネル エンドポイントまでの最大距離の設定 543
OSPF IPv4 リモート LFA IPFRR により作成されるトンネル インターフェイスの確認 544
OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute の設定例 545
例：リモート LFA トンネルの設定 545
例：トンネル エンドポイントまでの最大距離の設定 545
例：OSPF IPv4 リモート LFA IPFRR により作成されるトンネル インターフェイスの確認 545
その他の参考資料 546
OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute の機能情報 547
OSPFv3 マルチエリア隣接関係 549
機能情報の確認 549
OSPFv3 マルチエリア隣接関係の前提条件 550
OSPFv3 マルチエリア隣接関係の制約事項 550

OSPFv3 マルチエリア隣接関係について 550
OSPFv3 マルチエリア隣接関係の概要 550
OSPFv3 マルチエリア隣接関係の設定方法 551
OSPFv3 マルチエリア隣接関係の設定 551
OSPFv3 マルチエリア隣接関係の確認 553
OSPFv3 マルチエリア隣接関係の設定例 553
例：OSPFv3 マルチエリア隣接関係の設定 553
例：OSPFv3 マルチエリア隣接関係の確認 554
OSPFv3 マルチエリア隣接関係に関する追加情報 555
OSPFv3 マルチエリア隣接関係の機能情報 555
OSPF 隣接関係確立制限 557
機能情報の確認 557
OSPF 隣接関係確立制限について 558
隣接関係の制限の概要 558
隣接関係の確立の設定 558
OSPF 隣接関係確立制限の設定方法 559
グローバルな隣接関係確立の設定 559
ルータ コンフィギュレーション モードでの隣接関係制限の設定 559
アドレス ファミリ コンフィギュレーション モードでの隣接関係制限の設定 560
インターフェイス コンフィギュレーション モードでの隣接関係スタガリングのディセーブル化 562
隣接関係スタガリングの確認 563
OSPF 隣接関係確立制限の設定例 564
例：ルータ コンフィギュレーション モードでの隣接関係制限の設定 564
例：アドレス ファミリ コンフィギュレーション モードでの隣接関係制限の設定 565
例：インターフェイス コンフィギュレーション モードでの隣接関係のディセーブル化 565
OSPF 隣接関係確立制限に関する追加情報 565
OSPF 隣接関係確立制限の機能情報 566

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（アクセスおよびエッジルーティング用）以降、これら2つのリリースは、単一の統合されたリリースバージョンである Cisco IOS XE 16 に進化（合体）されています。これにより、スイッチングとルーティングのポートフォリオにおいて広範囲のアクセス製品およびエッジ製品をカバーする単一のリリースが提供されます。

（注） テクノロジー コンフィギュレーション ガイドにある「機能情報」表には、機能が導入された時期が記載されています。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。特定の機能がご使用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、ご使用の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 ガイドを参照してください。ご使用の製品のランディング ページにテクノロジー コンフィギュレーション ガイドが表示されていれば、その機能はプラットフォームでサポートされています。

第 2 章

『Configuring OSPF』

ここでは、Open Shortest Path First（OSPF）の設定方法について説明します。OSPF は、Internet Engineering Task Force（IETF）の OSPF ワーキング グループによって開発された内部ゲートウェイ プロトコル（IGP）です。OSPF は特に IP ネットワーク向けに設計されており、IP サブネット化、および外部から取得したルーティング情報のタギングをサポートしています。OSPF を使用するとパケット認証も可能になり、パケットを送受信するときに IP マルチキャストが使用されます。

シスコは、RFC 1253、「*OSPF Version 2 Management Information Base*」（1991 年 8 月）をサポートします。OSPF MIB は、OSPF に関連する管理情報を提供し、シスコ ルータでサポートされる IP ルーティング プロトコルを定義します。

OSPF と連動するプロトコルを選ばない機能については、「Configuring IP Routing Protocol-Independent Features」のモジュールを参照してください。

- 機能情報の確認，3 ページ
- OSPF に関する情報，4 ページ
- OSPF の設定方法，13 ページ
- OSPF の設定例，41 ページ
- OSPF Not-So-Stubby Areas（NSSA）に関する追加情報，59 ページ
- OSPF 設定の機能情報，60 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。

OSPF に関する情報

シスコの OSPF 実装

シスコの実装は、OSPF バージョン 2 仕様に準拠します。この詳細はインターネット RFC 2328 に記載されています。次に、シスコの OSPF 実装でサポートされている主要機能について説明します。

- スタブ エリア：スタブ エリアの定義がサポートされています。
- ルート再配布：任意の IP ルーティング プロトコルによって学習されたルートを、別の IP ルーティング プロトコルで再配布できます。ドメイン内レベルでは、OSPF は Interior Gateway Routing Protocol（IGRP）、Routing Information Protocol（RIP）、および Intermediate System-to-Intermediate System（IS-IS）で学習したルートをインポートできます。OSPF ルートを IGRP、RIP、および IS-IS にエクスポートすることもできます。ドメイン間レベルでは、OSPF は Exterior Gateway Protocol（EGP）および Border Gateway Protocol（BGP）で学習したルートをインポートできます。OSPF ルートは、EGP および BGP にエクスポートできます。
- 認証：エリア内の隣接ルータ間でのプレーン テキスト認証およびメッセージダイジェスト アルゴリズム 5（MD5）認証がサポートされています。
- ルーティング インターフェイス パラメータ：サポートされる設定可能なパラメータには、インターフェイス出力コスト、再送信インターバル、インターフェイス送信遅延、ルータ プライオリティ、ルータの「dead」インターバルと hello インターバル、認証キーなどがあります。
- 仮想リンク：仮想リンクがサポートされています。
- Not-So-Stubby Area（NSSA）：RFC 3101 が取って代わり、RFC 1587 との後方互換性があります。
- デマンド回線上の OSPF：RFC 1793。

OSPF のルータの調整

通常、OSPF を使用するには、多くの内部ルータ、複数のエリアに接続されたエリア境界ルータ（ABR）、および自律システム境界（ASBR）間での調整が必要です。OSPF ベースのルータまたはアクセス サーバの最小設定では、すべてのデフォルト パラメータ値、およびエリアに割り当てられたインターフェイスが使用され、認証は行われません。環境をカスタマイズする場合は、すべてのルータの調和が取れた設定が必要です。

OSPF のルート配布

ルート再配布を指定できます。ルート再配布の設定方法については、『*Network Protocols Configuration Guide, Part 1*』の「Redistribute Routing Information」を参照してください。

シスコの OSPF 実装を使用すると、必要に応じてインターフェイス固有の OSPF パラメータを変更できます。これらのパラメータを変更する必要はありませんが、一部のインターフェイス パラメータについては、接続されたネットワーク内のすべてのルータで統一性を維持する必要があります。これらのパラメータは、**ipospfhello-interval**、**ipospfdead-interval**、および **ipospfauthentication-key** インターフェイス コンフィギュレーション コマンドによって制御されます。したがって、これらのパラメータを設定する場合は、ネットワーク上のすべてのルータのコンフィギュレーションと互換性のある値にしてください。

デフォルトでは、OSPF は次の 3 種類のネットワークにメディアを分類します。

- ブロードキャスト ネットワーク（イーサネット、トークンリング、FDDI）
- 非ブロードキャスト マルチアクセス（NBMA）ネットワーク（スイッチド マルチメガビット データ サービス（SMDS）、フレーム リレー、および X.25）
- ポイントツーポイント ネットワーク（High-Level Data Link Control（HDLC）および PPP）

ブロードキャストまたは NBMA ネットワークとしてネットワークを設定できます。

X.25 およびフレーム リレーは、マップに設定できるオプションのブロードキャスト機能を提供し、これによって OSPF をブロードキャスト ネットワークとして実行できます。詳細については、『*Cisco IOS Wide-Area Networking Command Reference*』の **x25map** および **frame-relaymap** コマンド ページを参照してください。

OSPF ネットワーク タイプ

デフォルトのメディア タイプと無関係に、OSPF ネットワーク タイプをブロードキャストまたは NBMA として設定できます。たとえば、ユーザのネットワークにあるルータでマルチキャスト アドレッシングがサポートされない場合に、この機能を使用してブロードキャスト ネットワークを NBMA ネットワークとして設定できます。NBMA ネットワーク（X.25、フレームリレー、SMDS など）もブロードキャスト ネットワークとして設定できます。この機能により、以降の「非ブロードキャスト ネットワークの OSPF の設定」のセクションで説明するように、ネイバーを設定する必要がなくなります。

NBMA ネットワークをブロードキャストまたは非ブロードキャストとして構成する場合は、各ルータから各ルータ、つまりフルメッシュのネットワークにまで仮想回線（VC）があると想定されます。たとえば、コストの制約があったり、一部だけがメッシュ ネットワークになっている場合には設定できません。この場合は、OSPF ネットワークのタイプをポイントツーマルチポイント ネットワークとして設定できます。直接接続していない 2 つのルータ間のルーティングは、VC のあるルータを通過して 2 つのルータに到達します。この機能を使用する場合は、ネイバーを設定する必要はありません。

OSPFポイントツーマルチポイントインターフェイスは、1つ以上のネイバーを持つ番号付きポイントツーポイントインターフェイスとして定義されます。複数のホストルートが作成されます。OSPF ポイントツーマルチポイント ネットワークには、NBMA やポイントツーポイント ネットワークと比較した場合、次のような利点があります。

- ポイントツーマルチポイントはネイバー コマンドの設定が不要で、1 つの IP サブネットだけを使用し、指定ルータの選定も不要なため、設定が容易です。
- 完全にメッシュ化されたトポロジが必要ないため、コストが低くなります。
- VC の障害時に接続が維持されるため、信頼性が高まります。

ポイントツーマルチポイントブロードキャスト ネットワークでは、ネイバーの指定は不要です。ただし、**neighbor** ルータ コンフィギュレーション コマンドでネイバーを指定できます。この場合は、そのネイバーにコストを指定する必要があります。

point-to-multipoint キーワードが **ipospfnetwork** インターフェイス コンフィギュレーション コマンドに追加される前は、一部の OSPF ポイントツーマルチポイント プロトコル トラフィックがマルチキャスト トラフィックとして扱われていました。マルチキャストによってトラフィックが処理されるため、**neighbor** ルータ コンフィギュレーション コマンドが、ポイントツーマルチポイント インターフェイスに不要でした。hello、アップデート、確認応答の各メッセージは、マルチキャストを使用して送信されていました。特にマルチキャストの hello メッセージにより、すべてのネイバーが動的に検出されました。

ポイントツーマルチポイント インターフェイス（ブロードキャスト、非ブロードキャストを問わず）では、Cisco IOS ソフトウェアは各ネイバーへのコストが等しいと仮定していました。コストは **ipospfcost** インターフェイス コンフィギュレーション コマンドを使用して設定されました。実際には、各ネイバーへの帯域幅が異なるため、コストは違うはずです。この機能を使用すると、各ネイバーへのコストを個別に設定できます。この機能はポイントツーマルチポイント インターフェイスだけに適用されます。

OSPF ネットワークには多くのルータが接続している場合があるため、指定ルータがこのネットワーク用に選択されます。ブロードキャスト機能が設定されていない場合、指定ルータの選択には特別なコンフィギュレーション パラメータが必要になります。

これらのパラメータは、指定ルータまたはバックアップ指定ルータ（ルータ プライオリティ値が 0 以外のルータ）になる資格のあるデバイスだけに設定する必要があります。

次のネイバー パラメータを必要に応じて指定できます。

- 隣接ルータのプライオリティ
- 非ブロードキャストのポーリング間隔

ポイントツーマルチポイントの非ブロードキャスト ネットワークでは、**neighbor** ルータ コンフィギュレーション コマンドを使用してネイバーを特定します。ネイバーへのコストの割り当てはオプションです。

Cisco IOS Release 12.0 以前のバージョンでは、一部のユーザは非ブロードキャスト メディア（classic IP over ATM など）でポイントツーマルチポイントを使用していました。そのため、ルートのネイバーを動的に検出できませんでした。この機能を使用すると、**neighbor** ルータ コンフィギュレーション コマンドをポイントツーマルチポイント インターフェイスで使用できます。

エリア パラメータ

OSPF を使用しているセントラル サイトから別のルーティング プロトコルを使用しているリモート サイトに接続する必要があるインターネット サービス プロバイダー（ISP）またはネットワーク管理者は、OSPF Not-So-Stubby Area（NSSA）機能を使用して管理を簡素化できます。

スタブ エリアにはリモート サイトのルートが再配布されないため、NSSA が実装される前は、企業サイトの境界ルータとリモート ルータ間の接続に OSPF スタブ エリアを利用できず、2 つのルーティング プロトコルを維持する必要がありました。RIP のようなシンプルなプロトコルを実行して再配布を処理する方法が一般的でした。NSSA が実装されたことで、企業ルータとリモート ルータ間のエリアを NSSA として定義することにより、NSSA で OSPF を拡張してリモート接続をカバーできます。

OSPF スタブ エリアと同様に、NSSA エリアはタイプ 5 LSA による配布ルートに注入されません。NSSA エリアへのルート再配布に使用できるのは、NSSA エリアだけに存在可能な、タイプ 7 と呼ばれる特殊なタイプの LSA だけです。NSSA ASBR はタイプ 7 LSA を生成し、ルートの再配布が可能となります。これらのタイプ 7 LSA は、NSSA ABR によってタイプ 5 LSA に変換され、OSPF ルーティング ドメイン全体へフラッディングされます。変換中は集約とフィルタリングがサポートされます。

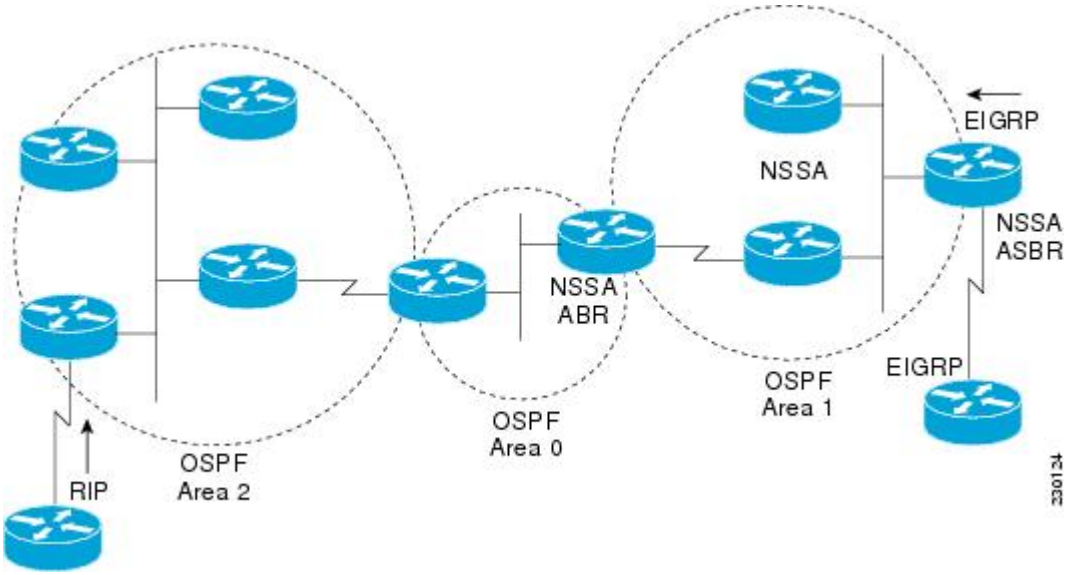
RFC 3101 を使用すると、NSSA ABR ルータを強制 NSSA LSA トランスレータとして設定できます。これは、NSSA ABR ルータが無条件に LSA トランスレータの役割を担うことを意味しており、トランスレータとして選ばれる候補に含めるだけのデフォルトの動作に取って代わります。

（注） 強制されたトランスレータがすべての LSA を変換しない場合でも、変換は各 LSA の内容によって異なります。

以下に示すネットワーク構成図では、OSPF エリア 1 がスタブ エリアとして定義されています。スタブ エリアでは再配布が許可されていないため、Enhanced Interior Gateway Routing Protocol

（EIGRP）ルートを OSPF ドメインに伝播できません。ただし、OSPF エリア 1 を NSSA として定義すれば、タイプ 7 LSA を生成することで OSPF NSSA に EIGRP ルートを注入できます。

図 *1*：*OSPF NSSA*



NSSA はスタブ エリアを拡張したものであるため、RIP ルータから再配布されたルートは OSPF エリア 1 内に到達できません。タイプ 5 LSA が排除される点など、スタブ エリアの特性はそのまま残っています。

ルート集約は、アドバタイズされるアドレスを統合することです。この機能により、ABR から他のエリアに、1 つの要約ルートだけをアドバタイズできます。OSPF では、ABR が 1 つのエリアのネットワークを別のエリアにアドバタイズします。あるエリアにおいて連続する複数のネットワーク番号が割り当てられている場合、指定された範囲に含まれるエリア内の個別のネットワークをすべてカバーするサマリー ルートをアドバタイズするように ABR を設定できます。

他のプロトコルからのルートが（「Configuring IP Routing Protocol-Independent Features」モジュールに記載されているように）OSPF に再配布される場合、各ルートは外部 LSA により個別にアドバタイズされます。ただし、ネットワーク アドレスとマスクの範囲を指定することにより、範囲内のすべての再配布ルートを含む単一ルートがアドバタイズされるように、Cisco IOS ソフトウェアを設定できます。この設定により、OSPF リンク ステート データベースのサイズを縮小できます。

OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンが不連続である場合、またはバックボーンが意図的に分割されている場合は、仮想リンクを確立できます。2 台の ABR を仮想リンクのエンドポイントとして設定できます。仮想リンクは両方のルータで設定される必要があります。各ルータの設定情報には、他の仮想エンドポイント（他の ABR）、および 2 台のルータに共通する非バックボーン エリア（中継エリア）があります。仮想リンクはスタブ エリアからは設定できません。

ASBR を設定し、強制的に OSPF ルーティング ドメインにデフォルト ルートを設定できます。OSPF ルーティング ドメイン内へのルート再配布を設定すると、常にルートは自動的に ASBR に

なります。ただし、デフォルトでは、ASBR はデフォルトルートを OSPF ルーティング ドメインに生成しません。

すべての OSPF show EXEC コマンド表示で使用する Domain Naming System（DNS）名のルックアップを行うよう、OSPF を設定できます。この機能を使用すると、ルータがルータ ID やネイバー ID ではなく名前で表示されるため、ルータを識別しやすくなります。

OSPF は、インターフェイスに設定されている最大の IP アドレスをルータ ID として使用します。この IP アドレスに関連付けられているインターフェイスがダウンした場合、または削除された場合、OSPF プロセスは新しいルータ ID を再計算し、すべてのルーティング情報をそのルータのインターフェイスから再送信する必要があります。

ループバック インターフェイスが IP アドレスによって設定されているときは、より大きい IP アドレスが他のインターフェイスにある場合でも、Cisco IOS ソフトウェアはこの IP アドレスをルータ ID として使用します。ループバック インターフェイスに障害は発生しないため、ルーティング テーブルの安定性が増大します。

OSPF では、自動的にループバック インターフェイスが他よりも優先されます。また、すべてのループバック インターフェイスの中で最も高位の IP アドレスが選択されます。ループバック インターフェイスが存在しない場合、ルータ内で最も高位の IP アドレスが選択されます。特定のインターフェイスを使用するように OSPF に指示することはできません。

Cisco IOS Release 10.3 およびそれ以降のリリースでは、デフォルトでインターフェイスの帯域幅に従ってインターフェイスの OSPF メトリックが計算されます。たとえば、64 kbps のリンクのメトリックは 1562、T1 リンクのメトリックは 64 になります。

OSPF メトリックは ref-bw 値を帯域幅の値で割ったものとして計算され、デフォルトで ref-bw 値は 108 です。帯域幅の値は bandwidth インターフェイス コンフィギュレーション コマンドによって決まります。この計算により FDDI のメトリックは 1 となります。帯域幅が広いリンクが複数ある場合、これらのリンクのコストに差をつけるには、より大きい数値を使用する必要があります。

アドミニストレーティブ ディスタンスは、個々のルータやルータのグループなど、ルーティング情報送信元の信頼性を表す数値です。数値的に、アドミニストレーティブ ディスタンスは 0 ～ 255 の整数です。通常は、値が大きいほど、信頼性の格付けが下がります。アドミニストレーティブ ディスタンスが 255 の場合はルーティング情報の送信元をまったく信頼できないため、無視する必要があります。

OSPF は、intra-area（エリア内）、interarea（エリア間）、および external（外部）の 3 つの異なるアドミニストレーティブ ディスタンスを使用します。エリア内のルートは intra-area、別のエリアへのルートは interarea、再配布を通じて学習された別のルーティング ドメインからのルートは external です。各タイプのルートのデフォルト距離は 110 です。

イーサネット上の 2 つのデバイス間にあるシンプレックス インターフェイスは 1 つのネットワーク セグメントだけを表すため、OSPF では送信側インターフェイスをパッシブ インターフェイスになるように設定する必要があります。この設定により、OSPF が送信側インターフェイスの hello パケットを送信するのを防ぎます。いずれのデバイスも、受信側インターフェイスに生成される hello パケットを通じて、お互いを表示できます。

OSPF がトポロジ変更を受信してから Shortest Path First（SPF）計算を開始するまでの遅延時間を設定できます。また、2 つの SPF 計算の間のホールド タイムも設定できます。

OSPF オンデマンド回路は OSPF プロトコルの拡張機能で、ISDN、X.25 相手先選択接続（SVC）、ダイヤルアップ回線などのオンデマンド回路で効率的に操作が利用できるようになりました。この機能は RFC 1793「Extending OSPF to Support Demand Circuits」をサポートしています。

従来の規格では、OSPF の定期的 hello と LSA アップデートは、hello 情報や LSA 情報に変更が生じていなくても、オンデマンド リンクに接続しているルータ間で交換されていました。

この機能によって定期的 hello は抑制され、LSA の定期的リフレッシュはデマンド回線を通してフラッディングされません。これらのパケットが最初に交換されたときか、パケットに含まれる情報に変更が生じたときだけにリンクが発生します。この動作を使用すると、ネットワーク トポロジが安定している場合に、下位のデータリンク層を閉じることができます。

この機能は、在宅勤務者や支社を、中央にある OSPF バックボーンに接続する場合に有効です。このような場合、OSPF オンデマンド回路を使用すると、余計な接続コストをかけずにドメイン全体に OSPF の利点を適用できます。hello アップデート、LSA アップデート、および他のプロトコル オーバーヘッドの定期的リフレッシュは、送信する「実際の」データがない場合にオンデマンド回路をイネーブル化しなくなります。

hello や LSA などのオーバーヘッド プロトコルは、初期セットアップ時と、トポロジでの変更を反映するときだけ、オンデマンド回路を通じて転送されます。これにより、新しい SPF 計算を必要とするトポロジの重大な変更が、ネットワーク トポロジの整合性を維持するために送信されます。ただし、変更を含まない定期的リフレッシュはリンクにまたがって送信されません。

OSPF LSA グループ ペーシング機能により、ルータで OSPF LSA をグループ化し、リフレッシュ、チェックサム、およびエージングの各機能を同期することが可能となります。グループ ペーシングを利用すると、ルータをより効率的に使用することができます。

ルータは OSPF LSA をグループ化し、CPU およびネットワーク リソースの使用量の急激な増加を防ぐため、これらの機能をペーシングします。この機能は大規模な OSPF ネットワークで最も効力を発揮します。

OSPF の LSA グループ ペーシングはデフォルトでイネーブルです。リフレッシュ、チェックサム、およびエージングのグループペーシングインターバルは、通常、デフォルトの設定で十分なので、この機能を設定する必要がありません。

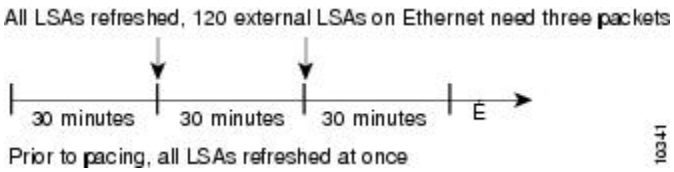
以前の LSA の動作

各 OSPF LSA には、LSA が有効であるかどうかを示すエージが設定されています。最大エージ（1 時間）に達した LSA は、廃棄されます。エージング プロセス中に、発信元ルータから 30 分ごとにリフレッシュ パケットが送信され、LSA がリフレッシュされます。リフレッシュ パケットは LSA の有効性を保持するために送信されるので、ネットワーク トポロジが変更されたかどうかは関係ありません。チェックサムはすべての LSA で 10 分おきに実行されます。ルータは、生成した LSA と、他のルータから受信した LSA を、継続的に追跡します。ルータが自分で生成した LSA はリフレッシュし、他のルータから受信した LSA はエージングします。

LSA グループ ペーシング機能が実装されるまで、Cisco ソフトウェアでは、リフレッシュ用に 1 つのタイマーを使用し、チェックサムとエージング用にもう 1 つのタイマーを使用していました。たとえば、リフレッシュの場合には、30 分ごとにデータベース全体がスキャンされ、経過時間に関係なく、ルータが生成したすべての LSA がリフレッシュされます。次の図に、すべての LSA の同時リフレッシュを示します。リフレッシュが必要なのはデータベースのごく一部であるにも

かかわらず、このプロセスは、かなりの CPU リソースを消費しました。大型の OSPF データベース（千単位の LSA 数）では、エージの異なる何千もの LSA が存在することになります。単一タイマーを使用したリフレッシュでは、すべての LSA のエージが同期化されるので、CPU の処理量が一度に増加する結果になります。LSA 数が膨大な場合には、ネットワーク トラフィックが急増し、短時間の間に大量のネットワーク リソースが消費されます。

図 *2*：グループ ペーシングを使用しない単一タイマーによる *OSPF LSA*



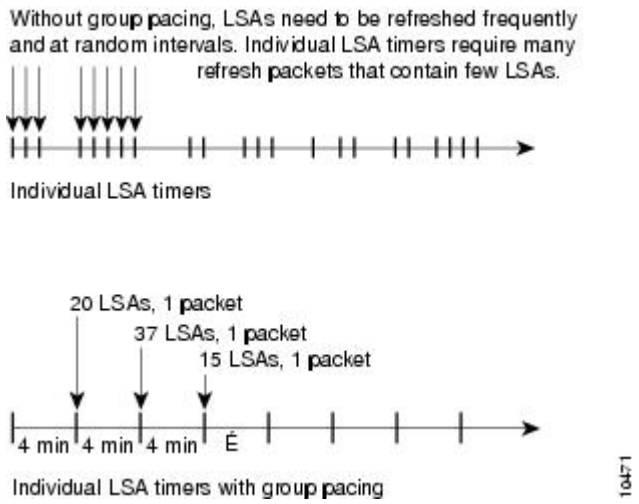
複数のタイマーを使用する LSA グループ ペーシング

各 LSA が独自のタイマーを持つように設定すると、過剰な CPU の処理や突然のネットワーク トラフィックの増加が回避されます。リフレッシュの例を再び使用するため、他の LSA とは関係なく、30 分が経過した時点で各 LSA をリフレッシュします。したがって、CPU は必要な場合にのみ使用されます。ただし、LSA をランダムな間隔で頻繁にリフレッシュしたのでは、ルータがリフレッシュして送信しなければならない少数の LSA に対して多数のパケットが必要になり、帯域幅を効率的に使用できません。

そのためルータは、個々のタイマーが指定時間を経過したとき、すぐに LSA のリフレッシュを実行するのではなく、一定時間だけリフレッシュ機能を保留します。この時間に累積された LSA をグループ化し、リフレッシュを実行して、1 つまたは複数のパケットで送出します。その結果、リフレッシュ パケットは、チェックサムおよびエージングと同時にペーシングされます。ペーシングの間隔は設定可能ですが、デフォルトは 4 分間です。さらに、同時実行を避けるためにランダム化されます。

次の図は、リフレッシュ パケットの場合を示しています。最初のタイムラインは、個別のLSA タイマーを示しています。2 つ目のタイムラインは、個別の LSA タイマーにグループ ペーシングを適用したものです。

図 *3*：個別タイマーとグループ ペーシングを使用した *OSPF LSA*



グループ ペーシングの間隔は、ルータがリフレッシュ、チェックサム、およびエージングを行う LSA の数と反比例します。たとえば、LSA 数が約 10,000 の場合には、ペーシング間隔を短くしたほうが効果的です。小さなデータベース（40 ～ 100 LSA）を使用する場合は、ペーシング インターバルを長くし、10 ～ 20 分に設定してください。

LSA グループ ペーシングのデフォルト値は、240 秒（4 分）です。値の範囲は、10～1800 秒（30 分）です。

デフォルトでは、OSPF は、LSA が到着したインターフェイスを除き、同じエリア内のすべてのインターフェイスで新しいLSA をフラッドします。確実なフラッディングを行うには、ある程度の冗長設定が必要になります。ただし、過度の冗長設定は帯域幅を浪費することになり、フルメッシュ型トポロジなどの特定のトポロジでは、リンク数とCPU使用率の超過によりネットワークが不安定になることがあります。この例としては完全メッシュ トポロジがあります。

OSPF の LSA フラッディングは、ネットワークのタイプに応じて、2 つの方法でブロックすることができます。

- ブロードキャスト、非ブロードキャスト、およびポイントツーポイントのネットワークでは、特定の OSPF インターフェイス上でフラッディングをブロックできます。
- ポイントツーマルチポイント ネットワークの場合には、指定したネイバーに対してフラッディングをブロックできます。

インターネットの成長により、OSPF などの IGP のスケーラビリティの重要性が高まっています。設計上、OSPF では、3,600 秒後に期限切れになる LSA をリフレッシュする必要があります。一部の実装ではリフレッシュの頻度を 30 分から約 50 分に減らして、フラッディングを改善しようとしてきました。このソリューションにより、リフレッシュのトラフィック量は減りますが、LSA の期限が切れるまでに最低1度はリフレッシュが必要になります。OSPFフラッディングを低減す

るソリューションでは、既知の変更されていない情報に対する、不要なリフレッシュとフラッディングの抑制が行われます。この低減を実現するため、LSA は現在フラッディング時に上位ビットが設定されます。LSA は現在「do not age」と設定されています。

Cisco ルータは、LSA タイプ 6 Multicast OSPF（MOSPF）をサポートしていません。ルータはこれらのパケットを受信すると、Syslog メッセージを生成します。ルータが多数の MOSPF パケットを受信している場合、パケットを無視するようにルータを設定して、大量の syslog メッセージが生成されないようにすることが必要な場合があります。

アップデート パケットを送信する OSPF の従来の実装は、効率面に改善の余地があります。リンクが低速の状態でアップデート パケットの一部が失われたり、ネイバーがアップデートを十分すばやく受信できなくなったり、あるいは、ルータがバッファ スペースを使い切ってしまったりすることがあります。たとえば、次のいずれかのトポロジが存在した場合にパケットがドロップされる可能性があります。

- 高速のルータがポイントツーポイント リンクを介して低速のルータと接続している。
- フラッディング中に、複数のネイバーから 1 台のルータに同時にアップデートが送信される。

OSPF アップデート パケットは自動的に同期されるようになり、33 ミリ秒未満の間隔で送信されます。ペーシングは、再送信間でも、送信効率を高めて再送信パケットの損失を最小にするために利用されます。インターフェイスへの送信を待機している LSA を表示することもできます。ペーシングの利点は、OSPF アップデートおよび再送信パケットの送信の効率をよくすることです。この機能を設定するタスクはありません。自動的に行われます。

IP ルーティング テーブルの内容、キャッシュの内容、およびデータベースの内容など、特定の統計情報を表示できます。提供される情報は、リソースの使用状況を判定してネットワークの問題を解決するために使用されます。また、ノードの到達可能性情報を表示して、デバイス パケットがネットワークを通過するときにとるルーティング パスを見つけることもできます。

OSPF の設定方法

OSPF を設定するには、ここで説明するタスクを実行します。「OSPF のイネーブル化」の項にあるタスクは必須です。残りの項のタスクは任意ですが、ご使用のアプリケーションによっては必須の場合もあります。インターフェイスの最大数については、「OSPF の制約事項」の項を参照してください。

OSPF のイネーブル化

手順の概要

1. イネーブル化
2. **configureterminal**
3. **router ospf***process-id*
4. **network***ip-addresswildcard-mask***area***area-id*
5. **end**

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	**configureterminal** 例： `Device# 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	**router ospf***process-id* 例： `Device(config)# router ospf 109`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**network***ip-addresswildcard-mask***area***area-id* 例： `Device(config-router)# network 192.168.129.16 0.0.0.3 area 20`	OSPF を実行するインターフェイスを定義し、そのインターフェイスに対するエリア ID を定義します。
ステップ 5	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

OSPF インターフェイス パラメータの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipospfcost***cost*
5. **ipospfretransmit-interval***seconds*
6. **ipospftransmit-delay***seconds*
7. **ipospfpriority***number-value*
8. **ipospfhello-interval***seconds*
9. **ipospfdead-interval***seconds*
10. **ipospfauthentication-key***key*
11. **ipospfmessage-digest-key***key-id***md5***key*
12. **ipospfauthentication** [**message-digest** | **null**]
13. **end**

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	**configureterminal** 例： `Device# 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	**interface***typenumber* 例： `Device(config)# interface Gigabitethernet 0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipospfcost***cost* 例： `Device(config-if)# ip ospf cost 65`	OSPF インターフェイスでパケットを送信するコストを明示的に指定します。

	コマンドまたはアクション	目的
ステップ 5	**ipospfretransmit-interval***seconds* 例： `Device(config-if)# ip ospf retransmit-interval 1`	OSPF インターフェイスに属する隣接に対してリンクステートアドバタイズメント（LSA）が再送信される間隔の秒数を指定します。
ステップ 6	**ipospftransmit-delay***seconds* 例： `Device(config-if)# ip ospf transmit-delay`	OSPF インターフェイスでリンクステート アップデート パケットを送信するために必要な予想時間を秒単位で設定できます。
ステップ 7	**ipospfpriority***number-value* 例： `Device(config-if)# ip ospf priority 1`	ネットワークの OSPF 指定ルータを確認するための優先順位を設定します。
ステップ 8	**ipospfhello-interval***seconds* 例： `Device(config-if)# ip ospf hello-interval 1`	OSPF インターフェイスで Cisco IOS ソフトウェアが 送信する hello パケットの間隔の時間を指定します。
ステップ 9	**ipospfdead-interval***seconds* 例： `Device(config-if)# ip ospf dead-interval 1`	デバイスが hello パケットを受信していないためネイバー OSPF ルータがダウンしていることを宣言するまでデバイスが待機する秒数を設定します。
ステップ 10	**ipospfauthentication-key***key* 例： `Device(config-if)# ip ospf authentication-key 1`	OSPF 簡易パスワード認証を使用しているネットワーク セグメント上で近接する OSPF ルータが使用するパスワードを割り当てます。
ステップ 11	**ipospfmessage-digest-key***key-id***md5***key* 例： `Device(config-if)# ip ospf message-digest-key 1 md5 23456789`	OSPF Message Digest 5（MD5）認証をイネーブルにします。*key-id* および *key* 引数の値は、ネットワーク セグメント上の他のネイバーに対して指定された値と一致している必要があります。

	コマンドまたはアクション	目的
ステップ 12	**ipospfauthentication** [**message-digest** | **null**] 例： `Device(config-if)# ip ospf authentication message-digest`	インターフェイスの認証タイプを指定します。
ステップ 13	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。

さまざまな物理ネットワークでの OSPF の設定

ポイントツーマルチポイント ブロードキャスト ネットワーク用 OSPF の設定

手順の概要

1. **configureterminal**
2. **interface***typenumber*
3. **ipospfnetworkpoint-to-multipoint**
4. **exit**
5. **routerospf***process-id*
6. **neighbor***ip-address* [**cost***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	**configureterminal** 例： `Device# 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 2	**interface***typenumber* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipospfnetworkpoint-to-multipoint** 例： `Device#(config-if) ip ospf network point-to-multipoint`	インターフェイスをブロードキャスト メディアのポイントツーマルチポイントとして設定します。
ステップ 4	**exit** 例： `Device#(config-if) exit`	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 5	**routerospf***process-id* 例： `Device#(config) router ospf 109`	OSPF ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 6	**neighbor***ip-address* [**cost***number*] 例： `Device#(config-router) neighbor 192.168.3.4 cost 180`	ネイバーを指定して、このネイバーにコストを割り当てます。 （注） コストを指定するネイバーごとに、このステップを繰り返します。それ以外の場合、ネイバーは **ipospfcost** インターフェイス コンフィギュレーション コマンドに基づいてインターフェイスのコストを推測します。

非ブロードキャスト ネットワークの OSPF の設定

手順の概要

1. **configureterminal**
2. **interface***typenumber*
3. **ipospfnetworkpoint-to-multipointnon-broadcast**
4. **exit**
5. **routerospf***process-id*
6. **neighbor***ip-address* [**cost***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	**configureterminal** 例： `Device# 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 2	**interface***typenumber* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ipospfnetworkpoint-to-multipointnon-broadcast** 例： `Device#(config-if) ip ospf network point-to-multipoint non-broadcast`	インターフェイスを非ブロードキャスト メディアのポイントツーマルチポイントとして設定します。
ステップ 4	**exit** 例： `Device#(config-if) exit`	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 5	**routerospf***process-id* 例： `Device#(config) router ospf 109`	OSPF ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 6	**neighbor***ip-address* [**cost***number*] 例： `Device#(config-router) neighbor 192.168.3.4 cost 180`	ネイバーを指定して、このネイバーにコストを割り当てます。 （注） コストを指定するネイバーごとに、このステップを繰り返します。それ以外の場合、ネイバーは **ipospfcost** インターフェイス コンフィギュレーション コマンドに基づいてインターフェイスのコストを推測します。

OSPF エリア パラメータの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id*
4. **area***area-id***authentication**
5. **area***area-id***stub** [**no summary**]
6. **area***area-id***default-cost***cost***
7. **end**

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	**configureterminal** 例： `Device# 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	**routerospf***process-id* 例： `Device(config)# router ospf 10`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**area***area-id***authentication** 例： `Device(config-router)# area 10.0.0.0 authentication`	OSPF エリアの認証をイネーブルにします。
ステップ 5	**area***area-id***stub** [**no summary**] 例： `Device(config-router)# area 10.0.0.0 stub no-summary`	エリアをスタブ エリアとして定義します。

	コマンドまたはアクション	目的
ステップ 6	**area***area-id***default-cost***cost* 例： `Device(config-router)# area 10.0.0.0 default-cost 1`	スタブ エリアまたは Not-So-Stubby エリア（NSSA）に送信されるデフォルト集約ルートのコストを指定します。
ステップ 7	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

OSPFv2 NSSA の設定

OSPFv2 NSSA エリアとそのパラメータの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router ospf***process-id*
4. **redistribute***protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*autonomous-system-number*] **[metric** {**metric-value** | **transparent**}] [**metric-type***type-value*] [**match** {**internal** | **external1** | **external2**}] [**tag***tag-value*] [**route-map***map-tag*] [**subnets**] [**nssa-only**]
5. **network***ip-address wildcard-mask* **area***area-id*
6. **area***area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric**] [**metric-type**]] [**no-summary**] [**nssa-only**]
7. **summary-address***prefix mask* [**not-advertise**] [**tag** *tag*] [**nssa-only**]
8. **end**

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）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# 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	**routerospf***process-id* 例： `Device(config)# router ospf 10`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。 • *process-id* 引数は OSPF プロセスを示します。有効な範囲は 1 ～ 65535 です。
ステップ 4	**redistribute***protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*autonomous-system-number*] **[metric** {**metric-value** | **transparent**}] [**metric-type***type-value*] [**match** {**internal** | **external1** | **external2**}] [**tag***tag-value*] [**route-map***map-tag*] [**subnets**] [**nssa-only**] 例： `Device(config-router)# redistribute rip subnets`	あるルーティング ドメインから別のルーティング ドメインへルートを再配布します。 • 例では、Routing Information Protocol（RIP）サブネットが OSPF ドメインに再配布されます。
ステップ 5	**network***ip-addresswildcard-mask***area***area-id* 例： `Device(config-router)# network 192.168.129.11 0.0.0.255 area 1`	OSPF が実行するインターフェイスと、それらのインターフェイスに対するエリア ID を定義します。
ステップ 6	**area***area-id***nssa**[**no-redistribution**] [**default-information-originate** [**metric**] [**metric-type**]] [**no-summary**] [**nssa-only**] 例： `Device(config-router)# area 1 nssa`	Not-So-Stubby Area（NSSA）エリアを設定します。
ステップ 7	**summary-address***prefix mask*[**not-advertise**] [**tag** *tag*] [**nssa-only**] 例： `Device(config-router)# summary-address 10.1.0.0 255.255.0.0 not-advertise`	変換時にルート集約とフィルタリングを制御し、NSSA エリアへの集約を制限します。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

強制 NSSA LSA トランスレータとしての NSSA ABR の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id*
4. **area***area-id***nssatranslate type7always**
5. **area***area-id***nssatranslate type7suppress-fa**
6. **end**

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	**configureterminal** 例： `Device# 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	**routerospf***process-id* 例： `Device(config)# router ospf 1`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。 • *process-id* 引数は OSPF プロセスを示します。有効な範囲は 1 ～ 65535 です。

	コマンドまたはアクション	目的
ステップ 4	**area***area-id***nssatranslate type7always** 例： `Device(config-router)# area 10 nssa translate type7 always`	Not-So-Stubby Area エリア境界ルータ（NSSA ABR）デバイスを、強制 NSSA リンクステート アドバタイズメント（LSA）トランスレータとして設定します。 （注） **areanssatranslate** コマンドで **always** キーワードを使用することにより、NSSA ABR デバイスを強制 NSSA LSA トランスレータとして設定できます。このコマンドは、RFC 3101 がディセーブルで RFC 1587 を使用している場合に使用できます。
ステップ 5	**area***area-id***nssatranslate type7suppress-fa** 例： `Device(config-router)# area 10 nssa translate type7 suppress-fa`	変換後のタイプ 5 LSA で ABR がフォワーディング アドレスを抑制できるようにします。
ステップ 6	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

RFC 3101 互換性のディセーブル化と RFC 1587 互換性のイネーブル化

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id*
4. **compatiblerfc1587**
5. **end**

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： `Device> 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： `Device# 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	**routerospf***process-id* 例： `Device(config)# router ospf 1`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。 • *process-id* 引数は OSPF プロセスを示します。 • OSPFv2 ルーティングをイネーブルにするには、**router ospf***process-id* コマンドを使用します。
ステップ 4	**compatiblerfc1587** 例： `Device(config-router)# compatible rfc1587`	デバイスをイネーブルにして RFC 1587 準拠にします。
ステップ 5	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

OSPF NSSA パラメータの設定

前提条件

この機能を実装する前に、次の注意事項を検討してください。

- 外部の宛先に到達するために使用可能なタイプ 7 のデフォルト ルートを設定できます。設定すると、デバイスはタイプ 7 デフォルトを Not-So-Stubby Area（NSSA）または NSSA エリア境界ルータ（ABR）に生成します。
- 同じエリア内のすべてのデバイスは、エリアが NSSA であることを認識する必要があります。そうでない場合、デバイスは通信できません。

OSPF エリア間のルート集約の設定

OSPF にルートを再配布する場合のルート集約の設定

手順の概要

1. **summary-address** {*ip-addressmask* | *prefixmask*} [**not-advertise**][**tag***tag* [**nssa-only**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**summary-address** {*ip-addressmask* | *prefixmask*} [**not-advertise**][**tag***tag* [**nssa-only**] 例： `Device#(config-router) summary-address 10.1.0.0 255.255.0.0`	再配布ルートをカバーするアドレスとマスクを指定します。1 つの要約ルートだけがアドバタイズされます。 • 任意指定の **not-advertise** キーワードを使用すると、一連のルートをフィルタリングすることができます。

仮想リンクの確立

手順の概要

1. **area***area-id***virtual-link***router-id* [**authentication**[**message-digest**|**null**]][**hello-interval***seconds*] [**retransmit-interval***seconds*] [**transmit-delay***seconds*] [**dead-interval***seconds*] [**authentication-key***key* | **message-digest-key***key-id***md5***key*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**area***area-id***virtual-link***router-id* [**authentication**[**message-digest**|**null**]][**hello-interval***seconds*] [**retransmit-interval***seconds*] [**transmit-delay***seconds*] [**dead-interval***seconds*] [**authentication-key***key*	**message-digest-key***key-id***md5***key*] 例： `Device(config-router-af)# area 1 virtual-link 10.1.1.1 router1`	仮想リンクを確立します。

デフォルト ルートの生成

手順の概要

1. イネーブル化
2. **configureterminal**
3. **router ospf***process-id*
4. **default-informationoriginate** [**always**] [**metric***metric-value*] [**metric-type***type-value*] [**route-map***map-name*]
5. **end**

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	**configureterminal** 例： `Device# 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	**router ospf***process-id* 例： `Device(config)# router ospf 109`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**default-informationoriginate** [**always**] [**metric***metric-value*] [**metric-type***type-value*] [**route-map***map-name*] 例： `Device(config-router)# default-information originate always`	ASBR を設定し、強制的に OSPF ルーティング ドメインにデフォルト ルートを生成できます。 （注） ルートマップを使用する場合、キーワード **always** には次の例外が含まれます。ルートマップを使用する場合、OSPF によるデフォルト ルートの送信は、ルーティング テーブル内にデフォルト ルートが存在するかどうかによって制限されません。
ステップ 5	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

DNS 名ルックアップの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipospfname-lookup**
4. **end**

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	**configureterminal** 例： `Device# 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	**ipospfname-lookup** 例： `Device# ip ospf name-lookup`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル 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。

ループバック インターフェイスによる強制的ルータ ID 選択

手順の概要

1. **configureterminal**
2. **interface***typenumber*
3. **ipaddress** *ip-addressmask*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# 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 2	**interface***typenumber* 例： `Device(config)# interface loopback 0`	ループバック インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ipaddress** *ip-addressmask* 例： `Device#(config-if) ip address 192.108.1.27 255.255.255.0`	このインターフェイスに IP アドレスを割り当てます。

デフォルト メトリックの制御

手順の概要

1. イネーブル化
2. **configureterminal**
3. **router ospf***process-id*
4. **auto-costreference-bandwidth***ref-bw*
5. **end**

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	**configureterminal** 例： `Device# 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	**router ospf***process-id* 例： `Device# router ospf 109`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**auto-costreference-bandwidth***ref-bw* 例： `Device(config-router)# auto-cost reference-bandwidth 101`	帯域幅が広いリンクに差をつけます。
ステップ 5	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

OSPF アドミニストレーティブ ディスタンスの変更

手順の概要

1. イネーブル化
2. **configureterminal**
3. **router ospf***process-id*
4. **distanceospf** {**intra-area** | **inter-area** | **external**} *dist*
5. **end**

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	**configureterminal** 例： `Device# 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	**router ospf***process-id* 例： `Device(config)# router ospf 109`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**distanceospf** {**intra-area** | **inter-area** | **external**} *dist* 例： `Device(config-router)# distance ospf external 200`	OSPF ディスタンス値を変更します。
ステップ 5	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

シンプレックス イーサネット インターフェイスでの OSPF の設定

コマンド	目的
passive-interface *interface-type interface-number*	指定されたインターフェイスを通じた hello パケットの送信を抑止します。

ルート計算タイマーの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **router ospf***process-id*
4. **timersthrottlespf***spf-startspf-holdspf-max-wait*
5. **end**

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**	**configureterminal** 例： `Device# 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**	**router ospf***process-id* 例： `Device(config)# router ospf 109`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。
ステップ **4**	**timersthrottlespf***spf-startspf-holdspf-max-wait* 例： `Device(config-router)# timers throttle spf 5 1000 9000`	ルート計算タイマーを設定します。
ステップ **5**	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

OSPF over On-Demand 回路の設定

手順の概要

1. **router ospf***process-id*
2. **interface***type number*
3. **ip ospf demand-circuit**

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*	OSPF 動作をイネーブルにします。
ステップ 2	**interface***type number*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip ospf demand-circuit**	オンデマンド回路の OSPF を設定します。

次の作業

（注） **ignore** keyword in the **ipospfdemand-circuit** コマンドを指定することにより、インターフェイスが他のルータからデマンド回線要求を受け入れるのを防ぐことができます。

前提条件

オンデマンド回路機能を実装する前に、以下の考慮事項を評価します。

- トポロジの変更を含む LSA はオンデマンド回路を通してフラッディングされるため、OSPF スタブエリア内やNSSA 内にデマンド回路を設置して、できるだけ多くのトポロジの変更から隔離しておくべきです。
- スタブエリアまたはNSSA 内のすべてのルータでは、オンデマンド回路の機能を利用するためにこの機能がロードされている必要があります。この機能が 1 つの通常エリア内に実装される場合、タイプ 5 外部 LSA がすべてのエリアを通してフラッディングされるため、デマンド回線機能が反映される前に他のすべての通常エリアもこの機能をサポートする必要があります。
- ハブ上にポイントツーマルチポイント（P2MP）OSPF インターフェイス タイプを備えたハブアンドスポーク ネットワーク トポロジは、必要なときにオンデマンド以外の回路に戻らな

い場合があります。デマンド回路モードから非デマンド回路モードへ戻る場合、P2MP セグメントのすべてのインターフェイスで、OSPF を同時に再設定する必要があります。

- ブロードキャスト ベースのネットワーク トポロジではこの機能を実装しないでください。hello パケットや LSA パケットなどのオーバーヘッド プロトコルが正常に抑制できないためです。リンクはそのまま残ります。
- 非同期インターフェイスによる OSPF オンデマンド回路用ルータの設定はサポートされていません。回路の両側でダイヤルインターフェイスを使用する設定はサポートされています。詳細については、「Why OSPF Demand Circuit Keeps Bringing Up the Link」を参照してください。

ネイバーの起動と停止のロギング

手順の概要

1. イネーブル化
2. **configureterminal**
3. **router ospf***process-id*
4. **log-adjacency-changes** [**detail**]
5. **end**

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	**configureterminal** 例： `Device# 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	**router ospf***process-id* 例： `Device(config)# router ospf 109`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**log-adjacency-changes** [**detail**] 例： `Device(config-router)# log-adjacency-changes detail`	LSA の グループ ペーシングを変更します。 （注） **debugipospfadjacency** EXEC コマンドを実行しないで、OSPF ネイバーが起動または停止したことを確認する必要がある場合、**log-adjacency-changes** コマンドを設定します。**log-adjacency-changes** コマンドでは、少ない出力でピアの関係を高レベルで表示するためです。それぞれの状態変化メッセージを確認する場合は、**log-adjacency-changesdetail** コマンドを設定します。
ステップ 5	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

LSA グループ ペーシング インターバルの変更

手順の概要

1. イネーブル化
2. **configureterminal**
3. **router ospf***process-id*
4. **timerspacinglsa-group***seconds*
5. **end**

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	**configureterminal** 例： `Device# 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	**router ospf***process-id* 例： `Device(config)# router ospf 109`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**timerspacinglsa-group***seconds* 例： `Device(config-router)# timers pacing lsa-group 60`	LSA の グループ ペーシングを変更します。
ステップ 5	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

OSPF LSA フラッディングのブロック

コマンド	目的
ip ospf database-filter all out	インターフェイスへの OSPF LSA パケットのフラッディングをブロックします。

ポイントツーマルチポイント ネットワークで、OSPF の LSA フラッディングをブロックするには、ルータ 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。

コマンド	目的
neighbor *ip-address* **database-filter all out**	指定したネイバーへの OSPF LSA パケットのフラッディングをブロックします。

LSA フラッディングの低減

コマンド	目的
ip ospf flood-reduction	安定したトポロジで LSA の不要なフラッディングを抑止します。

MOSPF LSA パケットの無視

コマンド	目的
ignore lsa mospf	MOSPF LSA パケットを受信したとき、ルータが Syslog メッセージを生成しないように設定します。

OSPF のモニタリングおよびメンテナンス

コマンド	目的
show ip ospf [*process-id*]	OSPF ルーティング プロセスに関する一般情報を表示します。
show ip ospf border-routers	ABR および ASBR までの内部 OSPF ルーティング テーブル エントリを表示します。
	OSPF データベースに関連する情報のリストを表示します。

コマンド	目的
show ip ospf [*process-id* [*area-id*]] **database** **show ip ospf** [*process-id* [*area-id*]] **database** [**database-summary**] **show ip ospf** [*process-id* [*area-id*]] **database** [**router**] [**self-originate**] **show ip ospf** [*process-id* [*area-id*]] **database** [**router**] [**adv-router** [*ip-address*]] **show ip ospf** [*process-id* [*area-id*]] **database** [**router**] [*link-state-id*] **show ip ospf** [*process-id* [*area-id*]] **database** [**network**] [*link-state-id*] **show ip ospf** [*process-id* [*area-id*]] **database** [**summary**] [*link-state-id*] **show ip ospf** [*process-id* [*area-id*]] **database** [**asbr-summary**] [*link-state-id*] **show ip ospf** [*process-id* [Router# *area-id*]] **database** [**external**] [*link-state-id*] **show ip ospf** [*process-id* [*area-id*]] **database** [**nssa-external**] [*link-state-id*] **show ip ospf** [*process-id* [*area-id*]] **database** [**opaque-link**] [*link-state-id*] **show ip ospf** [*process-id* [*area-id*]] **database** [**opaque-area**] [*link-state-id*] **show ip ospf** [*process-id* [*area-id*]] **database** [**opaque-as**] [*link-state-id*]	
show ip ospf flood-list interface *type*	（OSPF パケット ペーシングの観察のため）インターフェイスへのフラッディングを待機している LSA のリストを表示します。

コマンド	目的
show ip ospf interface [*type number*]	OSPF に関連するインターフェイス情報を表示します。
show ip ospf neighbor [*interface-name*] [*neighbor-id*] **detail**	OSPF ネイバー情報をインターフェイスごとに表示します。
show ip ospf request-list [*neighbor*] [*interface*] [*interface-neighbor*]	ルータで要求されるすべてのLSAのリストを表示します。
show ip ospf retransmission-list [*neighbor*] [*interface*] [*interface-neighbor*]	再送信を待機しているすべてのLSA のリストを表示します。
show ip ospf [*process-id*] **summary-address**	OSPF プロセスで設定されているサマリー アドレスのすべての再配布情報のリストを表示します。
show ip ospf virtual-links	OSPF に関連する仮想リンク情報を表示します。

OSPF プロセスを再起動するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
clear ip ospf [*pid*] {**process** | **redistribution** | **counters** [**neighbor** [**neighbor -** *interface*] [*neighbor-id*]]*}*	OSPF ルーティング プロセス ID に基づいて再配布をクリアします。*pid* オプションを指定しなかった場合、すべての OSPF プロセスがクリアされます。

OSPF アップデート パケットのペーシングの表示

手順の概要

1. **showipospfflood-list***interface-typeinterface-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	**showipospfflood-list***interface-typeinterface-number* 例： `Device> show ip ospf flood-list ethernet 1`	インターフェイス上でのフラッディングを待機している OSPF LSA のリストを表示します。

OSPF の制約事項

システムに数多くのインターフェイスがあると、ルータ LSA でアドバタイズされるリンクの数により、リンクステート アップデート パケットが「huge」Cisco バッファ サイズを超過するように OSPF が設定されることがあります。この問題を解決するには、OSPF リンクの数を減らすか、**buffershugesize***size* コマンドを入力して huge バッファ サイズを増やします。

ルータ LSA が含まれるリンクステート アップデート パケットは、通常 196 バイトの固定オーバーヘッドがあり、個々のリンクの説明に追加の 12 バイトが必要です。「huge buffer size」が 18024 バイトの場合、最大 1485 個のリンクの説明が用意できます。

IP パケットの最大サイズは 65,535 バイトであるため、ルータに用意できるリンクの数の上限はまだ大きくできます。

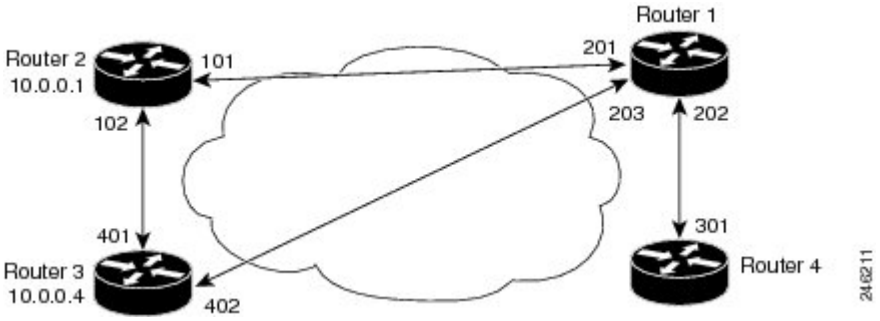
OSPF の設定例

例：OSPF ポイントツーマルチポイント

次の図で、ルータ 1 は、データリンク接続識別子（DLCI）201 を使用してルータ 2 と、DLCI 202 を使用してルータ 4 と、DLCI 203 を使用してルータ 3 と通信します。ルータ 2 は、DLCI 101 を使用してルータ 1 と、DLCI 102 を使用してルータ 3 と通信します。ルータ 3 は、ルータ 2（DLCI

401）およびルータ 1（DLCI 402）と通信します。ルータ 4 は、ルータ 1（DLCI 301）と通信します。設例を図の次に示します。

図 *4*：*OSPF* ポイントツーマルチポイントの例



ルータ 1 の設定

```
hostname Router 1
!
interface serial 1
 ip address 10.0.0.2 255.0.0.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 frame-relay map ip 10.0.0.1 201 broadcast
 frame-relay map ip 10.0.0.3 202 broadcast
 frame-relay map ip 10.0.0.4 203 broadcast
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
```

ルータ 2 設定

```
hostname Router 2
!
interface serial 0
 ip address 10.0.0.1 255.0.0.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 frame-relay map ip 10.0.0.2 101 broadcast
 frame-relay map ip 10.0.0.4 102 broadcast
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
```

ルータ 3 の設定

```
hostname Router 3
!
interface serial 3
 ip address 10.0.0.4 255.0.0.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 clock rate 1000000
 frame-relay map ip 10.0.0.1 401 broadcast
 frame-relay map ip 10.0.0.2 402 broadcast
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
```

ルータ 4 の設定

```
hostname Router 4
!
interface serial 2
 ip address 10.0.0.3 255.0.0.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 clock rate 2000000
 frame-relay map ip 10.0.0.2 301 broadcast
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
```

例：ブロードキャストを行う OSPF ポイントツーマルチポイント

次に、ブロードキャストを行うポイントツーマルチポイント ネットワークの例を示します。

```
interface Serial0
 ip address 10.0.1.1 255.255.255.0
 encapsulation frame-relay
 ip ospf cost 100
 ip ospf network point-to-multipoint
 frame-relay map ip 10.0.1.3 202 broadcast
 frame-relay map ip 10.0.1.4 203 broadcast
 frame-relay map ip 10.0.1.5 204 broadcast
 frame-relay local-dlci 200
!
router ospf 1
 network 10.0.1.0 0.0.0.255 area 0
 neighbor 10.0.1.5 cost 5
 neighbor 10.0.1.4 cost 10
```

次に、10.0.1.3 におけるネイバーの設定例を示します。

```
interface serial 0
 ip address 10.0.1.3 255.255.255.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 frame-relay local-dlci 301
 frame-relay map ip 10.0.1.1 300 broadcast
 no shutdown
!
 router ospf 1
 network 10.0.1.0 0.0.0.255 area 0
```

最初の設定でのネイバーの出力は、次のとおりです。

```
Device# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.1.1        1   FULL/  -        00:01:50    10.0.1.5        Serial0
172.16.1.4        1   FULL/  -        00:01:47    10.0.1.4        Serial0
172.16.1.8        1   FULL/  -        00:01:45    10.0.1.3        Serial0
```

最初の設定のルート情報は、次のとおりです。

```
Device# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
Gateway of last resort is not set
C    1.0.0.0/8 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O       10.0.1.3/32 [110/100] via 10.0.1.3, 00:39:08, Serial0
```

```
C       10.0.1.0/24 is directly connected, Serial0
O       10.0.1.5/32 [110/5] via 10.0.1.5, 00:39:08, Serial0
O       10.0.1.4/32 [110/10] via 10.0.1.4, 00:39:08, Serial0
```

例：非ブロードキャストの OSPF ポイントツーマルチポイント

次に、非ブロードキャストのポイントツーマルチポイント ネットワークの例を示します。

```
interface Serial0
 ip address 10.0.1.1 255.255.255.0
 ip ospf network point-to-multipoint non-broadcast
 encapsulation frame-relay
 no keepalive
 frame-relay local-dlci 200
 frame-relay map ip 10.0.1.3 202
 frame-relay map ip 10.0.1.4 203
 frame-relay map ip 10.0.1.5 204
 no shutdown
 !
 router ospf 1
  network 10.0.1.0 0.0.0.255 area 0
  neighbor 10.0.1.3 cost 5
  neighbor 10.0.1.4 cost 10
  neighbor 10.0.1.5 cost 15
```

次に、相手側のルータの設定例を示します。

```
interface Serial9/2
 ip address 10.0.1.3 255.255.255.0
 encapsulation frame-relay
 ip ospf network point-to-multipoint non-broadcast
 no ip mroute-cache
 no keepalive
 no fair-queue
 frame-relay local-dlci 301
 frame-relay map ip 10.0.1.1 300
 no shutdown
 !
 router ospf 1
  network 10.0.1.0 0.0.0.255 area 0
```

最初の設定でのネイバーの出力は、次のとおりです。

```
Device# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.1.1        1   FULL/  -        00:01:52    10.0.1.5        Serial0
172.16.1.4        1   FULL/  -        00:01:52    10.0.1.4        Serial0
172.16.1.8        1   FULL/  -        00:01:52    10.0.1.3        Serial0
```

例：可変長サブネット マスク

OSPF、スタティック ルート、および IS-IS は、VLSM をサポートします。VLSM により、異なるインターフェイスの同じネットワーク番号に別のマスクを使用できるため、IPアドレスを維持し、使用可能なアドレス空間をより効率的に使用できます。

次の例では、30 ビット サブネット マスクが使用され、2 ビットのアドレス空間はシリアル回線のホスト アドレス用に予約されています。ポイントツーポイント シリアル リンク上の 2 つのホスト エンドポイントには、十分なホスト アドレス空間があります。

```
interface ethernet 0
```

```
 ip address 172.16.10.1 255.255.255.0
! 8 bits of host address space reserved for ethernets
interface serial 0
 ip address 172.16.20.1 255.255.255.252
! 2 bits of address space reserved for serial lines
! Router is configured for OSPF and assigned AS 107
router ospf 107
! Specifies network directly connected to the router
 network 172.16.0.0 0.0.255.255 area 0.0.0.0
```

例：OSPF NSSA の設定

次の例では、Open Shortest Path First（OSPF）スタブ ネットワークは 5 台のデバイスを使用して、OSPF エリア 0 と OSPF エリア 1 を組み込むように設定されています。デバイス 3 は、NSSA の自律システム境界ルータ（ASBR）として設定されています。デバイス 2 は、NSSA のエリア境界ルータ（ABR）として設定されています。OSPF エリア 1 は、Not-So-Stubby Area（NSSA）として定義されています。

デバイス 1

```
hostname Device1
!
interface Loopback1
 ip address 10.1.0.1 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.0.1 255.255.255.0
 ip ospf 1 area 0
 no cdp enable
!
interface Serial10/0
 description Device2 interface s11/0
 ip address 192.168.10.1 255.255.255.0
 ip ospf 1 area 1
 serial restart-delay 0
 no cdp enable
!
router ospf 1
 area 1 nssa
!
end
```

デバイス 2

```
hostname Device2
!
!
interface Loopback1
 ip address 10.1.0.2 255.255.255.255
!
interface Serial10/0
 description Device1 interface s11/0
 no ip address
 shutdown
 serial restart-delay 0
 no cdp enable
!
interface Serial11/0
 description Device1 interface s10/0
 ip address 192.168.10.2 255.255.255.0
 ip ospf 1 area 1
 serial restart-delay 0
 no cdp enable
```

```
!
interface Serial14/0
 description Device3 interface s13/0
 ip address 192.168.14.2 255.255.255.0
 ip ospf 1 area 1
 serial restart-delay 0
 no cdp enable
!
router ospf 1
 area 1 nssa
!
end
```

Device 3

```
hostname Device3
!
interface Loopback1
 ip address 10.1.0.3 255.255.255.255
!
interface Ethernet3/0
 ip address 192.168.3.3 255.255.255.0
 no cdp enable
!
interface Serial13/0
 description Device2 interface s14/0
 ip address 192.168.14.3 255.255.255.0
 ip ospf 1 area 1
 serial restart-delay 0
 no cdp enable
!
router ospf 1
 log-adjacency-changes
 area 1 nssa
 redistribute rip subnets
!
router rip
 version 2
 redistribute ospf 1 metric 15
 network 192.168.3.0
end
```

デバイス 4

```
hostname Device4
!
interface Loopback1
 ip address 10.1.0.4 255.255.255.255
!
interface Ethernet3/0
 ip address 192.168.3.4 255.255.255.0
 no cdp enable
!
interface Ethernet4/1
 ip address 192.168.41.4 255.255.255.0
!
router rip
 version 2
 network 192.168.3.0
 network 192.168.41.0
!
end
```

デバイス 5

```
hostname Device5
!
```

```
interface Loopback1
 ip address 10.1.0.5 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.0.10 255.255.255.0
 ip ospf 1 area 0
 no cdp enable
!
interface Ethernet1/1
 ip address 192.168.11.10 255.255.255.0
 ip ospf 1 area 0
!
router ospf 1
!
end
```

例：RFC 3101 がディセーブル、RFC 1587 がアクティブな OSPF NSSA

次の例では、**showipospf** および **showipospfdatabasenssa** コマンドの出力として、RFC 3101 がディセーブル、RFC 1587 がアクティブ、NSSA エリア境界ルータ（ABR）デバイスが強制 NSSA LSA トランスレータとして設定された Open Shortest Path First Not-So-Stubby（OSPF NSSA）エリアが表示されます。RFC 3101 をディセーブルの場合、強制 NSSA LSA トランスレータは非アクティブのままとなります。

```
Device# show ip ospf

Routing Process "ospf 1" with ID 10.0.2.1
Start time: 00:00:25.512, Time elapsed: 00:01:02.200
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 1587)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 0 normal 0 stub 1 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
Area 1
Number of interfaces in this area is 1
It is a NSSA area
Configured to translate Type-7 LSAs, inactive (RFC3101 support
disabled)
Area has no authentication
SPF algorithm last executed 00:00:07.160 ago
SPF algorithm executed 3 times
Area ranges are
Number of LSA 3. Checksum Sum 0x0245F0
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
```

```
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
```

次の表に、**showipospf** の表示フィールドとその説明を示します。

表 *1*：*show ip ospf* フィールドの説明

フィールド	説明
Supports NSSA (compatible with RFC 1587)	RFC 1587 がアクティブであること、つまり、OSPF NSSA エリアが RFC 1587 と互換性があることが指定されています。
Configured to translate Type-7 LSAs, inactive (RFC3101 support disabled)	OSPF NSSA エリアに、タイプ 7 LSA の強制トランスレータとして動作するよう設定された ABR デバイスが存在することが指定されています。ただし、RFC 3101 がディセーブルなため、このデバイスは非アクティブです。

```
Device2# show ip ospf database nssa

Router Link States (Area 1)
LS age: 28
Options: (No TOS-capability, DC)
LS Type: Router Links
Link State ID: 10.0.2.1
Advertising Router: 10.0.2.1
LS Seq Number: 80000004
Checksum: 0x5CA2
Length: 36
Area Border Router
AS Boundary Router
Unconditional NSSA translator
Number of Links: 1
Link connected to: a Stub Network
(Link ID) Network/subnet number: 192.0.2.5
(Link Data) Network Mask: 255.255.255.0
Number of MTID metrics: 0
TOS 0 Metrics: 10
```

次の表に、**showipospf database nssa** の表示フィールドとその説明を示します。

表 *2*：*show ip ospf database nssa* フィールドの説明

フィールド	説明
Unconditional NSSA translator	NSSA ASBR デバイスが強制 NSSA LSA トランスレータであることが指定されています。

例：OSPF ルーティングおよびルート再配布

通常、OSPF では多くの内部ルータ、ABR、および ASBR 間での調整が必要です。OSPF ベースのルータは最低でも、すべてのデフォルト パラメータ値を使用し、認証なしで、インターフェイスをエリアに割り当てて設定できます。

次に、3 つのタイプの例を示します。

- 最初の例は、基本的な OSPF コマンドを示した簡単な設定です。
- 2 番目の例は、単一の任意に割り当てられた OSPF 自律システム内での内部ルータ、ABR、および ASBR の設定を示しています。
- 3 番目の例は、より複雑な設定と、OSPF ベースのルーティング環境の制御で使用できるさまざまなツールの用途を示しています。

例：OSPF の基本設定

次の例では、OSPF ルーティング プロセス 9000 をイネーブルにし、イーサネット インターフェイス 0 をエリア 0.0.0.0 に接続し、RIP を OSPF に再配布し、OSPF を RIP に再配布する単純な OSPF 設定を示します。

```
interface ethernet 0
 ip address 10.93.1.1 255.255.255.0
 ip ospf cost 1
!
interface ethernet 1
 ip address 10.94.1.1 255.255.255.0
!
router ospf 9000
 network 10.93.0.0 0.0.255.255 area 0.0.0.0
 redistribute rip metric 1 subnets
!
router rip
 network 10.94.0.0
 redistribute ospf 9000
 default-metric 1
```

例：内部ルータ、ABR、および ASBR の OSPF の基本設定

次の例では、4 つのエリア ID を 4 つの IP アドレス範囲に割り当てています。この例では、OSPF ルーティング プロセス 109 が起動し、4 つの OSPF エリア（10.9.50.0、2、3、0）が定義されています。エリア 10.9.50.0、2、および 3 では、特定のアドレス範囲をマスクし、エリア 0 は他のすべてのネットワークで OSPF をイネーブルにします。

```
router ospf 109
 network 192.168.10.0 0.0.0.255 area 10.9.50.0
 network 192.168.20.0 0.0.255.255 area 2
 network 192.168.30.0 0.0.0.255 area 3
 network 192.168.40.0 255.255.255.255 area 0
!
! Interface Ethernet0 is in area 10.9.50.0:
interface ethernet 0
 ip address 192.168.10.5 255.255.255.0
!
```

```
! Interface Ethernet1 is in area 2:
interface ethernet 1
 ip address 192.168.20.5 255.255.255.0
!
! Interface Ethernet2 is in area 2:
interface ethernet 2
 ip address 192.168.20.7 255.255.255.0
!
! Interface Ethernet3 is in area 3:
interface ethernet 3
 ip address 192.169.30.5 255.255.255.0
!
! Interface Ethernet4 is in area 0:
interface ethernet 4
 ip address 192.168.40.1 255.255.255.0
!
! Interface Ethernet5 is in area 0:
interface ethernet 5
 ip address 192.168.40.12 255.255.0.0
```

各 **networkarea** ルータ コンフィギュレーション コマンドは逐次的に評価されるため、設定内のこれらのコマンドの順序は重要です。シスコ ソフトウェアは、各インターフェイスの address/wildcard-mask ペアを順番に評価します。詳細については、『*Cisco IOS IP Routing: OSPF Command Reference*』の **networkarea** コマンドのページを参照してください。

最初の **networkarea** コマンドについて検討してみます。エリア ID 10.9.50.0 が、サブネット 192.168.10.0 があるインターフェイスに設定されます。イーサネット インターフェイス 0 の一致が判断されたとします。イーサネット インターフェイス 0 はエリア 10.9.50.0 だけに接続されています。

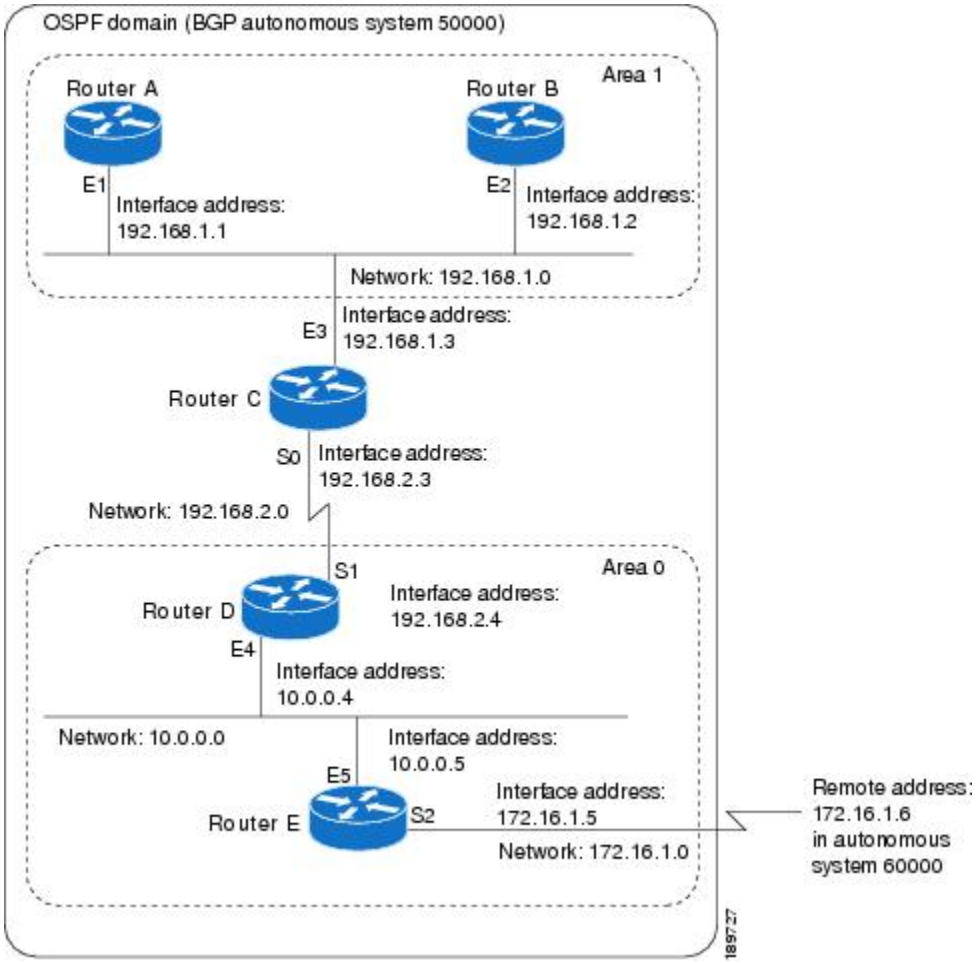
次に、2 番目の **networkarea** コマンドを評価します。エリア 2 では、すべてのインターフェイス（イーサネット インターフェイス 0 を除く）に同じプロセスが適用されています。一致は、イーサネット インターフェイス 1 について確認されるものとします。OSPF はそのインターフェイスでイネーブルになり、イーサネット インターフェイス 1 はエリア 2 に接続されます。

すべての **networkarea** コマンドに対して、この OSPF エリアへのインターフェイスの接続プロセスが続けられます。この例の最後の **networkarea** コマンドは特殊なケースです。このコマンドにより、使用可能なすべてのインターフェイス（別のエリアに明示的に接続されていない）はエリア 0 に接続されています。

例：複雑な内部ルータ、ABR、および ASBR

次の例は、単一の OSPF 自律システム内の複数のルータの設定の概略を示しています。下の図に、この設定例を示す一般的なネットワーク マップを示します。

図 *5*：*OSPF* 自律システム ネットワーク マップの例



この設定では、OSPF に 5 台のルータが設定されています。

- ルータ A とルータ B は、いずれもエリア 1 内の内部ルータです。
- ルータ C は OSPF ABR です。ルータ C では、エリア 1 が E3 に割り当てられ、エリア 0 が S0 に割り当てられることに注意してください。
- ルータ D は、エリア 0（バックボーン エリア）の内部ルータです。この場合、どちらの **network** ルータ コンフィギュレーション コマンドも同じエリア（エリア 0、つまりバックボーン エリア）を指定しています。

- ルータ E は OSPF ASBR です。BGP ルートは OSPF に再配布され、これらのルートは OSPF によってアドバタイズされることに注意してください。

（注） 自律システムのすべてのルータの設定に、OSPF 自律システムのすべてのエリアの定義を含める必要はありません。直接接続されたエリアだけを定義する必要があります。次の例では、ABR（ルータ C）がサマリー LSA をエリア 1 に挿入するとき、エリア 1（ルータ A とルータ B）のルータがエリア 0 のルートを学習します。

BGP 自律システム 109 内の OSPF ドメインは外部に接続され、BGP リンクを通じて IP アドレス 10.0.0.6 の外部ピアと接続しています。次に、設定例を示します。

次に、上の図の一般的なネットワーク マップの設定例を示します。

ルータ A の設定：内部ルータ

```
interface ethernet 1
 ip address 192.168.1.1 255.255.255.0
router ospf 1
 network 192.168.0.0 0.0.255.255 area 1
```

ルータ B の設定：内部ルータ

```
interface ethernet 2
 ip address 192.168.1.2 255.255.255.0
router ospf 202
 network 192.168.0.0 0.0.255.255 area 1
```

ルータ C の設定：ABR

```
interface ethernet 3
 ip address 192.168.1.3 255.255.255.0
interface serial 0
 ip address 192.168.2.3 255.255.255.0
router ospf 999
 network 192.168.1.0 0.0.0.255 area 1
 network 192.168.2.0 0.0.0.255 area 0
```

ルータ D の設定：内部ルータ

```
interface ethernet 4
 ip address 10.0.0.4 255.0.0.0
interface serial 1
 ip address 192.168.2.4 255.255.255.0
router ospf 50
 network 192.168.2.0 0.0.0.255 area 0
 network 10.0.0.0 0.255.255.255 area 0
```

ルータ E の設定：ASBR

```
interface ethernet 5
 ip address 10.0.0.5 255.0.0.0
interface serial 2
 ip address 172.16.1.5 255.255.255.0
router ospf 65001
 network 10.0.0.0 0.255.255.255 area 0
```

```
 redistribute bgp 109 metric 1 metric-type 1
router bgp 109
 network 192.168.0.0
 network 10.0.0.0
 neighbor 172.16.1.6 remote-as 110
```

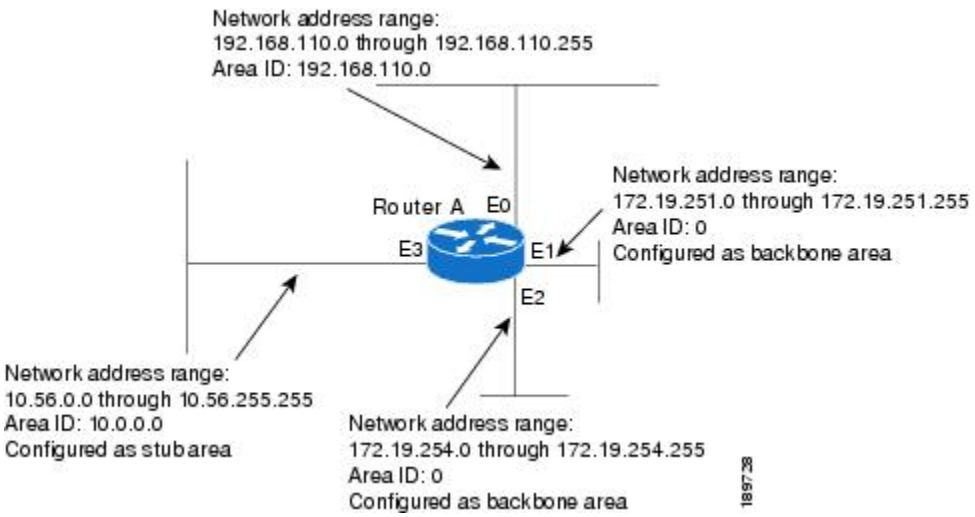
例：ABR の複雑な OSPF 設定

次の設定例では、ABR の設定でいくつかのタスクを実行しています。これらのタスクは 2 つの一般カテゴリに分けられます。

- 基本的な OSPF 設定
- ルートの再配布

この設定で概略を示した個々のタスクについて、次に簡単に説明します。次の図は、インターフェイスのネットワーク アドレス範囲とエリア割り当てを示します。

図 *6*：*OSPF* 設定例のインターフェイスとエリア仕様



この例の基本的な設定作業は、次のとおりです。

- イーサネット インターフェイス 0 からイーサネット インターフェイス 3 までのアドレス範囲を設定します。
- 各インターフェイスで OSPF をイネーブルにします。
- 各エリアおよび各ネットワークに OSPF 認証パスワードを設定します。
- リンクステート メトリックおよびその他の OSPF インターフェイス設定オプションを割り当てます。
- エリア ID 36.0.0.0 のスタブエリアを作成する（**area** ルータ コンフィギュレーション コマンドの **authentication** オプションと **stub** オプションは、別々の **area** コマンド入力で指定されますが、1 つの **area** コマンドにまとめることができます）。

- バックボーン エリア（エリア 0）を指定します。

再配布に関連した設定タスクを次に示します。

- さまざまなオプション（**metric-type**、**metric**、**tag**、および **subnet** など）を設定して、IGRP と RIP から OSPF への再配布を実行します。
- OSPF から RIP への再配布を実行します。

次に、OSPF の設定例を示します。

```
interface ethernet 0
 ip address 192.0.2.201 255.255.255.0
 ip ospf authentication-key abcdefgh
 ip ospf cost 10
!
interface ethernet 1
 ip address 172.19.251.202 255.255.255.0
 ip ospf authentication-key ijklmnop
 ip ospf cost 20
 ip ospf retransmit-interval 10
 ip ospf transmit-delay 2
 ip ospf priority 4
!
interface ethernet 2
 ip address 172.19.254.2 255.255.255.0
 ip ospf authentication-key abcdefgh
 ip ospf cost 10
!
interface ethernet 3
 ip address 10.56.0.0 255.255.0.0
 ip ospf authentication-key ijklmnop
 ip ospf cost 20
 ip ospf dead-interval 80
```

次の設定では、OSPF はネットワーク 172.16.0.0 にあります。

```
router ospf 201
 network 10.10.0.0 0.255.255.255 area 10.10.0.0
 network 192.42.110.0 0.0.0.255 area 192.42.110.0
 network 172.16.0.0 0.0.255.255 area 0
 area 0 authentication
 area 10.10.0.0 stub
 area 10.10.0.0 authentication
 area 10.10.0.0 default-cost 20
 area 192.42.110.0 authentication
 area 10.10.0.0 range 10.10.0.0 255.0.0.0
 area 192.42.110.0 range 192.42.110.0 255.255.255.0
 area 0 range 172.16.251.0 255.255.255.0
 area 0 range 172.16.254.0 255.255.255.0
 redistribute igrp 200 metric-type 2 metric 1 tag 200 subnets
 redistribute rip metric-type 2 metric 1 tag 200
```

次の設定では、IGRP 自律システム 200 は 192.0.2.1 上にあります。

```
router igrp 200
 network 172.31.0.0
!
! RIP for 192.168.110
!
router rip
 network 192.168.110.0
 redistribute igrp 200 metric 1
 redistribute ospf 201 metric 1
```

例：ルート マップ

ここでは、ルートマップを使用した場合と、使用しない場合の再配布の例を示します。IP および Connectionless Network Service（CLNS）のルーティング プロトコルの例が示されています。

次の例では、すべての OSPF ルートを IGRP に再配布しています。

```
router igrp 109
 redistribute ospf 110
```

次の例では、ホップ カウントが 1 の RIP ルートを OSPF に再配布しています。これらのルートはメトリック 5、メトリック タイプがタイプ 1、タグが 1 の外部 LSA として OSPF に再配布されます。

```
router ospf 109
 redistribute rip route-map rip-to-ospf
!
route-map rip-to-ospf permit
 match metric 1
 set metric 5
 set metric-type type1
 set tag 1
```

次の例では、OSPF で学習されたタグ 7 のルートを、RIP メトリック 15 として再配布しています。

```
router rip
 redistribute ospf 109 route-map 5
!
route-map 5 permit
 match tag 7
 set metric 15
```

次の例では、ネクスト ホップ ルータがシリアル インターフェイス 0 の OSPF intra-area および interarea ルートを、INTER_AS メトリック 5 の BGP に再配布しています。

```
router bgp 109
 redistribute ospf 109 route-map 10
!
route-map 10 permit
 match route-type internal
 match interface serial 0
 set metric 5
```

次の例では、2 つのタイプのルートを（IP と CLNS のいずれもサポートする）統合 IS-IS ルーティング テーブルに再配布しています。1 つめのタイプは、タグ 5 の OSPF 外部 IP ルートです。これらのルートは、メトリック 5 のレベル 2 IS-IS リンクステート パケット（LSP）に挿入されます。2 番目のタイプは CLNS アクセス リスト 2000 と一致する ISO-IGRP から発生した CLNS プレフィックスです。これらのルートはメトリック 30 のレベル 2 IS-IS LSP に再配布されます。

```
router isis
 redistribute ospf 109 route-map 2
 redistribute iso-igrp nsfnet route-map 3
!
route-map 2 permit
 match route-type external
 match tag 5
 set metric 5
 set level level-2
!
route-map 3 permit
 match address 2000
 set metric 30
```

次の設定では、タグ 1、2、3、および 5 の OSPF 外部ルータがそれぞれメトリック 1、1、5、および 5 の RIP に再配布されています。タグ 4 の OSPF ルートは再配布されません。

```
router rip
 redistribute ospf 109 route-map 1
!
route-map 1 permit
 match tag 1 2
 set metric 1
!
route-map 1 permit
 match tag 3
 set metric 5
!
route-map 1 deny
 match tag 4
!
route map 1 permit
 match tag 5
 set metric 5
```

次の設定では、ネットワーク 192.168.0.0 に対して RIP で学習されたルートと、プレフィックス 49.0001.0002 の ISO-IGRP で学習されたルートが、メトリック 5 のレベル 2 IS-IS LSP に再配布されます。

```
router isis
 redistribute rip route-map 1
 redistribute iso-igrp remote route-map 1
!
route-map 1 permit
 match ip address 1
 match clns address 2
 set metric 5
 set level level-2
!
 access-list 1 permit 192.168.0.0 0.0.255.255
 clns filter-set 2 permit 49.0001.0002...
```

次の設定例では、**default-information** ルータ コンフィギュレーション コマンドでルート マップを参照する手順を示しています。このタイプの参照は、*conditional default origination* と呼ばれます。OSPF は、172.16.0.0 がルーティング テーブルにある場合、タイプ 2、メトリック 5 のデフォルト ルート（ネットワーク 0.0.0.0）を発信します。

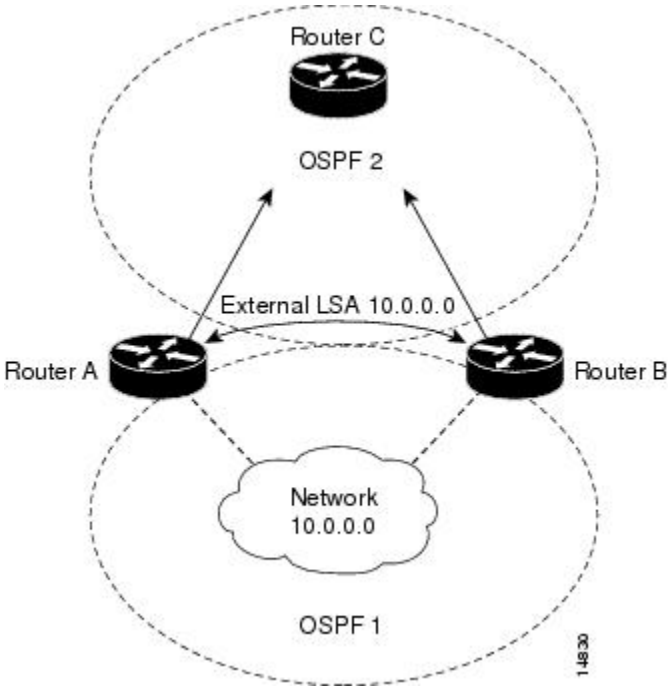
（注） 別個の OSPF プロセスから発生する非 OSPF ルートや OSPF ルートなどの OSPF プロセスに対する外部ルートだけがトラッキングに使用できます。

```
route-map ospf-default permit
 match ip address 1
 set metric 5
 set metric-type type-2
!
 access-list 1 permit 172.16.0.0 0.0.255.255
!
router ospf 109
 default-information originate route-map ospf-default
```

例：OSPF アドミニストレーティブ ディスタンスの変更

次の設定では、外部ディスタンスを 200 に変更し、信頼性を下げています。以下の図に例を示します。

図 7：***OSPF*** アドミニストレーティブ ディスタンス



ルータ A の設定

```
router ospf 1
 redistribute ospf 2 subnet
 distance ospf external 200
!
router ospf 2
 redistribute ospf 1 subnet
 distance ospf external 200
```

ルータ B の設定

```
router ospf 1
 redistribute ospf 2 subnet
 distance ospf external 200
!
router ospf 2
 redistribute ospf 1 subnet
 distance ospf external 200
```

例：OSPF over On-Demand ルーティング

次の設定により、オンデマンド回線上で OSPF が、次の図に示すように使用できるようになります。オンデマンド回線が片側（ルータ A の BRI 0）でのみ定義されていることに注意してください。両側で設定する必要はありません。

図 *8*：*OSPF over On-Demand* 回路

ルータ A の設定

```
username RouterB password 7 060C1A2F47
isdn switch-type basic-5ess
ip routing
!
interface TokenRing0
 ip address 192.168.50.5 255.255.255.0
 no shutdown
!
interface BRI0
 no cdp enable
 description connected PBX 1485
 ip address 192.168.45.30 255.255.255.0
 encapsulation ppp
 ip ospf demand-circuit
 dialer map ip 192.0.2.6 name RouterB broadcast 61484
 dialer-group 1
 ppp authentication chap
 no shutdown
!
router ospf 100
 network 192.168.45.0 0.0.0.255 area 0
 network 192.168.45.50 0.0.0.255 area 0
!
dialer-list 1 protocol ip permit
```

ルータ B の設定

```
username RouterA password 7 04511E0804
isdn switch-type basic-5ess
ip routing
!
interface Ethernet0
 ip address 192.168.50.16 255.255.255.0
 no shutdown
!
interface BRI0
 no cdp enable
 description connected PBX 1484
 ip address  192.168.45.17 255.255.255.0
 encapsulation ppp
 dialer map ip 192.168.45.19 name RouterA broadcast 61485
 dialer-group 1
 ppp authentication chap
 no shutdown
!
```

```
router ospf 100
 network 192.168.45.0 0.0.0.255 area 0
 network 192.168.45.50 0.0.0.255 area 0
!
dialer-list 1 protocol ip permit
```

例：LSA グループ ペーシング

次の例では、LSA グループ間の OSPF ペーシングを 60 秒に変更しています。

```
router ospf
 timers pacing lsa-group 60
```

例：OSPF LSA フラッディングのブロック

次に、イーサネット インターフェイス 0 経由で到達可能なブロードキャスト、非ブロードキャスト、ポイントツーポイント ネットワークに OSPF LSA がフラッディングされないようにする例を示します。

```
interface ethernet 0
 ip ospf database-filter all out
```

次の例では、ポイントツーマルチポイント ネットワークの IP アドレス 10.10.10.45 を持つネイバーへの OSPF LSA のフラッディングを防止しています。

```
router ospf 109
 neighbor 10.10.10.45 database-filter all out
```

例：MOSPF LSA パケットの無視

次に、ルータが MOSPF パケットを受信したときに syslog メッセージの送信を抑止する例を示します。

```
router ospf 109
 ignore lsa mospf
```

OSPF Not-So-Stubby Areas（NSSA）に関する追加情報

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 Command List, All Releases』
OSPF コマンド	『Cisco IOS IP Routing: OSPF Command Reference』

関連項目	マニュアル タイトル
OSPF で機能するプロトコル非依存の機能	『*IP Routing: Protocol-Independent Configuration Guide*』の Configuring IP Routing Protocol-Independent Features モジュール

RFC

RFC	Title
RFC 1587	『The OSPF NSSA Option』（1994 年 3 月）
RFC 3101	『The OSPF NSSA Option』（2003 年 1 月）

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

OSPF 設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *3* : *OSPF* の機能情報

機能名	リリース	機能情報
OSPF		OSPF は、IETF の OSPF ワーキング グループによって開発された IGP です。OSPF は特に IP ネットワーク向けに設計されており、IP サブネット化、および外部から取得したルーティング情報のタギングをサポートしています。OSPF を使用するとパケット認証も可能になり、パケットを送受信するときに IP マルチキャストが使用されます。
OSPFv3 RFC 3101 サポート	Cisco IOS XE Release 3.7S	**area nssa translate**（OSPFv3）、**compatible rfc1587**（OSPFv3）、および **show ospfv3** コマンドが追加されました。**nssa-only** キーワードが **summary-prefix**（OSPFv3）コマンドに追加されました。

第 3 章

IPv6 ルーティング：OSPFv3

Open Shortest Path First バージョン 3（OSPFv3）は、IPv6 と IPv4 ユニキャスト アドレス ファミリ（AF）をサポートする IPv4 および IPv6 リンクステート ルーティング プロトコルです。

- 機能情報の確認，63 ページ
- IPv6 ルーティング：OSPFv3 の前提条件，64 ページ
- IPv6 ルーティング：OSPFv3 の制約事項，64 ページ
- IPv6 ルーティングについて：OSPFv3，64 ページ
- OSPFv3 でのロード バランシングの設定方法，68 ページ
- OSPFv3 でのロード バランシングの設定例，74 ページ
- その他の参考資料，75 ページ
- IPv6 ルーティング：OSPFv3 の機能情報，77 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。

IPv6 ルーティング：OSPFv3 の前提条件

- ご使用の IPv6 ネットワークに対する OSPFv3 ネットワーク戦略と計画を完成させます。たとえば、複数のエリアが必要かどうかを決定します。
- IPv6 ユニキャスト ルーティングをイネーブルにする。
- インターフェイスで IPv6 をイネーブルにします。

IPv6 ルーティング：OSPFv3 の制約事項

OSPF バージョン 2 for IPv4 および OSPFv3 を使用してデュアルスタック IP ネットワークを実行している場合、OSPFv3 のイネーブル化に使用するコマンドのデフォルトを変更する際は、注意してください。これらのデフォルトを変更すると、OSPFv3 ネットワークに悪影響を及ぼすことがあります。

IPv6 ルーティングについて：OSPFv3

OSPFv3 の機能

OSPFv3 は、IPv4 および IPv6 のルーティング プロトコルです。これは、ディスタンスベクトル プロトコルではなく、リンクステートプロトコルです。リンクを、ネットワーキング デバイス上のインターフェイスとして考えます。リンクステート プロトコルは、送信元マシンと宛先マシンを接続するリンクの状態に基づいて、ルーティングの決定を行います。リンク ステートは、インターフェイスと、その隣接ネットワーキング デバイスとの関係を説明するものです。インターフェイス情報には、インターフェイスの IPv6 プレフィックス、ネットワーク マスク、接続先のネットワークのタイプ、そのネットワークに接続されているデバイスなどが含まれます。この情報は、さまざまなタイプのリンクステート アドバタイズメント（LSA）で伝播されます。

デバイスの LSA データの集まりは、リンクステートデータベースに格納されます。ダイクストラ アルゴリズムが採用されている場合、データベースの内容に基づいて OSPF ルーティング テーブルが作成されます。データベースとルーティング テーブルの違いは、データベースにはすべての raw データが含まれており、ルーティング テーブルには特定のデバイス インターフェイス ポートを介した既知の宛先への最短パスのリストが含まれていることです。

OSPFv3 は、RFC 5340 に説明されているように、IPv6 および IPv4 ユニキャスト AF をサポートしています。

OSPFv3 と OSPF バージョン 2 の比較

OSPF バージョン 3 の大部分は、OSPF バージョン 2 と同じです。RFC 5340 に説明されているように、OSPFv3 では、OSPF バージョン 2 が拡張され、IPv6 ルーティング プレフィックスと、より大きなサイズの IPv6 アドレスに対するサポートが提供されています。

OSPFv3 では、ルーティング プロセスを明示的に作成する必要はありません。インターフェイスで OSPFv3 をイネーブルにすると、ルーティング プロセス（およびその関連設定）が作成されます。

OSPFv3 では、各インターフェイスはインターフェイス コンフィギュレーション モードでコマンドを使用してイネーブルにする必要があります。この機能は、デバイス コンフィギュレーション モードを使用してインターフェイスが間接的にイネーブルになる OSPF バージョン 2 とは異なります。

ノンブロードキャスト マルチアクセス（NBMA）インターフェイスを OSPFv3 で使用する場合、ネイバーのリストを使用してデバイスを手動で設定する必要があります。隣接デバイスはデバイス ID で識別されます。

IPv6 では、インターフェイスの多数のアドレス プレフィックスを設定できます。OSPFv3 では、デフォルトで、1 つのインターフェイス上のすべてのアドレス プレフィックスが組み込まれます。OSPFv3 にインポートするアドレス プレフィックスを選択することはできません。1 つのインターフェイス上のすべてのアドレス プレフィックスがインポートされるか、1 つのインターフェイス上のアドレス プレフィックスがインポートされないかのいずれかです。

OSPF バージョン 2 とは異なり、OSPFv3 の複数のインスタンスを 1 つのリンク上で実行できます。

OSPF では、自動的にループバック インターフェイスが他よりも優先されます。また、すべてのループバック インターフェイスの中で最も高位の IP アドレスが選択されます。ループバック インターフェイスが存在しない場合、デバイス内で最も高位の IP アドレスが選択されます。特定のインターフェイスを使用するように OSPF に指示することはできません。

OSPFv3 の LSA タイプ

次に、それぞれ用途の異なる LSA タイプを示します。

- デバイス LSA（タイプ 1）：エリアへのデバイスのリンクのリンク ステートとコストが説明されます。これらの LSA は、エリア内でのみフラッディングされます。この LSA は、デバイスがエリア境界ルータ（ABR）か自律システム境界ルータ（ASBR）か、およびそのルータが仮想リンクの一端であるかどうかを示します。また、タイプ 1 の LSA は、スタブ ネットワークへのアドバタイズにも使用されます。OSPFv3 では、これらの LSA はアドレス情報を持たず、ネットワークプロトコルに依存しません。OSPFv3 では、デバイス インターフェイス情報は複数のデバイス LSA 間で拡散されます。受信者は、SPF 計算の実行時に、特定のデバイスから発信されたすべてのデバイス LSA を連結する必要があります。
- ネットワーク LSA（タイプ 2）：ネットワークに接続されているすべてのデバイスのリンクステートおよびコスト情報が説明されます。この LSA は、ネットワーク内のすべてのリンク

ステートおよびコスト情報を集約したものです。指定デバイスだけがこの情報を追跡し、ネットワーク LSA を生成できます。OSPFv3 では、ネットワーク LSA はアドレス情報を持たず、ネットワーク プロトコルに依存しません。

- ABR のエリア間プレフィックス LSA（タイプ 3）：他のエリア内のデバイス（エリア間ルート）に内部ネットワークがアドバタイズされます。タイプ 3 の LSA は、単一のネットワークを表すことも、1 つのアドバタイズメントとして集約された一連のネットワークを表すこともあります。サマリー LSA を生成するのは ABR だけです。OSPFv3 では、これらの LSA のアドレスは *address*, *mask* ではなく *prefix*, *prefix length* で表されます。デフォルト ルートは、長さが 0 のプレフィックスとして表現されます。
- ASBR のエリア間デバイス LSA（タイプ 4）：ASBR のロケーションがアドバタイズされます。外部ネットワークにアクセスしようとするデバイスは、これらのアドバタイズメントを使用して、ネクスト ホップへのベスト パスを決定します。タイプ 4 LSA は、ASBR の代わりに ABR により生成されます。
- 自律システム外部 LSA（タイプ 5）：別の自律システムからルートを再配布します。通常は別のルーティング プロトコルから OSPFv3 に再配布します。OSPFv3 では、これらの LSA のアドレスは *address*, *mask* ではなく *prefix*, *prefixlength* で表されます。デフォルト ルートは、長さが 0 のプレフィックスとして表現されます。
- リンク LSA（タイプ 8）：ローカルリンク フラッディング スコープを持ちます。関連付けられているリンクを越えてフラッディングされることはありません。リンク LSA は、リンクに接続されている他のすべてのデバイスに対してデバイスのリンクローカル アドレスを提供し、リンクに接続されている他のデバイスに、そのリンクに関連付けるプレフィックスのリストを通知します。また、デバイスが Options ビットの集まりをアサートして、リンクの起点となるネットワーク LSA と関連付けできるようにします。
- エリア内プレフィックス LSA（タイプ 9）：デバイスは、デバイスまたは中継ネットワークごとに、それぞれ固有のリンクステート ID を持つ複数のエリア内プレフィックス LSA を発信できます。各エリア内プレフィックス LSA のリンクステート ID は、デバイス LSA またはネットワーク LSA との関連性を表し、スタブ ネットワークおよび中継ネットワークのプレフィックスを含んでいます。

新しく定義された LSA のほとんどすべてに、アドレスプレフィックスが存在します。プレフィックスは、PrefixLength、PrefixOptions、および Address Prefix の 3 つのフィールドで表現されます。OSPFv3 では、これらの LSA のアドレスは *address*, *mask* ではなく *prefix*, *prefixlength* で表されます。デフォルト ルートは、長さが 0 のプレフィックスとして表現されます。タイプ 3 およびタイプ 9 LSA は、すべてのプレフィックス（サブネット）情報を伝送します。これは、OSPFv2 ではデバイス LSA およびネットワーク LSA に含まれます。特定の LSA（デバイス LSA、ネットワーク LSA、エリア間デバイス LSA、およびリンク LSA）の Options フィールドは、OSPFv3 をサポートするために 24 ビットに拡張されています。

OSPFv3 では、エリア間プレフィックス LSA、エリア間デバイス LSA、および自律システム外部 LSA のリンクステート ID の機能は、リンクステート データベースの個々の部分を識別することだけです。OSPF バージョン 2 ではリンクステート ID で表されたアドレスまたはデバイス ID はすべて、OSPFv3 では LSA の本体で伝送されます。

ネットワーク LSA およびリンク LSA のリンクステート ID は常に、説明されているリンク上の送信元デバイスのインターフェイス ID となります。このため、ネットワーク LSA およびリンク LSA は、サイズ制限ができない LSA だけになりました。ネットワーク LSA は、リンクに接続されているすべてのデバイスをリストする必要があります。リンク LSA は、リンクのデバイスのアドレス プレフィックスのすべてをリストする必要があります。

OSPFv3 でのロード バランシング

デバイスは、複数のルーティングプロセス（またはルーティングプロトコル）を使用して特定のネットワークへの複数のルートを認識すると、最短のアドミニストレーティブ ディスタンスを持つルートをルーティングテーブルにインストールします。同じアドミニストレーティブディスタンスを持つ同じルーティング プロセスを介して認識された多数のルートから、1 つのルートを選択する必要があることもあります。この場合、デバイスはその宛先へのコスト（またはメトリック）が最も小さいパスを選択します。各ルーティング プロセスはコストをそれぞれの方法で計算します。コストは、ロード バランシングを実現するために処理が必要なこともあります。

OSPFv3 では、次の方法でロードバランシングが自動的に実行されます。OSPFv3 により、複数のインターフェイスを通って宛先に到達できること、および各パスのコストが同じであることが検出された場合は、ルーティング テーブルに各パスがインストールされます。同じ宛先へのパスの数は、**maximum-paths** コマンドを指定しないかぎり制限されません。デフォルトの最大パスは 16 です。有効範囲は 1 ～ 64 です。

OSPFv3 にインポートされるアドレス

OSPFv3 が実行されているインターフェイスで指定されているアドレス セットを OSPFv3 にインポートする場合、特定のアドレスを選択してインポートすることはできません。すべてのアドレスがインポートされるか、いずれのアドレスもインポートされないかのどちらかです。

OSPFv3 のカスタマイゼーション

ネットワークに合わせて OSPFv3 をカスタマイズできますが、多くの場合、その必要はありません。OSPFv3 のデフォルトは、ほとんどのカスタマーや機能の要件を満たすように設定されています。デフォルトを変更する必要がある場合は、IPv6 コマンド リファレンスを参照して、適切な構文を確認してください。

注意 デフォルトを変更する際は、注意してください。デフォルトを変更すると、OSPFv3 ネットワークに悪影響を及ぼすことがあります。

OSPFv3 の強制的な SPF

clearipv6ospf コマンドとともに **process** キーワードが使用されている場合、OSPFv3 データベースのクリアおよび再入力の後に、SPF アルゴリズムが実行されます。**clearipv6ospf** コマンドとともに **force-spf** キーワードが使用されている場合、SPF アルゴリズムの実行前に OSPFv3 データベースはクリアされません。

OSPFv3 でのロード バランシングの設定方法

OSPFv3 デバイス プロセスの設定

ステップ 3 を完了し、OSPFv3 ルータ コンフィギュレーション モードを開始したら、必要に応じてこの作業の以降のステップを任意に設定して、OSPFv3 デバイス コンフィギュレーションを実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospfv3**[*process-id*]
4. **area***area-ID* [**default-cost** | **nssa** | **stub**]
5. **auto-costreference-bandwidth***Mbps*
6. **default** {**area***area-ID* [**range***ipv6-prefix* | **virtual-link***router-id*]} [**default-informationoriginate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list***prefix-listprefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths***paths* | **redistribute***protocol* | **summary-prefix***ipv6-prefix*]
7. **ignorelsamospf**
8. **interface-idsnmp-if-index**
9. **log-adjacency-changes** [**detail**]
10. **passive-interface** [**default** | *interface-typeinterface-number*]
11. **queue-depth**{**hello** | **update**} {*queue-size* | **unlimited**}
12. **router-id***router-id*

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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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	**routerospfv3**[*process-id*] 例： `Device(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリのルータ コンフィギュレーション モードを開始します。
ステップ 4	**area***area-ID* [**default-cost** | **nssa** | **stub**] 例： `Device(config-router)# area 1`	OSPFv3 エリアを設定します。
ステップ 5	**auto-costreference-bandwidth***Mbps* 例： `Device(config-router)# auto-cost reference-bandwidth 1000`	IPv4 OSPFv3 プロセスで、インターフェイスのメトリックを計算する際に OSPFv3 で使用される基準値を制御します。
ステップ 6	**default** {**area***area-ID* [**range***ipv6-prefix* | **virtual-link***router-id*]} [**default-informationoriginate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list***prefix-listprefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths***paths* | **redistribute***protocol* | **summary-prefix***ipv6-prefix*] 例： `Device(config-router)# default area 1`	OSPFv3 パラメータをデフォルト値に戻します。
ステップ 7	**ignorelsamospf** 例： `Device(config-router)# ignore lsa mospf`	デバイスが LSA タイプ 6 Multicast OSPFv3 パケットを受信した場合の syslog メッセージの送信を抑制します（LSA タイプ 6 Multicast OSPFv3 はサポートされていません）。
ステップ 8	**interface-idsnmp-if-index** 例： `Device(config-router)# interface-id snmp-if-index`	IPv4 および IPv6 の簡易ネットワーク管理プロトコル（SNMP）MIB-II インターフェイスインデックス（ifIndex）ID 番号を使用して OSPFv3 インターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 9	**log-adjacency-changes** [**detail**] 例： `Device(config-router)# log-adjacency-changes`	OSPFv3 ネイバーが起動または停止したときに、デバイスが syslog メッセージを送信するように設定します。
ステップ 10	**passive-interface** [**default** | *interface-typeinterface-number*] 例： `Device(config-router)# passive-interface default`	IPv4 OSPFv3 プロセスを使用しているときに、インターフェイスのルーティングアップデートの送信を抑制します。
ステップ 11	**queue-depth**{**hello** | **update**} {*queue-size* | **unlimited**} 例： `Device(config-router)# queue-depth update 1500`	IPv4 OSPFv3 プロセスのキューに保持できる着信パケット数を設定します。
ステップ 12	**router-id***router-id* 例： `Device(config-router)# router-id 10.1.1.1`	固定ルータ ID を使用するには、次のコマンドを入力します。

SPF 計算の強制実行

手順の概要

1. イネーブル化
2. **clearospfv3**[*process-id*] **force-spf**
3. **clearospfv3**[*process-id*] **process**
4. **clearospfv3**[*process-id*] **redistribution**
5. **clearipv6ospf** [*process-id*] {**process** | **force-spf** | **redistribution**}

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	**clearospfv3**[*process-id*] **force-spf** 例： `Device# clear ospfv3 1 force-spf`	OSPFv3 プロセスに対して SPF 計算を実行します。 • **clearospfv3force-spf** コマンドが設定されている場合、**clearipv6ospf** の設定が上書きされます。 • いったん **clearospfv3force-spf** コマンドを使用すると、**clearipv6ospf** コマンドは使用できなくなります。
ステップ 3	**clearospfv3**[*process-id*] **process** 例： `Device# clear ospfv3 2 process`	OSPFv3 プロセスをリセットします。 • **clearospfv3force-spf** コマンドが設定されている場合、**clearipv6ospf** の設定が上書きされます。 • いったん **clearospfv3force-spf** コマンドを使用すると、**clearipv6ospf** コマンドは使用できなくなります。
ステップ 4	**clearospfv3**[*process-id*] **redistribution** 例： `Device# clear ospfv3 redistribution`	OSPFv3 ルート再配布をクリアします。 • **clearospfv3force-spf** コマンドが設定されている場合、**clearipv6ospf** の設定が上書きされます。 • いったん **clearospfv3force-spf** コマンドを使用すると、**clearipv6ospf** コマンドは使用できなくなります。
ステップ 5	**clearipv6ospf** [*process-id*] {**process** | **force-spf** | **redistribution**} 例： `Device# clear ipv6 ospf force-spf`	OSPFv3 ルーティング プロセス ID に基づいて OSPFv3 状態をクリアし、SPF アルゴリズムを強制的に開始します。 • **clearospfv3force-spf** コマンドが設定されている場合、**clearipv6ospf** の設定が上書きされます。 • いったん **clearospfv3force-spf** コマンドを使用すると、**clearipv6ospf** コマンドは使用できなくなります。

OSPFv3 の設定と動作の確認

この作業は任意です。また、これらのコマンドは、必要に応じて任意の順序で入力できます。

手順の概要

1. イネーブル化
2. **showospfv3** [*process-id*] [*address-family*] **border-routers**
3. **showospfv3** [*process-id* [*area-id*]] [*address-family*] **database** [**database-summary** | **internal** | **external** [*ipv6-prefix*] [*link-state-id*] | **grace** | **inter-areaprefix** [*ipv6-prefix* | *link-state-id*] | **inter-arearouter** [*destination-router-id* | *link-state-id*] | **link** [**interface***interface-name* | *link-state-id*] | **network** [*link-state-id*] | **nssa-external** [*ipv6-prefix*] [*link-state-id*] | **prefix** [**ref-lsa** {**router** | **network**} | *link-state-id*] | **promiscuous** | **router** [*link-state-id*] | **unknown** [{**area** | **as** | **link**} [*link-state-id*]] [**adv-router***router-id*] [**self-originate**]
4. **showospfv3** [*process-id*] [*address-family*] **events** [**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**]
5. **show ospfv3** [*process-id*] [*area-id*] [*address-family*] **flood-list***interface-typeinterface-number*
6. **show ospfv3** [*process-id*] [*address-family*] **graceful-restart**
7. **showospfv3** [*process-id*] [*area-id*] [*address-family*] **interface** [*typenumber*] [**brief**]
8. **showospfv3** [*process-id*] [*area-id*] [*address-family*] **neighbor** [*interface-typeinterface-number*] [*neighbor-id*] [**detail**]
9. **showospfv3** [*process-id*] [*area-id*] [*address-family*] **request-list**[*neighbor*] [*interface*] [*interface-neighbor*]
10. **showospfv3** [*process-id*] [*area-id*] [*address-family*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]
11. **showospfv3** [*process-id*] [*address-family*] **statistic** [**detail**]
12. **showospfv3**[*process-id*] [*address-family*] **summary-prefix**
13. **showospfv3** [*process-id*] [*address-family*] **timersrate-limit**
14. **showospfv3**[*process-id*] [*address-family*] **traffic**[*interface-typeinterface-number*]
15. **showospfv3**[*process-id*] [*address-family*] **virtual-links**

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	**showospfv3** [*process-id*] [*address-family*] **border-routers** 例： `Device# show ospfv3 border-routers`	ABR および ASBR への内部 OSPFv3 ルーティングテーブルエントリを表示します。
ステップ 3	**showospfv3** [*process-id* [*area-id*]] [*address-family*] **database** [**database-summary**	**internal**	**external** [*ipv6-prefix*] [*link-state-id*]	**grace**	**inter-areaprefix** [*ipv6-prefix*	*link-state-id*]	**inter-arearouter** [*destination-router-id*	*link-state-id*]	**link** [**interface***interface-name*	*link-state-id*]		特定のデバイスの OSPFv3 データベースに関する情報のリストを表示します。

	コマンドまたはアクション	目的
	network [*link-state-id*] | **nssa-external** [*ipv6-prefix*] [*link-state-id*] | **prefix** [**ref-lsa** {**router** | **network**} | *link-state-id*] | **promiscuous** | **router** [*link-state-id*] | **unknown** [{**area** | **as** | **link**} [*link-state-id*]] [**adv-router***router-id*] [**self-originate**] 例： `Device# show ospfv3 database`	
ステップ 4	**showospfv3** [*process-id*] [*address-family*] **events** [**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**] 例： `Device# show ospfv3 events`	OSPFv3 イベントについての詳細情報を表示します。
ステップ 5	**show ospfv3** [*process-id*] [*area-id*] [*address-family*] **flood-list***interface-typeinterface-number* 例： `Device# show ospfv3 flood-list`	インターフェイス上でのフラッディングを待機している OSPFv3 LSA のリストを表示します。
ステップ 6	**show ospfv3** [*process-id*] [*address-family*] **graceful-restart** 例： `Device# show ospfv3 graceful-restart`	OSPFv3 グレースフル リスタートの情報を表示します。
ステップ 7	**showospfv3** [*process-id*] [*area-id*] [*address-family*] **interface** [*typenumber*] [**brief**] 例： `Device# show ospfv3 interface`	OSPFv3 関連のインターフェイス情報を表示します。
ステップ 8	**showospfv3** [*process-id*] [*area-id*] [*address-family*] **neighbor** [*interface-typeinterface-number*] [*neighbor-id*] [**detail**] 例： `Device# show ospfv3 neighbor`	OSPFv3 ネイバー情報をインターフェイスごとに表示します。
ステップ 9	**showospfv3** [*process-id*] [*area-id*] [*address-family*] **request-list**[*neighbor*] [*interface*] [*interface-neighbor*] 例： `Device# show ospfv3 request-list`	デバイスで要求されるすべての LSA のリストを表示します。

	コマンドまたはアクション	目的
ステップ 10	**showospfv3** [*process-id*] [*area-id*] [*address-family*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*] 例： `Device# show ospfv3 retransmission-list`	再送信を待機しているすべての LSA のリストを表示します。
ステップ 11	**showospfv3** [*process-id*] [*address-family*] **statistic** [**detail**] 例： `Device# show ospfv3 statistic`	OSPFv3 SPF 計算の統計情報を表示します。
ステップ 12	**showospfv3**[*process-id*] [*address-family*] **summary-prefix** 例： `Device# show ospfv3 summary-prefix`	OSPFv3 プロセスで設定されているサマリー アドレスのすべての再配布情報のリストを表示します。
ステップ 13	**showospfv3** [*process-id*] [*address-family*] **timersrate-limit** 例： `Device# show ospfv3 timers rate-limit`	レート リミット キュー内のすべての LSA を表示します。
ステップ 14	**showospfv3**[*process-id*] [*address-family*] **traffic**[*interface-typeinterface-number*] 例： `Device# show ospfv3 traffic`	OSPFv3 トラフィック統計情報を表示します。
ステップ 15	**showospfv3**[*process-id*] [*address-family*] **virtual-links** 例： `Device# show ospfv3 virtual-links`	OSPFv3 仮想リンクのパラメータと現在の状態を表示します。

OSPFv3 でのロード バランシングの設定例

例：OSPFv3 デバイス プロセスの設定

```
Device# show ospfv3 database
            OSPFv3 Device with ID (172.16.4.4) (Process ID 1)
                Device Link States (Area 0)
ADV Device         Age         Seq#        Fragment ID   Link count  Bits
```

```
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B
            Inter Area Prefix Link States (Area 0)
ADV Device         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
172.16.6.6         193         0x80000001  FEC0:3344::/32
172.16.6.6         82          0x80000001  FEC0::/32
            Inter Area Device Link States (Area 0)
ADV Device         Age         Seq#        Link ID    Dest DevID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3

            Link (Type-8) Link States (Area 0)
ADV Device         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0
            Intra Area Prefix Link States (Area 0)
ADV Device         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0


Device# show ospfv3 neighbor

OSPFv3 Device with ID (10.1.1.1) (Process ID 42)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
10.4.4.4        1    FULL/  -        00:00:39    12              vm1
OSPFv3 Device with ID (10.2.1.1) (Process ID 100)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
10.5.4.4          1    FULL/  -        00:00:35    12               vm1
```

例：SPF 設定の強制実行

次に、SPF をトリガーして、SPF を再実行し、ルーティング テーブルに値を再入力する例を示します。

```
clear ipv6 ospf force-spf
```

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
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』

関連項目	マニュアル タイトル
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』
IPv6 ルーティング：OSPFv3	*Configuring OSPF* モジュール

標準および RFC

標準/RFC	Title
IPv6 に関する RFC	IPv6 の RFC

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

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

IPv6 ルーティング：OSPFv3 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *4*：*IPv6* ルーティング：*OSPFv3* の機能情報

機能名	リリース	機能情報
IPv6 ルーティング：OSPFv3	12.2(33)SRA Cisco IOS XE Release 2.1	OSPF バージョン 3 for IPv6 では、OSPF バージョン 2 が拡張され、IPv6 ルーティング プレフィックスと、より大きなサイズの IPv6 アドレスに対するサポートが提供されています。

第 4 章

IPv6ルーティング：IPsecを使用したOSPFv3認証サポート

Open Shortest Path First バージョン 3（OSPFv3）パケットが変更されてデバイスに再送信されることがないように、OSPFv3 パケットを認証する必要があります。OSPFv3 は、IPsec セキュア ソケット API を使用して OSPFv3 パケットに認証を追加します。この API は IPv6 をサポートします。

- 機能情報の確認，79 ページ
- IPv6 ルーティング：IPsec を使用した OSPFv3 認証の前提条件，80 ページ
- IPv6 ルーティングについて：IPsec を使用した OSPFv3 認証サポート，80 ページ
- IPv6 ルーティングの設定方法：IPsec を使用した OSPFv3 認証サポート，81 ページ
- IPv6 ルーティングの設定例：IPsec を使用した OSPFv3 認証サポート，84 ページ
- IPv6 ルーティング：IPsec を使用した OSPFv3 認証サポートに関する追加情報，85 ページ
- IPv6 ルーティング：IPsec を使用した OSPFv3 認証サポートの機能情報，86 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。

IPv6 ルーティング：IPsec を使用した OSPFv3 認証の前提条件

認証および暗号化をイネーブルにするために、OSPFv3 に対して IP セキュリティ（IPSec）セキュア ソケット アプリケーション プログラム インターフェイス（API）を設定する。

IPv6 ルーティングについて：IPsec を使用した OSPFv3 認証サポート

IPsec を使用した OSPFv3 認証サポート

OSPFv3パケットが変更されてデバイスに再送信されることにより、デバイスがシステム管理者にとって望ましくない動作をすることにならないように、OSPFv3パケットを認証する必要があります。OSPFv3 は、IPsec セキュア ソケット API を使用して OSPFv3 パケットに認証を追加します。この API は IPv6 をサポートします。

OSPFv3 では、認証をイネーブルにするために IPsec を使用する必要があります。OSPFv3 で使用するために必要な IPsec API は暗号イメージのみに含まれるため、認証を使用するには暗号イメージが必要です。

OSPFv3 では、認証フィールドが OSPFv3 パケット ヘッダーから削除されています。IPv6 で OSPFv3 を実行する場合、ルーティング変更の整合性、認証、および機密性を確保するために、OSPFv3 には IPv6 認証ヘッダー（AH）または IPv6 ESP ヘッダーが必要です。IPv6 AH および ESP 拡張ヘッダーを使用すると、OSPFv3 に認証および機密性を提供できます。

IPsec AH を使用するには、**ipv6ospfauthentication** コマンドをイネーブルにする必要があります。IPsec ESP ヘッダーを使用するには、**ipv6ospfencryption** コマンドをイネーブルにする必要があります。ESP ヘッダーは、単独で適用することも、AH と組み合わせて適用することもできます。ESP を使用した場合、暗号化と認証の両方が提供されます。セキュリティ サービスは、通信する 1 組のホスト、通信する 1 組のセキュリティ ゲートウェイ、またはセキュリティ ゲートウェイとホストの間に提供できます。

IPsec を設定するには、セキュリティ ポリシーを設定します。これは、Security Policy Index（SPI）とキーの組み合わせです（このキーはハッシュ値の作成および検証に使用されます）。OSPFv3 の IPsec は、インターフェイスまたは OSPFv3 エリアに対して設定できます。セキュリティを強化するには、IPsec を設定する各インターフェイスで異なるポリシーを設定する必要があります。OSPFv3 エリアに対して IPsec を設定した場合、ポリシーはそのエリア内のすべてのインターフェイス（IPsec が直接設定されているインターフェイスを除く）に適用されます。いったん OSPFv3 に対して IPsec を設定すると、IPsec は見えなくなります。

トラフィックを保護するために、アプリケーションによりセキュア ソケット API が使用されます。この API によって、アプリケーションによるセキュア ソケットのオープン、リッスン、およ

びクローズを許可する必要があります。また、アプリケーションと Secure Socket Layer の間のバインディングにより、Secure Socket Layer は、接続のオープンやイベントのクローズなど、ソケットへの変更をアプリケーションに通知できます。セキュア ソケット API は、ソケットを識別できます。つまり、セキュリティを必要とするトラフィックを伝送するローカルおよびリモートのアドレス、マスク、ポート、およびプロトコルを識別できます。

各インターフェイスのセキュア ソケット ステートは、次のいずれかになります。

- NULL：エリアに対して認証が設定されていれば、インターフェイスに対してセキュア ソケットを作成しません。
- DOWN：インターフェイス（またはインターフェイスが含まれるエリア）に対して IPsec は設定されていますが、OSPFv3 がこのインターフェイスに対するセキュア ソケットの作成を IPsec に要求していないか、またはエラー条件が存在します。
- GOING UP：OSPFv3 はセキュア ソケットを IPsec に要求し、IPsec からの CRYPTO_SS_SOCKET_UP メッセージを待っています。
- UP：OSPFv3 は IPsec から CRYPTO_SS_SOCKET_UP メッセージを受信しました。
- CLOSING：インターフェイスのセキュア ソケットはクローズされています。インターフェイスに対して新しいソケットがオープンされることがあります。この場合、現在のセキュア ソケットは DOWN ステートに移行します。オープンされない場合、インターフェイスは UNCONFIGURED となります。
- UNCONFIGURED：インターフェイス上に認証は設定されていません。

DOWN 状態の間は、OSPFv3 はパケットを受け入れたり、送信したりすることはありません。

IPv6 ルーティングの設定方法：IPsec を使用した OSPFv3 認証サポート

OSPFv3 での IPsec の設定

OSPFv3 を設定し、認証を決定したら、グループ内の各デバイスでセキュリティ ポリシーを定義する必要があります。セキュリティ ポリシーは、キーと SPI の組み合わせで構成されます。セキュリティ ポリシーを定義するには、SPI およびキーを定義する必要があります。

認証ポリシーまたは暗号化ポリシーは、インターフェイスまたは OSPFv3 エリアのいずれにも設定できます。セキュリティ ポリシーは、エリアに対して設定した場合、エリア内のすべてのインターフェイスに適用されます。セキュリティを強化する場合は、各インターフェイスで異なるポリシーを使用してください。

認証および暗号化は、仮想リンク上に設定できます。

Defining Authentication on an Interface

はじめる前に

インターフェイスでIPsecを設定する前に、そのインターフェイスでOSPFv3を設定する必要があります。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. 次のいずれかを実行します。
   - **ospfv3authentication** {**ipsec***spi*} {**md5** | **sha1**}{*key-encryption-typekey*} | **null**
   - **ipv6 ospf authentication** {**null** | **ipsec spi***spiauthentication-algorithm* [*key-encryption-type*] [*key*]}

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	**configureterminal** 例： `Device# 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	**interface***typenumber* 例： `Device(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。 （注） Cisco ASR 901 シリーズ ルータでは、物理インターフェイスではなく VLANインターフェイスの OSPFv3 認証を設定する必要があります。次の例を参照してください。 `Device(config)# interface VLAN 60`
ステップ 4	次のいずれかを実行します。 • **ospfv3authentication** {**ipsec***spi*} {**md5** | **sha1**}{*key-encryption-typekey*} | **null**	インターフェイスの認証タイプを指定します。

	コマンドまたはアクション	目的

	• **ipv6 ospf authentication** {**null** | **ipsec spi***spiauthentication-algorithm* [*key-encryption-type*] [*key*]}
	
	例：
	`Device(config-if)# ospfv3 authentication md5 0 275761340947681324733020312097 27`
	
	例：
	または
	
	`Device(config-if)# ipv6 ospf authentication ipsec spi 500 md5 1234567890abcdef1234567890abcdef`	

OSPFv3 エリア内の認証の定義

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6routerospf***process-id*
4. **area***area-id***authenticationipsecspi***spi authentication-algorithm* [*key-encryption-type*] *key*

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	**configureterminal** 例： `Device# 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	**ipv6routerospf***process-id* 例： `Device(config)# ipv6 router ospf 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area***area-id***authenticationipsecspi***spi authentication-algorithm* [*key-encryption-type*] *key* 例： `Device(config-rtr)# area 1 authentication ipsec spi 678 md5 1234567890ABCDEF1234567890ABCDEF`	OSPFv3 エリア内の認証をイネーブルにします。

IPv6 ルーティングの設定例：IPsec を使用した OSPFv3 認証サポート

例：インターフェイスでの認証の定義

次に、イーサネット インターフェイス 0/0 で認証を定義する例を示します。

```
interface Ethernet0/0
 ipv6 enable
 ipv6 ospf 1 area 0
 ipv6 ospf authentication ipsec spi 500 md5 1234567890ABCDEF1234567890ABCDEF
interface Ethernet0/0
 ipv6 enable
 ipv6 ospf authentication null
 ipv6 ospf 1 area 0
```

次に、Cisco ASR 901 シリーズ ルータの VLAN インターフェイスで認証を定義する例を示します。

```
interface Vlan60
ipv6 ospf encryption ipsec spi 300 esp 3des 4D92199549E0F2EF009B4160F3580E5528A11A45017F3887
 md5 79054025245FB1A26E4BC422AEF54501
```

例：OSPFv3 エリア内の認証の定義

次に、OSPFv3 エリア 0 で認証を定義する例を示します。

```
ipv6 router ospf 1
 router-id 10.11.11.1
 area 0 authentication ipsec spi 1000 md5 1234567890ABCDEF1234567890ABCDEF
```

IPv6 ルーティング：IPsec を使用した OSPFv3 認証サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』
IPv6 ルーティング：IPsec を使用した OSPF for IPv6 認証サポート	『*IP Routing: OSPF Configuration Guide*』の *Configuring OSPF* モジュール

標準および RFC

標準/RFC	Title
IPv6 に関する RFC	IPv6 の RFC

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

IPv6 ルーティング：IPsec を使用した OSPFv3 認証サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *5*：*IPv6* ルーティング：*IPsec* を使用した *OSPF for IPv6* 認証サポートの機能情報

機能名	リリース	機能情報
IPv6 ルーティング：IPsec を使用した OSPF for IPv6 認証サポート	XE 3.14S	OSPFv3 は、IPsec セキュア ソケット API を使用して OSPFv3 パケットに認証を追加します。 次のコマンドが導入または変更されました。**area authentication (IPv6)**、**ipv6 ospf authentication**、**ipv6 router ospf**、**ospfv3 authentication**

第 5 章

OSPFv2 暗号化認証

ネットワークで不正または無効なルーティング アップデートを防止するため、Open Shortest Path First バージョン 2（OSPFv2）プロトコル パケットを認証する必要があります。

OSPFv2 で定義される認証方式は、プレーン テキスト認証と暗号化認証の 2 つがあります。ここでは、ハッシュ メッセージ認証コード - セキュア ハッシュ アルゴリズム（HMAC-SHA）を使用して暗号化認証を設定する方法について説明します。OSPFv2 仕様（RFC 2328）では暗号化認証に Message Digest 5（MD5）アルゴリズムだけが許可されます。ただし、RFC 5709（OSPFv2 HMAC-SHA 暗号化認証）では OSPFv2 で暗号化認証に HMAC-SHA アルゴリズムを使用できます。

- 機能情報の確認，87 ページ
- OSPFv2 暗号化認証の前提条件，88 ページ
- OSPFv2 暗号化認証について，88 ページ
- OSPFv2 暗号化認証の設定方法，89 ページ
- OSPFv2 暗号化認証の設定例，91 ページ
- OSPFv2 暗号化認証に関する追加情報，94 ページ
- OSPFv2 暗号化認証の機能情報，95 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。

OSPFv2 暗号化認証の前提条件

Open Shortest Path First バージョン 2（OSPFv2）がネットワークで設定されていることを確認します。

OSPFv2 暗号化認証について

OSPFv2 暗号化認証の設定

OSPFv2 暗号化認証機能を使用すると、OSPF インターフェイスにキー チェーンを設定し、HMAC-SHA アルゴリズムを使用して OSPFv2 パケットを認証することができます。別のプロトコルによって使用されている既存のキー チェーンを使用することも、OSPFv2 専用のキー チェーンを作成することもできます。

キーチェーンはキーのリストです。各キーは、パスワードやパスコードとも呼ばれるキーストリングで構成されます。キーストリングは、キーが機能するために不可欠です。各キーは、一意のキー ID で識別されます。OSPFv2 パケットを認証するには、暗号化認証アルゴリズムにキーが設定されることが必要です。OSPFv2 は、1 ～ 255 のキー ID を持つキーをサポートしています。暗号化認証アルゴリズムとキーの組み合わせは、セキュリティアソシエーション（SA）と呼ばれます。

キー チェーンの認証キーは、ライフタイムと呼ばれる特定の期間の間有効です。SA に、以下の設定可能なライフタイムがあります。

- 受け入れライフタイム
- 送信ライフタイム

新しいキーを追加するときは、ネットワークのすべてのデバイスで同じキーを設定してから新しいキーが有効になるように送信ライフタイムの時間を設定します。古いキーは、ネットワークのすべてのデバイスで新しいキーが有効になった後にのみ削除されます。パケットが受信されると、そのキーのデータを取得するためにキー ID が使用されます。パケットは、暗号化認証アルゴリズムと設定されたキー ID を使用して検証されます。キー ID が検出されない場合、そのパケットはドロップされます。

OSPFv2 暗号化認証のキー チェーンを設定するには、**ip ospf authentication key-chain** コマンドを使用します。

（注） キー チェーンを使用するように OSPFv2 を設定する場合、**ip ospf message-digest-key** コマンドを使用して以前に設定されたすべての MD5 キーは無視されます。

OSPFv2 暗号化認証の設定方法

キー チェーンの定義

手順の概要

1. イネーブル化
2. **configure terminal**
3. **key chain** *name*
4. **key** *key-id*
5. **key-string** *name*
6. **cryptographic-algorithm** *name*
7. **send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
8. **end**

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	**configure terminal** 例： `Device# 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	**key chain** *name* 例： `Device(config)# key chain sample1`	キー チェーンの名前を指定し、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。
ステップ 4	**key** *key-id* 例： `Device(config-keychain)# key 1`	キー ID を指定し、キー チェーン キー コンフィギュレーション モードを開始します。範囲は 1 ～ 255 です。

	コマンドまたはアクション	目的
ステップ 5	**key-string** *name* 例： `Device(config-keychain-key)# key-string string1`	キー ストリングを指定します。
ステップ 6	**cryptographic-algorithm** *name* 例： `Device(config-keychain-key)# cryptographic-algorithm hmac-sha-256`	指定した暗号アルゴリズムでキーを設定します。
ステップ 7	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*} 例： `Device(config-keychain-key)# send-lifetime local 10:00:00 5 July 2013 infinite`	キー チェーンの認証キーが、別のデバイスとのキー交換時に有効に送信される期間を設定します。
ステップ 8	**end** 例： `Device(config-keychain-key)# end`	キーチェーン キー コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

Defining Authentication on an Interface

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface** *type number*
4. **ip ospf authentication key-chain** *name*
5. **end**

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： `Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**interface** *type number* 例： `Device(config)# interface gigabitethernet0/0/0`	インターフェイスのタイプと番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip ospf authentication key-chain** *name* 例： `Device(config-if)# ip ospf authentication key-chain ospf1`	インターフェイスのキー チェーンを指定します。
ステップ 5	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。

OSPFv2 暗号化認証の設定例

例：キー チェーンの定義

次に、キー チェーンを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# key chain sample1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string ThisIsASampleKey12345
Device(config-keychain-key)# cryptographic-algorithm hmac-sha-256
Device(config-keychain-key)# send-lifetime local 10:00:00 5 July 2013 infinite
Device(config-keychain-key)# end
```

例：キー チェーンの確認

show key chain コマンドからの次の出力例に、キー チェーン情報が表示されます。

```
Device# show key chain Key-chain sample1

     key 1 -- text "ThisIsASampleKey12345"
         accept lifetime (always valid) - (always valid) [valid now]
         send lifetime (10:00:00 PDT Jul 5 2013) - (infinite)
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *6*：***show ip ospf interface*** フィールドの説明

フィールド	説明
キー	設定したキーのステータス。
accept lifetime	別のデバイスとのキー交換時にデバイスがそのキーを受け入れる期間。
send lifetime	別のデバイスとのキー交換時にデバイスがそのキーを送信する期間。

例：インターフェイスでの認証の定義

次に、ギガビット イーサネット インターフェイス 0/0/0 で認証を定義する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet0/0/0
Device (config-if)# ip ospf authentication key-chain sample1
Device (config-if)# end
```

例：インターフェイスでの認証の確認

次の **show ip ospf interface** コマンドの出力例に、暗号化の重要な情報を示します。

```
Device# show ip ospf interface GigabitEthernet0/0/0

GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 192.168.8.2/24, Area 1, Attached via Interface Enable
  Process ID 1, Router ID 10.1.1.8, Network Type BROADCAST, Cost: 10
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           10        no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.1.8, Interface address 192.168.8.2
  Backup Designated router (ID) 10.1.1.9, Interface address 192.168.8.9
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
```

```
IETF NSF helper support enabled
Can be protected by per-prefix Loop-Free FastReroute
Can be used for per-prefix Loop-Free FastReroute repair paths
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 10.1.1.9  (Backup Designated Router)
Suppress hello for 0 neighbor(s)
Cryptographic authentication enabled
  Sending SA: Key 25, Algorithm HMAC-SHA-256 - key chain sample1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *7*：*show ip ospf interface* フィールドの説明

フィールド	説明
GigabitEthernet	物理リンクのステータス、およびプロトコルの動作ステータス。
Internet Address	インターフェイス IP アドレス、サブネット マスク、およびエリア アドレス
エリア	OSPF エリア。
プロセス ID	OSPF プロセス ID
コスト	インターフェイスに割り当てられる管理コスト。
Topology-MTID	MTR トポロジマルチトポロジ識別子（MTID）は、ピアに送信する情報が関連付けられるトポロジをプロトコルが識別できるように割り当てられている番号です。
Transmit Delay	転送遅延（秒単位）、インターフェイス ステート、およびルータ プライオリティ
状態	インターフェイスの動作状態。
指定ルータ	指定ルータ ID および各インターフェイス IP アドレス。
Backup Designated router	バックアップ指定ルータ ID および各インターフェイス IP アドレス。
Timer intervals configured	タイマー インターバルの設定
Neighbor Count	ネットワーク ネイバーの数、および隣接ネイバーのリスト。

フィールド	説明
暗号化認証	暗号化認証のステータス。
Sending SA	SA（セキュリティ アソシエーション）送信のステータス。使用されるキー、暗号化アルゴリズム、およびキー チェーン。

OSPFv2 暗号化認証に関する追加情報

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 Command List, All Releases』
OSPF コマンド	『Cisco IOS IP Routing: OSPF Command Reference』

標準および RFC

規格	Title
RFC 2328	『OSPF Version 2』（1998 年 4 月）
RFC 5709	『OSPFv2 HMAC-SHA Cryptographic Authentication』（2009 年 10 月）

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

OSPFv2 暗号化認証の機能情報

表 *8*：*OSPFv2* 暗号化認証の機能情報

機能名	リリース	機能情報
OSPFv2 暗号化認証	15.4(1)T	OSPFv2 暗号化認証機能により、HMAC-SHA アルゴリズムを使用して Open Shortest Path First バージョン 2（OSPFv2）プロトコル パケットを認証することにより、ネットワークでの不正または無効なルーティングアップデートを防止します。 **ip ospf authentication** コマンドが変更されました。

第 6 章

OSPFv3 外部パス プリファレンス オプション

Open Shortest Path First バージョン 3（OSPFv3）の外部パス プリファレンス オプション機能では、RFC 5340 に従って外部パス プリファレンスを計算する方法を提供します。

- 機能情報の確認，97 ページ
- OSPFv3 外部パス プリファレンス オプションについて，98 ページ
- OSPFv3 外部パス プリファレンス オプションの計算方法，98 ページ
- OSPFv3 外部パス プリファレンス オプションの設定例，99 ページ
- その他の参考資料，100 ページ
- OSPFv3 外部パス プリファレンス オプションの機能情報，101 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。

OSPFv3 外部パス プリファレンス オプションについて

OSPFv3 外部パス プリファレンス オプション

RFC 5340 に従い、ASBR または転送アドレスに複数の AS 内パスを使用できる場合、どのパスが優先されるかは次のルールによって示されます。

- 非バックボーン エリアを使用するエリア内パスは、常に最優先されます。
- その他のパス（エリア内バックボーン パスおよびエリア間パス）の優先度は同等です。

これらのルールは、複数のエリアを通って ASBR に到達可能な場合、または複数存在する AS-external-LSA のいずれを優先するかを決定しようとする場合に適用されます。前者の場合、パスはすべて同じ ASBR で終端し、後者の場合は異なる ASBR または転送アドレスで終端します。いずれの場合も、各パスは異なるルーティング テーブルのエントリで表されます。この機能は、**no compatibility rfc1583** コマンドを使用して RFC 1583 との互換性がディセーブルに設定されている場合のみ適用されます（RFC 5340 は RFC 1583 の更新情報を提供します）。

注意 ルーティングループの可能性を最小限に抑えるには、OSPFルーティング ドメイン内のすべての OSPF ルータに対して同じ RFC の互換性を設定します。

OSPFv3 外部パス プリファレンス オプションの計算方法

RFC 5340 に従った OSPFv3 外部パス プリファレンスの計算

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospfv3**[*process-id*]
4. **nocompatiblerfc1583**

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： `Device> 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： `Device# 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	**routerospfv3**[*process-id*] 例： `Device(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**nocompatiblerfc1583** 例： `Device(config-router)# no compatible rfc1583`	RFC 5340 に従った外部パス プリファレンス計算に使用する方法を変更します。

OSPFv3 外部パス プリファレンス オプションの設定例

例：RFC 5340 に従った OSPFv3 外部パス プリファレンスの計算

```
show ospfv3

Routing Process "ospfv3 1" with ID 10.1.1.1
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Reference bandwidth unit is 100 mbps
 RFC 1583 compatibility disabled
    Area BACKBONE(0) (Inactive)
        Number of interfaces in this area is 1
        SPF algorithm executed 1 times
        Number of LSA 1. Checksum Sum 0x00D03D
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

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
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』
OSPFv3 外部パス プリファレンス オプション	*Configuring OSPF* モジュール

標準および RFC

標準/RFC	Title
IPv6 に関する RFC	IPv6 の RFC

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

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

OSPFv3 外部パス プリファレンス オプションの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *9*：*OSPFv3* 外部パス プリファレンス オプションの機能情報

機能名	リリース	機能情報
OSPFv3 外部パス プリファレンス オプション	Cisco IOS XE Release 3.4S	この機能により、RFC 5340 に従って外部パス プリファレンスを計算する方法が提供されます。 次のコマンドが導入または変更されました。**compatible rfc1583**、**show ospfv3**

第 7 章

『OSPFv3 Graceful Restart』

Open Shortest Path First バージョン 3（OSPFv3）でグレースフル リスタート機能を使用すると、OSPFv3 ルーティング プロトコル情報の復元中も、既知のルートを使用してノンストップ データ フォワーディングを実行できます。

- 機能情報の確認，103 ページ
- OSPFv3 グレースフル リスタートに関する情報，104 ページ
- OSPFv3 グレースフル リスタートをイネーブルにする方法，104 ページ
- OSPFv3 グレースフル リスタートの設定例，108 ページ
- その他の参考資料，109 ページ
- OSPFv3 グレースフル リスタートの機能情報，110 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。

OSPFv3 グレースフル リスタートに関する情報

『OSPFv3 Graceful Restart』

OSPFv3 でグレースフル リスタート機能を使用すると、OSPFv3 ルーティング プロトコル情報の復元中も、既知のルートを使用してノンストップデータ フォワーディングを実行できます。デバイスは、再起動モード（グレースフル リスタート対応デバイスなど）か、ヘルパー モード（グレースフルリスタート認識デバイスなど）のいずれかで、グレースフルリスタートに参加できます。

グレースフル リスタート機能を実行するには、デバイスがハイ アベイラビリティ（HA）ステートフル スイッチオーバー（SSO）モード（つまり、デュアル ルート プロセッサ（RP））になっている必要があります。グレースフル リスタート機能を備えたデバイスは、次の場合に、グレースフル リスタート機能を実行します。

- RP 障害が発生し、スタンバイ RP へのスイッチオーバーが行われた場合
- スタンバイ RP への計画的な RP スイッチオーバーが行われた場合

グレースフルリスタート機能では、隣接デバイスがグレースフルリスタート認識である必要があります。

SSO およびノンストップ フォワーディング（NSF）の詳細については、「Stateful Switchover」および「Cisco Nonstop Forwarding」を参照してください。

OSPFv3グレースフルリスタートをイネーブルにする方法

グレースフル リスタート対応ルータでの OSPFv3 グレースフル リスタートのイネーブル化

次のタスクは、Cisco IOS XE Release 3.4S 以降のリリースで実行できます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospfv3**[*process-id*]
4. **graceful-restart**[**restart-interval** *interval*]

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	**routerospfv3**[*process-id*] 例： `Router(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**graceful-restart**[**restart-interval** *interval*] 例： `Router(config-rtr)# graceful-restart`	グレースフルリスタート対応ルータで OSPFv3 グレースフル リスタート機能をイネーブルにします。

グレースフル リスタート対応ルータでの OSPFv3 グレースフル リスタートのイネーブル化

次のタスクは、Cisco IOS XE Release 3.4S 以前のリリースで実行できます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6routerospf***process-id*
4. **graceful-restart**[**restart-interval** *interval*]

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	**ipv6routerospf***process-id* 例： `Router(config)# ipv6 router ospf 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**graceful-restart**[**restart-interval** *interval*] 例： `Router(config-rtr)# graceful-restart`	グレースフルリスタート対応ルータで OSPFv3 グレースフル リスタート機能をイネーブルにします。

グレースフル リスタート認識ルータでの OSPFv3 グレースフル リスタートのイネーブル化

次のタスクは、Cisco IOS XE Release 3.4S 以降のリリースで実行できます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospfv3**[*process-id*]
4. **graceful-restarthelper** {**disable** | **strict-lsa-checking**

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	**routerospfv3**[*process-id*] 例： `Router(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**graceful-restarthelper** {**disable** | **strict-lsa-checking** 例： `Router(config-rtr)# graceful-restart helper strict-lsa-checking`	グレースフルリスタート認識ルータで OSPFv3 グレースフル リスタート機能をイネーブルにします。

例：

次の作業

グレースフル リスタート認識ルータでの OSPFv3 グレースフル リスタートのイネーブル化

次のタスクは、Cisco IOS XE Release 3.4S 以前のリリースで実行できます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6routerospf***process-id*
4. **graceful-restarthelper** {**disable** | **strict-lsa-checking**

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	**ipv6routerospf***process-id* 例： `Router(config)# ipv6 router ospf 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**graceful-restarthelper** {**disable** | **strict-lsa-checking** 例： `Router(config-rtr)# graceful-restart helper strict-lsa-checking`	グレースフルリスタート認識ルータでOSPFv3 グレースフル リスタート機能をイネーブルにします。

例：

次の作業

OSPFv3 グレースフル リスタートの設定例

例：OSPFv3 グレースフル リスタートのイネーブル化

```
Router# show ipv6 ospf graceful-restart
Routing Process "ospf 1"
 Graceful Restart enabled
    restart-interval limit: 120 sec, last restart 00:00:15 ago (took 36 secs)
  Graceful Restart helper support enabled
  Router status : Active
  Router is running in SSO mode
  OSPF restart state : NO_RESTART
  Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0
```

次の例に、グレースフル リスタート認識ルータでグレースフル リスタート ヘルパー サポートがイネーブルになっている OSPFv3 の情報を示します。

```
Router# show ospfv3
 Routing Process "ospfv3 1" with ID 10.0.0.1
 Supports IPv6 Address Family
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 Graceful restart helper support enabled
 Reference bandwidth unit is 100 mbps
 Relay willingness value is 128
 Pushback timer value is 2000 msecs
 Relay acknowledgement timer value is 1000 msecs
 LSA cache Disabled : current count 0, maximum 1000
 ACK cache Disabled : current count 0, maximum 1000
 Selective Peering is not enabled
 Hello requests and responses will be sent multicast
```

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
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
ステートフル スイッチオーバーおよびノンストップ フォワーディング	『*High Availability Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』
『OSPFv3 Graceful Restart』	*OSPF RFC 3623 Graceful Restart Helper Mode* モジュール
『OSPFv3 Graceful Restart』	*Configuring OSPF* モジュール
『OSPFv3 Graceful Restart』	*NSF-OSPF RFC 3623 OSPF Graceful Restart* モジュール

標準および RFC

標準/RFC	Title
IPv6 に関する RFC	IPv6 の RFC

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

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

OSPFv3 グレースフル リスタートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *10* : *OSPFv3* グレースフル リスタートの機能情報

機能名	リリース	機能情報
『OSPFv3 Graceful Restart』	Cisco IOS XE Release 2.1	OSPFv3 でグレースフル リスタート機能を使用すると、OSPFv3 ルーティング プロトコル情報の復元中も、既知のルートを使用してノンストップデータ フォワーディングを実行できます。 次のコマンドが導入または変更されました。**graceful-restart**、**graceful-restart helper**、**ipv6 router ospf**、**router ospfv3**、**show ipv6 ospf graceful-restart**、**show ospfv3 graceful-restart**

第 8 章

OSPFv3のグレースフルシャットダウンのサポート

この機能により、可能な限り安全な方法で Open Shortest Path First バージョン 3（OSPFv3）のプロセスやインターフェイスを一時的にシャットダウンし、これをネイバーに通知することができます。プロトコルのグレースフルシャットダウンは、すべてのOSPFv3インターフェイスまたは特定のインターフェイスで実行できます。

- 機能情報の確認，113 ページ
- OSPFv3 グレースフル シャットダウン サポートについて，114 ページ
- OSPFv3 グレースフル シャットダウン サポートの設定方法，114 ページ
- OSPFv3 グレースフル シャットダウン サポートの設定例，119 ページ
- OSPFv3 グレースフル シャットダウン サポートに関する追加情報，120 ページ
- OSPFv3 グレースフル シャットダウン サポートの機能情報，120 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。

OSPFv3 グレースフル シャットダウン サポートについて

OSPFv3 グレースフル シャットダウン

OSPFv3 のグレースフル シャットダウン機能では、可能な限り安全な方法で OSPFv3 プロトコルを一時的にシャットダウンして、これをネイバーに通知する機能を提供します。ネットワークに別のパスがあるすべてのトラフィックは、その代替パスに送信されます。OSPFv3 プロトコルのグレースフル シャットダウンは、ルータ コンフィギュレーション モードまたはアドレス ファミリ コンフィギュレーション モードで **shutdown** コマンドを使用して実行できます。

この機能は、特定のインターフェイスで OSPFv3 をシャットダウンする機能も提供します。この場合、OSPFv3 はインターフェイスをアドバタイズせず、インターフェイスを介して隣接関係を形成しません。ただし、すべての OSPFv3 インターフェイス設定が保持されます。インターフェイスのグレースフル シャットダウンを実行するには、インターフェイス コンフィギュレーション モードで **ipv6ospfshutdown** または **ospfv3shutdown** コマンドを使用します。

OSPFv3 グレースフル シャットダウン サポートの設定方法

OSPFv3 プロセスのグレースフル シャットダウンの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. 次のいずれかを実行します。
   - **ipv6routerospf***process-id*
   - **routerospfv3***process-id*
4. シャットダウン
5. **end**
6. 次のいずれかを実行します。
   - **showipv6ospf** [*process-id*]
   - **showospfv3** [*process-id*]

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	**configureterminal** 例： `Device# 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	次のいずれかを実行します。
	• **ipv6routerospf***process-id*
	• **routerospfv3***process-id*
	
	例：
	`Device(config)# ipv6 router ospf 1`
	
	例：
	`Device(config)# router ospfv3 101`
		OSPFv3 ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。

ステップ 4	シャットダウン 例： `Device(config-router)# shutdown`	選択したインターフェイスをシャットダウンします。
ステップ 5	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。

ステップ 6	次のいずれかを実行します。
	• **showipv6ospf** [*process-id*]
	• **showospfv3** [*process-id*]
	
	例：
	`Device# show ipv6 ospf`
	
	例：
	`Device# show ospfv3`
		（任意）OSPFv3 ルーティング プロセスに関する一般情報を表示します。

アドレス ファミリ コンフィギュレーション モードでの OSPFv3 プロセス のグレースフル シャットダウンの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospfv3**[*process-id*]
4. **address-family ipv6unicast** [**vrf** *vrf-name*]
5. シャットダウン
6. **end**
7. **showospfv3** [*process-id*]

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	**configureterminal** 例： `Device# 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	**routerospfv3**[*process-id*] 例： `Device(config)# router ospfv3 1`	IPv6 アドレス ファミリのルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**address-family ipv6unicast** [**vrf** *vrf-name*] 例： `Device(config-router)#address-family ipv6`	OSPFv3 の IPv6 アドレス ファミリ 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 5	シャットダウン 例： `Device(config-router-af)# shutdown`	選択したインターフェイスをシャットダウンします。
ステップ 6	**end** 例： `Device(config-router-af)# end`	特権 EXEC モードに戻ります。
ステップ 7	**showospfv3** [*process-id*] 例： `Device# show ospfv3`	（任意）OSPFv3 ルーティング プロセスに関する一般情報を表示します。

OSPFv3 インターフェイスの OSPFv3 グレースフル シャットダウンの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. 次のいずれかを実行します。
   - **ipv6ospfshutdown**
   - **ospfv3shutdown**
5. **end**
6. **showospfv3***process-id*[*area-id*][*address-family*][**vrf** {*vrf-name*| ***}] **interface** [*typenumber*] [**brief**]

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： `Device> 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： `Device# 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	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet`	インターフェイスのタイプと番号を設定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかを実行します。
	• **ipv6ospfshutdown**
	• **ospfv3shutdown**
	例：
	`Device(config-if)# ipv6 ospf shutdown`
	例：
	`Device(config-if)# ospfv3 process-id ipv6 shutdown`
		インターフェイス レベルで OSPFv3 プロトコル グレースフル シャットダウンを開始します。
		• **ipv6ospfshutdown** インターフェイス コマンドを入力すると、これを設定したインターフェイスは、停止しようとしているネイバーをアドバイスするリンクステート アップデートを送信します。これにより、ネイバーは、このデバイスを含む OSPFv3 トラフィックをルーティングできるようになります。

ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**showospfv3***process-id*[*area-id*][*address-family*][**vrf** {*vrf-name*| *****}] **interface** [*typenumber*] [**brief**] 例： `Device# show ospfv3 1 interface`	（任意）OSPFv3 関連のインターフェイス情報を表示します。

OSPFv3 グレースフル シャットダウン サポートの設定例

例：OSPFv3 プロセスのグレースフル シャットダウンの設定

次に、IPv6 ルータの OSPF コンフィギュレーション モードで OSPFv3 プロセスのグレースフル シャットダウンを設定する例を示します。

```
ipv6 router ospf 6
 router-id 10.10.10.10
 shutdown
```

次に、OSPFv3 ルータ コンフィギュレーション モードで OSPFv3 プロセスのグレースフル シャットダウンを設定する例を示します。

```
!
router ospfv3 1
 shutdown
 !
 address-family ipv6 unicast
  exit-address-family
```

次に、アドレス ファミリ コンフィギュレーション モードで OSPFv3 プロセスのグレースフル シャットダウンを設定する例を示します。

```
!
router ospfv3 1
 !
 address-family ipv6 unicast
  shutdown
  exit-address-family
```

例：OSPFv3 インターフェイスのグレースフル シャットダウンの設定

次に、**ipv6ospfshutdown** コマンドを使用して、OSPFv3 インターフェイスのグレースフル シャットダウンを設定する例を示します。

```
!
interface Serial2/1
 no ip address
 ipv6 enable
 ipv6 ospf 6 area 0
 ipv6 ospf shutdown
 serial restart-delay 0
 end
```

次に、**ospfv3shutdown** コマンドを使用して、OSPFv3 インターフェイスのグレースフル シャットダウンを設定する例を示します。

```
!
interface Serial2/0
 ip address 10.10.10.10 255.255.255.0
 ip ospf 1 area 0
 ipv6 enable
 ospfv3 shutdown
 ospfv3 1 ipv6 area 0
 serial restart-delay 0
 end
```

OSPFv3 グレースフル シャットダウン サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
『Configuring OSPF』	『Configuring OSPF』
OSPF コマンド	『Cisco IOS IP Routing: OSPF Command Reference』
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

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

OSPFv3 グレースフル シャットダウン サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *11* : *OSPFv3* グレースフル シャットダウン サポートの機能情報

機能名	リリース	機能情報
OSPFv3 のグレースフル シャットダウンのサポート	Cisco IOS XE Release 3.8	この機能により、可能な限り安全な方法で Open Shortest Path First バージョン 3（OSPFv3）のプロセスやインターフェイスを一時的にシャットダウンし、これをネイバーに通知することができます。 プロトコルのグレースフル シャットダウンは、すべての OSPFv3 インターフェイスまたは特定のインターフェイスで実行できます。 次のコマンドが導入されました。 • **ipv6ospfshutdown** • **ospfv3shutdown** • **shutdown(router ospfv3)**

第 9 章

『OSPF Stub Router Advertisement』

OSPF スタブ ルータ アドバタイズメント機能を使用すると、新しいルータをネットワークに組み込むときに、新しいルータがトラフィックのルーティングにすぐに使用されないようにできます。また、他のネットワーク宛のパケットをドロップすることなく、ルータを正常にシャットダウンしたり、リロードを実行できるようになります。

- 機能情報の確認，123 ページ
- OSPF スタブ ルータ アドバタイズメントに関する情報，124 ページ
- OSPF スタブ ルータ アドバタイズメントの設定方法，126 ページ
- OSPF スタブ ルータ アドバタイズメントの設定例，130 ページ
- その他の参考資料，131 ページ
- OSPF スタブ ルータ アドバタイズメントの機能情報，132 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。

OSPF スタブ ルータ アドバタイズメントに関する情報

OSPF スタブ ルータ アドバタイズメント機能

OSPF スタブ ルータ アドバタイズメント機能を使用すると、新しいルータをネットワークに組み込むときに、新しいルータがトラフィックのルーティングにすぐに使用されないようにできます。また、他のネットワーク宛のパケットをドロップすることなく、ルータを正常にシャットダウンしたり、リロードを実行できるようになります。この機能には3つの設定オプションがあります。これらのオプションによって、Open Shortest Path First（OSPF）プロトコルを実行するルータが、すべてのネイバーに対して最大メトリックまたは無限メトリックをアドバタイズするように設定できます。

これらの 3 つの設定オプションのいずれかがルータでイネーブルになっていると、ルータは、スタブではないリンクをすべて使用して、最大メトリック（LSInfinity: 0xFFFF）のリンクステートアドバタイズメント（LSA）を送信します。最大メトリックがアドバタイズされると、他のルータは、その新しいルータに対して、代替パスを使用するよりも高いコストを割り当てます。新しいルータを経由するパスに高いコストが割り当てられた結果、他のルータは、新しいルータを経由するパスを、他のネットワーク宛のトラフィックを転送するための通過パスとして使用しなくなります。これによって、スイッチング機能およびルーティング機能の準備が整い、ルーティング テーブルがコンバージされた後に、通過トラフィックのルーティングをこのルータで開始することができます。

（注） スタブ リンクのコストは常に出力インターフェイス コストに設定されているので、最大または無限のメトリックを設定しても、スタブ ネットワーク内の直接接続リンクには影響しません。

最大メトリックを使用したルーティング テーブルのコンバージ

OSPF スタブ ルータ アドバタイズメント機能に用意されている 2 つの設定オプションを使用すると、新しいルータをネットワークに組み込むときに、新しいルータがトラフィックのルーティングにすぐに使用されないようにできます。Interior Gateway Protocol（IGP）のコンバージェンスは、ルータの起動中またはリロード後に非常に短時間で行われ、通常、ボーダーゲートウェイプロトコル（BGP）のルーティング テーブルのコンバージよりも先に完了します。このため、これらの設定オプションが役に立ちます。ルータでBGPルーティングテーブルを構築中に、ネイバールータがこのルータを経由してトラフィック転送を行うと、受信した他の宛先のパケットをドロップする可能性があります。起動中に最大メトリックをアドバタイズすることによって、ルーティング テーブルがコンバージされた後に、他のネットワーク宛のトラフィックの送信をこのルータで開始することができます。

次の2つの設定オプションによって、ルータは起動時に最大メトリックをアドバタイズできます。

- ルータの起動時またはリロード時に、最大メトリックをアドバタイズするためのタイマーを設定します。このオプションを設定すると、タイマーが期限切れになるまで、ルータは最大メトリックをアドバタイズし、これにより、ネイバールータは強制的に代替パスを選択します。タイマーが期限切れになると、ルータは正しい（通常の）メトリックをアドバタイズし、他のルータはコストに応じてこのルータにトラフィックを送信します。タイマーの設定可能範囲は 5 ～ 86,400（秒）です。
- BGPルーティングテーブルがコンバージされるまでの間、または、デフォルトタイマー（600秒）が期限切れになるまでの間、ルータが最大メトリックをアドバタイズするように設定します。BGP ルーティング テーブルがコンバージされるか、または、デフォルト タイマーが期限切れになると、ルータは正しい（通常の）メトリックをアドバタイズし、他のルータはコストに応じてこのルータにトラフィックを送信します。

最大メトリックを使用したルータのグレースフル シャットダウン

OSPF スタブ ルータ アドバタイズメント機能に用意されている 3 つ目の設定オプションは、ルータのシャットダウンの前に、すべてのリンクを使用して最大メトリックをアドバタイズすることによって、他のルータが通過トラフィックの転送のために代替パスを選択するようにします。これにより、ルータをネットワークから正常に削除できます。ルータをネットワークから削除することが必要となる状況は多数あります。ルータがネットワークから削除され、物理インターフェイスがダウンしたことをネイバールータが検出できない場合、ネイバーは、デッドタイマーが期限切れになるまで待機してから、隣接関係を削除し、ルーティング テーブルを再コンバージします。シャットダウンしたルータと他のルータとの間にスイッチがある場合に、このような状況が発生する可能性があります。ネイバーのルーティング テーブルの再コンバージェンス中に、パケットをドロップする可能性があります。

この 3 つ目のオプションを設定すると、ルータが最大メトリックをアドバタイズするため、ルータのシャットダウンの前は、ネイバー ルータが通過トラフィックの転送のために代替パスを選択するようになります。また、この設定オプションを使用すると、他のネットワーク宛のトラフィックに影響を与えずに、クリティカルな状況のルータをネットワークから削除できます。

（注） ルータの実行コンフィギュレーションがグレースフル シャットダウンを行うよう設定されている場合は、その実行コンフィギュレーションを保存しないでください。保存すると、ルータが、リロード後に最大メトリックをアドバタイズし続けることになります。

OSPF スタブ ルータ アドバタイズメントの利点

安定性とアベイラビリティの向上

起動時またはリロード時にすべてのリンクを使用して最大メトリックをアドバタイズすることによって、ネイバー ルータがこのルータを経由するパスを通過パスとして使用することを防ぎま

す。これにより、パケットのドロップ数が減少し、ネットワークの安定性とアベイラビリティが向上します。

ネットワークからのグレースフルな削除

シャットダウン前に最大メトリックをアドバタイズすることによって、このルータを経由する通過パスがアクセス不可になる前に、他のルータが代替パスを選択するようにします。

OSPF スタブ ルータ アドバタイズメントの設定方法

次のタスクでは、最大メトリックをアドバタイズするよう OSPF を設定します。この機能には、3 つの異なる設定オプションがあります。すべてのタスクは任意で、個別に設定する必要があります。

起動時アドバタイズメントの設定

手順の概要

1. Router(config)# **router ospf** *process-id*
2. Router(config-router)# **max-metric router-lsa on-startup** *announce-time*

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(config)# **router ospf** *process-id*	ルータでルータ コンフィギュレーション モードを開始し、OSPF ルーティング プロセスをイネーブルにします。
ステップ 2	Router(config-router)# **max-metric router-lsa on-startup** *announce-time*	指定した期間最大メトリックを起動時にアドバタイズするよう、OSPF を設定します。*announce-time* 引数は、設定可能なタイマーです。**on-startup** キーワードの後に指定します。デフォルトのタイマー値はありません。構成可能な時間範囲は 5 ～ 86,400 秒です。

ルーティング テーブル コンバージ中のアドバタイズメントの設定

手順の概要

1. Router(config)# **router ospf** *process-id*
2. Router(config-router)# **max-metric router-lsa on-startup wait-for-bgp**

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(config)# **router ospf** *process-id*	ルータでルータ コンフィギュレーション モードを開始し、OSPF ルーティング プロセスをイネーブルにします。
ステップ 2	Router(config-router)# **max-metric router-lsa on-startup wait-for-bgp**	BGP ルーティング テーブルがコンバージされるまでの間、または、デフォルトタイマーが期限切れになるまでの間、最大メトリックをアドバタイズするように OSPF を設定します。**wait-for-bgp** キーワードは、**on-startup** キーワードの後に指定する必要があります。デフォルトのタイマー値は 600 秒です。

グレースフル シャットダウンのためのアドバタイズメントの設定

手順の概要

1. Router(config)# **router ospf**process-id
2. Router(config-router)# **max-metric router-lsa**
3. Router(config-router)# **end**
4. Router# **show ip ospf**

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(config)# **router ospf**process-id	ルータでルータ コンフィギュレーション モードを開始し、OSPF ルーティング プロセスをイネーブルにします。
ステップ 2	Router(config-router)# **max-metric router-lsa**	ルータがシャットダウンされるまでの間、最大メトリックをアドバタイズするように OSPF を設定します。
ステップ 3	Router(config-router)# **end**	コンフィギュレーション モードを終了して、ルータを特権 EXEC モードにします。
ステップ 4	Router# **show ip ospf**	OSPF ルーティング プロセスに関する一般情報を表示します。 • ルータをシャットダウンまたはリロードする前に **max-metric router-lsa** コマンドがイネーブルになっていることを確認するには、**show ip ospf** コマンドを使用します。

次の作業

（注） ルータの実行コンフィギュレーションがグレースフル シャットダウンを行うよう設定されている場合は、その実行コンフィギュレーションを保存しないでください。保存すると、ルータが、リロード後に最大メトリックをアドバタイズし続けることになります。

最大メトリックのアドバタイズメントの確認

最大メトリックのアドバタイズメントが正しく設定されていることを確認するには、**show ip ospf** または **show ip ospf database** コマンドを使用します。

show ip ospf コマンドの出力には、**max-metric router-lsa** コマンドで設定したオプションの種類に応じて、設定条件、状態、および、最大メトリック アドバタイズメントのタイマーの残り時間が表示されます。

on-startup キーワードおよび *announce-time* 引数を **max-metric router-lsa** コマンドに指定した場合に表示される出力は、次の出力例のようになります。

```
Router# show ip ospf
Routing Process "ospf 1998" with ID 10.18.134.155
     Supports only single TOS(TOS0) routes
     Supports opaque LSA
     It is an area border and autonomous system boundary router
     Redistributing External Routes from,
        static, includes subnets in redistribution
     Originating router-LSAs with maximum metric, Time remaining: 00:01:18
        Condition: on startup for 300 seconds, State: active
     SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
     Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
     Number of external LSA 7. Checksum Sum 0x47261
     Number of opaque AS LSA 0. Checksum Sum 0x0
     Number of DCbitless external and opaque AS LSA 0
     Number of DoNotAge external and opaque AS LSA 0
     Number of areas in this router is 2. 1 normal 0 stub 1 nssa
     External flood list length 0
        Area BACKBONE(0)
           Number of interfaces in this area is 1
           Area has no authentication
           SPF algorithm executed 3 times
           Area ranges are
           Number of LSA 8. Checksum Sum 0x474AE
           Number of opaque link LSA 0. Checksum Sum 0x0
```

on-startup および **wait-for-bgp** キーワードを **max-metric router-lsa** コマンドに指定した場合に表示される出力は、次の出力例のようになります。

```
Router# show ip ospf
Routing Process "ospf 1998" with ID 10.18.134.155
     Supports only single TOS(TOS0) routes
     Supports opaque LSA
     It is an area border and autonomous system boundary router
     Redistributing External Routes from,
        static, includes subnets in redistribution
     Originating router-LSAs with maximum metric, Time remaining: 00:01:18
        Condition: on startup while BGP is converging, State: active
     SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
     Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
     Number of external LSA 7. Checksum Sum 0x47261
```

```
     Number of opaque AS LSA 0. Checksum Sum 0x0
     Number of DCbitless external and opaque AS LSA 0
     Number of DoNotAge external and opaque AS LSA 0
     Number of areas in this router is 2. 1 normal 0 stub 1 nssa
     External flood list length 0
        Area BACKBONE(0)
           Number of interfaces in this area is 1
           Area has no authentication
           SPF algorithm executed 3 times
           Area ranges are
           Number of LSA 8. Checksum Sum 0x474AE
           Number of opaque link LSA 0. Checksum Sum 0x0
```

max-metric router-lsa コマンドにキーワードや引数を指定しなかった場合に表示される出力は、次の出力例のようになります。

```
Router# show ip ospf
Routing Process "ospf 1998" with ID 10.18.134.155
     Supports only single TOS(TOS0) routes
     Supports opaque LSA
     It is an area border and autonomous system boundary router
     Redistributing External Routes from,
        static, includes subnets in redistribution
     Originating router-LSAs with maximum metric
        Condition: always, State: active
     SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
     Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
     Number of external LSA 7. Checksum Sum 0x47261
     Number of opaque AS LSA 0. Checksum Sum 0x0
     Number of DCbitless external and opaque AS LSA 0
     Number of DoNotAge external and opaque AS LSA 0
     Number of areas in this router is 2. 1 normal 0 stub 1 nssa
     External flood list length 0
        Area BACKBONE(0)
           Number of interfaces in this area is 1
           Area has no authentication
           SPF algorithm executed 3 times
           Area ranges are
           Number of LSA 8. Checksum Sum 0x474AE
           Number of opaque link LSA 0. Checksum Sum 0x0
```

show ip ospf database コマンドの出力には、OSPF LSA に関する情報が表示され、ルータが最大のリンク コストをアナウンスしているかどうかが示されます。**max-metric router-lsa** コマンドをどのような形式で指定したかにかかわらず、表示される出力は次の出力例のようになります。

```
Router# show ip ospf database
       Exception Flag: Announcing maximum link costs
       LS age: 68
       Options: (No TOS-capability, DC)
       LS Type: Router Links
       Link State ID: 172.18.134.155
       Advertising Router: 172.18.134.155
       LS Seq Number: 80000002
       Checksum: 0x175D
       Length: 60
       Area Border Router
       AS Boundary Router
       Number of Links: 3

         Link connected to: a Transit Network
         (Link ID) Designated Router address: 192.168.1.11
         (Link Data) Router Interface address: 192.168.1.14
          Number of TOS metrics: 0
           TOS 0 Metrics: 65535 (metric used for local calculation: 10)

         Link connected to: a Transit Network
         (Link ID) Designated Router address: 10.1.145.11
         (Link Data) Router Interface address: 10.1.145.14
          Number of TOS metrics: 0
           TOS 0 Metrics: 65535 (metric used for local calculation: 10)
```

```
Link connected to: a Stub Network
(Link ID) Network/subnet number: 10.11.12.0
(Link Data) Network Mask: 255.255.255.0
 Number of TOS metrics: 0
  TOS 0 Metrics: 1
```

OSPF スタブ ルータ アドバタイズメントのモニタリングおよびメンテナンス

コマンド	目的
`Router#` **show ip ospf**	OSPF ルーティング プロセスに関する一般情報を表示します。OSPF スタブ ルータ アドバタイズメント機能の設定およびステータス情報も含まれています。
`Router#` **show ip ospf database router**	ルータ LSA に関する情報を表示します。ルータが最大のリンク コストをアナウンスしているかどうかがわかります。

OSPF スタブ ルータ アドバタイズメントの設定例

例：起動時アドバタイズメント

次の例では、OSPFを実行するルータを、起動時に300秒間最大メトリックをアドバタイズするように設定しています。

```
Router(config)# router ospf 100
 Router(config-router)# max-metric router-lsa on-startup 300
```

例：ルーティング テーブルのコンバージまでのアドバタイズメント

次の例では、OSPF を実行するルータを、BGP ルーティング テーブルがコンバージされるまでの間、または、デフォルト タイマー（600 秒）が期限切れになるまでの間、最大メトリックをアドバタイズするように設定しています。

```
Router(config)# router ospf 100
 Router(config-router)# max-metric router-lsa on-startup wait-for-bgp
```

例：グレースフル シャットダウン

次の例では、OSPFを実行するルータを、ルータがシャットダウンされるまでの間、最大メトリックをアドバタイズするように設定しています。

```
Router(config)# router ospf 100
 Router(config-router)# max-metric router-lsa
 Router(config-router)# end
 Router# show ip ospf
```

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』
OSPF コマンド：コマンド構文の詳細、コマンドモード、デフォルト設定、コマンド履歴、使用に関する注意事項および例	『*Cisco IOS IP Routing: OSPF Command Reference*』
『Configuring OSPF』	『*IP Routing: OSPF Configuration Guide*』の「Configuring OSPF」
OSPFv2 Loop-Free Alternate Fast Reroute	『*IP Routing: OSPF Configuration Guide*』の「OSPFv2 Loop-Free Alternate Fast Reroute」

標準および RFC

標準/RFC	Title
RFC 5286	『*Basic Specification for IP Fast Reroute: Loop-Free Alternates*』

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

OSPF スタブ ルータ アドバタイズメントの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *12* : *OSPF* スタブ ルータ アドバタイズメントの機能情報

機能名	リリース	機能情報
『OSPF Stub Router Advertisement』	Cisco IOS XE Release 2.1	OSPF スタブ ルータ アドバタイズメント機能を使用すると、新しいルータをネットワークに組み込むときに、新しいルータがトラフィックのルーティングにすぐに使用されないようにできます。また、他のネットワーク宛のパケットをドロップすることなく、ルータを正常にシャットダウンしたり、リロードを実行できるようになります。 次に示すコマンドは、この章に記載されている機能において、新たに導入または変更されたものです。 • **max-metricrouter-lsa** • **showipospf**

第 10 章

OSPF アップデート パケット ペーシング タイマー設定

この章では、OSPF アップデート パケット ペーシング タイマー設定機能について説明します。この機能を使用すると、OSPF LSA のフラッド ペーシング、再送信ペーシング、およびグループ ペーシングの更新間隔を設定できます。

- 機能情報の確認，135 ページ
- OSPF アップデート パケット ペーシング タイマー設定の制約事項，136 ページ
- OSPF アップデート パケットペーシング タイマー設定について，136 ページ
- OSPF パケットペーシング タイマーの設定方法，137 ページ
- OSPF アップデート パケット ペーシングの設定例，140 ページ
- その他の参考資料，141 ページ
- OSPF アップデート パケット ペーシング タイマー設定の機能情報，142 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。

OSPF アップデート パケット ペーシング タイマー設定の制約事項

OSPF パケット フラッディングの要件を満たす他のオプションをすべて使用した場合に限り、パケット ペーシング タイマーを変更してください。特に、ネットワーク オペレータは、デフォルト タイマーを変更する前に、要約、スタブエリアの使用方法、キューの調整、およびバッファの調整を優先して行う必要があります。さらに、タイマー値を変更するガイドラインはなく、各 OSPF 配備は一意であり、ケースバイケースで考慮する必要があります。ネットワーク オペレータは、デフォルト タイマー値の変更に関連したリスクを前提に考える必要があります。

OSPF アップデート パケットペーシング タイマー設定について

OSPF アップデート パケットペーシング タイマーの機能

状況によっては、非常に多数のリンクステート アドバタイズメント（LSA）のフラッディングによる、CPU またはバッファ使用率の問題を解消するため、Open Shortest Path First（OSPF）のパケット ペーシングのデフォルト タイマーの変更が必要になることがあります。OSPF アップデート パケット ペーシング タイマー設定機能を使用すると、OSPF LSA のフラッド ペーシング、再送信ペーシング、およびグループ ペーシングの更新間隔を設定できます。

- OSPF フラッド ペーシング タイマーを設定すると、OSPF 伝送キュー内の連続する各リンクステート アップデート パケットの間のパケット間スペースを制御できます。
- OSPF 再送信ペーシング タイマーを設定すると、OSPF 再送信キュー内の連続する各リンクステート アップデート パケットの間のパケット間スペースを制御できます。
- Cisco IOS XE ソフトウェアは、LSA の定期的なリフレッシュをグループ化して、大規模なトポロジでのリフレッシュに関する LSA パッキング密度を改善します。グループ タイマーは、グループ化された LSA のリフレッシュに使用する間隔を制御します。個々の LSA のリフレッシュ頻度（デフォルトのリフレッシュ間隔は 30 分）を変更するものではありません。

注意 大部分の OSPF 展開では、OSPF パケットペーシング タイマーのデフォルト設定で十分です。デフォルト タイマーの変更は最後の手段です。

OSPF アップデート パケットペーシング タイマー設定の利点

管理者は、OSPF アップデート パケット ペーシング タイマー設定機能を使用して、LSA の更新間隔を制御できます。これによって、非常に多数の LSA のフラッディングがエリアで発生した場合に、CPU またはバッファ使用率の上昇を抑制できます。

OSPF パケットペーシング タイマーの設定方法

このセクションのタスクでは、3 つの OSPF アップデート パケットペーシング タイマーを設定および確認する方法を説明します。

OSPF パケット ペーシング タイマーの設定

注意 大部分の OSPF 展開では、OSPF パケットペーシング タイマーのデフォルト設定で十分です。デフォルト タイマーの変更は最後の手段です。

フラッド パケット ペーシング タイマーを設定するには、グローバル 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. Router(config)# **router ospf** process-id
2. Router(config-router)# **timers pacing flood** milliseconds

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(config)# **router ospf** process-id	ルータでルータ コンフィギュレーション モードを開始し、OSPF ルーティング プロセスをイネーブルにします。
ステップ 2	Router(config-router)# **timers pacing flood** milliseconds	フラッド パケット ペーシング タイマーの待機時間（ミリ秒）を設定します。

再送信パケット ペーシング タイマーの設定

再送信パケット ペーシング タイマーを設定するには、グローバル 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. Router(config)# **router ospf** process-id
2. Router(config-router)# **timers pacing retransmission** milliseconds

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(config)# **router ospf** process-id	ルータでルータ コンフィギュレーション モードを開始し、OSPF ルーティング プロセスをイネーブルにします。
ステップ 2	Router(config-router)# **timers pacing retransmission** milliseconds	再送信パケット ペーシング タイマーの待機時間（ミリ秒）を設定します。

グループ パケット ペーシング タイマーの設定

グループ パケット ペーシング タイマーを設定するには、ルータ 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. Router(config)# **router ospf** process-id
2. Router(config-router)# **timers pacing lsa-group** seconds

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(config)# **router ospf** process-id	ルータでルータ コンフィギュレーション モードを開始し、OSPF ルーティング プロセスをイネーブルにします。
ステップ 2	Router(config-router)# **timers pacing lsa-group** seconds	LSA グループ パケット ペーシング タイマーの待機時間（秒）を設定します。

OSPF パケット ペーシング タイマーの確認

OSPF パケット ペーシングが設定されていることを確認するには、特権 EXEC コマンド show ip ospf を使用します。show ip ospf コマンドの出力には、設定可能ペーシング タイマーのタイプ（フラッド、再送信、グループ）および待機時間が表示されます。次に、show ip ospf コマンドの出力例を示します。

```
Router# show ip ospf
  Routing Process "ospf 1" with ID 10.0.0.1 and Domain ID 10.20.0.1
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
  Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
  LSA group pacing timer 100 secs
  Interface flood pacing timer 55 msecs
  Retransmission pacing timer 100 msecs
  Number of external LSA 0. Checksum Sum 0x0
  Number of opaque AS LSA 0. Checksum Sum 0x0
  Number of DCbitless external and opaque AS LSA 0
  Number of DoNotAge external and opaque AS LSA 0
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  External flood list length 0
     Area BACKBONE(0)
         Number of interfaces in this area is 2
         Area has message digest authentication
         SPF algorithm executed 4 times
         Area ranges are
         Number of LSA 4. Checksum Sum 0x29BEB
         Number of opaque link LSA 0. Checksum Sum 0x0
         Number of DCbitless LSA 3
         Number of indication LSA 0
         Number of DoNotAge LSA 0
         Flood list length 0
     Area 172.16.26.0
         Number of interfaces in this area is 0
         Area has no authentication
         SPF algorithm executed 1 times
         Area ranges are
            192.168.0.0/16 Passive Advertise
         Number of LSA 1. Checksum Sum 0x44FD
         Number of opaque link LSA 0. Checksum Sum 0x0
         Number of DCbitless LSA 1
         Number of indication LSA 1
         Number of DoNotAge LSA 0
         Flood list length 0
```

トラブルシューティングのヒント

OSPF パケット再送信数が急増した場合は、このパケット ペーシング タイマーの値を増やしてください。show ip ospf neighbor コマンドの出力には OSPF パケット再送信数が表示されます。

OSPF パケットペーシング タイマーのモニタリングおよびメンテナンス

コマンド	目的
`Router#` **show ip ospf**	OSPF ルーティング プロセスに関する一般情報を表示します。
`router#` **show ip ospf neighbor**	OSPF ネイバー情報をインターフェイスごとに表示します。
`Router#` **clear ip ospf redistribution**	OSPF ルーティング プロセス ID に基づいてルートの再配布をクリアします。

OSPF アップデート パケット ペーシングの設定例

例：LSA フラッド ペーシング

次の例は、OSPF ルーティング プロセス 1 に対して、LSA フラッド ペーシング更新が 50 ミリ秒間隔で発生する設定を示しています。

```
Router(config)# router ospf 1
Router(config-router)# timers pacing flood 50
```

例：LSA 再送信ペーシング

次に、OSPF ルーティング プロセス 1 に対して、LSA 再送信ペーシング更新が 100 ミリ秒間隔で発生するように設定する例を示します。

```
Router(config)# router ospf 1
Router(config-router)# timers pacing retransmission 100
```

例：LSA グループ ペーシング

次の例は、OSPF ルーティング プロセス 1 に対して、LSA グループ間の OSPF グループ ペーシング更新が 75 秒間隔で発生する設定を示しています。

```
Router(config)# router ospf 1
Router(config-router)# timers pacing lsa-group 75
```

その他の参考資料

OSPF アップデート パケット ペーシング タイマー設定機能に関する追加情報については、次の参考資料を参照してください。

関連資料

関連項目	マニュアル タイトル
『Configuring OSPF』	『Configuring OSPF』
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』

標準

規格	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

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

OSPF アップデート パケット ペーシング タイマー設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *13* : *OSPF* アップデート パケット ペーシング タイマー設定の機能情報

機能名	リリース	機能情報
OSPF アップデート パケット ペーシング タイマー設定	Cisco IOS XE Release 2.1	OSPF アップデート パケット ペーシング タイマー設定機能を使用すると、OSPF LSA のフラッドペーシング、再送信ペーシング、およびグループ ペーシングの更新間隔を設定できます。 次に示すコマンドは、この章に記載されている機能において、新たに導入または変更されたものです。 • **timerspacingflood** • **timerspacinglsa-group** • **timerspacingretransmission** • **showipospf**

第 11 章

MPLS VPN のための OSPF 模造リンクのサポート

このマニュアルでは、Open Shortest Path First（OSPF）プロトコルを実行し、OSPF バックドア リンクを共有している各バーチャル プライベート ネットワーク（VPN）クライアント サイトを、マルチプロトコル ラベル スイッチング（MPLS）VPN コンフィギュレーション内で接続するための、模造リンクの設定方法と使用方法について説明します。

- 機能情報の確認，145 ページ
- MPLS VPN のための OSPF 模造リンクのサポートの前提条件，146 ページ
- MPLS VPN のための OSPF 模造リンクのサポートの制約事項，146 ページ
- MPLS VPN のための OSPF 模造リンクのサポートについて，146 ページ
- OSPF 模造リンクの設定方法，150 ページ
- OSPF 模造リンクの設定例，153 ページ
- その他の参考資料，156 ページ
- MPLS VPN の OSPF 模造リンク サポートの機能情報，157 ページ
- 用語集，158 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。

MPLS VPN のための OSPF 模造リンクのサポートの前提条件

MPLS VPN で模造リンクを設定する前に、次のようにして OSPF をイネーブルにしておく必要があります。

- OSPF ルーティング プロセスを作成する。
- ルーティング プロセスに関連付ける IP アドレス範囲を指定する。
- IP アドレス範囲に関連付けるエリア ID を割り当てる。

MPLS VPN のための OSPF 模造リンクのサポートの制約事項

PE ルータと CE ルータ間のプロトコルとして OSPF を使用する場合、VPN バックボーン全体にルートがアドバタイズされる際に、OSPF メトリックは保持されます。このメトリックを使用して、リモート PE ルータは適切なルートを選択します。このため、OSPF から BGP への再配布、および、BGP から OSPF への再配布において、メトリック値を変更すべきではありません。メトリック値を変更すると、ルーティング ループが発生する可能性があります。

MPLS VPN のための OSPF 模造リンクのサポートについて

MPLS VPN のための OSPF 模造リンクのサポートの利点

MPLS VPN バックボーン経由のクライアント サイト接続

模造リンクによって、エリア間ルート（PE から PE へ）の代わりに、VPN サイト間のエリア内バックドア ルートが選択されるという、OSPF のデフォルト動作が行われなくなります。模造リンクによって、バックドア リンクを共有する OSPF クライアント サイトが、MPLS VPN バックボーンを介して通信を行い、VPN サービスを利用するようになります。

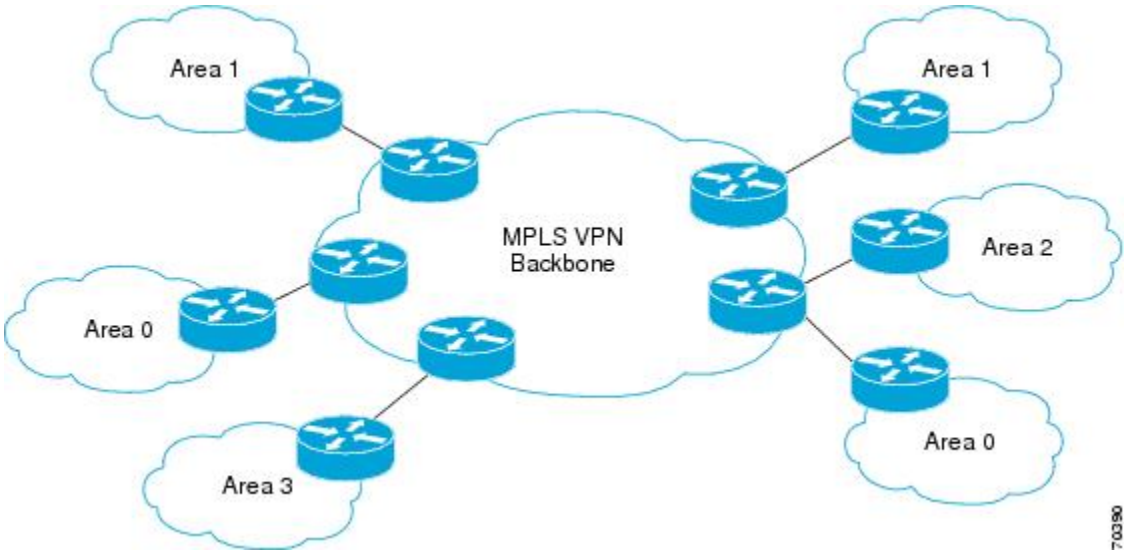
MPLS VPN 設定での柔軟なルーティング

MPLS VPN 設定で模造リンクに対して設定する OSPF コストを使用して、OSPF クライアント サイトのトラフィックを、バックドア リンク経由にするか、または VPN バックボーン経由にするかを指定できます。

PE-CE 間ルータ接続での OSPF の使用

MPLS VPN コンフィギュレーションにおいて、VPN バックボーン内でカスタマー エッジ（CE）ルータをサービス プロバイダー エッジ（PE）ルータに接続する方法の 1 つが OSPF プロトコルです。カスタマーにおける OSPF の一般的な用途は、OSPF をサイト内ルーティング プロトコルとして実行し、VPN サービスを利用し、MPLS VPN バックボーンで OSPF を使用して（移行時または常時）サイト間でルーティング情報を交換することです。

下の図 に、OSPF を実行する各 VPN クライアント サイトを、MPLS VPN バックボーンで接続する例を示します。



OSPF を使用して PE ルータと CE ルータを接続するには、VPN サイトから学習したすべてのルーティング情報を、着信インターフェイスに関連付けられた VPN Routing and Forwarding（VRF）インスタンスに格納します。VPN に接続された PE ルータ間では、ボーダー ゲートウェイ プロトコル（BGP）を使用して、VPN ルートが交換されます。CE ルータはこの VPN 内の他のサイトへのルートを、自分が接続された PE ルータとのピアリングによって学習します。MPLS VPN スーパーバックボーンは、OSPF を実行する各 VPN サイトを内部接続するための追加のルーティング階層レベルを提供します。

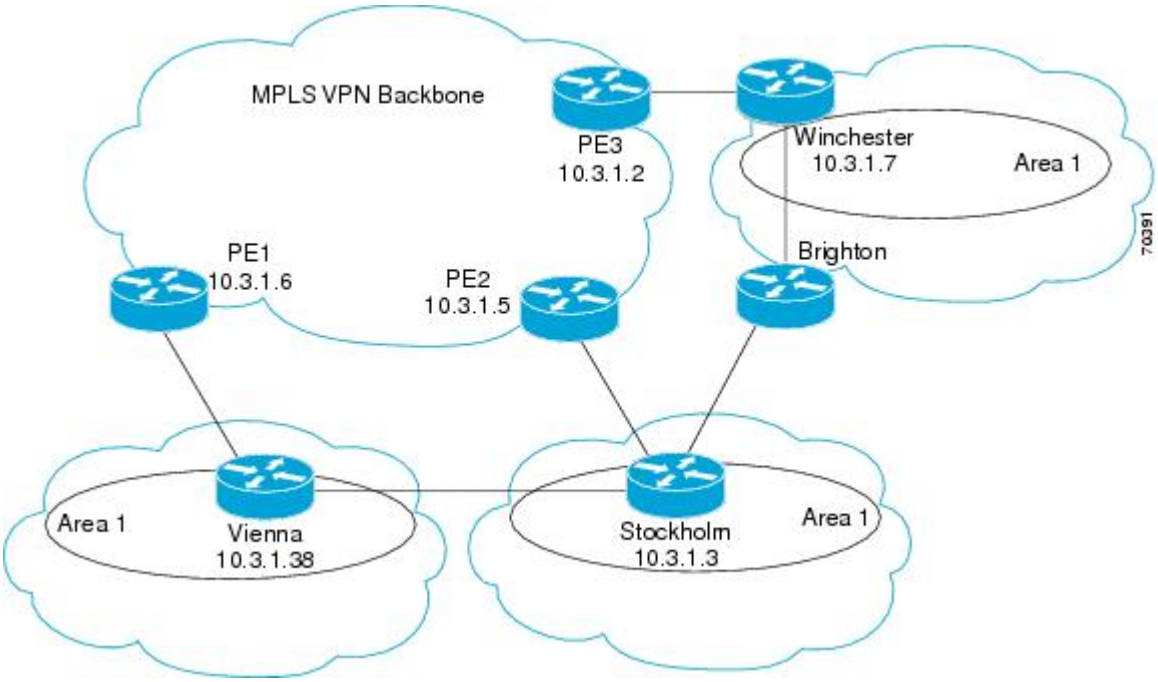
OSPF ルートが MPLS VPN バックボーン全体に伝播されると、プレフィックスに関する追加情報が、BGP 拡張コミュニティ形式（ルート タイプ、ドメイン ID 拡張コミュニティ）で BGP アップデートに付加されます。このコミュニティ情報を使用して、受信した PE ルータは、BGP ルートを OSPF PE-CE プロセスに再配布するときに生成するリンクステート アドバタイズメント（LSA）

のタイプを決定します。このようにして、同じ VPN に属し、VPN バックボーン全体にアドバタイズされる内部 OSPF ルートが、リモート サイト上でエリア内ルートとして認識されます。

MPLS VPN の設定方法に関する基本的な情報については、『*Cisco IOS XE MPLS Configuration Guide, Release 2*』を参照してください。

模造リンクを使用した OSPF バックドア ルーティングの修正方法

OSPF PE-CE 接続は、MPLS VPN バックボーンを経由するパスが、2 つのクライアント サイトの間にある唯一のパスであることを前提にしていますが、VPN サイト間にバックドア パス（下の図の灰色の線）も存在することがあります。これらのサイトが同じ OSPF エリアに属する場合、OSPF はエリア間パスよりもエリア内パスを優先するため、バックドア リンクのパスが常に選択されることになります（PE ルータは、エリア間パスとして VPN バックボーンから学習した OSPF ルートをアドバタイズします）。したがって、ルーティングがポリシーに従って実行されるには、VPN サイト間の OSPF バックドア リンクが考慮される必要があります。



たとえば、上の図には 3 つのクライアント サイトがあり、それぞれにバックドア リンクがあります。各サイトは同じエリア 1 コンフィギュレーション内で OSPF を実行しているため、これら 3 つのサイト間のルーティングでは、常にバックドア リンクを経由するエリア内パスが使用され、MPLS VPN バックボーンは経由されません。

次の例は、上の図の PE-1 ルータの BGP ルーティング テーブルにある、プレフィックス 10.3.1.7/32 のエントリを表示しています。このプレフィックスは Winchester CE ルータのループバック インターフェイスのものです。例中に太字で示すように、このループバック インターフェイスの情報

は、BGP によって PE-2 と PE-3 から学習されています。また、PE-1 上の BGP への再配布によって生成されています。

```
PE-1# show ip bgp vpnv4 all 10.3.1.7
BGP routing table entry for 100:251:10.3.1.7/32, version 58
Paths: (3 available, best #2)
  Advertised to non peer-group peers:
  10.3.1.2 10.3.1.5
  Local
    10.3.1.5 (metric 30) from 10.3.1.5 (10.3.1.5)
      Origin incomplete, metric 22, localpref 100, valid, internal
      Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
      RT:1:2:0 OSPF 2
  Local
    10.2.1.38 from 0.0.0.0 (10.3.1.6)
      Origin incomplete, metric 86, localpref 100, weight 32768,
      valid, sourced, best
      Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
      RT:1:2:0 OSPF 2
  Local
    10.3.1.2 (metric 30) from 10.3.1.2 (10.3.1.2)
      Origin incomplete, metric 11, localpref 100, valid, internal
      Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
      RT:1:2:0 OSPF 2
```

このローカルで生成されたルート（10.2.1.38）が、BGP では最適ルートとして認識されています。一方、次の例に太字で示すように、VRF ルーティング テーブルでは OSPF によって学習され、ネクスト ホップが 10.2.1.38（Vienna CE ルータ）となるパスが選択されています。

```
PE-1# show ip route vrf ospf 10.3.1.7
Routing entry for 10.3.1.7/32
  Known via "ospf 100", distance 110, metric 86, type intra area
  Redistributing via bgp 215
  Advertised by bgp 215
  Last update from 10.2.1.38 on Serial0/0/0, 00:00:17 ago
  Routing Descriptor Blocks:
  * 10.2.1.38
, from 10.3.1.7, 00:00:17 ago, via Serial0/0/0
      Route metric is 86, traffic share count is 1
```

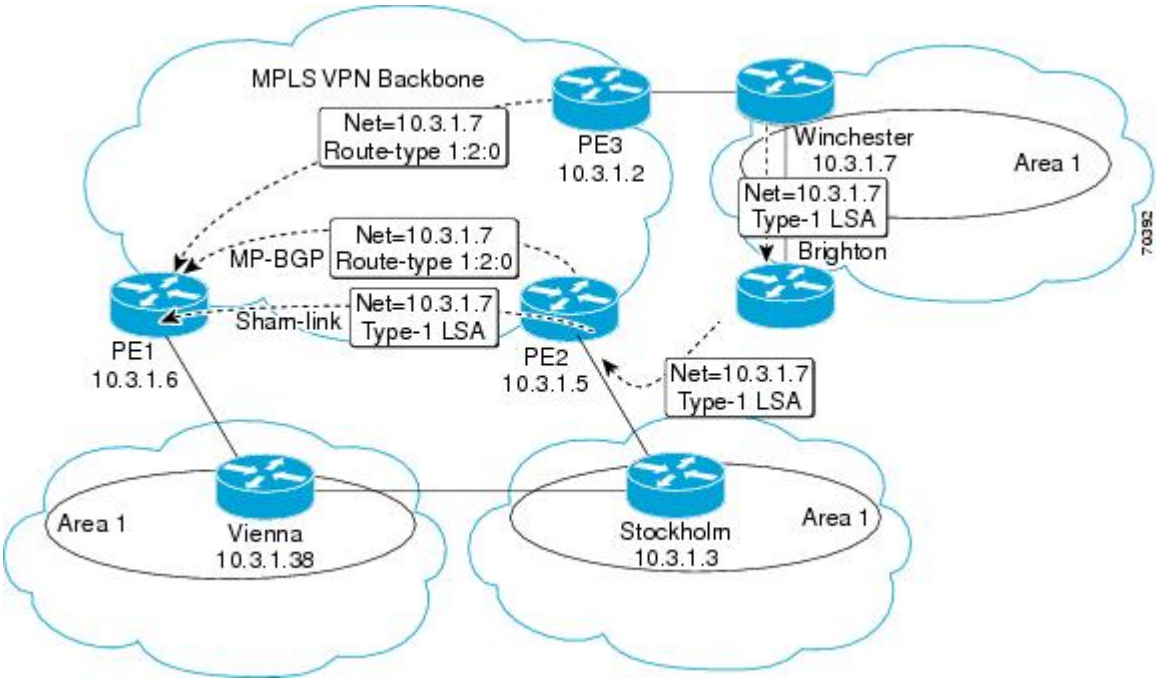
このパスが選択された理由は次のとおりです。

- OSPF エリア内パスは、PE-1 ルータで生成されたエリア間パス（MPLS VPN バックボーン経由）よりも優先される。
- OSPF ルートは、内部 BGP（同じ自律システム内のルータ間で実行される BGP）よりもアドミニストレーティブ ディスタンス（AD）が小さい。

サイト間のバックドア リンクを、バックアップ目的だけで使用し、VPN サービスに利用しない場合は、前の例に示すように、デフォルト ルート選択が不適切なものになります。MPLS VPN バックボーンに適切なパスを再確立するには、関連する PE ルータの入力 VRF と出力 VRF の間に、OSPF エリア内リンク（論理リンク）を追加作成する必要があります。このリンクは、模造リンクと呼ばれます。

模造リンクが必要なのは、同じ OSPF エリアに属し、OSPF バックドア リンクを共有する 2 つの VPN サイト間です。サイト間にバックドア リンクがない場合、模造リンクは不要です。

下の図に、PE-1 と PE-2 間の模造リンクの例を示します。模造リンクごとにコストが設定され、バックドア パスまたは模造リンク パスのどちらをトラフィックの送信に使用するか判断するために、それが使用されます。PE ルータ間に模造リンクを設定すると、PE は模造リンクから学習した OSPF ルートの情報を VRF ルーティング テーブルに書き込みます。



模造リンクは、PEルータ間のエリア内リンクであるかのように認識されるため、このリンクを通じて（特定のOSPFプロセス用の）OSPF隣接関係が確立され、データベース交換が行われます。これにより、PE ルータは、MPLS VPN バックボーンを介してサイト間で LSA をフラッディングすることができます。この結果、適切なエリア内接続が実現します。

OSPF 模造リンクの設定方法

模造リンクの作成

はじめる前に

MPLS VPN の PE ルータ間に模造リンクを作成する前に、次の設定が完了している必要があります。

- VPN バックボーンを介して模造リンクのリモートエンドに OSPF パケットを送信できるように、リモート PE 上に別の /32 アドレスを設定する。この /32 アドレスは、次の条件を満たす必要があります。
  - VRF に属する。
  - OSPF によってアドバタイズされない。
  - BGP によってアドバタイズされる。

この /32 アドレスは、他の模造リンクにも使用できます。

- 模造リンクを既存の OSPF エリアに関連付ける。

模造リンクを作成するには、EXEC モードで次のコマンドを使用します。

手順の概要

1. Router1# **configure terminal**
2. Router1(config)# **ip vrf** *vrf-name*
3. Router1(config-vrf)# **exit**
4. Router1(config)# **interface loopback** *interface-number*
5. Router1(config-if)# **ip vrf forwarding** *vrf-name*
6. Router1(config-if)# **ip address** *ip-address mask*
7. Router1(config-if)# **end**
8. Router1(config)# **end**
9. Router2# **configure terminal**
10. Router2(config)# **interface loopback** *interface-number*
11. Router2(config-if)# **ip vrf forwarding** *vrf-name*
12. Router2(config-if)# **ip address** *ip-address mask*
13. Router2(config-if)# **end**
14. Router1(config)# **end**
15. Router1(config)# **router ospf** *process-id* **vrf** *vrf-name*
16. Router1(config-if)# **area** *area-id* **sham-link** *source-address destination-address* **cost** *number*
17. Router2(config)# **router ospf** *process-id* **vrf** *vrf-name*
18. Router2(config-if)# **area** *area-id* **sham-link** *source-address destination-address* **cost** *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	Router1# **configure terminal**	最初の PE ルータで、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 2	Router1(config)# **ip vrf** *vrf-name*	VPN ルーティング/転送（VRF）インスタンスを定義し、VRF 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	Router1(config-vrf)# **exit**	VRF コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 4	Router1(config)# **interface loopback** *interface-number*	PE-1 で模造リンクのエンドポイントとして使用するループバック インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	Router1(config-if)# **ip vrf forwarding** *vrf-name*	ループバック インターフェイスに VRF を関連付けます。IP アドレスを削除します。

	コマンドまたはアクション	目的
ステップ 6	Router1(config-if)# **ip address** *ip-address mask*	PE-1 のループバック インターフェイスの IP アドレスを再設定します。
ステップ 7	Router1(config-if)# **end**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	Router1(config)# **end**	EXEC モードに戻ります。
ステップ 9	Router2# **configure terminal**	2 台目の PE ルータで、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 10	Router2(config)# **interface loopback** *interface-number*	PE-2 で模造リンクのエンドポイントとして使用するループバック インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	Router2(config-if)# **ip vrf forwarding** *vrf-name*	2 番目のループバック インターフェイスに VRF を関連付けます。IP アドレスを削除します。
ステップ 12	Router2(config-if)# **ip address** *ip-address mask*	PE-2 のループバック インターフェイスの IP アドレスを再設定します。
ステップ 13	Router2(config-if)# **end**	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	Router1(config)# **end**	EXEC モードに戻ります。
ステップ 15	Router1(config)# **router ospf** *process-id* **vrf** *vrf-name*	指定した OSPF プロセスに、PE-1 で模造リンク インターフェイスに関連付けた VRF を設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 16	Router1(config-if)# **area** *area-id* **sham-link** *source-address destination-address* **cost** *number*	PE-1 インターフェイス上の模造リンクを、指定した OSPF エリア内に設定します。エンドポイントとして各ループバック インターフェイスを IP アドレスで指定します。**cost** *number* によって、PE-1 の模造リンク インターフェイスで IP パケットを送信する際の OSPF コストを設定します。
ステップ 17	Router2(config)# **router ospf** *process-id* **vrf** *vrf-name*	指定した OSPF プロセスに、PE-2 で模造リンク インターフェイスに関連付けた VRF を設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 18	Router2(config-if)# **area** *area-id* **sham-link** *source-address destination-address* **cost** *number*	PE-2 インターフェイス上の模造リンクを、指定した OSPF エリア内に設定します。エンドポイントとして各ループバック インターフェイスを IP アドレスで指定します。**cost** *number* によって、PE-2 の模造リンク インターフェイスで IP パケットを送信する際の OSPF コストを設定します。

作成した模造リンクの確認

模造リンクが正常に作成されたことを確認するには、EXEC モードで **show ip ospf sham-links** コマンドを使用します。

```
Router# show ip ospf sham-links
Sham Link OSPF_SL0 to address 10.2.1.2 is up
Area 1 source address 10.2.1.1
  Run as demand circuit
  DoNotAge LSA allowed. Cost of using 40 State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
    Hello due in 00:00:04
    Adjacency State FULL (Hello suppressed)
    Index 2/2, retransmission queue length 4, number of
    retransmission 0
    First 0x63311F3C(205)/0x63311FE4(59) Next
    0x63311F3C(205)/0x63311FE4(59)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
    Link State retransmission due in 360 msec
```

模造リンクのモニタリングと維持

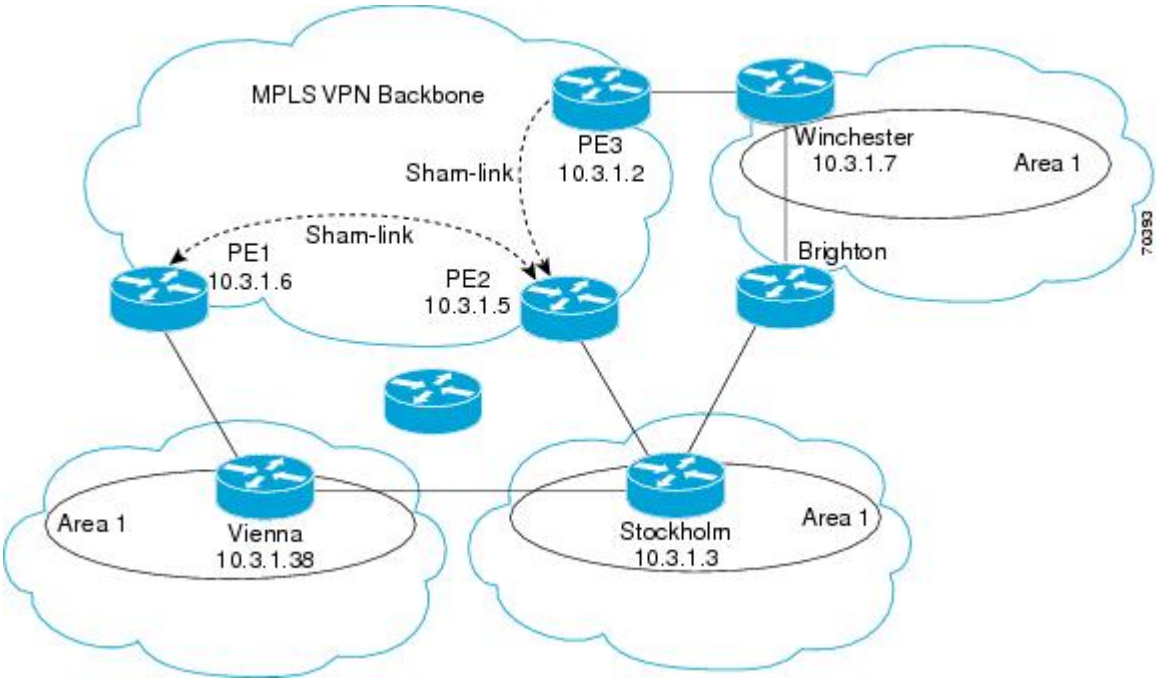
コマンド	目的
`Router#` **show ip ospf sham-links**	ルータに設定されているすべての模造リンクの動作状態を表示します。
`Router#` **show ip ospf data router** *ip-address*	2 台の PE ルータ間のアンナンバード ポイントツーポイント接続としてアドバタイズされる模造リンクの情報を表示します。

OSPF 模造リンクの設定例

例：模造リンクの設定

次の例では、PE ルータおよび CE ルータでの OSPF エリア内パス選択だけに影響するように模造リンクを使用する方法について説明します。PE ルータは MP-BGP から受信した情報も使用し、着信パケットの出ラベル スタックを設定して、どの出力 PE ルータ宛にパケットをラベル スイッチするか指定します。

下の図に、模造リンク設定が必要となる MPLS VPN トポロジの例を示します。VPN クライアントには 3 つのサイトがあり、それぞれにバックドア リンクがあります。2 つの模造リンクが設定されており、1 つは PE-1 と PE-2 の間、もう 1 つは PE-2 と PE-3 の間です。この設定では、Vienna と Winchester のサイトはバックドア リンクを共有していないため、PE-1 と PE-3 の間の模造リンクは不要です。



次の出力では、PE-1 が 10.3.1.7/32 プレフィックス（図の Winchester CE ルータの loopback1 インターフェイス）をどのように認識するかという観点から、サイト間で行われるフォワーディングを示しています。

```
PE-1# show ip bgp vpnv4 all 10.3.1.7
BGP routing table entry for 100:251:10.3.1.7/32, version 124
Paths: (1 available, best #1)
  Local
    10.3.1.2 (metric 30) from 10.3.1.2
 (10.3.1.2)
       Origin incomplete, metric 11, localpref 100, valid, internal,
       best
       Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
       RT:1:2:0 OSPF 2
PE-1# show ip route vrf ospf 10.3.1.7
Routing entry for 10.3.1.7/32
  Known via "ospf 100
", distance 110, metric 13, type intra area
  Redistributing via bgp 215
  Last update from 10.3.1.2 00:12:59 ago
  Routing Descriptor Blocks:
10.3.1.2 (Default-IP-Routing-Table), from 10.3.1.7, 00:12:59 ago
```

次の出力に示すフォワーディング情報では、ルートのネクスト ホップが、PE-2 ルータ（OSPF では最適パス）ではなく、10.3.1.2 の PE-3 ルータとなっています。この OSPF ルートが PE 上の BGP に再配布されなかった理由は、模造リンクの反対側のエンドポイントによって、すでに BGP に再配布されているため、重複して配布する必要がないからです。エリア内のパスの選択に影響を与えるためだけに、OSPF 模造リンクは使用されます。特定の宛先にトラフィックを送信する際、PE ルータは MP-BGP のフォワーディング情報を使用します。

```
PE-1# show ip bgp vpnv4 all tag | begin 10.3.1.7
   10.3.1.7/32      10.3.1.2
        notag/38

PE-1# show tag-switching forwarding 10.3.1.2
```

```
Local  Outgoing   Prefix           Bytes tag  Outgoing   Next Hop
tag    tag or VC  or Tunnel Id     switched   interface
31     42         10.3.1.2/32
       0          PO3/0/0    point2point
PE-1# show ip cef vrf ospf 10.3.1.7
10.3.1.7/32, version 73, epoch 0, cached adjacency to POS3/0/0
0 packets, 0 bytes
  tag information set
   local tag: VPN-route-head
   fast tag rewrite with PO3/0/0, point2point, tags imposed: {42 38
}
  via 10.3.1.2
, 0 dependencies, recursive
    next hop 10.1.1.17, POS3/0/0 via 10.3.1.2/32
    valid cached adjacency
    tag rewrite with PO3/0/0, point2point, tags imposed: {42 38}
```

模造リンクを介してプレフィックスが学習され、模造リンクのパスが最適パスとして選択されると、PEルータは、そのプレフィックスに関するMP-BGPアップデートを生成しません。ある模造リンクから、さらに別の模造リンクにはトラフィックをルーティングできません。

次の出力では、プレフィックスに関する MP-BGP アップデートが生成されていないことを、PE-2 で示しています。太字で示すように、10.3.1.7/32 は、OSPF によって模造リンクを介して学習されていますが、BGP へのローカルでのルート生成は実行されていません。BGP テーブルの唯一のエントリは、PE-3（10.3.1.7/32 プレフィックスへの出力 PE ルータ）から受信した MP-BGP アップデートです。

```
PE-2# show ip route vrf ospf 10.3.1.7
Routing entry for 10.3.1.7/32
  Known via "ospf 100
", distance 110, metric 12, type intra area
  Redistributing via bgp 215
  Last update from 10.3.1.2 00:00:10 ago
  Routing Descriptor Blocks:
  * 10.3.1.2 (Default-IP-Routing-Table), from 10.3.1.7, 00:00:10 ago
      Route metric is 12, traffic share count is 1
PE-2# show ip bgp vpnv4 all 10.3.1.7
BGP routing table entry for 100:251:10.3.1.7/32, version 166
Paths: (1 available, best #1)
  Not advertised to any peer
  Local
    10.3.1.2 (metric 30) from 10.3.1.2 (10.3.1.2)
      Origin incomplete, metric 11, localpref 100, valid, internal,
      best
      Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
      RT:1:2:0 OSPF 2
```

PEルータはMP-BGPから受信した情報を使用して、着信パケットの出ラベル スタックを設定し、どの出力 PE ルータ宛にパケットをラベル スイッチするか決定します。

例：2 つの PE ルータ間の模造リンク

次の例は、2 台の PE ルータ間で模造リンクを設定する方法を示しています。

```
Router1(config)
# interface loopback 1
Router1(config-if)# ip vrf forwarding ospf
Router1(config-if)# ip address 10.2.1.1 255.255.255.255
!
Router2(config)# interface loopback 1
Router2(config-if)# ip vrf forwarding ospf
Router2(config-if)# ip address 10.2.1.2 255.255.255.255
!
Router1(config)# router ospf 100 vrf ospf
```

```
Router1(config-if)# area 1 sham-link 10.2.1.1 10.2.1.2 cost 40
!
Router2(config)# router ospf 100 vrf ospf
Router2(config-if)# area 1 sham-link 10.2.1.2 10.2.1.1 cost 40
```

その他の参考資料

ここでは、MPLS VPN のための OSPF 模造リンクのサポート機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
『Configuring OSPF』	『Configuring OSPF』
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』
『MPLS Virtual Private Networks』	『MPLS Virtual Private Networks』

標準

規格	Title
なし	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 1163	『*A Border Gateway Protocol*』

RFC	Title
RFC 1164	『*Application of the Border Gateway Protocol in the Internet*』
RFC 2283	『*Multiprotocol Extensions for BGP-4*』
RFC 2328	『*Open Shortest Path First, Version 2*』
RFC 2547	『*BGP/MPLS VPNs*』

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

MPLS VPN の OSPF 模造リンク サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *14*：*MPLS VPN* の *OSPF* 模造リンク サポートの機能情報

機能名	リリース	機能情報
MPLS VPN のための OSPF 模造リンクのサポート	Cisco IOS XE Release 2.1	この機能により、OSPF を実行し、OSPF バックドア リンクを共有している各バーチャル プライベート ネットワーク（VPN）クライアント サイトを、マルチプロトコル ラベル スイッチング（MPLS）VPN コンフィギュレーション内で接続するための、模造リンクを使用できます。 次に示すコマンドは、この章に記載されている機能において、新たに導入または変更されたものです。 • **areasham-linkcost** • **showipospfsham-links**

用語集

BGP：Border Gateway Protocol（ボーダー ゲートウェイ プロトコル）。他の BGP システムとの間で到着可能性情報を交換するドメイン間ルーティング プロトコルです。RFC 1163 で定義されています。

CE ルータ：カスタマー エッジ ルータ。カスタマー ネットワークに属し、プロバイダー エッジ（PE）ルータとのインターフェイスとなるルータ。CE ルータは、関連する VPN を認識しません。

CEF：Cisco Express Forwarding（シスコ エクスプレス フォワーディング）。高度なレイヤ 3 IP スイッチング テクノロジーです。CEF は、大規模で動的なトラフィック パターンに対するネットワーク パフォーマンスとスケーラビリティを最適化します。

IGP：Interior Gateway Protocol（内部ゲートウェイ プロトコル）。自律システム内でルーティング情報の交換に使用するインターネット プロトコル。一般的な IGP の例として、IGRP、OSPF、および RIP があります。

LSA：Link-State Advertisement（リンクステート アドバタイズメント）。リンクステート プロトコルで使用されるブロードキャストパケット。LSA にはネイバーおよびパスコストに関する情報が含まれ、受信側ルータがルーティング テーブルを維持するために使用します。

MPLS：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。タグ スイッチングの基礎となる新しい業界標準です。

OSPF：Open Shortest Path First プロトコル。

PE ルータ：プロバイダー エッジ ルータ。サービス プロバイダー ネットワーク内にあり、カスタマー エッジ（CE）ルータに接続されたルータ。すべての VPN 処理は PE ルータで行われます。

SPF：Shortest Path First 計算。

VPN：Virtual Private Network（バーチャル プライベート ネットワーク）。1 つまたは複数の物理ネットワークでリソースを共有する、セキュアな IP ベース ネットワーク。VPN には、共有のバックボーンで安全に通信できる地理的に分散したサイトが含まれます。

VRF：VPN ルーティングおよび転送インスタンス。VRF は、IP ルーティング テーブル、取得されたルーティング テーブル、そのルーティング テーブルを使用する一連のインターフェイス、ルーティングテーブルに登録されるものを決定する一連のルールおよびルーティング プロトコルで構成されています。一般に、VRF には、PE ルータに付加されるカスタマー VPN サイトが定義されたルーティング情報が格納されています。

第 12 章

CE ルータでの OSPF マルチ VRF サポート

CE ルータでの OSPF マルチ VRF サポート機能は、OSPF と BGP プロトコルの間でパケットを相互に再配布する場合にループの防止に必要な、プロバイダー エッジ（PE）のチェックを抑制する機能を提供します。PE ではないルータ（BGP を実行していないルータ）で、VPN ルーティングおよび転送（VRF）を使用する場合、チェックをオフにすると、VRF ルーティング テーブルに、IP プレフィックスへのルート情報を正常に書き込むことができます。

OSPF マルチ VRF では、ルータを複数の仮想ルータに分割し、各仮想ルータで固有のインターフェイス セット、ルーティング テーブル、およびフォワーディング テーブルを設定できます。

- 機能情報の確認，161 ページ
- CE ルータでの OSPF マルチ VRF サポートについて，162 ページ
- CE ルータでの OSPF マルチ VRF サポートの設定方法，162 ページ
- CE ルータでの OSPF マルチ VRF サポートの設定例，165 ページ
- その他の参考資料，166 ページ
- CE ルータでの OSPF マルチ VRF サポートの機能情報，167 ページ
- 用語集，168 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。

CE ルータでの OSPF マルチ VRF サポートについて

CE ルータでの OSPF マルチ VRF サポート機能は、OSPF と BGP プロトコルの間でパケットを相互に再配布する場合にループの防止に必要な、プロバイダーエッジ（PE）のチェックを抑制する機能を提供します。PE ではないルータ（BGP を実行していないルータ）で、VPN ルーティングおよび転送（VRF）を使用する場合、チェックをオフにすると、VRF ルーティングテーブルに、IP プレフィックスへのルート情報を正常に書き込むことができます。

OSPF マルチ VRF では、ルータを複数の仮想ルータに分割し、各仮想ルータで固有のインターフェイスセット、ルーティングテーブル、およびフォワーディングテーブルを設定できます。また、OSPF マルチ VRF によって、ネットワークをセグメントに分割し、各セグメントで、正しいルーティング情報を維持しながら特定の機能を実行するように設定できます。

CE ルータでの OSPF マルチ VRF サポートの設定方法

OSPF ルーティングのためのマルチ VRF 機能の設定

はじめる前に

CEF がネットワークで実行されている必要があります。

手順の概要

1. イネーブル化
2. **showipospf**[*process-id*
3. **configureterminal**
4. **vpdn-group***name*
5. **exit**
6. **resource-poolprofilevpdn***name*
7. **vpdngroup***name*
8. **vpnvrf***vrf-name*| **id** *vpn-id*
9. **exit**
10. **routerospf***process-id* [**vrf** *vpn-name*]
11. **capabilityvrf-lite**

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 モードなど、高位の権限レベル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	**showipospf**[*process-id* 例： `Router# show ip ospf 1`	ルータのステータスを表示します。この表示に、PE ルータが VPN バックボーンに接続していることが示された場合は、**capability vrf-lite** コマンドを使用して、PE ルータを VPN バックボーンから切り離します。
ステップ 3	**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 4	**vpdn-group***name* 例： `Router(config)# vpdn-group mygroup`	VPDN グループを作成します。
ステップ 5	**exit** 例： `Router(config-vpdn)# exit`	コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**resource-poolprofilevpdn***name* 例： `Router(config)# resource-pool profile vpdn company1`	Virtual Private Dialup Network（VPDN）プロファイルを作成し、VPDN プロファイル コンフィギュレーション モードを開始します。
ステップ 7	**vpdngroup***name* 例： `Router(config-vpdn-profile)# vpdn group mygroup`	Virtual Private Dialup Network（VPDN）グループとカスタマーまたは VPDN プロファイルとを関連付けます。
ステップ 8	**vpnvrf***vrf-name*| **id** *vpn-id* 例： `Router(config-vpdn)# vpn vrf grc`	Virtual Private Dialup Network（VPDN）グループの送信元および宛先 IPv4 アドレスが、指定した Virtual Private Network（VPN）Routing and Forwarding（VRF）インスタンスに属するように指定します。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Router(config-vpdn)# exit`	コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**routerospf***process-id* [**vrf** *vpn-name*] 例： `Router(config)# router ospf 1 vrf grc`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。 • *process-id* 引数は OSPF プロセスを示します。 • **vrf** キーワードと *vpn-name* 引数を使用して VPN を指定します。
ステップ 11	**capabilityvrf-lite** 例： `Router(config-router)# capability vrf-lite`	OSPF プロセスにマルチ VRF 機能を適用します。

OSPF マルチ VRF 設定の確認

この機能に関連付けられた、特定の **debug** または **show** コマンドはありません。OSPF マルチ VRF 設定が正常に行われたことを確認するには、**show ip ospf** *process-id*] コマンドを使用して、ルータが VPN バックボーンに接続していないことを確認します。

show ip ospf process コマンドの出力から、現在 PE ルータがバックボーンに接続しているかどうかがわかります。

```
Router# show ip ospf 12
 Routing Process "ospf 12" with ID 172.16.1.1 and Domain ID 0.0.0.12
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Connected to MPLS VPN Superbackbone
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x0
 Number of opaque AS LSA 0. Checksum Sum 0x0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

router ospf コマンドに続いて、**capability vrf-lite** コマンドで OSPF VRF プロセスを設定すると、「Connected to MPLS VPN Superbackbone」が表示されなくなります。

CE ルータでの OSPF マルチ VRF サポートの設定例

例：マルチ VRF 機能の設定

この例では、OSPF 基本ネットワークに grc という名前の VRF を設定します。**capabilityvrf-lite** コマンドを実行して、PE チェックを抑制します。

```
!
ip cef
ip vrf grc
 rd 1:1
interface Serial2/0/0
 ip vrf forwarding grc
 ip address 192.168.1.1 255.255.255.252
!
interface Serial3/0/0
 ip vrf forwarding grc
 ip address 192.168.2.1 255.255.255.252
...
!
router ospf 9000 vrf grc
 log-adjacency-changes
 capability vrf-lite
 redistribute rip metric 1 subnets
 network 192.168.1.0 0.0.0.255 area 0
!
router rip
 address-family ipv4 vrf grc
 redistribute ospf 9000 vrf grc
 network 192.168.2.0
 no auto-summary
 end
Device# show ip route vrf grc
Routing Table: grc
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
O IA 192.168.192.0/24 [110/138] via 192.168.1.13, 00:06:08, Serial2/0/0
                      [110/138] via 192.168.1.9, 00:06:08, Serial3/0/0
O IA 192.168.242.0/24 [110/74] via 192.168.1.13, 00:06:08, Serial2/0/0
O IA 192.168.193.0/24 [110/148] via 192.168.1.13, 00:06:08, Serial2/0/0
                      [110/148] via 192.168.1.9, 00:06:08, Serial3/0/0
O IA 192.168.128.0/24 [110/74] via 192.168.1.9, 00:06:08, Serial3/0/0
O IA 192.168.129.0/24 [110/84] via 192.168.1.9, 00:06:08, Serial3/0/0
O IA 192.168.130.0/24 [110/84] via 192.168.1.9, 00:06:08, Serial3/0/0
     172.16.0.0/24 is subnetted, 2 subnets
O E2    172.16.9.0 [110/5] via 192.168.1.13, 00:06:08, Serial2/0/0
O E2    172.16.10.0 [110/5] via 192.168.1.13, 00:06:08, Serial2/0/0
O IA 192.168.131.0/24 [110/94] via 192.168.1.9, 00:06:20, Serial3/0/0
     192.168.1.0/30 is subnetted, 4 subnets
C       192.168.1.8 is directly connected, Serial3/0/0
C       192.168.1.12 is directly connected, Serial2/0/0
O       192.168.1.0 [110/128] via 192.168.1.9, 00:06:20, Serial3/0/0
O       192.168.1.4 [110/128] via 192.168.1.13, 00:06:20, Serial2/0/0
```

その他の参考資料

CE ルータでの OSPF マルチ VRF サポートに関する詳細情報については、次の参考資料を参照してください。

関連資料

関連項目	マニュアル タイトル
『Configuring OSPF』	『Configuring OSPF』
マルチプロトコル ラベル スイッチング（MPLS）	『*Cisco IOS XE Multiprotocol Label Switching Configuration Guide, Release 2*』
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』

標準

規格	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

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

CE ルータでの OSPF マルチ VRF サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *15* : *CE* ルータでの *OSPF* マルチ *VRF* サポートの機能情報

機能名	リリース	機能情報
CE ルータでの OSPF マルチ VRF サポート	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.1.0 SG	CE ルータでの OSPF マルチ VRF サポート機能は、OSPF と BGP プロトコルの間でパケットを相互に再配布する場合にループの防止に必要な、プロバイダー エッジ（PE）のチェックを抑制する機能を提供します。PE ではないルータ（BGP を実行していないルータ）で、VPN ルーティングおよび転送（VRF）を使用する場合、チェックをオフにすると、VRF ルーティング テーブルに、IP プレフィックスへのルート情報を正常に書き込むことができます。 次に示すコマンドは、この章に記載されている機能において、新たに導入または変更されたものです。 • **capabilityvrf-lite**

用語集

CE ルータ：カスタマー エッジ ルータ。C ネットワーク上のエッジ ルータで、P ルータに直接接続された C ルータとして定義されます。

C ネットワーク：顧客（企業またはサービス プロバイダー）ネットワーク。

C ルータ：顧客ルータ。C ネットワーク上のルータ。

LSA：Link-State Advertisement（リンクステート アドバタイズメント）。リンクステート プロトコルで使用されるブロードキャストパケット。ネイバーおよびパスコストの情報が含まれています。受信側ルータは、LSA を使用してルーティング テーブルのメンテナンスを行います。

PE ルータ：プロバイダー エッジ ルータ。P ネットワーク上のエッジ ルータで、C ルータに直接接続された P ルータとして定義されます。

P ネットワーク：MPLS 対応のサービス プロバイダーのコア ネットワーク。P ルータが MPLS を実行します。

P ルータ：プロバイダー ルータ。P ネットワークのルータです。

SPF：Shortest Path First。最短パス スパニングツリーを決定するためにパス長計算を繰り返すルーティング アルゴリズムです。

VPN：Virtual Private Network（バーチャル プライベート ネットワーク）。ネットワーク間のトラフィックをすべて暗号化することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できます。

VRF：VPN ルーティングおよび転送。

第 13 章

OSPFv2 マルチエリア隣接関係

ここでは、Open Shortest Path First バージョン 2（OSPFv2）のマルチエリア隣接関係を設定する方法について説明します。既存の OSPFv2 プライマリ インターフェイスには複数のエリアを追加できます。追加の論理インターフェイスはマルチエリア隣接関係をサポートしています。

- 機能情報の確認，171 ページ
- OSPFv2 マルチエリア隣接関係の前提条件，172 ページ
- OSPFv2 マルチエリア隣接関係の制約事項，172 ページ
- OSPFv2 マルチエリア隣接関係について，172 ページ
- OSPFv2 マルチエリア隣接関係の設定方法，173 ページ
- OSPFv2 マルチエリア隣接関係の設定例，175 ページ
- OSPFv2 マルチエリア隣接関係に関する追加情報，176 ページ
- OSPFv2 マルチエリア隣接関係の機能情報，177 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。

OSPFv2 マルチエリア隣接関係の前提条件

- Open Shortest Path First（OSPF）がプライマリ インターフェイスで設定されていることを確認します。
- プライマリ インターフェイス タイプがポイントツーポイントであることを確認します。

OSPFv2 マルチエリア隣接関係の制約事項

マルチエリア インターフェイスには次の制約事項があります。

- プライマリ インターフェイスで OSPF が設定されている場合にのみ動作します。
- OSPF のプライマリ インターフェイス上の論理構成体として存在しますが、プライマリ インターフェイス上のネイバー ステートは、マルチエリア インターフェイスと無関係です。
- 隣接デバイス上の対応するマルチエリア インターフェイスとのネイバー関係を確立します。マルチエリアとプライマリ インターフェイスの混在はサポートされていません。
- ネイバー ステートがフルの場合、デバイス リンクステート アドバタイズメント（LSA）のアンナンバード ポイントツーポイント リンクを、対応するエリアにアドバタイズします。
- プライマリ インターフェイスからすべての OSPF パラメータ（認証など）を継承します。マルチエリア インターフェイスでパラメータを設定することはできませんが、プライマリ インターフェイスではパラメータを設定できます。

OSPFv2 マルチエリア隣接関係について

OSPFv2 マルチエリア隣接関係の概要

Open Shortest Path First（OSPF）プロトコルでは、ネットワーク トポロジを個別のエリアに分割できます。OSPF が設定されているインターフェイスは、任意の時点で、1 つのエリアにのみ属します。このため、エリア内ルートがエリア間ルートより優先されることにより、特定のトポロジでは準最適ルーティングが発生します。

Open Shortest Path First バージョン 2（OSPFv2）では、単一の物理リンクを複数のエリアで共有することができます。このため、同じリンクを共有する該当のエリアそれぞれにエリア内パスを作成します。すべてのエリアには、OSPF が設定されるインターフェイスがあります。これらのインターフェイスの 1 つがプライマリ インターフェイスとして、その他がセカンダリ インターフェイスとして指定されます。

OSPFv2 マルチエリア隣接関係機能を使用すると、プライマリ インターフェイスにリンクを設定し、複数のエリアで最適化されたルーティングを有効にすることができます。各マルチエリア インターフェイスは、ポイントツーポイントアンナンバードリンクとして表明されます。マルチエ

リア インターフェイスは、既存のプライマリ インターフェイス上の論理構成体として存在します。プライマリ インターフェイス上のネイバー ステートはマルチエリア インターフェイスのネイバー ステートには依存しません。マルチエリアインターフェイスは隣接デバイス上の対応するマルチエリア インターフェイスとのネイバー関係を確立します。2 つの OSPF スピーカーのあるインターフェイスでのみマルチエリア隣接関係を設定できます。ネイティブ ブロードキャスト ネットワークの場合、インターフェイスを OSPF ポイントツーポイント タイプとして設定し、マルチエリア隣接関係についてインターフェイスを有効にする必要があります。

プライマリ OSPFv2 インターフェイスでマルチエリア隣接関係を設定するには、**ip ospf multi-area** コマンドを使用します。

OSPFv2 マルチエリア隣接関係の設定方法

OSPFv2 マルチエリア隣接関係の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typenumber*
4. **ip address** *ip-address mask*
5. **ip ospf** *proces-id* **area** *area-id*
6. **ip ospf network point-to-point**
7. **ip ospf multi-area** *multi-area-id*
8. **ip ospf multi-area** *multi-area-id* **cost** *interface-cost*
9. **end**

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	**configure terminal** 例： `Device# 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	**interface***typenumber* 例： `Device(config)# interface Ethernet 0/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Device(config)# ip address 10.0.12.1 255.255.255.0`	このインターフェイスに IP アドレスを割り当てます。
ステップ 5	**ip ospf** *proces-id* **area** *area-id* 例： `Device (config-if)# ip ospf 10 area 8`	OSPF プライマリ インターフェイスを設定します。 • *process-id* 引数は OSPF プロセスを示します。有効な範囲は 1 ～ 65535 です。 • *area-id* 引数は OSPF エリアを示します。範囲は 0 ～ 4294967295 にするか、または IP アドレスを使用できます。
ステップ 6	**ip ospf network point-to-point** 例： `Device (config-if)# ip ospf network point-to-point`	プライマリ インターフェイスのタイプをポイントツーポイントに指定します。
ステップ 7	**ip ospf multi-area** *multi-area-id* 例： `Device (config-if)# ip ospf multi-area 11`	インターフェイスでマルチエリア隣接関係を設定します。 • *multi-area-id* 引数は OSPF マルチエリアを示します。範囲は 0 ～ 4294967295 にするか、または IP アドレスを使用できます。
ステップ 8	**ip ospf multi-area** *multi-area-id* **cost** *interface-cost* 例： `Device (config-if)# ip ospf multi-area 11 cost 10`	（任意）Open Shortest Path First（OSPF）マルチエリア インターフェイス上でパケットを送信するコストを指定します。
ステップ 9	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。

OSPFv2 マルチエリア隣接関係の設定例

例：OSPFv2 マルチエリア隣接関係の設定

```
Device# enable
Device# configure terminal
Device(config)# interface Ethernet 0/0
Device (config-if)# ip address 10.0.12.1 255.255.255.0
Device (config-if)# ip ospf 1 area 0
Device (config-if)# ip ospf network point-to-point
Device (config-if)# ip ospf multi-area 2
Device (config-if)# ip ospf multi-area 2 cost 10
Device (config-if)# end
```

次に、**show ip ospf 2 multi-area** コマンドの出力例を示します。

```
Device# show ip ospf 2 multi-area

OSPF_MA1 is up, line protocol is up
  Primary Interface Ethernet0/0, Area 2
  Interface ID 2
  MTU is 1500 bytes
  Neighbor Count is 1
```

次に、**show ip ospf interface** コマンドの出力例を示します。

```
Device# show ip ospf interface

Ethernet0/0 is up, line protocol is up
  Internet Address 10.0.12.1/24, Area 0, Attached via Interface Enable
  Process ID 1, Router ID 10.0.0.2, Network Type POINT_TO_POINT, Cost: 10
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           10        no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:06
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Can be protected by per-prefix Loop-Free FastReroute
  Can be used for per-prefix Loop-Free FastReroute repair paths
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.0.0.1
  Suppress hello for 0 neighbor(s)
  Multi-area interface Count is 1
    OSPF_MA1 interface exists in area 2 Neighbor Count is 1
OSPF_MA1 is up, line protocol is up
  Interface is unnumbered. Using address of Ethernet0/0 (10.0.12.1), Area 2, Attached via
Multi-area
  Process ID 1, Router ID 10.0.0.2, Network Type POINT_TO_POINT, Cost: 10
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           10        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:06
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Can be protected by per-prefix Loop-Free FastReroute
```

```
Can be used for per-prefix Loop-Free FastReroute repair paths
Index 1/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 2
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 10.0.0.1
Suppress hello for 0 neighbor(s)
```

OSPFv2 マルチエリア隣接関係に関する追加情報

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 Command List, All Releases』
OSPF コマンド	『Cisco IOS IP Routing: OSPF Command Reference』
OSPF で機能するプロトコル非依存の機能	Configuring IP Routing Protocol-Independent Features モジュール

RFC

RFC	Title
RFC 5185	『*OSPF Multi-Area Adjacency*』（2008 年 5 月）

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

OSPFv2 マルチエリア隣接関係の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *16*：*OSPFv2* マルチエリア隣接関係の機能情報

機能名	リリース	機能情報
OSPFv2 マルチエリア隣接関係	Cisco IOS XE Release 3.10S	OSPFv2 マルチエリア隣接関係により、複数のOSPFエリア内のプライマリ インターフェイスでリンクを設定してルーティングを最適化することができます。 次のコマンドが導入または変更されました。**ip ospf multi-area**、**ip ospf multi-area cost**、**show ip ospf multi-area**

第 14 章

OSPFv2 自動ルート除外

OSPFv2 自動ルート除外機能を使用すると、特定の接続先およびプレフィックスでパケット転送においてトラフィック エンジニアリング（TE）トンネルを回避することができます。その他のプレフィックスでは TE トンネルを使用するように設定できます。除外されるプレフィックスは、TE トンネル パスを使用しません。ネイティブの非 TE パスだけがこのようなルートについて RIB にダウンロードされます。ここでは、OSPFv2 自動ルート除外機能の設定方法について説明します。

- 機能情報の確認，179 ページ
- OSPFv2 自動ルート除外の前提条件，180 ページ
- OSPFv2 自動ルート除外について，180 ページ
- OSPFv2 自動ルート除外の設定方法，181 ページ
- OSPFv2 自動ルート除外の設定例，182 ページ
- OSPFv2 自動ルート除外に関する追加情報，182 ページ
- OSPFv2 自動ルート除外の機能情報，183 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。

OSPFv2 自動ルート除外の前提条件

- Open Shortest Path First（OSPF）がネットワークで設定されている。
- シスコ エクスプレス フォワーディング（CEF）がイネーブルになっている。
- マルチプロトコル ラベル スイッチング（MPLS）TE トンネルが設定されている。

OSPFv2 自動ルート除外について

OSPFv2 自動ルート除外の概要

自動ルート機能は、OSPF が IP トラフィック ルートのパスを作成するために MPLS TE トンネルを使用することを強制する IP ルーティング方法です。

自動ルート機能を使用すると、そのルートに使用可能な代替の非 TE パスがある場合でも、すべてのルートで TE トンネルを使用することができます。

OSPFv2 自動ルート除外機能では、特定の接続先またはプレフィックスで TE トンネルを回避して、他のプレフィックスでは依然として TE トンネルを使用するように設定することができます。除外されるプレフィックスは、TE トンネル パスを使用しません。ネイティブの非 TE パスだけがこのようなルートについて RIB にダウンロードされます。

自動ルート除外オプションは、プレフィックス リストを使用してルータ OSPF コンフィギュレーション モードで設定されます。このプレフィックス リストのメンバである IP アドレスおよびプレフィックスは、自動ルートがイネーブルになっていても TE トンネルから除外されます。IP アドレスまたはプレフィックスがプレフィックス リストに追加される場合、TE トンネルを通過せずに動的にルーティングされます。IP アドレスまたはプレフィックスがプレフィックス リストから削除される場合、TE トンネル パスで動的に再ルーティングされるようになります。

OSPFv2 自動ルート除外の設定方法

OSPFv2 自動ルート除外の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router ospf***process-ID*
4. **router-id***ip-address*
5. **mpls traffic-eng router-id***interface-name*
6. **mpls traffic-eng area***number*
7. **mpls traffic-eng autoroute-exclude prefix-list***prefix-list-name*
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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	**configure terminal** 例： `Device# 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	**router ospf***process-ID* 例： `Device(config)# router ospf 18`	OSPF ルーティング プロセスを設定し、OSPF ルータ コンフィギュレーション モードを開始します。
ステップ 4	**router-id***ip-address* 例： `Device(config-router)# router-id 10.1.1.1`	ルータ コンフィギュレーション モードで固定ルータ ID を使用できるようにします。
ステップ 5	**mpls traffic-eng router-id***interface-name* 例： `Device(config-router)# mpls traffic-eng router-id Loopback0`	ノードのトラフィック エンジニアリング ルータ識別子および指定されたインターフェイスに関連付けられている IP アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 6	**mpls traffic-eng area***number* 例： `Device(config-router)# mpls traffic-eng area 0`	指定した OSPF エリアに対してトラフィック エンジニアリングをフラッディングするように、OSPF MPLS を実行しているルータを設定します。
ステップ 7	**mpls traffic-eng autoroute-exclude prefix-list***prefix-list-name* 例： `Device(config-router)# mpls traffic-eng autoroute-exclude prefix-list kmd`	特定の宛先およびプレフィックスを、TE トンネルによるルーティングを回避するように指定できます。 • 除外されるプレフィックスは、TE トンネル パスを使用しません。
ステップ 8	**exit** 例： `Device(config-router)# exit`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

OSPFv2 自動ルート除外の設定例

例：OSPFv2 自動ルート除外の設定

```
!
router ospf 1
 router-id 3.3.3.3
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 mpls traffic-eng autoroute-exclude prefix-list XX

!
```

OSPFv2 自動ルート除外に関する追加情報

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 Command List, All Releases』

関連項目	マニュアル タイトル
『Configuring OSPF』	*IP* ルーティング：*OSPF* コンフィギュレーション ガイド
基本的なシスコ エクスプレス フォワーディングの設定	『*IP Switching: Cisco Express Forwarding Configuration Guide*』
MPLS トラフィック エンジニアリング トンネル ソース	『*MPLS Traffic Engineering Path Calculation and Setup Configuration Guide*』

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

OSPFv2 自動ルート除外の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *17* : *OSPFv2* 自動ルート除外の機能情報

機能名	リリース	機能情報
OSPFv2 自動ルート除外	Cisco IOS XE 3.13S	OSPFv2 自動ルート除外機能により、特定の宛先およびプレフィックスを指定して、パケット転送用の TE トンネルを回避することができます。 次のコマンドが導入または変更されました。**mpls traffic-eng autoroute-exclude prefix list**

第 15 章

OSPFv3 アドレス ファミリ

Open Shortest Path First バージョン 3（OSPFv3）アドレス ファミリ機能では、IPv4 および IPv6 ユニキャスト トラフィックの両方がサポートされます。この機能を使用すると、ユーザはインターフェイスごとに 2 つのプロセスを持つことができますが、アドレス ファミリ（AF）ごとには 1 つのプロセスのみです。

- 機能情報の確認，185 ページ
- OSPFv3 アドレス ファミリの前提条件，186 ページ
- OSPFv3 アドレス ファミリに関する情報，186 ページ
- OSPFv3 アドレス ファミリの設定方法，187 ページ
- OSPFv3 アドレス ファミリの設定例，202 ページ
- その他の参考資料，202 ページ
- OSPFv3 アドレス ファミリの機能情報，204 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。

OSPFv3 アドレス ファミリの前提条件

- OSPFv3 で IPv4 ユニキャスト アドレス ファミリ（AF）を使用するには、リンクが IPv6 ユニキャスト AF に参加していない場合でも、リンクで IPv6 をイネーブルにする必要があります。
- OSPFv3 アドレス ファミリ機能を使用する場合、ユーザにはインターフェイスごとに 2 つのプロセス、AF ごとには 1 つのプロセスのみが提供される場合があります。AF が IPv4 である場合、最初に IPv4 アドレスをインターフェイス上で設定する必要がありますが、そのインターフェイスで IPv6 をイネーブルにする必要があります。

OSPFv3 アドレス ファミリに関する情報

OSPFv3 アドレス ファミリ

OSPFv3 アドレス ファミリ機能では、IPv4 および IPv6 ユニキャスト トラフィックの両方がサポートされます。この機能を使用すると、ユーザはインターフェイスごとに 2 つのプロセスを持つことができますが、AF ごとには 1 つのプロセスのみです。IPv4 AF を使用する場合は、最初に IPv4 アドレスをインターフェイス上で設定する必要がありますが、そのインターフェイスで IPv6 をイネーブルにする必要があります。同一のインターフェイス上での、1 つの IPv4 または IPv6 OSPFv3 プロセスによる複数のインスタンスの実行はサポートされていません。

OSPFv3 を使用する IPv6 ネットワークを IGP としているユーザは、同一の IGP を IPv4 ルートの伝送およびインストールに役立てることもできます。このネットワークのすべてのデバイスには、IPv6 転送スタックがあります。このネットワークのリンクの一部（または全部）では、IPv4 転送を実行したり、IPv4 アドレスを設定したりすることができます。IPv4 スタティックまたはダイナミック ルーティング プロトコルを実行しているエッジの周辺には、IPv4 専用デバイスのポケットが存在します。このシナリオでは、ユーザはトンネリング オーバーヘッドを使用せずに、これらのポケット間で IPv4 トラフィックを転送する機能が必要になります。つまり、すべての IPv4 中継デバイスが IPv4 と IPv6 両方の転送スタック（たとえばデュアル スタック）を持つことになります。

この機能を使用すると、IPv4 AF 用に別々の（異なる）トポロジを構築できます。この機能により IPv4 ルートが IPv4 RIB にインストールされた後、ネイティブで転送が行われます。OSPFv3 プロセスでは IPv4 AF トポロジがフル サポートされており、ルートをその他のすべての IPv4 ルーティング プロトコルとの間で再配布することができます。

OSPFv3 プロセスは、IPv4 または IPv6 のいずれにも設定できます。**address-family** コマンドは、どの AF を OSPFv3 プロセスで実行するかを決定するために使用されます。また、インスタンスごとに設定できるアドレス ファミリは 1 つだけです。AF を選択したら、ユーザはリンク上で複数のインスタンスをイネーブルにして、アドレスファミリ固有のコマンドをイネーブルにできます。

各 AF には、異なるインスタンス ID 範囲が使用されます。各 AF は異なる隣接関係を確立し、異なるリンク ステート データベースを持ち、異なる最短パス ツリーを計算します。その後、AF は

AF 固有の RIB にルートをインストールします。IPv6 ユニキャスト プレフィックスを伝送する LSA は、異なるインスタンス内で変更されることなく、各 AF のプレフィックスを伝送します。

OSPFv3 をイネーブルにしたインターフェイスに設定されている IPv4 サブネットは、IPv6 プレフィックスと同様に、エリア内プレフィックス LSA を介してアドバタイズされます。外部 LSA は、任意の IPv4 ルーティング プロトコル（接続およびスタティックを含む）から再配布された IPv4 ルートのアドバタイズに使用されます。IPv4 OSPFv3 プロセスは SPF 計算を実行して、IPv4 宛先への最短パスを検出します。計算されたこれらのルートは、その後 IPv4 RIB に挿入されます（IPv6 AF の場合、計算されたルートは IPv6 RIB に挿入されます）。

IPv4 OSPFv3 プロセスは一意の pdbindex を IPv4 RIB に割り当てるため、その他すべての IPv4 ルーティング プロトコルでそのルートを再配布できます。すべてのプロトコルの解析チェーンは同一であるため、IPv4 ルーティング プロトコルに **ospfv3** キーワードを追加すると、どの IPv4 ルーティング プロトコルから使用した場合でも、**redistribute** コマンドに OSPFv3 が表示されます。**ospfv3** キーワードを使用すると、**redistributeospfv3** コマンドで定義されているように、IPv4 OSPFv3 ルートをその他すべての IPv4 ルーティング プロトコルに再配布できます。

サードパーティ デバイスは、AF ビットを設定しないため、IPv4 AF の AF 機能を実行するデバイスとは隣接しません。そのため、これらのデバイスは IPv4 AF SPF 計算には参加せず、IPv6 RIB に IPv4 OSPFv3 ルートをインストールすることはありません。

OSPFv3 アドレス ファミリの設定方法

OSPFv3 ルータ プロセスの設定

ステップ 3 を完了し、OSPFv3 ルータ コンフィギュレーション モードを開始したら、必要に応じてこの作業の以降のステップを任意に実行して、OSPFv3 デバイス コンフィギュレーションを実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospfv3**[*process-id*]
4. **area***area-ID* [**default-cost** | **nssa** | **stub**]
5. **auto-costreference-bandwidth***Mbps*
6. **bfdall-interfaces**
7. **default** {**area***area-ID*[**range***ipv6-prefix* | **virtual-link***router-id*]} [**default-informationoriginate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list***prefix-listprefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths***paths* | **redistribute***protocol* | **summary-prefix***ipv6-prefix*]
8. **ignorelsamospf**
9. **interface-idsnmp-if-index**
10. **log-adjacency-changes** [**detail**]
11. passive-interface [**default** | *interface-typeinterface-number*]
12. **queue-depth**{**hello** | **update**} {*queue-size* | **unlimited**}
13. router-id {*router-id*}

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	**configureterminal** 例： `Device# 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	**routerospfv3**[*process-id*] 例： `Device(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area***area-ID* [**default-cost**	**nssa**	**stub**] 例： `Device(config-router)# area 1`	OSPFv3 エリアを設定します。

	コマンドまたはアクション	目的
ステップ 5	**auto-costreference-bandwidth***Mbps* 例： `Device(config-router)# auto-cost reference-bandwidth 1000`	IPv4 OSPFv3 プロセスで、インターフェイスのメトリックを計算する際に OSPFv3 で使用される基準値を制御します。
ステップ 6	**bfdall-interfaces** 例： `Device(config-router)# bfd all-interfaces`	OSPFv3 ルーティング プロセスの BFD をイネーブルにします。
ステップ 7	**default** {**area***area-ID*[**range***ipv6-prefix* | **virtual-link***router-id*]} [**default-informationoriginate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list***prefix-listprefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths***paths* | **redistribute***protocol* | **summary-prefix***ipv6-prefix*] 例： `Device(config-router)# default area 1`	OSPFv3 パラメータをデフォルト値に戻します。
ステップ 8	**ignorelsamospf** 例： `Device(config-router)# ignore lsa mospf`	デバイスが LSA タイプ 6 Multicast OSPFv3 パケットを受信した場合の syslog メッセージの送信を抑制します（LSA タイプ 6 Multicast OSPFv3 はサポートされていません）。
ステップ 9	**interface-idsnmp-if-index** 例： `Device(config-router)# interface-id snmp-if-index`	IPv4 および IPv6 の簡易ネットワーク管理プロトコル（SNMP）MIB-II インターフェイスインデックス（ifIndex）ID 番号を使用して OSPFv3 インターフェイスを設定します。
ステップ 10	**log-adjacency-changes** [**detail**] 例： `Device(config-router)# log-adjacency-changes`	OSPFv3 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 11	passive-interface [**default** | *interface-typeinterface-number*] 例： `Device(config-router)# passive-interface default`	IPv4 OSPFv3 プロセスを使用しているときに、インターフェイスのルーティングアップデートの送信を抑制します。

	コマンドまたはアクション	目的
ステップ 12	**queue-depth**{**hello** | **update**} {*queue-size* | **unlimited**} 例： `Device(config-router)# queue-depth update 1500`	IPv4 OSPFv3 プロセスのキューに保持できる着信パケット数を設定します。
ステップ 13	router-id {*router-id*} 例： `Device(config-router)# router-id 10.1.1.1`	固定デバイス ID を使用します。

OSPFv3 への IPv6 アドレス ファミリの設定

OSPFv3 に IPv6 アドレス ファミリを設定するには、次の作業を実行します。ステップ 4 を完了し、IPv6 アドレス ファミリ コンフィギュレーション モードを開始したら、必要に応じてこの作業の以降のステップを任意に実行して、IPv6 AF を設定します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospfv3**[*process-id*]
4. **address-familyipv6unicast**
5. **area***area-ID***range***ipv6-prefix*/*prefix-length*
6. **default** {**area***area-ID*[**range***ipv6-prefix* | **virtual-link***router-id*]} [**default-informationoriginate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list***prefix-listprefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths***paths* | **redistribute***protocol* | **summary-prefix***ipv6-prefix*]
7. **default-informationoriginate** [**always** | **metric***metric-value* | **metric-type***type-value*| **route-map***map-name*]
8. default-metric *metric-value*
9. **distance***distance*
10. **distribute-listprefix-list***list-name* {**in**[*interface-typeinterface-number*] | **out***routing-process* [*as-number*]}
11. **maximum-paths***number-paths*
12. **summary-prefix***prefix*[**not-advertise** | **tag***tag-value*]

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	**routerospfv3**[*process-id*] 例： `Router(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**address-familyipv6unicast** 例： 例： or 例： **address-family ipv4** **unicast** 例： `Router(config-router)# address-family ipv6 unicast` 例： 例： or	OSPFv3 の IPv6 アドレス ファミリ コンフィギュレーション モードを開始します。 または OSPFv3 の IPv4 アドレス ファミリ 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
	例： `Router(config-router)# address-family ipv4 unicast`	
ステップ 5	**area***area-ID***range***ipv6-prefix*/*prefix-length* 例： `Router(config-router-af)# area 1 range 2001:DB8:0:0::0/128`	OSPFv3 エリア パラメータを設定します。
ステップ 6	**default** {**area***area-ID*[**range***ipv6-prefix* | **virtual-link***router-id*]} [**default-informationoriginate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list***prefix-listprefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths***paths* | **redistribute***protocol* | **summary-prefix***ipv6-prefix*] 例： `Router(config-router-af)# default area 1`	OSPFv3 パラメータをデフォルト値に戻します。
ステップ 7	**default-informationoriginate** [**always** | **metric***metric-value* | **metric-type***type-value*| **route-map***map-name*] 例： `Router(config-router-af)# default-information originate always metric 100 metric-type 2`	デフォルトの外部ルートをルーティング ドメインの OSPFv3 に生成します。
ステップ 8	default-metric *metric-value* 例： `Router(config-router-af)# default-metric 10`	OSPFv3 ルーティング プロトコルに再配布される IPv4 および IPv6 ルートのデフォルト メトリック値を設定します。
ステップ 9	**distance***distance* 例： `Router(config-router-af)# distance 200`	ルーティング テーブルに挿入された OSPFv3 ルートのアドミニストレーティブ ディスタンスを設定します。

	コマンドまたはアクション	目的
ステップ 10	**distribute-listprefix-list***list-name* {**in**[*interface-typeinterface-number*] | **out***routing-process* [*as-number*]} 例： `Router(config-router-af)# distribute-list prefix-list PL1 in Ethernet0/0`	インターフェイス上で受信または送信される OSPFv3 ルーティング アップデートに、プレフィックス リストを適用します。
ステップ 11	**maximum-paths***number-paths* 例： `Router(config-router-af)# maximum-paths 4`	OSPFv3 ルーティングのプロセスでサポートできる等コスト ルートの最大数を制御します。
ステップ 12	**summary-prefix***prefix*[**not-advertise** | **tag***tag-value*] 例： `Router(config-router-af)# summary-prefix FEC0::/24`	OSPFv3 に IPv6 サマリー プレフィックスを設定します。

OSPFv3 への IPv4 アドレス ファミリの設定

OSPFv3 に IPv4 アドレス ファミリを設定するには、次の作業を実行します。ステップ 4 を完了し、IPv4 アドレス ファミリ コンフィギュレーション モードを開始したら、必要に応じてこの作業の以降のステップを任意に実行して、IPv4 AF を設定します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospfv3**[*process-id*]
4. **address-familyipv4unicast**
5. **area***area-id***range***ip-addressip-address-mask*[**advertise** | **not-advertise**] [**cost***cost*]
6. **default** {**area***area-ID*[**range***ipv6-prefix* | **virtual-link***router-id*]} [**default-informationoriginate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list***prefix-listprefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths***paths* | **redistribute***protocol* | **summary-prefix***ipv6-prefix*]
7. **default-informationoriginate** [**always** | **metric***metric-value* | **metric-type***type-value*| **route-map***map-name*]
8. default-metric *metric-value*
9. **distance***distance*
10. **distribute-listprefix-list***list-name* {**in**[*interface-typeinterface-number*] | **out***routing-process* [*as-number*]}
11. **maximum-paths***number-paths*
12. **summary-prefix***prefix*[**not-advertise** | **tag***tag-value*]

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	**configureterminal** 例： `Device# 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	**routerospfv3**[*process-id*] 例： `Device(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**address-familyipv4unicast** 例： `Device(config-router)# address-family ipv4 unicast`	OSPFv3 の IPv4 アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**area***area-id***range***ip-addressip-address-mask*[**advertise**	**not-advertise**] [**cost***cost*]	エリア境界でルートを統合および集約します。

	コマンドまたはアクション	目的
	例： `Device(config-router-af)# area 0 range 192.168.110.0 255.255.0.0`	
ステップ 6	**default** {**area***area-ID*[**range***ipv6-prefix* | **virtual-link***router-id*]} [**default-informationoriginate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list***prefix-listprefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths***paths* | **redistribute***protocol* | **summary-prefix***ipv6-prefix*] 例： `Device(config-router-af)# default area 1`	OSPFv3パラメータをデフォルト値に戻します。
ステップ 7	**default-informationoriginate** [**always** | **metric***metric-value* | **metric-type***type-value*| **route-map***map-name*] 例： `Device(config-router-af)# default-information originate always metric 100 metric-type 2`	デフォルトの外部ルートをルーティング ドメインの OSPFv3 に生成します。
ステップ 8	default-metric *metric-value* 例： `Device(config-router-af)# default-metric 10`	OSPFv3 ルーティング プロトコルに再配布されるIPv4およびIPv6ルートのデフォルト メトリック値を設定します。
ステップ 9	**distance***distance* 例： `Device(config-router-af)# distance 200`	ルーティングテーブルに挿入されたOSPFv3ルートのアドミニストレーティブ ディスタンスを設定します。
ステップ 10	**distribute-listprefix-list***list-name* {**in**[*interface-typeinterface-number*] | **out***routing-process* [*as-number*]} 例： `Device(config-router-af)# distribute-list prefix-list PL1 in Ethernet0/0`	インターフェイス上で受信または送信される OSPFv3 ルーティング アップデートに、プレフィックス リストを適用します。

	コマンドまたはアクション	目的
ステップ 11	**maximum-paths***number-paths* 例： `Device(config-router-af)# maximum-paths 4`	OSPFv3 ルーティングのプロセスでサポートできる等コスト ルートの最大数を制御します。
ステップ 12	**summary-prefix***prefix*[**not-advertise** | **tag***tag-value*] 例： `Device(config-router-af)# summary-prefix FEC0::/24`	OSPFv3 に IPv6 サマリー プレフィックスを設定します。

OSPFv3 へのルート再配布の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospfv3**[*process-id*]
4. **address-familyipv6unicast**
5. **redistribute** source-*protocol* [*process-id*] [*options*]

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	**routerospfv3**[*process-id*] 例： `Router(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。

ステップ 4	**address-familyipv6unicast**
	例：
	例：
	`or`
	例：
	address-family ipv4
	unicast
	例：
	`Router(config-router)# address-family ipv6 unicast`
	例：
	例：
	`or`
	例：
	`Router(config-router)# address-family ipv4 unicast`
		OSPFv3 の IPv6 アドレス ファミリ コンフィギュレーション モードを開始します。
		または
		OSPFv3 の IPv4 アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ 5	**redistribute** source-*protocol* [*process-id*] [*options*] 例：	あるルーティング ドメインから別のルーティング ドメインへ IPv6 および IPv4 ルートを再配布します。

インターフェイス上での OSPFv3 のイネーブル化

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. 次のいずれかを実行します。
   - **ospfv3***process-id***area***area-ID* {**ipv4** | **ipv6**} [**instance***instance-id*]
   - **ipv6ospf***process-id***area***area-id*[**instance***instance-id*]

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	**configureterminal** 例： `Device# 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	**interface***typenumber* 例： `Device(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 4	次のいずれかを実行します。 • **ospfv3***process-id***area***area-ID* {**ipv4** | **ipv6**} [**instance***instance-id*] • **ipv6ospf***process-id***area***area-id*[**instance***instance-id*] 例： `Device(config-if)# ospfv3 1 area 1 ipv4`	IPv4 または IPv6 AF を設定したインターフェイスで OSPFv3 をイネーブルにします。 または インターフェイスでOSPFv3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： `Device(config-if)# ipv6 ospf 1 area 0`	

IPv6 または IPv4 アドレス ファミリに対する OSPFv3 エリア範囲の定義

集約されたルートのコストは、集約されるルートの最高コストとなります。たとえば、次のルートが集約されるとします。

```
OI  2001:DB8:0:7::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:6F00, GigabitEthernet0/0/0
OI  2001:DB8:0:8::/64 [110/100]
     via FE80::A8BB:CCFF:FE00:6F00, GigabitEthernet0/0/0
OI  2001:DB8:0:9::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:6F00, GigabitEthernet0/0/0
```

これらは、次のように 1 つの集約されたルートとなります。

```
OI  2001:DB8::/48 [110/100]
     via FE80::A8BB:CCFF:FE00:6F00, GigabitEthernet0/0/0
```

はじめる前に

OSPFv3 ルーティングがイネーブルであること。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **address-family ipv6 unicast**
5. **area** *area-ID* **range** *ipv6-prefix*

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	**configure terminal** 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	**router ospfv3** [*process-id*] 例： `Router(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。

ステップ 4	**address-family ipv6 unicast**
	例：
	例：
	or
	例：
	address-family ipv4
	unicast
	例：
	`Router(config-router)# address-family ipv6 unicast`
	例：
	例：
	or
	例：
	`Router(config-router)# address-family ipv4 unicast`
		OSPFv3 の IPv6 アドレス ファミリ コンフィギュレーション モードを開始します。
		または
		OSPFv3 の IPv4 アドレス ファミリ 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 5	**area** *area-ID* **range** *ipv6-prefix* 例： `Router(config-router-af)# area 1 range 2001:DB8:0:0::0/128`	OSPFv3 エリア パラメータを設定します。

OSPFv3 エリア範囲の定義

次のタスクは、Cisco IOS XE Release 3.4S 以前のリリースで実行できます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6routerospf***process-id*
4. **area***area-id***range***ipv6-prefix*/*prefix-length***advertise** | **not-advertise**] [**cost***cost*]

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	**ipv6routerospf***process-id* 例： `Router(config)# ipv6 router ospf 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area***area-id***range***ipv6-prefix*/*prefix-length***advertise**	**not-advertise**] [**cost***cost*]	エリア境界でルートを統合および集約します。

	コマンドまたはアクション	目的
	例： `Router(config-rtr)# area 1 range 2001:DB8::/48`	

OSPFv3 アドレス ファミリの設定例

例：OSPFv3 アドレス ファミリの設定

```
Device# show ospfv3
 Routing Process "ospfv3 1" with ID 10.0.0.1
 Supports IPv6 Address Family
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 Graceful restart helper support enabled
 Reference bandwidth unit is 100 mbps
 Relay willingness value is 128
 Pushback timer value is 2000 msecs
 Relay acknowledgement timer value is 1000 msecs
 LSA cache Disabled : current count 0, maximum 1000
 ACK cache Disabled : current count 0, maximum 1000
 Selective Peering is not enabled
 Hello requests and responses will be sent multicast
```

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
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』
OSPFv3 アドレス ファミリ	*OSPF Forwarding Address Suppression in Translated Type-5 LSAs* モジュール

標準および RFC

標準/RFC	Title
IPv6 に関する RFC	IPv6 の RFC

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

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

OSPFv3 アドレス ファミリの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *18* : *OSPFv3* アドレス ファミリの機能情報

機能名	リリース	機能情報
OSPFv3 アドレス ファミリ	Cisco IOS XE Release 3.4S	

機能名	リリース	機能情報
		OSPFv3 アドレス ファミリ機能では、IPv4 および IPv6 ユニキャスト トラフィックを 1 つのネットワーク トポロジでサポートできます。 次のコマンドが導入または変更されました。**address-family ipv4 (OSPFv3)**、**address-family ipv6 (OSPFv3)**、**area (OSPFv3)**、**auto-cost (OSPFv3)**、**bfd all-interfaces (OSPFv3)**、**clear ospfv3 counters**、**clear ospfv3 force-spf**、**clear ospfv3 process**、**clear ospfv3 redistribution**、**clear ospfv3 traffic**、**debug ospfv3**、**debug ospfv3 database-timer rate-limit**、**debug ospfv3 events**、**debug ospfv3 lsdb**、**debug ospfv3 packet**、**debug ospfv3 spf statistic**、**default (OSPFv3)**、**default-information originate (OSPFv3)**、**default-metric (OSPFv3)**、**distance (OSPFv3)**、**distribute-list prefix-list (OSPFv3)**、**event-log (OSPFv3)**、**log-adjacency-changes (OSPFv3)**、**maximum-paths (OSPFv3)**、**ospfv3 area**、**ospfv3 authentication**、**ospfv3 bfd**、**ospfv3 cost**、**ospfv3 database-filter**、**ospfv3 dead-interval**、**ospfv3 demand-circuit**、**ospfv3 encryption**、**ospfv3 flood-reduction**、**ospfv3 hello-interval**、**ospfv3 mtu-ignore**、**ospfv3 network**、**ospfv3 priority**、**ospfv3 retransmit-interval**、**ospfv3 transmit-delay**、

機能名	リリース	機能情報
		passive-interface (OSPFv3)、**queue-depth (OSPFv3)**、**redistribute (OSPFv3)**、**router ospfv3**、**router-id (OSPFv3)**、**show ospfv3 border-routers**、**show ospfv3 database**、**show ospfv3 events**、**show ospfv3 flood-list**、**show ospfv3 graceful-restart**、**show ospfv3 interface**、**show ospfv3 max-metric**、**show ospfv3 neighbor**、**show ospfv3 request-list**、**show ospfv3 retransmission-list**、**show ospfv3 statistics**、**show ospfv3 summary-prefix**、**show ospfv3 timers rate-limit**、**show ospfv3 traffic**、**show ospfv3 virtual-links**、**summary-prefix (OSPFv3)**、**timers pacing flood (OSPFv3)**、**timers pacing lsa-group (OSPFv3)**、**timers pacing retransmission (OSPFv3)**

第 16 章

OSPFv3 認証トレーラ

RFC 6506 で指定される OSPFv3 認証トレーラ機能は、既存の OSPFv3 IPsec 認証の代わりとして Open Shortest Path First バージョン 3（OSPFv3）プロトコル パケットを認証するメカニズムを提供します。

- 機能情報の確認，209 ページ
- OSPFv3 認証トレーラに関する情報，210 ページ
- OSPFv3 認証トレーラの設定方法，211 ページ
- OSPFv3 認証トレーラの設定例，213 ページ
- OSPFv3 認証トレーラに関する追加情報，214 ページ
- OSPFv3 認証トレーラの機能情報，215 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。

OSPFv3 認証トレーラに関する情報

OSPFv3 認証トレーラの概要

OSPFv3 認証トレーラの前は、RFC 4552 で定義されている OSPFv3 IPsec がプロトコル パケットの認証を行う唯一のメカニズムでした。OSPFv3 認証トレーラ機能では、シーケンス番号を介してパケット リプレイ保護を追加で提供する OSPFv3 プロトコル パケットの認証を行う代替のメカニズムを定義しており、プラットフォームに依存しません。

非 IPsec 暗号化認証を実行するため、OSPFv3 デバイスは OSPFv3 パケットの末尾に特別なデータ ブロック（認証トレーラ）を追加します。認証トレーラの長さは OSPFv3 パケットの長さに含まれず、IPv6 ペイロード長に含まれます。リンクローカル シグナリング（LLS）ブロックは OSPFv3 hello およびデータベース説明パケットの「OSPFv3 Options」フィールドの L-bit 設定で確立されます。存在する場合、LLS データ ブロックは暗号化認証計算の OSPFv3 パケットにも含まれます。

新しい認証トレーラ（AT）ビットは OSPFv3 Options フィールドに導入されています。OSPFv3 デバイスは、このリンク上のすべてのパケットに認証トレーラが含まれてることを示すため、OSPFv3 Hello および Database Description パケットで AT-bit を設定する必要があります。OSPFv3 Hello および Database Description パケットでは、AT-bit は AT があることを示します。他の OSPFv3 パケット タイプでは、OSPFv3 Hello/Database Description 設定の OSPFv3 AT-bit 設定は OSPFv3 ネイバー データ構造に保持されます。OSPFv3 Options フィールドを含まない OSPFv3 パケット タイプでは、ネイバー データ構造の設定を使用して AT が必要かどうかを決定します。AT-bit は、認証トレーラを含むすべての OSPFv3 Hello および Database Description パケットで設定する必要があります。

認証トレーラを設定するには、OSPFv3 では既存の Cisco IOS **key chain** コマンドを使用します。発信 OSPFv3 パケットでは、次のルールを使用してキー チェーンからキーを選択します。

- 最後に期限切れになるキーを選択します。
- 2 つのキーの終了時間が同じ場合、最も大きいキー ID のキーを選択します。

セキュリティ アソシエーション（SA）ID は認証アルゴリズムと秘密鍵にマッピングされ、メッセージ ダイジェストの生成および検証に使用されます。認証が設定されていても、最後の有効なキーが期限切れになると、パケットはそのキーを使用して送信されます。syslog メッセージも生成されます。有効なキーが使用できない場合は、トレーラ認証なしでパケットが送信されます。パケットが受信されると、そのキーのデータを検索するためにキー ID が使用されます。キー チェーンにキー ID が見つからない、または SA が有効でない場合、パケットはドロップされます。そうでない場合、パケットはキー ID で設定されたアルゴリズムとキーを使用して検証されます。キー チェーンはキーのライフタイムを使用するロールオーバーをサポートします。新しいキーは、将来設定する開始時間の送信でキー チェーンに追加できます。この設定により、キーが実際に使用される前に新しいキーをすべてのデバイスで設定できます。

hello パケットの優先順位はその他の OSPFv3 パケットより優先順位の高いため、発信インターフェイスで順序変更することができます。この再順序付けにより、隣接デバイスでシーケンス番号の健勝に関する問題が発生することがあります。シーケンスの不一致を防ぐには、OSPFv3 でパケット タイプごとに個別にシーケンス番号を検証します。

認証手順の詳細については、RFC 6506 を参照してください。

OSPFv3 認証トレーラの設定方法

OSPFv3 認証トレーラの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface** *type number*
4. **ospfv3** [*pid*][**ipv4** | **ipv6**]**authentication**{**key-chain***chain-name* | **null**}
5. **router ospfv3** [*process-id*]
6. **address-family ipv6 unicast vrf** *vrf-name*
7. **area***area-id* **authentication**{**key-chain** *chain-name* | **null**}
8. **area***area-id* **virtual-link***router-id***authentication key-chain** *chain-name*
9. **area***area-id* **sham-link***source-addressdestination-address***authentication key-chain** *chain-name*
10. **authentication mode**{**deployment** | **normal**}
11. **end**
12. **show ospfv3 interface**
13. **show ospfv3 neighbor** [*detail*]
14. **debug ospfv3 vrf authentication**

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	**configure terminal** 例： `Device# 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	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 2/0`	インターフェイス タイプおよび番号を指定します。

	コマンドまたはアクション	目的
ステップ 4	**ospfv3** [*pid*][**ipv4** | **ipv6**]**authentication**{**key-chain***chain-name* | **null**} 例： `Device(config-if)# ospfv3 1 ipv4 authentication key-chain ospf-1`	OSPFv3インターフェイスの認証タイプを指定します。
ステップ 5	**router ospfv3** [*process-id*] 例： `Device(config-if)# router ospfv3 1`	OSPFv3ルータ コンフィギュレーション モードを開始します。
ステップ 6	**address-family ipv6 unicast vrf** *vrf-name* 例： `Device(config-router)# address-family ipv6 unicast vrf vrf1`	OSPFv3 プロセスに IPv6 アドレス ファミリを設定し、IPv6 アドレス ファミリ 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	**area***area-id* **authentication**{**key-chain** *chain-name* | **null**} 例： `Device(config-router-af)# area 1 authentication key-chain ospf-chain-1`	OSPFv3エリア内のすべてのインターフェイスの認証トレーラを設定します。
ステップ 8	**area***area-id* **virtual-link***router-id***authentication key-chain** *chain-name* 例： `Device(config-router-af)# area 1 virtual-link 1.1.1.1 authentication key-chain ospf-chain-1`	仮想リンクの認証を設定します。
ステップ 9	**area***area-id* **sham-link***source-addressdestination-address***authentication key-chain** *chain-name* 例： `Device(config-router-af)# area 1 sham-link 1.1.1.1 1.1.1.0 authentication key-chain ospf-chain-1`	模造リンクの認証を設定します。
ステップ 10	**authentication mode**{**deployment** | **normal**} 例： `Device(config-router-af)# authentication mode deployment`	OSPFv3インスタンスに使用する認証のタイプを指定します。 • **deployment** キーワードは、認証を設定済みのデバイスと未設定のデバイス間の隣接関係を表示します。
ステップ 11	**end** 例： `Device(config-router-af)# end`	IPv6 アドレス ファミリ 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。

	コマンドまたはアクション	目的
ステップ 12	**show ospfv3 interface** 例： `Device# show ospfv3`	（任意）OSPFv3 関連のインターフェイス情報を表示します。
ステップ 13	**show ospfv3 neighbor** [*detail*] 例： `Device# show ospfv3 neighbor detail`	（任意）OSPFv3 ネイバー情報をインターフェイスごとに表示します。
ステップ 14	**debug ospfv3 vrf authentication** 例： `Device# debug ospfv3 vrf authentication`	（任意）OSPFv3 のデバッグ情報を表示します。

OSPFv3 認証トレーラの設定例

例：OSPFv3 認証トレーラの設定

```
interface GigabitEthernet 0/0
 ospfv3 1 ipv4 authentication key-chain ospf-1
 router ospfv3 1
  address-family ipv6 unicast vrf vrf1
   area 1 authentication key-chain ospf-1
   area 1 virtual-link 1.1.1.1 authentication key-chain ospf-1
   area 1 sham-link 1.1.1.1 authentication key-chain ospf-1
   authentication mode deployment
!
key chain ospf-1
key 1
   key-string ospf
   cryptographic-algorithm hmac-sha-512
!
```

例：OSPFv3 認証トレーラの確認

次に、**show ospfv3** コマンドの出力例を示します。

```
Device# show ospfv3
 OSPFv3 1 address-family ipv6
 Router ID 1.1.1.1
…
RFC1583 compatibility enabled
 Authentication configured with deployment key lifetime
 Active Key-chains:
```

```
  Key chain mama: Send key 1, Algorithm HMAC-SHA-256, Number of interfaces 1
    Area BACKBONE(0)

Device# show ospfv3 neighbor detail

OSPFv3 1 address-family ipv6 (router-id 2.2.2.2)

 Neighbor 1.1.1.1
    In the area 0 via interface GigabitEthernet0/0
    Neighbor: interface-id 2, link-local address FE80::A8BB:CCFF:FE01:2D00
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 2.2.2.2 BDR is 1.1.1.1
    Options is 0x000413 in Hello (V6-Bit, E-Bit, R-Bit, AT-Bit)
    Options is 0x000413 in DBD (V6-Bit, E-Bit, R-Bit, AT-Bit)
    Dead timer due in 00:00:33
    Neighbor is up for 00:05:07
    Last packet authentication succeed
    Index 1/1/1, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec


Device# show ospfv3 interface

GigabitEthernet0/0 is up, line protocol is up
…
  Cryptographic authentication enabled
    Sending SA: Key 25, Algorithm HMAC-SHA-256 - key chain ospf-keys
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

OSPFv3 認証トレーラに関する追加情報

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 Command List, All Releases』
OSPF 機能の設定	IP ルーティング：OSPF コンフィギュレーション ガイド

標準および RFC

関連項目	マニュアル タイトル
OSPFv3 認証トレーラのサポートに関する RFC	RFC 6506
OSPFv3 の認証/機密性に関する RFC	RFC 4552

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

OSPFv3 認証トレーラの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *19* : *OSPFv3* 認証トレーラの機能情報

機能名	リリース	機能情報
OSPFv3 認証トレーラ	Cisco IOS XE Release 3.11S	RFC 6506 で OSPFv3 認証トレーラ機能を指定すると、既存の OSPFv3 IPsec 認証の代替として OSPFv3 プロトコルパケットを認証するための機能が提供されます。 次のコマンドが導入または変更されました。**ospfv3 authentication key-chain**、**authentication mode**、**debug ospfv3 vrf authentication**

第 17 章

OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）

OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）機能は、MPLS/TE IPv4 トンネルを介して IPv6 ルートをアドバタイズします。ここでは、OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）機能を設定する方法について説明します。

- 機能情報の確認，217 ページ
- OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）の前提条件，218 ページ
- OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）の制約事項，218 ページ
- OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）について，218 ページ
- OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）の設定方法，220 ページ
- OSPFv3 の自動ルート通知および Forwarding Adjacency の設定例，223 ページ
- OSPFv3 の自動ルート通知および Forwarding Adjacency に関する追加情報，224 ページ
- OSPFv3 の自動ルート通知および Forwarding Adjacency の機能情報，225 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。

OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）の前提条件

- OSPFv3 がネットワークで設定されている。
- シスコ エクスプレス フォワーディング（CEF）がイネーブルになっている。
- MPLS/TE トンネルが設定されている。

OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）の制約事項

- 自動ルート通知と Forwarding Adjacency（FA）は同じインターフェイスで同時に設定できません。
- 自動ルート通知を使用すると、OSPFv3 はトンネルをアドバタイズしません。
- Forwarding Adjacency（FA）を使用すると、OSPFv3 はトンネル リンクを LSA にアドバタイズします。

OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）について

OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）の概要

MPLS トラフィック エンジニアリングされたトンネルを介した Forwarding Adjacency（FA）の OSPFv3 サポート機能により、マルチプロトコル ラベル スイッチング（MPLS）トラフィック エンジニアリング（TE）トンネル機能に OSPFv3 サポートが追加され、ネットワーク管理者は最短パス優先（SPF）アルゴリズムに基づいて内部ゲートウェイ プロトコル（IGP）ネットワークのリンクとしてトラフィックエンジニアリング、MPLS トンネルを処理できるようになります。OSPFv3 Forwarding Adjacency（FA）は、同じエリアのルータ間で作成できます。

OSPFv3 は、トラフィックのルーティングおよび転送のために他のリンクが表示されるのと同様に、MPLS TE トンネルを OSPFv3 リンクステート アドバタイズメント（LSA）に含めます。ユーザは、トンネルに OSPFv3 コストを割り当てて他のリンクに対する優先を設定することができます。他のネットワーク デバイスには、物理リンクに加えてトンネルがリンクとして表示されます。

OSPFv3 は自動ルート通知（AA）または Forwarding Adjacency（FA）機能を使用して、MPLS/TE IPv4 トンネル経由の IPv6 ルートを IPv6 ルーティング テーブルにインストールします。TE トンネルは IPv4 を使用して作成され、OSPFv3 以外のルーティング プロトコルの使用を必要とします。OSPFv2 は IPv4 IGP として使用され、トンネルを作成するために TE が使用するデータを提供します。

OSPFv3 は自動ルート通知と Forwarding Adjacency（FA）のいずれかの TE トンネル インターフェイスで設定されます。また、ルータで終了するトンネルに TE が使用しているループバック インターフェイスのアドレスをアドバタイズするようにルータ モードで設定する必要があります。そのアドレスは、TE LSA でアドバタイズされます。

OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）の設定方法

OSPFv3 の自動ルート通知および Forwarding Adjacency の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip cef distributed**
4. **interface***type number*
5. **ip address***ip-address-mask*
6. **no shutdown**
7. **exit**
8. **interface** *type number*
9. **ospfv3** *pid af***mpls traffic-eng autoroute announce area***aid*
10. **ospfv3** *pidaf***mpls traffic-eng autoroute metric**{*metric* | **absolute** *metric*| **relative***delta*}
11. **ip ospf cost***cost*
12. **exit**
13. **interface** *type number*
14. **ospfv3** *pid af***mpls traffic-eng forwarding-adj area***aid*
15. **ospfv3**[*pid*[*af*]] **mpls traffic-eng forwarding-adj***interface ID* [**local** *ID*] [**nbr***ID*]
16. **ip ospf cost***cost*
17. **exit**
18. **router ospfv3***router-ID*
19. **address-family ipv4 unicast** [**vrf***vrf-name*]
20. **area***aid* **mpls traffic-engineering tunnel-tail***afinterface type*
21. **exit**
22. **show ospfv3 database**
23. **show ospfv3 mpls traffic-eng**

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）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# 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	**ip cef distributed** 例： `Device(config)# ip cef distributed`	分散型シスコ エクスプレス フォワーディング動作をイネーブルにします。
ステップ 4	**interface***type number* 例： `Device(config)# interface tunnel 0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip address***ip-address-mask* 例： `Device (config-if)# ip address 192.108.1.27 255.255.255.0`	指定されたインターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**no shutdown** 例： `Device (config-if)# no shutdown`	指定されたインターフェイスですべての機能をディセーブルにします。
ステップ 7	**exit** 例： `Device (config-if)# exit`	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、特権 EXEC モードに戻ります。
ステップ 8	**interface** *type number* 例： `Device (config)# interface loopback 0`	ループバック インターフェイスをイネーブルにし、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ospfv3** *pid af***mpls traffic-eng autoroute announce area***aid* 例： `Device(config-if)# ospfv3 1 af mpls traffic-eng autoroute announce area 1`	IP アドレス ファミリ（AF）があるインターフェイスで、Open Shortest Path First バージョン 3（OSPFv3）をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 10	**ospfv3** *pidaf***mpls traffic-eng autoroute metric**{*metric* | **absolute** *metric*| **relative***delta*} 例： `Device(config-if)# ospfv3 1 af mpls traffic-eng autoroute metric 1`	SPF 計算用に、MPLS トラフィック エンジニアリング自動ルート メトリック値を指定します。
ステップ 11	**ip ospf cost***cost* 例： `Device(config-if)# ip ospf cost 60`	OSPF インターフェイスでパケットを送信するコストを明示的に指定します。
ステップ 12	**exit** 例： `Device(config-if)# exit`	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、特権 EXEC モードに戻ります。
ステップ 13	**interface** *type number* 例： `Device (config)# interface tunnel 1`	トンネル インターフェイスをイネーブルにし、インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	**ospfv3** *pid af***mpls traffic-eng forwarding-adj area***aid* 例： `Device(config-if)# ospfv3 1 af mpls traffic-eng forwarding-adj area 1`	MPLS トラフィック エンジニアリング Forwarding Adjacency を設定します。
ステップ 15	**ospfv3**[*pid*[*af*]] **mpls traffic-eng forwarding-adj***interface ID* [**local** *ID*] [**nbr***ID*] 例： `Device(config-if)# ospfv3 1 af mpls traffic-eng forwarding-adj 1`	SPF 計算用に、MPLS トラフィック エンジニアリング Forwarding Adjacency を指定します。
ステップ 16	**ip ospf cost***cost* 例： `Device(config-if)# ip ospf cost 55`	OSPF インターフェイスでパケットを送信するコストを明示的に指定します。
ステップ 17	**exit** 例： `Device(config-if)# exit`	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、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 18	**router ospfv3***router-ID* 例： `Device(config)# router ospfv3 18`	OSPFv3 ルータ コンフィギュレーション モードを開始します。
ステップ 19	**address-family ipv4 unicast** [**vrf***vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast`	OSPFv3 プロセスに IPv4 アドレス ファミリを設定し、IPv4 アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 20	**area***aid* **mpls traffic-engineering tunnel-tail***afinterface type* 例： `Device(config-router-af)# area 1 mpls traffic-engineering tunnel-tail af loopback`	トラフィック エンジニアリング トンネルのテール エンドに OSPFv3 を設定します。
ステップ 21	**exit** 例： `Device(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 22	**show ospfv3 database** 例： `Device(config)# show ospfv3 database`	（任意）特定のルータの OSPFv3 データベースに関する情報のリストを表示します。
ステップ 23	**show ospfv3 mpls traffic-eng** 例： `Device(config)# show ospfv3 mpls traffic-eng`	（任意）自動ルート通知、Forwarding Adjacency、および OSPFv3 に関するトンネルテール情報を表示します。

OSPFv3 の自動ルート通知および Forwarding Adjacency の設定例

例：OSPFv3 の自動ルート通知および Forwarding Adjacency の設定

```
!
ip cef distributed
interface tunnel 0
```

```
 ip address 192.108.1.27 255.255.255.0
 no shutdown

interface loopback 0
 ospfv3 1 af mpls traffic-eng autoroute announce area 1
 ospfv3 1 af mpls traffic-eng autoroute metric 1
 ip ospf cost 60

interface tunnel 1
 ospfv3 1 af mpls traffic-eng forwarding-adj area 1
 ospfv3 1 af mpls traffic-eng forwarding-adj nbr 1
 ip ospf cost 55

router ospfv3 18
 address-family ipv4 unicast
   area 1 mpls traffic-engineering tunnel-tail af loopback

   !
  !
!
```

OSPFv3 の自動ルート通知および Forwarding Adjacency に関する追加情報

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 Command List, All Releases』
OSPF 機能の設定	IP ルーティング：OSPF コンフィギュレーション ガイド

標準および RFC

関連項目	マニュアル タイトル
ローカル アドレスの OSPF トラフィック エンジニアリング（TE）へのアドバタイズの拡張	RFC5786
OSPF バージョン 3 へのトラフィック エンジニアリングの拡張	RFC5329
『Traffic Engineering (TE) Extensions to OSPF Version 2』	RFC3630

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

OSPFv3 の自動ルート通知および Forwarding Adjacency の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *20*：*OSPFv3* の自動ルート通知および *Forwarding Adjacency* の機能情報

機能名	リリース	機能情報
OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）	Cisco IOS XE リリース 3.12S	OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）機能は、MPLS/TE IPv4 トンネルを介して IPv6 ルートをアドバタイズします。 次のコマンドが導入または変更されました。**ospfv3 af mpls traffic-eng autoroute announce area**、**ospfv3 mpls traffic-eng autoroute metric**、**ospfv3 mpls traffic-eng forwarding-adj area**

第 18 章

OSPFv3 自動ルート除外

OSPFv3 自動ルート除外機能では、特定の接続先とプレフィックス リストを使用して、パケット転送に TE トンネルではなくネイティブ パスを使用してルーティングされるプレフィックスのリストを指定できます。その他のプレフィックスでは TE トンネルを使用するように設定できます。除外されるプレフィックスは、TE トンネル パスを使用しません。TE トンネルを介した IPv6 ルートは、自動ルート通知（AA）または Forwarding Adjacency（FA）を使用する OSPFv3 によってサポートされます。

ここでは、OSPFv3 自動ルート除外機能の設定方法について説明します。

- 機能情報の確認，227 ページ
- OSPFv3 自動ルート除外の前提条件，228 ページ
- OSPFv3 自動ルート除外について，228 ページ
- OSPFv3 自動ルート除外の設定方法，229 ページ
- OSPFv3 自動ルート除外の設定例，230 ページ
- OSPFv3 自動ルート除外に関する追加情報，230 ページ
- OSPFv3 自動ルート除外の機能情報，231 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。

OSPFv3 自動ルート除外の前提条件

- Open Shortest Path First（OSPF）がネットワークで設定されている。
- シスコ エクスプレス フォワーディング（CEF）がイネーブルになっている。
- マルチプロトコル ラベル スイッチング（MPLS）TE トンネルが設定されている。
- 自動ルート通知と Forwarding Adjacency（FA）が設定されている。インターフェイスでは自動ルート通知と Forwarding Adjacency（FA）のいずれかを設定できます。同じインターフェイスに両方を設定することはできません。

OSPFv3 自動ルート除外について

OSPFv3 自動ルート除外の概要

自動ルート機能は、OSPF が IP トラフィック ルートのパスを作成するために MPLS TE トンネルを使用することを強制する IP ルーティング方法です。自動ルート機能を使用すると、そのルートに使用可能な代替の非 TE パスがある場合でも、すべてのルートで TE トンネルを使用することができます。

OSPFv3 自動ルート除外機能では、特定の IPv6 接続先またはプレフィックスで TE トンネルを回避して、他のプレフィックスでは依然として TE トンネルを使用するように設定することができます。除外されるプレフィックスは、TE トンネル パスを使用しません。ネイティブの非 TE パスだけがこのようなルートについて RIB にダウンロードされます。TE トンネルを介した IPv6 ルートは、自動ルート通知（AA）または Forwarding Adjacency（FA）を使用する OSPFv3 によってサポートされます。

自動ルート除外オプションは、プレフィックス リストを使用してルータ OSPF コンフィギュレーション モードで設定されます。このプレフィックス リストのメンバである IP アドレスおよびプレフィックスは、自動ルートがイネーブルになっていても TE トンネルから除外されます。IP アドレスまたはプレフィックスがプレフィックス リストに追加される場合、TE トンネルを通過せずに動的にルーティングされます。IP アドレスまたはプレフィックスがプレフィックス リストから削除される場合、TE トンネル パスで動的に再ルーティングされるようになります。

OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）の設定の詳細については、『*IP Routing: OSPF Configuration Guide*』の「Autoroute Announce and Forwarding Adjacencies For OSPFv3」を参照してください。

OSPFv3 自動ルート除外の設定方法

OSPFv3 自動ルート除外の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router ospfv3***process-ID*
4. **address-familyipv6 unicast**
5. **mpls traffic-engineeringautoroute-excludeprefix-list** *prefix-list-name*
6. **end**

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	**configure terminal** 例： `Device# 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	**router ospfv3***process-ID* 例： `Device(config)# router ospfv3 18`	OSPFv3 ルーティング プロセスを設定し、OSPF ルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-familyipv6 unicast** 例： `Device(config-router)# address-family ipv6 unicast`	OSPFv3 の IPv6 アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**mpls traffic-engineeringautoroute-excludeprefix-list** *prefix-list-name* 例： `Device(config-router-af)# mpls traffic-engineering autoroute-exclude prefix-list kmd`	特定の宛先およびプレフィックスを、TE トンネルによるルーティングを回避するように指定できます。 • 除外されるプレフィックスは、TE トンネル パスを使用しません。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

OSPFv3 自動ルート除外の設定例

例：OSPFv3 自動ルート除外の設定

```
!
router ospfv3 18
 address-family ipv6 unicast
  mpls traffic-engineering autoroute-exclude prefix-list kmd

!
```

OSPFv3 自動ルート除外に関する追加情報

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 Command List, All Releases』
『Configuring OSPF』	*IP* ルーティング：*OSPF* コンフィギュレーション ガイド
OSPFv3 の自動ルート通知と Forwarding Adjacency（FA）	*IP* ルーティング：*OSPF* コンフィギュレーション ガイド
基本的なシスコ エクスプレス フォワーディングの設定	『*IP Switching: Cisco Express Forwarding Configuration Guide*』

関連項目	マニュアル タイトル
MPLS トラフィック エンジニアリング トンネル ソース	『*MPLS Traffic Engineering Path Calculation and Setup Configuration Guide*』

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

OSPFv3 自動ルート除外の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *21*：*OSPFv3* 自動ルート除外の機能情報

機能名	リリース	機能情報
OSPFv3 自動ルート除外	Cisco IOS XE 3.14S	OSPFv3 自動ルート除外機能では、特定の接続先とプレフィックスリストを使用して、パケット転送に TE トンネルではなくネイティブパスを使用してルーティングされるプレフィックスのリストを指定できます。OSPFv3 による TE トンネル上での IPv6 ルーティングは、自動ルート通知および Forwarding Adjacency を使用してサポートされます。 次のコマンドが導入または変更されました。**mpls traffic-engineering autoroute-exclude prefix list**

第 19 章

OSPFv2 IP FRR ローカル マイクロループ回避

OSPFv2 IP FRR ローカル マイクロループ回避機能では、リンクダウン イベントが発生したノードとネイバー間でのローカル マイクロループの発生を回避することができます。このドキュメントでは、OSPFv2 IP FRR ローカル マイクロループ回避機能を設定する方法について説明します。

- 機能情報の確認，233 ページ
- OSPFv2 IP FRR ローカル マイクロループ回避について，234 ページ
- OSPFv2 IP FRR ローカル マイクロループ回避の設定方法，235 ページ
- OSPFv2 IP FRR ローカル マイクロループ回避の設定例，236 ページ
- OSPFv2 IP FRR ローカル マイクロループ回避に関する追加情報，236 ページ
- OSPFv2 IP FRR ローカル マイクロループ回避の機能情報，237 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。

OSPFv2 IP FRR ローカル マイクロループ回避について

OSPFv2 IP FRR ローカル マイクロループ回避の概要

IP Fast Reroute（IPFRR）では、通常のコンバージェンス メカニズムがコンバージェンス後のパスと見なされる新たに見つかったベスト パスにトラフィックを転送するまで、事前に計算されたバックアップパスにトラフィックを転送することによってリンクダウンイベント時に高速なコンバージェンスを提供します。

トラフィックがコンバージェンス後のパスに転送されると、マイクロループになる傾向があります。マイクロループは、パス上の各ノードが異なる時間に他のノードと無関係に計算を行う結果として形成されます。特定のノードがコンバージして、まだコンバージしていないネイバー ノードにトラフィックを送信する場合、トラフィックはこれらの 2 つのノードの間でループする可能性があります。

マイクロループは障害が検出されたルータとそのルータの間で形成されます。ローカル マイクロループは、リングまたは四角型トポロジで使用可能なローカル Loop-Free Alternate（LFA）バックアップがない場合に作成されます。このようなトポロジでは、リモート LFA はバックアップを提供しますが、高確率でローカルマイクロループが作成されるため、リモート LFA の高速コンバージェンスの利点を完全に活用することができません。ローカルマイクロ ループを回避すると、リングまたは四角型トポロジの高速コンバージェンスが大幅に改善されます。

（注） マイクロループ回避は、リモート LFA（rLFA）がイネーブルになるとすぐに自動的にイネーブルになります。

（フォワーディング プレーンに修復パスがインストールされている）プレフィックスにマイクロループ回避を使用しているとき、フォワーディング プレーンがトリガーされて事前にインストールされていた修復パスを使用するように切り替わると、OSPFv2 IP FRR ローカル マイクロループ回避機能がイネーブルになります。リンクダウンイベントのローカルマイクロループ回避では、次のトリガーをサポートします。

- インターフェイス ダウン イベント。
- 双方向フォワーディング検出（BFD）セッションのダウンによる隣接関係ダウンイベント。

フォワーディング プレーンに修復パスがインストールされているかどうかに関係なくマイクロループ回避を使用する場合は、加えて 3 番目のトリガーが使用されます。

- ネイバーの保留時間の期限切れによる隣接関係ダウン イベント。

ネイバーがリンクステート ネイバー アドバタイズメントで隣接関係の喪失をローカル システムに報告するとき、マイクロループ回避を使用する価値は、ネイバーの隣接関係の喪失を生じさせたリモート イベントがローカルのフォワーディング プレーンによって検出可能かどうか（つま

り、フォワーディング プレーンが反応して事前にプログラムされた修復パスの使用に切り替わるかどうか）に依存します。

OSPFv2 IP FRR ローカル マイクロループ回避の設定方法

OSPFv2 IP FRR ローカル マイクロループの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router ospf** *process-id*
4. **microloop avoidance** [**protected** | **disable**]
5. **microloop avoidance rib-update-delay** *delay-period*
6. **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： `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	**configure terminal** 例： `Device# 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	**router ospf** *process-id* 例： `Device(config)# router ospf 109`	OSPF ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**microloop avoidance** [**protected**	**disable**] 例： `Device(config-router)# microloop avoidance protected`	ノードとリンクダウンイベントが発生したそのネイバーとの間に、ローカル マイクロループ回避を設定します。 • **protected** キーワードを使用した場合、ローカルマイクロループ回避は有効なバックアップ パスを含むプレフィックスにのみ適用されます。 • **disable** キーワードを使用した場合、事前に自動的にイネーブルされていたローカルマイクロループ回避はディセーブルになります。

	コマンドまたはアクション	目的
ステップ 5	**microloop avoidance rib-update-delay** *delay-period* 例： `Device(config-router)# microloop avoidance rib-update-delay 6500`	設定した遅延期間に従い、ローカル マイクロループ回避を待機させます。
ステップ 6	**exit** 例： `Device(config-router)# exit`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

OSPFv2 IP FRR ローカル マイクロループ回避の設定例

例：OSPFv2 IP FRR ローカル マイクロループの設定

```
router ospf 10
 microloop avoidance protected
microloop avoidance rib-update-delay 6500
!
```

OSPFv2 IP FRR ローカル マイクロループ回避に関する追加情報

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 Command List, All Releases』
OSPF 機能の設定	IP ルーティング：OSPF コンフィギュレーション ガイド

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

OSPFv2 IP FRR ローカル マイクロループ回避の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *22*：*OSPFv2 IP FRR* ローカル マイクロループ回避の機能情報

機能名	リリース	機能情報
OSPFv2 IP FRR ローカル マイクロループ回避	Cisco IOS XE Release 3.11S 15.4(1)S	OSPFv2 IP FRR ローカル マイクロループ回避機能では、リンクダウンイベントが発生したノードとネイバー間でのローカル マイクロループの発生を回避することができます。 次のコマンドが導入または変更されました。**microloop avoidance**、**microloop avoidance rib-update-delay**

第 20 章

OSPFv2-OSPF Live-Live

OSPFv2-OSPF Live-Live 機能では、オーバーラップしないパスを経由してさまざまなアプリケーションにマルチキャスト ストリームを配信します。マルチキャスト トラフィックは保護されたネットワークの始めで複数のストリームに分割されます。あるパスでリンク障害が発生してもマルチキャスト トラフィックが他のパスを通じて配信されるように、すべてのストリームがオーバーラップしないパスを経由して流れます。すべてのストリームは保護されたネットワークの最後でマージされます。ここでは、OSPFv2-OSPF Live-Live 機能の設定方法について説明します。

- 機能情報の確認，239 ページ
- OSPFv2-OSPF Live-Live に関する情報，240 ページ
- OSPFv2-OSPF Live-Live の設定方法，241 ページ
- OSPFv2-OSPF Live-Live の設定例，245 ページ
- OSPFv2-OSPF Live-Live に関する追加情報，246 ページ
- OSPFv2-OSPF Live-Live の機能情報，246 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。

OSPFv2-OSPF Live-Live に関する情報

OSPFv2-OSPF Live-Live の概要

ネットワーキング市場の成長を促進する多くの新しいアプリケーションはマルチキャスト ベースです。インターネット プロトコル テレビジョン（IPTV）などのアプリケーションは通常、同時に多数の視聴者に膨大な量のセンシティブデータ ストリームを配信することが伴います。パケット ドロップはマルチメディア トラフィックでは重大な問題となります。ミリ秒の範囲まで、またはパケット損失ゼロまでマルチキャスト トラフィックの損失を減らす必要があります。単一のリンク障害発生時にマルチキャストのパケット損失がゼロのソリューションは、live-live とも呼ばれます。

live-live ネットワークでは、マルチキャスト ストリーム（通常は 2 つのフロー）は分散された物理リンクを介して独自のリバース パス フォワーディング（RPF）または最短パス ツリー（SPT）を形成し、1 つのリンクでの障害が他のリンクのマルチキャスト トラフィックに影響しないようにします。Cisco IOS ソフトウェアの既存のマルチ トポロジテクノロジーでは、複数のマルチキャスト トポロジをサポートします。

OSPFv2-OSPF Live-Live 機能を使用すると、Protocol Independent Multicast（PIM）で複数のマルチキャスト トポロジを処理できます。マルチキャスト トポロジが作成されて OSPF でイネーブルになると、各トポロジの IP プレフィックスがトポロジベースのルーティング情報ベース（RIB）に挿入されます。次に、PIM が RPF ルックアップに使用する RIB を決定します。

PIM RPF トポロジは、共有ツリーまたは送信元ツリーの作成時に RPF 操作を実行するために PIM によって使用されるルートの集合です。マルチ トポロジ環境では、複数の RPF トポロジを同一ネットワークに作成できます。特定の送信元には、トポロジの 1 つのみ、または異なるパスを経由する複数のトポロジで到達できる可能性があります。

特定のマルチキャスト配信ツリーに RPF トポロジを選択するには、次の点を考慮してください。

1. トポロジにグループの範囲をマッピングするポリシーを設定します。範囲内のグループの RP または送信元について RPF 情報を解決する必要があるとき、RPF ルックアップは指定されたトポロジで行われます。これは、PIM スパース モード（PIM-SM）、Source-Specific Multicast（SSM）、または双方向（Bidir）PIM に使用できます。
2. トポロジに送信元のプレフィックス範囲をマッピングするポリシーを設定します。これは、PIM-SM および PIM-SSM に使用できます。
3. 受信した PIM パケットの Join Attribute エンコーディングによって識別されるトポロジを使用します。

PIM Join Attribute は PIM シグナリングを拡張し、特定のマルチキャスト配信ツリーを構築するときに使用する必要があるトポロジを識別します。PIM Join Attribute の詳細については、IEEE ドラフト「PIM Multi-Topology ID (MT-ID) Join-Attribute」を参照してください。

OSPFv2-OSPF Live-Live の設定方法

OSPFv2-OSPF Live-Live の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip multicast-routing**
4. **ip multicast rpf multitopology**
5. **global-address-family ipv4 multicast**
6. **topology** {*topology-A* | *topology-B*}
7. **exit**
8. **interface***type number*
9. **ip address***address mask*
10. **ip pim sparse-dense-mode**
11. **ip ospf***process-id***area***area-id*
12. **topology ipv4 multicast***topology-name*
13. **exit**
14. **router ospf***process-id*
15. **network***ip-adddress mask***area***area-id*
16. **address-family ipv4 multicast**
17. **topology** *topology-name***tid***topology-id*
18. **end**
19. **configure terminal**
20. **ip multicast topology multicast***topology-name***tid***topology-id*
21. **ip multicast rpf select topology multicast***topology-nameaccess-list number*
22. **ip access-list extended***access-list-number*
23. **permit ip any***ip-adddress*
24. **end**
25. **show ip multicast topology multicast***topology-name*
26. **debug ip multicast 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： `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	**configure terminal** 例： `Device# 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	**ip multicast-routing** 例： `Device(config)# ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。
ステップ 4	**ip multicast rpf multitopology** 例： `Device(config)# ip multicast rpf multitopology`	IP マルチキャスト ルーティングに対するのマルチトポロジ ルーティング（MTR）サポートをイネーブルにします。
ステップ 5	**global-address-family ipv4 multicast** 例： `Device(config)# global-address-family ipv4 multicast`	グローバル アドレス ファミリ コンフィギュレーション モードを開始してマルチトポロジ ルーティングを設定します。
ステップ 6	**topology** {*topology-A* | *topology-B*} 例： `Device(config-af)# topology live-A`	指定したトポロジ インスタンスで IP トラフィックをルーティングするよう OSPF プロセスを設定します。
ステップ 7	**exit** 例： `Device(config-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface***type number* 例： `Device(config)# interface Gigabitethernet 1/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ip address***address mask* 例： `Device(config-if)# ip address 192.108.1.27 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 10	**ip pim sparse-dense-mode** 例： `Device(config-if)# ip pim sparse-dense-mode`	インターフェイスでPIMをイネーブルにし、マルチキャスト グループの動作モードに応じて、インターフェイスをsparse（スパース）モード動作またはdense（デンス）モード動作で処理します。
ステップ 11	**ip ospf***process-id***area***area-id* 例： `Device(config-if)# ip ospf 10 area 0`	インターフェイスに対してOSPFv2 をイネーブルにします。
ステップ 12	**topology ipv4 multicast***topology-name* 例： `Device(config-if)# topology ipv4 multicast live-A`	インターフェイス上でマルチトポロジインスタンスを設定します。
ステップ 13	**exit** 例： `Device(config-if)# exit`	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、グローバル コンフィギュレーション モードに入ります。 • ステップ 9 ～ 12 を繰り返して、次のトポロジ（**topology ipv4 multicast live-B**）を設定します。
ステップ 14	**router ospf***process-id* 例： `Device(config)# router ospf 102`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。
ステップ 15	**network***ip-adddress mask***area***area-id* 例： `Device(config-router)# network 192.168.129.16 0.0.0.3 area 20`	OSPFを実行するインターフェイスを定義し、そのインターフェイスに対するエリア ID を定義します。
ステップ 16	**address-family ipv4 multicast** 例： `Device(config-router)# address-family ipv4 multicast`	ルータ アドレス ファミリ コンフィギュレーション モードを開始し、IPv4 マルチキャスト プレフィックスを交換するよう OSPF を設定します。
ステップ 17	**topology** *topology-name***tid***topology-id* 例： `Device(config-router-af)# topology live-A tid 100`	指定したトポロジ インスタンスで IP トラフィックをルーティングするよう OSPF プロセスを設定します。 • このステップを繰り返して、OSPF プロセスが別のトポロジ インスタンス（**topology live-B tid 200**）で IP トラフィックをルーティングするよう設定します。

	コマンドまたはアクション	目的
ステップ 18	**end** 例： `Device(config-router-af)# end`	ルータ アドレス ファミリ 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 19	**configure terminal** 例： `Device# 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 20	**ip multicast topology multicast***topology-name***tid***topology-id* 例： `Device(config)# ip multicast topology multicast live-A tid 100`	マルチキャスト ストリーム用のトポロジ選択を設定します。 • このステップを繰り返して、別のトポロジ（**ip multicast topology multicast live-B tid 200**）を設定します。
ステップ 21	**ip multicast rpf select topology multicast***topology-nameaccess-list number* 例： `Device(config)# ip multicast rpf select topology multicast topology live-A 111`	マルチキャスト トポロジを、特定のルート エントリを含むマルチキャスト グループに関連付けます。 • このステップを繰り返して、トポロジを別のマルチキャスト グループ（**ip multicast rpf select topology multicast live-B 122**）に関連付けます。
ステップ 22	**ip access-list extended***access-list-number* 例： `Device(config)# ip access-list extended 111`	IP アクセス リストを定義して、IP ヘルパー アドレス宛先によるパケットのフィルタリングをイネーブルにし、拡張名前付きアクセス リスト コンフィギュレーション モードを開始します。
ステップ 23	**permit ip any***ip-adddress* 例： `Device(config-ext-nacl)# permit ip any 203.0.113.1`	パケットが名前付き IP アクセス リストを通過できる条件を設定します。 • ステップ 22 および 23 を繰り返して、別の IP アクセス リストを定義し、パケットが別の名前付き IP アクセス リストを通過できる条件を設定します。
ステップ 24	**end** 例： `Device(config-ext-nacl)# end`	拡張名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 25	**show ip multicast topology multicast***topology-name* 例： `Device# show ip multicast topology multicast live-A`	マルチキャスト ストリームのトポロジ情報を表示します。

	コマンドまたはアクション	目的
ステップ 26	**debug ip multicast topology** 例： `Device# debug ip multicast topology`	マルチキャスト ストリーム トポロジの出力のデバッグをイネーブルにします。

OSPFv2-OSPF Live-Live の設定例

例：OSPFv2-OSPF Live-Live の設定

```
ip multicast-routing
!
ip multicast rpf multitopology

!
global-address-family ipv4 multicast
  topology live-A
  topology live-B

int gigabitethernet 1/0
 ip address 192.0.2.1 255.255.255.0
 ip pim sparse-dense-mode
 ip ospf 10 area 20
 topology ipv4 multicast live-A
!
int gigabitethernet 2/0
 ip address 192.0.2.2 255.255.255.0
 ip pim sparse-dense-mode
 ip ospf 11 area 21
 topology ipv4 multicast live-B
!
router ospf 1
 network 192.168.129.16 0.0.0.3 area 20
  address-family ipv4 multicast
  !!
   topology live-A tid 10
   topology live-B tid 20
!
!!
ip multicast topology multicast live-A tid 100
ip multicast topology multicast live-B tid 200
!
!!
ip multicast rpf select topology multicast live-A 111
ip multicast rpf select topology multicast live-B 122

!
 ip access-list extended 111
 permit ip any 203.0.113.254

ip access-list extended 122
 permit ip any 203.0.113.251
```

OSPFv2-OSPF Live-Live に関する追加情報

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 Command List, All Releases』
OSPF 機能の設定	IP ルーティング：OSPF コンフィギュレーション ガイド

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

OSPFv2-OSPF Live-Live の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *23* : *OSPFv2-OSPF Live-Live* の機能情報

機能名	リリース	機能情報
OSPFv2-OSPF Live-Live	Cisco IOS XE Release 3.11S	OSPFv2-OSPF Live-Live 機能では、オーバーラップしないパスを経由してさまざまなアプリケーションにマルチキャストストリームを配信します。マルチキャスト トラフィックは保護されたネットワークの始めで複数のストリームに分割されます。あるパスでリンク障害が発生してもマルチキャスト トラフィックが他のパスを通じて配信されるように、すべてのストリームがオーバーラップしないパスを経由して流れます。すべてのストリームは保護されたネットワークの最後でマージされます。 追加または変更されたコマンドはありません。

第 21 章

変換後のタイプ 5 LSA での OSPF フォワーディング アドレス抑制

変換後のタイプ 5 LSA での OSPF フォワーディング アドレス抑制機能では、Not-So-Stubby Area（NSSA）エリア境界ルータ（ABR）がタイプ 7 リンクステート アドバタイズメント（LSA）をタイプ 5 LSA に変換します。ただし、フォワーディング アドレスとして、タイプ 7 LSA で指定されたものではなく 0.0.0.0 が使用されます。この機能を使用すると、フォワーディング アドレスをバックボーンにアドバタイズしないよう設定されているデバイスが、転送されたトラフィックを、変換を行う NSSA ABR に渡すようになります。

- 機能情報の確認，249 ページ
- OSPF フォワーディング アドレス抑制の前提条件，250 ページ
- OSPF フォワーディング アドレス抑制に関する情報，250 ページ
- OSPF フォワーディング アドレスを抑制する方法，252 ページ
- OSPF フォワーディング アドレス抑制の設定例，253 ページ
- その他の参考資料，253 ページ
- OSPF フォワーディング アドレス抑制の機能情報，255 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。

OSPF フォワーディング アドレス抑制の前提条件

このマニュアルは、OSPF がネットワーキング デバイス上で設定されていることを前提としています。OSPF の設定手順は記載されていません。

OSPF フォワーディング アドレス抑制に関する情報

OSPF フォワーディング アドレス抑制の利点

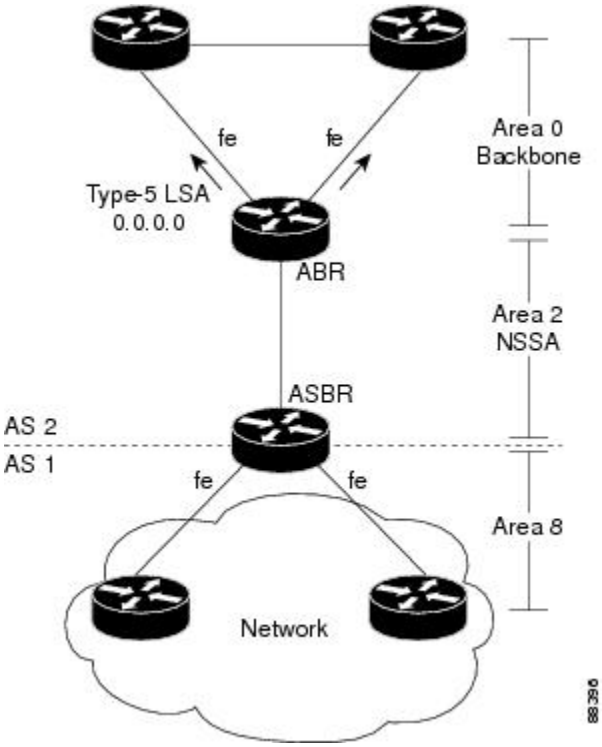
変換後のタイプ 5 LSA での OSPF フォワーディング アドレス抑制機能では、NSSA ABR でタイプ 7 LSA がタイプ 5 LSA に変換されます。ただし、フォワーディング アドレスとして、タイプ 7 LSA で指定されたものではなく 0.0.0.0 が使用されます。この機能を使用すると、フォワーディング アドレスをバックボーンにアドバタイズしないよう設定されているデバイスが、転送されたトラフィックを、変換を行う NSSA ASBR に渡すようになります。

変換後のタイプ 5 LSA で OSPF フォワーディング アドレスを抑制する場合

下の図では、バックボーン（エリア 0）に導入されるルートの数を最小に抑えるため、エリア 0 からエリア 2 のアドレスをフィルタリングすることが有効です。ただし、**arearange** コマンドでエリア境界（エリア 2 のアドレスをフィルタリング）でルートを統合および要約しようとしても、エリア 2 アドレスに ASBR で生成されたタイプ 7 LSA 用のフォワーディング アドレスが含まれるため、機能しません。これらのタイプ 7 LSA フォワーディング アドレスがエリア 0 でフィルタリ

ングされていると、バックボーン ルータは変換元のタイプ 5 LSA（自律システム外部 LSA）でアドバタイズされるプレフィックスに到達できません。

図 *9*：変換後のタイプ *5 LSA* での *OSPF* フォワーディング アドレス抑制



この問題は、フォワーディング アドレスを ABR で抑制し、タイプ 7 LSA から変換されたタイプ 5 LSA でフォワーディング アドレスを 0.0.0.0 に設定することで解決します。フォワーディング アドレスを 0.0.0.0 に設定すると、外部宛先のパケットを、アドバタイズ先の OSPF デバイス（ここでは変換先の NSSA ABR）に転送する必要があることが示されます。

この機能を設定するには、次の点に注意してください。

注意 この機能を設定すると、デバイスが RFC 1587 に準拠しなくなります。また、宛先のフォワーディング アドレスに到達するためのさらによいパスが存在する可能性があるため、次善ルーティングとなる可能性があります。この機能は、慎重に検討し、ネットワーク トポロジを理解するまでは設定しないことを推奨します。

OSPF フォワーディング アドレスを抑制する方法

変換後のタイプ 5 LSA での OSPF フォワーディング アドレスの抑制

このタスクでは、変換後のタイプ 5 LSA で OSPF フォワーディング アドレスを抑制する手順について説明します。この機能を設定するには、次の点に注意してください。

注意 この機能を設定すると、デバイスが RFC 1587 に準拠しなくなります。また、宛先のフォワーディング アドレスに到達するためのさらによいパスが存在する可能性があるため、次善ルーティングとなる可能性があります。この機能は、慎重に検討し、ネットワーク トポロジを理解するまでは設定しないことを推奨します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id*
4. **area***area-id***nssatranslatetype7suppress-fa**
5. **end**

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 モードなど、高位の権限レベル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： `Device# 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	**routerospf***process-id* 例： `Device(config)# router ospf 1`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。 • *process-id* 引数は OSPF プロセスを示します。

	コマンドまたはアクション	目的
ステップ 4	**area***area-id***nssatranslatetype7suppress-fa** 例： `Device(config-router)# area 10 nssa translate type7 suppress-fa`	エリアを Not-So-Stubby-Area（NSSA）として設定し、変換後のタイプ 7 LSA でフォワーディング アドレスを抑制します。
ステップ 5	**end** 例： `Device(config-router)# end`	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。

OSPF フォワーディング アドレス抑制の設定例

変換後のタイプ 5 LSA での OSPF フォワーディング アドレスの抑制：例

この例では、変換後のタイプ 5 LSA でフォワーディング アドレスを抑制しています。

```
interface gigabitethernet 0/0/0
 ip address 10.93.1.1 255.255.255.0
 ip ospf cost 1
!
interface gigabitethernet 0/01
 ip address 10.94.1.1 255.255.255.0
!
router ospf 1
 network 10.93.0.0 0.0.255.255 area 0.0.0.0
 network 10.94.0.0 0.0.255.255 area 10
 area 10 nssa translate type7 suppress-fa
```

その他の参考資料

ここでは、変換後のタイプ 5 LSA での OSPF フォワーディング アドレスの抑制に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』

関連項目	マニュアル タイトル
『Configuring OSPF』	『Configuring OSPF』
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』
OSPFv3 アドレス ファミリ	*OSPFv3 Address Families* モジュール

標準

規格	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 1587	『*The OSPF NSSA Option*』 （注） 変換後のタイプ 5 LSA での OSPF フォワーディング アドレス抑制機能を設定すると、ルータが RFC 1587 に準拠しなくなります。『*The OSPF NSSA Option*』

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

OSPF フォワーディング アドレス抑制の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *24*：変換後のタイプ *5 LSA* での *OSPF* フォワーディング アドレス抑制の機能情報

機能名	リリース	機能情報
変換後のタイプ 5 LSA での OSPF フォワーディング アドレス抑制	Cisco IOS XE Release 2.1	変換後のタイプ 5 LSA での OSPF フォワーディング アドレス抑制機能では、Not-So-Stubby Area（NSSA）エリア境界ルータ（ABR）がタイプ 7 リンクステート アドバタイズメント（LSA）をタイプ 5 LSA に変換します。ただし、フォワーディング アドレスとして、タイプ 7 LSA で指定されたものではなく 0.0.0.0 が使用されます。この機能を使用すると、フォワーディングアドレスをバックボーンにアドバタイズしないよう設定されているルータが、転送されたトラフィックを、変換を行う NSSA ABR に渡すようになります。 次に示すコマンドは、この章に記載されている機能において、新たに導入または変更されたものです。 • **areanssatranslate** • **showipospf**

第 22 章

配布リスト付きのルートマップによるOSPFインバウンド フィルタリング

配布リスト付きのルート マップによる OSPF インバウンド フィルタリング機能を使用すると、ユーザはルート マップを定義して、ルーティング テーブルへの Open Shortest Path First（OSPF）ルートの追加を防止できます。そのルートマップでは、ユーザはOSPFルートのすべての属性と適合することができます。

- 機能情報の確認，257 ページ
- 配布リスト付きのルート マップによる OSPF インバウンド フィルタリングの前提条件，258 ページ
- 配布リスト付きのルート マップによる OSPF インバウンド フィルタリングについて，258 ページ
- ルート マップを使用した OSPF インバウンド フィルタリングの設定方法，259 ページ
- 配布リスト付きのルート マップによる OSPF インバウンド フィルタリングの設定例，261 ページ
- その他の参考資料，261 ページ
- 配布リスト付きのルート マップによる OSPF インバウンド フィルタリングの機能情報，263 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。

配布リスト付きのルート マップによる OSPF インバウンド フィルタリングの前提条件

ご使用のネットワークで OSPF が設定されていることが前提になります。

配布リスト付きのルート マップによる OSPF インバウンド フィルタリングについて

OSPF ルートマップベースフィルタリングの利点

ユーザはルート マップを定義して、ルーティング テーブルへの OSPF ルートの追加を防止できます。このフィルタリングは、OSPF がルーティング テーブルにルートをインストールするときに行われます。この機能は、LSA のフラッディングに影響を与えません。そのルート マップでは、ユーザは OSPF ルートのすべての属性と適合することができます。ルート マップは、次の **match** オプションに基づいています。

- **matchinterface**
- **matchipaddress**
- **matchipnext-hop**
- **matchiproute-source**
- **matchmetric**
- **matchroute-type**
- **matchtag**

この機能は、ASBR でプレフィックスが再配布されるとき、ユーザがこのプレフィックスにタグを付け、その後このタグで、プレフィックスを他のルータのルーティング テーブルにインストールしないようにフィルタリングする場合に有効です。

ルート タグに基づいたフィルタリング

ユーザは外部ルートが OSPF に再配布される際にタグの割り当てができます。次に、**route-map** および **distribute-list in** コマンドでそのタグを識別することにより、OSPF ドメインで外部ルートを許可または拒否できます。

ルート タイプに基づいたフィルタリング

OSPF では、外部ルートはタイプ 1 またはタイプ 2 のいずれかとなります。ユーザはルート マップを作成し、タイプ 1 またはタイプ 2 のいずれかと照合して **distribute-list in** コマンドを使用して特定のプレフィックスをフィルタリングします。また、ルート マップは内部ルート（エリア内とエリア間）も識別し、内部ルートもフィルタリングできます。

ルート ソースに基づいたフィルタリング

ルート ソースで照合が終わると、ルート ソースはプレフィックスがアドバタイズされる LSA 発信者の OSPF ルータ ID を示します。

インターフェイスに基づいたフィルタリング

インターフェイスで照合が終わると、インターフェイスは OSPF がルーティング テーブルでインストールしようとしているルートの発信インターフェイスを示します。

ネクストホップに基づいたフィルタリング

ネクスト ホップで照合が終わると、ネクスト ホップは OSPF がルーティング テーブルでインストールしようとしているルートのネクスト ホップを示します。

ルート マップを使用した OSPF インバウンド フィルタリングの設定方法

ルート マップによる OSPF インバウンド フィルタリングの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **route-map***map-tag*[**permit** | **deny**] [*sequence-number*]
4. **matchtag***tag-name*
5. **route-map** および **match** コマンドを使用して、ステップ 3 と 4 を繰り返します。
6. **exit**
7. **routerospf***process-id*
8. **distribute-listroute-map***map-tag***in**
9. **end**

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	**route-map***map-tag*[**permit** | **deny**] [*sequence-number*] 例： `Router(config)# route-map tag-filter deny 10`	フィルタリングを制御するルートマップを定義します。

ステップ 4	**matchtag***tag-name*
	
	例：
	
	例：
	`or other match commands`
	
	例：
	`Router(config-router)# match tag 777`
		ルートと、ルート マップの参照対象として使用される指定名を照合します。
		• 少なくとも 1 つの **match** コマンドが必要ですが、この例の **match** コマンドである必要はありません。これはあくまでも一例です。
		• このタイプのルート マップで使用できる **match** コマンドのリストが **distribute-list in** コマンド リファレンスのページに示されています。
		• このタイプのルート マップには **set** コマンドがありません。

ステップ 5	**route-map** および **match** コマンドを使用して、ステップ 3 と 4 を繰り返します。	--
ステップ 6	**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 7	**routerospf***process-id* 例： `Router(config)# router ospf 1`	OSPF 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 8	**distribute-listroute-map***map-tag***in** 例： `Router(config-router)# distribute-list route-map tag-filter in`	OSPF ルートマップに基づいたフィルタリングをイネーブルにします。
ステップ 9	**end** 例： `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了します。

配布リスト付きのルート マップによる OSPF インバウンド フィルタリングの設定例

例：OSPF ルート マップ ベースのフィルタリング

この例では、OSPF 外部 LSA にはタグが存在します。タグの値は、プレフィックスがルーティング テーブルにインストールされる前に検査されます。値が 777 の OSPF 外部プレフィックスは、すべてフィルタリングされます（ルーティング テーブルにインストールされません）。シーケンス番号 20 の permit ステートメントには照合条件がありません。シーケンス番号 20 の後には他の route-map ステートメントがないため、他のすべての条件が許可されます。

```
route-map tag-filter deny 10
 match tag 777
route-map tag-filter permit 20
!
router ospf 1
 router-id 10.0.0.2
 log-adjacency-changes
 network 172.16.2.1 0.0.0.255 area 0
 distribute-list route-map tag-filter in
```

その他の参考資料

ここでは、配布リスト付きのルート マップによる OSPF インバウンド フィルタリングの設定に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
『Configuring OSPF』	『Configuring OSPF』
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』

標準

規格	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

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

配布リスト付きのルート マップによる OSPF インバウンド フィルタリングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *25*：配布リスト付きのルート マップによる *OSPF* インバウンド フィルタリングの機能情報

機能名	リリース	機能情報
配布リスト付きのルート マップによる OSPF インバウンド フィルタリング	Cisco IOS XE Release 2.1	配布リスト付きのルート マップによる OSPF インバウンド フィルタリング機能を使用すると、ユーザはルート マップを定義して、ルーティング テーブルへの OSPF ルートの追加を防止できます。 次に示すコマンドは、この章に記載されている機能において、新たに導入または変更されたものです。 • **distribute-listin(IP)**

第 23 章

distribute-list を使用した OSPFv3 ルート フィルタリング

distribute-list を使用した OSPFv3 ルート フィルタリング機能を使用すると、ルーティング テーブルにプログラムされた着信ルート、およびアドバタイズされた発信ルートをフィルタリングできます。

- 機能情報の確認，265 ページ
- distribute-list を使用した OSPFv3 ルート フィルタリングの前提条件，266 ページ
- distribute-list を使用した OSPFv3 ルート フィルタリングについて，266 ページ
- distribute-list を使用した OSPFv3 ルート フィルタリングの設定方法，267 ページ
- その他の参考資料，272 ページ
- 配布リストを使用した OSPFv3 ルート フィルタリングの機能情報，273 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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

distribute-list を使用した OSPFv3 ルート フィルタリングの前提条件

ご使用のネットワークで OSPF が設定されていることが前提になります。

distribute-list を使用した OSPFv3 ルート フィルタリングについて

ユーザはルート マップを定義して、ルーティング テーブルへの OSPF ルートの追加を防止できます。このフィルタリングは、OSPF がルーティング テーブルにルートをインストールするときに行われます。この機能は、リンクステート アドバタイズメント（LSA）のフラッディングに影響を与えません。

この機能は、自律システム境界ルータ（ASBR）でプレフィックスが再配布されるとき、ユーザがこのプレフィックスにタグを付け、その後このタグで、プレフィックスを他のルータのルーティング テーブルにインストールしないようにフィルタリングする場合に有効です。下記のオプションは、route-map を使用する distribute-list フィルタリングでのみ使用できます。

ルート タグに基づいたフィルタリング

ユーザは外部ルートが OSPF に再配布される際にタグの割り当てができます。次に、**route-map** および **distribute-listin** または **distribute-list out** コマンドでそのタグを識別することにより、OSPF ドメインで外部ルートを許可または拒否できます。

ルート タイプに基づいたフィルタリング

OSPF では、外部ルートはタイプ 1 またはタイプ 2 のいずれかとなります。ユーザはルート マップを作成し、タイプ 1 またはタイプ 2 のいずれかと照合して **distribute-listin** コマンドを使用して特定のプレフィックスをフィルタリングします。また、ルート マップは内部ルート（エリア内とエリア間）も識別し、内部ルートもフィルタリングできます。

ルート ソースに基づいたフィルタリング

ルート ソースで照合が終わると、ルート ソースはプレフィックスがアドバタイズされる LSA 発信者の OSPF ルータ ID を示します。

インターフェイスに基づいたフィルタリング

インターフェイスで照合が終わると、インターフェイスは OSPF がルーティング テーブルでインストールしようとしているルートの発信インターフェイスを示します。

ネクスト ホップに基づいたフィルタリング

ネクスト ホップで照合が終わると、ネクスト ホップは OSPF がルーティング テーブルでインストールしようとしているルートのネクスト ホップを示します。

（注） **distribute-listin** コマンドでは、ルートがグローバル ルーティング情報ベース（RIB）にインストールされないように設定できます。OSPF ローカル RIB（OSPF ローカル RIB の機能情報については、『OSPFv2 Local RIB』を参照してください）が実装される前は、OSPF は選択されないほうのルート（エリア間パスがフィルタリングされる際のエリア内ルートなど）をインストールしようとしていました。OSPF ローカル RIB が実装されると、最適なルートだけ（ローカル RIB が保持する唯一のルートであるため）がインストールの対象となります。「次善の」OSPF ルートという概念はありません。Cisco OSPF ルータで使用されるルーティング アルゴリズムの詳細については RFC 2328 を参照してください。

distribute-list を使用した OSPFv3 ルート フィルタリングの設定方法

OSPFv3（IPv4 アドレス ファミリ）の設定

コマンド モード：アドレス ファミリ モード（アドレス ファミリ IPv4 ユニキャスト）。構文は次のとおりです。

```
[no] distribute-list [<access-list #> | <access-list name>] |
                     {prefix <name1> gateway <name2>} |
                     {prefix <name1>} | {gateway <name2>} |
      {route-map name} in [<interface>]

[no] distribute-list [<access-list #> | <access-list name>] | [prefix <name>] out
     [{ <routing-process> | <interface> }]
```

インターフェイス：着信（インバウンド フィルタリングで使用）または送信（アウトバウンド フィルタリングで使用）インターフェイス。

ルーティング プロセス：フィルタするルートの送信元プロトコル。

インバウンド フィルタリング：ルート マップの設定

手順の概要

1. OSPFv3 を設定します。
2. アドレス ファミリ IPv4 ユニキャストを設定します。
3. 適切なルート マップを使用して配布リストを設定します。

手順の詳細

ステップ 1 OSPFv3 を設定します。
```
Device(config)#router ospfv3 1
```

ステップ 2 アドレス ファミリ IPv4 ユニキャストを設定します。
```
Device(config-router)#address-family ipv4 unicast
```

ステップ 3 適切なルート マップを使用して配布リストを設定します。
```
Device(config-router-af)#distribute-list route-map rmap-name in
```
ルート マップでは次の match オプションがサポートされます。

- match interface
- match ip address
- match ip next-hop
- match ip route-source
- match metric
- match route-type
- match tag

インバウンド フィルタリング：プレフィックス リスト/アクセス リストの設定

手順の概要

1. OSPFv3 を設定します。
2. アドレス ファミリ IPv4 ユニキャストを設定します。
3. 使用するプレフィックス リストとフィルタの方向を定義します。

手順の詳細

ステップ 1 OSPFv3 を設定します。
```
Device(config)#router ospfv3 1
```

ステップ 2 アドレス ファミリ IPv4 ユニキャストを設定します。
```
Device(config-router)#address-family ipv4 unicast
```

ステップ 3 使用するプレフィックス リストとフィルタの方向を定義します。
```
Device(config-router-af)#distribute-list prefix pfxname in
```

（注） 使用可能なオプションの引数は次のとおりです。これらの引数を使用して、着信インターフェイスに基づくフィルタリングを実行できます。デバイスで使用可能ないずれかのインターフェイスを選択します。

```
Ethernet            IEEE 802.3
  Loopback            Loopback interface
  Null                Null interface
  Port-channel        Ethernet Channel of interfaces
  Serial              Serial
  Tunnel              Tunnel interface
  Vlan                Catalyst Vlans
```

アウトバウンド フィルタリングの設定

手順の概要

1. OSPFv3 を設定します。
2. アドレス ファミリ IPv4 ユニキャストを設定します。
3. 適切なルート マップを使用して配布リストを設定します。

手順の詳細

ステップ 1 OSPFv3 を設定します。

```
Device(config)#router ospfv3 1
```

ステップ 2 アドレス ファミリ IPv4 ユニキャストを設定します。

```
Device(config-router)#address-family ipv4 unicast
```

ステップ 3 適切なルート マップを使用して配布リストを設定します。

```
Device(config-router-af)#distribute-list prefix pfxlist-name out
```

（注） 使用可能なオプションの引数は次のとおりです。ルートの送信元プロトコルに基づいて、これらのオプションをフィルタリングに使用できます。

```
bgp         Border Gateway Protocol (BGP)
  connected  Connected
  eigrp      Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis       ISO IS-IS
  lisp       Locator ID Separation Protocol (LISP)
  ospf       Open Shortest Path First (OSPF)
  ospfv3     OSPFv3
  rip        Routing Information Protocol (RIP)
  static     Static routes
```

OSPFv3（IPv6アドレスファミリ）の配布リストを使用したルートフィルタリングの設定

モード：アドレス ファミリ モード（アドレス ファミリ IPv6 ユニキャスト）。プレフィックス リストおよびルートマップはフィルタリング オプションとしてサポートされます。構文は次のとおりです。

```
[no] distribute-list prefix-list <name> in [<interface>]
[no] distribute-list route-map <name> in
[no] distribute-list prefix-list <name> out <routing-process>
```

インターフェイス：着信（インバウンド フィルタリングで使用）または送信（アウトバウンド フィルタリングで使用）インターフェイス。

ルーティング プロセス：フィルタするルートの送信元プロトコル。

インバウンド フィルタリング：ルート マップの設定

手順の概要

1. OSPFv3 を設定します。
2. アドレス ファミリ IPv6 ユニキャストを設定します。
3. ルート マップを定義します。

手順の詳細

ステップ 1 OSPFv3 を設定します。

```
Device(config)#router ospfv3 1
```

ステップ 2 アドレス ファミリ IPv6 ユニキャストを設定します。

```
Device(config-router)#address-family ipv6 unicast
```

ステップ 3 ルート マップを定義します。

```
Device(config-router-af)#distribute-list route-map rmap-name in
```

ルート マップでは次の match オプションがサポートされます。

- match interface
- match ip address
- match ip next-hop
- match metric
- match route-type
- match tag

インバウンド フィルタリング：プレフィックス リストの設定

手順の概要

1. OSPFv3 を設定します。
2. アドレス ファミリ IPv6 ユニキャストを設定します。
3. プレフィックス リストの名前を定義します。
4. 着信ルーティング アップデートのフィルタを定義します。

手順の詳細

ステップ 1 OSPFv3 を設定します。

```
Device(config)#router ospfv3 1
```

ステップ 2 アドレス ファミリ IPv6 ユニキャストを設定します。

```
Device(config-router)#address-family ipv6 unicast
```

ステップ 3 プレフィックス リストの名前を定義します。

```
Device(config-router-af)#distribute-list prefix pfxlist-name
```

ステップ 4 着信ルーティング アップデートのフィルタを定義します。

```
Device(config-router-af)#distribute-list prefix pfxname in
```

（注） 使用可能なオプションの引数は次のとおりです。これらの引数を使用して、着信インターフェイスに基づくフィルタリングを実行できます。デバイスで使用可能ないずれかのインターフェイスを選択します。

```
Ethernet            IEEE 802.3
  Loopback            Loopback interface
  Null                Null interface
  Port-channel        Ethernet Channel of interfaces
  Serial              Serial
  Tunnel              Tunnel interface
  Vlan                Catalyst Vlans
```

アウトバウンド フィルタリングの設定

手順の概要

1. OSPFv3 を設定します。
2. アドレス ファミリ IPv6 ユニキャストを設定します。
3. プレフィックス リストの名前を定義します。

手順の詳細

ステップ 1 OSPFv3 を設定します。

```
Device(config)#router ospfv3 1
```

ステップ 2 アドレス ファミリ IPv6 ユニキャストを設定します。

```
Device(config-router)#address-family ipv6 unicast
```

ステップ 3 プレフィックス リストの名前を定義します。

```
Device(config-router-af)#distribute-list prefix-list pfxlist-name out
```

（注） これらはルーティング プロセスに使用できるオプションです。IPv6 アウトバウンド ルート フィルタリングでは、<**routing-process**> 引数は必須です。

```
bgp         Border Gateway Protocol (BGP)
  connected  Connected Routes
  eigrp      Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis       ISO IS-IS
  lisp       Locator ID Separation Protocol (LISP)
  ospf       Open Shortest Path First (OSPFv3)
  rip        IPv6 Routing Information Protocol (RIPv6)
  static     Static Routes
```

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
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

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

配布リストを使用した OSPFv3 ルート フィルタリングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *26*：配布リストを使用した *OSPFv3* ルート フィルタリングの機能情報

機能名	リリース	機能情報
distribute-list を使用した OSPFv3 ルート フィルタリング	Cisco IOS XE Denali 16.3.1	配布リストを使用した OSPFv3 ルート フィルタリングに対するルートマップ サポートが提供されます。

第 24 章

OSPF Shortest Path First スロットリング

OSPF Shortest Path First スロットリング機能により、最短パス優先（SPF）スケジューリングをミリ秒間隔で設定して、ネットワークが不安定な場合にSPF計算を遅らせることができます。トポロジ変化が発生した場合、Shortest Path Tree（SPT）を再計算するようにSPFがスケジューリングされます。SPFが1回実行されると、複数のトポロジ変化イベントが発生します。

SPF計算の実行間隔は、ネットワークのトポロジ変化の頻度に応じて動的に選択されます。ユーザ指定値の範囲内で、間隔は選択されます。ネットワーク トポロジが不安定な場合、トポロジが安定するまで、SPF スロットリング機能は SPF スケジューリング間隔を長目に計算します。

- 機能情報の確認，275 ページ
- OSPF SPF スロットリングについて，276 ページ
- OSPF SPF スロットリングの設定方法，277 ページ
- OSPF SPF スロットリングの設定例，278 ページ
- その他の参考資料，279 ページ
- OSPF Shortest Path First スロットリングの機能情報，280 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。

OSPF SPF スロットリングについて

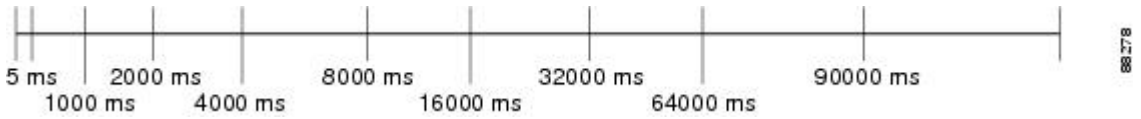
SPF の計算は、**timersthrottlespf** コマンドで設定した間隔で実行されます。待機期間とは、次の SPF 計算が実行されるまで待機する時間のことです。計算を行うたびに、待機期間はその前の待機期間の 2 倍の長さになり、指定された最大待機期間に達するまでそれが行われます。

SPF タイミングについて、例を使用して説明します。この例では、開始時待機期間が 5 ミリ秒（ms）、待機期間が 1000 ミリ秒、最大待機期間が 90,000 ミリ秒に設定されています。

```
timers throttle spf 5 1000 90000
```

次の図に、ある待機期間中に少なくとも 1 回のトポロジ変化イベントを受信する場合の、SPF 計算の実行間隔を示します。

図 *10*：*timers throttle spf* コマンドで設定される *SPF* の計算間隔

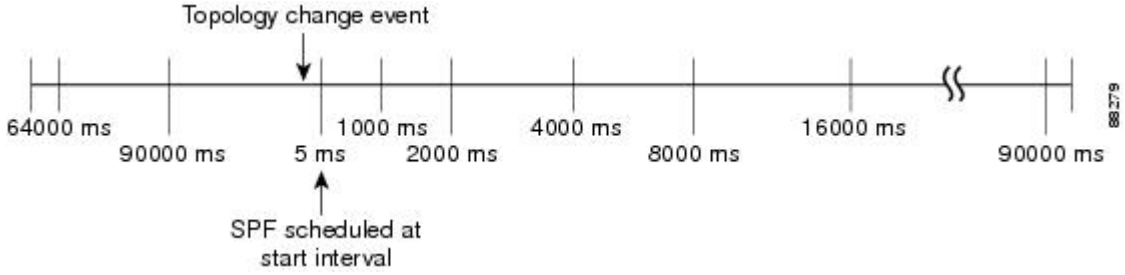


前の待機期間中に少なくとも 1 回のトポロジ変化イベントを受信すると、SPF 計算の待機期間が 2 倍になることに注意してください。最大待機期間に達すると、トポロジが安定し、待機期間中にイベントを受信しなくなるまで、待機期間が変化しなくなります。

現在の待機期間の経過後に、最初のトポロジ変化イベントを受信した場合は、開始時待機期間として指定されている時間だけ SPF 計算が遅延されます。その後の待機期間は、動的パターンに従います。

最大待機期間の開始後に、最初のトポロジ変化イベントが発生した場合、SPF 計算は開始時待機期間で再びスケジューリングされ、その後の待機期間は **timersthrottlespf** コマンドで指定されたパラメータに従ってリセットされます。次の図では、最大待機期間の開始後にトポロジ変化イベントを受信して、SPF 間隔がリセットされることに注意してください。

図 *11*：トポロジ変化イベント後のタイマー間隔のリセット



OSPF SPF スロットリングの設定方法

OSPF SPF スロットリングの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id*
4. **timersthrottlespf***spf-startspf-holdspf-max-wait*
5. **end**

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 モードなど、高位の権限レベル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	**routerospf***process-id* 例： `Router(config)# router ospf 1`	OSPF ルーティング プロセスを設定します。
ステップ 4	**timersthrottlespf***spf-startspf-holdspf-max-wait* 例： `Router(config-router)# timers throttle spf 10 4800 90000`	OSPF スロットリング タイマーを設定します。
ステップ 5	**end** 例： `Router(config-router)# end`	設定モードを終了します。

SPF スロットル値の確認

SPF スロットル タイマー値を確認するには、**show ip ospf** コマンドを使用します。これらの値は、「Initial SPF schedule delay...」、「Minimum hold time between two consecutive SPFs...」、および「Maximum wait time between two consecutive SPFs...」で始まる各行に表示されます。

```
Router# show ip ospf
 Routing Process "ospf 1" with ID 10.10.10.2 and Domain ID 0.0.0.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 It is an autonomous system boundary router
 Redistributing External Routes from,
    static, includes subnets in redistribution
Initial SPF schedule delay 5 msecs
 Minimum hold time between two consecutive SPFs 1000 msecs
 Maximum wait time between two consecutive SPFs 90000 msecs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 4. Checksum Sum 0x17445
 Number of opaque AS LSA 0. Checksum Sum 0x0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        Area has no authentication
        SPF algorithm last executed 19:11:15.140 ago
        SPF algorithm executed 28 times
        Area ranges are
        Number of LSA 4. Checksum Sum 0x2C1D4
        Number of opaque link LSA 0. Checksum Sum 0x0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

OSPF SPF スロットリングの設定例

例：スロットル タイマー

この例では、ルータに、**timers throttle spf** コマンドの開始時待機期間、待機期間、および最大待機期間として、それぞれ 5、1,000、および 90,000 ミリ秒を設定しています。

```
router ospf 1
 router-id 10.10.10.2
 log-adjacency-changes
 timers throttle spf 5 1000 90000
 redistribute static subnets
 network 21.21.21.0 0.0.0.255 area 0
 network 22.22.22.0 0.0.0.255 area 00
```

その他の参考資料

ここでは、OSPF Shortest Path First スロットリングに関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
『Configuring OSPF』	『Configuring OSPF』
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』

標準

標準	Title
なし	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
なし	--

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

OSPF Shortest Path First スロットリングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *27* : *OSPF Shortest Path First* スロットリングの機能情報

機能名	リリース	機能情報
OSPF Shortest Path First スロットリング	Cisco IOS XE Release 2.1	OSPF Shortest Path First スロットリング機能により、SPF スケジューリングをミリ秒間隔で設定して、ネットワークが不安定な時に Shortest Path First（SPF）計算を遅らせることができます。トポロジ変化が発生した場合、Shortest Path Tree（SPT）を再計算するように SPF がスケジューリングされます。 次に示すコマンドは、この章に記載されている機能において、新たに導入または変更されたものです。 • **timerspf-interval** • **timersthrottlespf**

第 25 章

fast hello パケットに対する OSPF のサポート

fast hello パケットに対する OSPF のサポートには、1 秒未満のインターバルで hello パケットの送信を設定する方法が用意されています。このような設定により、Open Shortest Path First（OSPF）ネットワークでの統合がより迅速になります。

（注） fast hello パケットではなく、双方向フォワーディング検出（BFD）を使用することをお勧めします。

- 機能情報の確認，283 ページ
- fast hello パケットに対する OSPF のサポートの前提条件，284 ページ
- fast hello パケットに対する OSPF のサポートについて，284 ページ
- OSPF fast hello パケットの設定方法，285 ページ
- fast hello パケットに対する OSPF のサポートの設定例，287 ページ
- その他の参考資料，287 ページ
- fast hello パケットに対する OSPF のサポートの機能情報，288 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。

fast hello パケットに対する OSPF のサポートの前提条件

OSPF がネットワークですでに設定されているか、fast hello パケットに対する OSPF のサポートと同時に設定される必要があります。

fast hello パケットに対する OSPF のサポートについて

OSPF Hello インターバルおよび dead 間隔

OSPF hello パケットとは、OSPF プロセスがネイバーとの接続を維持するために OSPF ネイバーに送信するパケットです。hello パケットは、設定可能なインターバル（秒単位）で送信されます。デフォルトのインターバルは、イーサネット リンクの場合 10 秒、ブロードキャスト以外のリンクの場合 30 秒です。hello パケットには、デッド インターバル中に受信したすべてのネイバーのリストが含まれます。デッド インターバルも設定可能なインターバル（秒単位）で送信されます。デフォルトは hello インターバルの値の 4 倍です。hello インターバルの値は、ネットワーク内ですべて同一にする必要があります。デッド インターバルの値も、ネットワーク内ですべて同一にする必要があります。

この 2 つのインターバルは、リンクが動作していることを示すことにより、接続を維持するために連携して機能します。ルータがデッド インターバル内にネイバーから hello パケットを受信しない場合、ルータはこのネイバーがダウンしていると判定します。

OSPF fast hello パケット

OSPF fast hello パケットとは、1 秒よりも短いインターバルで送信される hello パケットのことです。fast hello パケットを理解するには、OSPF hello パケット インターバルとデッド インターバルとの関係についてあらかじめ理解しておく必要があります。「OSPF Hello インターバルおよび dead 間隔, （284 ページ）」の項を参照してください。

OSPF fast hello パケットは、**ip ospf dead-interval** コマンドで設定されます。dead 間隔は 1 秒に設定され、hello-multiplier の値は、その 1 秒間に送信する hello パケット数に設定されるため、1 秒未満の「fast」hello パケットになります。

インターフェイスで fast hello パケットが設定されている場合、このインターフェイスから送出される hello パケットでアドバタイズされる hello 間隔は 0 に設定されます。このインターフェイス経由で受信した hello パケットの hello 間隔は無視されます。

デッド インターバルは、1 つのセグメント上で一貫している必要があり、1 秒に設定するか（fast hello パケットの場合）、他の任意の値を設定します。デッド インターバル内に少なくとも 1 つの hello パケットが送信される限り、hello multiplier がセグメント全体で同じである必要はありません。

OSPF fast hello パケットの利点

fast hello パケットに対する OSPF のサポート機能を利用すると、ネットワークがこの機能を使用しない場合よりも、短い時間で統合されます。この機能によって、失われたネイバーを 1 秒以内に検出できるようになります。この機能は、ネイバーの損失が Open System Interconnection（OSI）物理層またはデータ リンク層で検出されないことがあっても、特に LAN セグメントで有効です。

OSPF fast hello パケットの設定方法

OSPF fast hello パケットの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipospfdead-intervalminimalhello-multiplier***multiplier*
5. **end**
6. **showipospfinterface**[*interface-typeinterface-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	イネーブル化 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベル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	**interface***typenumber* 例： `Router(config)# interface gigabitethernet 0/0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ipospfdead-intervalminimalhello-multiplier***multiplier* 例： `Router(config-if)# ip ospf dead-interval minimal hello-multiplier 5`	少なくとも 1 個の hello パケットの受信が必要なインターバルを設定します。受信されなければ、ネイバーがダウンしていると判断されます。 • ここでは、**minimal** キーワードおよび **hello-multiplier** キーワードと値を指定することにより、fast hello パケットに対する OSPF のサポートがイネーブルになっています。multiplier キーワードが 5 に設定されているため、hello パケットが毎秒 5 回送信されます。
ステップ 5	**end** 例： `Router(config-if)# end`	（任意）コンフィギュレーション コマンドを実行コンフィギュレーション ファイルに保存し、コンフィギュレーション モードを終了して特権 EXEC モードに戻ります。 • コンフィギュレーション モードの終了と、設定ファイルへの設定内容の保存の用意ができたらこのコマンドを使用してください。
ステップ 6	**showipospfinterface**[*interface-typeinterface-number*] 例： `Router# show ip ospf interface gigabitethernet 0/0/1`	（任意）OSPF 関連のインターフェイス情報を表示します。 • OSPF fast hello パケットを確認する関連フィールドについては、次の表の出力例を参照してください。

例

この出力例では、fast hello パケットに対する OSPF のサポートが設定されているかを確認できます。「Timer intervals configured」で始まる行では、hello インターバルは 200 ミリ秒、デッド インターバルは 1 秒で、次の hello パケットの発生期限は 76 ミリ秒です。

```
Router# show ip ospf interface gigabitethernet 0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Internet Address 172.16.1.2/24, Area 0
  Process ID 1, Router ID 172.17.0.2, Network Type BROADCAST, Cost:1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.17.0.2, Interface address 172.16.1.2
  Backup Designated router (ID) 172.16.0.1, Interface address 172.16.1.1
  Timer intervals configured, Hello 200 msec, Dead 1, Wait 1, Retransmit 5
    Hello due in 76 msec
Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 3
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
```

```
  Adjacent with neighbor 172.16.0.1  (Backup Designated Router)
Suppress hello for 0 neighbor(s)
```

fast hello パケットに対する OSPF のサポートの設定例

例：OSPF fast hello パケット

次に、OSPF fast hello パケットを設定する例を示します。デッドインターバルは 1 秒に設定され、毎秒 5 個の hello パケットが送信されます。

```
interface gigabitethernet 0/0/1
 ip ospf dead-interval minimal hello-multiplier 5
```

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
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』
OSPFv3 外部パス プリファレンス オプション	*Configuring OSPF* モジュール

標準および RFC

標準/RFC	Title
IPv6 に関する RFC	IPv6 の RFC

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

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

fast hello パケットに対する OSPF のサポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *28* : *fast hello* パケットに対する *OSPF* のサポートの機能情報

機能名	リリース	機能情報
fast hello パケットに対する OSPF のサポート	Cisco IOS XE Release 2.1	fast hello パケットに対する OSPF のサポートには、1 秒未満のインターバルで hello パケットの送信を設定する方法が用意されています。このような設定により、Open Shortest Path First（OSPF）ネットワークでの統合がより迅速になります。

第 26 章

OSPF のインクリメンタル SPF

Open Shortest Path First（OSPF）プロトコルは、Shortest Path First（SPF）ルートを計算するインクリメンタル SPF アルゴリズムを使用するように設定できます。インクリメンタル SPF は、フル SPF アルゴリズムよりも効率的で、ネットワーク イベントに対応する新しいルーティング トポロジで、OSPF をより速くコンバージすることができます。

- 機能情報の確認，291 ページ
- OSPF のインクリメンタル SPF の前提条件，292 ページ
- OSPF のインクリメンタル SPF について，292 ページ
- OSPF のインクリメンタル SPF をイネーブルにする方法，292 ページ
- OSPF のインクリメンタル SPF の設定例，293 ページ
- その他の参考資料，293 ページ
- OSPF のインクリメンタル SPF の機能情報，295 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。

OSPF のインクリメンタル SPF の前提条件

ご使用のネットワークで OSPF が設定されていることが前提になります。

OSPF のインクリメンタル SPF について

OSPF は最短パス ツリー（SPT）の計算に、ダイクストラの SPF アルゴリズムを使用します。SPT の計算中に、各ノードまでの最短パスが検出されます。トポロジツリーは、ルーティングテーブルに IP ネットワークへのルートを入力するために使用されます。タイプ 1 またはタイプ 2 リンクステート アドバタイズメント（LSA）に対する変更がエリア内で発生すると、すべての SPT が再計算されます。多くの場合は、ほとんどのツリーが変更されないため、SPT 全体を計算する必要はありません。インクリメンタル SPF を使用すると、システムはツリー中の影響を受ける部分だけを再計算できます。ツリー全体でなく、ツリーの一部だけを再計算すると、OSPF コンバージェンスが高速になり、CPU リソースが節約されます。ルータ自身を計算しているときにタイプ 1 またはタイプ 2 の LSA が変更されると、フル SPT が実行されることに注意してください。

インクリメンタル SPF は、フル SPF と同様にスケジューリングされます。インクリメンタル SPF をイネーブルにされたルータ、およびインクリメンタル SPF をイネーブルにされてないルータは、同じインターネットワークで機能できます。

OSPF のインクリメンタル SPF をイネーブルにする方法

インクリメンタル SPF のイネーブル化

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id*
4. **ispf**
5. **end**

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	**routerospf***process-id* 例： `Router(config)# router ospf 1`	OSPF ルーティング プロセスを設定します。
ステップ 4	**ispf** 例： `Router(config-router)# ispf`	インクリメンタル SPF をイネーブルにします。
ステップ 5	**end** 例： `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了します。

OSPF のインクリメンタル SPF の設定例

例：インクリメンタル SPF

この例では、インクリメンタル SPF をイネーブルにします。

```
router ospf 1
 ispf
```

その他の参考資料

ここでは、OSPF のインクリメンタル SPF に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
『Configuring OSPF』	『Configuring OSPF』
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』

標準

規格	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

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

OSPF のインクリメンタル SPF の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *29* : *OSPF* のインクリメンタル *SPF* の機能情報

機能名	リリース	機能情報
OSPF のインクリメンタル SPF	Cisco IOS XE Release 2.1	OSPF は、Shortest Path First（SPF）ルートを計算するインクリメンタル SPF アルゴリズムを使用するように設定できます。インクリメンタル SPF は、フル SPF アルゴリズムよりも効率的で、ネットワーク イベントに対応する新しいルーティング トポロジで、OSPF をより速くコンバージすることができます。 次に示すコマンドは、この章に記載されている機能において、新たに導入または変更されたものです。 • **ispf**

第 27 章

OSPF のルート再配布数の制限

Open Shortest Path First（OSPF）は、別のプロトコルまたは別の OSPF プロセスから OSPF 内に再配布できるプレフィックスの最大数をユーザが定義する機能をサポートします。こうした制限により、ルータが大量のルートの再配布でフラッディングを起こすことを回避できます。

- 機能情報の確認，297 ページ
- OSPF のルート再配布数制限の前提条件，298 ページ
- OSPF のルート再配布数制限について，298 ページ
- OSPF のルート再配布数を制限する方法，298 ページ
- OSPF のルート再配布数制限の設定例，302 ページ
- その他の参考資料，302 ページ
- OSPF のルート再配布数制限の機能情報，304 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。

OSPF のルート再配布数制限の前提条件

ご使用のネットワークに OSPF と、再配布する別のプロトコルまたは OSPF プロセスが設定されていることが前提になります。

OSPF のルート再配布数制限について

Border Gateway Protocol（BGP）の OSPF への再配布で大量の IP ルートが OSPF に送信されると、ネットワークで深刻なフラッディング状態になるおそれがあります。ルートの再配布数を制限すると、この潜在的な問題を回避できます。

OSPF は、ルーティング可能でないアドレス（たとえば、0.0.0.0/7）からのパケットを受信し、受け入れることができます。

OSPF のルート再配布数を制限する方法

ここでは次の手順について説明します。これらは相互に排他的です。プレフィックスの再配布数を制限すると同時に、警告を発生することはできません。

再配布されるルート数の制限

（注） プレフィックスの再配布数を制限すると同時に、警告を発生することはできません。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id*
4. **redistribute***protocol*[*process-id* | *as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match**{**internal**| **external 1**| **external 2**}][**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]
5. **redistributemaximum-prefix***maximum*[*threshold*]
6. **end**
7. **showipospf**[*process-id*]

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	**routerospf***process-id* 例： `Router(config)# router ospf 1`	OSPF ルーティング プロセスを設定します。
ステップ 4	**redistribute***protocol*[*process-id* | *as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match**{**internal**| **external 1**| **external 2**}][**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] 例： `Router(config-router)# redistribute eigrp 10`	ルートを 1 つのルーティング ドメインから他のルーティング ドメインに再配布します。
ステップ 5	**redistributemaximum-prefix***maximum*[*threshold*] 例： `Router(config-router)# redistribute maximum-prefix 100 80`	OSPF への再配布が許可される IP プレフィックスの最大数を設定します。 • 引数 *maximum* のデフォルト値はありません。 • *threshold* 値はデフォルトで 75% に設定されています。 （注） **warning-only** キーワードをこのコマンドで設定すると、再配布数の制限は設定されません。警告メッセージのログが記録されるだけです。
ステップ 6	**end** 例： `Router(config-router)# end`	ルータ 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 7	**showipospf**[*process-id*] 例： `Router# show ip ospf 1`	（任意）OSPF ルーティング プロセスに関する一般情報を表示します。 • 再配布の制限が設定されていると、出力にはプレフィックスの再配布数の最大制限値と、警告メッセージが生成されるしきい値が含まれます。

OSPF へのルートの再配布数に関する警告の要求

（注） プレフィックスの再配布数を制限すると同時に、警告を発生することはできません。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id*
4. **redistribute***protocol*[*process-id* | *as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match**{**internal**| **external 1**| **external 2**}][**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]
5. **redistributemaximum-prefix***maximum*[*threshold*] **warning-only**
6. **end**

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	**routerospf***process-id* 例： `Router(config)# router ospf 1`	OSPF ルーティング プロセスを設定します。
ステップ 4	**redistribute***protocol*[*process-id* | *as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match**{**internal**| **external 1**| **external 2**}][**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] 例： `Router(config-router)# redistribute eigrp 10`	ルートを 1 つのルーティング ドメインから他のルーティング ドメインに再配布します。
ステップ 5	**redistributemaximum-prefix***maximum*[*threshold*] **warning-only** 例： `Router(config-router)# redistribute maximum-prefix 1000 80 warning-only`	IP プレフィックスの最大数が OSPF 内に再配布されたときに警告メッセージのログが記録されます。 • **warning-only** キーワードが含まれているため、OSPF へのプレフィックスの再配布数に制限は設定されません。 • 引数 *maximum* のデフォルト値はありません。 • *threshold* 値はデフォルトで 75% に設定されています。 • ここでは、1000 の 80%（800 個のルート再配布）で警告する場合と、1000 個のルート再配布で警告する場合の、2 つの例について説明します。
ステップ 6	**end** 例： `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了します。

OSPF のルート再配布数制限の設定例

例：OSPF のルート再配布数の制限

次の例で、OSPF プロセス 1 に再配布できるプレフィックスの最大数を 1200 に設定する方法を示します。再配布されたプレフィックス数が 1200 の 80%（960 個のプレフィックス）に達すると、警告メッセージのログが記録されます。制限に達すると、もう 1 種類の警告ログが記録され、これ以降、プレフィックスは再配布されなくなります。

```
router ospf 1
 router-id 10.0.0.1
 domain-id 5.6.7.8
 log-adjacency-changes
 timers lsa-interval 2
 network 10.0.0.1 0.0.0.0 area 0
 network 10.1.5.1 0.0.0.0 area 0
 network 10.2.2.1 0.0.0.0 area 0
 redistribute static subnets
 redistribute maximum-prefix 1200 80
```

例：ルートの再配布数に関する警告の要求

ここでは、プレフィックスの再配布数が 600 の 85%（510 個のプレフィックス）に達した場合と、ルートの再配布数が 600 に達した場合に出される警告メッセージについて説明します。ただし、再配布されるルート数は制限されません。

```
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 redistribute eigrp 10 subnets
 redistribute maximum-prefix 600 85 warning-only
```

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』
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
OSPFv3 アドレス ファミリ	*OSPFv3 Address Families* モジュール

標準

標準	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 5187	『*OSPFv3 Graceful Restart*』

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

OSPF のルート再配布数制限の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *30*：*OSPF* のルート再配布数制限の機能情報

機能名	リリース	機能情報
OSPF のルート再配布数の制限	Cisco IOS XE Release 2.1、Cisco IOS XE Release 2.6	OSPF は、別のプロトコルまたは別の OSPF プロセスから OSPF 内に再配布できるプレフィックスの最大数をユーザが定義する機能をサポートします。こうした制限により、ルータが大量のルートの再配布でフラッディングを起こすことを回避できます。 次に示すコマンドは、この章に記載されている機能において、新たに導入または変更されたものです。 • **redistributemaximum-prefix** • **showipospf** • **showipospfdatabase**

第 28 章

OSPFv3 高速コンバージェンス：LSA および SPF スロットリング

Open Shortest Path First バージョン 3（OSPFv3）のリンクステート アドバタイズメント（LSA）および最短パス優先（SPF）スロットリング機能では、ネットワークが不安定な間、OSPFv3 でのリンクステート アドバタイズメント アップデートを低速化するためのダイナミック メカニズムを提供します。さらに LSA のレート制限をミリ秒単位で指定することにより、OSPFv3 コンバージェンス時間の短縮が可能になります。

- 機能情報の確認，305 ページ
- OSPFv3 高速コンバージェンスについて：LSA および SPF スロットリング，306 ページ
- OSPFv3 高速コンバージェンスの設定方法：LSA および SPF スロットリング，306 ページ
- OSPFv3 高速コンバージェンスの設定例：LSA および SPF スロットリング，309 ページ
- その他の参考資料，310 ページ
- OSPFv3 高速コンバージェンス：LSA および SPF スロットリングの機能情報，311 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。

OSPFv3 高速コンバージェンスについて：LSA および SPF スロットリング

高速コンバージェンス：LSA および SPF スロットリング

OSPFv3 の LSA および SPF スロットリング機能は、ネットワークが不安定な間、OSPFv3 でのリンクステート アドバタイズメント アップデートを低速化するためのダイナミック メカニズムを提供します。さらにLSAのレート制限をミリ秒単位で指定することにより、OSPFv3コンバージェンス時間の短縮が可能になります。

OSPFv3 ではレート制限 SPF 計算および LSA 生成にスタティック タイマーを使用できます。これらのタイマーを設定することもできますが、使用する値は秒単位で指定するため、OSPFv3 コンバージェンスに制限が課せられます。LSA および SPF スロットリングは、すばやく応答できる高度な SPF および LSA レート制限メカニズムを提供することにより、1 秒未満単位でのコンバージェンスを実現し、長引く不安定期間中にも安定性および保護を提供します。

OSPFv3 高速コンバージェンスの設定方法：LSA および SPF スロットリング

OSPFv3高速コンバージェンスに対するLSAおよびSPFタイマーの調整

この作業は、Cisco IOS Release 15.1(3)S および 15.2(1)T 以降のリリースで実行できます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospfv3**[*process-id*]
4. **timerslsaarrival***milliseconds*
5. **timerspacingflood***milliseconds*
6. **timerspacinglsa-group***seconds*
7. **timerspacingretransmission***milliseconds*

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： `Device> 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： `Device# 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	**routerospfv3**[*process-id*] 例： `Device(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**timerslsaarrival***milliseconds* 例： `Device(config-rtr)# timers lsa arrival 300`	ソフトウェアが OSPFv3 ネイバーから同じ LSA を受け入れる最小間隔を設定します。
ステップ 5	**timerspacingflood***milliseconds* 例： `Device(config-rtr)# timers pacing flood 30`	LSA フラッド パケット ペーシングを設定します。
ステップ 6	**timerspacinglsa-group***seconds* 例： `Device(config-router)# timers pacing lsa-group 300`	OSPFv3 LSA を収集してグループ化し、リフレッシュ、チェックサム、またはエージングを行う間隔を変更します。
ステップ 7	**timerspacingretransmission***milliseconds* 例： `Device(config-router)# timers pacing retransmission 100`	IPv4 OSPFv3 での LSA 再送信パケット ペーシングを設定します。

OSPFv3 高速コンバージェンスに対する LSA および SPF スロットリングの設定

この作業は、Cisco IOS Release 15.1(3)S および 15.2(1)T よりも前のリリースで実行できます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6routerospf***process-id*
4. **timersthrottlespf***spf-startspf-holdspf-max-wait*
5. **timersthrottlelsa***start-intervalhold-intervalmax-interval*
6. **timerslsaarrival***milliseconds*
7. **timerspacingflood***milliseconds*

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	**configureterminal** 例： `Device# 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	**ipv6routerospf***process-id* 例： `Device(config)# ipv6 router ospf 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**timersthrottlespf***spf-startspf-holdspf-max-wait* 例： `Device(config-rtr)# timers throttle spf 200 200 200`	SPF スロットリングをオンにします。

	コマンドまたはアクション	目的
ステップ 5	**timersthrottlelsa***start-intervalhold-intervalmax-interval* 例： `Device(config-rtr)# timers throttle lsa 300 300 300`	OSPFv3 LSA 生成に対するレート制限値を設定します。
ステップ 6	**timerslsaarrival***milliseconds* 例： `Device(config-rtr)# timers lsa arrival 300`	ソフトウェアが OSPFv3 ネイバーから同じ LSA を受け入れる最小間隔を設定します。
ステップ 7	**timerspacingflood***milliseconds* 例： `Device(config-rtr)# timers pacing flood 30`	LSA フラッド パケット ペーシングを設定します。

OSPFv3 高速コンバージェンスの設定例：LSA および SPF スロットリング

OSPFv3 高速コンバージェンスに対する LSA および SPF スロットリングの設定例

次に、SPF および LSA スロットリング タイマーの設定値を表示する例を示します。

```
Device# show ipv6 ospf

Routing Process "ospfv3 1" with ID 10.9.4.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 It is an autonomous system boundary router
 Redistributing External Routes from,
    ospf 2
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
```

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
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』
OSPFv3 高速コンバージェンス：LSA および SPF スロットリング	*OSPF Link-State Advertisement Throttling* モジュール

標準および RFC

標準/RFC	Title
IPv6 に関する RFC	IPv6 の RFC

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

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

OSPFv3 高速コンバージェンス：LSA および SPF スロットリングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *31*：*OSPFv3* 高速コンバージェンス：*LSA* および *SPF* スロットリングの機能情報

機能名	リリース	機能情報
OSPFv3 高速コンバージェンス：LSA および SPF スロットリング	Cisco IOS XE Release 2.1	OSPFv3 の LSA および SPF スロットリング機能は、ネットワークが不安定な間、OSPFv3 でのリンクステート アドバタイズメント アップデートを低速化するためのダイナミック メカニズムを提供します。

第 29 章

OSPFv3 Max-Metric ルータ LSA

Open Shortest Path First バージョン 3（OSPFv3）Max-Metric ルータ リンクステート アドバタイズメント（LSA）機能により、OSPFv3 はローカルで生成されたルータ LSA を最大メトリックでアドバタイズできるようになります。この機能を使用すると OSPFv3 プロセスはデバイスを通過する中継トラフィックをコンバージできるようになりますが、より適切な代替パスが存在する場合は、中継トラフィックを引き込むことはできません。

- 機能情報の確認，313 ページ
- OSPFv3 Max-Metric ルータ LSA について，314 ページ
- OSPFv3 Max-Metric ルータ LSA の設定方法，314 ページ
- OSPFv3 Max-Metric ルータ LSA の設定例，316 ページ
- OSPF ノンストップ ルーティングに関する追加情報，316 ページ
- OSPFv3 Max-Metric ルータ LSA の機能情報，317 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。

OSPFv3 Max-Metric ルータ LSA について

OSPFv3 Max-Metric ルータ LSA

OSPFv3 Max-Metric ルータ LSA 機能により、OSPFv3 はローカルで生成されたルータ LSA を最大メトリックでアドバタイズできるようになります。この機能を使用すると OSPFv3 プロセスはデバイスを通過する中継トラフィックをコンバージできるようになりますが、より適切な代替パスが存在する場合は、中継トラフィックを引き込むことはできません。指定したタイムアウトまたは Border Gateway Protocol（BGP）からの通知の後、OSPFv3 は通常のメトリックで LSA をアドバタイズします。

Max-Metric LSA 制御では、LSA アドバタイズメントの使用により OSPFv3 ルータがスタブ ルータ ロールになります。スタブ ルータは、直接接続されたリンクを宛先とするパケットのみを転送します。OSPFv3 ネットワークでは、デバイスが接続しているリンクに対して大きなメトリックをアドバタイズすると、このデバイスを通るパスのコストは代替パスのコストよりも大きくなり、このデバイスはスタブ ルータになる場合があります。OSPFv3 スタブ ルータ アドバタイズメントを使用すると、デバイスは、ルータ LSA 内の接続しているリンクに対して無限メトリック（0xFFFF）をアドバタイズできます。また、リンクがスタブ ネットワークの場合は、通常のインターフェイス コストをアドバタイズします。

OSPFv3 Max-Metric ルータ LSA の設定方法

OSPFv3 Max-Metric ルータ LSA の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospfv3***process-id*
4. **address-family ipv6 unicast**
5. **max-metricrouter-lsa** [**external-lsa**[*max-metric-value*]] [**include-stub**] [**inter-area-lsas**[*max-metric-value*]] [**on-startup**{*seconds* | **wait-for-bgp**}] [**prefix-lsa**] [**stub-prefix-lsa**[*max-metric-value*]] [**summary-lsa**[*max-metric-value*]]
6. **end**
7. **showospfv3**[*process-id*]**max-metric**

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	**configureterminal** 例： `Device# 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	**routerospfv3***process-id* 例： `Device(config)# router ospfv3 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**address-family ipv6 unicast** 例： `Device(config)# address-family ipv6 unicast`	IPv6 アドレス ファミリの OSPFv3 プロセスのインスタンスを設定します。
ステップ 5	**max-metricrouter-lsa** [**external-lsa**[*max-metric-value*]] [**include-stub**] [**inter-area-lsas**[*max-metric-value*]] [**on-startup**{*seconds* | **wait-for-bgp**}] [**prefix-lsa**] [**stub-prefix-lsa**[*max-metric-value*]] [**summary-lsa**[*max-metric-value*]] 例： `Device(config-router-af)# max-metric router-lsa on-startup wait-for-bgp`	OSPFv3 プロトコルを実行するデバイスが最大メトリックをアドバタイズするように設定して、他のデバイスがそのデバイスを SPF 計算で中継ホップとして優先しないようにします。
ステップ 6	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 7	**showospfv3**[*process-id*]**max-metric** 例： `Device# show ospfv3 1 max-metric`	OSPFv3 最大メトリックの起点情報を表示します。

OSPFv3 Max-Metric ルータ LSA の設定例

例：OSPFv3 Max-Metric ルータ LSA の確認

```
Router# show ipv6 ospf max-metric

           OSPFv3 Router with ID (192.1.1.1) (Process ID 1)

 Start time: 00:00:05.886, Time elapsed: 3d02h
 Originating router-LSAs with maximum metric
    Condition: always, State: active
```

OSPF ノンストップ ルーティングに関する追加情報

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 Command List, All Releases』
OSPF コマンド	『Cisco IOS IP Routing: OSPF Command Reference』
IETF NSF または Cisco NSF の設定	『*Cisco IOS High Availability Configuration Guide*』の Configuring NSF-OSPF モジュール

標準および RFC

標準/RFC	Title
RFC 2328	『*OSPF Version 2*』
RFC 3623	『*Graceful OSPF Restart*』

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

OSPFv3 Max-Metric ルータ LSA の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *32* : ***OSPFv3 Max-Metric ルータ LSA* の機能情報**

機能名	リリース	機能情報
OSPFv3 Max-Metric ルータ LSA	Cisco IOS XE Release 3.4S	OSPFv3 Max-Metric ルータ LSA 機能により、OSPF はローカルで生成されたルータ LSA を最大メトリックでアドバタイズできるようになります。 次のコマンドが導入または変更されました。**max-metric router-lsa**、**show ipv6 ospf max-metric**、**show ospfv3 max-metric**

第 30 章

OSPF リンクステート アドバタイズメント スロットリング

OSPF リンクステート アドバタイズメント スロットリング機能では、ネットワークが不安定になっているときに、Open Shortest Path First（OSPF）のリンクステート アドバタイズメント（LSA）更新を抑制する、動的なメカニズムが得られます。さらに LSA のレート制限をミリ秒単位で指定することにより、OSPF コンバージェンス時間の短縮が可能になります。

- 機能情報の確認，319 ページ
- OSPF LSA スロットリングの前提条件，320 ページ
- OSPF LSA スロットリングについて，320 ページ
- OSPF LSA スロットリングのカスタマイズ方法，321 ページ
- OSPF LSA スロットリングの設定例，326 ページ
- その他の参考資料，326 ページ
- OSPF リンクステート アドバタイズメント スロットリングの機能情報，327 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。

OSPF LSA スロットリングの前提条件

ご使用のネットワークで OSPF が設定されていることが前提になります。

OSPF LSA スロットリングについて

OSPF LSA スロットリングの利点

OSPF LSA スロットリング機能が実装される以前は、LSA の生成が 5 秒間にレート制限されていました。LSA での変更をミリ秒単位では伝播できないため、OSPF ネットワークでミリ秒単位のコンバージェンスが不可能でした。

OSPF LSA スロットリング機能はデフォルトでイネーブルになっていて、OSPF コンバージェンス時間をより短く（ミリ秒単位に）できます。この機能はカスタマイズできます。1 つのコマンドが LSA の生成（送信）を制御し、もう 1 つのコマンドが受信間隔を制御します。この機能では、ネットワークが不安定になっている間、OSPF の LSA の更新頻度をダイナミックに制限することができます。

OSPF LSA スロットリングの動作

timers throttle lsa all コマンドが LSA の生成（送信）を制御します。最初の LSA は、OSPF トポロジが変更されるとすぐに必ず生成され、次の LSA の生成は最小開始間隔で制御されます。同じ LSA に対してこの後生成される LSA は、最大間隔に達するまでレート制限されます。「同じ LSA」とは、同じ LSA ID 番号、LSA タイプ、およびアドバタイズ ルータ ID を含む LSA インスタンスを意味します。

timers lsa arrival コマンドは、同じ LSA を受信する最小間隔を制御します。同じ LSA のインスタンスが、設定されている間隔が経過する前に到着した場合、その LSA はドロップされます。到着間隔は、**timers throttle lsa all** コマンドのホールド時間間隔以内にすることを推奨します。

OSPF LSA スロットリングのカスタマイズ方法

OSPF LSA スロットリングのカスタマイズ

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id*
4. **timersthrottlelsaall***start-intervalhold-intervalmax-interval*
5. **timerslsaarrival***milliseconds*
6. **end**
7. **showipospftimersrate-limit**
8. **showipospf**

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	**routerospf***process-id* 例： `Router(config)# router ospf 1`	OSPF ルーティング プロセスを設定します。
ステップ 4	**timersthrottlelsaall***start-intervalhold-intervalmax-interval* 例： `Router(config-router)# timers throttle lsa all 100 10000 45000`	（任意）LSA の生成に対するレート制限値（ミリ秒）を設定します。 • デフォルト値は次のとおりです。 • *start-interval* は 0 ミリ秒です • *hold-interval* は 5000 ミリ秒です

	コマンドまたはアクション	目的
		• *max-interval* は 5000 ミリ秒です
ステップ 5	**timerslsaarrival***milliseconds* 例： `Router(config-router)# timers lsa arrival 2000`	（任意）同じLSAを受信するインスタンス間の最小間隔（ミリ秒）を設定します。 • デフォルト値は 1000 ミリ秒です。 • LSA 到着タイマーの *milliseconds* 値は、**timers throttle lsa all** コマンドのネイバーの *hold-interval* 値以下にすることを推奨します。
ステップ 6	**end** 例： `Router(config-router)# end`	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 7	**showipospftimersrate-limit**
	例：
	`Router# show ip ospf timers rate-limit`
	例：
	例：
	`LSAID: 10.1.1.1 Type: 1 Adv Rtr: 172.16.2.2 Due in: 00:00:00.028`
	例：
	`LSAID: 192.168.4.1 Type: 3 Adv Rtr: 172.17.2.2 Due in: 00:00:00.028`
		（任意）レート制限キューにある（生成中の）LSA のリストを表示します。
		• この例ではキューに2つのLSAが入っています。各 LSA は LSA ID 番号、（LSA の）タイプ、アドバタイジング ルータ ID、および LSA が生成されるまでの時間を「時間：分：秒（ミリ秒）」で示したもので識別されます。

ステップ 8	**showipospf** 例： `Router# show ip ospf` 例：	（任意）OSPF に関する情報を表示します。 • 初期スロットル遅延、LSA スロットルの最小保留時間、およびLSA スロットルの最大遅延時間を指定する出力行に、LSA スロットリング値が示されます。

	コマンドまたはアクション	目的

	例：
	`Routing Process "ospf 4" with ID 10.10.24.4`
	例：
	`Supports only single TOS(TOS0) routes`
	例：
	`Supports opaque LSA`
	例：
	`Supports Link-local Signaling (LLS)`
	例：
	`Initial SPF schedule delay 5000 msecs`
	例：
	`Minimum hold time between two consecutive SPFs 10000 msecs`
	例：
	`Maximum wait time between two consecutive SPFs 10000 msecs`
	例：
	`Incremental-SPF disabled`
	例：
	`Initial LSA throttle delay 100 msecs`
	例：
	`Minimum hold time for LSA throttle 10000 msecs`
	例：
	`Maximum wait time for LSA throttle 45000 msecs`	

	コマンドまたはアクション	目的

	例：
	`Minimum LSA arrival 1000 msecs`
	
	例：
	`LSA group pacing timer 240 secs`
	
	例：
	`Interface flood pacing timer 33 msecs`
	
	例：
	`Retransmission pacing timer 66 msecs`
	
	例：
	`Number of external LSA 0. Checksum Sum 0x0`
	
	例：
	`Number of opaque AS LSA 0. Checksum Sum 0x0`
	
	例：
	`Number of DCbitless external and opaque AS LSA 0`
	
	例：
	`Number of DoNotAge external and opaque AS LSA 0`
	
	例：
	`Number of areas in this router is 1. 1 normal 0 stub 0 nssa`
	
	例：
	`External flood list length 0`
	
	例：
	`Area 24`	

	コマンドまたはアクション	目的
	例： Number of interfaces in this area is 2 例： Area has no authentication 例： SPF algorithm last executed 04:28:18.396 ago 例： SPF algorithm executed 8 times 例： Area ranges are 例： Number of LSA 4. Checksum Sum 0x23EB9 例： Number of opaque link LSA 0. Checksum Sum 0x0 例： Number of DCbitless LSA 0 例： Number of indication LSA 0 例： Number of DoNotAge LSA 0 例： Flood list length 0	

OSPF LSA スロットリングの設定例

例：OSPF LSA スロットリング

この例では、OSPF LSA スロットリングをカスタマイズして、開始間隔が 200 ミリ秒、ホールド間隔が 10,000 ミリ秒、最大間隔が 45,000 ミリ秒になるようにしています。同じ LSA を受信するインスタンス間の最小間隔は 2000 ミリ秒です。

```
router ospf 1
 log-adjacency-changes
 timers throttle lsa all 200 10000 45000
 timers lsa arrival 2000
 network 10.10.4.0 0.0.0.255 area 24
 network 10.10.24.0 0.0.0.255 area 24
```

その他の参考資料

ここでは、OSPF LSA スロットリングに関する参考資料を紹介します。

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』
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
『Configuring OSPF』	『Configuring OSPF』
OSPFv3 高速コンバージェンス：LSA および SPF スロットリング	*OSPFv3 Fast Convergence: LSA and SPF Throttling* モジュール
OSPFv3 Max-Metric ルータ LSA	*OSPFv3 Max-Metric Router LSA* モジュール

標準

規格	Title
なし	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
なし	--

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

OSPF リンクステート アドバタイズメント スロットリングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *33* : *OSPF* リンクステート アドバタイズメント スロットリングの機能情報

機能名	リリース	機能情報
OSPF リンクステート アドバタイズメント スロットリング	Cisco IOS XE Release 2.1、Cisco IOS XE Release 2.6	OSPF リンクステート アドバタイズメント スロットリング機能では、ネットワークが不安定になっているときに、OSPF のリンクステート アドバタイズメント（LSA）更新を抑制する、動的なメカニズムが得られます。さらに LSA のレート制限をミリ秒単位で指定することにより、OSPF コンバージェンス時間の短縮が可能になります。 次に示すコマンドは、この章に記載されている機能において、新たに導入または変更されたものです。 • **debugipospfdatabase-timerrate-limit** • **showipospf** • **showipospftimersrate-limit** • **timerslsaarrival** • **timersthrottlelsaall**

第 31 章

PE ルータごとに無制限なソフトウェア VRF の OSPF サポート

マルチプロトコル ラベル スイッチング - バーチャル プライベート ネットワーク（MPLS-VPN）の展開で、OSPF を実行するように設定するには、VPN ルーティングおよび転送（VRF）インスタンスごとに個別の Open Shortest Path First（OSPF）プロセスが必要です。プロバイダー エッジ（PE）ルータごとに無制限のソフトウェア VRF を OSPF がサポートする機能によって、OSPF VPN の 32 プロセス制限が排除され、OSPF VPN のスケーラビリティに関する問題を解決できます。

- 機能情報の確認，329 ページ
- PE ルータごとに無制限なソフトウェア VRF の OSPF サポートの前提条件，330 ページ
- PE ルータごとに無制限なソフトウェア VRF の OSPF サポートの制約事項，330 ページ
- PE ルータごとに無制限なソフトウェア VRF の OSPF サポートについて，330 ページ
- PE ルータごとに無制限のソフトウェア VRF を OSPF がサポートする設定方法，331 ページ
- PE ルータごとの無制限のソフトウェア VRF に対する OSPF サポートの設定例，332 ページ
- その他の参考資料，333 ページ
- PE ルータごとの無制限のソフトウェア VRF に対する OSPF サポートの機能情報，335 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。

PEルータごとに無制限なソフトウェアVRFのOSPFサポートの前提条件

ご使用のネットワークで OSPF が設定されている必要があります。

PEルータごとに無制限なソフトウェアVRFのOSPFサポートの制約事項

1 つの VRF でサポートできるのは 32 プロセスだけです。VRF プロセス間での相互の制限はありません。

PEルータごとに無制限なソフトウェアVRFのOSPFサポートについて

Cisco IOS リリース 12.3(4)T および 12.0(27)S 以前は、OSPF によって VPN ルートを受信する VRF ごとに、個別の OSPF が必要でした。VPN を導入すると、MPLS プロバイダー エッジ（PE）ルータは、VPN 配布用にマルチプロトコル ボーダー ゲートウェイ プロトコル（BGP）、PE-P 接続用に Interior Gateway Protocol（IGP）を実行します。OSPF は、カスタマー エッジ（CE）ルータと PE ルータの間の IGP として一般的に使用されます。OSPF には 32 プロセスの制限があるため、VPN 導入においてスケーラブルではありません。デフォルトでは、接続されたルート用に 1 つのプロセスが使用され、スタティック ルート用にまた別のプロセスが使用されます。このため、VRF 用に作成できるのは 28 プロセスだけです。

プロバイダー エッジ ルータごとに無制限のソフトウェア VRF を OSPF がサポートする機能を使用すると、プラットフォームと、そのプラットフォームで実行中のアプリケーション、プロセス、およびプロトコルに応じて、約 300 ～ 10,000 の VRF を作成できます。

PE ルータごとに無制限のソフトウェア VRF を OSPF がサポートする設定方法

PE ルータごとの無制限のソフトウェア VRF の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipvrf***vpn-name*
4. **exit**
5. **routerospf***process-id* [**vrf** *vpn-name*]
6. **end**
7. **showipospf** [*process-id*]

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	**ipvrf***vpn-name* 例： `Router(config)# ip vrf crf-1`	VPN ルーティング/転送（VRF）インスタンスを定義し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Router(config-vrf)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**routerospf***process-id* [**vrf** *vpn-name*] 例： `Router(config)# router ospf 1 vrf crf-1`	OSPF ルーティングをイネーブルにします。 • *process-id* 引数は OSPF プロセスを示します。 • ステップ 3 ですでに定義した VPN を識別するには、**vrf** キーワードおよび *vpn-name* 引数を使用します。 （注） これで、OSPF VRF プロセスを必要な数だけ設定できます。必要に応じてステップ 3 ～ 5 を繰り返します。
ステップ 6	**end** 例： `Router(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 7	**showipospf** [*process-id*] 例： `Router# show ip ospf 1`	OSPF ルーティング プロセスに関する一般情報を表示します。

PEルータごとの無制限のソフトウェアVRFに対するOSPFサポートの設定例

例：PE ルータごとの無制限のソフトウェア VRF に対する OSPF サポートの設定

次の例は、**router ospf** コマンドを使用して、first、second、および third という名前の各 VRF に、OSPF VRF プロセスを設定する、基本的な OSPF 設定を示しています。

```
Router> enable
Router# configure terminal
Router(config)# ip vrf first
Router(config-vrf)# exit
Router(config)# ip vrf second
Router(config-vrf)# exit
Router(config)# ip vrf third
Router(config-vrf)# exit
Router(config)# router ospf 12 vrf first
Router(config-router)# exit
Router(config)# router ospf 13 vrf second
Router(config-router)# exit
```

```
Router(config)# router ospf 14 vrf third
Router(config)# end
```

例：PE ルータごとの無制限のソフトウェア VRF に対する OSPF サポートの確認

次の例は、first という名前の VRF に OSPF VRF プロセス 12 が作成されたことを確認するための、**show ip ospf** コマンドの出力表示を示しています。VRF first に関連する出力を太字で示してあります。

```
Router# show ip ospf 12
main ID type 0x0005, value 0.0.0.100
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Connected to MPLS VPN Superbackbone, VRF first
 It is an area border router
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x0
 Number of opaque AS LSA 0. Checksum Sum 0x0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm last executed 00:00:15.204 ago
        SPF algorithm executed 2 times
        Area ranges are
        Number of LSA 1. Checksum Sum 0xD9F3
        Number of opaque link LSA 0. Checksum Sum 0x0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

その他の参考資料

ここでは、プロバイダー エッジ ルータごとに無制限のソフトウェア VRF を OSPF がサポートする機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
『Configuring OSPF』	『Configuring OSPF』

標準

規格	Title
なし	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
なし	--

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

PEルータごとの無制限のソフトウェアVRFに対するOSPFサポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *34*：プロバイダー エッジ ルータごとの無制限のソフトウェア *VRF* に対する *OSPF* サポートの機能情報

機能名	リリース	機能情報
プロバイダー エッジ ルータごとに無制限なソフトウェア VRF の OSPF サポート	Cisco IOS XE Release 2.1	マルチプロトコル ラベル スイッチング-バーチャル プライベート ネットワーク（MPLS-VPN）の展開で、OSPF を実行するように設定するには、VPN ルーティングおよび転送（VRF）インスタンスごとに個別の Open Shortest Path First（OSPF）プロセスが必要です。プロバイダー エッジ ルータごとに無制限のソフトウェア VRF を OSPF がサポートする機能によって、OSPF VPN の 32 プロセス制限が排除され、OSPF VPN のスケーラビリティに関する問題を解決できます。

第 32 章

OSPF エリア中継機能

OSPF エリア中継機能は、通常では仮想リンク パスを通過する必要のある転送トラフィックが、中継エリアを介してより短時間で通過できるパスを検出する機能を、OSPF エリア境界ルータ（ABR）に提供します。この機能により、Cisco IOS XE ソフトウェアが RFC 2328、*OSPF Version 2* に準拠したものとなります。

- 機能情報の確認，337 ページ
- OSPF エリア トランジット機能について，338 ページ
- OSPF エリア トランジット機能をディセーブルにする方法，338 ページ
- その他の参考資料，339 ページ
- OSPF エリア中継機能の機能情報，340 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。

OSPF エリア トランジット機能について

OSPF エリア トランジット機能の動作

OSPFエリア中継機能はデフォルトでイネーブルになっています。RFC 2328では、OSPFエリア中継機能が、OSPF エリア自身において発信と着信のいずれでもないデータ トラフィックを伝送するエリアの機能として定義されています。この機能により、OSPF ABR は中継エリアを介した短いパスを検出できるようになり、最適ではない仮想リンクまたは仮想パスを使用する代わりに、検出されたパスでトラフィックを転送できるようになります。

OSPF エリア トランジット機能の詳細については、『RFC 2328, OSPF Version 2』を参照してください。

OSPF エリア トランジット機能をディセーブルにする方法

エリア境界ルータでの OSPF エリア中継機能のディセーブル化

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id* [**vrf** *vpn-name*]
4. **nocapabilitytransit**

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	**routerospf***process-id* [**vrf** *vpn-name*] 例： `Router(config)# router ospf 100`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。 • *process-id* 引数は OSPF プロセスを示します。
ステップ 4	**nocapabilitytransit** 例： `Router(config-router)# no capability transit`	OSPF エリア中継機能を、ルータが処理するすべてのエリアでディセーブルにします。

その他の参考資料

ここでは、OSPF エリア中継機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
『Configuring OSPF』	『Configuring OSPF』
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』

標準

規格	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 2328	『OSPF Version 2』

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

OSPF エリア中継機能の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *35* : *OSPF* エリア中継機能の機能情報

機能名	リリース	機能情報
OSPF エリア中継機能	Cisco IOS XE Release 2.1	OSPF エリア中継機能は、通常では仮想リンク パスを通過する必要のある転送トラフィックが、中継エリアを介してより短時間で通過できるパスを検出する機能を、OSPF エリア境界ルータ（ABR）に提供します。この機能により、Cisco IOS XE ソフトウェアが RFC 2328 に準拠したものとなります。 この機能に関連するコマンドは次のとおりです。 • **capabilitytransit**

第 33 章

OSPFインターフェイス単位リンクローカル シグナリング

OSPF インターフェイス単位リンクローカル シグナリング機能では、以前設定したグローバル（ルータ レベル）設定に関係なく、特定のインターフェイスに対するリンクローカル シグナリング（LLS）をイネーブルにするか、ディセーブルにするかを選択できます。

- 機能情報の確認，343 ページ
- OSPF インターフェイス単位リンクローカル シグナリングについて，344 ページ
- OSPF インターフェイス単位リンクローカル シグナリングの設定方法，344 ページ
- OSPF インターフェイス単位リンクローカル シグナリングの設定例，346 ページ
- その他の参考資料，347 ページ
- OSPF インターフェイス単位リンクローカル シグナリングの機能情報，349 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。

OSPF インターフェイス単位リンクローカル シグナリングについて

LLS では、追加のビット スペースを提供できるよう、既存の OSPF パケットの拡張が可能です。追加のビット スペースによって、OSPF ネイバー間のパケット交換ごとの情報がより多く指定できるようになります。たとえば、この機能は、OSPF ノンストップ フォワーディング（NSF）認識機能で使用され、NSF を認識する宅内機器（CPE）ルータが、NSF 対応ルータによるパケットのノンストップ フォワーディング実行をサポートします。

LLS は、ルータ レベルでイネーブルになっていると、すべてのインターフェイスで自動的にイネーブルになります。OSPF のインターフェイス単位のリンクローカル シグナリング機能により、特定のインターフェイスに対する LLS をイネーブルにするか、ディセーブルにするか選択できます。ご使用のネットワーク設計によっては、インターフェイス単位で LLS をディセーブルにできます。たとえば、RFC 2328 に準拠していない可能性のあるシスコ製以外のデバイスに接続しているインターフェイス上で LLS をディセーブルにすると、ネットワーク内の OSPF ネイバーの形成に関する問題を回避できます。

OSPF インターフェイス単位リンクローカル シグナリングの設定方法

インターフェイス単位での LLS の停止

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typeslot*/*port*
4. **ipaddress***ip-addressmask* [**secondary**]
5. **noipdirected-broadcast** [*access-list-number* | *extended access-list-number*]
6. **ipospfmessage-digest-key***key-idencryption-type***md5***key*
7. [**no** | **default**] **ip ospf lls** [**disable**]

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	**interface***typeslot*/*port* 例： `Router(config)# interface gigabitethernet 1/1/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipaddress***ip-addressmask* [**secondary**] 例： `Router(config-if)# ip address 10.2.145.20 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 5	**noipdirected-broadcast** [*access-list-number* | *extended access-list-number*] 例： `Router(config-if)# no ip directed-broadcast`	インターフェイスが接続されたサブネットを宛先とするダイレクトブロードキャストを、ブロードキャストすることなくドロップします。 • イーサネット インターフェイス 1/0 上での IP ダイレクトブロードキャストのフォワーディングをディセーブルにします。
ステップ 6	**ipospfmessage-digest-key***key-idencryption-type***md5***key* 例： `Router(config-if)# ip ospf message-digest-key 100 md5 testing`	OSPF Message Digest 5（MD5）アルゴリズム認証をイネーブルにします。
ステップ 7	[**no** | **default**] **ip ospf lls** [**disable**] 例： `Router(config-if)# ip ospf lls disable`	グローバル（ルータ レベル）の設定にかかわらず、インターフェイス上の LLS をディセーブルにします。

次の作業

特定のインターフェイスで LLS がイネーブルになっているか、ディセーブルになっているかを確認するには、**showipospfinterface** コマンドを使用します。表示される情報の例については、「例：OSPFインターフェイス単位リンクローカル シグナリング機能の設定」の項を参照してください。

OSPF インターフェイス単位リンクローカル シグナリングの設定例

例：OSPF インターフェイス単位リンクローカル シグナリングの設定と確認

次の例では、LLS は、ギガビット イーサネット インターフェイス 1/1/0 ではイネーブルに、ギガビット イーサネット インターフェイス 2/1/0 でディセーブルになっています。

```
interface gigabitethernet1/1/0
 ip address 10.2.145.2 255.255.255.0
 no ip directed-broadcast
 ip ospf message-digest-key 1 md5 testing
 ip ospf lls
!
interface gigabitethernet2/1/0
 ip address 10.1.145.2 255.255.0.0
 no ip directed-broadcast
 ip ospf message-digest-key 1 md5 testing
!
 ip ospf lls disable
interface Ethernet3/0
 ip address 10.3.145.2 255.255.255.0
 no ip directed-broadcast
!
router ospf 1
 log-adjacency-changes detail
 area 0 authentication message-digest
 redistribute connected subnets
 network 10.0.0.0 0.255.255.255 area 1
 network 10.2.3.0 0.0.0.255 area 1
```

次の例では、**show ip ospf interface** コマンドを入力して、LLS がギガビット イーサネット インターフェイス 1/1/0 でイネーブルになっていることと、ギガビット イーサネット インターフェイス 2/1/0 でディセーブルになっていることを確認します。

```
Router# show ip ospf interface
GigabitEthernet1/1/0 is up, line protocol is up
  Internet Address 10.2.145.2/24, Area 1
  Process ID 1, Router ID 10.22.222.2, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.2.2.3, Interface address 10.2.145.1
  Backup Designated router (ID) 10.22.222.2, Interface address 10.2.145.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
!   Supports Link-local Signaling (LLS)
Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
```

```
  Last flood scan length is 2, maximum is 8
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.3  (Designated Router)
  Suppress hello for 0 neighbor(s)
GigabitEthernet2/1/0 is up, line protocol is up
  Internet Address 10.1.145.2/16, Area 1
  Process ID 1, Router ID 10.22.222.2, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.2.2.3, Interface address 10.1.145.1
  Backup Designated router (ID) 10.22.222.2, Interface address 10.1.145.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
!   Does not support Link-local Signaling (LLS)
Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 11
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 45.2.2.3  (Designated Router)
    Suppress hello for 0 neighbor(s)
GigabitEthernet3/1/0 is up, line protocol is up
  Internet Address 10.3.145.2/24, Area 1
  Process ID 1, Router ID 10.22.222.2, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.2.2.3, Interface address 10.3.145.1
  Backup Designated router (ID) 10.22.222.2, Interface address 10.3.145.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07
!   Supports Link-local Signaling (LLS)
Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 11
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.3  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

その他の参考資料

ここでは、OSPF インターフェイス単位リンクローカル シグナリング機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
『Configuring OSPF』	『Configuring OSPF』
OSPF NSF Awareness の設定	『Cisco Nonstop Forwarding』
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』

標準

規格	Title
なし	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 2328	『*OSPF Version 2*』

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

OSPF インターフェイス単位リンクローカル シグナリングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *36*：*OSPF* インターフェイス単位リンクローカル シグナリングの機能情報

機能名	リリース	機能情報
OSPF インターフェイス単位リンクローカル シグナリング	Cisco IOS XE Release 2.1	OSPF インターフェイス単位リンクローカル シグナリング機能では、以前設定したグローバル（ルータ レベル）設定に関係なく、特定のインターフェイスに対するリンクローカル シグナリング（LLS）をイネーブルにするか、ディセーブルにするかを選択できます。 次に示すコマンドは、この章に記載されている機能において、新たに導入または変更されたものです。 • **ipospflls**

第 34 章

OSPFリンクステートデータベースオーバーロードの防止

OSPF リンクステート データベース オーバーロード防止機能では、指定された Open Shortest Path First（OSPF）プロセスの非自己生成のリンクステート アドバタイズメント（LSA）の数に制限を設けることができます。OSPF ドメイン内で他のルータによって生成された大量の LSA は、ルータの CPU およびメモリ リソースを大量に消費する可能性があります。

- 機能情報の確認，351 ページ
- OSPF リンクステート データベース オーバーロード防止機能の前提条件，352 ページ
- OSPF リンクステート データベース オーバーロード防止機能について，352 ページ
- OSPF リンクステート データベース オーバーロード防止の設定方法，353 ページ
- OSPF リンクステート データベース オーバーロード防止の設定例，355 ページ
- その他の参考資料，356 ページ
- OSPF リンクステート データベース オーバーロード防止の機能情報，358 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。

OSPF リンクステート データベース オーバーロード防止機能の前提条件

ご使用のネットワークで OSPF が実行されていることが前提になります。

OSPF リンクステート データベース オーバーロード防止機能について

OSPF リンクステート データベース オーバーロード防止機能を使用する利点

OSPF リンクステート データベース オーバーロード防止機能は、指定された OSPF プロセスの非自己生成の LSA 数を制限するためのメカニズムを OSPF レベルで提供します。ネットワーク内の他のルータで設定の誤りがあると、多数のプレフィックスの再配布といった大量の LSA が生成される場合があります。この保護メカニズムを使用すると、ルータが大量の LSA を受信したり、CPU とメモリが不足することを回避できます。

OSPF リンクステート データベース オーバーロード防止機能の動作

OSPF リンクステート データベース オーバーロード防止機能がイネーブルになっていると、ルータは受信した（非自己生成）LSA の数を保持します。設定された LSA のしきい値数に達すると、エラーメッセージのログが記録されます。設定された LSA の最大数を超過すると、ルータから通知が送信されます。受信した LSA の数が 1 分経過しても設定されている最大値よりも依然として大きい場合、OSPF プロセスはすべての隣接関係を解除し、OSPF データベースを消去します。この ignore 状態では、この OSPF プロセスに属するインターフェイスで受信された OSPF パケットがすべて無視されます。これらのインターフェイスでは OSPF パケットは生成されません。OSPF プロセスは、**max-lsa** コマンドの **ignore-time** キーワードで設定された期間、ignore 状態のままとなります。OSPF プロセスが ignore 状態になるたびにカウンタの値が 1 つ増えます。このカウンタが **ignore-count** キーワードで設定された数（分）よりも大きくなると、OSPF プロセスは同じ ignore 状態のままになります。このプロセスの ignore 状態を解除するには、手動操作が必要です。ignore 状態のカウンタが 0 にリセットされ、OSPF プロセスは **reset-time** キーワードで指定された期間、通常の動作状態のままとなります。

max-lsa コマンドの **warning-only** キーワードが設定されると、OSPF プロセスは LSA の最大値を超過していることを示す警告だけを送信します。

OSPF リンクステート データベース オーバーロード防止の設定方法

OSPF プロセスの自己生成 LSA 数の制限

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id*
4. **router-id***ip-address*
5. **log-adjacency-changes** [**detail**]
6. **max-lsa***maximum-number* [*threshold-percentage*] [**warning-only**] [**ignore-time***minutes*] [**ignore-count***count-number*] [**reset-time***minutes*]
7. **network***ip-addresswildcard-mask***area***area-id*
8. **end**
9. **showipospf**[*process-idarea-id*]**database**[**database-summary**]

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	**routerospf***process-id* 例： `Router(config)# router ospf 1`	OSPF ルーティングをイネーブルにします。 • *process-id* 引数は OSPF プロセスを示します。

	コマンドまたはアクション	目的
ステップ 4	**router-id***ip-address* 例： `Router(config-router)# router-id 10.0.0.1`	OSPF プロセスの固定ルータ ID を指定します。
ステップ 5	**log-adjacency-changes** [**detail**] 例： `Router(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	**max-lsa***maximum-number* [*threshold-percentage*] [**warning-only**] [**ignore-time***minutes*] [**ignore-count***count-number*] [**reset-time***minutes*] 例： `Router(config-router)# max-lsa 12000`	OSPF ルーティング プロセスが OSPF リンクステート データベース（LSDB）で保持できる非自己生成 LSA 数を制限します。
ステップ 7	**network***ip-addresswildcard-mask***area***area-id* 例： `Router(config-router)# network 209.165.201.1 255.255.255.255 area 0`	OSPF を実行するインターフェイスを定義し、それらのインターフェイスに対するエリア ID を定義します。
ステップ 8	**end** 例： `Router(config-router)# end`	現在の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 9	**showipospf**[*process-idarea-id*]**database**[**database-summary**] 例： `Router# show ip ospf 2000 database database-summary`	特定のルータの OSPF データベースに関連する情報のリストを表示します。 • ルータで非自己生成 LSA 数を確認するには、このコマンドを使用します。

例

showipospf コマンドに **database-summary** キーワードを指定して入力すると、ルータで実際の非自己生成 LSA 数を確認できます。このコマンドはいつでも使用でき、特定のルータに関する、OSPF データベースに関連する情報のリストが表示されます。

```
Router# show ip ospf 2000 database database-summary

            OSPF Router with ID (192.168.1.3) (Process ID 2000)
```

```
Area 0 database summary
  LSA Type      Count    Delete   Maxage
  Router        5        0        0
  Network       2        0        0
  Summary Net   8        2        2
  Summary ASBR  0        0        0
  Type-7 Ext    0        0        0
    Prefixes redistributed in Type-7  0
  Opaque Link   0        0        0
  Opaque Area   0        0        0
  Subtotal      15       2        2
Process 2000 database summary
  LSA Type      Count    Delete   Maxage
  Router        5        0        0
  Network       2        0        0
  Summary Net   8        2        2
  Summary ASBR  0        0        0
  Type-7 Ext    0        0        0
  Opaque Link   0        0        0
  Opaque Area   0        0        0
  Type-5 Ext    4        0        0
    Prefixes redistributed in Type-5  0
  Opaque AS     0        0        0
  Non-self      16
  Total         19       2        2
```

OSPF リンクステート データベース オーバーロード防止の設定例

LSA 生成制限の設定：例

ここでは、最大値の 14,000 を超過した場合、非自己生成 LSA をこれ以上受け入れないように設定されます。

```
Router(config)# router ospf 1
Router(config-router)# router-id 192.168.0.1
Router(config-router)# log-adjacency-changes
Router(config-router)# max-lsa 14000
Router(config-router)# area 33 nssa
Router(config-router)# network 192.168.0.1 0.0.0.0 area 1
Router(config-router)# network 192.168.5.1 0.0.0.0 area 1
Router(config-router)# network 192.168.2.1 0.0.0.0 area 0
```

ここでは、設定の確認に **show ip ospf** コマンドを入力してあります。

```
Router# show ip ospf 1
Routing Process "ospf 1" with ID 192.168.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Maximum number of non self-generated LSA allowed 14000
   Threshold for warning message 75%
   Ignore-time 5 minutes, reset-time 10 minutes
   Ignore-count allowed 5, current ignore-count 0
It is an area border and autonomous system boundary router
```

ここでは、ルータが ignore 状態のときに、**show ip ospf** コマンドが入力された場合の出力が示されています。

```
Router# show ip ospf 1
Routing Process "ospf 1" with ID 192.168.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Maximum number of non self-generated LSA allowed 14000
   Threshold for warning message 75%
   Ignore-time 5 minutes, reset-time 10 minutes
   Ignore-count allowed 5, current ignore-count 1
   Ignoring all neighbors due to max-lsa limit, time remaining: 00:04:52
It is an area border and autonomous system boundary router
```

ここでは、ルータが ignore 状態を終了後、**show ip ospf** コマンドが入力された場合の出力が示されています。

```
Router# show ip ospf 1
Routing Process "ospf 1" with ID 192.168.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Maximum number of non self-generated LSA allowed 14000
   Threshold for warning message 75%
   Ignore-time 5 minutes, reset-time 10 minutes
   Ignore-count allowed 5, current ignore-count 1 - time remaining: 00:09:51
It is an area border and autonomous system boundary router
```

ここでは、ignore 状態のままのルータに対して **show ip ospf** コマンドが入力された場合の出力が示されています。

```
Router# show ip ospf 1
Routing Process "ospf 1" with ID 192.168.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Maximum number of non self-generated LSA allowed 14000
   Threshold for warning message 75%
   Ignore-time 5 minutes, reset-time 10 minutes
   Ignore-count allowed 5, current ignore-count 6
   Permanently ignoring all neighbors due to max-lsa limit
It is an area border and autonomous system boundary router
```

その他の参考資料

ここでは、OSPF リンクステート データベース オーバーロード防止機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
『Configuring OSPF』	『Configuring OSPF』
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』

関連項目	マニュアル タイトル
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』

標準

規格	Title
なし	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
なし	--

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

OSPF リンクステート データベース オーバーロード防止の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *37* : *OSPF* リンクステート データベース オーバーロード防止の機能情報

機能名	リリース	機能情報
OSPF リンクステート データベース オーバーロードの防止	Cisco IOS XE Release 2.1	OSPF リンクステート データベース オーバーロード防止機能では、指定された OSPF プロセスの非自己生成のリンクステート アドバタイズメント（LSA）の数に制限を設けることができます。OSPF ドメイン内で他のルータによって生成された大量の LSA は、ルータの CPU およびメモリ リソースを大量に消費する可能性があります。 次に示すコマンドは、この章に記載されている機能において、新たに導入または変更されたものです。 • **max-lsa**

第 35 章

RFC 1850 の OSPF MIB サポートおよび最新の拡張

RFC 1850 の OSPF MIB サポートおよび最新の拡張機能では、Open Shortest Path First（OSPF）ルーティング プロトコルに、簡易ネットワーク管理プロトコル（SNMP）によるモニタリング機能が追加されます。MIB オブジェクトを使用すると、プロトコル パラメータに関連する情報や、移行ステート変更などの重大なネットワーク イベントの発生を示すトラップ通知オブジェクトを収集できます。これによって、OSPF ネットワークのステート変更を、より効果的な方法で常にモニタリングできるようになります。OSPF の MIB オブジェクトおよびトラップ オブジェクトによって収集したプロトコル情報からは、ネットワーク全体のパフォーマンスのモニタリングと改善に役立つ統計情報を生成できます。

- 機能情報の確認，359 ページ
- RFC 1850 の OSPF MIB サポートおよび最新の拡張の前提条件，360 ページ
- RFC 1850 の OSPF MIB サポートおよび最新の拡張について，360 ページ
- RFC 1850 の OSPF MIB サポートおよび最新の拡張をイネーブルにする方法，366 ページ
- RFC 1850 の OSPF MIB サポートおよび最新の拡張の設定例，371 ページ
- 次の作業，371 ページ
- その他の参考資料，371 ページ
- RFC 1850 の OSPF MIB サポートおよび最新の拡張の機能情報，373 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。

RFC 1850 の OSPF MIB サポートおよび最新の拡張の前提条件

- ルータで OSPF が設定されている必要があります。
- 通知（トラップ）の設定またはSNMP GET操作を行うには、簡易ネットワーク管理プロトコル（SNMP）を事前にイネーブルにする必要があります。

RFC 1850 の OSPF MIB サポートおよび最新の拡張について

ここでは、RFC 1850 の中で標準化され、OSPF-MIB および OSPF-TRAP-MIB で定義された、MIB オブジェクトについて説明します。また、シスコの2種類のプライベートMIB（CISCO-OSPF-MIB および CISCO-OSPF-TRAP-MIB）で定義される、RFC 1850 オブジェクトの拡張についても説明します。

RFC 1850 をサポートするための OSPF MIB の変更

OSPF MIB

ここでは、RFC 1850 の定義によって新しく追加された MIB オブジェクトについて説明します。これらの OSPF MIB 定義は、以前の RFC 1253 をサポートする標準 OSPF MIB にはなかった機能を、新しく提供します。すべての OSPF MIB オブジェクトを確認するには、OSPF-MIB ファイルを参照してください。

次の表に、RFC 1850 定義によって新しく追加された OSPF-MIB オブジェクトを示します。OSPF-MIB ファイルに記述されている順序で、オブジェクトが書き込まれるテーブルごとに示してあります。

表 *38*：新しい *OSPF-MIB* オブジェクト

OSPF-MIB のテーブル	新しい MIB オブジェクト
OspfAreaEntry テーブル	• OspfAreaSummary • OspfAreaStatus
OspfStubAreaEntry	• OspfStubMetricType

OSPF-MIB のテーブル	新しい MIB オブジェクト
OspfAreaRangeEntry	• OspfAreaRangeEffect
OspfHostEntry	• OspfHostAreaID
OspfIfEntry	• OspfIfStatus • OspfIfMulticastForwarding • OspfIfDemand • OspfIfAuthType
OspfVirtIfEntry	• OspfVirtIfAuthType
OspfNbrEntry	• OspfNbmaNbrPermanence • OspfNbrHelloSuppressed
OspfVirtNbrEntry	• OspfVirtNbrHelloSuppressed
OspfExtLsdbEntry	• OspfExtLsdbType • OspfExtLsdbLsid • OspfExtLsdbRouterId • OspfExtLsdbSequence • OspfExtLsdbAge • OspfExtLsdbChecksum • OspfExtLsdbAdvertisement
OspfAreaAggregateEntry	• OspfAreaAggregateAreaID • OspfAreaAggregateLsdbType • OspfAreaAggregateNet • OspfAreaAggregateMask • OspfAreaAggregateStatusospfSetTrap • OspfAreaAggregateEffect

OSPF トラップ MIB

ここでは、RFC 1850 をサポートするために追加されたスカラ オブジェクトおよび MIB オブジェクトについて説明します。

次のスカラ オブジェクトが OSPF-TRAP-MIB に追加されています。OSPF-TRAP-MIB ファイルに記述されている順序で示します。

- OspfExtLsdbLimit
- OspfMulticastExtensions
- OspfExitOverflowInterval
- OspfDemandExtensions

ospfSetTrap コントロール MIB オブジェクトには、IOS CLI で OSPF トラップのイネーブル化およびディセーブル化を行う OSPF トラップ MIB オブジェクトが含まれています。これらの OSPF トラップ MIB オブジェクトは、RFC 1850 の標準 OSPF MIB です。OSPF トラップをイネーブルまたはディセーブルにする方法については、RFC 1850 の OSPF MIB サポートおよび最新の拡張をイネーブルにする方法, （366 ページ）を参照してください。

次の表に、OSPF トラップ MIB オブジェクトを、OSPF-TRAP-MIB ファイルに記述されている順序で示します。

表 *39*：新しい *OSPF-TRAP-MIB* オブジェクト

OSPF コントロール MIB オブジェクト	トラップ MIB オブジェクト
ospfSetTrap	• ospfIfStateChange • ospfVirtIfStateChange • ospfNbrStateChange • ospfVirtNbrState • ospfIfConfigError • ospfVirtIfConfigError • ospfIfAuthFailure • ospfVirtIfAuthFailure • ospfIfRxBadPacket • ospfVirtIfRxBadPacket • ospfTxRetransmit • ospfVirtIfTxRetransmit • ospfOriginateLsa • ospfMaxAgeLsa

CISCO OSPF MIB

ここでは、スカラ オブジェクトと、シスコ固有の OSPF MIB オブジェクトについて説明します。これらは、RFC 1850 OSPF MIB 定義をサポートするための拡張であり、標準 MIB にはない機能を提供します。

次のスカラ オブジェクトが OSPF-OSPF-MIB に追加されています。

- cospfRFC1583Compatibility
- cospfOpaqueLsaSupport
- cospfOpaqueASLsaCount
- cospfOpaqueASLsaCksumSum

次に、テーブル エントリごとに、RFC 1850 OSPF MIB 定義をサポートするための拡張として追加された、シスコ固有の新しい MIB オブジェクトを示します。シスコ固有の全 OSPF MIB オブジェクトについては、CISCO-OSPF-MIB ファイルを参照してください。

次の表に、RFC 1850 定義によって新しく追加された CISCO-OSPF-MIB オブジェクトを示します。CISCO-OSPF-MIB ファイルに記述されている順序で、オブジェクトが書き込まれるテーブルごとに示してあります。

表 *40*：新しい *CISCO-OSPF-MIB* オブジェクト

CISCO-OSPF-MIB テーブル	新しい MIB オブジェクト
cospfAreaEntry	• cospfOpaqueAreaLsaCount • cospfOpaqueAreaLsaCksumSum • cospfAreaNssaTranslatorRole • cospfAreaNssaTranslatorState • cospfAreaNssaTranslatorEvents
cospfLsdbEntry	• cospfLsdbType • cospfLsdbSequence • cospfLsdbAge • cospfLsdbChecksum • cospfLsdbAdvertisement
cospfIfEntry	• cospfIfLsaCount • cospfIfLsaCksumSum

CISCO-OSPF-MIB テーブル	新しい MIB オブジェクト
cospfVirtIfEntry	• cospfVirtIfLsaCount • cospfVirtIfLsaCksumSum
cospfLocalLsdbEntry	• cospfLocalLsdbIpAddress • cospfLocalLsdbAddressLessIf • cospfLocalLsdbType • cospfLocalLsdbLsid • cospfLocalLsdbRouterId • cospfLocalLsdbSequence • cospfLocalLsdbAge • cospfLocalLsdbChecksum • cospfLocalLsdbAdvertisement
cospfVirtLocalLsdbEntry	• cospfVirtLocalLsdbTransitArea • cospfVirtLocalLsdbNeighbor • cospfVirtLocalLsdbType • cospfVirtLocalLsdbLsid • cospfVirtLocalLsdbRouterId • cospfVirtLocalLsdbSequence • cospfVirtLocalLsdbAge • cospfVirtLocalLsdbChecksum • cospfVirtLocalLsdbAdvertisement

CISCO OSPF トラップ MIB

cospfSetTrap MIB オブジェクトは、CISCO-OSPF-TRAP-MIB 内のトラップ イベントを表します。これはビットマップであり、最初のビットが最初のトラップを表します。次の MIB オブジェクトは、RFC 1850 をサポートするために追加されたトラップ イベントです。シスコの全 OSPF トラップ MIB オブジェクトについては、CISCO-OSPF-TRAP-MIB ファイルを参照してください。

次の図に、CISCO-TRAP-MIB 内の cospfSetTrap MIB オブジェクトに書き込まれるトラップ イベントを示します。

表 *41* : *CISCO-OSPF* トラップ イベント

CISCO-OSPF-TRAP-MIB トラップ イベント	トラップ イベントの説明
cospfIfConfigError	非仮想 OSPF ネイバーが隣接関係を確立する際に、MTU パラメータのミスマッチ エラーが発生した場合に生成されます。
cospfVirtIfConfigError	仮想 OSPF ネイバーが隣接関係を確立する際に、MTU パラメータのミスマッチ エラーが発生した場合に生成されます。
cospfTxRetransmit	非仮想インターフェイスから送信されたパケットが、不透明LSAである場合に生成されます。不透明リンクステート アドバタイズメント（LSA）は、ネットワークのリンクの容量やトポロジなどの属性を配信するときに、MPLS トラフィック エンジニアリングで使用されます。この LSA のスコープは、ローカル ネットワーク（タイプ 9、リンクローカル）、OSPF エリア（タイプ20、エリアローカル）、または自律システム（タイプ 11、AS スコープ）に限定できます。不透明 LSA の情報は、OSPF ネットワークで外部アプリケーションにより使用できます。
cospfVirtIfTxRetransmit	仮想インターフェイスから送信されたパケットが、不透明 LSA である場合に生成されます。
cospfOriginateLsa	トポロジに変化が生じた時に、ルータから不透明 LSA が送信された場合に生成されます。
cospfMaxAgeLsa	不透明 LSA の場合に生成されます。
cospfNssaTranslatorStatusChange	OSPF タイプ 7 の LSA を OSPF タイプ 5 の LSA に変換するルータの能力に変化が生じた場合に生成されます。

OSPF MIB トラップをイネーブルにする方法については、「RFC 1850 の OSPF MIB サポートおよび最新の拡張をイネーブルにする方法, （366 ページ）」を参照してください。

OSPF MIB の利点

以前の RFC 1253 OSPF MIB ではサポートされなかったテーブル オブジェクトやトラップ通知オブジェクトが新しく追加されたため、ネットワーク管理者は、OSPF MIB（OSPF-MIB と OSPF-TRAP-MIB）およびシスコのプライベート OSPF MIB（CISCO-OSPF-MIB と CISCO-OSPF-TRAP-MIB）を使用して、OSPF ルーティング プロトコルをより効果的にモニタリングできるようになりました。

OSPF MIB サポート オブジェクトや、シスコ固有のエラー、再送信、および状態変化のトラップに関する SNMP 通知をイネーブルにするために、CLI コマンドも新しく追加されています。SNMP 通知は、OSPF ネットワークのエラーや重大イベントに関する情報を提供します。

RFC 1850 の OSPF MIB サポートおよび最新の拡張をイネーブルにする方法

OSPF MIB サポートのイネーブル化

はじめる前に

RFC 1850 の OSPF MIB サポートおよび最新の拡張機能を使用する前に、ルータに対して SNMP サーバを設定しておく必要があります。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **snmp-servercommunity***string1***ro**
4. **snmp-servercommunity***string2***rw**
5. **snmp-serverhost** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
6. **snmp-serverenabletrapsospf**
7. **end**

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	**snmp-servercommunity***string1***ro** 例： `Router(config)# snmp-server community public ro`	MIB内の全オブジェクトに対する読み取りアクセス権をイネーブルにしますが、コミュニティ ストリングへのアクセスは許可しません。
ステップ 4	**snmp-servercommunity***string2***rw** 例： `Router(config)# snmp-server community private rw`	MIB 内の全オブジェクトに対する読み取りおよび書き込みアクセス権をイネーブルにしますが、コミュニティ ストリングへのアクセスは許可しません。
ステップ 5	**snmp-serverhost** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] 例： `Router(config)# snmp-server host 172.20.2.162 version 2c public ospf`	SNMP通知操作の受信者（ターゲットホスト）を指定します。 • *notification-type* が指定されていない場合は、イネーブルになっている全通知（トラップまたは応答要求）が、指定されたホストに送信されます。 • 指定されたホストに OSPF 通知だけを送信するには、オプションの **ospf** キーワードを *notification-types* の 1 つとして指定します（例を参照）。**ospf** キーワードを入力すると、ospfSetTrap トラップ コントロール MIB オブジェクトがイネーブルになります。
ステップ 6	**snmp-serverenabletrapsospf** 例： `Router(config)# snmp-server enable traps ospf`	OSPF MIB内に定義されている全SNMP通知をイネーブルにします。 （注） このステップが必要となるのは、全 OSPF トラップをイネーブルにする場合だけです。**no snmp-server enable traps ospf** コマンドを入力すると、全OSPF トラップがディセーブルになります。
ステップ 7	**end** 例： `Router(config)# end`	コンフィギュレーション セッションを終了し、グローバル コンフィギュレーション モードを終了します。

次の作業

一部のOSPFトラップだけをイネーブルにする場合は、次の項のステップに従い、1つまたは複数の OSPF トラップのタイプを選択してイネーブルにします。

特定の OSPF トラップのイネーブル化

手順の概要

1. イネーブル化
2. **configureterminal**
3. **snmp-serverenabletrapsospfcisco-specificerrors**[**config-error**] [**virt-config-error**]
4. **snmp-serverenabletrapsospfcisco-specificretransmit**[**packets**] [**virt-packets**]
5. **snmp-serverenabletrapsospfcisco-specificstate-change**[**nssa-trans-change**] [**shamlink-state-change**]
6. **snmp-serverenabletrapsospfcisco-specificlsa**[**lsa-maxage**] [**lsa-originate**]
7. **snmp-serverenabletrapsospferrors**[**authentication-failure**] [**bad-packet**] [**config-error**] [**virt-authentication-failure**] [**virt-config-error**]
8. **snmp-serverenabletrapsospflsa**[**lsa-maxage**] [**lsa-originate**]
9. **snmp-serverenabletrapsospfrate-limit***secondstrap-number*
10. **snmp-serverenabletrapsospfretransmit**[**packets**] [**virt-packets**]
11. **snmp-serverenabletrapsospfstate-change**[**if-state-change**] [**neighbor-state-change**] [**virtif-state-change**] [**virtneighbor-state-change**]

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	**snmp-serverenabletrapsospfcisco-specificerrors**[**config-error**] [**virt-config-error**] 例： `Router(config)# snmp-server enable traps ospf cisco-specific errors config-error`	シスコ固有の OSPF 設定ミスマッチ エラーに関する SNMP 通知をイネーブルにします。 • **snmp-server enable traps ospf cisco-specific errors** コマンドに、オプションの **virt-config-error** キーワードを指定して実行すると、仮想インターフェイスに関する設定ミスマッチ エラーの SNMP 通知だけがイネーブルになります。
ステップ 4	**snmp-serverenabletrapsospfcisco-specificretransmit**[**packets**] [**virt-packets**] 例： `Router(config)# snmp-server enable traps ospf cisco-specific retransmit packets virt-packets`	パケットの再送信に関するシスコ固有の OSPF エラーに対するエラー トラップをイネーブルにします。 • **snmp-server enable traps ospf cisco-specific retransmit** コマンドに、オプションの **virt-packets** キーワードを指定して実行すると、仮想インターフェイスに関する再送信パケットの SNMP 通知だけがイネーブルになります。
ステップ 5	**snmp-serverenabletrapsospfcisco-specificstate-change**[**nssa-trans-change**] [**shamlink-state-change**] 例： `Router(config)# snmp-server enable traps ospf cisco-specific state-change`	シスコ固有の OSPF 移行ステート変更に対する全エラー トラップをイネーブルにします。
ステップ 6	**snmp-serverenabletrapsospfcisco-specificlsa**[**lsa-maxage**] [**lsa-originate**] 例： `Router(config)# snmp-server enable traps ospf cisco-specific lsa`	不透明 LSA に対するエラー トラップをイネーブルにします。
ステップ 7	**snmp-serverenabletrapsospferrors**[**authentication-failure**] [**bad-packet**] [**config-error**] [**virt-authentication-failure**] [**virt-config-error**] 例： `Router(config)# snmp-server enable traps ospf errors virt-config-error`	OSPF 設定エラーに対するエラー トラップをイネーブルにします。 • **snmp-server enable traps ospf errors** コマンドに、オプションの **virt-config-error** キーワード

	コマンドまたはアクション	目的
		を指定して実行すると、仮想インターフェイスに関する OSPF 設定エラーの SNMP 通知だけがイネーブルになります。
ステップ 8	**snmp-serverenabletrapsospflsa**[**lsa-maxage**] [**lsa-originate**] 例： `Router(config)# snmp-server enable traps ospf lsa`	OSPF LSA エラーに対するエラー トラップをイネーブルにします。
ステップ 9	**snmp-serverenabletrapsospfrate-limit***secondstrap-number* 例： `Router(config)# snmp-server enable traps ospf rate-limit 20 20`	各 OSPF SNMP 通知のレート制限ウィンドウで、SNMP OSPF 通知の数に対するレート制限を設定します。
ステップ 10	**snmp-serverenabletrapsospfretransmit**[**packets**] [**virt-packets**] 例： `Router(config)# snmp-server enable traps ospf retransmit`	再送信パケットに関する SNMP OSPF 通知をイネーブルにします。
ステップ 11	**snmp-serverenabletrapsospfstate-change**[**if-state-change**] [**neighbor-state-change**] [**virtif-state-change**] [**virtneighbor-state-change**] 例： `Router(config)# snmp-server enable traps ospf state-change`	OSPF の移行ステート変更に関する SNMP OSPF 通知をイネーブルにします。

ルータ上の OSPF MIB トラップの確認

手順の概要

1. イネーブル化
2. **showrunning-config**[*options*]

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	**showrunning-config**[*options*] 例： `Router# show running-config | include traps`	現在の実行コンフィギュレーションファイルの内容を表示します。イネーブルになっているトラップに関する情報が含まれています。 • イネーブルになっているトラップを確認します。

RFC 1850 の OSPF MIB サポートおよび最新の拡張の設定例

例：OSPF MIB サポート トラップのイネーブル化と確認

次の例では、全 OSPF トラップをイネーブルにします。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# snmp-server enable traps ospf
Router(config)# end
```

show running-config コマンドを実行して、トラップがイネーブルになっていることを確認します。

```
Router# show running-config | include traps
snmp-server enable traps ospf
```

次の作業

SNMP および SNMP 操作の詳細については、『Cisco IOS XE Network Management Configuration Guide, *Release 2*』の「Configuring SNMP Support」の章を参照してください。

その他の参考資料

ここでは、OSPFv2 機能のインターフェイス モードにおけるエリア コマンドに関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
OSPF の設定タスク	Configuring OSPF モジュール

標準

規格	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 2328	『*OSPF Version 2*』

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

RFC 1850 の OSPF MIB サポートおよび最新の拡張の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *42*：*RFC 1850* の *OSPF MIB* サポートおよび最新の拡張の機能情報

機能名	リリース	機能情報
RFC 1850 の OSPF MIB サポートおよび最新の拡張	Cisco IOS XE Release 2.1	RFC 1850 の OSPF MIB サポートおよび最新の拡張機能では、Open Shortest Path First（OSPF）ルーティング プロトコルに、簡易ネットワーク管理プロトコル（SNMP）によるモニタリング機能が追加されます。MIB オブジェクトを使用すると、プロトコル パラメータに関連する情報や、移行ステート変更などの重大なネットワーク イベントの発生を示すトラップ通知オブジェクトを収集できます。これによって、OSPF ネットワークのステート変更を、より効果的な方法で常にモニタリングできるようになります。OSPF の MIB オブジェクトおよびトラップ オブジェクトによって収集したプロトコル情報からは、ネットワーク全体のパフォーマンスのモニタリングと改善に役立つ統計情報を生成できます。 次に示すコマンドは、この章に記載されている機能において、新たに導入または変更されたものです。 • **snmp-server enable traps ospf** • **snmp-server enable traps ospf cisco-specific errors** • **snmp-server enable traps ospf cisco-specific lsa** • **snmp-server enable traps ospf cisco-specific retransmit** • **snmp-server enable traps ospf cisco-specific state-change** • **snmp-server enable traps ospf errors** • **snmp-server enable traps ospf lsa** • **snmp-server enable traps ospf rate-limit** • **snmp-server enable traps ospf retransmit** • **snmp-server enable traps ospf state-change**

第 36 章

OSPF 拡張トラフィックの統計情報

ここでは、OSPFv2 および OSPFv3 の拡張 OSPF トラフィック統計情報を提供する、新しいコマンドと変更されたコマンドについて説明します。より詳細なトラフィック統計情報を収集して表示する機能によって、トラブルシューティングのプロセスが効率化され、OSPF ネットワークのアベイラビリティが向上します。

新しい OSPF トラフィック統計情報では、次の情報が収集され表示されるようになりました。

- OSPF Hello 入力キューおよび OSPF プロセス キューのステータス情報と統計情報
- グローバル OSPF トラフィック統計情報
- OSPF インターフェイス単位のトラフィック統計情報
- OSPF プロセス単位のトラフィック統計情報

- 機能情報の確認，377 ページ
- OSPF 拡張トラフィック統計情報の前提条件，378 ページ
- OSPF 拡張トラフィック統計情報について，378 ページ
- OSPF 拡張トラフィック統計情報を表示およびクリアする方法，378 ページ
- OSPF 拡張トラフィック統計情報の設定例，380 ページ
- その他の参考資料，384 ページ
- OSPF 拡張トラフィック統計情報の機能情報，385 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。

OSPF 拡張トラフィック統計情報の前提条件

ルータで OSPFv2 または OSPFv3 が設定されている必要があります。

OSPF 拡張トラフィック統計情報について

OSPF 拡張トラフィック統計情報はデフォルトでイネーブルになっています。ディセーブルにはできません。

詳細な OSPF トラフィック統計情報は、次のタイプの OSPF の不安定状態についてトラブルシューティングする際に特に役に立ちます。

- OSPF プロセスが、OSPF に対して送信されたトラフィック量を処理できるかどうかネットワーク管理者が判断する際に、OSPF プロセス キューのステータス情報および統計情報が役に立ちます。
- OSPF パケット ヘッダー エラーおよび LSA エラーに関する統計情報には、受信した OSPF パケットのなかに検出されたさまざまなエラーが記録されます。

また、OSPF 拡張トラフィック制御統計情報は、OSPF プロセス間で交換されるトラフィック制御の量をモニタします。低速リンクを使用し、かつ、トポロジ変化が頻繁に発生するネットワーク環境では、トラフィック制御の量は重要な考慮事項です。

OSPF拡張トラフィック統計情報を表示およびクリアする方法

OSPFv2 の OSPF トラフィック統計情報の表示とクリア

手順の概要

1. イネーブル化
2. **showipospf** [*process-id*] **traffic**[*interface-type interface-number*]
3. **clearipospftraffic**

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	**showipospf** [*process-id*] **traffic**[*interface-type interface-number*] 例： `Router# show ip ospf 10 traffic gigabitethernet 0/0/0`	OSPFv2 トラフィック統計情報を表示します。
ステップ 3	**clearipospftraffic** 例： `Router# clear ip ospf traffic`	OSPFv2 トラフィック統計情報をクリアします。

OSPFv3 の OSPF トラフィック統計情報の表示とクリア

手順の概要

1. イネーブル化
2. **showipv6ospf**[*process-id*] **traffic**[*interface-type interface-number*]
3. **clearipv6ospftraffic**

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	**showipv6ospf**[*process-id*] **traffic**[*interface-type interface-number*]	OSPFv3 トラフィック統計情報を表示します。

	コマンドまたはアクション	目的
	例： `Router# show ipv6 ospf traffic`	
ステップ 3	**clearipv6ospftraffic** 例： `Router# clear ipv6 ospf traffic`	OSPFv3 トラフィック統計情報をクリアします。

OSPF 拡張トラフィック統計情報の設定例

例：OSPFv2 の拡張トラフィック統計情報の表示とクリア

次の例は、OSPFv2 の **show ip ospf traffic** コマンドの出力を示しています。

```
Router# show ip ospf traffic
OSPF statistics:
 Rcvd: 55 total, 0 checksum errors
        22 hello, 7 database desc, 2 link state req
        6 link state updates, 6 link state acks
  Sent: 68 total
        45 hello, 7 database desc, 2 link state req
        10 link state updates, 4 link state acks
            OSPF Router with ID (10.1.1.1) (Process ID 8)
OSPF queues statistic for process ID 8:
  OSPF Hello queue size 0, no limit, drops 0, max size 0
  OSPF Router queue size 0, limit 200, drops 0, max size 0
Interface statistics:
    Interface GigabitEthernet0/0/1
OSPF packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      0                    0
  RX DB des     0                    0
  RX LS req     0                    0
  RX LS upd     0                    0
  RX LS ack     0                    0
  RX Total      0                    0
  TX Failed     0                    0
  TX Hello      16                   1216
  TX DB des     0                    0
  TX LS req     0                    0
  TX LS upd     0                    0
  TX LS ack     0                    0
  TX Total      16                   1216
OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 0,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, Hello 0,
  MTU Mismatch 0, Nbr Ignored 0, LLS 0,
  Authentication 0,
```

```
OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
Summary traffic statistics for process ID 8:
OSPF packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      0                    0
  RX DB des     0                    0
  RX LS req     0                    0
  RX LS upd     0                    0
  RX LS ack     0                    0
  RX Total      0                    0
  TX Failed     0                    0
  TX Hello      16                   1216
  TX DB des     0                    0
  TX LS req     0                    0
  TX LS upd     0                    0
  TX LS ack     0                    0
  TX Total      16                   1216
OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 0,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, Hello 0,
  MTU Mismatch 0, Nbr Ignored 0, LLS 0,
  Authentication 0,
OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
           OSPF Router with ID (10.1.1.4) (Process ID 1)
OSPF queues statistic for process ID 1:
  OSPF Hello queue size 0, no limit, drops 0, max size 2
  OSPF Router queue size 0, limit 200, drops 0, max size 2
Interface statistics:
    Interface Serial2/0/0
OSPF packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      11                   528
  RX DB des     4                    148
  RX LS req     1                    60
  RX LS upd     3                    216
  RX LS ack     2                    128
  RX Total      21                   1080
  TX Failed     0                    0
 TX Hello      14                   1104
  TX DB des     3                    252
  TX LS req     1                    56
  TX LS upd     3                    392
  TX LS ack     2                    128
  TX Total      23                   1932
OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 0,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, Hello 0,
  MTU Mismatch 0, Nbr Ignored 0, LLS 0,
  Authentication 0,
OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
    Interface GigabitEthernet0/0/0
OSPF packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      13                   620
  RX DB des     3                    116
  RX LS req     1                    36
  RX LS upd     3                    228
  RX LS ack     4                    216
  RX Total      24                   1216
  TX Failed     0                    0
  TX Hello      17                   1344
  TX DB des     4                    276
  TX LS req     1                    56
  TX LS upd     7                    656
  TX LS ack     2                    128
```

```
  TX Total      31                  2460
OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 13,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, Hello 0,
  MTU Mismatch 0, Nbr Ignored 0, LLS 0,
  Authentication 0,
OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,

Summary traffic statistics for process ID 1:
OSPF packets received/sent
  Type          Packets             Bytes
  RX Invalid    0                   0
  RX Hello      24                  1148
  RX DB des     7                   264
  RX LS req     2                   96
  RX LS upd     6                   444
  RX LS ack     6                   344
  RX Total      45                  2296
  TX Failed     0                   0
  TX Hello      31                  2448
  TX DB des     7                   528
  TX LS req     2                   112
  TX LS upd     10                  1048
  TX LS ack     4                   256
  TX Total      54                  4392
OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 13,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, Hello 0,
  MTU Mismatch 0, Nbr Ignored 0, LLS 0,
  Authentication 0,
OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
```

ネットワーク管理者は **clear ip ospf traffic** コマンドを実行して、すべてのカウンタをリセットし、すべての統計情報の収集を再起動できます。

```
Router# clear ip ospf traffic
```

例：OSPFv3 の拡張トラフィック統計情報の表示とクリア

次の例は、OSPFv3 の **show ipv6 ospf traffic** コマンドの出力を示しています。

```
Router# show ipv6 ospf traffic

OSPFv3 statistics:
  Rcvd: 32 total, 0 checksum errors
        10 hello, 7 database desc, 2 link state req
        9 link state updates, 4 link state acks
        0 LSA ignored
  Sent: 45 total, 0 failed
        17 hello, 12 database desc, 2 link state req
        8 link state updates, 6 link state acks
            OSPFv3 Router with ID (10.1.1.4) (Process ID 6)
OSPFv3 queues statistic for process ID 6
  Hello queue size 0, no limit, max size 2
  Router queue size 0, limit 200, drops 0, max size 2
Interface statistics:
    Interface Serial2/0/0
OSPFv3 packets received/sent
  Type          Packets             Bytes
  RX Invalid    0                   0
  RX Hello      5                   196
  RX DB des     4                   172
  RX LS req     1                   52
  RX LS upd     4                   320
```

```
  RX LS ack     2                   112
  RX Total      16                  852
  TX Failed     0                   0
  TX Hello      8                   304
  TX DB des     3                   144
  TX LS req     1                   52
  TX LS upd     3                   252
  TX LS ack     3                   148
  TX Total      18                  900
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
Interface GigabitEthernet0/0/0
OSPFv3 packets received/sent
  Type          Packets             Bytes
  RX Invalid    0                   0
  RX Hello      6                   240
  RX DB des     3                   144
  RX LS req     1                   52
  RX LS upd     5                   372
  RX LS ack     2                   152
  RX Total      17                  960
  TX Failed     0                   0
  TX Hello      11                  420
  TX DB des     9                   312
  TX LS req     1                   52
  TX LS upd     5                   376
  TX LS ack     3                   148
  TX Total      29                  1308
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
Summary traffic statistics for process ID 6:
OSPFv3 packets received/sent
  Type          Packets             Bytes
  RX Invalid    0                   0
  RX Hello      11                  436
  RX DB des     7                   316
  RX LS req     2                   104
  RX LS upd     9                   692
  RX LS ack     4                   264
  RX Total      33                  1812
  TX Failed     0                   0
  TX Hello      19                  724
  TX DB des     12                  456
  TX LS req     2                   104
  TX LS upd     8                   628
  TX LS ack     6                   296
  TX Total      47                  2208
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
```

ネットワーク管理者は **clear ipv6 ospf traffic** コマンドを実行して、すべてのカウンタをリセットし、すべての統計情報の収集を再起動できます。

```
Router# clear ipv6 ospf traffic
```

その他の参考資料

ここでは、OSPF 模造リンク MIB サポート機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
OSPF 模造リンクの設定	MPLS VPN のための OSPF 模造リンクのサポート
SNMP コンフィギュレーション	『*Cisco IOS Network Management Configuration Guide*』
SNMP コマンド	『*Cisco IOS Network Management Command Reference*』

標準

規格	Title
なし	--

MIB

MIB	MIB のリンク
• CISCO-OSPF-MIB • CISCO-OSPF-TRAP-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
なし	--

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、Cisco.com でまず登録手続きを行ってください。	http://www.cisco.com/en/US/support/index.html

OSPF 拡張トラフィック統計情報の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *43* : *OSPFv2* および *OSPFv3* の *OSPF* 拡張トラフィック統計情報の機能情報

機能名	リリース	機能情報
OSPFv2 および OSPFv3 の OSPF 拡張トラフィック統計情報	Cisco IOS XE Release 2.1	このマニュアルでは、新しいコマンドまたは変更されたコマンドである、OSPFv2 および OSPFv3 の show コマンドを実行して得られる、詳細な OSPF トラフィック統計情報について説明します。 次に示すコマンドは、この章に記載されている機能において、新たに導入または変更されたものです。 • **clearipv6ospftraffic** • **showipospftraffic** • **showipv6ospftraffic**

第 37 章

IPv6 での OSPFv3 の TTL セキュリティ サポート

IPv6 機能での Open Shortest Path First バージョン 3（OSPFv3）の存続可能時間（TTL）セキュリティ サポートにより、OSPFv3 サービス妨害攻撃に対する保護が強化されます。

- 機能情報の確認，387 ページ
- IPv6 での OSPFv3 の TTL セキュリティ サポートの制約事項，388 ページ
- IPv6 での OSPFv3 の TTL セキュリティ サポートの前提条件，388 ページ
- IPv6 での OSPFv3 の TTL セキュリティ サポートについて，388 ページ
- IPv6 での OSPFv3 の TTL セキュリティ サポートの設定方法，389 ページ
- IPv6 での OSPFv3 の TTL セキュリティ サポートの設定例，392 ページ
- その他の参考資料，393 ページ
- IPv6 での OSPFv3 の TTL セキュリティ サポートの機能情報，394 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。

IPv6 での OSPFv3 の TTL セキュリティ サポートの制約事項

- OSPFv3 TTL セキュリティは、仮想リンクおよび模造リンクに対してのみ設定できます。
- OSPFv3 TTL セキュリティは、IPv6 アドレス ファミリ コンフィギュレーション モード（config-router）で設定する必要があります。IPv6 アドレス ファミリ コンフィギュレーション モードを開始するには、**address-family ipv6** コマンドを使用します。
- 模造リンクは、デフォルトの Virtual Routing and Forwarding（VRF）では設定できません。

IPv6 での OSPFv3 の TTL セキュリティ サポートの前提条件

IPv6 での OSPFv3 の TTL セキュリティ サポート機能は、OSPFv3 ルーティング機能のあるプラットフォームでのみ使用できます。

IPv6 での OSPFv3 の TTL セキュリティ サポートについて

仮想および模造リンクの OSPFv3 TTL セキュリティ サポート

OSPFv3 では、すべてのエリアはバックボーンエリアに接続している必要があります。バックボーンが不連続である場合、またはバックボーンが意図的に分割されている場合は、仮想リンクを確立できます。仮想リンクは、分割されたバックボーンを接続するために使用する 2 つのデバイスで設定する必要があります。各デバイスの設定情報には、他の仮想エンドポイント（他のエリア境界ルータ（ABR））、および 2 台のデバイスに共通する非バックボーン エリア（中継エリア）があります。仮想リンクはスタブ エリアからは設定できません。模造リンクは多くの点で仮想リンクに似ていますが、模造リンクは MPLS バックボーン経由でプロバイダー エッジ（PE）ルータを接続するためにレイヤ 3 マルチプロトコル ラベル スイッチング（MPLS）VPN ネットワークで使用されます。

（注） 仮想リンクや模造リンクなどのマルチホップ隣接関係ではグローバル IPv6 アドレスを使用するため、パケットが通過できるホップ数を制御するように TTL セキュリティを設定する必要があります。

TTL セキュリティを有効にする場合、OSPFv3 は IP ヘッダーの TTL 値が 255 の発信パケットを送信し、TTL 値が設定可能なしきい値未満の着信パケットを廃棄します。IP パケットを転送する各

デバイスが TTL 値を減らすため、直接（1 ホップ）接続で受信したパケットの値は 255 になります。2つのホップを通過するパケットの値は254というようになります。受信しきい値は、パケットが移動する可能性がある最大ホップ数で設定されます。この *hop-count* 引数の値は 1 ～ 254 の数であり、デフォルトは 1 です。

仮想リンクまたは模造リンクを確立するには、それぞれ **areavirtual-link** または **areasham-linkcost** コマンドを使用します。仮想リンクまたは模造リンクで TTL セキュリティを設定するには、いずれかのコマンドで **ttl-security** キーワードおよび *hop-count* 引数を設定します。この場合、*hop-count* 引数値は必須です。

（注） OSPFv3 TTL セキュリティは仮想リンクおよび模造リンクのみで設定でき、IPv6 アドレス ファミリのアドレス ファミリ コンフィギュレーション（config-router-af）モードで設定する必要があります。

IPv6 での OSPFv3 の TTL セキュリティ サポートの設定方法

IPv6 での OSPFv3 の仮想リンクに対する TTL セキュリティ サポートの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospfv3**[*process-id*]
4. **address-familyipv6unicastvrf** *vrf-name*
5. **area***area-ID***virtual-link***router-id***ttl-securityhops***hop-count*
6. **end**

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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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	**routerospfv3**[*process-id*] 例： `Device(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリのルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**address-familyipv6unicastvrf** *vrf-name* 例： `Device(config-router)# address-family ipv6 unicast vrf vrf1`	OSPFv3 のアドレス ファミリ コンフィギュレーション モードを開始し、IPv6 ユニキャスト アドレス プレフィックスを指定し、後でアドレス ファミリ コンフィギュレーション モード コマンドに関連付けるために VRF インスタンスの名前を指定してます。
ステップ 5	**area***area-ID***virtual-link***router-id***ttl-securityhops***hop-count* 例： `Device(config-router-af)# area 1 virtual-link 10.1.1.1 ttl-security hops 10`	OSPFv3 仮想リンクを定義し、仮想リンクの TTL セキュリティを設定します。
ステップ 6	**end** 例： `Device(config-router-af)# end`	（任意）特権 EXEC モードに戻ります。

IPv6 での OSPFv3 の模造リンクに対する TTL セキュリティ サポートの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospfv3**[*process-id*]
4. **address-familyipv6unicastvrf** *vrf-name*
5. **area***area-id***sham-link** *source-address destination-address***ttl-securityhops***hop-count*
6. **end**

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	**configureterminal** 例： `Device# 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	**routerospfv3**[*process-id*] 例： `Device(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**address-familyipv6unicastvrf** *vrf-name* 例： `Device(config-router)# address-family ipv6 unicast vrf vrf1`	OSPFv3 のアドレス ファミリ コンフィギュレーション モードを開始し、IPv6ユニキャストアドレスプレフィックスを指定し、後でアドレス ファミリ コンフィギュレーション モード コマンドに関連付けるために VRF インスタンスの名前を指定してます。
ステップ 5	**area***area-id***sham-link** *source-address destination-address***ttl-securityhops***hop-count* 例： `Device(config-router-af)# area 1 sham-link 2001:DB8:1::1`	OSPFv3 模造リンクを定義し、模造リンクの TTL セキュリティを設定します。

	コマンドまたはアクション	目的
	2001:DB8:0:A222::2 ttl-security hops 10	
ステップ 6	**end** 例： Device(config-router-af)# end	（任意）特権 EXEC モードに戻ります。

IPv6 での OSPFv3 の TTL セキュリティ サポートの設定例

例：IPv6 での OSPFv3 の仮想リンクに対する TTL セキュリティ サポート

次に、仮想リンク TTL セキュリティを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# router ospfv3 1
Device(config-router)# address-family ipv6 unicast vrf vrf1
Device(config-router-af)# area 1 virtual-link 10.1.1.1 ttl-security hops 10
Device(config-router-af)# end
Device# show ospfv3 virtual-links
OSPFv3 1 address-family ipv6 (router-id 10.1.1.7)
Virtual Link OSPFv3_VL0 to router 10.1.1.2 is down
  Interface ID 23, IPv6 address ::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 1, Cost of using 65535
  Transmit Delay is 1 sec, State DOWN,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Strict TTL checking enabled, up to 10 hops allowed
```

例：IPv6 での OSPFv3 の模造リンクに対する TTL セキュリティ サポート

次に、模造リンク TTL セキュリティを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# router ospfv3 1
Device(config-router)# address-family ipv6 unicast vrf vrf1
Device(config-router-af)# area 1 sham-link 2001:DB8:1::1 2001:DB8:0:A222::2 ttl-security
hops 10
Device(config-router-af)# end
Device#
```

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』
OSPF コマンド	『Cisco IOS IP Routing: OSPF Command Reference』
IPv6 ルーティング：OSPFv3	IPv6 Routing: OSPFv3 モジュール

MIB

MIB	MIB のリンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

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

IPv6 での OSPFv3 の TTL セキュリティ サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *44*：*IPv6* での *OSPFv3* の *TTL* セキュリティ サポート

機能名	ソフトウェア リリース	機能情報
IPv6 での OSPFv3 の TTL セキュリティ サポート	Cisco IOS XE Release 3.7S	IPv6 での OSPFv3 の TTL セキュリティ サポート機能により、OSPFv3 サービス妨害攻撃に対する保護を強化が強化されます。 この機能により次のコマンドが導入または変更されました。**area sham-link**、**area virtual-link**

第 38 章

OSPF TTL セキュリティ チェックと OSPF グレースフル シャットダウンの設定

ここでは、Open Shortest Path First（OSPF）などのさまざまなオプションを設定する設定タスクについて説明します。このモジュールには、コマンドを使用して、OSPF セッションを CPU 使用率ベースの攻撃から保護する軽量のセキュリティ メカニズムを設定するタスクと、プロトコル設定を失うことなくプロトコルを一時的にシャットダウンするようにルータを設定するタスクが含まれます。

- 機能情報の確認，395 ページ
- OSPF TTL セキュリティ チェックと OSPF グレースフル シャットダウンについて，396 ページ
- OSPF TTL セキュリティ チェックと OSPF グレースフル シャットダウンの設定方法，398 ページ
- OSPF TTL セキュリティ チェックおよび OSPF グレースフル シャットダウンの設定例，403 ページ
- その他の参考資料，403 ページ
- OSPF TTL セキュリティ チェックおよびOSPF グレースフル シャットダウンの機能情報，405 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。

OSPF TTL セキュリティ チェックと OSPF グレースフル シャットダウンについて

OSPF の TTL セキュリティ チェック

TTL セキュリティ チェック機能がイネーブルになっている場合、OSPF は、IP ヘッダー存続可能時間（TTL）の値が 255 の発信パケットを送信し、設定可能なしきい値よりも低い TTL 値の入力パケットを廃棄します。IP パケットを転送する各デバイスは TTL が低下するため、直接（1 ホップ）接続により受信されたパケットの TTL 値は 255 になります。2 つのホップを通過するパケットの値は254というようになります。受信しきい値は、パケットが移動する可能性がある最大ホップ数で設定されます。この *hop-count* 引数の値は 1 ～ 254 の数であり、デフォルトは 1 です。

TTL セキュリティ チェック機能は、OSPF ルータ サブモードで設定する（この場合は OSPF が実行されるすべてのインターフェイスに適用される）か、またはインターフェイスごとに設定することができます。

TTL セキュリティ チェックを使用するための既存ネットワークの移行

ネットワークで現在 OSPF が実行されている場合に、ネットワークを停止せずにインターフェイスごとに TTL セキュリティを実装するには、**ipospfttl-security** コマンドを使用して引数 hop-count を 254 に設定します。この設定により、発信パケットは TTL 値 255 で送信されますが、着信パケットについてはいずれの値も許可されません。リンクの反対側のデバイスで TTL セキュリティが有効になると、その後は、ホップ カウントを指定せずに **ipospfttl-security** を使用することにより、着信パケットにホップ リミットを適用できるようになります。このプロセスにより、TTL セキュリティの一時的な不一致が原因で OSPF パケットがドロップされることがなくなります。

OSPF 仮想リンクおよび模造リンクの TTL セキュリティ チェック

OSPF では、すべてのエリアがバックボーンエリアに接続されている必要があります。バックボーンが不連続である場合、またはバックボーンが意図的に分割されている場合は、仮想リンクを確立できます。仮想リンクは両方のデバイスで設定される必要があります。各デバイスの設定情報には、他の仮想エンドポイント（他のエリア境界ルータ（ABR））、および 2 台のデバイスに共通する非バックボーンエリア（中継エリア）があります。仮想リンクはスタブエリアからは設定できません。模造リンクは多くの点で仮想リンクに似ていますが、模造リンクは、レイヤ 3 マルチプロトコル ラベル スイッチング（MPLS）のバーチャル プライベート ネットワーク（VPN）で使用されて、MPLS バックボーンを通じてプロバイダー エッジ（PE）ルータを接続します。

仮想リンクまたは模造リンクを確立するには、ルータ コンフィギュレーション モードで、**areavirtual-link** または **areasham-linkcost** コマンドをそれぞれ使用します。仮想リンクまたは模造リンクで TTL セキュリティ チェック機能を設定するには、それぞれのコマンドで、**ttl-security** キーワードおよび *hop-count* 引数を設定します。この場合、*hop-count* 引数値は必須です。

TTL セキュリティ チェックに対する OSPF サポートの利点

TTL セキュリティ チェックに対する OSPF サポート機能は、OSPF ネイバー セッションを CPU 利用率に基づく攻撃から防御する、効果的で容易に導入できるソリューションを提供します。この機能がイネーブルの場合、ホストがローカル OSPF ネットワークまたはリモート OSPF ネットワークのメンバでない場合、あるいはホストがローカル OSPF ネットワークとリモート OSPF ネットワークの間のネットワーク セグメントに直接接続されていない場合、ホストは OSPF セッションを攻撃できません。このソリューションは、OSPF 自律システムへのサービス妨害（DoS）攻撃の効果を大幅に軽減します。

OSPF グレースフル シャットダウン

OSPF グレースフル シャットダウン機能では、可能な限り安全な方法で OSPF プロトコルを一時的にシャットダウンして、これをネイバーに通知する機能を提供します。ネットワークに別のパスがあるすべてのトラフィックは、その代替パスに送信されます。OSPF プロトコルのグレースフル シャットダウンは、ルータ コンフィギュレーション モードで **shutdown** コマンドを使用して実行できます。

この機能は、特定のインターフェイスで OSPF をシャットダウンする機能も提供します。この場合、OSPF はインターフェイスをアドバタイズせず、インターフェイスを介して隣接関係を形成しません。ただし、すべての OSPF インターフェイス設定が保持されます。インターフェイスのグレースフル シャットダウンを実行するには、インターフェイス コンフィギュレーション モードで **ip ospf shutdown** コマンドを使用します。

OSPF TTL セキュリティ チェックと OSPF グレースフル シャットダウンの設定方法

すべての OSPF インターフェイスでの TTL セキュリティ チェックの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id*
4. **ttl-securityall-interfaces** [**hops***hop-count*]
5. **end**

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	**configureterminal** 例： `Device# 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	**routerospf***process-id* 例： `Device(config)# router ospf 109`	OSPF ルーティングをイネーブルにします。これにより、デバイスはルータ コンフィギュレーション モードに設定されます。
ステップ 4	**ttl-securityall-interfaces** [**hops***hop-count*] 例： `Device(config-router)# ttl-security all-interfaces`	すべての OSPF インターフェイスでの TTL セキュリティ チェックを設定します。 （注） この設定手順は、通常の OSPF インターフェイスだけに適用されます。TTL セキュリティ保護を必要とする仮想リンクまたは模造リンクには適用されません。仮想リンクと模造リンクは個別に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 5	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。

インターフェイス単位での TTL セキュリティ チェックの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipospfttl-security**[**hops***hop-count* | **disable**]
5. **end**
6. **showipospf** [*process-id*] **interface**[*interfacetypeinterface-number*] [**brief**] [**multicast**] [**topology** *topology-name* |**base**}]
7. **showipospfneighbor***interface-typeinterface-number* [*neighbor-id*][**detail**]
8. **showipospf** [*process-id*] **traffic** [*interface-typeinterface-number*]
9. **debugipospfadj**

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	**configureterminal** 例： `Device# 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	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipospfttl-security**[**hops***hop-count* | **disable**] 例： `Device(config-if)# ip ospf ttl-security`	特定のインターフェイスに対しTTLセキュリティチェック機能を設定します。 • 引数 *hop-count* の範囲は 1 ～ 254 です。 • **disable** キーワードを使用して、インターフェイスの TTL セキュリティをディセーブルにすることができます。これは、**ttl-securityall-interfaces** コマンドによってすべてのOSPFインターフェイスのTTLセキュリティが最初にイネーブルになっている場合のみ有効です。この場合、**disable** は、オーバーライドとして、または特定のインターフェイスの TTL セキュリティをオフにするために使用できます。 • 例では、TTL セキュリティはギガビット イーサネット インターフェイス 0/0/0 上でディセーブルになっています。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**showipospf** [*process-id*] **interface**[*interfacetypeinterface-number*] [**brief**] [**multicast**] [**topology** *topology-name* |**base**}] 例： `Device# show ip ospf interface gigabitethernet 0/0/0`	（任意）OSPF 関連のインターフェイス情報を表示します。
ステップ 7	**showipospfneighbor***interface-typeinterface-number* [*neighbor-id*][**detail**] 例： `Device# show ip ospf neighbor 10.199.199.137`	（任意）OSPF ネイバー情報をインターフェイスごとに表示します。 • 接続の一方の側にイネーブルの TTL セキュリティがある場合、もう一方の側には INIT 状態のネイバーが表示されます。

	コマンドまたはアクション	目的
ステップ 8	**showipospf** [*process-id*] **traffic** [*interface-typeinterface-number*] 例： `Device# show ip ospf traffic`	（任意）OSPF トラフィック統計情報を表示します。 • TTL セキュリティ チェックが失敗した回数が出力に表示されます。
ステップ 9	**debugipospfadj** 例： `Device# debug ip ospf adj`	（任意）OSPF 隣接イベントのデバッグを開始します。 • ドロップされたパケットに関する情報（インターフェイスのタイプと番号、ネイバー IP アドレス、TTL 値など）が、コマンドの出力に表示されます。

インターフェイス単位での OSPF グレースフル シャットダウンの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipospfshutdown**
5. **end**
6. **showipospf[***process-id***]interface[***interfacetypeinterface-number***][brief/** [**multicast**] [**topology***topology-name*|**base**}]
7. **showipospf[***process-id***]**

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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet 0/1/0`	インターフェイスのタイプと番号を設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipospfshutdown** 例： `Device(config-if)# ip ospf shutdown`	インターフェイス レベルで OSPF プロトコル グレースフル シャットダウンを開始します。 • **ipospfshutdown** インターフェイス コマンドを入力すると、これを設定したインターフェイスは、停止しようとしているネイバーをアドバイスするリンクステート アップデートを送信します。これにより、ネイバーは、このルータを含む OSPF トラフィックをルーティングできるようになります。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**showipospf[***process-id***]interface[***interfacetypeinterface-number***][brief]** [**multicast**] [**topology***topology-name*|**base**}]] 例： `Device# show ip ospf interface GigabitEthernet 0/1/0`	（任意）OSPF 関連のインターフェイス情報を表示します。
ステップ 7	**showipospf[***process-id***]** 例： `Device# show ip ospf`	（任意）OSPF ルーティング プロセスに関する一般情報を表示します。

OSPF TTL セキュリティ チェックおよび OSPF グレースフル シャットダウンの設定例

例：TTL セキュリティ チェックを使用するための既存ネットワークの移行

次に、既存の OSPF ネットワークで TTL セキュリティをインターフェイス単位でイネーブルする例を示します。

既存のネットワークでの TTL セキュリティの設定手順は、次の 3 ステップからなります。

1. 送信側デバイスの OSPF インターフェイスで、ホップ カウントを 254 に指定して TTL セキュリティを設定します。
2. 送信側デバイスの OSPF インターフェイスで、ホップ カウントなしで TTL セキュリティを設定します。
3. 送信側の OSPF インターフェイスをホップ カウントなしで再設定します。

```
configure terminal
 ! Configure the following command on the sending side router.
 interface gigabitethernet 0/1/0
  ip ospf ttl-security hops 254
 ! Configure the next command on the receiving side router.
 interface gigabitethernet 0/1/0
  ip ospf ttl-security
 ! Reconfigure the sending side with no hop count.
  ip ospf ttl-security
  end
```

その他の参考資料

ここでは、OSPF TTL セキュリティ チェックおよび OSPF グレースフル シャットダウン機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
『Configuring OSPF』	『Configuring OSPF』
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』

標準

規格	Title
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	--

MIB

MIB	MIB のリンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、 ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	--

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

OSPF TTL セキュリティ チェックおよび OSPF グレースフル シャットダウンの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *45*：*OSPF TTL* セキュリティ チェックおよび *OSPF* グレースフル シャットダウンの機能情報

機能名	リリース	機能情報
OSPF グレースフル シャットダウン	Cisco IOS XE Release 2.1	この機能により、可能な限り安全な方法でプロトコルを一時的にシャットダウンして、これをネイバーに通知することができます。 プロトコルのグレースフル シャットダウンは、すべての OSPF インターフェイス、または特定のインターフェイスで開始できます。 次のコマンドが導入または変更されました。 • **ipospfshutdown** • **showipospf** • **showipospfinterface** • **shutdown(routerOSPF)**

機能名	リリース	機能情報
OSPF TTL セキュリティ チェック	Cisco IOS XE Release 2.1	この機能により、OSPF サービス妨害攻撃に対する保護を強化し、ネイバーからの OSPF パケット上の TTL 値をチェックして、ネイバーに送信される TTL 値をユーザが設定できるようになります。 次のコマンドが導入または変更されました。 • **areasham-linkcost** • **areavirtual-link** • **debugipospfadj** • **ipospfttl-security** • **showipospfinterface** • **showipospfneighbor** • **showipospftraffic** • **ttl-securityall-interfaces**

第 39 章

OSPF 模造リンク MIB サポート

この機能では、新しいテーブルおよびトラップ MIB オブジェクトを Cisco OSPF MIB（CISCO-OSPF-MIB）および Cisco OSPF Trap MIB（CISCO-OSPF-TRAP-MIB）に追加することにより、OSPF 模造リンク機能の MIB サポートが導入されます。また、Open Shortest Path First（OSPF）模造リンク トラップ オブジェクトの簡易ネットワーク管理プロトコル（SNMP）通知をイネーブルにするための、新しいコマンドが追加されています。模造リンク インターフェイス全体におけるエラー、ステート変更、および再送信についての通知が提供されます。

- 機能情報の確認，407 ページ
- OSPF 模造リンク MIB サポートの前提条件，408 ページ
- OSPF 模造リンク MIB サポートの制約事項，408 ページ
- OSPF 模造リンク MIB サポートに関する情報，408 ページ
- OSPF 模造リンク MIB サポートの設定方法，411 ページ
- OSPF 模造リンク MIB サポートの設定例，417 ページ
- 次の作業，419 ページ
- その他の参考資料，419 ページ
- OSPF 模造リンク MIB サポートの機能情報，421 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。

OSPF 模造リンク MIB サポートの前提条件

- OSPF 模造リンクをすでに設定済みであることが前提になります。
- 通知（トラップ）の設定、またはSNMP GET動作を実行するルータで、SNMPがイネーブルになっている必要があります。

OSPF 模造リンク MIB サポートの制約事項

この機能によって導入されるすべての拡張機能は、Cisco プライベート MIB（CISCO-OSPF-MIB および CISCO-OSPF-TRAP-MIB）によってのみ提供されます。

OSPF 模造リンク MIB サポートに関する情報

PE-PE 間ルータ接続における OSPF 模造リンク

マルチプロトコルラベルスイッチング（MPLS）バーチャルプライベートネットワーク（VPN）設定では、模造リンクと呼ばれる仮想接続を設定することにより、同じ OSPF エリア内にある必要がある2つのVPNサイトを相互接続できます。模造リンクは、2つのプロバイダーエッジ（PE）ルータを接続する MPLS VPN トンネルに加えて設定します。OSPF パケットは、模造リンク上で伝搬されます。模造リンクの設定の詳細については、「MPLS VPN のための OSPF 模造リンクのサポート」を参照してください。

Cisco OSPF MIB および Cisco OSPF トラップ MIB の拡張機能

OSPF 模造リンク MIB サポート機能では、新しいテーブルおよびトラップ MIB オブジェクトを Cisco OSPF MIB（CISCO-OSPF-MIB）および Cisco OSPF トラップ MIB（CISCO-OSPF-TRAP-MIB）に追加することにより、OSPF模造リンク機能のMIBサポートが導入されます。また、OSPF模造リンク トラップ オブジェクトの SNMP 通知をイネーブルにするための、新しいコマンドライン インターフェイス（CLI）コマンドが追加されています。模造リンク インターフェイス全体におけるエラー、ステート変更、および再送信についての通知が提供されます。

OSPF 模造リンク設定のサポート

cospfShamLinksTable テーブル オブジェクトには、OSPF エリアに対して設定されている模造リンクに関する情報が保存されます。cospfShamLinksTableテーブルを使用すると、次のMIBオブジェクトにアクセスできます。

- cospfShamLinksAreaId
- cospfShamLinksLocalIpAddrType
- cospfShamLinksLocalIpAddr
- cospfShamLinksRemoteIpAddrType
- cospfShamLinksRemoteIpAddr
- cospfShamLinksRetransInterval
- cospfShamLinksHelloInterval
- cospfShamLinksRtrDeadInterval
- cospfShamLinksState
- cospfShamLinksEvents
- cospfShamLinksMetric

OSPF 模造リンク ネイバーのサポート

cospfShamLinkNbrTable テーブル オブジェクトには、すべての OSPF 模造リンク ネイバーのエントリが記述されます。cospfShamLinkNbrTable を使用すると、次の MIB オブジェクトにアクセスできます。

- cospfShamLinkNbrArea
- cospfShamLinkNbrIpAddrType
- cospfShamLinkNbrIpAddr
- cospfShamLinkNbrRtrId
- cospfShamLinkNbrOptions
- cospfShamLinkNbrState
- cospfShamLinkNbrEvents
- cospfShamLinkNbrLsRetransQLen
- cospfShamLinkNbrHelloSuppressed

OSPF 模造リンク インターフェイスの移行ステート変更のサポート

OSPF 模造リンク インターフェイスにおける移行ステート変更についてネットワーク マネージャに通知するには、cospfShamLinksStateChange トラップ オブジェクトを使用します。cospfShamLinksStateChange トラップ オブジェクトには、次の MIB オブジェクトが含まれます。

- ospfRouterId
- cospfShamLinksAreaId
- cospfShamLinksLocalIpAddrType
- cospfShamLinksLocalIpAddr
- cospfShamLinksRemoteIpAddrType
- cospfShamLinksRemoteIpAddr
- cospfShamLinksState

OSPF 模造リンク ネイバーの移行ステート変更のサポート

OSPF 模造リンク ネイバーにおける移行ステート変更についてネットワーク マネージャに通知するには、cospfShamLinkNbrStateChange トラップ オブジェクトを使用します。cospfShamLinkNbrStateChange トラップ オブジェクトには、次の MIB オブジェクトが含まれます。

- ospfRouterId
- cospfShamLinkNbrArea
- cospfShamLinksLocalIpAddrType
- cospfShamLinksLocalIpAddr
- cospfShamLinkNbrIpAddrType
- cospfShamLinkNbrIpAddr
- cospfShamLinkNbrRtrId
- cospfShamLinkNbrState

模造リンクのエラー

OSPF 模造リンクの設定、認証、および不良パケットのエラーに関するトラップ通知が行われます。これらのエラーには、次のトラップ オブジェクトが含まれます。

- cospfShamLinkConfigError
- cospfShamLinkAuthFailure
- cospfShamLinkRxBadPacket

OSPF 模造リンク MIB サポートの設定方法

ルータによる SNMP 通知送信のイネーブル化の設定

手順の概要

1. イネーブル化
2. **showrunning-config**
3. **configureterminal**
4. **snmp-serverhost** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
5. **snmp-serverenabletrapsospf**
6. **end**

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	**showrunning-config** 例： `Router# show running-config`	SNMP エージェントがすでに実行中かどうかが判別される実行コンフィギュレーションが表示されます。 • SNMP の情報が表示されない場合は、次のステップに進みます。SNMP 情報が表示される場合、必要に応じて、情報を変更できます。
ステップ 3	**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 4	**snmp-serverhost** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]	SNMP 通知操作の受信者（ターゲット ホスト）を指定します。 • *notification-type* が指定されていない場合は、イネーブルになっている全通知（トラップまたは応答要求）が、指定されたホストに送信されます。

	コマンドまたはアクション	目的
	例： `Router(config)# snmp-server host 172.20.2.162 version 2c public ospf`	• 指定されたホストに OSPF 通知だけを送信するには、オプションの **ospf** キーワードを *notification-types* の 1 つとして指定します（例を参照）。
ステップ 5	**snmp-serverenabletrapsospf** 例： `Router(config)# snmp-server enable traps ospf`	OSPF MIB 内に定義されている全 SNMP 通知をイネーブルにします。 （注） この手順が必要なのは、すべての OSPF トラップ（OSPF 模造リンクのトラップを含む）をイネーブルにする場合だけです。**no snmp-server enable traps ospf** コマンドを入力すると、すべての OSPF トラップ（OSPF 模造リンクのトラップを含む）がディセーブルになります。
ステップ 6	**end** 例： `Router(config)# end`	コンフィギュレーション セッションを終了し、グローバル コンフィギュレーション モードを終了します。

OSPF 模造リンク エラー トラップ送信のイネーブル化

手順の概要

1. イネーブル化
2. **configureterminal**
3. **snmp-serverenabletrapsospfcisco-specificerrorsconfig-error**
4. **snmp-serverenabletrapsospfcisco-specificerrorsshamlink** [**authentication** [**bad-packet** [**config**] | **config** [**bad-packet**]]
5. **end**

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	**snmp-serverenabletrapsospfcisco-specificerrorsconfig-error** 例： `Router(config)# snmp-server enable traps ospf cisco-specific errors config-error`	OSPF 非仮想インターフェイスの不一致エラーに対するエラー トラップをイネーブルにします。 （注） 両方のトラップが同じ場所で生成され、仮想リンクで同様の設定エラーがあった場合に一貫性を維持するようにするには、**snmp-server enable traps ospf cisco-specific errors shamlink** コマンドを入力する前に、**snmp-server enable traps ospf cisco-specific errors config-error** コマンドを入力する必要があります。cospfospfConfigError トラップを設定する前に cospfShamLinkConfigError トラップをイネーブルにしようとすると、cospfConfigError トラップを最初に設定しなければならないことを通知するエラー メッセージが表示されます。
ステップ 4	**snmp-serverenabletrapsospfcisco-specificerrorsshamlink** [**authentication** [**bad-packet** [**config**] | **config** [**bad-packet**]] 例： `Router(config)# snmp-server enable traps ospf cisco-specific errors shamlink`	OSPF 模造リンクのエラーに対するエラー トラップをイネーブルにします。 • **authentication** キーワードを使用すると、OSPF 模造リンク インターフェイス上での認証障害のみに対する SNMP 通知がイネーブルになります。 • **bad-packet** キーワードを使用すると、OSPF 模造リンク インターフェイス上でのパケット解析エラーのみに対する SNMP 通知がイネーブルになります。 • **config** キーワードを使用すると、OSPF 模造リンク インターフェイス上での設定不一致エラーのみに対する SNMP 通知がイネーブルになります。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Router(config)# end`	コンフィギュレーションセッションを終了し、グローバル コンフィギュレーション モードを終了します。

OSPF 模造リンクの再送信トラップのイネーブル化

手順の概要

1. イネーブル化
2. **configureterminal**
3. **snmp-serverenabletrapsospfcisco-specificretransmit** [**packets** [**shamlink** | **virt-packets**] | **shamlink** [**packets** | **virt-packets**] | **virt-packets** [**shamlink**]]
4. **end**

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	**snmp-serverenabletrapsospfcisco-specificretransmit** [**packets** [**shamlink**	**virt-packets**]	**shamlink** [**packets**	**virt-packets**]	**virt-packets** [**shamlink**]] 例： `Router(config)# snmp-server enable traps ospf cisco-specific retransmit shamlink`	OSPF 模造リンクの再送信エラーに対するエラートラップをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Router(config)# end`	コンフィギュレーション セッションを終了し、グローバル コンフィギュレーション モードを終了します。

OSPF 模造リンクのステート変更トラップのイネーブル化

（注） 置き換えられた cospfShamLinkChange トラップは現在もイネーブルにできますが、新しい cospfShamLinksStateChange トラップをイネーブルにする場合にはイネーブルにできません。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **snmp-serverenabletrapsospfcisco-specificstate-change**[**nssa-trans-change** | **shamlink** [**interface** | **interface-old** | **neighbor**]]
4. **end**

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	**snmp-serverenabletrapsospfcisco-specificstate-change**[**nssa-trans-change** | **shamlink** [**interface** | **interface-old** | **neighbor**]] 例： `Router(config)# snmp-server enable traps ospf cisco-specific state-change`	cospfShamLinksStateChange および cospfShamLinkNbrStateChange トラップなど、すべての Cisco 固有の OSPF ステート変更トラップをイネーブルにします。 • **neighbor** キーワードを使用すると、OSPF 模造リンク ネイバーのステート変更トラップがイネーブルになります。 • **interface** キーワードを使用すると、OSPF 模造リンク インターフェイスのステート変更トラップがイネーブルになります。 • **interface-old** を使用すると、cospfShamLinksStateChange および cospfShamLinkNbrStateChange トラップにより置換された元の OSPF 模造リンク インターフェイスのステート変更トラップがイネーブルになります。 （注） 新しいおよび置換された模造リンク インターフェイスの移行ステート変更トラップの両方をイネーブルにできないため、**interface** および **interface-old** の両方のキーワードを入力できません。これらのトラップは、いずれか一方だけを設定するか、両方とも設定しないでください。
ステップ 4	**end** 例： `Router(config)# end`	コンフィギュレーション セッションを終了し、グローバル コンフィギュレーション モードを終了します。

ルータ上の OSPF 模造リンク MIB トラップの確認

手順の概要

1. イネーブル化
2. **showrunning-config | include traps**

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	**showrunning-config | include traps** 例： `Router# show running-config | include traps`	現在の実行コンフィギュレーション ファイルの内容を表示します。イネーブルになっているトラップに関する情報が含まれています。 • トラップがイネーブルになっているかどうかを確認します。

OSPF 模造リンク MIB サポートの設定例

例：OSPF 模造リンク エラー トラップのイネーブル化と確認

次に、シスコ固有の OSPF 模造リンクのエラー トラップをすべてイネーブルにする例を示します。**snmp-server enable traps ospf cisco-specific errors shamlink** コマンドの入力を最初に試みると、**snmp-server enable traps ospf cisco-specific errors config-error** コマンドの入力を最初に入力する必要があることを示すエラー メッセージが表示されます。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# snmp-server enable traps ospf cisco-specific errors shamlink

% Sham-link config error trap not enabled.
% Configure "cisco-specific errors config-error" first.
% This requirement allows both traps to be sent.
Router(config)# snmp-server enable traps ospf cisco-specific errors config-error
Router(config)# snmp-server enable traps ospf cisco-specific errors shamlink
Router(config)# end
```

show running-config コマンドを実行して、トラップがイネーブルになっていることを確認します。

```
Router# show running-config | include traps
snmp-server enable traps ospf cisco-specific errors config-error
snmp-server enable traps ospf cisco-specific errors shamlink
```

トラップをディセーブル化する際に、**snmp-server enable traps ospf cisco-specific errors shamlink** コマンドよりも前に **no snmp-server enable traps ospf cisco-specific errors config-error** コマンドを入力すると、模造リンク設定エラー トラップもディセーブル化されたことを示すメッセージが表示されます。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no snmp-server enable traps ospf cisco-specific errors config-error
! This command also disables the previously-enabled shamlink configuration error traps.
Router(config)# end
```

例：OSPF ステート変更トラップのイネーブル化と確認

次の例では、cospfShamLinksStateChange および cospfShamLinkNbrStateChange トラップなど、すべての Cisco 固有の OSPF ステート変更トラップをイネーブルにします。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# snmp-server enable traps ospf cisco-specific state-change shamlink
```

show running-config コマンドを実行して、トラップがイネーブルになっていることを確認します。

```
Router# show running-config | include traps
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
```

snmp-server enable traps ospf cisco-specific state-change shamlink コマンドにより、cospfShamLinksStateChange トラップの模造リンク インターフェイス ステート変更がイネーブル化されることに注意してください。

従来の cospfShamLinkStateChange トラップをイネーブルにするには、最初に cospfShamLinksStateChange トラップをディセーブルにする必要があります。**snmp-server enable traps ospf cisco-specific state-change shamlink interface-old** コマンドの入力を試みると、次のエラーメッセージが表示されます。

```
Router(config)# snmp-server enable traps ospf cisco-specific state-change shamlink
interface-old
% Cannot enable both sham-link state-change interface traps.
% Deprecated sham link interface trap not enabled.
Router(config)# no snmp-server enable traps ospf cisco-specific state-change shamlink
interface
Router(config)# snmp-server enable traps ospf cisco-specific state-change shamlink
interface-old
```

例：OSPF 模造リンク再送信トラップのイネーブル化と確認

次に、OSPF 模造リンクの再送信トラップをすべてイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Router(config)# snmp-server enable traps ospf cisco-specific retransmit shamlink
Router(config)# end
```

show running-config コマンドを実行して、トラップがイネーブルになっていることを確認します。

```
Router# show running-config | include traps
snmp-server enable traps ospf cisco-specific retransmit shamlink
```

次の作業

SNMP および SNMP 操作の詳細については、『Cisco IOS XE Network Management Configuration Guide, *Release 2*』の「Configuring SNMP Support」の章を参照してください。

その他の参考資料

ここでは、OSPF 模造リンク MIB サポート機能に関する参考資料を紹介します。

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』
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
OSPF 模造リンクの設定	MPLS VPN のための OSPF 模造リンクのサポート
SNMP コンフィギュレーション	「Configuring SNMP Support」
SNMP コマンド	『*Cisco IOS Network Management Command Reference*』
『Configuring OSPF』	『Configuring OSPF』
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』

標準

規格	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
• CISCO-OSPF-MIB • CISCO-OSPF-TRAP-MIB	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

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

OSPF 模造リンク MIB サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *46*：*OSPF* 模造リンク *MIB* サポートの機能情報

機能名	リリース	機能情報
OSPF 模造リンク MIB サポート	Cisco IOS XE Release 2.1、Cisco IOS XE Release 2.6	この機能では、新しいテーブルおよびトラップ MIB オブジェクトを Cisco OSPF MIB（CISCO-OSPF-MIB）および Cisco OSPF Trap MIB（CISCO-OSPF-TRAP-MIB）に追加することにより、OSPF 模造リンク機能の MIB サポートが導入されます。また、Open Shortest Path First（OSPF）模造リンク トラップ オブジェクトの簡易ネットワーク管理プロトコル（SNMP）通知をイネーブルにするための、新しいコマンドが追加されています。模造リンク インターフェイス全体におけるエラー、ステート変更、および再送信についての通知が提供されます。 次に示すコマンドは、この章に記載されている機能において、新たに導入または変更されたものです。 • snmp-server enable traps ospf cisco-specific errors • snmp-server enable traps ospf cisco-specific lsa-mismatch • snmp-server enable traps ospf cisco-specific retransmit • snmp-server enable traps ospf cisco-specific state-change

第 40 章

データ フィールドのインターフェイス ID の OSPF SNMP ifIndex 値

この機能では、Open Shortest Path First バージョン 2（OSPFv2）および設定し、Open Shortest Path First バージョン 3（OSPFv3）データ フィールドのインターフェイス ID 値を設定できます。現在のインターフェイス番号か、インターフェイス ID の Simple Network Management Protocol（SNMP）MIB-II インターフェイス インデックス（ifIndex）値のどちらかを使用することを選択できます。SNMP MIB-II ifIndex 値を使用する利点は、SNMP のレポートでユーザが見る番号と、この番号が対応していることです。

- 機能情報の確認，423 ページ
- データ フィールドのインターフェイス ID の SNMP ifIndex 値の前提条件，424 ページ
- データ フィールドのインターフェイス ID の SNMP ifIndex 値について，424 ページ
- データ フィールドにインターフェイス ID として SNMP ifIndex 値を設定する方法，425 ページ
- データ フィールドのインターフェイス ID としての SNMP ifIndex 値の設定例，427 ページ
- その他の参考資料，431 ページ
- インターフェイス ID としての OSPF SNMP ifIndex 値の機能情報，432 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。

データ フィールドのインターフェイス ID の SNMP ifIndex 値の前提条件

インターフェイス ID の SNMP ifIndex 値を使用するには、OSPF をルータで設定する必要があります。

データ フィールドのインターフェイス ID の SNMP ifIndex 値について

SNMP MIB-II ifIndex 値でインターフェイスを識別する利点

OSPF ネットワークで SNMP を使用している場合に、OSPF：SNMP ifIndex Value for Interface ID in OSPFv2 and OSPFv3 Data Fields 機能を設定すると、次のような利点があります。

- SNMP MIB-II ifIndex 識別番号は、SNMP のレポートでネットワーク管理者が見る番号に対応しているため、この番号を OSPF 識別に使用すると、管理者はインターフェイスを容易に特定できるようになります。
- リンクステート アドバタイズメント（LSA）では、インターフェイス ID のフィールドに使用されている値が、SNMP で報告されるものと同じ値になります。
- **show ipv6 ospf interface** コマンドの出力で、インターフェイス ID 番号は SNMP で報告されるものと同じ値になります。
- SNMP MIB-II ifIndex の使用は、OSPFv2 に対しては OSPF RFC 2328 で、OSPFv3 に対しては RFC 2740 で推奨されています（必須ではありません）。

OSPFv2 および OSPFv3 での SNMP MIB-II ifIndex 値の使用方法

OSPF インターフェイスで SNMP MIB-II ifIndex 番号を使用するには、特定の OSPF プロセスで **interface-id snmp-if-index** コマンドを実行します。その特定の OSPF プロセスのインターフェイスに SNMP ifIndex 番号がない場合、そのインターフェイスで OSPF はイネーブルになりません。

OSPFv2 の場合、アンナンバード ポイントツーポイント インターフェイスおよび模造リンクのルータ LSA のリンク データ フィールドに、ifIndex 番号が使用されます。**interface-id snmp-if-index** コマンドを実行すると、反映された LSA がすぐに再送信されます。

OSPFv3 の場合、ネットワーク LSA およびリンク LSA の LSID として、また、hello パケットのインターフェイス ID として、ルータ LSA のインターフェイス ID に ifIndex 番号が使用されます。ネットワーク LSA を参照する Intra-Area-Prefix LSA の [Referenced LSID] フィールドにはネットワーク LSA の LSID があるため、これらも **interface-id snmp-if-index** コマンドが実行されると更新されます。ネットワーク LSA に関連する古いネットワーク LSA、リンク LSA、および Intra-Area-Prefix LSA はフラッシュされます。

OSPFv2 および OSPFv3 のいずれの場合でも、隣接関係のフラップは発生しません。ただし、隣接関係をフルに確立した OSPFv3 デマンド回線（仮想リンクを含む）の場合は別です。

OSPFv2 および OSPFv3 のいずれの場合でも、インターフェイスに SNMP ifIndex 番号がないのにインターフェイス ID が要求されると（OSPFv2 の場合、この状況はアンナンバードのインターフェイスおよび模造リンクにだけ該当します）、エラー メッセージが生成され、そのインターフェイスはディセーブルになります。インターフェイスを再びイネーブルにするには、**no interface-id snmp-if-index** コマンドを実行します。

データ フィールドにインターフェイス ID として SNMP ifIndex 値を設定する方法

OSPF インターフェイスによる SNMP MIB-II ifIndex 番号の使用の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. 次のいずれかを実行します。
   - **routerospf***process-id*[**vrf***vpn-name*]
   -
   - **ipv6routerospf***process-id*
4. **interface-idsnmp-if-index**
5. **end**
6. **showsnmpmibifmibifindex** [*typenumber*] [**detail**][**free-list**]

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： `Device> 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： `Device# 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	次のいずれかを実行します。
	• **routerospf***process-id*[**vrf***vpn-name*]
	•
	• **ipv6routerospf***process-id*
	例：
	`Device(config)# router ospf 4`
	例：
	例：
	`Device(config)# ipv6 router ospf 4`
		OSPFv2 ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
		OSPFv3 ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
		（注） IPv6 を使用する OSPFv3 ルーティング プロセスを設定する場合は、IPv6 を事前にイネーブルにしている必要があります。

ステップ 4	**interface-idsnmp-if-index** 例： `Device(config-router)# interface-id snmp-if-index`	OSPF インターフェイスに SNMP インターフェイス インデックス識別番号（ifIndex 値）を設定します。
ステップ 5	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。 SNMP MIB-II ifIndex 番号を使用するインターフェイスの全 OSPF プロセスについて、このタスクを繰り返してください。
ステップ 6	**showsnmpmibifmibifindex** [*typenumber*] [**detail**][**free-list**] 例： `Device# show snmp mib ifmib ifindex GigabitEtherent 0/0`	すべてのシステム インターフェイスまたは指定したシステム インターフェイスに対し、SNMP インターフェイス インデックス ID 番号（ifIndex 値）を表示します。

データ フィールドのインターフェイス ID としての SNMP ifIndex 値の設定例

例：OSPFv2 のインターフェイス ID としての SNMP ifIndex 値の設定

次の例では、インターフェイス ID として SNMP ifIndex 値を使用するように OSPF インターフェイスを設定します。**showsnmpmibifmibifindex** コマンドによって、OSPFv2 のデータ フィールドにインターフェイス ID 値として SNMP MIB-II ifIndex 値が使用されていることを確認します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# router ospf 1
Device(config-router)# interface-id snmp-if-index
Device(config-router)# ^Z
Device# show ip ospf 1 1 data router self
OSPF Router with ID (172.16.0.1) (Process ID 1)
Router Link States (Area 1)
LS age: 6
Options: (No TOS-capability, DC)
LS Type: Router Links
Link State ID: 172.16.0.1
Advertising Router: 172.16.0.1
LS Seq Number: 80000007
Checksum: 0x63AF
Length: 48
Area Border Router
Number of Links: 2
Link connected to: another Router (point-to-point)
(Link ID) Neighboring Router ID: 172.17.0.1
(Link Data) Router Interface address: 0.0.0.53
Number of TOS metrics: 0
TOS 0 Metrics: 64
Link connected to: a Stub Network
(Link ID) Network/subnet number: 192.168.0.11
(Link Data) Network Mask: 255.255.255.255
Number of TOS metrics: 0
TOS 0 Metrics: 1
Device# show snmp mib ifmib ifindex serial 13/0

Serial13/0: Ifindex = 53
```

例：OSPFv3 のインターフェイス ID としての SNMP ifIndex 値の設定

次の例では、インターフェイス ID として SNMP ifIndex 値を使用するように OSPFv3 インターフェイスを設定します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ipv6 router ospf 1
Device(config-router)# interface-id snmp-if-index
```

showsnmpmibifmibifindex コマンドの出力から、OSPFv2 のデータ フィールドにインターフェイス ID 値として SNMP MIB-II ifIndex 値が使用されていることを確認します。

```
Device# show snmp mib ifmib ifindex GigabitEthernet 0/0/0
0/0/0: Ifindex = 5
Device# show ipv6 ospf interface
OSPF_VL0 is up, line protocol is up
  Interface ID 71
  Area 0, Process ID 1, Instance ID 0, Router ID 172.16.0.1
  Network Type VIRTUAL_LINK, Cost: 10
  Configured as demand circuit.
  Run as demand circuit.
  DoNotAge LSA allowed.
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Index 1/2/3, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.0.0.1  (Hello suppressed)
  Suppress hello for 1 neighbor(s)
GigabitEthernet is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6F02, Interface ID 10
  Area 0, Process ID 1, Instance ID 0, Router ID 172.16.0.1
  Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.0.1, local address FE80::A8BB:CCFF:FE00:6F02
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/1/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
GigabitEthernet is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6F01, Interface ID 6
  Area 1, Process ID 1, Instance ID 2, Router ID 172.16.0.1
  Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.0.1, local address FE80::A8BB:CCFF:FE00:6F01
  Backup Designated router (ID) 10.0.0.1, local address FE80::A8BB:CCFF:FE00:6E01
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.0.0.1  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
Device# show ipv6 ospf database network adv-router 172.16.0.1
OSPFv3 Router with ID (172.16.0.1) (Process ID 1)
Net Link States (Area 1)
  LS age: 144
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Network Links
  Link State ID: 6 (Interface ID of Designated Router)
  Advertising Router: 172.16.0.1
  LS Seq Number: 80000001
  Checksum: 0x1FC0
  Length: 32
        Attached Router: 172.16.0.1
        Attached Router: 10.0.0.1
Device# show ipv6 ospf database prefix adv-router 172.16.0.1
OSPFv3 Router with ID (172.16.0.1) (Process ID 1)
Intra Area Prefix Link States (Area 0)
Routing Bit Set on this LSA
```

```
LS age: 196
LS Type: Intra-Area-Prefix-LSA
Link State ID: 0
Advertising Router: 172.16.0.1
LS Seq Number: 80000001
Checksum: 0x6F11
Length: 44
  Referenced LSA Type: 2001
  Referenced Link State ID: 0
  Referenced Advertising Router: 172.16.0.1
  Number of Prefixes: 1
  Prefix Address: 2002:0:2::
  Prefix Length: 64, Options: None, Metric: 10
Intra Area Prefix Link States (Area 1)
  Routing Bit Set on this LSA
  LS age: 161
  LS Type: Intra-Area-Prefix-LSA
  Link State ID: 0
  Advertising Router: 172.16.0.1
  LS Seq Number: 80000001
  Checksum: 0xB6E7
  Length: 52
  Referenced LSA Type: 2001
  Referenced Link State ID: 0
  Referenced Advertising Router: 172.16.0.1
  Number of Prefixes: 1
  Prefix Address: 2002:0:2:0:A8BB:CCFF:FE00:6F02
  Prefix Length: 128, Options: LA , Metric: 0
  Routing Bit Set on this LSA
  LS age: 151
  LS Type: Intra-Area-Prefix-LSA
  Link State ID: 1006
  Advertising Router: 172.16.0.1
  LS Seq Number: 80000001
  Checksum: 0x6E24
  Length: 44
  Referenced LSA Type: 2002
  Referenced Link State ID: 6
  Referenced Advertising Router: 172.16.0.1
  Number of Prefixes: 1
  Prefix Address: 2002:0:1::
  Prefix Length: 64, Options: None, Metric: 0
Device# show ipv6 ospf database router
OSPFv3 Router with ID (10.0.0.1) (Process ID 1)
Router Link States (Area 0)
  Routing Bit Set on this LSA
  LS age: 5 (DoNotAge)
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Router Links
  Link State ID: 0
  Advertising Router: 10.0.0.1
  LS Seq Number: 80000004
  Checksum: 0xEE5C
  Length: 40
  Area Border Router
  Number of Links: 1
    Link connected to: a Virtual Link
      Link Metric: 10
      Local Interface ID: 70
      Neighbor Interface ID: 71
      Neighbor Router ID: 172.16.0.1
LS age: 162
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Router Links
Link State ID: 0
Advertising Router: 172.16.0.1
LS Seq Number: 80000004
Checksum: 0xCE7C
Length: 40
Area Border Router
Number of Links: 1
    Link connected to: a Virtual Link
      Link Metric: 10
```

```
      Local Interface ID: 71
      Neighbor Interface ID: 70
      Neighbor Router ID: 10.0.0.1
Router Link States (Area 1)
Routing Bit Set on this LSA
LS age: 176
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Router Links
Link State ID: 0
Advertising Router: 10.0.0.1
LS Seq Number: 80000003
Checksum: 0xC807
Length: 40
Area Border Router
Number of Links: 1
    Link connected to: a Transit Network
Link Metric: 10
Local Interface ID: 6
Neighbor (DR) Interface ID: 6
Neighbor (DR) Router ID: 172.16.0.1
LS age: 175
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Router Links
Link State ID: 0
Advertising Router: 172.16.0.1
LS Seq Number: 80000004
Checksum: 0xBD10
Length: 40
Area Border Router
Number of Links: 1
    Link connected to: a Transit Network
Link Metric: 10
Local Interface ID: 6
Neighbor (DR) Interface ID: 6
Neighbor (DR) Router ID: 172.16.0.1
Device# show ipv6 ospf database link adv-router 172.16.0.1
OSPFv3 Router with ID (172.16.0.1) (Process ID 1)
Link (Type-8) Link States (Area 0)
  LS age: 245
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Link-LSA (Interface: GigabitEthernet2/0)
  Link State ID: 10 (Interface ID)
  Advertising Router: 172.16.0.1
  LS Seq Number: 80000002
  Checksum: 0xA0CB
  Length: 56
  Router Priority: 1
  Link Local Address: FE80::A8BB:CCFF:FE00:6F02
  Number of Prefixes: 1
  Prefix Address: 2002:0:2::
  Prefix Length: 64, Options: None
Link (Type-8) Link States (Area 1)
LS age: 250
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Link-LSA (Interface: GigabitEthernet1/0)
Link State ID: 6 (Interface ID)
Advertising Router: 172.16.0.1
LS Seq Number: 80000001
Checksum: 0x4F94
Length: 44
Router Priority: 1
Link Local Address: FE80::A8BB:CCFF:FE00:6F01
Number of Prefixes: 0
```

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』
OSPF コマンド	『Cisco IOS IP Routing: OSPF Command Reference』
TE トンネル インターフェイスの保護	『*Cisco IOS Multiprotocol Label Switching Configuration Guide*』の「MPLS Traffic Engineering--Fast Reroute Link and Node Protection」の項。

標準

規格	Title
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	--

MIB

MIB	MIB のリンク
• なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 5286	『Basic Specification for IP Fast Reroute: Loop-Free Alternates』

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

インターフェイス ID としての OSPF SNMP ifIndex 値の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *47* : *OSPF* : *OSPFv2* および *OSPFv3* データ フィールドのインターフェイス *ID* としての *SNMP ifIndex* 値の機能情報

機能名	リリース	機能情報
OSPF：OSPFv2 および OSPFv3 データ フィールドのインターフェイス ID として使用する SNMP ifIndex 値	Cisco IOS XE Release 2.6	これにより、OSPFv2 および OSPFv3 データ フィールドにインターフェイス ID として、現在のインターフェイス番号または SNMP ifIndex 値を選択できます。SNMP MIB-II ifIndex 値を使用する利点は、SNMP のレポートでユーザが見る番号と、この番号が対応していることです。 次のコマンドは、このモジュールに記述された機能で導入または変更されています。 **interface-idsnmp-if-index**

第 41 章

OSPFv2 ローカル RIB

OSPFv2 ローカル RIB 機能を使用すると、各 OSPF プロトコル インスタンスに固有のローカル ルーティング情報ベース（RIB）が設定されます。OSPF ローカル RIB は、OSPF の SPF ルート計算のプライマリ状態として機能します。SPF の計算中、中間結果でグローバル RIB が更新されることはありません。ルータが追加、削除、または変更されたときだけ更新されるため、グローバル RIB 計算の機会が減少します。この更新アクティビティの減少により、ドロップされるパケットが減少する場合があります。

この機能はデフォルトでイネーブルになっているため、設定は不要です。この文書では、グローバル RIB 機能とローカル RIB 機能を変更するための、いくつかの任意指定の設定タスクについて説明します。ただし、これらはデフォルト設定のままにすることを推奨します。

- 機能情報の確認，435 ページ
- OSPFv2 ローカル RIB の前提条件，436 ページ
- OSPFv2 ローカル RIB の制約事項，436 ページ
- OSPFv2 ローカル RIB について，436 ページ
- OSPFv2 ローカル RIB の設定方法，437 ページ
- OSPFv2 ローカル RIB の設定例，440 ページ
- その他の参考資料，441 ページ
- OSPFv2 ローカル RIB の機能情報，442 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。

OSPFv2 ローカル RIB の前提条件

この機能を設定する前に、OSPF ルーティング プロトコルを設定しておく必要があります。

OSPFv2 ローカル RIB の制約事項

この機能を使用できるのは、IP バージョン 4 ネットワークだけです。

OSPFv2 ローカル RIB について

OSPFv2 を実行しているルータは、すべてのルートをネイバーで学習した宛先に格納するローカル RIB を維持します。個々の SPF の最後に、OSPF はローカル RIB にある宛先に対して最適な（最もコストのかからない）ルートをグローバル IPv4 ルーティング テーブルにインストールしようとします。グローバル RIB は、ルータが追加、削除、または変更されたときだけ更新されます。ローカル RIB および転送情報ベース（FIB）におけるルートは、SPF 中に中間結果が計算されるときには計算を行いません。この結果、一部の環境ではドロップされるパケットが少なくなります。

デフォルトでは、グローバル RIB の内容は、タイプ 5 LSA およびタイプ 7 LSA のエリア間集約、NSSA 変換、およびフォワーディング アドレスを計算するために使用されます。これらの機能はそれぞれグローバル RIB ではなく OSPF ローカル RIB の内容を使用して計算を行うように設定されます。計算にローカル RIB を使用すると、一部の環境では若干計算速度が上がる場合がありますが、ローカル RIB には OSPF の特定のインスタンスだけに対応する情報が含まれているため、これを計算に使用すると正しくない結果が出る可能性があります。発生する可能性のある問題には、ルーティング ループやブラック ホール ルートなどがあります。デフォルト値は安定性があり、現在の RIB 動作を保持しているため、変更しないことを推奨します。

デフォルトでは、OSPF は、廃棄ルートを他のルータにアドバタイズする任意のエリア範囲（内部）プレフィックスまたは集約アドレス（外部）プレフィックスの null0 にインストールします。要約部分に、RIB 内の限定されたルートがない場合、廃棄ルートのインストールによってルーティング ループを回避できます。通常、内部廃棄ルートはアドミニストレーティブ ディスタンス 110 にインストールされます。一方外部廃棄ルートにはアドミニストレーティブ ディスタンス 254 があります。

ただし、他の値が必要になる場合もあります。たとえば、1 つの OSPF プロセスが別の OSPF で設定されているエリア範囲と完全に一致するルートをインストールすると、2 つ目の OSPF プロセスの内部廃棄ルートにはより大きい（望ましくない）アドミニストレーティブ ディスタンスが割り当てられることがあります。

OSPFv2 ローカル RIB の設定方法

ここで説明するコマンドは、デフォルト設定のままにすることを推奨しますが、任意でデフォルト設定から変更することもできます。

デフォルトのローカル RIB 基準の変更

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id*[**vrf***vpn-name*]
4. **local-rib-criteria**[**forwarding-address**] [**inter-area-summary**] [**nssa-translation**]
5. **end**
6. **showipospf***process-id***rib**[**redistribution**] [*network-prefix*] [*network-mask*] [**detail**]

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	**configureterminal** 例： `Device# 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	**routerospf***process-id*[**vrf***vpn-name*] 例： `Device(config)# router ospf 23`	OSPFv2 ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**local-rib-criteria**[**forwarding-address**] [**inter-area-summary**] [**nssa-translation**] 例： `Device(config-router)# local-rib-criteria forwarding-address`	OSPF ローカル RIB がルート検証に使用されることを指定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 6	**showipospf***process-id***rib**[**redistribution**] [*network-prefix*] [*network-mask*] [**detail**] 例： `Device# show ip ospf 23 rib`	OSPF ローカル RIB またはローカルに再配布されるルートの情報を表示します。

廃棄ルートのアドミニストレーティブ ディスタンスの変更

（注） デフォルト設定のままにしておくことをお勧めします。ただし、この項の手順に従って、廃棄ルートのアドミニストレーティブ ディスタンスを変更することができます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id*[**vrf***vpn-name*]
4. **discard-route** [**external** [*distance*]] [**internal** [*distance*]]
5. **end**
6. **showiproute** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*] | **staticdownload**]

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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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	**routerospf***process-id*[**vrf***vpn-name*] 例： `Device(config)# router ospf 23`	OSPFv2 ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**discard-route** [**external** [*distance*]] [**internal** [*distance*]] 例： `Device(config-router)# discard-route external 150`	以前に削除した外部廃棄ルートまたは内部廃棄ルートを、もう一度インストールします。 （注） これで外部廃棄ルートまたは内部廃棄ルートのアドミニストレーティブ ディスタンスを指定できるようになりました。
ステップ 5	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 6	**showiproute** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*] | **staticdownload**] 例： `Device# show ip route ospf 23`	ルーティング テーブルの現在の状態を表示します。 （注） **showiproute** コマンドを入力すると、外部廃棄ルートまたは内部廃棄ルートのアドミニストレーティブ ディスタンスの変更後の値を確認できます。

例

showiproute コマンドで表示される出力例では、IP ルート 192.168.0.0/24 のアドミニストレーティブ ディスタンスは 110 であることが確認されます。

```
Device# show ip route 192.168.0.0 255.255.255.0
Routing entry for 192.168.0.0/24
  Known via "ospf 1", distance 110, metric 0, type intra area
```

```
  Routing Descriptor Blocks:
  * directly connected, via Null0
       Route metric is 0, traffic share count is 1
```

トラブルシューティングのヒント

debug ip ospf rib コマンドの出力を調べると、ローカル RIB の機能、およびルート再配布プロセスとグローバル RIB との間の関係を知ることができます。たとえば、OSPF がグローバル RIB に格納したルートが、予想と異なる理由がわかります。

OSPFv2 ローカル RIB の設定例

例：デフォルトのローカル RIB 基準の変更

次の例は、**local-rib-criteria** コマンドをキーワードを指定しないで入力すると、フォワーディングアドレス、エリア間集約、および NSSA 変換オプションすべての基準として、ローカル RIB が使用されることを示しています。

```
router ospf 1
 router-id 10.0.0.6
 local-rib-criteria
```

例：廃棄ルートのアドミニストレーティブ ディスタンスの変更

次の例では、外部廃棄ルートのアドミニストレーティブディスタンスが25、内部廃棄ルートのアドミニストレーティブ ディスタンスが 30 に設定されています。

```
router ospf 1
 router-id 10.0.0.6
 log-adjacency-changes
 discard-route external 25 internal 30
 area 4 range 10.2.0.0 255.255.0.0
 summary-address 192.168.130.2 255.255.255.0
 redistribute static subnets
 network 192.168.129.2 0.255.255.255 area 0
 network 192.168.130.12 0.255.255.255 area 0
```

showiproute コマンドの出力で、内部ルート 10.2.0.0/16 のアドミニストレーティブ ディスタンスが 30 に設定されていることが確認されます。

```
Device# show ip route 10.2.0.0 255.255.0.0
Routing entry for 10.2.0.0/16
Known via "ospf 1", distance 30, metric 1, type intra area
  Routing Descriptor Blocks:
  * directly connected, via Null0
      Route metric is 1, traffic share count is 1
```

showiproute コマンドの出力で、外部ルート 192.168.130.2/24 のアドミニストレーティブ ディスタンスが 25 に設定されていることが確認されます。

```
Device# show ip route 192.168.130.2 255.255.255.0
Routing entry for 192.168.130.2/24
 Known via "ospf 1", distance 25, metric 20, type intra area
  Routing Descriptor Blocks:
  * directly connected, via Null0
      Route metric is 20, traffic share count is 1
```

その他の参考資料

ここでは、OSPFv2 ローカル RIB に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
『Configuring OSPF』	『Configuring OSPF』
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』

標準

規格	Title
なし	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
なし	--

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

OSPFv2 ローカル RIB の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *48* : *OSPFv2* ローカル *RIB* の機能情報

機能名	リリース	機能情報
OSPFv2 ローカル RIB	Cisco IOS XE Release 2.1	OSPFv2 ローカル RIB 機能を使用すると、各 OSPF プロトコルインスタンスに固有のローカルルーティング情報ベース（RIB）が設定されます。OSPF ローカル RIB は、OSPF の SPF ルート計算のプライマリ状態として機能します。SPF の計算中、中間結果でグローバル RIB が更新されることはありません。ルータが追加、削除、または変更されたときだけ更新されるため、グローバル RIB 計算の機会が減少します。この更新アクティビティの減少により、ドロップされるパケットが減少する場合があります。 この機能はデフォルトでイネーブルになっているため、設定は不要です。この文書では、グローバル RIB 機能とローカル RIB 機能を変更するための、いくつかの任意指定の設定タスクについて説明します。ただし、これらはデフォルト設定のままにすることを推奨します。 次のコマンドが導入または変更されました。**debugipospfrib**、**discard-route**、**local-rib-criteria**、**showipospfrib**

第 42 章

MPLS TE トンネルを介した Forwarding Adjacency（FA）の OSPF サポート

MPLS トラフィック エンジニアリングされたトンネルを介した Forwarding Adjacency（FA）の OSPF サポート機能により、マルチプロトコル ラベル スイッチング（MPLS）トラフィック エンジニアリング（TE）Forwarding Adjacency（FA）機能に Open Shortest Path First（OSPF）サポートが追加され、ネットワーク管理者は最短パス優先（SPF）アルゴリズムに基づいて内部ゲートウェイ プロトコル（IGP）ネットワークのリンクとしてトラフィック エンジニアリング、ラベルスイッチドパス（LSP）トンネルを処理できるようになります。OSPF Forwarding Adjacency（FA）は、同じエリアのルータ間で作成できます。

MPLS トラフィック エンジニアリングされたトンネルを介した Forwarding Adjacency（FA）の OSPF サポート機能の履歴

リリース	変更内容
12.0(24)S	この機能が導入されました。
12.2(25)S	この機能は、Cisco IOS Release 12.2(25)S に統合されました。
12.2(18)SXE	この機能は、Cisco IOS Release 12.2(18)SXE に統合されました。
12.2(27)SBC	この機能は、Cisco IOS Release 12.2(27)SBC に統合されました。
Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータで実装されました。

- 機能情報の確認，446 ページ
- OSPF Forwarding Adjacency（FA）の前提条件，446 ページ

- OSPF Forwarding Adjacency（FA）について，446 ページ
- OSPF Forwarding Adjacency（FA）の設定方法，447 ページ
- OSPF Forwarding Adjacency の設定例，450 ページ
- その他の参考資料，451 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。

OSPF Forwarding Adjacency（FA）の前提条件

- OSPF がネットワークで設定されている。
- シスコ エクスプレス フォワーディング（CEF）がイネーブルになっている。
- 「MPLS Traffic Engineering Forwarding Adjacency」で説明されている Forwarding Adjacency（FA）の MPLS TE トンネルを理解している。

OSPF Forwarding Adjacency（FA）について

OSPFは、トラフィックのルーティングおよび転送のために他のリンクが表示されるのと同様に、MPLS TE トンネルを OSPF リンクステート データベースに含めます。MPLS TE トンネルがネットワーク デバイス間で設定されると、そのリンクはForwarding Adjacency（FA）と見なされます。ユーザは、トンネルにコストを割り当ててリンクの優先度を示すことができます。他のネットワーク デバイスには、物理リンクに加えてトンネルがリンクとして表示されます。

OSPF Forwarding Adjacency（FA）の設定方法

OSPF Forwarding Adjacency の設定

（注） 2 つの LSP トンネルで双方向の（A から B および B から A）Forwarding Adjacency を設定します。そうしない場合、Forwarding Adjacency はアドバタイズされますが、IGP ネットワークで使用されません。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipcefdistributed**
4. **mplstraffic-engtunnels**
5. **interfaceloopback***number*
6. **ipaddress***ip-addressmask*
7. **noshutdown**
8. **exit**
9. **interfacetunnel***number*
10. **tunnelmodemplstraffic-eng**
11. **tunnelmplstraffic-engforwarding-adjacency**{**holdtime** *value*}
12. **ipospfcost***cost*
13. **exit**
14. **routerospf***process-id*
15. **mplstraffic-engrouter-id***interface*
16. **mplstraffic-engarea***number*
17. **end**

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	**ipcefdistributed** 例： `Router(config)# ip cef distributed`	シスコ エクスプレス フォワーディング（CEF）をイネーブルにします。
ステップ 4	**mplstraffic-engtunnels** 例： `Router(config)# mpls traffic-eng tunnels`	デバイスで MPLS トラフィック エンジニアリング トンネル シグナリングをイネーブルにします。
ステップ 5	**interfaceloopback***number* 例： `Router(config)# interface loopback0`	ループバック インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 • 32 ビット マスクでループバック インターフェイスを設定し、CEF をイネーブルにし、MPLS トラフィック エンジニアリングをイネーブルにして、MPLS ネットワークのルーティング プロトコル（OSPF）を設定します。
ステップ 6	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.1.1.1 255.255.255.255`	ループバック インターフェイスの IP アドレスとサブネット マスクを設定します。
ステップ 7	**noshutdown** 例： `Router(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 8	**exit** 例： `Router(config-if)# exit`	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。

	コマンドまたはアクション	目的
ステップ 9	**interfacetunnel***number* 例： `Router(config)# interface tunnel 1`	Forwarding Adjacency 用のトンネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	**tunnelmodemplstraffic-eng** 例： `Router(config-if)# tunnel mode mpls traffic-eng`	トンネルのモードを、トラフィック エンジニアリングの MPLS に設定します。
ステップ 11	**tunnelmplstraffic-engforwarding-adjacency**{**holdtime** *value*} 例： `Router(config-if)# tunnel mpls traffic-eng forwarding-adjacency holdtime 10000`	TE トンネルを IGP ネットワーク内にリンクとしてアドバタイズします。 • **holdtime** *value* キーワード引数の組み合わせは、TE トンネルが停止してからネットワークに通知するまでの待機時間（ミリ秒）を表します。指定できる範囲は 0 ～ 4,294,967,295 ms です。デフォルト値は 0 です
ステップ 12	**ipospfcost***cost* 例： `Router(config-if)# ip ospf cost 4`	（任意）Forwarding Adjacency として使用するトンネル インターフェイスのコスト メトリックを設定します。
ステップ 13	**exit** 例： `Router(config-if)# exit`	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 14	**routerospf***process-id* 例： `Router(config)# router ospf 1`	OSPF ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 15	**mplstraffic-engrouter-id***interface* 例： `Router(config-router)# mpls traffic-eng router-id ethernet 1/0`	ノードのトラフィック エンジニアリング ルータ識別子が、指定されたインターフェイスに関連付けられている IP アドレスになるように指定します。

	コマンドまたはアクション	目的
ステップ 16	**mplstraffic-engarea***number* 例： `Router(config-router)# mpls traffic-eng area 1`	指定した OSPF エリアに対してトラフィック エンジニアリングをフラッディングするように、OSPF MPLS を実行しているルータを設定します。
ステップ 17	**end** 例： `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了します。

OSPF Forwarding Adjacency の設定例

例：OSPF Forwarding Adjacency

次の例で、トンネルの宛先は、他のルータ上のループバック インターフェイスです。ルータは OSPF TE 拡張機能により設定され、OSPF エリア 0 のトラフィック エンジニアリング リンク ステート アドバタイズメント（LSA）をフラッディングします。ノードのトラフィック エンジニアリング ルータ識別子は、Loopback 0 に関連付けられている IP アドレスになります。この例の最後の行が、この場合の OSPF である MPLS ネットワークのルーティング プロトコルを設定します。

（注） トンネル内に Forwarding Adjacency を設定する場合は、**mpls traffic-eng autoroute announce** コマンドを使用しないでください。

```
ip routing
ip cef distributed
mpls traffic-eng tunnels
!
interface Loopback0
 ip address 127.0.0.1 255.255.255.255
 no shutdown
!
interface Tunnel1
 ip unnumbered Loopback0
 no ip directed-broadcast
 tunnel destination 10.1.1.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng forwarding-adjacency holdtime 10000
 ip ospf cost 4
 tunnel mpls traffic-eng priority 2 2
 tunnel mpls traffic-eng bandwidth  10
 tunnel mpls traffic-eng path-option 2 dynamic
router ospf 5
 log-adjacency-changes
 network 10.1.1.1 0.0.0.0 area 0
```

```
 mpls traffic-eng router-id loopback0
 mpls traffic-eng area 0
```

自己生成ルータ LSA を確認すると、これは、ルータ LSA のリンクの 1 つとして表示されます（次の出力に太字で表示）。

```
Router# show ip ospf database route self-originate
OSPF Router with ID (10.5.5.5) (Process ID 5)
                Router Link States (Area 0)
  LS age:332
  Options:(No TOS-capability, DC)
  LS Type:Router Links
  Link State ID:10.5.5.5
  Advertising Router:10.5.5.5
  LS Seq Number:80000004
  Checksum:0x1D24
  Length:72
  Number of Links:4
    Link connected to another Router (point-to-point)
     (Link ID) Neighboring Router ID:10.3.3.3
     (Link Data) Router Interface address:0.0.0.23
      Number of TOS metrics:0
       TOS 0 Metrics:1562
    Link connected to:a Transit Network
     (Link ID) Designated Router address:172.16.0.1
     (Link Data) Router Interface address:172.16.0.2
      Number of TOS metrics:0
       TOS 0 Metrics:10
    Link connected to:a Transit Network
     (Link ID) Designated Router address:172.16.0.3
     (Link Data) Router Interface address:172.16.0.4
      Number of TOS metrics:0
       TOS 0 Metrics:10
    Link connected to:a Stub Network
     (Link ID) Network/subnet number:10.5.5.5
     (Link Data) Network Mask:255.255.255.255
      Number of TOS metrics:0
       TOS 0 Metrics:1
```

その他の参考資料

ここでは、OSPF LSA Forwarding Adjacency に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
MPLS トラフィック エンジニアリング Forwarding Adjacency	MPLS トラフィック エンジニアリング転送隣接
MPLS トラフィック エンジニアリング用の OSPF の設定	MPLS トラフィック エンジニアリングおよび拡張機能
MPLS トラフィック エンジニアリング：LSP 属性	MPLS トラフィック エンジニアリング：LSP 属性

標準

標準	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

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

第 43 章

インターフェイスごとのOSPFv2のイネーブル化

このマニュアルでは、インターフェイス単位で Open Shortest Path First バージョン 2（OSPFv2）をイネーブルにすることにより、番号が付いていないインターフェイスの設定を簡素化する方法について説明します。**ipospfarea** コマンドを使用すると、インターフェイス上での OSPFv2 を明示的にイネーブルにできます。**ipospfarea** コマンドは、**networkarea** コマンドによって指定したアドレス範囲に一致するインターフェイスのアドレスを使用して OSPFv2 をイネーブルにするのに代わる方法になります。

- 機能情報の確認，453 ページ
- インターフェイスごとに OSPFv2 をイネーブルにする前提条件，454 ページ
- インターフェイスごとの OSPFv2 のイネーブル化の制約事項，454 ページ
- インターフェイスごとの OSPFv2 のイネーブル化について，454 ページ
- インターフェイスごとに OSPFv2 をイネーブルにする方法，456 ページ
- インターフェイス上での OSPFv2 のイネーブル化の設定例，457 ページ
- その他の参考資料，458 ページ
- インターフェイス単位での OSPFv2 のイネーブル化の機能情報，459 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。

インターフェイスごとにOSPFv2をイネーブルにする前提条件

OSPFv2 がネットワークで実行されている必要があります。

インターフェイスごとのOSPFv2のイネーブル化の制約事項

ip ospf area コマンドは、OSPFv2 においてのみサポートされます。

インターフェイスごとのOSPFv2のイネーブル化について

インターフェイスごとに OSPFv2 をイネーブルにする利点

インターフェイスのネットワーク アドレスが、ルータ コンフィギュレーション モードで実行した **network area** コマンドで指定したアドレス範囲と一致する場合、そのインターフェイスで OSPF がイネーブルになります。また、インターフェイス コンフィギュレーション モードで実行される **ip ospf area** コマンドを使用することで OSPFv2 をインターフェイスで明示的にイネーブルにすることもできます。この機能により、番号が付いていないインターフェイスをさまざまなエリアで簡単に設定できるようになります。

ip ospf area コマンドはインターフェイスに対して明示的に設定されるため、**network area** コマンドの効果よりも優先されます。これはネットワーク レベルで実行され、**network area** コマンドで指定されたアドレス範囲内にあるアドレスのインターフェイスに影響します。

後で **ip ospf area** コマンドをディセーブルにしても、インターフェイスのネットワーク アドレスが、**network area** コマンドで指定したアドレス範囲に一致する限り、そのインターフェイスは OSPFv2 を実行し続けます。

ルータごとまたはインターフェイスごとの OSPFv2 の設定の影響

ip ospf area コマンドを使用してインターフェイスで OSPFv2 をイネーブルにする前に、次のシナリオおよびコマンド動作を理解しておくことをお勧めします。**network area** コマンド（ルータ コンフィギュレーション モードで OSPFv2 を設定）を使用する場合と、**ip ospf area** コマンド（イン

ターフェイス コンフィギュレーション モードで OSPFv2 を設定）を使用する場合の影響があります。

同じエリアおよびプロセスを使用する network area コマンドにより、インターフェイスの OSPFv2 はすでにイネーブルになっている

network area コマンドにより OSPFv2 がイネーブルになっているインターフェイス上で **ip ospf area** コマンドを入力した場合、インターフェイスのプロセス ID およびエリア ID は変更されず、インターフェイスのステータスは変更されません。ただし、インターフェイスはインターフェイス コンフィギュレーション モードから設定されたとしてフラグ付けされ、設定データはインターフェイス記述ブロック（IDB）に保存されます。

異なるエリアおよびプロセスを使用する network area コマンドにより、インターフェイスはすでに設定されている

network area コマンドにより OSPFv2 がイネーブルになっているインターフェイス上で **ip ospf area** コマンドを入力した場合に、新しい設定情報が IDB に保存された後に、インターフェイスのプロセス ID およびエリア ID を変更して設定を変更した場合、インターフェイスは削除されてから再接続されます。したがって、インターフェイスは元のエリアおよびプロセスから削除され、新しいエリアおよびプロセスに追加されます。また、インターフェイスのステートもリセットされます。

インターフェイスが network area コマンドによって設定されていない

network area コマンドによりインターフェイスの OSPFv2 がイネーブルになっていない場合は、エリアおよびOSPF ルータ インスタンスが必要に応じて作成されます。ルータをリロードすると、システムの初期化が完了するまで OSPF プロセスの実行は開始されません。OSPF ルータ インスタンスを削除するには、**no router ospf** コマンドを入力します。インターフェイス モードで **ip ospf area** コマンドを削除すると、OSPF ルータ インスタンスが削除されます。

ip ospf area コマンドを削除する

ip ospf area コマンドを削除すると、インターフェイスがエリアから切断されます。接続されている他のインターフェイスがない場合、そのエリアは削除されます。インターフェイスのアドレスが **network area** コマンドの範囲に含まれている場合は、そのインターフェイスが存在するネットワークのエリアにおいて、インターフェイスが再びイネーブルになります。

新しいプロセス

router ospf コマンドまたは **interface** コマンドが設定されている場合に、OSPF プロセスがまだ存在しておらず、ルータ ID を選択できない場合は、プロキシミティ データベース（PDB）とプロセスが作成されますが、プロセスは非アクティブになります。**router-id** コマンドを使用してプロセスを明示的に設定するか、または IP アドレスが使用可能になったときに、ルータ ID が選択されると、プロセスはアクティブになります。ただし、ルータ ID を選択できなくても、**router ospf** コマンドは受け入れられる状態になり、コマンドライン インターフェイス（CLI）は OSPF 設定コンテキストになることに注意してください。したがって、IP アドレスが使用可能になる前に **router-id** コマンドが入力されます。プロセスがアクティブではなく、**show ip ospf** コマンドが入力

されていない場合は、「%OSPF: Router process X is not running, please provide a router-id」というメッセージが表示されます。

リンクステート アドバタイズメントと Shortest Path First

ステートの変更が **ip ospf area** コマンドの結果として発生した場合は、新しいルータのリンクステート アドバタイズメント（LSA）が（インターフェイスによってエリアが変更される場合は、古いエリアに対しても）生成され、古いエリアと新しいエリアの両方における最短パス優先（SPF）の実行がスケジュールされます。

インターフェイスごとにOSPFv2をイネーブルにする方法

インターフェイス上での OSPFv2 のイネーブル化

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipospf***process-id***area***area-id*[**secondariesnone**]
5. **end**
6. **showipospfinterface** [*type-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	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	**configureterminal** 例： `Device# 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	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet 0/2/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ipospf***process-id***area***area-id*[**secondariesnone**] 例： `Device(config-if)# ip ospf 1 area 0 secondaries none`	インターフェイスに対して OSPFv2 をイネーブルにします。 • インターフェイス上のセカンダリ IP アドレスがアドバタイズされるのを防ぐため、任意の **secondaries** キーワードを入力し、その後ろに **none** キーワードを入力する必要があります。
ステップ 5	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。
ステップ 6	**showipospfinterface** [*type-number*] 例： `Device# show ip ospf interface GigabitEthernet 0/2/1`	OSPF に関連するインターフェイス情報を表示します。 • インターフェイス上での OSPFv2 をイネーブルにすると、**showipospfinterface** コマンドを入力して設定を確認できます。

インターフェイス上でのOSPFv2のイネーブル化の設定例

例：インターフェイス上での OSPFv2 のイネーブル化

次に、ギガビット イーサネット インターフェイス 0/0/0 上で OSPFv2 を明示的に設定する例を示します。

```
Device(config)# interface GigabitEthernet 0/2/1
Device(config-if)# bandwidth 10000
Device(config-if)# ip address 172.16.1.1 255.255.255.0
Device(config-if)# ip ospf hello-interval 1
Device(config-if)# ip ospf 1 area 0
```

showipospfinterface コマンドを入力すると、次のような出力により、OSPFv2 を実行するためにインターフェイス コンフィギュレーション モードでギガビット イーサネット インターフェイス 0/0/0 が設定されたことが示されます。また、インターフェイス上のセカンダリ IP アドレスもアドバタイズされます。

```
Device# show ip ospf interface GigabitEthernet 0/2/1
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 172.16.1.1/24, Area 0
  Process ID 1, Router ID 172.16.11.11, Network Type BROADCAST, Cost: 10
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.11.11, Interface address 172.16.1.1
```

```
Backup Designated router (ID) 172.16.22.11, Interface address 172.16.1.2
Timer intervals configured, Hello 1, Dead 4, Wait 4, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:00
Supports Link-local Signaling (LLS)
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 172.26.22.11  (Backup Designated Router)
Suppress hello for 0 neighbor(s)
```

その他の参考資料

ここでは、インターフェイス上での OSPFv2 のイネーブル化に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
『Configuring OSPF』	『Configuring OSPF』
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』

標準

規格	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 2328	『*OSPF Version 2*』

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

インターフェイス単位でのOSPFv2のイネーブル化の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *49* : インターフェイス単位での *OSPFv2* のイネーブル化の機能情報

機能名	リリース	機能情報
インターフェイスごとの OSPFv2 のイネーブル化 （注） この機能は、最初は「OSPFv2 機能のインターフェイス モードにおけるエリア コマンド」と呼ばれていました。	Cisco IOS XE Release 2.1	このマニュアルでは、インターフェイス単位で OSPFv2 をイネーブルにすることにより、番号が付いていないインターフェイスの設定を簡素化する方法について説明します。**ipospfarea** コマンドを使用すると、インターフェイス上での OSPFv2 を明示的にイネーブルにできます。**ipospfarea** コマンドは、**networkarea** コマンドによって指定したアドレス範囲に一致するインターフェイスのアドレスを使用して OSPFv2 をイネーブルにするのに代わる方法になります。 次に示すコマンドは、この章に記載されている機能において、新たに導入または変更されたものです。 • **ipospfarea**

第 44 章

OSPF ノンストップ ルーティング

OSPF ノンストップ ルーティング機能を使用すると、冗長ルート プロセッサ（RP）を持つデバイスが計画内外の RP スイッチオーバーで Open Shortest Path First（OSPF）ステートと隣接関係を維持することができます。OSPF ステートは、アクティブ RP からスタンバイ RP で OSPF からステート情報のチェックポイントを実行することによって維持されます。スタンバイ RP へのスイッチオーバー後、OSPF はチェックポイントされた情報を使用して中断することなく動作を継続します。

- 機能情報の確認，461 ページ
- OSPF NSR の前提条件，462 ページ
- OSPF NSR の制約事項，462 ページ
- OSPFv3 認証トレーラに関する情報，462 ページ
- OSPF ノンストップ ルーティングの設定方法，463 ページ
- OSPF ノンストップ ルーティングの設定例，464 ページ
- その他の参考資料，465 ページ
- OSPF NSR の機能情報，466 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。

OSPF NSR の前提条件

- OSPF NSR は、Cisco IOS リリース XE 3.3S 以降のリリースを実行する冗長 RP または Cisco IOS ソフトウェア冗長性を備えたプラットフォームで使用できます。

OSPF NSR の制約事項

- OSPF ノンストップ ルーティング（NSR）では、動作の特定の段階で OSPF に使用されるメモリを大幅に増やすことができます。CPU使用率も増やすことができます。ルータのメモリ容量を認識し、OSPF NSR の考えられるメモリ要件を見積もっておく必要があります。詳細については、「OSPF NSR の設定」を参照してください。メモリと CPU が制約を受けるルータでは、代わりにOSPF NSF の使用を検討する場合があります。詳細については、OSPF RFC 3623 グレースフル リスタート ヘルパー モードを参照してください。
- アクティブからスタンバイ RP へのスイッチオーバーは、ハードウェア プラットフォームによって数秒かかることがあります。この間、OSPF は hello パケットを送信できません。そのため、短い OSPF dead 間隔を使用する設定ではスイッチオーバーで隣接関係を維持できない可能性があります。

OSPFv3 認証トレーラに関する情報

OSPF NSR 機能

OSPF ノンストップ ルーティング（NSR）は OSPF ノンストップ フォワーディング（NSF）と同様の機能を提供しますが、しくみは異なります。NSF では、新しいアクティブ スタンバイ RP の OSPF にステート情報はありません。OSPF はOSPF プロトコルの拡張を使用して、隣接するOSPF デバイスからステートを回復します。リカバリが機能するためには、ネイバーが NSF プロトコル拡張をサポートし、再起動するデバイスの「ヘルパー」として積極的に動作する必要があります。ネイバーはまた、プロトコル ステートのリカバリが行われる間、再起動するデバイスにデータ トラフィックを転送し続ける必要もあります。

一方、NSR では、スイッチオーバーを実行するデバイスはデバイス ステートを内部的に保持し、ほとんどの場合、ネイバーはスイッチオーバーを認識しません。隣接デバイスからのサポートが必要ないため、NSR は NSF を使用できない状況で使用できます。たとえば、一部のネイバーが NSF プロトコル拡張を実装していないネットワーク、または NSF を当てにできなくなるリカバリ中にネットワーク トポロジを変更するネットワークでは、NSF の代わりに NSR を使用します。

OSPF ノンストップ ルーティングの設定方法

OSPF NSR の設定

OSPF NSR を設定するには、次の作業を実行します。

NSR により、OSPF ルータ モード コンフィギュレーションに新しい 1 行「nsr」が追加されます。どんな理由であれ、NSR をサポートしないルータではこのコマンドを使用できません。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id*
4. **nsr**
5. **end**
6. **showipospf[***process-id***]nsr[[objects]|[statistics]]**

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	**routerospf***process-id* 例： `Router(config)# router ospf 109`	ルータでルータ コンフィギュレーション モードを開始し、OSPF ルーティング プロセスを設定します。
ステップ 4	**nsr** 例： `Router(config-router)# nsr`	NSR を設定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**showipospf[***process-id***]nsr[[objects]||[statistics]]** 例： `Router# show ip ospf 109 nsr`	OSPF NSR のステータス情報を表示します。

トラブルシューティングのヒント

OSPF NSR により、OSPF デバイス プロセスで使用されるメモリの量を増加できます。NSR なしでOSPF が現在使用しているメモリの量を確認するには、**showprocesses** および **showprocessesmemory** コマンドを使用します。

```
Device# show processes|include OSPF

 276 Mwe  133BE14         1900       1792    1060 8904/12000  0 OSPF-1 Router
 296 Mwe  133A824           10        971      10 8640/12000  0 OSPF-1 Hello
```

プロセス 276 は、確認する必要がある OSPF デバイス プロセスです。このプロセスの現在のメモリ使用量を表示するには、**showprocessesmemory** コマンドを使用します。

```
Device# show processes memory 276

Process ID: 276
Process Name: OSPF-1 Router
Total Memory Held: 4454800 bytes
```

上の例では、OSPF は 4,454,800 バイト、つまり約 4.5 メガバイト（MB）を使用しています。OSPF NSR は短期間にこの倍のメモリを消費する場合があるため、OSPF NSR をイネーブルにする前に、デバイスに少なくとも 5 MB の空きメモリがあることを確認してください。

OSPF ノンストップ ルーティングの設定例

例：OSPF NSR の設定

次に、OSPF NSR を設定する例を示します。

```
Device> enable
Device# configure terminal
```

```
Device(config)# router ospf 1
Device(config-router)# nsr
Device(config-router)# end
Device# show ip ospf 1 nsr
Standby RP
 Operating in duplex mode
 Redundancy state: STANDBY HOT
 Peer redundancy state: ACTIVE
 ISSU negotation complete
 ISSU versions compatible
Routing Process "ospf 1" with ID 10.1.1.100
 NSR configured
 Checkpoint message sequence number: 3290
 Standby synchronization state: synchronized
 Bulk sync operations:  1
 Last sync start time:  15:22:48.971 UTC Fri Jan 14 2011
 Last sync finish time: 15:22:48.971 UTC Fri Jan 14 2011
 Last sync lost time:   -
 Last sync reset time:  -
 LSA Count: 2, Checksum Sum 0x00008AB4
```

出力には、OSPF NSR が設定されていること、スタンバイ RP 上で OSPF が完全に同期されていて、アクティブな RP に障害が発生したり手動スイッチオーバーが実行されても操作を続行する準備ができていることが示されています。

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』
OSPF コマンド：コマンド構文の詳細、コマンドモード、デフォルト設定、コマンド履歴、使用に関する注意事項および例	『*Cisco IOS IP Routing: OSPF Command Reference*』
『Configuring OSPF』	『*IP Routing: OSPF Configuration Guide*』の「Configuring OSPF」
OSPFv2 Loop-Free Alternate Fast Reroute	『*IP Routing: OSPF Configuration Guide*』の「OSPFv2 Loop-Free Alternate Fast Reroute」

標準および RFC

標準/RFC	Title
RFC 5286	『*Basic Specification for IP Fast Reroute: Loop-Free Alternates*』

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

OSPF NSR の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *50*：*OSPF NSR* の機能情報

機能名	リリース	機能情報
OSPF NSR	XE 3.3S Cisco IOS Release 15.1(1)SY	OSPF NSR 機能により、冗長なルート プロセッサを装備したルータが、計画されたおよび計画されていない RP スイッチオーバーで、OSPF の状態と隣接関係を維持できるようになります。 この機能は、Cisco IOS Release XE 3.3S で導入されました。 次のコマンドが導入または変更されました。**nsr**、**showipospfnsr**

第 45 章

OSPFv3 NSR

OSPFv3 NSR 機能を使用すると、冗長ルート プロセッサ（RP）を持つルータが計画内外の RP スイッチオーバーで Open Shortest Path First（OSPF）ステートと隣接関係を維持することができます。これは、アクティブ RP からスタンバイ RP で OSPFv3 からステート情報のチェックポイントを実行することによって行われます。スタンバイ RP へのスイッチオーバー後、OSPFv3 はチェックポイントされたこの情報を使用して中断することなく動作を継続することができます。

- 機能情報の確認，467 ページ
- OSPFv3 NSR について，468 ページ
- OSPFv3 NSR の設定方法，468 ページ
- OSPFv3 NSR の設定例，472 ページ
- その他の参考資料，474 ページ
- OSPFv3 NSR の機能情報，475 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。

OSPFv3 NSR について

OSPFv3 NSR 機能

OSPFv3 NSR は OSPFv3 グレースフル リスタート機能と同様の機能を提供しますが、異なる方法で動作します。グレースフル リスタートでは、新しいアクティブ スタンバイ RP の OSPFv3 に最初はステート情報がないため、OSPFv3 プロトコルの拡張を使用して隣接する OSPFv3 デバイスからステートを回復します。これを機能させるには、ネイバーがグレースフル リスタート プロトコル拡張をサポートし、再起動するデバイスのヘルパーとして機能できる必要があります。また、このリカバリの実行中、再起動するデバイスへのデータ トラフィックの転送を継続する必要があります。

一方、NSR では、スイッチオーバーを実行するデバイスはデバイス ステートを内部的に保持し、ほとんどの場合、ネイバーは何かが起こっていることを認識しません。隣接デバイスからのサポートが必要ないため、NSR はグレースフル リスタートを使用できない状況で使用できます。たとえば、一部のネイバーがグレースフル リスタート プロトコル拡張を実装していないネットワーク、またはリカバリ中にネットワーク トポロジを変更するネットワークでは、グレースフル リスタートを当てにすることができません。

（注） NSR を有効にすると、OSPF の応答性と拡張性が低下します。パフォーマンスの低下は、スタンバイ ルート プロセッサ（RP）にデータをチェックポイントするのに OSPF が CPU とメモリを使用するために発生します。

OSPFv3 NSR の設定方法

OSPFv3 NSR の設定

OSPFv3 NSR を設定するには、次の作業を実行します。

（注） NSR をサポートしていないデバイスでは **nsr** (OSPFv3) コマンドを使用できません。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **routerospfv3** *process-id*
4. **nsr**
5. **end**
6. **show ospfv3** [*process-id*] [*address-family*] **nsr**

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	**configure terminal** 例： `Device# 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	**routerospfv3** *process-id* 例： `Device(config)# router ospfv3 109`	デバイスでルータ コンフィギュレーション モードを開始し、OSPFv3 ルーティング プロセスを設定します。
ステップ 4	**nsr** 例： `Device(config-router)# nsr`	NSR を設定します。
ステップ 5	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**show ospfv3** [*process-id*] [*address-family*] **nsr** 例： `Device# show ospfv3 109 nsr`	OSPFv3 NSR のステータス情報を表示します。

アドレス ファミリに対する OSPFv3 NSR の設定

アドレス ファミリ コンフィギュレーション モードでは、特定のアドレス ファミリの NSR を設定できます。アドレス ファミリの OSPFv3 NSR をイネーブルにするには、次の作業を実行します。

（注） NSR をサポートしていないデバイスでは **nsr** (OSPFv3) コマンドを使用できません。

手順の概要

1. **routerospfv3** *process-id*
2. **address-family** {**ipv4** | **ipv6**} **unicast** [**vrf***vrf-name*]
3. **nsr** [**disable**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**routerospfv3** *process-id* 例： `Device(config)# router ospfv3 109`	デバイスでルータ コンフィギュレーション モードを開始し、OSPFv3 ルーティング プロセスを設定します。
ステップ 2	**address-family** {**ipv4**	**ipv6**} **unicast** [**vrf***vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast`	OSPFv3 ルータ コンフィギュレーション モードで、IPv4 または IPv6 アドレス ファミリ 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	**nsr** [**disable**] 例： `Device(config-router-af)# nsr`	設定済みのアドレス ファミリの NSR をイネーブルにします。

アドレス ファミリの OSPFv3 NSR の表示

アドレス ファミリ コンフィギュレーション モードでは、**nsr** コマンドでオプションの **disable** キーワードを使用できます。アドレス ファミリの OSPFv3 NSR をディセーブルにするには、次の作業を実行します。

手順の概要

1. **routerospfv3** *process-id*
2. **address-family** {**ipv4** | **ipv6**} **unicast** [**vrf***vrf-name*]
3. **nsr** [**disable**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**routerospfv3** *process-id* 例： `Device(config)# router ospfv3 109`	デバイスでルータ コンフィギュレーション モードを開始し、OSPFv3 ルーティング プロセスを設定します。
ステップ 2	**address-family** {**ipv4** | **ipv6**} **unicast** [**vrf***vrf-name*] 例： `Device(config-router)# address-family ipv6 unicast`	OSPFv3 ルータ コンフィギュレーション モードで、IPv4 または IPv6 アドレス ファミリ 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	**nsr** [**disable**] 例： `Device(config-router-af)# nsr disable`	設定済みのアドレス ファミリの NSR をディセーブルにします。

トラブルシューティングのヒント

OSPFv3 NSR により、OSPFv3 デバイス プロセスで使用されるメモリの量を増加できます。NSR なしで OSPFv3 が現在使用しているメモリの量を確認するには、**showprocesses** および **showprocessesmemory** コマンドを使用します。

```
Device# show processes
 | include OSPFv3
 276 Mwe  133BE14         1900       1792    1060 8904/12000  0 OSPFv3-1 Router
 296 Mwe  133A824           10        971      10 8640/12000  0 OSPFv3-1 Hello
```

プロセス 276 は、確認する必要がある OSPFv3 デバイス プロセスです。このプロセスの現在のメモリ使用量を表示するには、**showprocessesmemory** コマンドを使用します。

```
Device# show processes memory 276
Process ID: 276
Process Name: OSPFv3-1 Router
Total Memory Held: 4454800 bytes
```

この例では、OSPFv3 は 4,454,800 バイト、つまり約 4.5 メガバイト（MB）を使用しています。OSPFv3 NSR は短期間にこの倍のメモリを消費する場合があるため、OSPFv3 NSR をイネーブルにする前に、デバイスに少なくとも 5 MB の空きメモリがあることを確認してください。

OSPFv3 NSR の設定例

例：OSPFv3 NSR の設定

次に、OSPFv3 NSR を設定し、イネーブルになっているかを確認する例を示します。

```
Device(config)# router ospfv3 1
Device(config-router)# nsr
Device(config-router)# end
Device# show ospfv3 1
  OSPFv3 1 address-family ipv4
  Router ID 10.0.0.1
  Supports NSSA (compatible with RFC 3101)
  Event-log enabled, Maximum number of events: 1000, Mode: cyclic
  It is an area border and autonomous system boundary router
  Redistributing External Routes from,
  Router is not originating router-LSAs with maximum metric
  Initial SPF schedule delay 5000 msecs
  Minimum hold time between two consecutive SPFs 10000 msecs
  Maximum wait time between two consecutive SPFs 10000 msecs
  Minimum LSA interval 5 secs
  Minimum LSA arrival 1000 msecs
  LSA group pacing timer 240 secs
  Interface flood pacing timer 33 msecs
  Retransmission pacing timer 66 msecs
  Retransmission limit dc 24 non-dc 24
  Number of external LSA 0. Checksum Sum 0x000000
  Number of areas in this router is 3. 2 normal 0 stub 1 nssa
  Non-Stop Routing enabled
  Graceful restart helper support enabled
  Reference bandwidth unit is 100 mbps
  RFC1583 compatibility enabled
     Area BACKBONE(0) (Inactive)
         Number of interfaces in this area is 1
         SPF algorithm executed 3 times
         Number of LSA 6. Checksum Sum 0x03C938
         Number of DCbitless LSA 0
         Number of indication LSA 0
         Number of DoNotAge LSA 0
         Flood list length 0
     Area 1
         Number of interfaces in this area is 3
         SPF algorithm executed 3 times
         Number of LSA 6. Checksum Sum 0x024041
         Number of DCbitless LSA 0
         Number of indication LSA 0
         Number of DoNotAge LSA 0
         Flood list length 0
     Area 3
         Number of interfaces in this area is 1
         It is a NSSA area
         Perform type-7/type-5 LSA translation
         SPF algorithm executed 4 times
         Number of LSA 5. Checksum Sum 0x024910
         Number of DCbitless LSA 0
         Number of indication LSA 0
         Number of DoNotAge LSA 0
         Flood list length 0
```

```
OSPFv3 1 address-family ipv6
Router ID 10.0.0.1
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an area border and autonomous system boundary router
Redistributing External Routes from,
   ospf 2
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Retransmission limit dc 24 non-dc 24
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 3. 2 normal 0 stub 1 nssa
Non-Stop Routing enabled
Graceful restart helper support enabled
Reference bandwidth unit is 100 mbps
RFC1583 compatibility enabled
   Area BACKBONE(0) (Inactive)
       Number of interfaces in this area is 2
       SPF algorithm executed 2 times
       Number of LSA 6. Checksum Sum 0x02BAB7
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0
   Area 1
       Number of interfaces in this area is 4
       SPF algorithm executed 2 times
       Number of LSA 7. Checksum Sum 0x04FF3A
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0
   Area 3
       Number of interfaces in this area is 1
       It is a NSSA area
       Perform type-7/type-5 LSA translation
       SPF algorithm executed 3 times
       Number of LSA 5. Checksum Sum 0x011014
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0
```

出力には、OSPFv3 NSR が設定されていることが示されています。

例：OSPFv3 NSR の確認

次に、OSPFv3 NSR ステータスを表示する例を示します。

```
Device# show ospfv3 1 nsr
  Active RP
  Operating in duplex mode
  Redundancy state: ACTIVE
  Peer redundancy state: STANDBY HOT
  Checkpoint peer ready
  Checkpoint messages enabled
  ISSU negotiation complete
  ISSU versions compatible


           OSPFv3 1 address-family ipv4 (router-id 10.0.0.1)
  NSR configured
  Checkpoint message sequence number: 29
```

```
Standby synchronization state: synchronized
Bulk sync operations:  1
Next sync check time:  12:00:14.956 PDT Wed Jun 6 2012
LSA Count: 17, Checksum Sum 0x00085289


         OSPFv3 1 address-family ipv6 (router-id 10.0.0.1)
NSR configured
Checkpoint message sequence number: 32
Standby synchronization state: synchronized
Bulk sync operations:  1
Next sync check time:  12:00:48.537 PDT Wed Jun 6 2012
LSA Count: 18, Checksum Sum 0x0008CA05
```

出力には、OSPFv3 NSR が設定されていること、スタンバイ RP 上で OSPFv3 が完全に同期されていて、アクティブな RP に障害が発生したり手動スイッチオーバーが実行されても操作を続行する準備ができていることが示されています。

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』
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
OSPFv3 アドレス ファミリ	*OSPFv3 Address Families* モジュール

標準

標準	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 5187	『*OSPFv3 Graceful Restart*』

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

OSPFv3 NSR の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *51*：*OSPFv3 NSR* の機能情報

機能名	リリース	機能情報
OSPFv3 NSR	15.1(2)SY 15.2(4)S	OSPFv3 NSR 機能により、冗長な RP を装備したルータが、計画されたおよび計画されていない RP スイッチオーバーで、OSPFv3 の状態と隣接関係を維持できるようになります。 次のコマンドが導入または変更されました。**clear ospfv3 nsr**、**nsr (OSPFv3)**、**show ospfv3 nsr**

第 46 章

OSPFv2 Loop-Free Alternate Fast Reroute

OSPFv2 Loop-Free Alternate Fast Reroute 機能では、プライマリのネクスト ホップで障害が発生したときに、事前に計算された代替のネクスト ホップを使用して障害を軽減します。プレフィックスごとの Loop-Free Alternate（LFA）パスを設定し、プライマリ ネイバー以外のネクスト ホップにトラフィックをリダイレクトすることができます。他のルータが障害を知ることなく転送の決定が行われ、サービスが復元されます。

- 機能情報の確認，477 ページ
- OSPFv2 Loop-Free Alternate Fast Reroute の前提条件，478 ページ
- OSPFv2 Loop-Free Alternate Fast Reroute の制約事項，478 ページ
- OSPFv2 Loop-Free Alternate Fast Reroute に関する情報，478 ページ
- OSPFv2 Loop-Free Alternate Fast Reroute の設定方法，481 ページ
- OSPFv2 Loop-Free Alternate Fast Reroute の設定例，487 ページ
- その他の参考資料，488 ページ
- OSPFv2 Loop-Free Alternate Fast Reroute の機能情報，490 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。

OSPFv2 Loop-Free Alternate Fast Reroute の前提条件

Open Shortest Path First（OSPF）は、フォワーディング プレーンでこの機能をサポートするプラットフォームでのみ IP FRR をサポートします。プラットフォーム サポートについては、Cisco Feature Navigator（http://www.cisco.com/go/cfn）を参照してください。Cisco.com のアカウントは必要ありません。

OSPFv2 Loop-Free Alternate Fast Reroute の制約事項

OSPFv2 Loop-Free Alternate Fast Reroute 機能は、仮想リンクのヘッドエンドであるルータではサポートされません。

OSPFv2 Loop-Free Alternate Fast Reroute 機能は、グローバル VPN ルーティングおよび転送（VRF）OSPF インスタンスでのみサポートされます。

トラフィック エンジニアリング（TE）トンネル インターフェイスは保護されたインターフェイス トラフィックとして設定できません。これらのトンネルを保護するには、MPLS トラフィック エンジニアリング - Fast Reroute リンクおよびノード保護機能を使用します。詳細については、『*Cisco IOS XE Multiprotocol Label Switching Configuration Guide*』の「MPLS Traffic Engineering--Fast Reroute Link and Node Protection」セクションを参照してください。

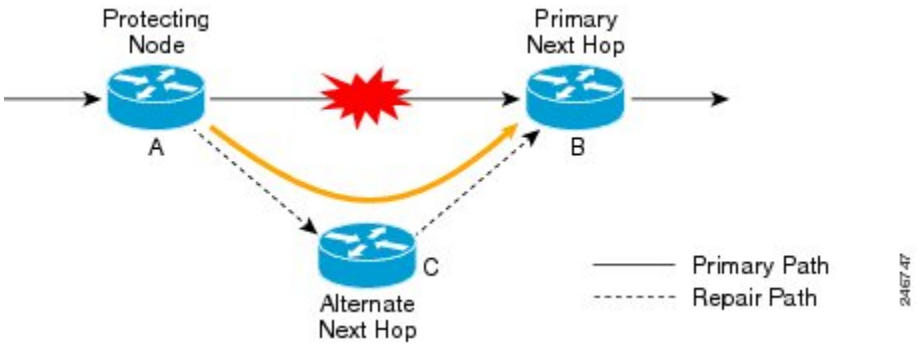
修復パスで TE トンネル インターフェイスを設定できますが、OSPF はトンネルの配置を確認しません。保護する物理インターフェイスを通らないことを確認する必要があります。

すべてのルートが修復パスを持つわけではありません。マルチパス プライマリ ルートは、ネットワーク トポロジ、コンピューティング ルータの接続、および修復パスに必要な属性に応じて、すべて、一部、またはゼロのプライマリ パスに対して修復パスを持つことがあります。

OSPFv2 Loop-Free Alternate Fast Reroute に関する情報

LFA 修復パス

リンクに障害が発生した場合に OSPFv2 Loop-Free Alternate Fast Reroute 機能がトラフィックを再ルーティングする方法を次の図に示します。保護ルータはプレフィックス単位の修復パスを事前に計算し、グローバル ルーティング情報ベース（RIB）にこれらをインストールします。保護されたプライマリ パスで障害が発生すると、保護ルータはライブ トラフィックをプライマリ パスから格納された修復パスに転送します。このとき、他のルータはネットワーク トポロジを再計算する必要がなく、ネットワーク トポロジが変更されたことを認識する必要もありません。



LFA 修復パス属性

プライマリ パスで障害が発生すると、多数のパスが修復の候補になります。OSPFv2 Loop-Free Alternate Fast Reroute 機能のデフォルト選択ポリシーでは次の順序で属性の優先順位が付けられています。

1. srlg
2. primary-path
3. interface-disjoint
4. lowest-metric
5. linecard-disjoint
6. node-protecting
7. broadcast-interface-disjoint

評価によって候補が選択されない場合、修復パスは暗黙的なロード バランシングによって選択されます。これは、修復パスの選択がプレフィックスによって変わることを意味します。

show ip ospf fast-reroute コマンドを使用すると、現在の設定を表示できます。

fast-reroute tie-break コマンドを使用すると、候補から選択するために、次のセクションで説明する 1 つ以上の修復パス属性を設定できます。

共有リスク リンク グループ

共有リスク リンク グループ（SRLG）は、同時に障害が発生する可能性が高い修復パスおよび保護されたプライマリ パスのネクストホップ インターフェイスのグループです。OSPFv2 ループフリー Fast Reroute 機能では、コンピューティング ルータでローカルに設定された SRLG のみがサポートされます。単一の物理インターフェイス上の VLAN は SRLG の例です。物理インターフェイスで障害が発生すると、すべての VLAN インターフェイスが同時にエラーになります。デフォルトの修復パス属性では、ある VLAN のプライマリ パスが別の VLAN 上の修復パスによって保護される可能性があります。srlg 属性を設定すると、LFA 修復パスがプライマリ パスと同じ SRLG ID を共有しないように指定することができます。インターフェイスを SRLG に割り当てるには、**srlg** コマンドを使用します。

インターフェイスの保護

ポイントツーポイントインターフェイスには、プライマリ ゲートウェイで障害が発生した場合、再ルーティングのための代替のネクスト ホップはありません。interface-disjoint 属性を設定すると、このような修復パスの選択を防ぐことができるため、インターフェイスが保護されます。

ブロードキャスト インターフェイス保護

LFA 修復パスは、修復パスと保護されたプライマリ パスが異なるネクストホップ インターフェイスを使用するときにリンクを保護します。ただし、ブロードキャストインターフェイスでは、LFA 修復パスがプライマリ パスと同じインターフェイスを介して計算されても、ネクストホップ ゲートウェイが異なる場合、ノードは保護されますがリンクは保護されないことがあります。broadcast-interface-disjoint 属性を設定すると、プライマリ パスがポイントするブロードキャスト ネットワークを修復パスが経由しない（つまり、インターフェイスと、これに接続されるブロードキャスト ネットワークを使用できない）ように指定することができます。

このタイブレーカーを必要とするネットワーク トポロジについては、RFC 5286 の『Broadcast and Non-Broadcast Multi-Access (NBMA) Links』、「*Basic Specification for IP Fast Reroute: Loop-Free Alternates*」を参照してください。

ノード保護

デフォルトの修復パス属性では、プライマリ パスのネクストホップであるルータは保護されないことがあります。ノード保護属性を設定すると、修復パスがプライマリパス ゲートウェイ ルータをバイパスするように指定することができます。

ダウンストリーム パス

高レベルのネットワーク障害や複数の同時ネットワーク障害が発生すると、代替パスを介して送信されるトラフィックはOSPFがプライマリ パスを再計算するまでループする可能性があります。downstream 属性を設定して、保護された宛先への修復パスのメトリックが保護ノードの宛先へのメトリックより小さくなる必要があるように指定することができます。これによりトラフィックが失われる可能性がありますが、ループは防止されます。

ラインカード Disjoint インターフェイス

ラインカードにラインカードの活性挿抜（OIR）などの問題がある場合、同じラインカード上のすべてのインターフェイスで同時に障害が発生するため、ラインカードインターフェイスはSRLGと似ています。linecard-disjoint 属性を設定すると、LFA 修復パスがプライマリパスのライン カードのものとは異なるインターフェイスを使用するように指定することができます。

メトリック

LFA 修復パスは最も効率的な候補である必要はありません。高レベルのネットワーク障害に対する保護機能を提供する場合、高コストな修理パスがより魅力的と考えられることがあります。メトリック属性を設定すると、最小のメトリックを持つ修復パス ポリシーを指定することができます。

等コスト マルチパス プライマリ パス

プライマリ最短パス優先（SPF）修復時に検出される等コスト マルチパス パス（ECMP）は、トラフィックが任意の単一リンクの容量を超過することがわかっているネットワーク設計では望ましくないことがあります。primary-path 属性を設定して ECMP セットから LFA 修復パスを指定したり、secondary-path 属性を設定して ECMP セットからでない LFA 修復パスを指定したりすることができます。

修復パスの候補リスト

OSPF は修復パスを計算するとき、メモリを節約するため、すべての候補パスのうちベスト パスのみをローカル RIB に保持します。**fast-reroute keep-all-paths** コマンドを使用すると、考えられたすべての修復パス候補のリストを作成できます。この情報はトラブルシューティングに役立つ可能性がありますが、メモリ消費が大幅に増加することがあるため、テストとデバッグを目的として使用する必要があります。

OSPFv2 Loop-Free Alternate Fast Reroute の設定方法

プレフィックスごとの OSPFv2 Loop-Free Alternate Fast Reroute のイネーブル化

プレフィックスごとの OSPFv2 Loop-Free Alternate Fast Reroute をイネーブル化して、OSPF エリアでのプレフィックス優先度を選択するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id*
4. **fast-rerouteper-prefixenableprefix-priority***priority-level*
5. **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	**routerospf***process-id* 例： `Router(config)# router ospf 10`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**fast-rerouteper-prefixenableprefix-priority***priority-level* 例： `Router (config-router)# fast-reroute per-prefix enable prefix-priority low`	修復パス計算をイネーブルにし、修理パスのプライオリティ レベルを選択します。 • プライオリティを低くすると、すべてのプレフィックスの保護の基準が同じになります。プライオリティを高くすると、プライオリティの高いプレフィックスのみが保護されます。
ステップ 5	**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、グローバル コンフィギュレーション モードに戻ります。

LFA FRR によるプレフィックス保護の指定

どのプレフィックスを LFA FRR で保護するかを指定するには、次の作業を実行します。ルートマップで指定されたプレフィックスだけが保護されます。

（注） ルート マップでは、次の 3 つの match キーワードだけ が認識されます：**match tag**、**match route-type**、および **match ip address prefix-list**。

>

手順の概要

1. イネーブル化
2. **configureterminal**
3. **route-map***map-tag* [permit | deny] [*sequence-number*]
4. **matchtag***tag-name*
5. **exit**
6. **routerospf***process-id*
7. **prefix-priority***priority-level***route-map***map-tag*
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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	**route-map***map-tag* [permit | deny] [*sequence-number*] 例： `Router(config)# route-map OSPF-PREFIX-PRIORITY`	ルート マップ コンフィギュレーション モードを開始し、マップ名を指定します。
ステップ 4	**matchtag***tag-name* 例： `Router(config-route-map)# match tag 886`	照合されるプレフィックスを指定します。 • タグと一致するプレフィックスだけが保護されます。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Router(config-route-map)# exit`	ルートマップインターフェイスコンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**routerospf***process-id* 例： `Router(config)# router ospf 10`	OSPF ルーティングをイネーブルにして、ルータ 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	**prefix-priority***priority-level***route-map***map-tag* 例： `Router(config-router)# prefix-priority high route-map OSPF-PREFIX-PRIORITY`	修復パスの優先度レベルを設定し、プレフィックスを定義するルート マップを指定します。
ステップ 8	**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、グローバル コンフィギュレーション モードに戻ります。

修復パスの選択ポリシーの設定

タイブレーキング状態を指定して修復パス選択ポリシーを設定するには、次の作業を実行します。タイブレーキング属性の詳細については、LFA 修復パス属性, （479 ページ）を参照してください）。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id*
4. **fast-rerouteper-prefixtie-break***attribute***[required]index***index-level*
5. **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	**routerospf***process-id* 例： `Router(config)# router ospf 10`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**fast-rerouteper-prefixtie-break***attribute* **[required]index***index-level* 例： `Router(config-router)# fast-reroute per-prefix tie-break srlg required index 10`	タイブレーキング状態を指定して優先度レベルを設定することにより、修復パス選択ポリシーを設定します。
ステップ 5	**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、グローバル コンフィギュレーション モードに戻ります。

考慮する修復パス リストの作成

LFA FRR に対して検討されるパス リストを作成するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospf***process-id*
4. **fast-reroutekeep-all-paths**
5. **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	**routerospf***process-id* 例： `Router(config)# router ospf 10`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**fast-reroutekeep-all-paths** 例： `Router(config-router)# fast-reroute keep-all-paths`	LFA FRR に対して検討されるパス リストを作成するよう指定します。
ステップ 5	**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、グローバル コンフィギュレーション モードに戻ります。

インターフェイスのネクスト ホップとしての使用の禁止

インターフェイスが修復パスでネクスト ホップとして使用されるのを禁止するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipospffast-rerouteper-prefixcandidatedisable**
5. **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	**interface***typenumber* 例： `Router(config)# interface GigabitEthernet 0/0/0`	指定したインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipospffast-rerouteper-prefixcandidatedisable** 例： `Router(config-if)# ip ospf fast-reroute per-prefix candidate disable`	インターフェイスが修復パスでネクスト ホップとして使用されるのを禁止します。
ステップ 5	**exit** 例： `Router(config-if)# exit`	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、グローバル コンフィギュレーション モードに戻ります。

OSPFv2 Loop-Free Alternate Fast Reroute の設定例

例：プレフィックスごとの LFA IP FRR のイネーブル化

次に、プレフィックスごとの OSPFv2 Loop-Free Alternate Fast Reroute をイネーブル化して、OSPF エリアでのプレフィックス優先度を選択する例を示します。

```
Router(config)# router ospf 10
fast-reroute per-prefix enable prefix-priority low
```

例：プレフィックス保護優先度の指定

次に、どのプレフィックスを LFA FRR で保護するかを指定する例を示します。

```
Router(config)# router ospf 10
prefix-priority high route-map OSPF-PREFIX-PRIORITY
fast-reroute per-prefix enable prefix-priority high
network 192.0.2.1 255.255.255.0 area 0
route-map OSPF-PREFIX-PRIORITY permit 10
match tag 866
```

例：修復パスの選択ポリシーの設定

次に、タイブレーキング属性として、SRLG、ラインカード障害、およびダウンストリームを設定し、それらの優先度インデックスを設定する修復パス選択ポリシーを設定する例を示します。

```
router ospf 10
  fast-reroute per-prefix enable prefix-priority low
  fast-reroute per-prefix tie-break srlg required index 10
  fast-reroute per-prefix tie-break linecard-disjoint index 15
  fast-reroute per-prefix tie-break downstream index 20
  network 192.0.2.1 255.255.255.0 area 0
```

例：修復パスの選択の監視

次に、修復パスの選択を記録する例を示します。

```
router ospf 10
  fast-reroute per-prefix enable prefix-priority low
  fast-reroute keep-all-paths
  network 192.0.2.1 255.255.255.0 area 0
```

例：インターフェイスの保護インターフェイス化の禁止

次に、インターフェイスの保護インターフェイス化を禁止する例を示します。

```
Router(config)# interface GigabitEthernet 0/0/0
  ip addres
s 192.0.2.1 255.255.255.0
  ip ospf fast-reroute per-prefix candidate disable
```

その他の参考資料

ここでは、OSPF RFC 3623 のグレースフル リスタート機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
OSPF 設定	『Configuring OSPF』
Cisco ノンストップ フォワーディング	『Cisco Nonstop Forwarding』
『OSPFv3 Graceful Restart』	*OSPFv3 Graceful Restart* モジュール

標準

規格	Title
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 2328	『*OSPF Version 2*』
RFC 3623	『*Graceful OSPF Restart*』

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、Cisco.com でまず登録手続きを行ってください。	http://www.cisco.com/en/US/support/index.html

OSPFv2 Loop-Free Alternate Fast Reroute の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *52*：*OSPFv2 Loop-Free Alternate Fast Reroute* の機能情報

機能名	リリース	機能情報
OSPFv2 Loop-Free Alternate Fast Reroute	Cisco IOS XE Release 3.4S	この機能では、プライマリのネクスト ホップが失敗した場合に、事前に計算された代替のネクスト ホップを使用して、障害対応時間を短縮します。 次のコマンドが導入または変更されました。 **debugipospffast-reroute**、**fast-reroutekeep-all-paths**、**fast-rerouteper-prefix(OSPF)**、**fast-reroutetie-break(OSPF)**、**ipospffast-rerouteper-prefix**、**prefix-priority**、**showipospffast-reroute**、**showipospfinterface**、**showipospfneighbor**、**showipospfrib**

第 47 章

OSPFv3 MIB

OSPFv3 MIB 機能は、標準の Simple Network Management Protocol（SNMP）管理ワークステーションを使用する、Open Shortest Path First バージョン 3（OSPFv3）プロセスのリモート モニタリングおよびトラブルシューティングを可能にします。OSPFv3 の MIB オブジェクトおよびトラップ オブジェクトによって収集したプロトコル情報からは、ネットワーク全体のパフォーマンスのモニタリングと改善に役立つ統計情報を生成できます。

- 機能情報の確認，493 ページ
- OSPFv3 MIB の前提条件，494 ページ
- OSPFv3 MIB サポートの制約事項，494 ページ
- OSPFv3 MIB について，494 ページ
- OSPFv3 MIB の設定方法，495 ページ
- OSPFv3 MIB の設定例，497 ページ
- OSPFv3 MIB に関する追加情報，498 ページ
- OSPFv3 MIB の機能情報，499 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。

OSPFv3 MIB の前提条件

- Open Shortest Path First バージョン 3（OSPFv3）がデバイスで設定されていることを確認します。
- 通知（トラップ）の設定または SNMP GET 操作を行う前に、Simple Network Management Protocol（SNMP）がデバイスでイネーブルになっていることを確認します。

OSPFv3 MIB サポートの制約事項

- 複数の Open Shortest Path First バージョン 3（OSPFv3）プロセスをモニタするには、各プロセスを Simple Network Management Protocol（SNMP）コンテキストに関連付ける必要があります。
- 複数の VRF をモニタするには、各 VRF を SNMP コンテキストと関連付ける必要があります。

OSPFv3 MIB について

OSPFv3 MIB

Open Shortest Path First バージョン 3（OSPFv3）は、OSPF の IPv6 実装です。OSPFv3 MIB は RFC 5643 に記述されており、Simple Network Management Protocol（SNMP）を介して OSPFv3 プロセスを管理するための MIB を定義しています。

ユーザは、MIB オブジェクトを使用することで OSPF ネットワークの変化するステートを継続的にモニタすることができます。MIB オブジェクトは、プロトコル パラメータ、および移行ステート変更などの重要なネットワーク イベントの発生を通知できるトラップ通知オブジェクトに関する情報を収集します。

OSPFv3 トラップ MIB

ospfv3Notifications MIB オブジェクトには、Cisco IOS CLI で OSPF トラップのイネーブル化およびディセーブル化を行う OSPFv3 トラップ MIB オブジェクトが含まれています。これらの OSPFv3 トラップ MIB オブジェクトは、RFC 5643 の標準 OSPFv3 MIB で提供されています。

OSPFv3 MIB の設定方法

特定の OSPFv3 トラップのイネーブル化

手順の概要

1. イネーブル化
2. **configure terminal**
3. **snmp-serverhost** {*hostname* | *ip-address*} [**vrf***vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port***port*] [*notification-type*]
4. **snmp-serverenabletrapsospfv3errors**[**bad-packet**] [**config-error**] [**virt-bad-packet**] [**virt-config-error**]
5. **snmp-serverenabletrapsospfv3rate-limit** *seconds trap-number*
6. **snmp-serverenabletrapsospfv3state-change**[**if-state-change**] [**neighbor-restart-helper-status-change**] [**neighbor-state-change**] [**nssa-translator-status-change**] [**restart-status-change**] [**virtif-state-change**] [**virtneighbor-restart-helper-status-change**] [**virtneighbor-state-change**]
7. **end**

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	**configure terminal** 例： `Device# 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	**snmp-serverhost** {*hostname* | *ip-address*} [**vrf***vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port***port*] [*notification-type*] 例： `Device(config)# snmp-server host 172.20.2.162 version 2c public ospfv3`	簡易ネットワーク管理プロトコル（SNMP）通知操作の受信者（ターゲット ホスト）を指定します。 • *notification-type* が指定されていない場合は、イネーブルになっている全通知（トラップまたは応答要求）が、指定されたホストに送信されます。 • 指定されたホストに Open Shortest Path First バージョン 3（OSPFv3）通知だけを送信するには、オプションの **ospfv3** キーワー

	コマンドまたはアクション	目的
		ドを *notification-types* として指定します。**ospfv3** キーワードを入力すると、ospfv3Notifications MIB オブジェクトがイネーブルになります。
ステップ 4	**snmp-serverenabletrapsospfv3errors**[**bad-packet**] [**config-error**] [**virt-bad-packet**] [**virt-config-error**] 例： `Device(config)# snmp-server enable traps ospfv3 errors`	OSPFv3 エラーに関する SNMP 通知をイネーブルにします。
ステップ 5	**snmp-serverenabletrapsospfv3rate-limit** *seconds trap-number* 例： `Device(config)# snmp-server enable traps ospfv3 rate-limit 20 20`	各 OSPFv3 SNMP 通知のレート制限ウィンドウで、送信される SNMP OSPFv3 通知の数に対するレート制限を設定します。
ステップ 6	**snmp-serverenabletrapsospfv3state-change**[**if-state-change**] [**neighbor-restart-helper-status-change**] [**neighbor-state-change**] [**nssa-translator-status-change**] [**restart-status-change**] [**virtif-state-change**] [**virtneighbor-restart-helper-status-change**] [**virtneighbor-state-change**] 例： `Device(config)# snmp-server enable traps ospfv3 state-change`	OSPFv3 の移行状態の変更に関する SNMP OSPFv3 通知をイネーブルにします。
ステップ 7	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

デバイスでの OSPFv3 MIB トラップの確認

手順の概要

1. イネーブル化
2. **showrunning-config**[*options*]

手順の詳細

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 **showrunning-config**[*options*]

例：

```
Device# show running-config | include traps
```

現在の実行コンフィギュレーション ファイルの内容を表示します。イネーブルになっているトラップに関する情報が含まれています。

- イネーブルになっているトラップを確認します。

OSPFv3 MIB の設定例

例：OSPFv3 MIB トラップのイネーブル化と確認

次に、すべての OSPFv3 エラー トラップをイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# snmp-server enable traps ospfv3 errors
Device(config)# end
```

次に、トラップがイネーブルされていることを確認する例を示します。

```
Device> enable
Device# show running-config | include traps

snmp-server enable traps ospfv3 errors
```

OSPFv3 MIB に関する追加情報

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 Command List, All Releases』
OSPF コマンド	『Cisco IOS IP Routing: OSPF Command Reference』
OSPF の設定タスク	『*IP Routing: OSPF Configuration Guide*』の Configuring OSPF モジュール

標準および RFC

規格	Title
RFC 5643	『*Management Information Base for OSPFv3*』

MIB

MIB	MIB のリンク
OSPFv3 MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

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

OSPFv3 MIB の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *53*：*OSPFv3 MIB* の機能情報

機能名	リリース	機能情報
OSPFv3 MIB	Cisco IOS XE Release 3.7S	OSPFv3 MIB 機能により、標準の SNMP 管理ワークステーションを使用した OSPFv3 プロセスのリモート モニタリングおよびトラブルシューティングが可能になります。 次のコマンドが導入または変更されました。**snmp-server host**、**snmp-server enable traps ospfv3 errors**、**snmp-server enable traps ospfv3 rate-limit**、**snmp-server enable traps ospfv3 state-change**

第 48 章

OSPFv3 のプレフィックス抑制のサポート

この機能を使用すると、Open Shortest Path First バージョン 3（OSPFv3）でリンクステート アドバタイズメント（LSA）から接続済みネットワークの IPv4 および IPv6 プレフィックスを隠すことができます。OSPFv3 が大規模ネットワークに配置されている場合、OSPFv3 LSA に伝送される IPv4 および IPv6 プレフィックスの数を制限すると OSPFv3 のコンバージェンス速度を上げることができます。

この機能では、ネットワーク管理者が内部ノードへの IP ルーティングを回避できるようにすることにより、OSPFv3 ネットワークのセキュリティも強化されます。

- 機能情報の確認，501 ページ
- OSPFv3 のプレフィックス抑制サポートの前提条件，502 ページ
- OSPFv3 プレフィックス抑制サポートについて，502 ページ
- OSPFv3 プレフィックス抑制サポートの設定方法，503 ページ
- OSPFv3 プレフィックス抑制サポートの設定例，508 ページ
- OSPFv3 プレフィックス抑制サポートに関する追加情報，509 ページ
- OSPFv3 プレフィックス抑制サポートの機能情報，509 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。

OSPFv3 のプレフィックス抑制サポートの前提条件

このメカニズムを使用して IPv4 および IPv6 プレフィックスを LSA から除外するには、その前に OSPFv3 ルーティング プロトコルを設定しておく必要があります。

OSPFv3 プレフィックス抑制サポートについて

OSPFv3 プレフィックス抑制サポート

OSPFv3 プレフィックス抑制サポート機能を使用すると、OSPFv3 を実行しているインターフェイスで設定された IPv4 および IPv6 プレフィックスを隠すことができます。

OSPFv3 では、アドレッシング セマンティクスが OSPF プロトコル パケットと主な LSA タイプから削除され、ネットワーク プロトコルを選ばないコアが残っています。これは、ルータ LSA とネットワーク LSA がネットワーク アドレスを含まなくなり、単にトポロジ情報を表すことを意味します。プレフィックスを隠すプロセスは OSPFv3 でより単純であり、非表示のプレフィックスはエリア内プレフィックス LSA から単に削除されます。プレフィックスはまた、リンク LSA を介して OSPFv3 で伝播されます。

OSPFv3 プレフィックス抑制機能では多くの利点があります。特定のプレフィックスのアドバタイズメントの除外は、LSA ストレージ、LSA フラッディングの帯域幅とバッファ、LSA の発信とフラッディングの CPU サイクル、および SPF 計算により多くのメモリを使用できることを意味します。プレフィックスはまた、リンク LSA からもフィルタリングされます。デバイスは、ローカルに設定されたプレフィックスのみをフィルタリングし、リンク LSA を介して学習したプレフィックスはフィルタリングしません。また、中継のみのネットワークを隠してリモート攻撃の可能性を減らすことでセキュリティが改善されています。

OSPFv3 プロセスの設定による IPv4 および IPv6 プレフィックス アドバタイズメントのグローバルな抑制

prefix-suppression コマンドをルータ コンフィギュレーション モードまたはアドレスファミリ コンフィギュレーション モードで使用し、デバイス上で OSPFv3 プロセスを設定すると、すべての IPv4 および IPv6 プレフィックスのアドバタイズメントを防ぎ、OSPFv3 のコンバージェンス時間を短縮できます。

（注） ループバック、セカンダリ IP アドレス、およびパッシブ インターフェイスと関連付けられたプレフィックスは、通常のネットワーク設計では到達可能であり続けるためにプレフィックスが必要になるため、**routermode** または **address-family** 設定コマンドによって抑制されません。

インターフェイスごとの IPv4 および IPv6 プレフィックス アドバタイズメントの抑制

インターフェイス コンフィギュレーション モードで **ipv6ospfprefix-suppression** コマンドまたは **ospfv3prefix-suppression** コマンドを使用すると、OSPFv3 インターフェイスが IP ネットワークをネイバーにアドバタイズしないように明示的に設定することができます。

（注） **prefix-suppression** ルータ コンフィギュレーション コマンドを設定して、接続している IP ネットワークから IPv4 および IPv6 プレフィックスをグローバルに抑制した場合、インターフェイス コンフィギュレーション コマンドは、ルータ コンフィギュレーション コマンドよりも優先されます。

OSPFv3 プレフィックス抑制サポートの設定方法

OSPFv3 プロセスのプレフィックス抑制サポートの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospfv3***process-id*[**vrf***vpn-name*]
4. **prefix-suppression**
5. **end**
6. **showospfv3**

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	**configureterminal** 例： `Device# 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	**routerospfv3***process-id*[**vrf***vpn-name*] 例： `Device(config)# router ospfv3 23`	OSPFv3 ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**prefix-suppression** 例： `Device(config-router)# prefix-suppression`	ループバック、セカンダリ IP アドレスおよびパッシブ インターフェイスに関連付けられているプレフィックスを除き、すべての IPv4 および IPv6 プレフィックスを OSPFv3 がアドバタイズするのを防ぎます。
ステップ 5	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 6	**showospfv3** 例： `Device# show ospfv3`	OSPFv3 ルーティング プロセスに関する一般的な情報を表示します。 （注） このコマンドを使用して、IPv4 および IPv6 プレフィックスの抑制がイネーブルになっていることを確認します。

アドレス ファミリ コンフィギュレーション モードでの OSPFv3 プレフィックス抑制サポートの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospfv3***process-id*[**vrf***vpn-name*]
4. **address-familyipv6unicast**
5. **prefix-suppression**
6. **end**
7. **showospfv3**

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	**configureterminal** 例： `Device# 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	**routerospfv3***process-id*[**vrf***vpn-name*] 例： `Device(config)# router ospfv3 23`	OSPFv3 ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-familyipv6unicast** 例： `Device(config-router)# address-family ipv6 unicast`	OSPFv3 の IPv6 アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**prefix-suppression** 例： `Device(config-router-af)# prefix-suppression`	ループバック、セカンダリ IP アドレスおよびパッシブ インターフェイスに関連付けられているプレフィックスを除き、すべての IPv4 および IPv6 プレフィックスを OSPFv3 がアドバタイズするのを防ぎます。
ステップ 6	**end** 例： `Device(config-router-af)# end`	特権 EXEC モードに戻ります。
ステップ 7	**showospfv3** 例： `Device# show ospfv3`	OSPFv3 ルーティング プロセスに関する一般的な情報を表示します。 （注） このコマンドを使用して、IPv4 および IPv6 プレフィックスの抑制がイネーブルになっていることを確認します。

インターフェイス単位でのプレフィックス抑制サポートの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. 次のいずれかを実行します。
   - **ipv6ospfprefix-suppression**[**disable**]
   - **ospfv3prefix-suppressiondisable**
5. **end**
6. **showospfv3interface**

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	**configureterminal** 例： `Device# 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	**interface***typenumber* 例： `Device(config)# interface serial 0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	次のいずれかを実行します。 • **ipv6ospfprefix-suppression**[**disable**] • **ospfv3prefix-suppressiondisable** 例： `Device(config-if)# ipv6 ospf prefix-suppression`	セカンダリ IP アドレスに関連付けられているプレフィックスを除き、特定のインターフェイスに属する IPv4 および IPv6 プレフィックスを OSPFv3 がアドバタイズするのを防止します。 • インターフェイス コンフィギュレーション モードで入力された **ipv6ospfprefix-suppression** コマンドまたは **ospfv3prefix-suppression** コマンドは、ルータ コンフィ

	コマンドまたはアクション	目的
	例： `Device(config-if)# ospfv3 1 prefix-suppression disable`	ギュレーション モードで入力された **prefix-suppression** コマンドより優先されます。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**showospfv3interface** 例： `Device# show ospfv3 interface`	OSPFv3 関連のインターフェイス情報を表示します。 （注） このコマンドで、IPv4 および IPv6 プレフィックス抑制が特定のインターフェイスでイネーブルになっていることを確認します。

IPv4 および IPv6 プレフィックス抑制のトラブルシューティング

手順の概要

1. イネーブル化
2. **debugospfv3lsa-generation**
3. **debugconditioninterface***interface-typeinterface-number* [**dlci***dlci*] [**vc** {*vci* | *vpi* | *vci*}]
4. **showdebugging**
5. **showlogging**[**slot***slot-number* | **summary**]

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	**debugospfv3lsa-generation** 例： `Device# debug ospfv3 lsa-generation`	生成された OSPFv3 LSA のそれぞれ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 3	**debugconditioninterface***interface-typeinterface-number* [**dlci***dlci*] [**vc** {*vci* | *vpi* | *vci*}] 例： `Device# debug condition interface serial 0/0`	インターフェイスまたは仮想回線に基づいて、一部の **debug** コマンドの出力を制限します。
ステップ 4	**showdebugging** 例： `Device# show debugging`	デバイスでイネーブルに設定されているデバッグのタイプに関する情報を表示します。
ステップ 5	**showlogging**[**slot***slot-number* | **summary**] 例： `Device# show logging`	syslog の状態と標準システム ロギング バッファの内容を表示します。

OSPFv3 プレフィックス抑制サポートの設定例

例：OSPFv3 プレフィックス抑制サポートの設定

次に、ルータ コンフィギュレーション モードで OSPFv3 のプレフィックス抑制サポートを設定する例を示します。

```
router ospfv3 1
 prefix-suppression
 !
 address-family ipv6 unicast
  router-id 0.0.0.6
  exit-address-family
```

次に、アドレス ファミリ コンフィギュレーション モードで OSPFv3 のプレフィックス抑制サポートを設定する例を示します。

```
router ospfv3 1
 !
 address-family ipv6 unicast
  router-id 10.0.0.6
  prefix-suppression
  exit-address-family
```

次に、インターフェイス コンフィギュレーション モードで OSPFv3 のプレフィックス抑制サポートを設定する例を示します。

```
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0
 ipv6 address 2001:201::201/64
```

```
ipv6 enable
ospfv3 prefix-suppression
ospfv3 1 ipv4 area 0
ospfv3 1 ipv6 area 0
end
```

OSPFv3 プレフィックス抑制サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
『Configuring OSPF』	『Configuring OSPF』
OSPF コマンド	『Cisco IOS IP Routing: OSPF Command Reference』
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

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

OSPFv3 プレフィックス抑制サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *54* : *OSPFv3* プレフィックス抑制サポートの機能情報

機能名	リリース	機能情報
OSPFv3 のプレフィックス抑制のサポート	Cisco IOS XE Release 3.8S	この機能を使用すると、Open Shortest Path First バージョン 3（OSPFv3）でリンクステートアドバタイズメント（LSA）から接続済みネットワークの IPv4 および IPv6 プレフィックスを隠すことができます。 この機能を使用して、ネットワーク管理者が内部ノードへの IP ルーティングを回避できるようにすることにより、OSPFv3 ネットワークのセキュリティも強化することもできます。 次のコマンドが導入または変更されました。 • **ipv6ospfprefix-suppression** • **ospfv3prefix-suppression** • **prefix-suppression (OSPFv3)**

第 49 章

OSPFv3 VRF-Lite/PE-CE

OSPFv3 VRF-Lite/PE-CE 機能では、デフォルト以外の VPN ルーティングおよび転送（VRF）インスタンスに対して Open Shortest Path First バージョン 3（OSPFv3）のサポートが追加されます。OSPFv3 は、RFC 6565、「*OSPFv3 as a Provider Edge to Customer Edge (PE-CE) Routing Protocol*」で指定されているように、プロバイダーエッジ - カスタマーエッジ（PE-CE）ルーティング プロトコルとして使用できます。デフォルト以外の VRF インスタンスの OSPFv3 では、IPv4 および IPv6 アドレス ファミリのルーティングがサポートされます。

- 機能情報の確認，511 ページ
- OSPFv3 VRF-Lite/PE-CE の制約事項，512 ページ
- OSPFv3 VRF-Lite/PE-CE について，512 ページ
- VRF-Lite/PE-CE の設定方法，513 ページ
- OSPFv3 VRF-Lite/PE-CE の設定例，522 ページ
- OSPFv3 VRF-Lite/PE-CE に関する追加情報，524 ページ
- OSPFv3 VRF-Lite/PE-CE の機能情報，525 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。

OSPFv3 VRF-Lite/PE-CE の制約事項

Cisco IOS Release 15.2(2)S 以降のリリースでは、VRF インターフェイス コンフィギュレーション モードで**ipv6 ospf**形式の OSPFv3 インターフェイス コマンドはサポートされません。新しいフォーマット **ospfv3** でコマンドを設定する必要があります。

ospfv3 コマンドは次のいずれかの形式にできます。

- **ospfv3**：指定されたインターフェイス上のすべての OSPFv3 プロセスおよびアドレス ファミリに適用されます。
- **ospfv3***process-id*：プロセス ID が設定済みの OSPFv3 プロセス、および IPv4 アドレス ファミリと IPv6 アドレス ファミリの両方に適用されます。
- **ospfv3***process-idaddress-family-ID*：プロセス ID とアドレス ファミリが設定済みの OSPFv3 プロセスに適用されます。

次に降順で示すように、より特定性の高いコマンドが特定性の低いコマンドより優先されます。

1. プロセス ID とアドレス ファミリを指定するコマンド。
2. プロセス ID だけを指定するコマンド。
3. プロセス ID もアドレス ファミリも指定しないコマンド。

Cisco IOS Release 15.2(2)S 以降のリリースでは、**ipv6 ospf router***process-id* コマンドを使用して OSPFv3 VRF インスタンスを設定することはできません。グローバル コンフィギュレーション モードで **router ospfv3***process-id* コマンドを設定し、ルータ コンフィギュレーション モードで設定済みの VRF のアドレス ファミリを指定することができます。

OSPFv3 VRF-Lite/PE-CE について

OSPFv3 VRF-Lite および PE-CE のサポート

Open Shortest Path First バージョン 3（OSPFv3）は IPv4 と IPv6 の両方のアドレス ファミリの非デフォルトの VPN ルーティングおよび転送（VRF）インスタンスで動作し、Border Gateway Protocol（BGP）またはマルチプロトコル ラベル スイッチング（MPLS）のバックボーンを介してルートを転送します。プロバイダー エッジ（PE）デバイスでは、顧客のルートは共通の VRF またはアドレス ファミリの OSPFv3 および BGP によって一緒にインストールされ、各プロトコルは別のプロトコルのルートを再配布するように設定されます。BGP は再配布されたプレフィックスを VRF に定義されている route-distinguisher 値と組み合わせ、必要に応じて VPNv4 または VPNv6 アドレス ファミリを使用する同じ自律システム内の他の MPLS-BGP スピーカーにアドバタイズします。

OSPFv3 ルート選択アルゴリズムでは、MPLS バックボーンを介したエリア間ルートよりも、バックドア リンクを経由するエリア内ルートを優先します。模造リンクは、異なる PE の OSPFv3 インスタンスを接続する MPLS バックボーンを介した仮想リンクの 1 つです。OSPFv3 インスタン

スは、バックボーンを使用してプロトコル パケットをトンネリングし、隣接関係を確立します。OSPFv3 は模造リンクをエリア内接続と見なすため、模造リンクはエリア内バックドア リンクの有効な代わりとして機能します。

ドメイン ID はルートが内部と外部のどちらであるかを判断するために使用されます。これらは、ルートが始まる OSPFv3 インスタンスの管理ドメインを説明しています。すべての PE に 48 ビットのプライマリ ドメイン ID（NULL の可能性もあり）と、ゼロ個以上のセカンダリ ドメイン ID があります。

VRF-Lite/PE-CE の設定方法

IPv6 アドレス ファミリでの VRF への OSPFv3 の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **routerospfv3**[*process-id*]
7. **address-family ipv6** [**unicast**] [**vrf***vrf-name*]
8. **end**

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	**configure terminal** 例： `Device# 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	**vrf definition** *vrf-name* 例： `Device(config)# vrf definition vrfsample`	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 10:1`	VRF のルーティング テーブルと転送テーブルを作成します。
ステップ 5	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**routerospfv3**[*process-id*] 例： `Device(config)# router ospfv3 2`	OSPF ルーティング プロセスを設定し、ルータ 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	**address-family ipv6** [**unicast**] [**vrf***vrf-name*] 例： `Device(config-router)# address-family ipv6 unicast vrf vrfsample`	IPv6 アドレス ファミリの VRF ルーティング テーブルで OSPFv3 プロセスのインスタンスを設定し、ルータ アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 8	**end** 例： `Device(config-router-af)# end`	ルータ アドレス ファミリ 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。

VRF インターフェイスでの OSPFv3 IPv6 アドレス ファミリのイネーブル化

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name* [**downstream** *vrf-name2*]
5. **ipv6 enable**
6. **ospfv3***process-id* {**ipv4** | **ipv6**} **area***area-id* [**instance***instance-id*]
7. **end**

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	**configure terminal** 例： `Device# 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	**interface** *type number* 例： `Device(config)# interface Serial6/0`	インターフェイスのタイプと番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**vrf forwarding** *vrf-name* [**downstream** *vrf-name2*] 例： `Device(config-if)# vrf forwarding v1`	インターフェイスを VRF に関連付けます。
ステップ 5	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	VRF に関連付けられたインターフェイスで IPv6 処理をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 6	**ospfv3***process-id* {**ipv4** | **ipv6**} **area***area-id* [**instance***instance-id*] 例： `Device(config-if)# ospfv3 1 ipv6 area 0`	VRF インターフェイスで OSPFv3 IPv6 アドレス ファミリをイネーブルにします。
ステップ 7	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。

OSPFv3 PE-CE への模造リンクの設定

はじめる前に

OSPFv3 PE-CE 機能は、ボーダー ゲートウェイ プロトコル（BGP）ルート上の直接転送をサポートします。

模造リンクを設定する前に、マルチプロトコル ラベル スイッチング（MPLS）のバックボーンを作成し、MPLS VPN の PE デバイスとしてデバイスを設定し、Virtual Routing and Forwarding（VRF）インスタンスのプロバイダー エッジ カスタマー エッジ（PE-CE）プロトコルとして OSPFv3 を設定する必要があります。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interfaceloopback***interface-number*
4. **description***string*
5. **vrfforwarding***vrf-name*
6. **ipv6address** *ipv6-address/prefix-length*
7. **ipv6enable**
8. **end**
9. **router ospfv3***process-id*
10. **address-family** {**ipv4** | **ipv6**} [**unicast** | **multicast**] [**vrf***vrf-name*]
11. **redistribute***process-id* [*options*]
12. **area***area-id***sham-link***source-address destination-address* [**cost***number*] [**ttl-security hops***hop-count*]
13. **end**

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	**configure terminal** 例： `Device# 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	**interfaceloopback***interface-number* 例： `Device(config)# interface loopback 0`	プロバイダー エッジ デバイスで模造リンクのエンドポイントとして使用するループバック インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**description***string* 例： `Device(config-if)# description Sham-link endpoint`	インターフェイスのステータスを追跡し易くするために、インターフェイスの説明を追加します。
ステップ 5	**vrfforwarding***vrf-name* 例： `Device(config-if)# vrf forwarding vrf1`	ループバック インターフェイスに VRF を関連付けます。
ステップ 6	**ipv6address** *ipv6-address/prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:0:ABCD::1/48`	プロバイダー エッジ デバイス上のループバック インターフェイスの IPv6 アドレスを設定します。
ステップ 7	**ipv6enable** 例： `Device(config-if)# ipv6 enable`	ループバック インターフェイスで IPv6 処理をイネーブルにします。
ステップ 8	**end** 例： `Device# end`	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、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**router ospfv3***process-id* 例： `Device(config)# router ospfv3 1`	ルータ コンフィギュレーション モードを開始します。
ステップ 10	**address-family** {**ipv4** | **ipv6**} [**unicast** | **multicast**] [**vrf***vrf-name*] 例： `Device(config-router)# address-family ipv6 unicast vrf vrf1`	OSPFv3 の IPv6 アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 11	**redistribute***process-id* [*options*] 例： `Device(config-router-af)# redistribute bgp 2`	指定した送信元 BGP ルーティング ドメインから指定した宛先のルーティング ドメインに IPv6 ルートを再配布します。 （注） PE-CE は常に BGP から再配布します。
ステップ 12	**area***area-id***sham-link***source-address destination-address* [**cost***number*] [**ttl-security hops***hop-count*] 例： `Device(config-router-af)# area 0 sham-link 2001:DB8:0:ABCD::1 2001:DB8:0:ABCD::2 cost 100`	模造リンクをイネーブルにして、送信元と宛先のアドレスを指定します。
ステップ 13	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

OSPFv3 PE-CE へのドメイン ID の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **routerospfv3**[*process-id*]
7. **address-family ipv6** [**unicast**] [**vrf***vrf-name*]
8. **domain-idtype***type***value** *hex-value*
9. **end**

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	**configure terminal** 例： `Device# 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	**vrf definition** *vrf-name* 例： `Device(config)# vrf definition vrfsample`	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 10:1`	VRF のルーティング テーブルと転送テーブルを作成します。
ステップ 5	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**routerospfv3**[*process-id*] 例： `Device(config)# router ospfv3 2`	ルータ 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	**address-family ipv6** [**unicast**] [**vrf***vrf-name*] 例： `Device(config-router)# address-family ipv6 unicast vrf vrfsample`	IPv6 アドレス ファミリの VRF ルーティング テーブルで OSPFv3 プロセスのインスタンスを設定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 8	**domain-idtype***type***value** *hex-value* 例： `Device(config-router-af)# domain-id type 0205 value 800EFFFF12AB`	BGP ドメイン ID を設定します。 • **type** の値は、0005、0105、0205、または 8005 のいずれかです。 • **value** の値は、12 の 16 進数の数字として符号化された任意の 48 ビット値です。
ステップ 9	**end** 例： `Device(config-router-af)# end`	ルータ アドレス ファミリ 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。

OSPFv3 への VRF-Lite 機能の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **routerospfv3**[*process-id*]
7. **address-family ipv6** [**unicast**] [**vrf***vrf-name*]
8. **capabilityvrf-lite**
9. **end**

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	**configure terminal** 例： `Device# 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	**vrf definition** *vrf-name* 例： `Device(config)# vrf definition vrfsample`	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 10:1`	VRF のルーティング テーブルと転送テーブルを作成します。
ステップ 5	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**routerospfv3**[*process-id*] 例： `Device(config)# router ospfv3 2`	IPv4 または IPv6 アドレス ファミリのルータ コンフィギュレーション モードをイネーブルにします。
ステップ 7	**address-family ipv6** [**unicast**] [**vrf***vrf-name*] 例： `Device(config-router)# address-family ipv6 unicast vrf vrfsample`	IPv6 アドレス ファミリの VRF ルーティング テーブルで OSPFv3 プロセスのインスタンスを設定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 8	**capabilityvrf-lite** 例： `Device(config-router-af)# capability vrf-lite`	OSPF プロセスにマルチ VRF 機能を適用します。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config-router-af)# end`	ルータ アドレス ファミリ 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。

OSPFv3 VRF-Lite/PE-CE の設定例

例：IPv4 および IPv6 ルーティングを提供するためのプロバイダーエッジ デバイスの設定

次に、VRF「v1」上のユーザに IPv6 および IPv4 ルーティングを、VRF「v2」上のユーザに IPv6 ルーティングを提供するために、プロバイダーエッジ（PE）デバイスを設定する例を示します。

```
vrf definition v1
 rd 1:1
 route-target export 100:1
 route-target import 100:1
!
address-family ipv4
 exit-address-family
!
address-family ipv6
 exit-address-family
!
vrf definition v2
 rd 2:2
 route-target export 200:2
 route-target import 200:2
!
address-family ipv6
 exit-address-family
!
interface Loopback1
 vrf forwarding v1
 ipv6 address 2001:DB8:0:ABCD::1/48
!
interface Serial5/0
 vrf forwarding v2
 no ip address
 ipv6 address 2001:DB8:0:ABCD::3/48
 ospfv3 1 ipv6 area 1
!
interface Serial6/0
 vrf forwarding v1
 ip address 10.0.0.1 255.255.255.0
 ipv6 enable
 ospfv3 1 ipv6 area 0
 ospfv3 1 ipv4 area 10.1.1.1
!
router ospfv3
!
log-adjacency-changes detail
```

```
!
address-family ipv4 unicast vrf v1
 router-id 10.2.2.2
 redistribute bgp 1
 exit-address-family
!
address-family ipv6 unicast vrf v1
 router-id 2001:DB8:1::1
 domain-id type 0205 value 111111222222
 area 0 sham-link 2001:DB8:0:ABCD::5 2001:DB8:0:ABCD::7
 redistribute bgp 1
 exit-address-family
address-family ipv6 unicast vrf v2
 router-id 2001:DB8:1::3
 redistribute bgp 1
 exit
!
router bgp 1
 bgp router-id 10.3.3.3
 no bgp default ipv4-unicast
 neighbor 10.0.0.4 remote-as 1
 neighbor 10.0.0.4 update-source-Loopback0
!
address-family ipv4
 exit-address-family
!
address-family vpnv4
 neighbor 10.0.0.4
 neighbor 10.0.0.4 send-community extended
 exit-address-family
!
address-family vpnv6
 neighbor 10.0.0.4 activate
 neighbor 10.0.0.4 send-community extended
 exit-address-family
!
address-family ipv4 vrf v1
 redistribute ospfv3 1
 exit-address-family
!
address-family ipv6 vrf v1
 redistribute ospf 1
 exit-address-family
!
address-family ipv6 vrf v2
 redistribute ospf 1
 exit-address-family
!
```

例：VRF-Lite に対するプロバイダー エッジ デバイスの設定

```
vrf definition v1
 rd 1:1
 !
address-family ipv4
 exit-address-family
!
address-family ipv6
 exit-address-family
!
vrf definition v2
 rd 2:2
 !
address-family ipv6
 exit-address-family
!
interface FastEthernet0/0
 no ip address
 !
```

```
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 vrf forwarding v1
 ip address 192.168.1.1 255.255.255.0
 ipv6 enable
 ospfv3 1 ipv6 area 0
 ospfv3 1 ipv4 area 0
!
interface FastEthernet0/0.200
 encapsulation dot1Q 200
 vrf forwarding v2
 ipv6 enable
 ospfv3 1 ipv6 area 0
!
interface FastEthernet0/1
 rf forwarding v1
 ip address 10.1.1.1 255.255.255.0
 ipv6 enable
 ospfv3 1 ipv6 area 1
 ospfv3 1 ipv4 area 0
 no keepalive
!
interface FastEthernet0/2
 vrf forwarding v2
 no ip address
 ipv6 address 2001:DB8:1::1
 ipv6 enable
 ospfv3 1 ipv6 area 1
!
router ospfv3 1
!
address-family ipv6 unicast vrf v2
 router-id 192.168.2.1
 capability vrf-lite
 exit-address-family
!
address-family ipv4 unicast vrf v1
  router-id 192.168.1.4
  capability vrf-lite
exit-address-family
!
address-family ipv6 unicast vrf v1
 router-id 192.168.1.1
 capability vrf-lite
 exit-address-family
!
```

OSPFv3 VRF-Lite/PE-CE に関する追加情報

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 Command List, All Releases』
OSPF コマンド	『Cisco IOS IP Routing: OSPF Command Reference』

RFC

RFC	Title
RFC 5838	『Support of Address Families in OSPFv3』
RFC 6565	『OSPFv3 as a Provider Edge to Customer Edge (PE-CE) Routing Protocol』

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

OSPFv3 VRF-Lite/PE-CE の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *55*：*OSPFv3 VRF-Lite/PE-CE* の機能情報

機能名	リリース	機能情報
OSPFv3 VRF-Lite/PE-CE	Cisco IOS XE Release 3.6S	OSPFv3 VRF-Lite/PE-CE 機能では、非デフォルトの VRF インスタンスに OSPFv3 サポートが追加されます。 次のコマンドが導入または変更されました。**area sham-link**（OSPFv3）、**capability vrf-lite**（OSPFv3）

第 50 章

OSPFv3 ABR タイプ 3 LSA フィルタリング

この機能によって Open Shortest Path First バージョン 3（OSPFv3）プロトコルを実行しているエリア境界ルータ（ABR）の機能が拡張され、異なる OSPFv3 エリア間で送信されるフィルタ タイプ 3 リンクステートアドバタイズメント（LSA）をフィルタリングできます。この機能を使用すると、1 つのエリアから他のエリアに指定したプレフィックスの付いたパケットだけが送信され、他のプレフィックスのついたパケットはすべて制限されます。このタイプのエリア フィルタリングは、特定の OSPFv3 エリアから、特定の OSPFv3 エリアへ、または同じ OSPFv3 エリアへ（から）同時に適用できます。

- 機能情報の確認，527 ページ
- OSPFv3 ABR タイプ 3 LSA フィルタリング，528 ページ
- OSPFv3 ABR タイプ 3 LSA フィルタリングについて，528 ページ
- OSPFv3 ABR タイプ 3 LSA フィルタリングの設定方法，528 ページ
- OSPFv3 ABR タイプ 3 LSA フィルタリングの設定例，529 ページ
- OSPFv3 ABR タイプ 3 LSA フィルタリングに関する追加情報，530 ページ
- OSPFv3 ABR タイプ 3 LSA フィルタリングの機能情報，531 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。

OSPFv3 ABR タイプ 3 LSA フィルタリング

OSPFv3 ABR タイプ 3 LSA フィルタリング

フィルタリングされるのは、ABR から送信されるタイプ 3 LSA だけです。

OSPFv3 ABR タイプ 3 LSA フィルタリングについて

エリア フィルタのサポート

OSPFv3 エリア フィルタを使用すると、ABR でエリア間プレフィックス LSA のフィルタリングを行うことができます。フィルタは、IPv6 プレフィックスのリストに基づき、両方向に適用できます。「イン」方向では、エリア間プレフィックス LSA を指定したエリアに送信するときに他のすべてのエリアからの LSA を除外します。「アウト」方向では、指定したエリアに対して生成されたエリア間プレフィックス LSA を除外します。

エリア フィルタのサポート機能により、管理者による OSPFv3 エリア間のルート配布の制御が改善されます。

OSPFv3 ABR タイプ 3 LSA フィルタリングの設定方法

OSPFv3 のエリア フィルタ サポートの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerospfv3***process-id*
4. **area***area-id***filter-listprefix***prefix-list-name* {**in** | **out**}
5. **end**
6. **ipv6prefix-list***list-name* [**seq***seq-number*] {**deny***ipv6-prefix*/*prefix-length* | **permit***ipv6-prefix*/*prefix-length* | **description** *text*} [**ge***ge-value*] [**le***le-value*]

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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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	**routerospfv3***process-id* 例： `Device(config)# router ospfv3 1`	OSPFv3 プロセスを実行するよう、ルータを設定します。
ステップ 4	**area***area-id***filter-listprefix***prefix-list-name* {**in** | **out**} 例： `Device(config-router)# area 1 filter-list prefix test_ipv6 out`	指定したエリアから送信されるエリア間ルートをフィルタリングするよう、ルータを設定します。
ステップ 5	**end** 例： `Device(config-router)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ipv6prefix-list***list-name* [**seq***seq-number*] {**deny***ipv6-prefix*/*prefix-length* | **permit***ipv6-prefix*/*prefix-length* | **description** *text*} [**ge***ge-value*] [**le***le-value*] 例： `Device(config)# ipv6 prefix-list test_ipv6 seq 5 permit 2011::1/128`	*list-name* 引数に指定した名前で、プレフィックス リストを作成します。

OSPFv3 ABR タイプ 3 LSA フィルタリングの設定例

例：OSPFv3 のエリア フィルタ サポート

次に、OSPFv3 のエリア フィルタ サポートを設定する例を示します。

```
router ospfv3 1
!
address-family ipv4 unicast
 area 2 filter-list prefix test_ipv4 in
exit-address-family
!
```

```
address-family ipv6 unicast
 area 2 filter-list prefix test_ipv6 in
exit-address-family
!
ip prefix-list test_ipv4 seq 5 permit 2.2.2.2/32
!
!
ipv6 prefix-list test_ipv6 seq 5 deny 2011::1/128
```

OSPFv3 ABR タイプ 3 LSA フィルタリングに関する追加情報

関連資料

関連項目	マニュアル タイトル
『Configuring OSPF』	『Configuring OSPF』
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』

標準

規格	Title
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	—

RFC

RFC	Title
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	—

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

OSPFv3 ABR タイプ 3 LSA フィルタリングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *56*：*OSPFv3 ABR* タイプ *3 LSA* フィルタリングの機能情報

機能名	リリース	機能情報
OSPFv3 ABR タイプ 3 LSA フィルタリング	Cisco IOS XE Release 3.8 15.3(1)S 15.2(1)E	OSPFv3 ABR タイプ 3 LSA フィルタリング機能では、OSPFv3 プロトコルを実行している ABR の機能を拡張して、異なる OSPFv3 エリア間で送信されるタイプ 3 LSA をフィルタリングできます。この機能を使用すると、1 つのエリアから他のエリアに指定したプレフィックスの付いたパケットだけが送信され、他のプレフィックスのついたパケットはすべて制限されます。このタイプのエリア フィルタリングは、特定の OSPFv3 エリアから、特定の OSPFv3 エリアへ、または同じ OSPFv3 エリアへ（から）同時に適用できます。

第 51 章

OSPFv3 デマンド回路の無視

この機能を有効にすると、**ipv6ospfdemand-circuit** コマンドで ignore キーワードを指定することにより、インターフェイスがその他のデバイスからのデマンド回路の要求を受け入れないようにすることができます。

- 機能情報の確認，533 ページ
- OSPFv3 デマンド回線無視について，534 ページ
- OSPFv3 デマンド回線無視の設定方法，534 ページ
- OSPFv3 デマンド回線無視の設定例，536 ページ
- OSPFv3 デマンド回線無視に関する追加情報，536 ページ
- OSPFv3 デマンド回線無視の機能情報，537 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。

OSPFv3 デマンド回線無視について

デマンド回線の無視のサポート

デマンド回線の無視のサポートを有効にすると、**ipv6ospfdemand-circuit** コマンドで ignore キーワードを指定することにより、インターフェイスがその他のデバイスからのデマンド回路の要求を受け入れないようにすることができます。デマンド回路の無視はルータがデマンド回路（DC）ネゴシエーションを受け入れないように指示するため、ハブ ルータのポイントツーマルチポイント インターフェイスに便利な設定オプションです。

OSPFv3 デマンド回線無視の設定方法

OSPFv3 デマンド回線無視の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. 次のいずれかのコマンドを入力します。
   - **ipv6ospfdemand-circuitignore**
   - **ospfv3demand-circuitignore**
5. **end**
6. **showospfv3***process-id*[*area-id*][*address-family*]**[vrf** {*vrf-name*|*****}] **interface** [*typenumber*] [**brief**]

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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet 0/1/0`	インターフェイスのタイプと番号を設定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかのコマンドを入力します。
	• **ipv6ospfdemand-circuitignore**
	• **ospfv3demand-circuitignore**
	例：
	`Device(config-if)# ipv6 ospf demand-circuit ignore`
	例：
	`Device(config-if)# ospfv3 demand-circuit ignore`
		インターフェイスが他のデバイスからのデマンド回線要求を受け入れるのを防止します。

ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**showospfv3***process-id*[*area-id*][*address-family*]**[vrf** {*vrf-name*|*****}] **interface** [*typenumber*] [**brief**] 例： `Device# show ospfv3 interface GigabitEthernet 0/1/0`	（任意）OSPFv3 関連のインターフェイス情報を表示します。

OSPFv3 デマンド回線無視の設定例

例：OSPFv3 デマンド回線無視のサポート

次に、OSPFv3 デマンド回線無視のサポートを設定する例を示します。

```
interface Serial0/0
 ip address 6.1.1.1 255.255.255.0
 ipv6 enable
 ospfv3 network point-to-multipoint
 ospfv3 demand-circuit ignore
 ospfv3 1 ipv6 area 0
```

OSPFv3 デマンド回線無視に関する追加情報

ここでは、OSPFv3 デマンド回線無視機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
OSPF の設定タスク	『Configuring OSPF』
OSPF コマンド	『*Cisco IOS IP Routing: OSPF Command Reference*』
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

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

OSPFv3 デマンド回線無視の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *57* : *OSPFv3* デマンド回線無視の機能情報

機能名	リリース	機能情報
OSPFv3 デマンド回路の無視	Cisco IOS XE Release 3.8	OSPFv3 デマンド回線無視機能では、**ipv6ospfdemand-circuit** コマンドで ignore キーワードを指定することにより、インターフェイスが他のデバイスからデマンド回線要求を受け入れるのを防ぐことができます。 次のコマンドが導入または変更されました。 • **ipv6ospfdemand-circuit** • **ospfv3demand-circuit**

第 52 章

OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute

OSPF IPv4 リモート Loop-Free Alternate（LFA）IP Fast Reroute（IPFRR）では、ネットワークに障害が発生した場合、ダイナミック ルーティング プロトコルを使用して事前に計算されたバックアップ ルートを使用します。バックアップ ルート（修復パス）は事前に計算され、プライマリ パスのバックアップとしてルータにインストールされます。ルータは、リンクまたは隣接ノードの障がいを検出すると、バックアップ パスに切り替えてトラフィック損失を回避します。

OSPF IPv4 リモート LFA IPFRR では、バックアップ パスを複数のホップにすることができます。この機能は、LFA を保護ルータに直接接続する必要がない一部のトポロジ（一般的なリング トポロジなど）で特に役立ちます。

- 機能情報の確認，539 ページ
- OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute の前提条件，540 ページ
- OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute の制約事項，540 ページ
- OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute について，541 ページ
- OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute の設定方法，542 ページ
- OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute の設定例，545 ページ
- その他の参考資料，546 ページ
- OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute の機能情報，547 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。

OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute の前提条件

- このモジュールの作業を実行する前に、「OSPFv2 Loop-Free Alternate Fast Reroute」モジュールで説明している概念をよく理解しておく必要があります。
- LFA が有効である必要があります。
- ネットワークでマルチプロトコル ラベル スイッチング（MPLS）を設定している必要があります。

OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute の制約事項

- OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute 機能は、仮想リンク ヘッドエンド デバイスではサポートされません。
- この機能は、グローバル VPN ルーティングおよび転送（VRF）OSPF インスタンスでのみサポートされます。
- サポートされるトンネリング メソッドは MPLS のみです。
- トラフィック エンジニアリング（TE）トンネル インターフェイスは保護されたインターフェイス トラフィックとして設定できません。これらのトンネルを保護するには、MPLS トラフィック エンジニアリング：高速再ルーティングおよびノード保護機能を使用します。詳細については、『*Multiprotocol Label Switching Configuration Guide*』の「MPLS Traffic Engineering—Fast Reroute Link and Node Protection」の項を参照してください。
- TE トンネル インターフェイスを修復パス内に設定することは可能ですが、OSPF によりトンネルの配置が確認されることはないため、保護する必要がある物理インターフェイスに交差しないようにする必要があります。
- すべてのルートが修復パスを持つわけではありません。マルチパスのプライマリ ルートでは、修復パスをすべてまたは一部のプライマリ パスに指定するか、またはいずれのプライマリ パスにも指定しない場合があります。これは、ネットワーク トポロジ、コンピューティング ルータの接続性、および修復パスの必須属性によって決定されます。
- トンネルの終端ポイントとして選択できるデバイスには、リモート LFA がイネーブルになっているエリアでアドバタイズされる /32 アドレスが必要です。このアドレスはトンネル終端

の IP として使用されます。デバイスが /32 アドレスをアドバタイズしない場合、リモート LFA トンネルの終端として使用されない場合があります。

- トンネルの終端点として選択できるようにするネットワーク内のデバイスはすべて、**mpls ldp discovery targeted-hello accept** コマンドにより、ターゲットを絞った LDP セッションを受け入れるよう設定される必要があります。

OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute について

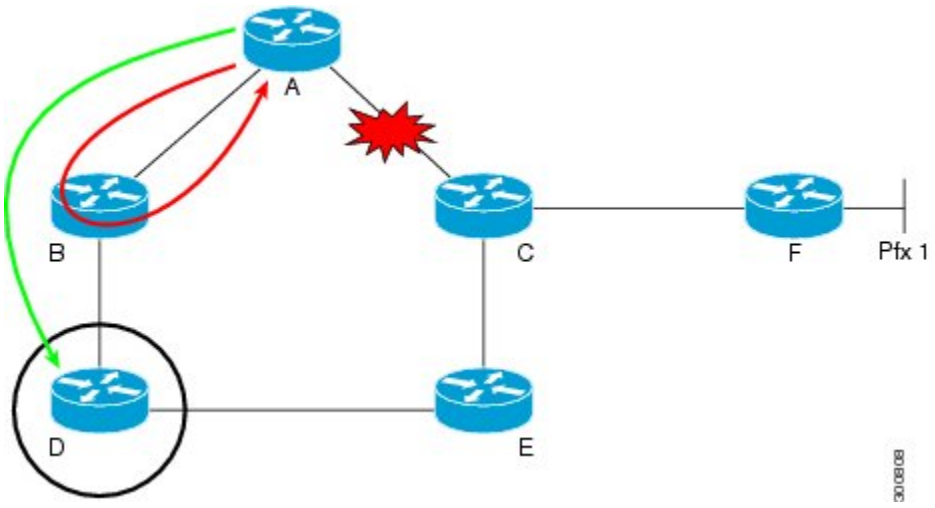
IP 高速再ルーティング

IP 高速再ルーティング（IPFRR）の LFA 計算は、リンク障害に対する保護を提供します。ローカルで計算された修復パスを使用して、障害後ネットワークの再収束で生じるループによるパケット損失を防止します。IPFRR についての詳細は、RFC 5286「*Basic Specification for IP Fast Reroute: Loop-Free Alternates*」を参照してください。

リング トポロジを含む OSPF IPv4 リモート IPFRR LFA

一部のトポロジ（一般に使用されるリング ベース のトポロジなど）は、LFA FRR で提供できない保護を必要とします。下の図 のトポロジについて考えます。

図 *12*：リング トポロジを含むリモート *IPFRR LFA*



赤色のループしている矢印は、ノード A と C の間に障害が起きた直後（ネットワークの再コンバージェンス前）にループしたトラフィックを表しています。デバイス A は、F を宛先として B

にネクストホップするトラフィックを送信しようと試みます。ノード C および F によってアドバタイズされているプレフィックスの LFA として、デバイス B を使用することはできません。ただし、ノード D は、保護ノード A に直接接続されていません。C によりアドバタイズされるプレフィックスを保護するには、障害中のリンクをトンネルが通過しない条件で、ノード A は、障害中の A - C リンクを含むパケットをノード D までトンネリングする必要があります。

OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute 機能により、障害のあるリンクを含むパケットを、リモート Loop-Free Alternate（複数の離れたホップ）までトンネリングすることができます。上の図で、A と D の間の緑色の矢印は、OSPF の IPv4 リモート Loop-Free Alternate IP Fast Reroute 機能により、ルーピングをバイパスするために自動的に生成されたトンネルを表しています。

（注） 上の図では、リモート LFA をイネーブルにするためにデバイス A を **fast-reroute per-prefix remote-lfa tunnel mpls-ldp** で設定し、ターゲットを絞った LDP セッションを受け入れるために、デバイス D を **mpls ldp discovery targeted-hello accept** で設定する必要があります。

OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute の設定方法

リモート LFA トンネルの設定

リモート LFA トンネルにトラフィックをリダイレクトするプレフィックスごとの LFA FRR パスを設定するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **router ospf***process-id*
4. **fast-reroute per-prefix remote-lfa** [**area***area-id*] **tunnel mpls-ldp**

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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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	**router ospf***process-id* 例： `Device(config)# router ospf 10`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**fast-reroute per-prefix remote-lfa** [**area***area-id*] **tunnel mpls-ldp** 例： `Device(config-router)# fast-reroute per-prefix remote-lfa area 2 tunnel mpls-ldp`	MPLS-LDP によってリモート LFA トンネルにトラフィックをリダイレクトするプレフィックスごとの LFA FRR パスを設定します。 • LFA FRR を有効にするエリアを指定するには、**area***area-id* キーワードおよび引数を使用します。

トンネル エンドポイントまでの最大距離の設定

リモート LFA トンネルにトラフィックをリダイレクトするプレフィックスごとの LFA FRR パス内のトンネル エンドポイントへの最大距離を設定するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **router ospf***process-id*
4. **fast-reroute per-prefix remote-lfa** [**area***area-id*] **maximum-cost***distance*

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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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	**router ospf***process-id* 例： `Device(config)# router ospf 10`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**fast-reroute per-prefix remote-lfa** [**area***area-id*] **maximum-cost***distance* 例： `Device(config-router)# fast-reroute per-prefix remote-lfa area 2 maximum-cost 30`	リモート LFA トンネルにトラフィックをリダイレクトするプレフィックスごとの LFA FRR パス内のトンネル エンドポイントへの最大距離を設定します。 • LFA FRR を有効にするエリアを指定するには、**area***area-id* キーワードおよび変数を使用します。

OSPF IPv4 リモート LFA IPFRR により作成されるトンネル インターフェイスの確認

手順の概要

1. イネーブル化
2. **show ip ospffast-rerouteremote-lfa tunnels**

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）。

	コマンドまたはアクション	目的
ステップ 2	**show ip ospffast-rerouteremote-lfa tunnels** 例： `Device# show ip ospf fast-reroute remote-lfa tunnels`	OSPF のプレフィックスごとの LFA FRR 設定に関する情報を表示します。

OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute の設定例

例：リモート LFA トンネルの設定

次に、エリア 2 でプレフィックスごとのリモート LFA FRR を設定する例を示します。リモートトンネルのタイプには MPLS-LDP が指定されています。

```
Router(config-router)# fast-reroute per-prefix remote-lfa area 2 tunnel mpls-ldp
```

例：トンネル エンドポイントまでの最大距離の設定

次に、エリア 2 の最大コストを 30 を設定する例を示します。

```
Router(config-router)# fast-reroute per-prefix remote-lfa area 2 maximum-cost 30
```

例：OSPF IPv4 リモート LFA IPFRR により作成されるトンネル インターフェイスの確認

次の例に、OSPF IPv4 LFA IPFRR によって作成されたトンネル インターフェイスに関する情報を示します。

```
Router# show ip ospf fast-reroute remote-lfa tunnels

      OSPF Router with ID (192.168.1.1) (Process ID 1)
      Area with ID (0)
      Base Topology (MTID 0)

Interface MPLS-Remote-Lfa3
 Tunnel type: MPLS-LDP
 Tailend router ID: 192.168.3.3
 Termination IP address: 192.168.3.3
 Outgoing interface: Ethernet0/0
 First hop gateway: 192.168.14.4
 Tunnel metric: 20
 Protects:
  192.168.12.2 Ethernet0/1, total metric 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』
OSPF コマンド：コマンド構文の詳細、コマンドモード、デフォルト設定、コマンド履歴、使用に関する注意事項および例	『*Cisco IOS IP Routing: OSPF Command Reference*』
『Configuring OSPF』	『*IP Routing: OSPF Configuration Guide*』の「Configuring OSPF」
OSPFv2 Loop-Free Alternate Fast Reroute	『*IP Routing: OSPF Configuration Guide*』の「OSPFv2 Loop-Free Alternate Fast Reroute」

標準および RFC

標準/RFC	Title
RFC 5286	『*Basic Specification for IP Fast Reroute: Loop-Free Alternates*』

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

OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *58*：*OSPF IPv4* リモート *Loop-Free Alternate IP Fast Reroute* の機能情報

機能名	リリース	機能情報
OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute	15.2(2)S Cisco IOS XE Release 3.11S	OSPF IPv4 リモート Loop-Free Alternate IP Fast Reroute 機能により、パスが複数の離れたホップである場合でも、ノード障害時のバックアップ修復パスが有効になります。 次のコマンドが導入または変更されました。 **fast-reroute per-prefix remote-lfa maximum-cost**、**fast-reroute per-prefix remote-lfa tunnel** および **show ip ospf fast-reroute**

第 53 章

OSPFv3 マルチエリア隣接関係

OSPFv3 マルチエリア隣接関係を使用すると、最適化されたルーティングを可能にするために Open Shortest Path First バージョン 3（OSPFv3）エリアが共有できるリンクを設定することができます。既存の OSPFv3 プライマリ インターフェイスには複数のエリアを追加できます。

- 機能情報の確認，549 ページ
- OSPFv3 マルチエリア隣接関係の前提条件，550 ページ
- OSPFv3 マルチエリア隣接関係の制約事項，550 ページ
- OSPFv3 マルチエリア隣接関係について，550 ページ
- OSPFv3 マルチエリア隣接関係の設定方法，551 ページ
- OSPFv3 マルチエリア隣接関係の確認，553 ページ
- OSPFv3 マルチエリア隣接関係の設定例，553 ページ
- OSPFv3 マルチエリア隣接関係に関する追加情報，555 ページ
- OSPFv3 マルチエリア隣接関係の機能情報，555 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。

OSPFv3 マルチエリア隣接関係の前提条件

- Open Shortest Path First バージョン 3（OSPFv3）がプライマリ インターフェイスで設定されていることを確認します。
- プライマリ インターフェイス タイプがポイントツーポイントであることを確認します。

OSPFv3 マルチエリア隣接関係の制約事項

- マルチエリア インターフェイスは、プライマリ インターフェイスで OSPFv3 が設定されており、プライマリ インターフェイスの OSPFv3 ネットワーク タイプがポイントツーポイントである場合のみ動作します。
- マルチエリア インターフェイスは、OSPFv3 のプライマリ インターフェイス上の論理構成体として存在しますが、プライマリ インターフェイス上のネイバー ステートは、マルチエリア インターフェイスと無関係です。
- マルチエリア インターフェイスは、隣接するデバイス上の対応するマルチエリア インターフェイスとの隣接関係を確立します。マルチエリアとプライマリ インターフェイスの混在はサポートされていません。
- ネイバー ステートがフルの場合、マルチエリア インターフェイスは、デバイスのリンク ステートアドバタイズメント（LSA）内の他のデバイスへのポイントツーポイント接続を、対応するエリアにアドバタイズします。
- マルチエリア インターフェイスはプライマリ インターフェイスからすべての OSPFv3 パラメータ（認証など）を継承します。マルチエリア インターフェイスでパラメータを設定することはできませんが、プライマリ インターフェイスではパラメータを設定できます。

OSPFv3 マルチエリア隣接関係について

OSPFv3 マルチエリア隣接関係の概要

Open Shortest Path First バージョン 3（OSPFv3）では、単一の物理リンクを複数のエリアで共有することができます。このため、同じリンクを共有する該当のエリアそれぞれにエリア内パスを作成します。すべてのエリアには、OSPFv3 を設定できるインターフェイスがあります。これらのインターフェイスの 1 つがプライマリ インターフェイスとして、その他がセカンダリ インターフェイスとして指定されます。

OSPFv3 マルチエリア隣接関係機能を使用すると、プライマリ インターフェイスにリンクを設定し、複数のエリアで最適化されたルーティングを有効にすることができます。各マルチエリア インターフェイスは、ポイントツーポイントアンナンバードリンクとして表明されます。マルチエ

リア インターフェイスは、既存のプライマリ インターフェイス上の論理構成体として存在します。プライマリ インターフェイス上のネイバー ステートはマルチエリア インターフェイスのネイバー ステートには依存しません。マルチエリアインターフェイスは隣接デバイス上の対応するマルチエリア インターフェイスとのネイバー関係を確立します。2 つの OSPFv3 スピーカーのあるインターフェイスでのみマルチエリア隣接関係を設定できます。

プライマリ OSPFv3 インターフェイスでマルチエリア隣接関係を設定するには、**ospfv3 multi-area** コマンドを使用します。

OSPFv3 マルチエリア隣接関係の設定方法

OSPFv3 マルチエリア隣接関係の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 enable**
5. **ospfv3 multi-area** *multi-area-id*
6. **ospfv3 multi-area** *multi-area-id* **cost** *interface-cost*
7. **ospfv3** *process-id* **ipv6 area** *area-id*
8. **serial restart-delay** *count*
9. **end**

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	**configure terminal** 例： `Device# 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	**interface** *type number* 例： `Device(config)# interface serial 2/0`	インターフェイス タイプおよび番号を指定します。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 5	**ospfv3 multi-area** *multi-area-id* 例： `Device(config-if)# ospfv3 multi-area 100`	インターフェイスでマルチエリア隣接関係を設定します。 • *multi-area-id* 引数は、OSPFv3 マルチエリアを示します。範囲は 0 ～ 4294967295 にするか、または IP アドレスを使用できます。
ステップ 6	**ospfv3 multi-area** *multi-area-id* **cost** *interface-cost* 例： `Device(config-if)# ospfv3 multi-area 100 cost 512`	（任意）OSPFv3 マルチエリア インターフェイスでパケットを送信するコストを指定します。マルチエリア インターフェイスのコストをプライマリ インターフェイスのコストとは異なるようにする必要がある場合のみ、このコマンドを使用してコストを指定します。
ステップ 7	**ospfv3** *process-id* **ipv6 area** *area-id* 例： `Device(config-if)# ospfv3 1 ipv6 area 0`	OSPFv3 インターフェイスを設定します。 • *process-id* 引数は OSPF プロセスを示します。有効な範囲は 1 ～ 65535 です。 • *area-id* 引数は OSPF エリアを示します。範囲は 0 ～ 4294967295 にするか、または IP アドレスを使用できます。
ステップ 8	**serial restart-delay** *count* 例： `Device(config-if)# serial restart-delay 0`	ルータがダウンした場合に、ルータがシリアル インターフェイスを起動するまで待機する時間を設定します。*count* 引数は、ハードウェアがリセットされる頻度を秒単位で指定します。範囲は 0 ～ 900 です。
ステップ 9	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

OSPFv3 マルチエリア隣接関係の確認

手順の概要

1. イネーブル化
2. **show ospfv3 interface brief**
3. **show ospfv3 multi-area**
4. **show ospfv3 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： `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	**show ospfv3 interface brief** 例： `Device# show ospfv3 interface brief`	Open Shortest Path First バージョン 3（OSPFv3）インターフェイスに関する簡単な情報を表示します。
ステップ 3	**show ospfv3 multi-area** 例： `Device# show ospfv3 multi-area`	OSPFv3 マルチエリア インターフェイスに関する情報を表示します。
ステップ 4	**show ospfv3 interface** 例： `Device# show ospfv3 interface`	OSPFv3インターフェイスに関する情報を表示します。

OSPFv3 マルチエリア隣接関係の設定例

例：OSPFv3 マルチエリア隣接関係の設定

```
Device> enable
Device# configure terminal
Device(config)# interface serial 2/0
Device(config-if)# ipv6 enable
Device(config-if)# ospfv3 multi-area 100
Device(config-if)# ospfv3 multi-area 100 cost 512
Device(config-if)# ospfv3 1 ipv6 area 0
```

```
Device(config-if)# serial restart-delay 0
Device(config-if)# end
```

例：OSPFv3 マルチエリア隣接関係の確認

show ospfv3 interface brief コマンドの出力例

Open Shortest Path First バージョン 3（OSPFv3）インターフェイスに関する簡単な情報を表示するには、特権 EXEC モードで **show ospfv3 interface brief** コマンドを使用します。

```
Device# show ospfv3 interface brief

Interface PID Area  AF   Cost  State Nbrs F/C
Se2/0     1   0    ipv6  64    P2P   1/1
MA2 1     1   100  ipv6  512   P2P   1/1
```

show ospfv3 multi-area コマンドの出力例

OSPFv3 マルチエリア インターフェイスの情報を表示するには、特権 EXEC モードで **show ospfv3 multi-area** コマンドを使用します。

```
Device# show ospfv3 multi-area

OSPFV3_MA2 is up, line protocol is up
Primary Interface Serial2/0, Area 100
Interface ID 10
MTU is 1500 bytes
Neighbor Count is 1
```

show ospfv3 interface コマンドの出力例

OSPFv3 インターフェイスの情報を表示するには、特権 EXEC モードで **show ospfv3 interface** コマンドを使用します。

```
Device# show ospfv3 interface

Serial2/0 is up, line protocol is up
Link Local Address 2001:DB8:0:ABCD::1, Interface ID 10
Area 0, Process ID 1, Instance ID 0, Router ID 10.0.0.12
Network Type POINT_TO_POINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:07
Graceful restart helper support enabled
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 10.0.0.22
Suppress hello for 0 neighbor(s)
Multi-area interface Count is 1
OSPFV3_MA2 interface exists in area 100 Neighbor Count is 1
OSPFV3_MA2 is up, line protocol is up
Link Local Address 2001:DB8:0:ABCD::1, Interface ID 10
Area 100, Process ID 1, Instance ID 0, Router ID 10.0.0.12
Network Type POINT_TO_POINT, Cost: 512
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:08
Graceful restart helper support enabled
Index 1/1/2, flood queue length 0
```

```
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 10.0.0.22
```

OSPFv3 マルチエリア隣接関係に関する追加情報

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 Command List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

OSPFv3 マルチエリア隣接関係の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

機能名	リリース	機能情報
OSPFv3 マルチエリア隣接関係		OSPFv3 マルチエリア隣接関係を使用すると、最適化されたルーティングを可能にするために Open Shortest Path First バージョン 3（OSPFv3）エリアが共有できるリンクを設定することができます。既存の OSPFv3 プライマリ インターフェイスには複数のエリアを追加できます。

第 54 章

OSPF 隣接関係確立制限

OSPF 隣接関係同時確立制限機能により、OSPF エリア内の隣接関係の数を制限することができます。

- 機能情報の確認，557 ページ
- OSPF 隣接関係確立制限について，558 ページ
- OSPF 隣接関係確立制限の設定方法，559 ページ
- OSPF 隣接関係確立制限の設定例，564 ページ
- OSPF 隣接関係確立制限に関する追加情報，565 ページ
- OSPF 隣接関係確立制限の機能情報，566 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。

OSPF 隣接関係確立制限について

隣接関係の制限の概要

OSPF：同時隣接関係確立の制限機能を使用すると、同時に「交換」または「ロード中」ステートにある隣接関係の数を制限することができます。プロセスの制限（PL）は、「確立中」の隣接関係の数を決定し、プロセス全体のすべての隣接関係に適用されます。「確立中」とは、「交換」または「ロード中」ステートにある隣接関係のことです。隣接関係は、エリアの作成後の初期にOSPF エリアで確立されます。初期制限は、OSPF エリアで「フル」ステートに達した隣接関係がないときに適用されます。エリアに「フル」の隣接関係がある場合、新しい隣接関係はプロセス制限によって管理されます。ある時点では、プロセス制限と初期制限が OSPF エリアで有効になります。エリアに「確立中」の隣接関係がないときは、指定された最大の制限とは無関係に少なくとも 1 つの隣接関係の確立が許可されます。つまり、隣接関係の最大数は、1 つまたは複数のエリアで隣接関係が確立されるまでは超えることができます。（エリア数）- 1 の数が上限を超えることができます。

制限に達すると、EXCHANGE 未満のステートの隣接関係が終了します。隣接関係を終了するには、ネイバーのデバイス ID を持たないネイバーに hello パケットを送信します。これにより、ネイバーの隣接関係はINIT ステートになります。このため、ネイバーが別のインターフェイスで隣接関係の確立をブロックしている場合に発生する可能性がある、ネイバーとのデッドロックが防止されます。ネイバーの隣接関係をINITにすることにより、ネイバーは別のインターフェイスで隣接関係を確立できるようになります。制限に達したり超過した場合、不明なネイバーからのパケットは無視されます。

グレースフル リスタートまたはCisco Nonstop Forwarding を設定する場合、隣接するすべてのデバイスから hello パケットを受け入れる必要があります。再起動するデバイスは hello パケットにネイバーのデバイス ID を含め、ネイバーによって隣接関係がドロップされないようにする必要があります。グレースフルリスタートが設定されている場合、猶予のリンクステートアドバタイズメント（LSA）はスロットリング モードではなく通常モードで送信する必要があります。デバイスがグレースフル リスタートを実行しているときに制限に達した場合、新しい隣接関係は 2-WAY または EXSTART のままにすることができます。ただし、確立中の隣接関係の数が制限未満になるまでは EXCHANGE に進むことができません。

隣接関係の確立の設定

ルータまたはアドレスファミリ コンフィギュレーション モードでエリアの上限および初期制限を設定するには、**adjacency stagger** コマンドを使用します。初期制限はプロセスの制限以下にする必要があります。デフォルト値は 300 で、最小値は 1 です。**none** キーワードを使用する場合、上限のみが有効になります。**none** キーワードはエリアの初期制限も無効にします。エリアで制限に達して隣接関係が確立されていない場合、隣接関係確立のグローバル数が PL 未満になるまで、エリアでの隣接関係の確立が許可されなくなります。

インターフェイスでずらすことを無効にするには、**ip ospf adjacency stagger disable** または **ospfv3 adjacency stagger disable** コマンドを使用します。無効なインターフェイスでの隣接関係の確立は、

スロットリングの制限にカウントされます。インターフェイスのスロットリングを無効にすると、上限に達したときに上限を超えることができ、スロットリングが無効になっているインターフェイスで新しい隣接関係が確立されます。

（注） **no adjacency stagger** コマンドを使用してこの機能を無効にすると、実行コンフィギュレーションにコマンドが表示されます。デフォルト値に戻すには、**default adjacency stagger** コマンドを使用します。このコマンドを使用すると、**adjacency stagger** コマンドは実行コンフィギュレーションに表示されません。

OSPF 隣接関係確立制限の設定方法

グローバルな隣接関係確立の設定

ルータ コンフィギュレーション モードでの隣接関係制限の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router ospf***process-id*
4. **adjacency stagger** {*initial-limit* | **none**} *maximum-limit*
5. **end**

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	**configure terminal** 例： `Device# 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	**router ospf***process-id* 例： `Device(config)# router ospf 109`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**adjacency stagger** {*initial-limit* | **none**} *maximum-limit* 例： `Device(config-router)# adjacency stagger 10 50`	エリア内の隣接関係の数を制御します。 • *initial-limit*：エリア内で許可する隣接関係の最小数。 • *maximum-limit*：エリア内で許可する隣接関係の最大数。 • **none**：エリア内に隣接関係を 1 つも許可しない。
ステップ 5	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

アドレス ファミリ コンフィギュレーション モードでの隣接関係制限の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. 次のいずれかを実行します。
   - **address-family ipv4 unicast**
   - **address-family ipv6 unicast**
5. **adjacency stagger** {*initial-limit* | **none**} {*maximum-limit*| **disable**}
6. **end**

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	**configure terminal** 例： `Device# 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	**router ospfv3** [*process-id*] 例： `Device(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。

ステップ 4	次のいずれかを実行します。
	• **address-family ipv4 unicast**
	• **address-family ipv6 unicast**
	
	例：
	`Device(config-router)# address-family ipv4 unicast`
	
	例：
	`Device(config-router)# address-family ipv6 unicast`
		OSPFv3 の IPv4 または IPv6 アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ 5	**adjacency stagger** {*initial-limit* | **none**} {*maximum-limit*| **disable**} 例： `Device(config-router-af)# adjacency stagger 10 50`	エリア内の隣接関係の数を制御します。 • *initial-limit*：エリア内で許可する隣接関係の最小数。 • **none**：エリア内に隣接関係を 1 つも許可しない。 • *maximum-limit*：エリア内で許可する隣接関係の最大数。 • **disable**：隣接関係の確立をディセーブルにします。
ステップ 6	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

インターフェイス コンフィギュレーション モードでの隣接関係スタガリングのディセーブル化

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***type number*
4. 次のいずれかを実行します。
   - **ip ospf adjacency stagger disable**
   - **ospfv3 adjacency stagger disable**
5. **end**

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	**configure terminal** 例： `Device# 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	**interface***type number* 例： `Device(config)# interface serial 2/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかを実行します。
	• **ip ospf adjacency stagger disable**
	• **ospfv3 adjacency stagger disable**
	
	例：
	`Device(config-if)# ip ospf adjacency stagger disable`
	
	例：
	`Device(config-if)# ospfv3 adjacency stagger disable`
		インターフェイスで隣接関係スタガリングをディセーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

隣接関係スタガリングの確認

手順の概要

1. イネーブル化
2. **show ip ospf**
3. **show ospfv3**

手順の詳細

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　show ip ospf

例：
```
Device# show ip ospf

 Routing Process "ospf 10" with ID 10.8.3.3
 Start time: 2w0d, Time elapsed: 00:16:43.033
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Supports NSSA (compatible with RFC 3101)
 Supports Database Exchange Summary List Optimization (RFC 5243)
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 EXCHANGE/LOADING adjacency limit: initial 300, process maximum 300
```

```
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
 IETF NSF helper support enabled
 Cisco NSF helper support enabled
 Reference bandwidth unit is 100 mbps
```

OSPF ルーティング プロセスに関する情報を表示します。

ステップ 3 **show ospfv3**

例：

```
Device# show ospfv3

 OSPFv3 12 address-family ipv6
 Router ID 10.8.3.3
 Supports NSSA (compatible with RFC 3101)
 Supports Database Exchange Summary List Optimization (RFC 5243)
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Retransmission limit dc 24 non-dc 24
 EXCHANGE/LOADING adjacency limit: initial 10, process maximum 50
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 Graceful restart helper support enabled
 Reference bandwidth unit is 100 mbps
 RFC1583 compatibility enabled
```

OSPFv3 ルーティング プロセスに関する情報を表示します。

OSPF 隣接関係確立制限の設定例

例：ルータ コンフィギュレーション モードでの隣接関係制限の設定

```
Device> enable
Device# configure terminal
Device(config)# router ospf 109
Device(config-router)# adjacency stagger 10 50
Device(config-router)# end
```

例：アドレス ファミリ コンフィギュレーション モードでの隣接関係制限の設定

```
Device> enable
Device# configure terminal
Device(config)# router ospfv3 1
Device(config-router)# address-family ipv6 unicast
Device(config-router-af)# adjacency stagger 10 50
Device(config-router-af)# end
```

例：インターフェイス コンフィギュレーション モードでの隣接関係のディセーブル化

```
Device> enable
Device# configure terminal
Device(config)# interface serial 2/0
Device(config-if)# ospfv3 adjacency stagger disable
Device(config-if)# end
```

OSPF 隣接関係確立制限に関する追加情報

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 Command List, All Releases』
OSPF コマンド	『Cisco IOS IP Routing: OSPF Command Reference』
『Configuring OSPF』	『Configuring OSPF』
マルチエリア隣接関係	• OSPFv2 マルチエリア隣接関係 • OSPFv3 マルチエリア隣接関係

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

OSPF 隣接関係確立制限の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 *59*：*OSPF* 隣接関係確立制限の機能情報

機能名	リリース	機能情報
OSPF：隣接関係同時確立制限	Cisco IOS XE Release 3.15S	OSPF 隣接関係同時確立制限機能により、OSPF エリア内の隣接関係の数を制限することができます。 次のコマンドが導入または変更されました。**adjacency stagger**、**ip ospf adjacency stagger disable**、**ip ospfv3 adjacency stagger disable**、**show ip ospf**、**show ip ospfv3**