



Cisco Nexus 3600 スイッチ NX-OS ユニキャスト ルーティング 構成ガイド、リリース 10.4(x)[

最終更新：2025 年 8 月 7 日

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/>



目次

Trademarks ?

はじめに :

はじめに xxix

対象読者 xxix

表記法 xxix

Cisco Nexus 3000 シリーズ スイッチの関連資料 xxx

マニュアルに関するフィードバック xxxi

通信、サービス、およびその他の情報 xxxi

第 1 章

新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

第 2 章

概要 3

ライセンス要件 3

サポートされるプラットフォーム 4

レイヤ 3 ユニキャスト ルーティングについて 4

ルーティングの基礎 4

パケット交換 5

ルーティング メトリック 6

パス長 6

Reliability 6

ルーティング遅延 6

帯域幅 6

負荷	6
通信コスト	7
ルータ ID	7
自律システム	7
コンバージェンス	8
ロード バランシングおよび等コスト マルチパス	9
ルートの再配布	9
アドミニストレーティブ ディスタンス	9
スタブ ルーティング	10
ルーティング アルゴリズム	11
スタティック ルートおよびダイナミック ルーティング プロトコル	11
内部および外部ゲートウェイ プロトコル	12
リンクステート プロトコル	12
レイヤ 3 仮想化	13
CiscoNX-OS フォワーディング アーキテクチャ	13
ユニキャスト RIB	13
隣接マネージャ	14
ユニキャスト転送分散モジュール	14
FIB	15
ハードウェア フォワーディング	15
ソフトウェア転送	16
レイヤ 3 ユニキャスト ルーティング機能のまとめ	16
IPv4 and IPv6	16
Open Shortest Path First (OSPF)	16
EIGRP	16
BGP	17
スタティック ルーティング	17
レイヤ 3 仮想化	17
Route Policy Manager	17
ファーストホップ冗長プロトコル	17
オブジェクト トラッキング	18
関連項目	18

第 3 章

IPv4 の設定 19

IPv4 の概要 19

複数の IPv4 アドレス 20

アドレス解決プロトコル 20

ARP キャッシング 21

ARP を使用しないデバイス 21

Reverse ARP 22

プロキシ ARP 22

ローカルプロキシ ARP 23

Gratuitous ARP 23

収集スロットル 23

ICMP 24

ICMP 到達不能サポートによる送信元インターフェイスの設定 24

仮想化のサポート 24

ECMP を使用した IPv4 ルート 25

IPv4 の前提条件 25

注意事項と制約事項 25

デフォルト設定 26

IPv4 の設定 27

IPv4 アドレス指定の設定 27

複数の IP アドレスの設定 28

LPM インターネット ピアリング ルーティング モードの設定 29

LPM インターネット ピアリング ルーティング モードの追加設定 31

スタティック ARP エントリの設定 32

プロキシ ARP の設定 33

ローカルプロキシ ARP の設定 35

無償 ARP の設定 36

サブネット外の ARP 解決の構成 37

SVI インターフェイスごとの ARP キャッシュの構成 38

IP ダイレクトブロードキャストの設定 39

IP 収集スロットルの設定	39
ハードウェア IP 収集スロットルのタイムアウトの設定	40
ICMP 送信元 IP フィールドのインターフェイス IP アドレスの設定	41
IP パケットのソフトウェア転送のロギングの設定	42
IPv4 設定の確認	44
IPv4 の設定例	44

第 4 章

IPv6 の設定 45

IPv6 について	45
IPv6 アドレス形式	46
IPv6 ユニキャスト アドレス	47
集約可能グローバルアドレス	47
リンクローカルアドレス	49
IPv4 互換 IPv6 アドレス	49
ユニーク ローカルアドレス	50
サイトローカルアドレス	51
IPv4 パケット ヘッダー	51
簡易 IPv6 パケット ヘッダー	51
IPv6 の DNS	55
IPv6 のパス MTU ディスカバリ	55
CDP IPv6 アドレスのサポート	56
IPv6 の ICMP	56
IPv6 ネイバー探索	57
IPv6 ネイバー送信要求メッセージ	57
ルータ アドバタイズメント メッセージ	59
IPv6 ネイバー リダイレクト メッセージ	60
仮想化のサポート	61
ECMP を使用した IPv6 ルート	61
IPv6 の前提条件	61
IPv6 の注意事項および制約事項	62
デフォルト設定	62

IPv6 の設定	63
IPv6 アドレッシングの設定	63
LPM インターネット ピアリング ルーティング モードの設定	65
LPM インターネット ピアリング ルーティング モードの追加設定	66
IPv6 ネイバー探索の構成	68
オプションの IPv6 ネイバー探索	71
IPv6 パケット検証の構成	71
IPv6 設定の確認	72
IPv6 の設定例	73

第 5 章

OSPFv2 の設定	75
OSPFv2 について	75
Hello パケット	76
ネイバー情報	76
隣接関係	77
指定ルータ	77
エリア	78
リンクステート アドバタイズメント	79
LSA タイプ	79
リンク コスト	81
フラッドイングと LSA グループ ペーシング	81
リンクステート データベース	82
不透明 LSA	82
OSPFv2 およびユニキャスト RIB	82
認証	83
簡易パスワード認証	83
暗号化認証	83
MD5 認証	83
高度な機能	83
スタブ エリア	84
Not-So-Stubby Area	84

仮想リンク	85
ルートの再配布	85
ルート集約	85
OSPFv2 スタブ ルータ アドバタイズメント	86
複数の OSPFv2 インスタンス	86
SPF 最適化	87
BFD	87
仮想化のサポート	87
OSPFv2 の前提条件	87
注意事項と制約事項	87
デフォルト設定	88
基本的な OSPFv2 の設定	88
OSPFv2の有効化	88
OSPFv2インスタンスの作成	89
OSPFv2 インスタンスのオプション パラメータの設定	91
OSPFv2でのネットワークの設定	92
エリアの認証の設定	95
インターフェイスの認証の設定	97
高度なOSPFv2の設定	100
境界ルータのフィルタ リストの設定	100
スタブ エリアの設定	102
Totally Stubby エリアの設定	103
NSSA の設定	104
仮想リンクの設定	106
再配布の設定	109
再配布されるルート数の制限	111
ルート集約の設定	113
スタブ ルート アドバタイズメントの設定	115
デフォルト タイマーの変更	116
OSPFv2 インスタンスの再起動	119
仮想化による OSPFv2 の設定	120

OSPFv2 設定の確認	122
OSPFv2 統計情報の表示	123
OSPFv2 の設定例	123
その他の参考資料	123
関連資料	124
MIB	124

第 6 章

OSPFv3 の設定	125
OSPFv3 について	125
OSPFv3 と OSPFv2 の比較	126
Hello パケット	126
ネイバー情報	127
隣接関係	128
指定ルータ	128
エリア	129
リンクステートアドバタイズメント	130
LSA タイプ	130
リンク コスト	133
フラッドイングと LSA グループ ペーシング	133
リンクステート データベース	134
マルチエリア隣接関係 (Multi-Area Adjacency)	134
OSPFv3 と IPv6 ユニキャスト RIB	134
アドレス ファミリのサポート	135
認証および暗号化	135
高度な機能	136
スタブ エリア	136
Not-So-Stubby Area	136
仮想リンク	137
ルートの再配布	137
ルート集約	138
高可用性およびグレースフル リスタート	138

複数の OSPFv3 インスタンス	139
SPF 最適化	139
BFD	140
仮想化のサポート	140
OSPFv3 の前提条件	140
OSPFv3 の注意事項および制約事項	140
デフォルト設定	141
基本的な OSPFv3 の設定	141
OSPFv3 の有効化	142
OSPFv3 インスタンスの作成	143
OSPFv3 でのネットワークの設定	145
OSPFv3 IPSec 認証の設定	148
高度な OSPFv3 の設定	153
境界ルータのフィルタ リストの設定	153
スタブ エリアの設定	155
Totally Stubby エリアの設定	156
NSSA の設定	157
マルチエリアの隣接関係の設定	159
仮想リンクの設定	161
再配布の設定	163
再配布されるルート数の制限	165
ルート集約の設定	167
デフォルト タイマーの変更	169
グレースフル リスタートの設定	171
OSPFv3 インスタンスの再起動	173
仮想化による OSPFv3 の設定	174
暗号化および認証の構成	176
ルータ レベルでの OSPFv3 暗号化の設定	177
エリア レベルでの OSPFv3 暗号化の設定	178
インターフェイスレベルでの OSPFv3 暗号化の設定	179
仮想リンクの OSPFv3 暗号化の設定	181

ルータ レベルで OSPFv3 認証の構成	182
エリア レベルで OSPFv3 認証の構成	184
インターフェイス レベルで OSPFv3 認証の構成	186
仮想リンク レベルでの OSPFv3 認証の構成	187
OSPFv3 の設定の確認	189
OSPFv3のモニタリング	190
OSPFv3 の設定例	191
関連項目	191
その他の参考資料	191
MIB	192

第 7 章**EIGRP の設定 193**

EIGRP に関する情報	193
EIGRP コンポーネント	194
信頼性の高いトランスポート プロトコル	194
ネイバー探索およびネイバー回復	194
拡散更新アルゴリズム	195
EIGRP ルート更新	195
内部ルート メトリック	196
外部ルート メトリック	196
EIGRP とユニキャスト RIB	197
高度な EIGRP	197
アドレス ファミリ	197
認証	197
スタブ ルータ	198
ルート集約	198
ルートの再配布	199
ロード バランシング	199
Split Horizon	199
仮想化のサポート	200
EIGRP の前提条件	200

注意事項と制約事項	200
デフォルト設定	201
基本的な EIGRP の設定	202
EIGRP 機能の有効化	202
EIGRP インスタンスの作成	203
EIGRP インスタンスの再起動	206
EIGRP インスタンスのシャットダウン	206
高度な EIGRP の設定	206
EIGRP での認証の設定	206
EIGRP スタブ ルーティングの設定	209
EIGRP のサマリー アドレスの設定	210
EIGRP へのルートの再配布	210
再配布されるルート数の制限	212
EIGRP でのロードバランスの設定	214
hello パケット間のインターバルとホールド タイムの調整	216
スプリット ホライズンの無効化	217
EIGRP の調整	217
EIGRP の仮想化の設定	219
EIGRP の設定の確認	221
EIGRP 統計情報の表示	222
EIGRP の設定例	222
関連項目	222
その他の参考資料	223
MIB	223

第 8 章

IS-IS の設定	225
IS-IS について	225
IS-IS の概要	225
IS-IS エリア	226
NET およびシステム ID	227
DIS	227

IS-IS 認証	227
メッシュ グループ	228
過負荷ビット	228
ルート集約	229
再配布の設定	229
プレフィックスの抑制のリンク	231
ロード バランシング	231
BFD	231
仮想化のサポート	231
高可用性およびグレースフル リスタート	232
複数の IS-IS インスタンス	232
IS-IS の前提条件	232
IS-IS に関する注意事項および制限事項	233
デフォルト設定	233
IS-IS の設定	234
IS-IS コンフィギュレーション モード	234
ルータ コンフィギュレーション モード	234
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	234
IS-IS 機能の有効化	234
IS-IS インスタンスの作成	235
IS-IS インスタンスの再起動	238
IS-IS のシャットダウン	238
エリアでの IS-IS 認証の設定	239
インターフェイスでの IS-IS 認証の設定	240
メッシュ グループの設定	242
指定中継システムの設定	242
ダイナミック ホスト交換の設定	243
過負荷ビットの設定	243
接続ビットの設定	244
hello パディングの一時モードの設定	244
サマリー アドレスの設定	245

再配布の設定	246
再配布されるルート数の制限	248
パッシブインターフェイスプレフィックスのみのアドバタイズ	250
インターフェイスでのプレフィックスの抑制	251
厳密な隣接モードのディセーブル化	252
グレースフル リスタートの設定	253
仮想化の設定	255
IS-IS の調整	257
IS-IS 設定の確認	259
IS-IS の監視	260
IS-IS の設定例	261
関連項目	261

第 9 章

基本的 BGP の設定 263

基本的な BGP について	263
BGP 自律システム	264
4 バイトの AS 番号のサポート	264
アドミニストレーティブ ディスタンス	264
BGP ピア	265
BGP セッション	265
プレフィックス ピアおよびインターフェイス ピアのダイナミック AS 番号	265
BGP ルータ ID	266
BGP パスの選択	266
ステップ 1 : パス ペアの比較	267
ステップ 2 : 比較順序の決定	269
ステップ 3 : ベストパス変更の抑制の決定	269
BGP およびユニキャスト RIB	270
BGP プレフィックス独立コンバージェンス	270
BGP の仮想化	271
基本 BGP の前提条件	271
BGP に関する注意事項と制約事項	271

CLI コンフィギュレーション モード	272
グローバル コンフィギュレーション モード	272
アドレス ファミリ設定モード	273
ネイバー コンフィギュレーション モード	273
ネイバー アドレス ファミリ コンフィギュレーション モード	273
デフォルト設定	274
基本的 BGP の設定	275
BGP 機能のイネーブル化	275
BGP インスタンスの作成	276
BGP インスタンスの再起動	278
BGP のシャットダウン	278
BGP ピア設定	278
デフォルト スタティック ルートをすべての BGP VRF に配布	280
更新アナウンス遅延タイマーの構成	282
BGP 再接続間隔の構成	284
プレフィックス ピアのダイナミック AS 番号の設定	285
BGP PIC エッジの設定	287
BGP 情報の消去	289
ベーシック BGP の設定の確認	292
BGP 統計情報の表示	294
ベーシック BGP の設定例	294
関連項目	295
次の作業	295
その他の参考資料	295
MIB	295

第 10 章

高度な BGP の設定	297
拡張 BGP の概要	297
ピア テンプレート	298
認証	298
ルート ポリシーおよび BGP セッションのリセット	298

eBGP	299
eBGP ネクストホップ変更なし	300
iBGP	300
AS 連合	300
ルート リフレクタ	301
機能ネゴシエーション	302
ルート ダンプニング	302
ロード シェアリングおよびマルチパス	303
ルート集約	303
BGP 条件付きアドバタイズメント	304
BGP ネクスト ホップ アドレス トラッキング	304
Site of Origin	305
ルートの再配布	305
BFD	306
BGP の調整	306
BGP タイマー	306
ベストパス アルゴリズムの調整	307
マルチプロトコル BGP	307
RFC 5549	307
拡張 BGP の前提条件	307
拡張 BGP に関する注意事項と制限事項	308
BGP のデフォルト設定	311
高度な BGP の設定	311
インターフェイスでの IP 転送の有効化	311
BGP セッション テンプレートの設定	312
BGP peer-policy テンプレートの設定	315
BGP peer テンプレートの設定	317
プレフィックス ピアリングの設定	320
IPv4 および IPv6 アドレス ファミリー向け IPv6 リンク ローカル経由の BGP インターフェイス ピアリングの設定	322
BGP 認証の設定	326
BGP セッションのリセット	328

ネクストホップアドレスの変更	329
BGP ネクスト ホップ アドレス トラッキングの設定	329
ネクスト ホップ フィルタリングの設定	330
ネクストホップセルフによるリフレクト ルートの制御	330
セッションがダウンした場合のネクストホップ グループの縮小	331
機能ネゴシエーションのディセーブル化	331
BGP 追加パスの設定	332
追加パスの送受信機能のアドバタイズ	332
追加パスの送受信の設定	333
アドバタイズされるパスの設定	334
追加パス選択の設定	335
eBGP の設定	336
eBGP ネクストホップ変更なしの構成	336
eBGP シングルホップ チェックの無効化	337
eBGP マルチホップの設定	337
同じ自律システムで eBGP ルートの構成	338
高速外部フェールオーバーのディセーブル化	339
AS パス属性の制限	339
ローカル AS サポートの設定	339
AS 連合の設定	340
BGP 向け BFD の構成例	341
BGP 属性フィルタリングの設定とエラー処理	341
BGP 更新メッセージからのパス属性の取り消しとしての処理	342
BGP 更新メッセージからのパス属性の破棄	342
拡張属性エラー処理のイネーブル化またはディセーブル化	343
取り消されたパス属性または破棄されたパス属性の表示	343
独自の自律システムを含む自律システム パスの設定	344
ルート リフレクタの設定	346
ルート ダンプニングの設定	348
ロード シェアリングおよび ECMP の設定	348
最大プレフィックス数の設定	349

ダイナミック機能の設定	349
集約アドレスの設定	350
BGP ルートの抑制	350
BGP 条件付きアドバタイズメントの設定	351
ルートの再配布の設定	353
再分配による BGP 減衰の無効化	355
マルチプロトコル BGP の設定	356
元の BGP 拡張コミュニティ サイトの構成	357
BGP の調整	358
仮想化の設定	358
BGP グレースフル シャットダウン	360
BGP グレース フル シャットダウンに関する情報	360
グレースフル シャットダウンの認識とアクティブ化	361
グレースフル シャットダウンのコンテキスト	361
ルート マップによるグレースフル シャットダウン	362
注意事項と制約事項	364
グレースフル シャットダウン タスクの概要	364
リンクのグレースフル シャットダウンの設定	365
GRACEFUL_SHUTDOWN コミュニティに基づく BGP ルートのフィルタリングとローカル プリファレンスの設定	366
すべての BGP ネイバーのグレースフル シャットダウンの設定	368
GRACEFUL_SHUTDOWN コミュニティを使用したすべてのルートのプリファレンスの制 御	369
GRACEFUL_SHUTDOWN コミュニティのピアへの送信の防止	370
グレースフル シャットダウン情報の表示	371
グレースフル シャットダウンの設定例	372
グレースフル リスタートの設定	374
拡張 BGP の設定の確認	377
BGP 統計情報の表示	379
関連項目	379
その他の参考資料	380
MIB	380

第 11 章

RIP の設定 381

RIP について 381

RIP の概要 381

RIPv2 認証 382

Split Horizon 382

ルートのフィルタリング 383

ルート集約 383

ルートの再配布 383

ロード バランシング 384

RIP のハイ アベイラビリティ 384

RIP 仮想化のサポート 384

RIP のライセンス要件 384

RIP の前提条件 384

RIP に関する注意事項と制約事項 384

RIP パラメータのデフォルト設定 385

RIP の設定 385

RIP のイネーブル化 385

RIP インスタンスの作成 386

RIP インスタンスの再起動 387

インターフェイスでの RIP の設定 388

RIP 認証の設定 389

パッシブ インターフェイスの設定 391

ポイズン リバー스를指定したスプリット ホライズンの設定 391

ルート集約の設定 392

ルートの再配布の設定 392

Cisco IOS RIP との互換性のため、Cisco NX-OS RIP を設定 394

仮想化の設定 396

RIP の調整 398

RIP の設定の確認 400

RIP 統計情報の表示 400

RIP の設定例 400

関連項目 401

第 12 章

スタティック ルーティングの設定 403

スタティック ルーティングについて 403

アドミニストレーティブ ディスタンス 404

直接接続のスタティック ルート 404

完全指定のスタティック ルート 404

フローティング スタティック ルート 404

スタティック ルートのリモート ネクスト ホップ 405

BFD 405

仮想化のサポート 405

スタティック ルーティングの前提条件 405

注意事項と制約事項 406

デフォルト設定 406

スタティック ルーティングの設定 406

スタティック ルーティングの設定 406

仮想化の設定 407

スタティック ルーティングの設定確認 409

設定：スタティック スタティック ルーティングの例 409

第 13 章

レイヤ 3 仮想化の設定 411

レイヤ 3 仮想化について 411

レイヤ 3 仮想化の概要 411

VRF およびルーティング 412

VRF-Lite 412

VRF 認識サービス 413

Reachability 413

フィルタリング 414

到達可能性とフィルタリングの組み合わせ 414

VRF の注意事項と制約事項 414

VRF-Lite の注意事項と制限事項	415
VRF ルート リークの注意事項と制約事項	415
デフォルト設定	416
VRF の設定	416
VRF の作成	416
インターフェイスへの VRF メンバーシップの割当て	418
ルーティング プロトコル用の VRF パラメータの設定	419
VRF 認識サービスの設定	421
VRF スコープの設定	422
VRF の設定の確認	423
VRF の設定例	423

第 14 章

ユニキャスト RIB および FIB の設定	427
ユニキャスト RIB および FIB について	427
レイヤ 3 整合性チェッカー	428
FIB テーブル	428
仮想化のサポート	429
ユニキャスト RIB および FIB の管理	429
モジュールの FIB 情報の表示	429
ユニキャスト FIB でのロードシェアリングの設定	430
ルーティング情報と隣接情報の表示	436
レイヤ 3 整合性チェッカーのトリガー	437
FIB 内の転送情報の消去	438
ルートのメモリ要件の見積もり	439
ユニキャスト RIB 内のルートの消去	439
ユニキャスト RIB および FIB の確認	440

第 15 章

Route Policy Manager の設定	443
Route Policy Manager について	443
プレフィックス リスト	443
プレフィックス リストのマスク	444

MAC リスト	444
ルート マップ	445
一致基準	445
設定変更	446
アクセス リスト	446
BGP の AS 番号	446
BGP の AS パス リスト	446
BGP のコミュニティ リスト	447
BGP の拡張コミュニティ リスト	447
ルートの再配布およびルート マップ	447
Route Policy Manager の注意事項と制約事項	448
デフォルト設定	449
Route Policy Manager の設定	449
IP プレフィックス リストの設定	449
MAC リストの設定	451
AS パス リストの設定	452
BGP AS-path 属性の置き換え	453
完全な AS パスの置き換え	454
AS パスでの選択した AS 番号の置き換え	455
コミュニティ リストの設定	457
ルート マップの設定	458
Route Policy Manager の設定の確認	465
関連項目	465

 第 16 章

双方向フォワーディング検出の設定 467

BFD に関する情報	467
非同期モード	468
BFD の障害検出	468
BFD エコー機能	469
セキュリティ	469
仮想化のサポート	469

BFD の前提条件	469
注意事項と制約事項	469
デフォルト設定	471
BFD マルチホップ	471
BFD マルチホップのホップ数	472
BFD マルチホップの注意事項と制約事項	472
BFD の設定	472
設定階層	472
BFD 設定のタスク フロー	473
BFD 機能のイネーブル化	473
グローバルな BFD パラメータの設定	474
インターフェイス上での BFD の設定	475
ポート チャネルの BFD の設定	477
BFD エコー機能の設定	479
BGP での BFD の設定	480
PIM (Protocol Independent Multicast) での BFD の設定	482
OSPFv2 での BFD の設定	483
スタティック ルートの BFD の設定	484
IPv6 の BFD を構成する	485
IPv6 のグローバルな BFD パラメータの構成	485
IPv6 のインターフェイス BFD パラメータの構成	486
OSPFv3 での IPv6 用 BFD の構成	487
IPv6 スタティックルートの BFD の構成	488
BFD エコー モードの設定	490
BFD セッション エコー間隔の構成	490
BFD エコー インターフェイスの構成	491
BFD 低速タイマーの設定	492
TCAM リージョン サイズの設定	493
BFD マルチホップ セッション グローバル インターバル パラメータの設定	494
マルチホップ セッション単位の BFD パラメータの設定	495
BFD 設定の確認	496

BFD のモニタリング 496

第 17 章

ポリシーベース ルーティングの設定 499

ポリシーベース ルーティングについて 499

ポリシー ルート マップ 500

ポリシーベース ルーティングの set 基準 500

ルート マップ処理ロジック 501

ポリシーベース ルーティング フィルタリング オプション 501

ポリシーベース ルーティングの前提条件 502

ポリシーベース ルーティングの注意事項と制約事項 502

デフォルト設定 503

ポリシーベース ルーティングの設定 503

ポリシーベース ルーティング機能のイネーブル化 503

ECMP 上のポリシーベース ルーティングの有効化 504

ルート ポリシーの設定 506

ポリシーベース ルーティングの設定の確認 508

ポリシーベース ルーティングの設定例 508

第 18 章

『Configuring HSRP』 511

HSRP について 511

HSRP の概要 512

HSRP for IPv4 513

HSRP のバージョン 514

HSRP サブネット VIP 514

HSRP 認証 515

HSRP メッセージ 515

HSRP ロード シェアリング 515

オブジェクト トラッキングおよび HSRP 516

仮想化のサポート 516

HSRP の前提条件 517

HSRP の注意事項と制約事項 517

HSRP のデフォルト設定	518
『Configuring HSRP』	518
HSRP 機能のイネーブル化	518
HSRP バージョン設定	519
IPv4 の HSRP グループの設定	519
HSRP 仮想 MAC アドレスの設定	521
HSRP の認証	522
HSRP オブジェクト トラッキングの設定	524
HSRP プライオリティの設定	527
HSRP のカスタマイズ	528
HSRP 設定の確認	529
HSRP の設定例	529
その他の参考資料	530
関連資料	531
MIB	531

第 19 章

VRRP の設定	533
VRRP の概要	533
VRRP の動作	533
VRRP の利点	535
複数の VRRP グループ	536
VRRP ルータのプライオリティおよびプリエンプション	537
VRRP のアダプタイズメント	537
VRRP 認証	537
VRRPv3	538
仮想化のサポート	538
VRRP の注意事項と制約事項	538
VRRP のデフォルト設定	539
VRRP の設定	540
VRRP 機能のイネーブル化	540
VRRP グループの設定	540

VRRP プライオリティの設定	542
VRRP 認証の設定	544
アドバタイズメント パケットのタイム インターバルの設定	545
プリエンプションのディセーブル化	547
VRRP インターフェイス ステート トラッキングの設定	549
VRRPv3 の設定	551
VRRPv3 の有効化	551
VRRPv3 グループの構成	551
FHRP クライアント前の初期化前遅延時間の構成	554
VRRPv3 コントロールグループの設定	554
VRRPv2 設定の確認	556
VRRPv3 設定の確認	556
VRRP 統計情報の表示	557
VRRPv2 の設定例	557
VRRPv3 の構成例	559
その他の参考資料	559
関連資料	559

第 20 章

オブジェクト トラッキングの設定	561
オブジェクト トラッキングについて	561
オブジェクト トラッキングの概要	561
オブジェクト トラッキング リスト	562
仮想化のサポート	563
オブジェクト トラッキングに関する注意事項と制約事項	563
オブジェクト トラッキングのデフォルト設定	563
オブジェクト トラッキングの設定	563
インターフェイスに対するオブジェクト トラッキングの設定	563
ルート到達可能性に対するオブジェクト トラッキングの設定	565
ブール式を含むオブジェクト トラッキング リストの設定	566
パーセンテージしきい値を含むオブジェクト トラッキング リストの設定	567
重みしきい値を含むオブジェクト トラッキング リストの設定	569

オブジェクト トラッキングの遅延の設定	570
非デフォルト VRF に対するオブジェクト トラッキングの設定	573
オブジェクト トラッキングの設定の確認	574
オブジェクト トラッキングの設定例	574
関連項目	575
その他の参考資料	575
関連資料	575

付 録 A :	IETF RFC	577
	IETF RFC	577

【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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: <https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html>. Cisco product warranty information is available at <https://www.cisco.com/c/en/us/products/warranty-listing.html>. US Federal Communications Commission Notices are found here <https://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.



はじめに

この前書きは、次の項で構成されています。

- [対象読者](#) (xxix ページ)
- [表記法](#) (xxix ページ)
- [Cisco Nexus 3000 シリーズ スイッチの関連資料](#) (xxx ページ)
- [マニュアルに関するフィードバック](#) (xxxi ページ)
- [通信、サービス、およびその他の情報](#) (xxxi ページ)

対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
<i>italic</i>	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x y]	いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
variable	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。 string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

表記法	説明
screen フォント	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字のスクリーンフォントで示しています。
イタリック体の <i>screen</i> フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコ (<>) で囲んで示しています。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。

Cisco Nexus 3000 シリーズ スイッチの関連資料

Cisco Nexus 3000 シリーズ スイッチ全体のマニュアルセットは、次の URL にあります。

<https://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/tsd-products-support-series-home.html>

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によって求めるビジネス成果を得るには、[Cisco Services](#) [英語] にアクセスしてください。
- サービス リクエストを送信するには、[Cisco Support](#) にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco DevNet](#) [英語] にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

Cisco バグ検索ツール

[Cisco Bug Search Tool](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。



第 1 章

新機能および変更された機能に関する情報

- [新機能および変更された機能に関する情報（1 ページ）](#)

新機能および変更された機能に関する情報

この表では、Cisco Nexus 3600 スイッチ NX-OS ユニキャストルーティング構成ガイド、リリース 10.4(x) に記載されている新機能および変更機能をまとめています。

表 1: 新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
L3 インターフェイスの ARP キャッシュを制限する機能	インターフェイスごとに許可される ARP キャッシュエントリの最大数を構成する ip arp cache intf-limit コマンドが追加されました。	10.4(2)F	注意事項と制約事項（25 ページ） SVI インターフェイスごとの ARP キャッシュの構成（38 ページ）
OSPFv3 のキーチェーンサポート	キーチェーンサポートは、OSPFv3 暗号化および認証コマンドに対して提供されます。キーチェーン構成では、タイプ 6 暗号化形式のキーを構成することを推奨します。	10.4(1)F	認証および暗号化（135 ページ） OSPFv3 の注意事項および制約事項（140 ページ） 暗号化および認証の構成（176 ページ） OSPFv3 の設定例（191 ページ）

特長	説明	変更が行われたリリース	参照先
サブネット外の ARP 応答のサポート	ARP パケット処理、ARP エントリの学習、およびサブネット外トラフィックに対する応答の送信を許可する ip arp outside-subnet コマンドが追加されました。	10.4 (1) F	注意事項と制約事項 (25 ページ) サブネット外の ARP 解決の構成 (37 ページ)



第 2 章

概要

この章では、Cisco Nexus 3600 プラットフォーム スイッチでのレイヤ 3 ユニキャスト ルーティング プロトコルの基本概念を紹介します。

この章は、次の項で構成されています。

- [ライセンス要件 \(3 ページ\)](#)
- [サポートされるプラットフォーム \(4 ページ\)](#)
- [レイヤ 3 ユニキャスト ルーティングについて \(4 ページ\)](#)
- [ルーティング アルゴリズム \(11 ページ\)](#)
- [レイヤ 3 仮想化 \(13 ページ\)](#)
- [Cisco NX-OS フォワーディング アーキテクチャ \(13 ページ\)](#)
- [ユニキャスト RIB \(13 ページ\)](#)
- [隣接マネージャ \(14 ページ\)](#)
- [ユニキャスト転送分散モジュール \(14 ページ\)](#)
- [FIB \(15 ページ\)](#)
- [ハードウェア フォワーディング \(15 ページ\)](#)
- [ソフトウェア転送 \(16 ページ\)](#)
- [レイヤ 3 ユニキャスト ルーティング機能のまとめ \(16 ページ\)](#)
- [ファーストホップ冗長プロトコル \(17 ページ\)](#)
- [オブジェクト トラッキング \(18 ページ\)](#)
- [関連項目 \(18 ページ\)](#)

ライセンス要件

Cisco NX-OS ライセンス方式の推奨の詳細と、ライセンスの取得および適用の方法については、『[Cisco NX-OS ライセンス ガイド](#)』および『[Cisco NX-OS ライセンス オプション ガイド](#)』を参照してください。

サポートされるプラットフォーム

Cisco NX-OS リリース 7.0(3)I7(1) 以降では、[Nexus スイッチ プラットフォーム サポート マトリクス](#)に基づいて、選択した機能をさまざまな Cisco Nexus 9000 および 3000 スイッチで使用するために、どの Cisco NX-OS リリースが必要かを確認してください。

レイヤ 3 ユニキャスト ルーティングについて

レイヤ 3 ユニキャスト ルーティングには 2 つの基本的動作（最適なルーティング パスの決定およびパケットの交換）があります。ルーティングアルゴリズムを使用すると、ルータから宛先までの最適なパス（経路）を計算できます。この計算方法は、選択したアルゴリズム、ルート メトリック、そしてロード バランシングや代替パスの探索などの考慮事項により異なります。

ルーティングの基礎

ルーティングプロトコルは、メトリックを使用して、宛先までの最適なパスを調べます。メトリックとは、パス帯域幅などの、ルーティングアルゴリズムが宛先までの最適なパスを決定するために使用する測定基準です。パスを決定しやすいように、ルーティングアルゴリズムは、ルート情報（IP 接続先アドレス、および次のルータまたはホップのアドレスなど）を含むルーティング テーブルを初期化して維持します。宛先とネクスト ホップの関連付けにより、ルータは、接続先までの途中にあるネクストホップとなる特定のルータにパケットを送信すると、最適なパスで IP 接続先まで届けられることを判定できます。ルータは、着信パケットを受信すると、接続先アドレスをチェックし、このアドレスをネクストホップと関連付けようとします。ルート テーブルの詳細については、「[ユニキャスト RIB](#)」の項を参照してください。

ルーティングテーブルには、パスの優先度に関するデータなど、その他の情報が含まれていることもあります。ルータは、メトリックを比較して最適なルートを決めます。これらのメトリックは、使用しているルーティングアルゴリズムの設計によって異なります。「[ルーティング メトリック](#)」の項を参照してください。

各ルータは互いに通信し、さまざまなメッセージを送信して、そのルーティングテーブルを維持します。ルーティング更新メッセージはこれらのメッセージのいずれかであり、ルーティング テーブルのすべてまたは一部で構成されます。ルータは、他のすべてのルータからのルーティング更新情報を分析して、ネットワーク トポロジの詳細な図を構築できます。ルータ間で送信されるメッセージのもう 1 つの例であるリンクステートアドバタイズメントは、送信ルータのリンク状態を他のルータに通知します。リンク情報を使用して、ルータが、ネットワーク宛先までの最適なルートを決めるようにすることもできます。詳細については、「[ルーティング アルゴリズム](#)」の項を参照してください。

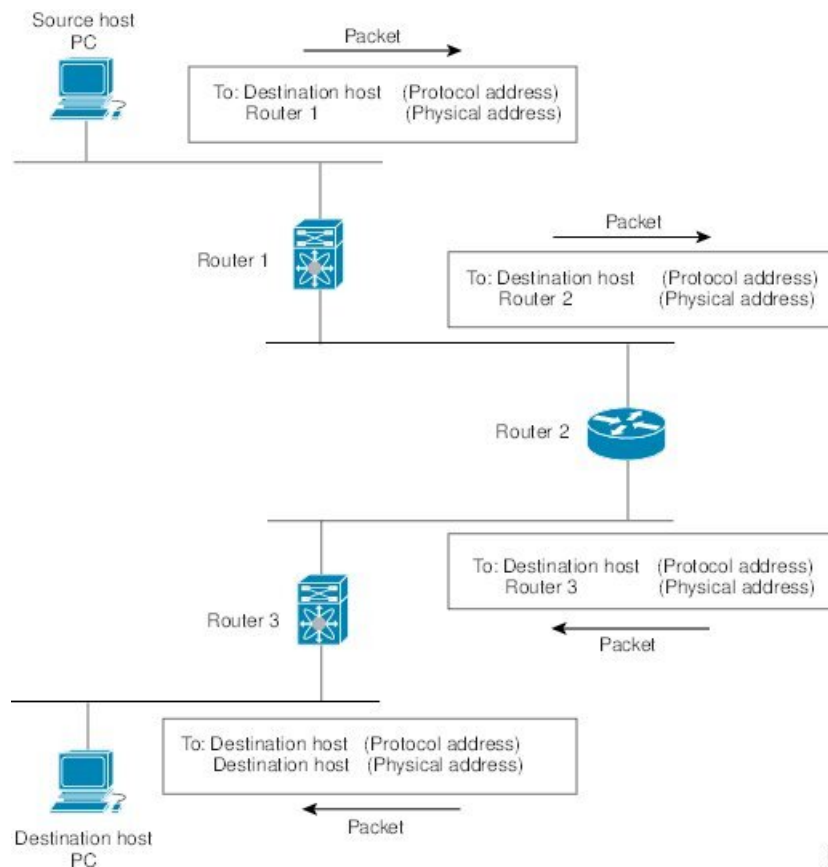
パケット交換

パケット交換では、ホストが、パケットを別のホストに送信する必要があることを決定します。なんらかの方法でルータのアドレスを入手したら、送信元ホストはパケットを明確に、宛先ホストの IP（ネットワーク層）アドレスを含むルータの物理（メディアアクセスコントロール（MAC）レイヤ）アドレス宛に送信します。

ルータは宛先の IP アドレスを調べ、ルーティングテーブルでその IP アドレスを探します。ルータがパケットの転送方法を認識していない場合は、通常はパケットをドロップします。パケットの転送方法がわかった場合、ルータは、宛先の MAC アドレスをネクスト ホップ ルータの MAC アドレスに変更し、パケットを送信します。

ネクストホップが宛先のホストである場合や、同じ交換決定処理を行う別のルータである場合があります。パケットがインターネットワークを介して移動するにつれ、パケットの物理アドレスは変化しますが、プロトコルアドレスは一定のままです（次の図を参照）。

図 1: ネットワークを介したパケット ヘッダーの更新



ルーティング メトリック

ルーティング アルゴリズムは、多くの異なるメトリックを使用して最適なルートを決定します。高度なルーティング アルゴリズムは、複数のメトリックに基づいてルートを選択している場合があります。

パス長

パスの長さは、最も一般的なルーティング メトリックです。一部のルーティング プロトコルでは、各ネットワーク リンクに恣意的なコストの割り当てが可能です。この場合、パスの長さは、経由した各リンクに関連付けられたコストの合計となります。それ以外のルーティング プロトコルでは、パケットが送信元から宛先までに経由する必要がある、ルータなどのネットワーク間製品の通過回数を指定するメトリックであるホップ数が定義されます。

Reliability

ルーティング アルゴリズムとの関連における信頼性は、各ネットワーク リンクの信頼性（ビット誤り率で示される）です。一部のネットワーク リンクは、他のネットワーク リンクよりダウンする頻度が高い場合があります。ネットワークがダウンした後、特定のネットワーク リンクが他のリンクより容易に、または短時間に修復される場合もあります。信頼性のランクを割り当てるときに考慮できる信頼性係数は、一般的にネットワーク リンクに割り当てる任意の数値です。

ルーティング遅延

ルーティング遅延は、送信元から宛先に、インターネットワークを通過してパケットを移動するために必要な時間の長さです。遅延は、中間のネットワーク リンクの帯域幅、経由する各ルータでのポートキュー、中間の全ネットワーク リンクでのネットワークの輻輳状況、パケットが移動する物理的な距離など、多くの要素に応じて異なります。ルーティング遅延はいくつかの重要な変数の組み合わせであるため、一般的で便利なメトリックです。

帯域幅

帯域幅は、リンクで使用可能なトラフィック容量です。たとえば、10 ギガビット イーサネット リンクは 1 ギガビット イーサネット リンクより容量が大きく、優れています。帯域幅は、リンクで達成可能な最大スループットですが、帯域幅のより大きいリンクを経由するルートが、帯域幅のより小さいリンクを経由するルートより優れているとは限りません。たとえば、帯域幅の大きいリンクの方が混雑していると、実際には、パケットを宛先に送信するためにさらに長い時間がかかる場合があります。

負荷

負荷は、ルータなどのネットワーク リソースの使用状況の度合いです。負荷は、CPU 使用状況や処理される 1 秒あたりのパケット数など、さまざまな方法で計算できます。これらのパラメータを継続的にモニタすると、リソースに負担がかかる場合があります。

通信コスト

通信コストは、リンク上でルーティングするための稼働コストの測定単位です。通信コストは重要なメトリックの1つで、特にパフォーマンスより稼働コストの削減が優先される場合に使用されます。たとえば、専用回線での回線遅延が公衆回線より大きくても、使用時間に応じて課金される公衆回線上でなく、自身の専用回線上でパケットを送信できます。

ルータ ID

各ルーティングプロセスには、ルータ ID が関連付けられています。ルータ ID は、システムのあらゆるインターフェイスに設定できます。ルータ ID を構成しなかった場合、Cisco NX-OS は次の基準に基づいてルータ識別子を選択します。

- Cisco NX-OS は、他のあらゆるインターフェイスよりも loopback0 を優先します。loopback0 が存在しなかった場合、Cisco NX-OS は、他のあらゆるインターフェイスタイプよりも、最初のループバック インターフェイスを優先します。
- ループバック インターフェイスを構成しなかった場合、Cisco NX-OS はルータ識別子として構成ファイルの最初のインターフェイスを使用します。Cisco NX-OS がルータ識別子を選択した後、いずれかのループバック インターフェイスを構成した場合は、ループバック インターフェイスがルータ識別子となります。ループバック インターフェイスが loopback0 ではなく、後で loopback0 を IP アドレスで設定した場合は、ルータ ID が loopback0 の IP アドレスに変更されます。
- ルータ ID の元であるインターフェイスが変更されると、新しい IP アドレスがルータ ID となります。他のどのインターフェイスの IP アドレスが変更されても、ルータ ID はまったく変更されません。

自律システム

自律システム (AS) とは、単一の技術的管理エンティティにより制御されるネットワークです。自律システムにより、グローバルな外部ネットワークが個々のルーティングドメインに分割され、これらのドメインでは、ローカルのルーティングポリシーが適用されます。この構成により、ルーティングドメインの管理と一貫したポリシー設定が簡素化されます。

各自律システムは、ルートの再配布により動的にルーティング情報を交換する、複数の内部ルーティングプロトコルをサポートできます。地域インターネットレジストリにより、インターネットに直接接続する各公共自律システムに一意の番号が割り当てられます。この自律システム番号で、ルーティング処理と自律システムの両方が識別されます。

Cisco NX-OS は 4 バイト AS 番号をサポートしています。次の表は、AS 番号の範囲を示します。

表 2: 表 1-1 AS 番号

2 バイト番号	AS ドット表記での 4 バイト番号	プレーンテキスト表記での 4 バイト番号	目的
1 ～ 64511	0.1 ～ 0.64511	1 ～ 64511	公共 AS (RIR により割り当てられる) (注) RIR = 地域インターネット レジストリ
64512 ～ 65534	0.64512 ～ 0.65534	64512 ～ 65534	専用 AS (ローカルの管理者により割り当てられる)
65535	0.65535	65535	予約済み (Reserved)
なし	1.0 ～ 65535.65535	65536 ～ 4294967295	公共 AS (RIR により割り当てられる) (注) RIR = 地域インターネット レジストリ

専用自律システム番号は内部ルーティング ドメインに使用されますが、インターネット上にルーティングされたトラフィック向けに、ルータにより変換される必要があります。ルーティングプロトコルを、専用自律システム番号が外部ネットワークにアドバタイズされるように設定しないでください。デフォルトでは、Cisco NX-OS は専用自律システム番号をルーティング更新情報から削除しません。



(注) 公共ネットワークおよび専用ネットワークの自律システム番号は、インターネット割り当て番号局 (IANA) により管理されています。予約済み番号の割り当てを含む自律システム番号の詳細について、または、AS 番号の登録を申請するには、次の URL を参照してください。

<http://www.iana.org/>

コンバージェンス

ルーティング アルゴリズム測定の際となる要素の 1 つは、ルータがネットワーク トポロジの変化に対応するために要する時間です。リンク障害など、なんらかの理由でネットワークの一部が変化すると、さまざまなルータのルーティング情報が一致なくなる場合があります。変化したトポロジに関する情報が更新されているルータと、古い情報が残っているルータがあるためです。コンバージェンスとは、ネットワーク内のすべてのルータが更新され、ルーティング情報が一致するまでにかかる時間の長さです。コンバージェンス時間は、ルーティングアル

ゴリズムによって異なります。コンバージェンスが速い場合は、不正確なルーティング情報によるパッケージ損失の可能性が小さくなります。

ロードバランシングおよび等コストマルチパス

ルーティングプロトコルでは、ロードバランシングまたは等コストマルチパス（ECMP）を使用して、複数のパス上のトラフィックを共有できます。ルータは、特定のネットワークへのルートを複数検出すると、最もアドミニストレーティブディスタンスの低いルートをルーティングテーブルにインストールします。ルータが、同じアドミニストレーティブディスタンスと宛先までのコストを持つ複数のパスを受信し、インストールすると、ロードバランシングが発生する場合があります。ロードバランシングでは、すべてのパス上にトラフィックが配布され、負荷が共有されます。使用されるパスの数は、ルーティングプロトコルによりルーティングテーブルに配置されるエントリの数に制限されます。Cisco NX-OS は、宛先までの 16 のパスをサポートします。

Enhanced Interior Gateway Routing Protocol（EIGRP）は、等コストでないロードバランシングもサポートしています。詳細については、「[EIGRP の設定（193 ページ）](#)」を参照してください。

ルートの再配布

ネットワークに複数のルーティングプロトコルが設定されている場合は、各プロトコルにルートの再配布を設定して、ルーティング情報を共有するように設定できます。たとえば、OSPF（Open Shortest Path First）を設定して、ボーダーゲートウェイプロトコル（BGP）で検出したルートをアドバタイズできます。また、スタティックルートを、どのダイナミックルーティングプロトコルにも再配布できます。他のプロトコルからのルートを再配布するルータは、再配布されたルートの固定ルートメトリックを設定し、異なるルーティングプロトコル間で互換性のないルートメトリックの問題を防ぎます。たとえば、EIGRP から OSPF に再配布されたルートには、OSPF が認識できる固定リンクコストメトリックが割り当てられます。

ルート再配布では、アドミニストレーティブディスタンス（「[アドミニストレーティブディスタンス](#)」セクションを参照）の使用によっても、2つの異なるルーティングプロトコルで検出されたルートが区別されます。優先ルーティングプロトコルには、より低いアドミニストレーティブディスタンスが与えられており、そのルートが、より高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た他のプロトコルからのルートに優先して選択されます。

アドミニストレーティブディスタンス

アドミニストレーティブディスタンスは、ルーティング情報源の信頼性を示す評価基準です。値が高いほど信頼性の評価は低くなります。一般的にルートは、複数のプロトコルを通じて検出されます。アドミニストレーティブディスタンスは、複数のプロトコルから学習したルートを区別するために使用されます。最もアドミニストレーティブディスタンスが低いルートが IP ルーティングテーブルに組み込まれます。

スタブルーティング

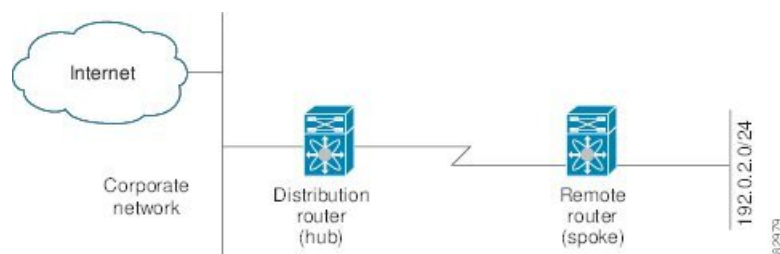
スタブルーティングはハブアンドスポーク型ネットワークトポロジで使用できます。このトポロジでは、1つ以上の終端（スタブ）ネットワークが1台のリモートルータ（スポーク）に接続され、そのリモートルータは1つ以上のディストリビューションルータ（ハブ）に接続されています。リモートルータは、1つ以上のディストリビューションルータにのみ隣接しています。リモートルータへ流れるIPトラフィックのルートは、ディストリビューションルータ経由のルートのみです。このタイプの設定は、ディストリビューションルータが直接WANに接続されているWANトポロジで使用されるのが一般的です。ディストリビューションルータは、さらに多くのリモートルータに接続できます。ディストリビューションルータが100台以上のリモートルータに接続されていることも、よくあります。ハブアンドスポーク型トポロジでは、リモートルータがすべての非ローカルトラフィックをディストリビューションルータに転送する必要があります。これにより、リモートルータが完全なルーティングテーブルを保持する必要はなくなります。通常、分散ルータは、デフォルトのルートのみをリモートルータに送信します。

指定されたルートのみが、リモート（スタブ）ルータから伝播されます。スタブルータは、サマリー、接続されているルート、再配布されたスタティックルート、外部ルート、および内部ルートに対するクエリすべてに、応答として「inaccessible」というメッセージを返します。スタブとして設定されているルータは、自身のスタブルータとしてのステータスを報告するために、特殊なピア情報パケットがすべての隣接ルータに送信されます。

スタブルータの状態を通知するパケットを受信した隣接ルータは、ルートについてはスタブルータに照会しません。また、スタブピアを持つルータは、そのピアについては照会しません。スタブルータは、ディストリビューションルータを使用して適切なアップデートをすべてのピアに送信します。

次の図は、単純なハブアンドスポーク型のコンフィギュレーションを示しています。

図 2: 単純なハブアンドスポーク ネットワーク



スタブルーティングを使用する場合でも、リモートルータにルータをアドバタイズできます。この単純なハブアンドスポークネットワークの図は、リモートルータが、分散ルータを介してのみ、企業ネットワークとインターネットにアクセスできることを示しています。この例では、企業ネットワークとインターネットへのパスが常に分散ルータを経由するため、リモートルータ上の完全なルートテーブルの機能は無意味です。より大規模なルートテーブルを使用しても、リモートルータに必要なメモリの量が削減されるだけです。使用される帯域幅とメモリは、分散ルータでルートを要約し、フィルタリングすると、削減できます。このネットワークトポロジでリモートルータは、他のネットワークから検出されたルートを受信する必要はありません。これは、宛先がどこであっても、リモートルータは、すべての非ローカルトラ

フィックを分散ルータに送信する必要があるためです。真のスタブ ネットワークを設定するには、リモート ルータへのデフォルト ルートのみを送信するよう、分散ルータを設定する必要があります。

OSPF はスタブ エリアをサポートしており、EIGRP はスタブ ルータをサポートしています。



(注) EIGRP スタブ ルーティング機能は、スタブ デバイスだけで使用します。スタブ デバイスは、コア中継トラフィックが通過しないネットワーク コアまたはディストリビューション レイヤに接続されたデバイスとして定義されます。リモート ルータへ流れる IP トラフィックのルートは、ディストリビューション ルータ経由のルートのみです。スタブ デバイスがディストリビューション デバイス以外の EIGRP ネイバーを持つことはできません。この制限を無視すると、望ましくない動作が発生します。

ルーティング アルゴリズム

ルーティングアルゴリズムによって、ルータが到達可能性情報を収集して報告する方法、トポロジの変化に対応する方法、宛先までの最適ルートを決定する方法が決まります。ルーティングアルゴリズムにはさまざまなタイプがあり、各アルゴリズムがネットワークやルータリソースに与える影響もさまざまです。ルーティングアルゴリズムは、最適なルートの計算に影響するさまざまなメトリックを使用します。ルーティングアルゴリズムは、スタティックまたはダイナミック、内部または外部など、タイプで分類できます。

スタティック ルートおよびダイナミック ルーティング プロトコル

スタティック ルートは、手動で設定するルートテーブルエントリです。スタティック ルートは、手動で再設定しない限り、変更されません。スタティック ルートは設計が簡単で、ネットワークトラフィックが比較的予想しやすい環境や、ネットワーク設計が比較的単純な環境での使用に適しています。

スタティック ルーティング システムはネットワークの変化に対応できないため、絶えず変化する今日の大規模ネットワークには使用すべきではありません。今日のほとんどのルーティング プロトコルは、ダイナミック ルーティング アルゴリズムを使用しています。このアルゴリズムでは、着信ルーティング更新メッセージを分析して、ネットワーク状況の変化に合わせて調整します。メッセージがネットワークが変化したことを示している場合は、ルーティング ソフトウェアはルートを再計算し、新しいルーティングアップデートメッセージを送信します。これらのメッセージがネットワークを通過すると、ルータがそのアルゴリズムを再実行し、それに従ってルーティング テーブルを変更します。

適切であれば、ダイナミック ルーティング アルゴリズムをスタティック ルートで補完することができます。たとえば、各サブネットワークに IP デフォルト ゲートウェイまたは、ラストリゾートルータ（ルーティングできないすべてのパケットが送信されるルータ）へのスタティック ルートを設定する必要があります。

内部および外部ゲートウェイ プロトコル

ネットワークを、一意のルーティングドメインまたは自律システムに分割できます。自律システムは、管理ガイドラインの特定のセットで規制された共通の管理機関の下での内部ネットワークの一部です。自律システム間でのルートを設定するルーティングプロトコルは、外部ゲートウェイ プロトコルまたはドメイン間プロトコルと呼ばれます。BGP は、外部ゲートウェイ プロトコルの例です。1つの自律システム内で使用されるルーティングプロトコルは、内部ゲートウェイ プロトコルまたはドメイン内プロトコルと呼ばれます。EIGRP および OSPF は、内部ゲートウェイ プロトコルの例です。

リンクステート プロトコル

リンクステートプロトコルは、最短パス優先（SPF）とも呼ばれ、情報を隣接ルータと共有します。各ルータはリンクステートアドバタイズメント（LSA）を構築し、ここに、各リンクおよび直接接続されたネイバー ルータに関する情報が含まれます。

各 LSA にはシーケンス番号があります。ルータが LSA を受信し、そのリンクステートデータベースを更新すると、その LSA はすべての隣接ネイバーにフラッディングされます。ルータが同じシーケンス番号の 2 つの LSA（同じルータからの）を受信した場合は、LSA 更新ループを防ぐために、ルータは最後に受信した LSA をネイバールータにフラッディングしません。ルータは、受信直後に LSA をフラッディングするため、リンクステートプロトコルのコンバージェンス時間は最小となります。

ネイバー ルータの探索と隣接関係の確立は、リンクステート プロトコルの重要な部分です。ネイバー ルータは、特別な hello パケットを使用して探索されます。このパケットは、各ネイバー ルータのキープアライブ通知としても機能します。隣接関係は、ネイバー ルータ間のリンクステート プロトコルの一般的な動作パラメータ セットで確立されます。

ルータが受信した LSA は、そのリンクステートデータベースに追加されます。各エントリは、次のパラメータで構成されます。

- ルータ ID（LSA を構築したルータの）
- ネイバー ID
- リンク コスト
- LSA のシーケンス番号
- LSA エントリの作成時からの経過時間

ルータは、リンクステート データベース上で SPF アルゴリズムを実行し、そのルータの最短パス ツリーを構築します。この SPF ツリーを使用して、ルーティング テーブルにデータが入力されます。

リンクステートアルゴリズムでは、各ルータはネットワークの全体像をそのルーティングテーブルに構築します。リンクステートアルゴリズムが小さな更新を全体的に送信するのに対し、ディスタンスベクトルアルゴリズムは、より大きな更新をネイバールータのみに送信します。

リンクステート アルゴリズムは、より短時間でコンバージェンスするため、ディスタンス ベクトル アルゴリズムより、ルーティング ループがやや発生しにくくなっています。ただし、リンクステート アルゴリズムはディスタンス ベクトル アルゴリズムより、大きな CPU パワーとメモリを必要とします。リンクステート アルゴリズムは、実装とサポートにより多くの費用がかかる場合があります。一般的に、リンクステート プロトコルはディスタンス ベクトル プロトコルよりもスケーラブルです。

OSPF は、リンクステート プロトコルの一例です。

レイヤ3 仮想化

Cisco NX-OS は、複数の仮想ルーティングおよび転送（VRF）インスタンスおよび複数のルーティング情報ベース（RIB）をサポートしているため、複数のアドレス ドメインがサポートされます。各 VRF は RIB に関連付けられており、この情報が転送情報ベース（FIB）によって収集されます。VRF は、レイヤ3 アドレス指定ドメインを表します。各レイヤ3 インターフェイス（論理または物理）は、1 つの VRF に属します。詳細については、「[レイヤ3 仮想化の設定](#)」を参照してください。

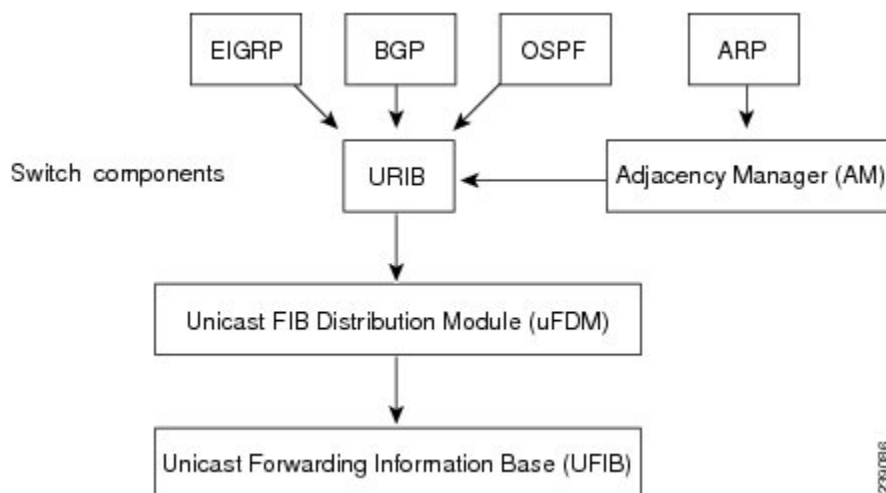
CiscoNX-OS フォワーディング アーキテクチャ

Cisco NX-OS フォワーディング アーキテクチャは、スイッチにおけるすべてのルーティング アップデートの処理および転送情報の入力を担います。

ユニキャスト RIB

Cisco NX-OS の転送アーキテクチャは、次の図に示すように、複数のコンポーネントから構成されています。

図 3: Cisco NX-OS 転送アーキテクチャ



ユニキャスト RIB は、直接接続のルート、スタティック ルート、ダイナミック ユニキャスト ルーティングプロトコルで検出されたルートを含むルーティングテーブルを維持しています。また、アドレス解決プロトコル（ARP）などの送信元から、隣接情報を収集します。ユニキャスト RIB は、ルートに最適なネクストホップを決定し、さらにユニキャスト FIB 分散モジュール（FDM）のサービスを使用して、ユニキャスト転送情報ベース（FIB）にデータを入力します。

各ダイナミック ルーティング プロトコルは、タイムアウトしたあらゆるルートについて、ユニキャスト RIB を更新する必要があります。その後、ユニキャスト RIB はそのルートを削除し、そのルートに最適なネクストホップを再計算します（代わりに使用できるパスがある場合）。

隣接マネージャ

隣接マネージャは、ARP、ネイバー探索プロトコル（NDP）、スタティック設定など、各種プロトコルの隣接情報を保持しています。最も基本的な隣接情報は、これらのプロトコルで探索されたレイヤ3からレイヤ2へのアドレスマッピングです。発信レイヤ2パケットは、隣接情報を使用して、レイヤ2ヘッダーの作成を終了します。

ARP プロセスは、ARP 要求による、レイヤ3からレイヤ2への特定のマッピングの探索をトリガーできます。新しいマッピングは、対応するARP返信を受信し、処理すると、隣接マネージャで使えるようになります。

ユニキャスト転送分散モジュール

ユニキャスト転送分散モジュールは、ユニキャスト RIB およびその他の送信元からの転送パス情報を配布します。ユニキャスト RIB は、ユニキャスト FIB がハードウェア転送テーブルにプ

ログラムする転送情報を生成します。また、ユニキャスト転送分散モジュールは、新規挿入されたモジュールへの FIB 情報のダウンロードも行います。

ユニキャスト転送分散モジュールは、隣接情報を収集し、ユニキャスト FIB でのルートの更新時に、この情報およびその他のプラットフォーム依存の情報を書き直し（リライト）します。隣接情報およびリライト情報には、インターフェイス、ネクストホップ、およびレイヤ 3 からレイヤ 2 へのマッピング情報が含まれています。インターフェイスとネクストホップの情報は、ユニキャスト RIB からのルート更新情報で受信します。レイヤ 3 からレイヤ 2 へのマッピングは、隣接マネージャから受信します。

FIB

ユニキャスト FIB は、ハードウェア転送エンジンに使用される情報を作成します。ユニキャスト FIB は、ユニキャスト転送分散モジュールからルート更新情報を受信し、ハードウェア転送エンジンにプログラミングされるよう、この情報を送信します。ユニキャスト FIB は、ルート、パス、隣接関係の追加、削除、変更を管理します。

ユニキャスト FIB は、VRF ごとおよびアドレスファミリごとに維持されます。ルート更新メッセージに基づいて、ユニキャスト FIB は、VRF ごとのプレフィックスとネクストホップ隣接情報データベースを維持します。ネクストホップ隣接データ構造には、ネクストホップの IP アドレスとレイヤ 2 リライト情報が含まれます。同じネクストホップ隣接情報構造を複数のプレフィックスで使用できます。

またユニキャスト FIB は、インターフェイスごとのユニキャスト リバース パス転送（RPF）チェックをイネーブルまたはディセーブルにします。Cisco Nexus 3600 プラットフォーム スイッチは、各入力側インターフェイスに設定される、次の 2 つの RPF モードをサポートします。

- RPF Strict チェック：ルータ転送テーブルで検証可能な送信元アドレスを持たないパケット、または送信元へのリターン パスに到着しないパケットはドロップされます。
- RPF Loose チェック：パケットはルータ転送テーブルで検証可能な送信元アドレスを持ち、送信元は物理インターフェイスを通じて到達可能です。パケットを受信する入力側インターフェイスは、FIB 内のインターフェイスに一致する必要はありません。

ハードウェア フォワーディング

Cisco NX-OS は、分散パケット転送をサポートしています。入力ポートは、パケットヘッダーから該当する情報を取得し、その情報をローカル スイッチング エンジンに渡します。ローカル スイッチング エンジンはレイヤ 3 ルックアップを行い、この情報を使って、パケットヘッダーをリライトします。入力モジュールは、パケットを出力ポートに転送します。出力ポートが別のモジュール上にある場合は、スイッチファブリックを使って、パケットが出力モジュールに転送されます。出力モジュールは、レイヤ 3 転送決定には関与しません。

ソフトウェア転送

Cisco NX-OS のソフトウェア転送パスは、主に、ハードウェアでサポートされない機能、またはハードウェア処理中に発生したエラーへの対処に使用されます。通常、IP オプション付きのパケットまたはフラグメンテーションの必要なパケットは CPU に渡されます。ユニキャスト RIB および隣接マネージャは、ソフトウェアでスイッチされるかまたは終了されるパケットに基づいて転送を決定します。

ソフトウェア転送は、コントロールプレーンポリシーおよびレートリミッタによって管理されます。

レイヤ 3 ユニキャストルーティング機能のまとめ

ここでは、Cisco NX-OS でサポートされるレイヤ 3 ユニキャスト機能およびプロトコルを簡単に説明します。

レイヤ 3 は、IPv4 プロトコルを使用します。詳細については、「[IPv4 の構成](#)」を参照してください。

IPv4 and IPv6

レイヤ 3 は、IPv4 プロトコルまたは IPv6 プロトコルを使用します。IPv6 では、ネットワークアドレスビット数が 32 ビット (IPv4 の場合) から 128 ビットに増やされています。詳細については、[IPv4 の設定 \(19 ページ\)](#) または [IPv6 の設定 \(45 ページ\)](#) を参照してください。

Open Shortest Path First (OSPF)

OSPF プロトコルは、自律システム内のネットワーク到達可能性情報の交換に使用されるリンクステートルーティングプロトコルです。各 OSPF ルータは、そのアクティブなリンクに関する情報をネイバー ルータにアドバタイズします。リンク情報には、リンクタイプ、リンクメトリック、およびリンクに接続されたネイバー ルータが含まれます。このリンク情報を含むアドバタイズメントは、リンクステートアドバタイズメントと呼ばれます。詳細については、[OSPFv2 の設定 \(75 ページ\)](#) または [OSPFv3 の設定 \(125 ページ\)](#) を参照してください。

EIGRP

EIGRP プロトコルは、ディスタンスベクトルとリンクステートの両ルーティングプロトコルの特徴を備えたユニキャストルーティングプロトコルです。これは、シスコ専用ルーティングプロトコルである IGRP の改良バージョンです。EIGRP は、典型的なディスタンスベクトルルーティングプロトコルのように、ルートを提供するためにネイバー ルータを必要とします。また、リンクステートプロトコルのように、ネイバー ルータからアドバタイズされたルートからネットワークトポロジを構築し、この情報を使用して、ループの発生しない、宛先まで

のパスを選択します。詳細については、「[EIGRP の設定 \(193 ページ\)](#)」を参照してください。

BGP

BGP は自律システム間ルーティング プロトコルです。BGP ルータは、信頼性の高い転送メカニズムとして伝送制御プロトコル (TCP) を使用し、他の BGP ルータにネットワーク到達可能性情報をアドバタイズします。ネットワーク到達可能性情報には、宛先ネットワーク プレフィックス、宛先に到達するまでに通過する必要がある自律システムのリスト、およびネクストホップルータが含まれます。到達可能性情報には、ルートの優先度、ルートの始点、コミュニティなどの詳細なパス属性が含まれます。詳細については、「[基本的 BGP の設定 \(263 ページ\)](#)」および「[高度な BGP の設定 \(297 ページ\)](#)」を参照してください。

スタティック ルーティング

スタティック ルーティングを使用して、宛先までの一定のルートを入力できます。この機能は、単純なトポロジの小規模ネットワークでは便利です。また、スタティック ルーティングは、他のルーティング プロトコルとともに、デフォルト ルートおよびルート配布の管理に使用されます。詳細については、「[スタティック ルーティングの設定](#)」を参照してください。

レイヤ 3 仮想化

仮想化を使用すると、複数の管理ドメインにわたる物理リソースを共有できます。

Cisco NX-OS は、仮想ルーティングおよび転送 (VRF) を含むレイヤ 3 仮想化をサポートしています。VRF では、レイヤ 3 ルーティング プロトコルを構成するための別のアドレス ドメインが提供されます。詳細については、「[レイヤ 3 仮想化の設定](#)」を参照してください。

Route Policy Manager

Route Policy Manager は、でルート フィルタリング機能を提供します。Route Policy Manager はルート マップを使用して、さまざまなルーティング プロトコルや、特定のルーティング プロトコル内のさまざまなエンティティ間で配布されたルートをフィルタリングします。フィルタリングは、特定の一致基準に基づいて行われます。これは、アクセス コントロール リストによるパケット フィルタリングに似ています。詳細については、「[Route Policy Manager の設定 \(443 ページ\)](#)」を参照してください。

ファーストホップ冗長プロトコル

ファーストホップ冗長プロトコル (FHRP) は、ホストへの冗長接続を可能にします。アクティブなファーストホップ ルータがダウンした場合は、その機能を引き継ぐスタンバイ ルータが FHRP によって自動的に選択されます。アドレスは仮想のものであり、FHRP グループ内の各ルータ間で共有されているため、ホストを新しい IP アドレスで更新する必要はありません。

Hot Standby Router Protocol（HSRP）の詳細については、「[HSRP の設定](#)」を参照してください。Virtual Router Redundancy Protocol（VRRP）の詳細については、「[VRRP の設定](#)」を参照してください。

オブジェクトトラッキング

オブジェクトトラッキングを使用すると、インターフェイス回線プロトコル状態、IP ルーティング、ルート到達可能性などの、ネットワーク上の特定のオブジェクトをトラッキングし、トラッキングしたオブジェクトの状態が変化したときに対処することができます。この機能により、ネットワークのアベイラビリティが向上し、オブジェクトがダウンした場合のリカバリ時間が短縮されます。詳細については、「[オブジェクトトラッキングの設定](#)」を参照してください。

関連項目

レイヤ 3 スイッチング機能に関連する Cisco マニュアルは、次のとおりです。

- [自律システムの数を検索する](#)



第 3 章

IPv4 の設定

この章では、Cisco NX-OS スイッチ上でのインターネット プロトコル バージョン 4 (IPv4) (アドレス指定を含む)、アドレス解決プロトコル (ARP) および Internet Control Message Protocol (ICMP) の設定方法を説明します。

この章は、次の項で構成されています。

- [IPv4 の概要 \(19 ページ\)](#)
- [IPv4の前提条件 \(25 ページ\)](#)
- [注意事項と制約事項 \(25 ページ\)](#)
- [デフォルト設定 \(26 ページ\)](#)
- [IPv4 の設定 \(27 ページ\)](#)
- [IPv4 設定の確認 \(44 ページ\)](#)
- [IPv4 の設定例 \(44 ページ\)](#)

IPv4 の概要

スイッチで IP を設定して、IP アドレスをネットワーク インターフェイスに割り当てられます。IP アドレスを割り当てると、インターフェイスがイネーブルになり、そのインターフェイス上のホストと通信できるようになります。

IP アドレスは、スイッチ上でプライマリまたはセカンダリとして設定できます。インターフェイスには、1つのプライマリ IP アドレスと複数のセカンダリ アドレスを設定できます。スイッチが生成したパケットは、常にプライマリ IPv4 アドレスを使用するため、インターフェイス上のすべてのネットワーキング スイッチは、同じプライマリ IP アドレスを共有する必要があります。各 IPv4 パケットは、送信元または宛先 IP アドレスからの情報に基づいています。詳細については、[複数の IPv4 アドレス](#)のセクションを参照してください。

サブネットを使用して、IP アドレスをマスクできます。マスクは、IP アドレスがどのサブネットに属するかを決定するために使用されます。IP アドレスは、ネットワーク アドレスとホスト アドレスで構成されています。マスクで、IP アドレス中のネットワーク番号を示すビットが識別できます。マスクを使用してネットワークをサブネット化した場合、そのマスクはサブネット マスクと呼ばれます。サブネット マスクは 32 ビット値で、これにより IP パケットの受信者は、IP アドレスのネットワーク ID 部分とホスト ID 部分を区別できます。

Cisco NX-OS システムの IP 機能には、IPv4 パケットの処理と IPv4 パケットの転送を行う役割があります。これには、IPv4 ユニキャストおよびマルチキャスト ルート検索、リバース パス 転送 (RPF) チェック、およびソフトウェアアクセス制御リスト (ACL) 転送が含まれます。また、IP 機能は、ネットワーク インターフェイス IP アドレス設定、重複アドレス チェック、スタティック ルート、および IP クライアントのパケット送受信インターフェイスも管理します。

複数の IPv4 アドレス

Cisco NX-OS システムは、インターフェイスごとに複数の IP アドレスをサポートしています。さまざまな状況に備え、いくつでもセカンダリ アドレスを指定できます。最も一般的な状況は次のとおりです。

- 特定のネットワーク インターフェイスのホスト IP アドレスの数が不足している場合。たとえば、サブネットにより、論理サブネットごとに 254 までのホストを使用できるが、物理サブネットの 1 つに 300 のホスト アドレスが必要な場合は、ルータ上またはアクセス サーバ上でセカンダリ IP アドレスを使用して、1 つの物理サブネットで 2 つの論理サブ ネットを使用できます。
- 1 つのネットワークの 2 つのサブネットは、別の方法で、別のネットワークにより分離できる場合があります。別のネットワークによって物理的に分離された複数のサブネットから、セカンダリ アドレスを使用して、1 つのネットワークを作成できます。このような場合、最初のネットワークは、2 番めのネットワークの上に拡張されます。つまり、上の階層となります。サブネットは、同時に複数のアクティブなインターフェイス上に表示できません。



(注) ネットワーク セグメント上のいずれかのスイッチがセカンダリ IPv4 アドレスを使用している場合は、同じネットワーク インターフェイス上の他のすべてのスイッチも、同じネットワークまたはサブネットからのセカンダリ アドレスを使用する必要があります。ネットワーク セグメント上で、一貫性のない方法でセカンダリ アドレスを使用すると、ただちにルーティング ループが発生する可能性があります。

アドレス解決プロトコル

ネットワーク スイッチおよびレイヤ 3 スイッチは、アドレス解決プロトコル (ARP) を使用して、IP (ネットワーク層) アドレスをメディアアクセス コントロール (MAC) レイヤ アドレスにマップし、IP パケットのネットワーク間の送信を可能にします。スイッチは、別のスイッチにパケットを送信する前に、独自の ARP キャッシュを調べて、宛先スイッチの MAC アドレスおよび対応する IP アドレスがあるかどうかを確認します。エントリがない場合、発信元のスイッチは、ネットワーク上のすべてのスイッチにブロードキャスト メッセージを送信します。

各スイッチは、IP アドレスをそれぞれ自身の IP アドレスと比較します。一致する IP アドレスを持つスイッチだけが、スイッチの MAC アドレスを含むパケットとともにデータを送信した

スイッチに返信します。送信元スイッチは、以降の参照用に宛先スイッチの MAC アドレスを自身の ARP テーブルに追加し、データリンク ヘッダーの作成とパケットをカプセル化するトレーラの作成を行った後、データ転送を開始します。次の図は、ARP ブロードキャストと応答プロセスを示しています。

図 4: ARP 処理



接続先スイッチが別のスイッチの背後のリモートネットワークにある場合、データを送信するルーターがデフォルト ゲートウェイの MAC アドレスに対する ARP 要求を送信する場合を除いてプロセスは同じです。アドレスが解決され、デフォルト ゲートウェイがデータ パケットを受信した後に、デフォルト ゲートウェイは、接続されているネットワーク上で宛先の IP アドレスをブロードキャストします。宛先スイッチのネットワーク上のスイッチは、ARP を使用して宛先スイッチの MAC アドレスを取得し、パケットを配信します。ARP はデフォルトでイーサネットにされています。

デフォルトのシステム定義 CoPP ポリシーは、ARP ブロードキャスト パケットのレート制限を行います。デフォルトのシステム定義 CoPP ポリシーは、ARP ブロードキャスト ストリームによるコントロールプレーン トラフィックへの影響を防止し、ブリッジド パケットに影響しません。

ARP キャッシング

ARP キャッシングにより、ブロードキャストが最小になり、ネットワーク リソースの浪費が抑制されます。IP アドレスの MAC アドレスへのマッピングは、インターネットワークを送信される各パケットに対しネットワーク上のホップ（スイッチ）ごとに発生します。そのため、ネットワーク パフォーマンスに影響を与えます。

ARP キャッシングでは、ネットワーク アドレスとそれに関連付けられたデータリンク アドレスが一定の期間、メモリに格納されるため、パケットが送信されるたびに同じアドレスを求めてブロードキャストする場合の、貴重なネットワーク リソースの使用が最小限となります。キャッシュ エントリは、定期的に失効するように設定されているため、保守が必要です。これは、古い情報が無効となる場合があるためです。ネットワーク上のすべてのスイッチは、アドレスがブロードキャストされるとそれぞれのテーブルを更新します。

ARP を使用しないデバイス

ネットワークが2つのセグメントに分割されると、ブリッジによりセグメントが結合され、各セグメントへのトラフィックが MAC アドレスに基づいてフィルタリングされます。スイッチとは対照的に MAC アドレスだけを使用するブリッジは、独自のアドレス テーブルを作成します。スイッチの場合には、IP アドレスおよび対応する MAC アドレスを含む ARP キャッシュがあります。

パッシブハブは、ネットワーク内の他のスイッチを物理的に接続する中央接続スイッチです。これは、そのすべてのポートからスイッチに対してメッセージを送信し、レイヤ1で動作しますが、アドレス テーブルは維持しません。

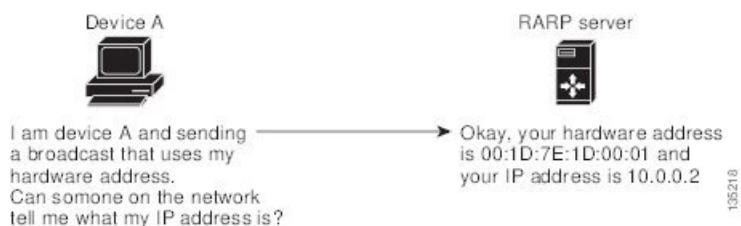
レイヤ2スイッチは、すべてのポートからメッセージを送信するハブとは異なり、メッセージの宛先であるデバイスに接続されるポートを決定し、そのポートにだけ送信します。ただし、レイヤ3スイッチは、ARP キャッシュ (テーブル) を作成するスイッチです。

Reverse ARP

RFC 903 で定義された Reverse ARP (RARP) は、ARP と同じように動作しますが、RARP 要求パケットは MAC アドレスではなく IP アドレスを要求する点が異なります。RARP は多くの場合、ディスクレスワークステーションで使用されます。これは、このタイプのデバイスには、起動時に使用する IP アドレスを格納する手段がないためです。認識できるアドレスは MAC アドレスだけで、これはハードウェアに焼き付けられているためです。

RARP を使用するには、ルータ インターフェイスとして、同じネットワーク セグメント上に RARP サーバが必要です。次の図に、RARP の仕組みを示します。

図 5: Reverse ARP



RARP には、いくつかの制限があります。これらの制限により、ほとんどの企業では、DHCP を使用してダイナミックに IP アドレスを割り当てています。DHCP は、RARP よりコスト効率が高く、必要な保守作業も少ないためです。最も重要な制限は次のとおりです。

- RARP はハードウェアアドレスを使用するため、多くの物理ネットワークを含む大規模なネットワークの場合は、各セグメント上に、冗長性のための追加サーバを備えた RARP サーバが必要です。各セグメントに 2 台のサーバを保持すると、コストがかかります。
- 各サーバは、ハードウェアアドレスと IP アドレスのスタティック マッピングのテーブルで設定する必要があります。IP アドレスの保守は困難です。
- RARP は、ホストの IP アドレスだけを提供し、サブネットマスクもデフォルトゲートウェイも提供しません。

プロキシ ARP

プロキシ ARP によって、あるネットワーク上に物理的に存在するスイッチが、同じスイッチまたはファイアウォールに接続された別の物理ネットワークの論理的な一部であることが可能になります。プロキシ ARP によって、ルータの背後のプライベート ネットワーク上のスイッチをパブリック IP アドレスを使用して隠すことができ、さらに、ルータの手前のパブリック

ネットワークにあるように見せることができます。ルータはそのアイデンティティを隠すことにより、実際の宛先までパケットをルーティングする役割を担います。プロキシ ARP を使用すると、サブネット上のスイッチは、ルーティングもデフォルトゲートウェイも設定せずにリモートサブネットまで到達できます。

スイッチが同じデータリンク層ネットワークには存在しないが、同じ IP ネットワークに存在する場合、それらのスイッチはローカルネットワーク上に存在するものとして、相互にデータ送信を試みます。ただし、これらのスイッチを隔てるルータは、ブロードキャストメッセージを送信しません。これは、ルータがハードウェアレイヤのブロードキャストを渡さず、アドレスが解決されないためです。

スイッチでプロキシ ARP をイネーブルにし、ARP 要求を受信すると、プロキシ ARP はこれを、ローカル LAN 上にないシステムに対する要求と見なします。スイッチは、ブロードキャストがアドレス指定されたリモートの宛先であるかのように、そのスイッチの MAC アドレスをリモートの宛先の IP アドレスと関連付ける ARP 応答で応答します。ローカルスイッチは、宛先に直接接続されていると確信しますが、実際には、パケットはローカルスイッチによってローカルサブネットワークから宛先サブネットワークへ転送されます。デフォルトでは、プロキシ ARP はディセーブルになっています。

ローカル プロキシ ARP

ローカル Proxy ARP を使用すると、通常ルーティングが必要ないサブネット内の IP アドレスを求める ARP 要求に対し、スイッチが応答するようにできます。ローカルプロキシ ARP をイネーブルにすると、ARP は、サブネット内の IP アドレスを求めるすべての ARP 要求に応答し、サブネット内のホスト間ですべてのトラフィックを転送します。この機能は、接続先スイッチ上での設定により、意図的にホスト間の直接的なコミュニケーションが禁止されているサブネットについてだけ使用してください。

Gratuitous ARP

Gratuitous ARP は、送信元 IP アドレスと宛先 IP アドレスが同じである要求を送信し、重複する IP アドレスを検出します。Cisco NX-OS は Gratuitous ARP 要求または ARP キャッシュの更新の有効または無効をサポートします。

収集スロットル

着信 IP パケットを転送するときに、ネクストホップのアドレス解決プロトコル (ARP) 要求が解決されない場合、パケットは ARP 解決のために中央処理装置 (CPU) にパントされます。CPU はネクストホップの MAC アドレスを解決し、ハードウェアをプログラミングします。

デバイスのハードウェアには、スーパーバイザを収集トラフィックから保護する収集レートリミッタがあります。エントリの最大数を超過している場合、ARP 要求が解決されなかったパケットは、ハードウェアでドロップされるのではなく、ソフトウェアで処理され続けます。

ARP 要求が送信されると、ソフトウェアは、同じネクストホップ IP アドレスへのパケットがスーパーバイザに転送されないようにするために、ハードウェア内に /32 ドロップ隣接関係を

追加します。ARPが解決されると、そのハードウェアエントリは正しいMACアドレスで更新されます。タイムアウト期間が経過するまでにARPエントリが解決されない場合、そのエントリはハードウェアから削除されます。



(注) Glean スロットリングはIPv4 および IPv6 でサポートされますが、IPv6 リンクローカルアドレスはサポートされません。

ICMP

ICMPを使用して、IP処理に関連するエラーおよびその他の情報を報告するメッセージパケットを提供できます。ICMPは、ICMP宛先到達不能メッセージ、ICMPエコー要求（2つのホスト間でパケットを往復送信する）、およびエコー返信メッセージなどのエラーメッセージを生成します。ICMPは多くの診断機能も備えており、ホストへのエラーパケットの送信およびリダイレクトが可能です。デフォルトでは、ICMPがイネーブルにされています。

次に示すのは、ICMPメッセージタイプの一部です。

- ネットワーク エラー メッセージ
- ネットワーク輻輳メッセージ
- トラブルシューティング情報
- タイムアウト告知



(注) ICMPリダイレクトは、ローカルプロキシARP機能がイネーブルになっているインターフェイスではディセーブルになります。

ICMP 到達不能サポートによる送信元インターフェイスの設定

ICMPエラーメッセージを処理するようにICMPソースIPフィールドのインターフェイスIPアドレスを設定できます。ICMPパケットがネットワークスタック内で構築される場合、パケットは構成されたインターフェイスIPアドレスを使用します。イーサネット、ループバック、またはポートチャネルインターフェイスを選択して、IPアドレスを構成できます。

仮想化のサポート

IPv4は、仮想ルーティングおよび転送（VRF）インスタンスをサポートしています。デフォルトでは、特に別のVRFを設定しない限り、Cisco NX-OSはユーザーをデフォルトのVRFに配置します。詳細については、「[レイヤ3仮想化の設定](#)」を参照してください。

ECMP を使用した IPv4 ルート

ルートのすべてのネクストホップが収集、ドロップ、またはパントの場合、すべてのネクストホップはマルチパス ハードウェア テーブルにそのままプログラムされます。

ルートの一部のネクストホップがグリーンニング、ドロップ、またはパントであり、残りのネクストホップがそうでない場合、非グリーンニング、ドロップ、またはパントのネクストホップのみがマルチパス ハードウェア テーブルにプログラムされます。

ECMP ルートの特定のネクストホップが解決されると（ARP ND が解決されると）、それに応じてマルチパス ハードウェア テーブルが更新されます。

IPv4の前提条件

IPv4 には、次の前提条件があります。

- IPv4 はレイヤ 3 インターフェイス上だけで設定可能です。

注意事項と制約事項

IPv4 設定時の注意事項および制約事項は、次のとおりです。

- セカンダリ IP アドレスは、プライマリ IP アドレスの設定後にだけ設定できます。
- スイッチをレイヤ 2 またはレイヤ 3 の終端スイッチとして使用する場合、Cisco はすべての VLAN で **mac-address-table-aging-time** から 1800（デフォルトの ARP エージング時間の 1500 秒よりも長く）に設定することを推奨します。
- スイッチは VLAN 単位の VLAN cam エージング タイマーをサポートしません。
- Cisco Nexus 3600-R プラットフォーム スイッチの場合、インターネット ピアリング モードは、グローバルインターネットルーティングテーブルで配信されるプレフィックスパターンでのみ使用されます。このモードでは、他のプレフィックス配布またはパターンは動作できません。その結果、プレフィックスパターンが実際のインターネット プレフィックス パターンである場合にのみ、達成可能な最大 LPM/LEM スケールが信頼できます。インターネット ピアリング モードでは、グローバルインターネットルーティングテーブル内のルートプレフィックスパターン以外のルートプレフィックスパターンが使用されている場合、スイッチは文書化されたスケーラビリティの数値を正常に達成できない可能性があります。
- Cisco NX-OS リリース 10.4(1)F 以降、サブネット外の ARP 解決のサポートは、Cisco Nexus 3600 シリーズ プラットフォーム スイッチで次の L3 インターフェイスに提供されます。
 - イーサネット
 - サブインターフェイス
 - ポート チャネル

- FEX
- IP アンナナバード インターフェイス



(注) • サブネット外 ARP 解決機能は、SVI L3 インターフェイス、および vPC、HSRP、または VXLAN 展開ではサポートされません。

- Cisco NX-OS リリース 10.4(2)F 以降では、次の機能を使用して、Cisco NX-OS デバイスのインターフェイスごとに ARP キャッシュ エントリを制限する **ip arp cache intf-limit** 構成がサポートされています。
 - グローバルモードとインターフェイスモードでサポートされます。ただし、インターフェイスモードの構成は、グローバルモードよりも優先されます。
 - 次の L3 インターフェイスでのみサポートされます。
 - SVI
 - SVI アンナナバード インターフェイス
 - 次の L3 インターフェイスではサポートされていません。
 - イーサネット
 - サブインターフェイス
 - ポート チャネル
 - アンナナバード インターフェイス
- 構成がサポートされていないインターフェイスに適用される場合、この構成はグローバルモードに適用されます。

デフォルト設定

次の表は、IP パラメータのデフォルト設定をリスト表示しています。

表 3: デフォルト IP パラメータ

パラメータ	デフォルト
ARP タイムアウト	1500 秒

パラメータ	デフォルト
『Proxy ARP』	無効化

IPv4 の設定

IPv4 アドレス指定の設定

ネットワーク インターフェイスにプライマリ IP アドレスを割り当てることができます。

手順の概要

1. **configure terminal**
2. **interface ethernet number**
3. **no switchport**
4. **ip address ip-address / length [secondary]**
5. (任意) **show ip interface**
6. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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 ethernet number 例 : switch(config)# interface ethernet 2/3 switch(config-if)#	インターフェイス設定モードを開始します。
ステップ 3	no switchport 例 : switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	ip address ip-address / length [secondary] 例 :	インターフェイスに対するプライマリ IPv4 アドレスまたはセカンダリ IPv4 アドレスを指定します。

	コマンドまたはアクション	目的
	switch(config-if)# ip address 192.2.1.1 255.0.0.0	• 4 分割ドット付き 10 進表記のアドレスでネットワークマスクを指定します。たとえば、255.0.0.0 は、1 に等しい各ビットが、ネットワークアドレスに属した対応するアドレスビットを意味することを示します。 • ネットワーク マスクは、スラッシュ (/) および数字、つまり、プレフィックス長として示される場合もあります。プレフィックス長は、アドレスの高次の連続ビットのうち、何個がプレフィックス（アドレスのネットワーク部分）を構成しているかを指定する 10 進数値です。スラッシュは 10 進数値の前に置かれ、IP アドレスとスラッシュの間にスペースは入りません。
ステップ 5	（任意） show ip interface 例： switch(config-if)# show ip interface	IPv4 用に設定されたインターフェイスを表示します。
ステップ 6	（任意） copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	この設定変更を保存します。

例

次に、IPv4 アドレスを割り当てる例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no switchport
switch(config-if)# ip address 192.2.1.1 255.0.0.0
switch(config-if)# copy running-config startup-config
```

複数の IP アドレスの設定

セカンダリ IP アドレスは、プライマリ IP アドレスの設定後にのみ追加できます。

手順の概要

1. **configure terminal**
2. **interface ethernet number**
3. **no switchport**
4. **ip address ip-address / length [secondary]**

5. (任意) **show ip interface**
6. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 ethernet number 例 : <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 3	no switchport 例 : <pre>switch(config-if)# no switchport</pre>	そのインターフェイスを、レイヤ3ルーテッドインターフェイスとして設定します。
ステップ 4	ip address ip-address / length [secondary] 例 : <pre>switch(config-if)# ip address 192.2.1.1 255.0.0.0 secondary</pre>	設定したアドレスをセカンダリ IPv4 アドレスとして指定します。
ステップ 5	(任意) show ip interface 例 : <pre>switch(config-if)# show ip interface</pre>	IPv4 用に設定されたインターフェイスを表示します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	この設定変更を保存します。

LPM インターネット ピアリング ルーティング モードの設定

Cisco NX-OS リリース9.3(1) 以降では、IPv4 および IPv6 LPM インターネット ルート エントリをサポートするために LPM インターネット ピアリング ルーティング モードを設定できます。このモードは、IPv4 プレフィックス (/32 までのプレフィックス長) および IPv6 プレフィックス (/83 までのプレフィックス長) のダイナミック トライ (ツリー ビット ルックアップ) をサポートします。このルーティング モードをサポートするのは、Cisco Nexus 3600-R プラットフォーム スイッチです。



(注) この設定は、IPv4 および IPv6 両方のアドレス ファミリに影響を及ぼします。



(注) LPM インターネット ピアリング ルーティング モードのスケール数については、『[Cisco Nexus 3600 Series NX-OS Verified Scalability Guide](#)』を参照してください。LPM インターネット ピアリング モードの Cisco Nexus 3600-R プラットフォーム スイッチは、インターネット ピアリング プレフィックスを使用する場合にのみ、予測どおりにスケールアウトします。Cisco Nexus 3600-R プラットフォーム スイッチが他のプレフィックス パターンを使用している場合は、文書化されたスケーラビリティの数値を達成できない可能性があります。

手順の概要

1. **configure terminal**
2. **[no] system routing template-internet-peering**
3. (任意) **show system routing mode**
4. **copy running-config startup-config**
5. **reload**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	[no] system routing template-internet-peering 例 : <pre>switch(config)# system routing template-internet-peering</pre>	デバイスを LPM インターネット ピア ルーティング モードにして、IPv4 および IPv6 LPM インターネット ルート エントリをサポートします。
ステップ 3	(任意) show system routing mode 例 : <pre>switch(config)# show system routing mode Configured System Routing Mode: Internet Peering Applied System Routing Mode: Internet Peering</pre>	LPM ルーティング モードを表示します。
ステップ 4	copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

	コマンドまたはアクション	目的
ステップ 5	reload 例 : <pre>switch(config)# reload</pre>	デバイス全体をリブートします。

LPM インターネット ピアリング ルーティング モードの追加設定

大規模ルーティング環境で LPM インターネット ピアリング ルーティング モードで Cisco Nexus スイッチを導入する場合、またはネクストホップ数が増加するルートの場合は、VDC リソース テンプレートで IPv4 のメモリ制限を増やす必要があります。

手順の概要

1. **configure terminal**
2. (任意) **show routing ipv4 memory estimate routes routes next-hops hops**
3. **vdc switch id id**
4. **limit-resource u4route-mem minimum min-limit maximum max-limit**
5. **exit**
6. **copy running-config startup-config**
7. **reload**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	(任意) show routing ipv4 memory estimate routes routes next-hops hops 例 : <pre>switch(config)# show routing ipv4 memory estimate routes 262144 next-hops 32 Shared memory estimates: Current max 512 MB; 78438 routes with 64 nhs in-use 2 MB; 2642 routes with 1 nhs (average) Configured max 512 MB; 78438 routes with 64 nhs Estimate memory with fixed overhead: 1007 MB; 262144 routes with 32 nhs Estimate with variable overhead included: - With MVPN enabled VRF: 1136 MB - With OSPF route (PE-CE protocol): 1375 MB - With EIGRP route (PE-CE protocol): 1651 M</pre>	共有メモリの見積もりを表示して、ルートのメモリ要件を判断します。

	コマンドまたはアクション	目的
ステップ 3	vdc switch id id 例 : <code>switch(config)# vdc switch id 1</code> <code>switch(config-vdc)#</code>	VDC スイッチ ID を指定します。
ステップ 4	limit-resource u4route-mem minimum min-limit maximum max-limit 例 : <code>switch(config-vdc)# limit-resource u4route-mem minimum 1024 maximum 1024</code>	IPv4 メモリの制限をメガバイト単位で指定します。
ステップ 5	exit 例 : <code>switch(config-vdc)# exit</code> <code>switch(config)#</code>	VDC 設定モードを終了します。
ステップ 6	copy running-config startup-config 例 : <code>switch(config)# copy running-config startup-config</code>	この設定変更を保存します。
ステップ 7	reload 例 : <code>switch(config)# reload</code>	デバイス全体をリブートします。

スタティック ARP エントリの設定

スイッチ上に、IP アドレスを MAC ハードウェア アドレス（スタティック マルチキャスト MAC アドレスを含む）にマップするスタティック ARP エントリを設定できます。

手順の概要

1. **configure terminal**
2. **interface ethernet number**
3. **no switchport**
4. **ip arp ipaddr mac_addr**
5. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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 ethernet number 例 : switch(config)# interface ethernet 2/3 switch(config-if)#	インターフェイス設定モードを開始します。
ステップ 3	no switchport 例 : switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッドインターフェイスとして設定します。
ステップ 4	ip arp ipaddr mac_addr 例 : switch(config-if)# ip arp 192.2.1.1 0019.076c.1a78	IP アドレスを MAC アドレスにスタティック エントリとして関連付けます。
ステップ 5	copy running-config startup-config 例 : switch(config-if)# copy running-config startup-config	この設定変更を保存します。

例

次に、スタティック ARP エントリを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no switchport
switch(config-if)# ip arp 1 92.2.1.1 0019.076c.1a78
switch(config-if)# copy running-config startup-config
```

プロキシ ARP の設定

スイッチで、別のネットワークまたはサブネット上のホストのメディアアドレス定義する Proxy ARP を設定できます。

手順の概要

1. configure terminal

2. **interface ethernet number**
3. **no switchport**
4. **ip proxy-arp**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 ethernet number 例 : <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 3	no switchport 例 : <pre>switch(config-if)# no switchport</pre>	そのインターフェイスを、レイヤ3ルーテッドインターフェイスとして設定します。
ステップ 4	ip proxy-arp 例 : <pre>switch(config-if)# ip proxy-arp</pre>	インターフェイス上でプロキシ ARP をイネーブルにします。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、プロキシ ARP を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no switchport
switch(config-if)# ip proxy-arp
switch(config-if)# copy running-config startup-config
```

ローカル プロキシ ARP の設定

スイッチ上でローカル プロキシ ARP を設定できます。

手順の概要

1. **configure terminal**
2. **interface ethernet number**
3. **no switchport**
4. **ip local-proxy-arp**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 ethernet number 例 : <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 3	no switchport 例 : <pre>switch(config-if)# no switchport</pre>	そのインターフェイスを、レイヤ3ルーテッドインターフェイスとして設定します
ステップ 4	ip local-proxy-arp 例 : <pre>switch(config-if)# ip local-proxy-arp</pre>	インターフェイス上でローカル プロキシ ARP をイネーブルにします。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、ローカル プロキシ ARP を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no switchport
switch(config-if)# ip local-proxy-arp
switch(config-if)# copy running-config startup-config
```

無償 ARP の設定

インターフェイス上で Gratuitous ARP を設定できます。

手順の概要

1. **configure terminal**
2. **interface ethernet number**
3. **no switchport**
4. **ip arp gratuitous { request | update }**
5. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 ethernet number 例 : <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 3	no switchport 例 : <pre>switch(config-if)# no switchport</pre>	そのインターフェイスを、レイヤ3ルーテッドインターフェイスとして設定します。
ステップ 4	ip arp gratuitous { request update } 例 : <pre>switch(config-if)# ip arp gratuitous request</pre>	インターフェイス上で無償 ARP をイネーブルにします。デフォルトはイネーブルです。
ステップ 5	copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、IP 収集スロットルを有効にする例を示します。

```
switch# configure terminal
switch(config)# hardware ip glean throttle
switch(config-if)# copy running-config startup-config
```

サブネット外の ARP 解決の構成

Cisco NX-OS リリース 10.4(1)F 以降では、**ip arp outside-subnet** コマンドを使用してサブネット外 ARP 解決を有効または無効にできます。

このコマンドは、グローバル モードとインターフェイス モードの両方で使用できます。このコマンドが有効になっている場合、**config-replace** およびデュアル ステージ コミットには影響しません。



(注) このコマンドを有効にすると、Cisco NX-OS リリース 10.4(1)F からのダウングレードが制限され、ダウングレードを続行する前に、サブネット外 ARP 解決構成を削除するように求めるエラー メッセージがユーザーに表示されます。

手順の概要

1. **configure terminal**
2. **[no] ip arp outside-subnet**
3. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	[no] ip arp outside-subnet 例 : switch(config)# ip arp outside-subnet	接続されたホストのサブネット パケット トランザクションからの ARP を有効または無効にします。
ステップ 3	(任意) copy running-config startup-config 例 :	この設定変更を保存します。

	コマンドまたはアクション	目的
	<code>switch(config)# copy running-config startup-config</code>	

SVI インターフェイスごとの ARP キャッシュの構成

Cisco NX-OS リリース 10.4(2)F 以降では、Cisco NX-OS デバイスの SVI インターフェイスごとに許可される ARP キャッシュ エントリの最大数を設定できます。この構成は、グローバルモードとインターフェイス モードの両方でサポートされます。

手順の概要

1. **configure terminal**
2. **interface vlan *vlan-id***
3. **[no] ip arp cache intf-limit *value***
4. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <code>switch# configure terminal</code> <code>switch(config)#</code>	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 vlan <i>vlan-id</i> 例 : <code>switch(config)# interface vlan 5</code> <code>switch(config-if)#</code>	VLAN インターフェイスを作成し、SVI の設定モードを開始します。
ステップ 3	[no] ip arp cache intf-limit <i>value</i> 例 : <code>switch(config-if)# ip arp cache intf-limit 50000</code> <code>switch(config-if)#</code>	SVI インターフェイスの ARP キャッシュ エントリの制限を構成します。有効な ARP エントリの範囲は 1 ～ 128000 です。 intf-limit : インターフェイスごとの有効なダイナミック ARP エントリの数を指定します。 構成を削除するには、この no コマンドの no 形式を使用します。
ステップ 4	(任意) copy running-config startup-config 例 : <code>switch(config)# copy running-config startup-config</code>	この設定変更を保存します。

IP ダイレクト ブロードキャストの設定

IP ダイレクト ブロードキャストは、宛先アドレスが何らかの IP サブネットの有効なブロードキャストアドレスであるにもかかわらず、その宛先サブネットに含まれないノードから発信される IP パケットです。

宛先サブネットに直接接続されていないスイッチは、ユニキャスト IP パケットをそのサブネット上のホストに転送するのと同じ方法で、IP ダイレクト ブロードキャストを転送します。ダイレクトブロードキャストパケットが、宛先サブネットに直接接続されたスイッチに到着すると、宛先サブネット上のブロードキャストとして「展開」されます。パケットの IP ヘッダー内の宛先アドレスはそのサブネットに設定された IP ブロードキャスト アドレスに書き換えられ、パケットはリンク層ブロードキャストとして送信されます。

あるインターフェイスでダイレクトブロードキャストがイネーブルになっている場合、着信した IP パケットが、そのアドレスに基づいて、そのインターフェイスが接続されているサブネットを対象とするダイレクトブロードキャストとして識別されると、そのパケットはそのサブネット上にブロードキャストとして展開されます。

IP ダイレクトブロードキャストをイネーブルにするには、インターフェイスコンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
ip directed-broadcast	ダイレクトブロードキャストの物理ブロードキャストへの変換を有効にします。

IP 収集スロットルの設定

Cisco NX-OS ソフトウェアは、収集トラフィックからスーパーバイザを保護する収集スロットル レート リミッタをサポートします。



- (注) 到達不能な、または存在しないネクスト ホップの ARP 解決のために、スーパーバイザに送信された不要な収集パケットをフィルタリングするために、「**hardware ip glean throttle**」コマンドを使用して、IP 収集スロットル機能を構成することを推奨します。IP 収集スロットルは、ソフトウェアのパフォーマンスを向上させ、トラフィックをより効率的に管理します。



- (注) Glean スロットリングは IPv4 および IPv6 でサポートされますが、IPv6 リンクローカルアドレスはサポートされません。

手順の概要

1. **configure terminal**
2. **hardware ip glean throttle**

3. **no hardware ip glean throttle**
4. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	hardware ip glean throttle 例 : switch(config)# hardware ip glean throttle	ARP スロットリングを有効にします。
ステップ 3	no hardware ip glean throttle 例 : switch(config)# no hardware ip glean throttle	ARP スロットリングを無効にします。
ステップ 4	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	この設定変更を保存します。

例

次に、IP 収集スロットルを有効にする例を示します。

```
switch# configure terminal
switch(config)# hardware ip glean throttle
switch(config-if)# copy running-config startup-config
```

ハードウェア IP 収集スロットルのタイムアウトの設定

インストールされたドロップ隣接関係が FIB 内に残る時間のタイムアウトを設定できます。

手順の概要

1. **configure terminal**
2. **hardware ip glean throttle maximum timeout timeout-in-seconds**
3. **[no] hardware ip glean throttle maximum timeout timeout-in-seconds**
4. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	hardware ip glean throttle maximum timeout timeout-in-seconds 例 : <pre>switch(config)# hardware ip glean throttle maximum timeout 300</pre>	インストールされたドロップ隣接関係が FIB 内に残る時間のタイムアウトを設定します。
ステップ 3	[no] hardware ip glean throttle maximum timeout timeout-in-seconds 例 : <pre>switch(config)# no hardware ip glean throttle maximum timeout 300</pre>	デフォルトの制限値を適用します。 タイムアウト値は秒単位です。範囲は300秒（5分）～1800秒（30分）です。 （注） タイムアウト期間を超えた後、ドロップ隣接関係は FIB から削除されます。
ステップ 4	（任意） copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、Gratuitous ARP 要求をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# hardware ip glean throttle maximum timeout 300
switch(config-if)# copy running-config startup-config
```

ICMP 送信元 IP フィールドのインターフェイス IP アドレスの設定

ICMP エラー メッセージを処理するように ICMP ソース IP フィールドのインターフェイス IP アドレスを設定できます。

手順の概要

1. configure terminal

2. `[no] ip source {ethernet slot/port | loopback number | port-channel number} {icmp-errors}`

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	<code>[no] ip source {ethernet slot/port loopback number port-channel number} {icmp-errors}</code> 例 : <pre>switch(config)# ip source loopback 0 icmp-errors</pre>	ICMP 送信元 IP フィールドのインターフェイス IP アドレスを設定し、ICMP エラー メッセージをルーティングします。

例

この例では、ICMP 送信元 IP フィールドでインターフェイス IP アドレスを構成する方法を示します。

```
switch# configure terminal
switch(config)# ip source ethernet 1/1 icmp-errors
```

この例では、ICMP 送信元 IP フィールドでインターフェイス IP アドレスを構成する方法を示します。

```
switch# configure terminal
switch(config)# no ip source ethernet 1/1 icmp-errors
```

IP パケットのソフトウェア転送のログギングの設定

NX-OS ソフトウェアによって転送される IP パケットのログギング条件を設定できます。条件は次のとおりです。

- パケットの最小数（サイズ）
- オプションの期間（ログギング間隔）

ログギング条件により、1秒あたりのパケット数（pps）のしきい値が作成されます。トラフィックが条件を満たしているか超えると、NX-OS はコンソール メッセージをログに記録します。次に例を示します。

```
2019 jul 31 15:28:31 switch-1 %$ VDC-1 %$ %USER-3-SYSTEM_MSG: Packets per second exceeded
the configured threshold 40, current PPS: 1262 - netstack
```

ip pps threshold unicast-forward コマンドを使用して、転送されるパケットの条件を設定できます。この機能を無効にするには、**no ip pps threshold unicast-forward**を使用します。

手順の概要

1. **config terminal**
2. **ip pps threshold unicast-forward pps-threshold [syslog-interval]**
3. (オプション) **show ip pps threshold**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	config terminal 例 : <pre>switch-1# config terminal Enter configuration commands, one per line. End with CNTL/Z. switch-1(config)#</pre>	端末の構成を開始します
ステップ 2	ip pps threshold unicast-forward pps-threshold [syslog-interval] 例 : <pre>switch-1(config)# ip pps threshold unicast-forward 50 5 switch-1(config)#</pre>	この機能を有効にして条件を設定します。 • pps-threshold は 1 ～ 30000 パケットです。 • syslog-interval は 1 ～ 60 秒です。デフォルト値は 1 秒です。
ステップ 3	(オプション) show ip pps threshold 例 : <pre>switch-1(config) show ip traffic pps PPS type : unicast-forward, PPS limit : 50, Log Interval: 5 switch-1(config)#</pre>	現在の PPS しきい値設定を表示します。

例

次の例は、特定のフローで転送されるパケット数が、設定されたパケット数および 2 秒ごとに 4000 パケットというログギング間隔を超えた場合に、コンソール メッセージを設定する方法を示しています。

```
switch-1# configure terminal
switch-1(config)# ip pps threshold unicast-forward 4000 2
switch-1(config)# copy running-config startup-config
```

IPv4 設定の確認

IPv4 の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
how hardware forwarding ip verify	IP パケット検証の設定を表示します。
show ip adjacency	隣接関係テーブルを表示します。
show ip arp	ARP テーブルを表示します。
show ip interface	IP に関連するインターフェイス情報を表示します。
show ip arp statistics [vrf vrf-name]	ARP 統計情報を表示します。
show ip adjacency summary	スロットル隣接関係の数のサマリーを表示します。
show ip arp summary	スロットル隣接関係の数のサマリーを表示します。
show ip interface	IP に関連するインターフェイス情報を表示します。

IPv4 の設定例

次に、IPv4 アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config)# no switchport
switch(config-if)# ip address 192.2.1.1/1
```



第 4 章

IPv6 の設定

この章では、Cisco NX-OS デバイス上でのインターネット プロトコル バージョン 6 (IPv6) (アドレス指定を含む)、ネイバー探索プロトコル (ND)、および Internet Control Message Protocol (ICMP) の構成方法を説明します。

この章は、次の項で構成されています。

- [IPv6 について \(45 ページ\)](#)
- [IPv6 の前提条件 \(61 ページ\)](#)
- [IPv6 の注意事項および制約事項 \(62 ページ\)](#)
- [デフォルト設定 \(62 ページ\)](#)
- [IPv6 の設定 \(63 ページ\)](#)
- [IPv6 設定の確認 \(72 ページ\)](#)
- [IPv6 の設定例 \(73 ページ\)](#)

IPv6 について

IPv6 は、IPv4 の後継として設計されており、ネットワーク アドレス ビット数が 32 ビット (IPv4 の場合) から 128 ビットに増やされています。IPv6 は IPv4 に基づいていますが、アドレス空間が大幅に拡大されており、メインヘッダーと拡張ヘッダーの簡素化など、その他の機能強化が含まれています。

拡大された IPv6 アドレス空間により、ネットワークのスケラビリティが可能となり、グローバルな到達可能性が提供されます。簡素化された IPv6 パケット ヘッダー形式により、パケットの処理効率が向上しています。柔軟性の高い IPv6 アドレス空間により、プライベート アドレスの必要性和、プライベート (グローバルに一意ではない) アドレスを限られた数のパブリック アドレスに変換するネットワーク アドレス変換 (NAT) の使用が削減されます。IPv6 を使用すると、ネットワークの境界にある境界ルータによる特別な処理を必要としない新しいアプリケーション プロトコルがイネーブルになります。

プレフィックス集約、簡易ネットワーク再番号割り当て、IPv6 サイト マルチホーミング機能などの IPv6 機能により、さらに効率的にルーティングが行われます。IPv6 は、IPv6 向け Open Shortest Path First (OSPF) やマルチプロトコル ボーダー ゲートウェイ プロトコル (BGP) をサポートしています。

IPv6 アドレス形式

IPv6 アドレスは 128 ビットつまり 16 バイトです。このアドレスは、x:x:x:x:x:x:x のように、コロン (:) で区切られた 16 ビット 16 進数のブロック 8 つに分かれています。次に、IPv6 アドレスの例を 2 つ示します。

```
2001:0DB8:7654:3210:FEDC:BA98:7654:32102001:0DB8:0:0:8:800:200C:417A
```

IPv6 アドレスの中には、連続するゼロが含まれます。IPv6 アドレスの先頭、中間、または末尾で、この連続するゼロの代わりに 2 つのコロン (::) を使用できます。次の表は、圧縮された IPv6 アドレス フォーマットの一覧です。



- (注) IPv6 アドレスでは、アドレス中で最も長く連続するゼロの代わりに、2 つのコロン (::) を 1 度だけ使用できます。

連続する 16 ビット値がゼロで示されている場合は、2 つのコロンを IPv6 アドレスの一部として使用できます。インターフェイスごとに複数の IPv6 アドレスを設定できますが、設定できるリンクローカルアドレスは 1 つだけです。

IPv6 アドレス中の 16 進数の文字の大文字と小文字は区別されません。

表 4: 圧縮された IPv6 アドレス形式

IPv6 アドレス タイプ	優先形式	圧縮形式
ユニキャスト	2001:0:0:0:0DB8:800:200C:417A	2001::0DB8:800:200C:417A
マルチキャスト	FF01:0:0:0:0:0:101	FF01::101
ループバック	0:0:0:0:0:0:0:1	::1
未指定	0:0:0:0:0:0:0:0	::

ノードは表「圧縮された IPv6 アドレス形式 (Compressed IPv6 Address Formats)」にあるループバック アドレスを使用して、IPv6 パケットを自分宛てでテーブルに送信できます。IPv6 のループバック アドレスは、IPv4 のループバック アドレスと同じです。詳細については、[概要 \(3 ページ\)](#) を参照してください。



- (注) IPv6 ループバック アドレスは、物理インターフェイスに割り当ててはできません。送信元または宛先のアドレスとして IPv6 ループバック アドレスを含むパケットは、そのパケットを作成したノードの外には転送できません。IPv6 ルータは、IPv6 ループバック アドレスを送信元アドレスまたは宛先アドレスとするパケットを転送しません。



- (注) IPv6 未指定アドレスは、インターフェイスに割り当てることはできません。未指定 IPv6 アドレスは、IPv6 パケット内の宛先アドレスまたは IPv6 ルーティング ヘッダーとして使用しないでください。

IPv6 プレフィックスは、RFC 2373 で規定された形式です。この形式では、IPv6 アドレスが、コロンに囲まれた 16 ビット値を使用した 16 進数で指定されています。プレフィックス長は、アドレスの高次の連続ビットのうち、何個がプレフィックス（アドレスのネットワーク部分）を構成しているかを指定する 10 進数値です。たとえば、2001:0DB8:8086:6502::/32 は有効な IPv6 プレフィックスです。

IPv6 ユニキャスト アドレス

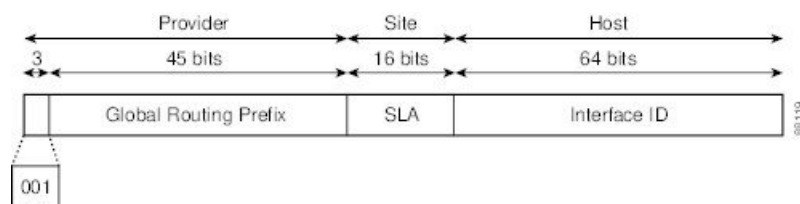
IPv6 ユニキャストアドレスは、1つのノード上の1つのインターフェイスの ID です。ユニキャストアドレスに送信されたパケットは、そのアドレスが示すインターフェイスに配信されます。

集約可能グローバル アドレス

集約可能グローバルアドレスは、集約可能なグローバルユニキャストプレフィックスによる IPv6 アドレスです。集約可能グローバルユニキャストアドレスの構造により、グローバルルーティングテーブル内のルーティングテーブル エントリ数を制限するルーティングプレフィックスの厳密な集約が可能になります。集約可能グローバルアドレスは、組織を上に向かって、最終的にインターネットサービスプロバイダー（ISP）まで集約されるリンク上で使用されます。

集約可能なグローバル IPv6 アドレスは、グローバルルーティングプレフィックス、サブネット ID、およびインターフェイス ID により定義されます。バイナリ 000 で始まるアドレスを除き、グローバルユニキャストアドレスはすべて 64 ビット インターフェイス ID を持ちます。IPv6 グローバルユニキャストアドレスの割り当てには、バイナリ値 001 (2000::/3) から始まるアドレスの範囲が使用されます。次の図は、集約可能グローバルアドレスの構造を示しています。

図 6: 集約可能グローバルアドレス形式



2000::/3 (001) ~ E000::/3 (111) のプレフィックスを持つアドレスには、Extended Universal Identifier (EUI) 64 形式の 64 ビット インターフェイス識別子が必要です。インターネット割り当て番号局（IANA）は、2000::/16 の範囲の IPv6 アドレス空間を地域レジストリに割り当てます。

集約可能なグローバルアドレスは、48 ビットグローバルルーティングプレフィックスと、16 ビットサブネット ID または Site-Level Aggregator (SLA) で構成されます。IPv6 集約可能グローバルユニキャストアドレスの形式に関するドキュメント (RFC 2374) によると、グローバルルーティングプレフィックスには、Top-Level Aggregator (TLA) と Next-Level Aggregator (NLA) という 2 つの階層構造のフィールドが含まれています。TLS フィールドおよび NLA フィールドはポリシーベースであるため、IETF は、これらのフィールドを RFC から削除することを決定しました。この変更以前に展開された既存の IPv6 ネットワークの中には、依然として、古いアーキテクチャ上のネットワークを使用しているものもあります。

個々の組織は、16 ビットサブネットフィールドであるサブネット ID を使用して、ローカルアドレス指定階層を作成したり、サブネットを識別したりできます。サブネット ID は IPv4 でのサブネットに似ていますが、IPv6 サブネット ID を持つ組織では最大 65,535 個のサブネットをサポートできるという点が異なります。

インターフェイス ID により、リンク上のインターフェイスが識別されます。インターフェイス ID は、リンク上では一意です。多くの場合、インターフェイス ID は、インターフェイスのリンク層アドレスと同じか、リンク層アドレスに基づいています。集約可能なグローバルユニキャストやその他の IPv6 アドレス タイプで使用されるインターフェイス ID は 64 ビットであり、形式は変更済み EUI-64 フォーマットです。

インターフェイス ID は、次のいずれかに該当する修正 EUI-64 形式です。

- すべての IEEE 802 インターフェイス タイプ（イーサネット、およびファイバ分散データ インターフェイスなど）の場合は、最初の 3 オクテット（24 ビット）がそのインターフェイスの 48 ビットリンク層アドレス（MAC アドレス）の Organizationally Unique Identifier (OUI)、4 番めと 5 番めのオクテット（16 ビット）が FFFE の固定 16 進数値、そして、最後の 3 オクテット（24 ビット）が MAC アドレスの最後の 3 オクテットです。最初のオクテットの 7 番めのビットである Universal/Local (U/L) ビットの値は 0 または 1 です。ゼロはローカルに管理されている ID を表し、1 はグローバルに一意の IPv6 インターフェイス ID を表します。
- その他すべてのインターフェイス タイプ（シリアル、ループバック、ATM、フレーム リレー、トンネルインターフェイス タイプなど、IPv6 オーバーレイ トンネルで使用されるトンネルインターフェイスを除く）の場合、インターフェイス ID は IEEE 802 インターフェイス タイプのインターフェイス ID に似ていますが、ルータの MAC アドレスプールの最初の MAC アドレスが識別子として使用されます（インターフェイスには MAC アドレスがないため）。
- IPv6 オーバーレイ トンネルで使用されるトンネルインターフェイス タイプの場合、インターフェイス ID は、識別子の上位 32 ビットがすべてゼロであるトンネルインターフェイスに割り当てられた IPv4 アドレスです。



- (注) PPP (ポイントツーポイントプロトコル) を使用するインターフェイスの場合は、接続の両端のインターフェイスが同じMACアドレスを持つため、接続の両端のインターフェイスIDが、両方のIDが一意となるまでネゴシエートされます (ランダムに選択され、必要に応じて再構築されます)。ルータの最初のMACアドレスが、PPPを使用するインターフェイスのIDとして使用されます。

ルータに IEEE 802 インターフェイス タイプがない場合は、ルータのインターフェイスでリンクローカル IPv6 アドレスが次のシーケンスで生成されます。

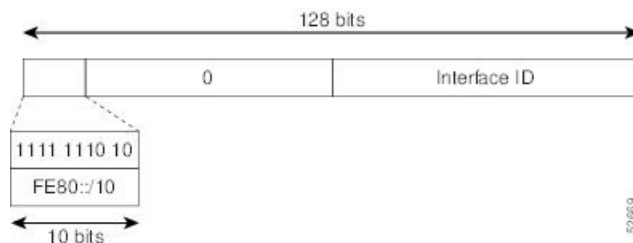
1. ルータに MAC アドレスが (ルータの MAC アドレス プールから) 照会されます。
2. 使用可能な MAC アドレスがルータにない場合は、ルータのシリアル番号を使用してリンクローカルアドレスが作成されます。
3. リンクローカルアドレスの作成にルータのシリアル番号を使用できない場合、ルータは MD5 ハッシュを使用して、ルータのホスト名からルータの MAC アドレスを決定します。

リンクローカルアドレス

リンクローカルアドレスは、リンクローカルプレフィックス FE80::/10 (1111 1110 10) と変更された EUI-64 形式のインターフェイス識別子を使用するすべてのインターフェイスを自動的に設定できる IPv6 ユニキャストアドレスです。リンクローカルアドレスは、ネイバー探索プロトコル (NDP) で使用されます。ローカルリンク上のノードは、リンクローカルアドレスを使用して通信できます。ノードの通信にグローバルに一意のアドレスは不要です。次の図は、以下のリンクローカルアドレスの構造を示しています。

IPv6 ルータは、送信元または宛先がリンクローカルアドレスであるパケットを他のリンクに転送できません。

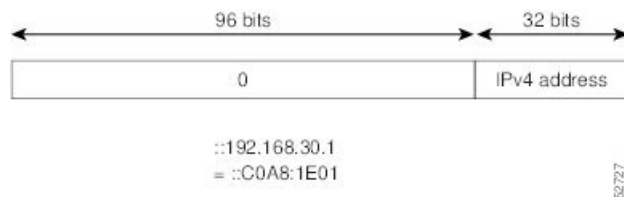
図 7: リンクローカルアドレス形式



IPv4 互換 IPv6 アドレス

IPv4 互換 IPv6 アドレスは、アドレスの上位 96 ビットがゼロであり、アドレスの下位 32 ビットが IPv4 アドレスである IPv6 ユニキャストアドレスです。IPv4 互換 IPv6 アドレスの形式は、0:0:0:0:0:A.B.C.D または ::A.B.C.D です。IPv4 互換 IPv6 アドレスの 128 ビット全体がノードの IPv6 アドレスとして使用され、下位 32 ビットに埋め込まれた IPv4 アドレスがノードの IPv4 アドレスとして使用されます。IPv4 互換 IPv6 アドレスは、IPv4 と IPv6 の両方のプロトコル

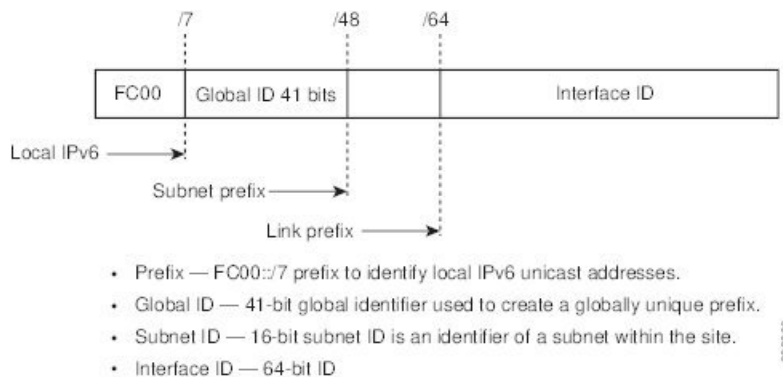
図 8: IPv4 互換 IPv6 アドレス形式



一意のローカルアドレスは、グローバルに一意であり、ローカル通信を目的とした IPv6 ユニキャストアドレスです。グローバルなインターネット上でのルーティングには対応しておらず、サイトなどの限られたエリア内だけでルーティング可能です。限られた複数のサイト間もルーティングできる場合もあります。アプリケーションは、ユニーク ローカルアドレスをグローバル スコープのアドレスのように扱うことができます。

- ・グローバルに一意のプレフィックスを持っている（一意である可能性が大）。
- ・既知のプレフィックスがあるため、サイト境界で簡単にフィルタリングできる。
- ・アドレス競合を発生させたり、これらのプレフィックスを使用するインターフェイスのリナンバリングを必要としたりすることなく、サイトを結合またはプライベートに相互接続できる。
- ・ISP に依存せず、永続的または断続的なインターネット接続がなくてもサイト内での通信に使用できる。
- ・ルーティングやドメイン ネーム サーバ（DNS）を通して誤ってサイト外に漏れても、他のどのアドレスとも競合しない。

図 9: ユニーク ローカル アドレスの構造



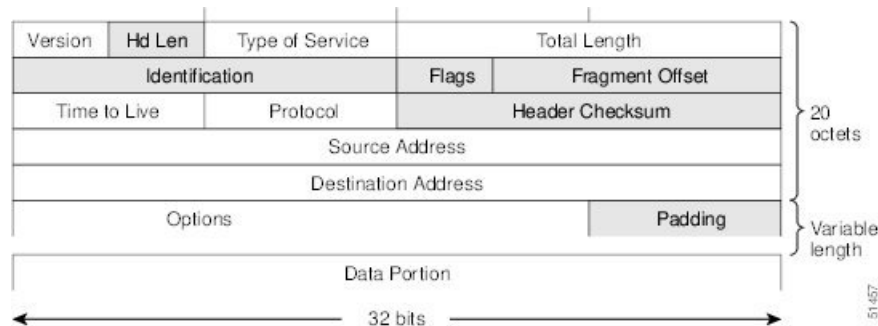
サイトローカルアドレス

RFC 3879 によりサイトローカルアドレスの使用が廃止されたため、プライベート IPv6 アドレスの設定時には、RFC 4193 で推奨されるユニーク ローカルアドレス（UCA）を使用する必要があります。

IPv4 パケット ヘッダー

基本 IPv4 パケット ヘッダーには、合計サイズが 20 オクテット（160 ビット）の 12 のフィールドがあります（以下の図を参照）。この 12 個のフィールドのあとにはオプション フィールドが、さらにそのあとに、通常はトランスポート レイヤ パケットであるデータ部分が続く場合があります。可変長のオプション フィールドは、IPv4 パケット ヘッダーの合計サイズに加算されます。IPv4 パケット ヘッダーのグレーの部分のフィールドは、IPv6 パケット ヘッダーに含まれません。

図 10: IPv4 パケット ヘッダー形式



簡易 IPv6 パケット ヘッダー

base IPv6 パケット ヘッダーには、合計サイズが 40 オクテット（320 ビット）の 8 のフィールドがあります（次の図を参照）。フラグメンテーションはパケットの送信元により処理され、データリンク層のチェックサムとトランスポート層が使用されます。ユーザ データグラム プロトコル（UDP）チェックサムにより、内部パケットと基本 IPv6 パケット ヘッダーの整合性がチェックされ、オプション フィールドが 64 ビットに揃えられるため、IPv6 パケットの処理が容易になります。

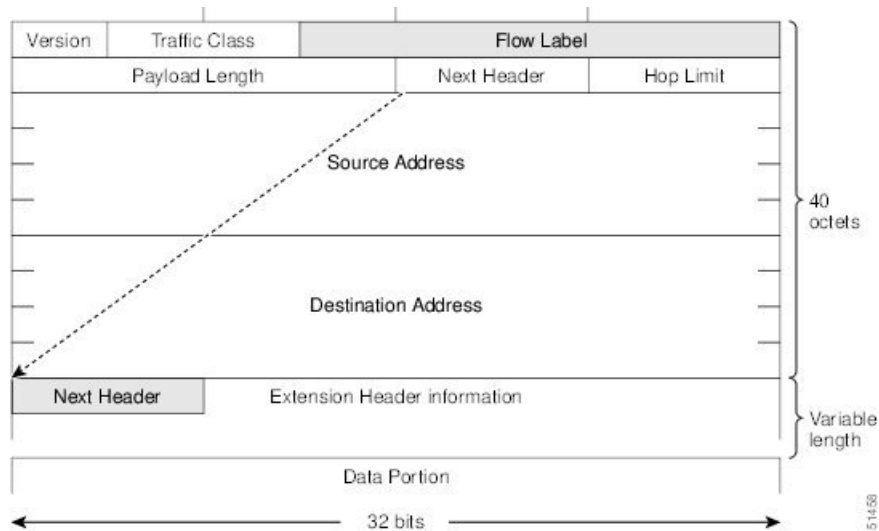
次の表に、基本 IPv6 パケット ヘッダーのフィールドをリストします。

表 5: 表 3-2 基本 IPv6 パケット ヘッダーのフィールド

フィールド	説明
バージョン	IPv4 パケット ヘッダーのバージョン フィールドに該当しますが、IPv4 で示される数字 4 の代わりに、IPv6 では数字 6 が示されます。

フィールド	説明
トラフィック クラス	IPv4 パケット ヘッダーのタイプオブサービス フィールドと同様です。トラフィック クラス フィールドは、差別化されたサービスで 사용되는トラフィック クラスのタグをパケットに付けます。
フロー ラベル	IPv6 パケット ヘッダーの新規フィールドです。フロー ラベル フィールドは、ネットワーク層でパケットを差別化する特定のフローのタグをパケットに付けます。
ペイロード長	IPv4 パケット ヘッダーの合計長フィールドと同様です。ペイロード長 フィールドは、パケットのデータ部分の合計長を示します。
次ヘッダー	IPv4 パケットヘッダーのプロトコルフィールドと同様です。次ヘッダー フィールドの値により、基本 IPv6 ヘッダーに続く情報のタイプが決まります。基本 IPv6 ヘッダーに続く情報のタイプは、次の図に示すように、TCP パケット、UDP パケット、または拡張ヘッダーなどのトランスポート層パケットです。
ホップ リミット	IPv4 パケット ヘッダーの存続可能時間フィールドと同様です。ホップ リミット フィールドの値は、IPv6 パケットが無効と見なされる前に通過できるルータの最大数です。各ルータを通過するたびに、この値が 1 つずつ減少します。IPv6 ヘッダーにはチェックサムがないため、ルータは値を減らすたびにチェックサムを再計算する必要がなく、処理リソースが節約されます。
送信元アドレス	IPv4 パケットヘッダーの送信元アドレス フィールドと同様ですが、IPv4 の 32 ビット送信元アドレスの代わりに、IPv6 では 128 ビットの送信元アドレスが含まれます。
宛先アドレス	IPv4 パケットヘッダーの宛先アドレス フィールドと同様ですが、IPv4 の 32 ビット宛先アドレスの代わりに、IPv6 では 128 ビットの宛先アドレスが含まれます。

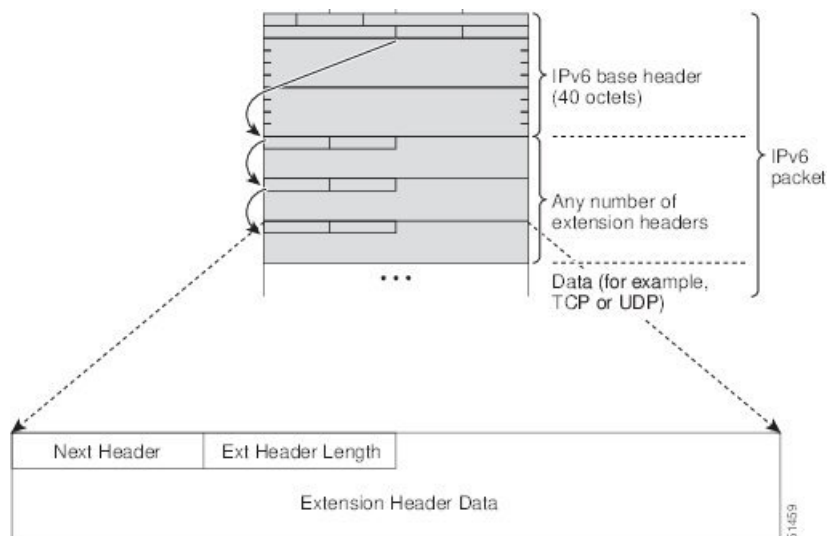
図 11: IPv6 パケット ヘッダー形式



IPv6 拡張ヘッダー

任意に使用できる拡張ヘッダーおよびパケットのデータ部分は、基本 IPv6 パケット ヘッダーの 8 つのフィールドのあとに続きます。存在する場合は、各拡張ヘッダーが 64 ビットに揃えられます。IPv6 パケットの拡張ヘッダーの数は固定されていません。各拡張ヘッダーは、前のヘッダーの次ヘッダー フィールドによって識別されます。通常は、最後の拡張ヘッダーに、TCP や UDP などのトランスポートレイヤプロトコルの次ヘッダー フィールドがあります。次の図は、IPv6 拡張ヘッダーの形式を示しています。

図 12: IPv6 拡張ヘッダー形式



次の表に、拡張ヘッダー タイプとその次ヘッダー フィールド値をリストします。

表 6: IPv6 拡張ヘッダー タイプ

ヘッダー タイプ	次ヘッダー の値	説明
ホップバイホップ オプション ヘッダー	0	パケットのパス上のすべてのホップで処理されるヘッダー。存在する場合、ホップバイホップオプションヘッダーは、常に基本 IPv6 パケット ヘッダーの直後に続きます。
宛先オプション ヘッダー	60	任意のホップバイホップオプションヘッダーのあとに続くことのあるヘッダー。このヘッダーは、最終の宛先、およびルーティングヘッダーで指定された各通過アドレスで処理されます。または、接続先オプションヘッダーを任意のカプセル化セキュリティペイロード (ESP) ヘッダーの後に続けることができます。接続先オプションヘッダーは、最終接続先でのみ処理されます。
ルーティング ヘッダー	43	送信元ルーティングに使用されるヘッダー。
フラグメント ヘッダー	44	送信元が、送信元と宛先の間のパスの最大伝送単位 (MTU) より大きいパケットをフラグメント化するとき使用されるヘッダー。フラグメントヘッダーは、フラグメント化された各パケットで使用されます。
上位層ヘッダー	6 (TCP) 17 (UDP)	データ転送のためにパケット内で使用されるヘッダー。2つの主要なトランスポート プロトコルは TCP と UDP です。



(注) 一部のスイッチモデルは、IPv6 拡張ヘッダー タイプのサブセットのみをサポートします。次のリストに、Cisco Nexus 3600 プラットフォームスイッチ (N3K-C36180YC-R および N3K-C3636C-R)、および N9K-X9636Q-R、N9K-X9636C-RX、および N9K-X96136YC-R ラインカードを搭載した Cisco Nexus 9504 および 9508 モジュラ シャーシでサポートされる拡張ヘッダー タイプを示します。。

サポート対象：宛先オプション (60)、ルーティング (43)、フラグメント (44)、モビリティ (135)、ホストアイデンティティ プロトコル (HIP) (139)、シム 6 (140)。

サポート対象外：ホップバイホップ オプション (0)、カプセル化セキュリティ ペイロード (50)、認証ヘッダー (51)、および試験的ヘッダー (253 および 254)。

Cisco NX-OS リリース 9.3(7) 以降では、ここにリストされているデバイスで IPv6 ACL を設定する場合、拡張ヘッダーを含む IPv6 パケットの処理に関する新しいルールを含める必要があります。必要な設定手順については、NX-OS リリース 9.3(x) 以降の『Cisco Nexus 3600 NX-OS Security Configuration Guide』の「Configuring an ACL for IPv6 Extension Headers」を参照してください。

IPv6 の DNS

IPv6 では、DNS の名前からアドレスおよびアドレスから名前のルックアッププロセスでサポートされる DNS レコードタイプがサポートされます。DNS レコードタイプは IPv6 アドレスをサポートしています（次の表を参照）。



（注） IPv6 では、IPv6 アドレスから DNS 名への逆マッピングもサポートされます。

表 7: IPv6 DNS レコードタイプ

レコードタイプ	説明	フォーマット (Format)
AAAA	ホスト名を IPv6 アドレスにマッピングします (IPv4 の A レコードと同等)。	www.abc.test AAAA 3FFE:YYYY:C18:1::2
PTR	IPv6 アドレスをホスト名にマッピングします (IPv4 の PTR レコードと同等)。	2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0.y.y.y.e.f.f.3.ip6.int PTR www.abc.test

IPv6 のパス MTU ディスカバリ

IPv4 の場合と同様に、ホストがダイナミックに、データパス上のすべてのリンクの MTU サイズの差を検出し、それに合わせて調整できるよう、IPv6 でパス MTU ディスカバリを使用できます。ただし、IPv6 では、特定のデータパス上の 1 つのリンクのパス MTU がパケットのサイズに十分に対応できる大きさでない場合に、フラグメンテーションはパケットの送信元によって処理されます。IPv6 ホストでパケットフラグメンテーションを処理すると、IPv6 ルータの処理リソースが節約され、IPv6 ネットワークの効率が向上します。ICMP の Too Big メッセージの到着によってパス MTU が削減されると、Cisco NX-OS はその低い値を保持します。この接続では、スループットを測定するためにセグメントサイズが増加することはありません。



（注） IPv6 では、最小リンク MTU は 1280 オクテットです。IPv6 リンクには、1500 オクテットの MTU 値の使用を推奨します。

CDP IPv6 アドレスのサポート

ネイバー情報機能用の Cisco Discovery Protocol (CDP) IPv6 アドレスのサポートを使用して、2 台のシスコ デバイス間で IPv6 アドレス指定情報を転送できます。IPv6 アドレス向け Cisco Discovery Protocol サポートは、ネットワーク管理製品およびトラブルシューティングツールに IPv6 情報を提供します。

IPv6 の ICMP

IPv6 の ICMP を使用して、ネットワークのヘルスの情報について説明します。IPv6 で動作する ICMPv6 は、パケットを正しく処理できない場合にエラーを報告し、ネットワークのステータスに関する情報メッセージを送信します。たとえば、パケットが大きすぎて別のネットワークに送信できないためにルータがパケットを転送できない場合、ルータは発信元ホストに ICMPv6 メッセージを送信します。さらに、IPv6 の ICMP パケットは IPv6 ネイバー探索およびパス MTU ディスカバリに使用されます。パス MTU ディスカバリ プロセスでは、特定のルートでサポートされる最大サイズを使用してパケットが送信されます。

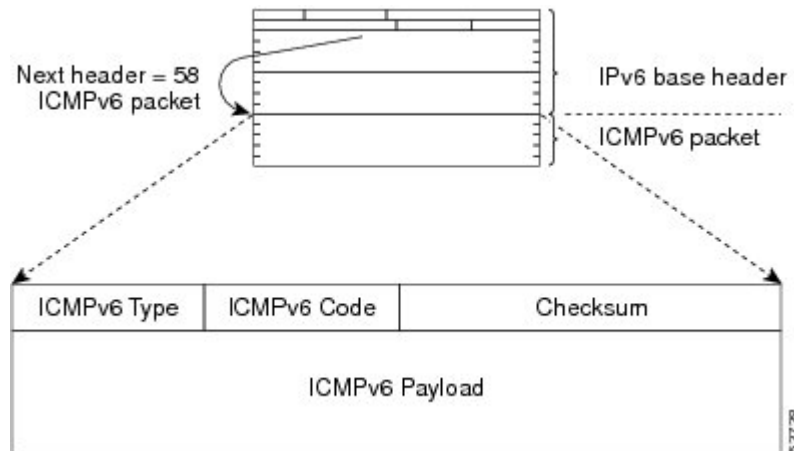
基本 IPv6 パケット ヘッダーの次ヘッダー フィールドの値が 58 の場合は、IPv6 ICMP パケットであることを意味します。ICMP パケットは、すべての拡張ヘッダーの後に続き、IPv6 パケットの最後の情報です。IPv6 ICMP パケット内の [ICMPv6 タイプ (ICMPv6 Type)] フィールドと [ICMPv6 コード (ICMPv6 Code)] フィールドは、ICMP メッセージタイプなどの IPv6 ICMP パケットの詳細を識別します。[チェックサム (Checksum)] フィールドの値は、送信側で計算され、IPv6 ICMP パケットと IPv6 疑似ヘッダーのフィールドから受信者によって確認されます。



- (注) IPv6 ヘッダーにはチェックサムがありません。ただし、トランスポート層上のチェックサムにより、パケットが正しく配信されていないかどうかを判定できます。計算に IP アドレスを含むすべてのチェックサム計算は、新しい 128 ビット アドレスに対応するように IPv6 用に変更する必要があります。チェックサムは、疑似ヘッダーを使用して生成されます。

ICMPv6 ペイロード フィールドには、IP パケット処理に関連するエラー情報または診断情報が含まれます。次の図は、IPv6 ICMP パケット ヘッダーの形式を示しています。

図 13: IPv6 ICMP パケット ヘッダーの形式



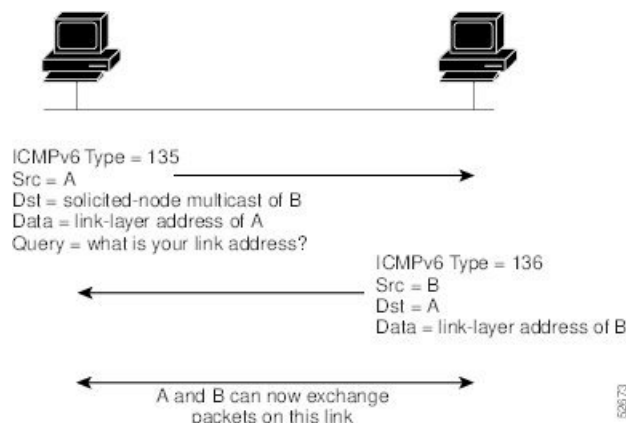
IPv6 ネイバー探索

IPv6 ネイバー探索プロトコル (NDP) を使用して、ネイバー ルータが到達可能かどうかを判断できます。IPv6 ノードは、ネイバー探索を使用して、同じネットワーク (ローカルリンク) 上のノードのアドレスを決定し、パケットを転送できるネイバー ルータを見つけ、ネイバー ルータが到達可能かどうかを確認し、リンク層アドレスの変更を検出します。NDP は、ICMP メッセージを使用して、到達不能な隣接ルータにパケットが送信されたかどうかを検出します。

IPv6 ネイバー送信要求メッセージ

ノードは、同じローカルリンク上の別のノードのリンク層アドレスを決定するときに、ICMP パケット ヘッダーのタイプ フィールドの値が 135 であるネイバー送信要求メッセージをローカルリンクで送信します (次の図を参照)。送信元アドレスは、ネイバー送信要求メッセージを送信するノードの IPv6 アドレスです。宛先アドレスは、宛先ノードの IPv6 アドレスに対応する送信要求ノードマルチキャスト アドレスです。ネイバー送信要求メッセージには、送信元ノードのリンク層アドレスも含まれます。

図 14: IPv6 ネイバー探索 - ネイバー送信要求メッセージ



ネイバー送信要求メッセージを受信した後に、宛先ノードは、ICMP パケットヘッダーのタイプフィールドに値 136 を含むネイバー アドバタイズメントメッセージをローカルリンクに送信することで応答します。送信元アドレスは、ネイバー アドバタイズメントメッセージを送信するノードの IPv6 アドレス（ノードインターフェイスの IPv6 アドレス）です。宛先アドレスは、ネイバー送信要求メッセージを送信するノードの IPv6 アドレスです。データ部分には、ネイバーアドバタイズメントメッセージを送信するノードのリンク層アドレスが含まれます。

送信元ノードがネイバーアドバタイズメントを受信すると、送信元ノードと宛先ノードが通信できるようになります。

ネイバー送信要求メッセージは、ノードがネイバーのリンク層アドレスを識別した後に、ネイバーの到達可能性を確認できます。ノードがあるネイバーの到達可能性を検証する場合、そのネイバーのユニキャストアドレスとして、ネイバー送信要求メッセージ内の宛先アドレスを使用します。

ネイバー アドバタイズメント メッセージは、ローカルリンク上のノードのリンク層アドレスが変更されたときにも送信されます。変更があった場合、ネイバーアドバタイズメントの宛先アドレスは全ノードマルチキャストアドレスになります。

ネイバー到達不能検出では、ネイバーの障害またはネイバーへの転送パスの障害が識別されます。この検出は、ホストとネイバーノード（ホストまたはルータ）間のすべてのパスで使用されます。ネイバー到達不能検出は、ユニキャストパケットだけが送信されるネイバーに対して実行され、マルチキャストパケットが送信されるネイバーに対しては実行されません。

ネイバーは、（以前にネイバーに送信されたパケットが受信され、処理されたことを示す）肯定確認応答がネイバーから返された場合に、到達可能と見なされます。肯定確認応答（TCP などの上位層プロトコルからの）は、接続が順調に進んでいる（接続先に到達しつつある）ことを示します。パケットがピアに到達している場合、それらのパケットは送信元のネクストホップネイバーにも到達しています。転送の進行により、ネクストホップネイバーが到達可能であることも確認されます。

ローカルリンク上にない宛先の場合、転送の進行は、ファーストホップルータが到達可能であることを暗に意味します。上位層プロトコルからの確認応答がない場合、ノードは、ユニキャストネイバー送信要求メッセージを使用してネイバーを探し、転送パスがまだ機能していることを確認します。ネイバーから返信された請求ネイバー アドバタイズメント メッセージ

は、転送パスがまだ機能しているという肯定確認応答です（請求フラグが値1に設定されたネイバー アドバタイズメント メッセージは、ネイバー請求メッセージへの返信としてだけ送信されます）。非送信要求メッセージでは、送信元ノードから宛先ノードへの一方向パスだけが確認されます。送信要求ネイバー アドバタイズメント メッセージは、両方向のパスが機能していることを示します。



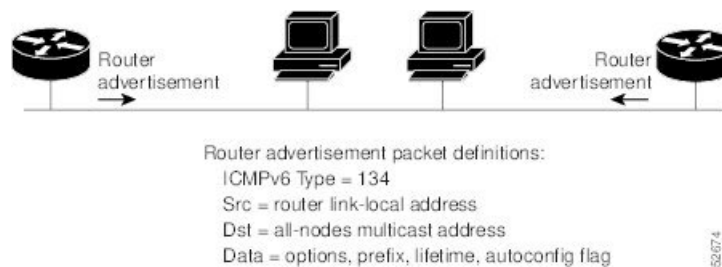
(注) 送信要求フラグが値0に設定されたネイバー アドバタイズメント メッセージは、転送パスがまだ機能していることを示す肯定確認応答とは見なされません。

ルータ アドバタイズメント メッセージ

ルータ アドバタイズメント (RA) メッセージは、ICMP パケット ヘッダーのタイプ フィールドが値 134 であり、IPv6 ルータの構成済みの各インターフェイスへ定期的に送信されます。

RA メッセージは、全ノード マルチキャスト アドレスに送信されます（以下の図を参照）。

図 15: IPv6 ネイバー検出 : RA メッセージ



RA メッセージには、通常次の情報が含まれています。

- ローカル リンク上のノードがその IPv6 アドレスの自動設定に使用できる 1 つ以上のオンライン IPv6 プレフィックス
- アドバタイズメントに含まれる各プレフィックスのライフタイム情報
- デフォルト ルータ情報（アドバタイズメントを送信しているルータをデフォルト ルータとして使用する必要があるかどうか、および、その場合は、ルータがデフォルトルータとして使用される秒単位の時間）
- ホストが発信するパケットで使用する必要のあるホップリミットやMTUなど、ホストに関する詳細情報

RA は、ルータ送信要求メッセージへの応答としても送信されます。ICMP パケット ヘッダーのタイプフィールドの値が 133 であるルータ送信要求メッセージは、システム始動時にホストによって送信されるため、ホストは次のスケジュールされた RA メッセージを待機することなくすぐに自動設定できます。通常、送信元アドレスは未指定の IPv6 アドレス (0:0:0:0:0:0:0:0) です。ホストに設定済みのユニキャストアドレスがある場合、ルータ送信要求メッセージを送信するインターフェイスのユニキャストアドレスが、メッセージ内の送信元アドレスとして使用されます。宛先アドレスは、リンク範囲の全ルータ マルチキャストアドレス。ルータ送信

要求に応答して RA が送信される場合、RA メッセージ内の宛先アドレスはルータ送信要求メッセージの送信元のユニキャストアドレスです。

次の RA メッセージ パラメータを構成できます。

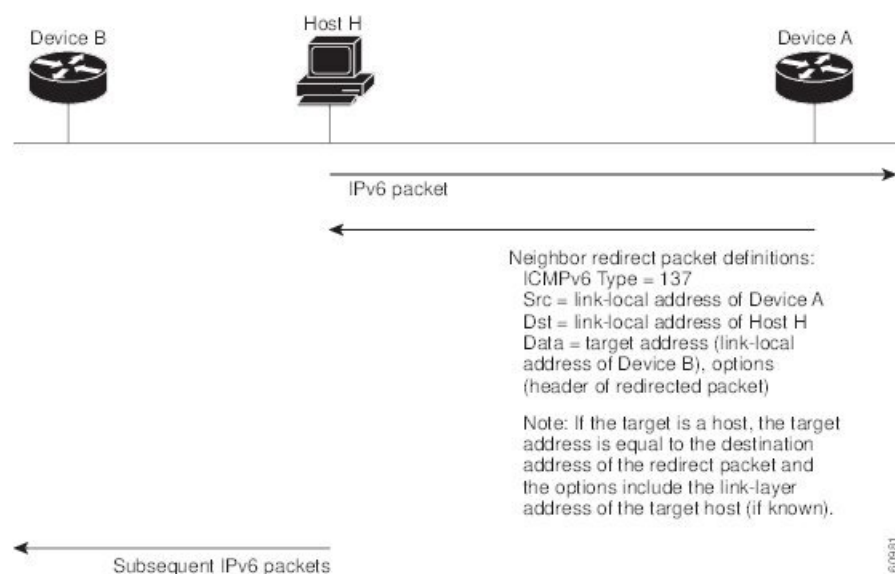
- RA メッセージの定期的な時間間隔
- (特定のリンク上のすべてのノードで使用される) デフォルトルータとしてのルータの実用性を示す「ルータ ライフタイム」値
- 特定のリンクで使用されているネットワーク プレフィックス
- (特定のリンクで) ネイバー送信要求メッセージが再送信される時間の間隔
- ノードによってネイバーが到達可能である (特定のリンク上のすべてのノードで使用できる) と見なされるまでの時間

設定されたパラメータはインターフェイスに固有です。RA メッセージ (デフォルト値を含む) の送信は、イーサネットとインターフェイス上では自動的にイネーブルになります。他のインターフェイスタイプの場合は、**no ipv6 nd suppress-ra** コマンドを入力して RA メッセージを送信する必要があります。個々のインターフェイスでは、**ipv6 nd suppress-ra** コマンドを入力して、RA メッセージ機能を無効にできます。

IPv6 ネイバー リダイレクト メッセージ

ルータは、ネイバー リダイレクト メッセージを送信して、接続先へのパス上のより適切なファーストホップノードをホストに通知します (次の図を参照)。ICMP パケットヘッダーのタイプフィールドの値 137 は、IPv6 ネイバー リダイレクト メッセージを示します。

図 16: IPv6 ネイバー探索 - ネイバー リダイレクトメッセージ





- (注) リダイレクト メッセージ内のターゲット アドレス（最終的な宛先）によって隣接ルータのリンクローカル アドレスが確実に識別されるように、ルータは各隣接ルータのリンクローカル アドレスを判断する必要があります。静的ルーティングの場合は、ルータのリンクローカル アドレスを使用してネクストホップ ルータのアドレスを指定する必要があります。動的ルーティングの場合、隣接ルータのリンクローカルアドレスを交換するように、すべての IPv6 ルーティング プロトコルを構成する必要があります。

パケットの転送後に、次の条件が満たされる場合、ルータはパケットの送信元にリダイレクト メッセージを送信します。

- パケットの宛先アドレスがマルチキャスト アドレスではない。
- パケットがルータにアドレッシングされていなかった。
- パケットが、そのパケットを受信したインターフェイスから送信されようとしている。
- ルータが、パケットにより適したファーストホップ ノードはパケットの送信元と同じリンク上にあると判断した。
- パケットの送信元アドレスが、同じリンク上のネイバーのグローバル IPv6 アドレス、またはリンクローカル アドレスである。

仮想化のサポート

IPv6 は、仮想ルーティング/転送（VRF）インスタンスをサポートします。

ECMP を使用した IPv6 ルート

ルートのすべてのネクストホップが収集、ドロップ、またはパントの場合、すべてのネクストホップはマルチパス ハードウェア テーブルにそのままプログラムされます。

ルートの一部のネクストホップがグリーンニング、ドロップ、またはパントであり、残りのネクストホップがそうでない場合、非グリーンニング、ドロップ、またはパントのネクストホップのみがマルチパス ハードウェア テーブルにプログラムされます。

ECMP ルートの特定のネクストホップが解決されると（ARP/IPV6ND が解決されると）、それに応じてマルチパス ハードウェア テーブルが更新されます。

IPv6の前提条件

IPv6 には、次の前提条件があります。

- IPv6 アドレッシング、IPv6 ヘッダー情報、ICMPv6、IPv6 Neighbor Discovery（ND）プロトコルなど、IPv6 の基本を理解する必要があります。

- デバイスをデュアルスタック デバイス (IPv4/IPv6) にする場合は、必ずメモリ/処理の注意事項に従ってください。

IPv6 の注意事項および制約事項

IPv6 設定時の注意事項および制約事項は、次のとおりです。

- スイッチは、IPv6 フレームを転送する前にレイヤ 3 パケット情報を確認しないため、IPv6 パケットは、レイヤ 2 LAN スイッチに対して透過的です。IPv6 ホストは、レイヤ 2 LAN スイッチに直接接続できます。
- インターフェイスの同じプレフィックス内に複数の IPv6 グローバル アドレスを設定できます。ただし、1 つのインターフェイス上での複数の IPv6 リンクローカル アドレスはサポートされません。
- RFC 3879 によりサイトローカルアドレスの使用が廃止されたため、RFC 4193 のユニークローカルアドレス (UCA) の推奨に従って、プライベート IPv6 アドレスを設定する必要があります。
- Cisco Nexus 3600-R プラットフォーム スイッチの場合、インターネット ピアリング モードは、グローバルインターネット ルーティング テーブルで配信されるプレフィックス パターンでのみ使用されます。このモードでは、他のプレフィックス配布またはパターンは動作できますが、予測できません。その結果、プレフィックスパターンが実際のインターネット プレフィックス パターンである場合にのみ、達成可能な最大 LPM/LEM スケールが信頼できます。インターネット ピアリング モードでは、グローバルインターネット ルーティング テーブル内のルートプレフィックス パターン以外のルートプレフィックス パターンが使用されている場合、スイッチは文書化されたスケーラビリティの数値を正常に達成できない可能性があります。

デフォルト設定

次の表に、IPv6 パラメータのデフォルト設定を示します。

表 8: デフォルト IPv6 パラメータ

パラメータ	デフォルト
ND reachable time	0 ミリ秒
ネイバー要求再送信間隔	1000 ミリ秒

IPv6 の設定

IPv6 アドレッシングの設定

インターフェイスの IPv6 アドレスを設定して、インターフェイスが IPv6 トラフィックを転送できるようにします。インターフェイスでグローバル IPv6 アドレスを設定すると、リンクローカルアドレスが自動的に設定され、そのインターフェイスで IPv6 が有効となります。

手順の概要

1. **configure terminal**
2. **interface ethernet number**
- 3.
4. (任意) **show ipv6 interface**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション		目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>		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 ethernet number 例 : <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>		インターフェイス設定モードを開始します。
ステップ 3	オプション	説明	
	コマンド	目的	
	ipv6 address { addr [eui64] [route-preference preference] [secondary] tag tag-id }	インターフェイスに割り当てられている IPv6 アドレスを指定し、そのインターフェイスで IPv6 処理をイネーブルにします。 ipv6 address コマンドを入力すると、IPv6 アドレスの下位 64 ビットにインターフェイス ID を含む	

コマンドまたはアクション		目的
	オプション	説明
		グローバル IPv6 アドレスが設定されます。指定する必要があるのはアドレスの 64 ビットネットワーク プレフィックスだけです。最後の 64 ビットはインターフェイス ID から自動的に計算されます。
	ipv6 address use-link-local-only	ipv6 address use-link-local-only コマンドを入力すると、インターフェイスのリンクローカルアドレスが設定されます。このアドレスは、IPv6 がインターフェイスでイネーブルになっているときに自動的に設定されるリンクローカルアドレスの代わりに使用されます。 このコマンドは、IPv6 アドレスを設定せずに、インターフェイス上で IPv6 処理をイネーブルにします。
例 : <pre>switch(config-if)# ipv6 address 2001:0DB8::1/10</pre> または <pre>switch(config-if)# ipv6 address use-link-local-only</pre>		
ステップ 4	(任意) show ipv6 interface	IPv6 用に設定されたインターフェイスを表示します。
例 : <pre>switch(config-if)# show ipv6 interface</pre>		
ステップ 5	(任意) copy running-config startup-config	この設定変更を保存します。
例 : <pre>switch(config-if)# copy running-config startup-config</pre>		

例

次に、IPv6 アドレスを設定する例を示します。


```

switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# ipv6 address ?
A:B::C:D/LEN IPv6 prefix format: xxxx:xxxx/ml, xxxx:xxxx::/ml,
xxxx::xx/128
use-link-local-only Enable IPv6 on interface using only a single link-local
address
switch(config-if)# ipv6 address 2001:db8::/64 eui64

```

次に、IPv6 インターフェイスを表示する例を示します。

```

switch(config-if)# show ipv6 interface ethernet 3/1
Ethernet3/1, Interface status: protocol-down/link-down/admin-down, iod: 36
IPv6 address: 0dc3:0dc3:0000:0000:0218:baff:fed8:239d
IPv6 subnet: 0dc3:0dc3:0000:0000:0000:0000:0000/64
IPv6 link-local address: fe80::0218:baff:fed8:239d (default)
IPv6 multicast routing: disabled
IPv6 multicast groups locally joined:
ff02::0001:ffd8:239d ff02::0002 ff02::0001 ff02::0001:ffd8:239d
IPv6 multicast (S,G) entries joined: none
IPv6 MTU: 1500 (using link MTU)
IPv6 RP inbound packet-filtering policy: none
IPv6 RP outbound packet-filtering policy: none
IPv6 inbound packet-filtering policy: none
IPv6 outbound packet-filtering policy: none
IPv6 interface statistics last reset: never
IPv6 interface RP-traffic statistics: (forwarded/originated/consumed)
Unicast packets: 0/0/0
Unicast bytes: 0/0/0
Multicast packets: 0/0/0
Multicast bytes: 0/0/0

```

LPM インターネット ピアリング ルーティング モードの設定

Cisco NX-OS リリース9.3(1) 以降では、IPv4 および IPv6 LPM インターネット ルート エントリをサポートするために LPM インターネット ピアリング ルーティング モードを設定できます。このモードは、IPv4 プレフィックス (/32 までのプレフィックス長) および IPv6 プレフィックス (/83 までのプレフィックス長) のダイナミック トライ (ツリー ビット ルックアップ) をサポートします。このルーティング モードをサポートするのは、Cisco Nexus 3600-R プラットフォーム スイッチです。



(注) この設定は、IPv4 および IPv6 両方のアドレス ファミリに影響を及ぼします。



(注) LPM インターネット ピアリング ルーティング モードのスケール数については、『[Cisco Nexus 3600 Series NX-OS Verified Scalability Guide](#)』を参照してください。LPM インターネット ピアリング モードの Cisco Nexus 3600-R プラットフォーム スイッチは、インターネット ピアリング プレフィックスを使用する場合にのみ、予測どおりにスケールアウトします。Cisco Nexus 3600-R プラットフォーム スイッチが他のプレフィックス パターンを使用している場合は、文書化されたスケーラビリティの数値を達成できない可能性があります。

手順の概要

1. **configure terminal**
2. **[no] system routing template-internet-peering**
3. (任意) **show system routing mode**
4. **copy running-config startup-config**
5. **reload**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] system routing template-internet-peering 例 : switch(config)# system routing template-internet-peering	デバイスを LPM インターネット ピア ルーティング モードにして、IPv4 および IPv6 LPM インターネッ ト ルート エントリをサポートします。
ステップ 3	(任意) show system routing mode 例 : switch(config)# show system routing mode Configured System Routing Mode: Internet Peering Applied System Routing Mode: Internet Peering	LPM ルーティング モードを表示します。
ステップ 4	copy running-config startup-config 例 : switch(config)# copy running-config startup-config	この設定変更を保存します。
ステップ 5	reload 例 : switch(config)# reload	デバイス全体をリブートします。

LPM インターネット ピアリング ルーティング モードの追加設定

大規模ルーティング環境で LPM インターネット ピアリング ルーティング モードで Cisco Nexus スイッチを導入する場合、またはネクストホップ数が増加するルートの場合は、VDC リソース テンプレートで IPv4 のメモリ制限を増やす必要があります。

手順の概要

1. **configure terminal**

2. (任意) **show routing ipv4 memory estimate routes routes next-hops hops**
3. **vdc switch id id**
4. **limit-resource u4route-mem minimum min-limit maximum max-limit**
5. **exit**
6. **copy running-config startup-config**
7. **reload**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	(任意) show routing ipv4 memory estimate routes routes next-hops hops 例 : <pre>switch(config)# show routing ipv4 memory estimate routes 262144 next-hops 32 Shared memory estimates: Current max 512 MB; 78438 routes with 64 nhs in-use 2 MB; 2642 routes with 1 nhs (average) Configured max 512 MB; 78438 routes with 64 nhs Estimate memory with fixed overhead: 1007 MB; 262144 routes with 32 nhs Estimate with variable overhead included: - With MVPN enabled VRF: 1136 MB - With OSPF route (PE-CE protocol): 1375 MB - With EIGRP route (PE-CE protocol): 1651 M</pre>	共有メモリの見積もりを表示して、ルートメモリの要件を判断します。
ステップ 3	vdc switch id id 例 : <pre>switch(config)# vdc switch id 1 switch(config-vdc)#</pre>	VDC スイッチ ID を指定します。
ステップ 4	limit-resource u4route-mem minimum min-limit maximum max-limit 例 : <pre>switch(config-vdc)# limit-resource u4route-mem minimum 1024 maximum 1024</pre>	IPv4 メモリの制限をメガバイト単位で指定します。
ステップ 5	exit 例 : <pre>switch(config-vdc)# exit switch(config)#</pre>	VDC 設定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 6	copy running-config startup-config 例 : switch(config)# copy running-config startup-config	この設定変更を保存します。
ステップ 7	reload 例 : switch(config)# reload	デバイス全体をリブートします。

IPv6 ネイバー探索の構成

ルータで IPv6 ネイバー探索を構成できます。NDP は、IPv6 ノードとルータを有効にして、同じリンク上のネイバーのリンク層アドレスを特定し、隣接ルータを見つけ、ネイバーの動向を把握します。

始める前に

最初にインターフェイスで IPv6 を有効にする必要があります。

手順の概要

1. **configure terminal**
2. **interface ethernet number**
3. **ipv6 nd [hop-limit hop-limit | managed-config-flag | mtu mtu | ns-interval interval | other-config-flag | prefix | ra-interval interval | ra-lifetime lifetime | reachable-time time | redirects | retrans-timer time | suppress-ra]**
4. (任意) **show ipv6 nd interface**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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 ethernet number 例 : switch(config)# interface ethernet 2/31 switch(config-if)#	インターフェイス設定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	ipv6 nd [hop-limit <i>hop-limit</i> managed-config-flag mtu <i>mtu</i> ns-interval <i>interval</i> other-config-flag prefix ra-interval <i>interval</i> ra-lifetime <i>lifetime</i> reachable-time <i>time</i> redirects retrans-timer <i>time</i> suppress-ra] 例 : <pre>switch(config-if)# ipv6 nd prefix</pre>	IPv6 アドレスを設定する場合は、ネイバー探索が自動的に有効になります。このコマンドにより、インターフェイスで次の追加の IPv6 ネイバー探索オプションが有効になります。 • hop-limit <i>hop-limit</i> : IPv6 ネイバー検出パケットでホップリミットをアドバタイズします。値の範囲は 0 ～ 255 です。 • managed-config-flag : ステートフルアドレス自動構成を使用してアドレス情報を取得するために、ICMPv6 ルータ アドバタイズメント メッセージ内でアドバタイズします。 • mtu <i>mtu</i> : このリンク上で ICMPv6 ルータ アドバタイズメント メッセージで最大伝送単位 (MTU) をアドバタイズします。範囲は 1280 ～ 65535 バイトです。 • ns-interval <i>interval</i> : IPv6 ネイバー送信要求メッセージ間の再送信間隔を構成します。範囲は 1000 ～ 3600000 ミリ秒です。 • other-config-flag : ICMPv6 ルータ アドバタイズメント メッセージで、ホストがアドレス以外の関連情報を取得するためにステートフル自動構成を使用することを示します。 • prefix : ルータ アドバタイズメント メッセージで IPv6 プレフィックスをアドバタイズします。 • ra-interval <i>interval</i> : ICMPv6 ルータ アドバタイズメント メッセージの送信間の間隔を構成します。範囲は 4 ～ 1800 秒です。 • ra-lifetime <i>lifetime</i> : ICMPv6 ルータ アドバタイズメント メッセージで、デフォルト ルータのライフタイムをアドバタイズします。範囲は 0 ～ 9000 秒です。 • reachable-time <i>time</i> : ICMPv6 ルータ アドバタイズメント メッセージで、ノードが到達可能性確認を受信したあとにネイバーをアップしていると思なした時間をアドバタイズします。範囲は 0 ～ 9000 秒です。 • redirects : ICMPv6 リダイレクト メッセージの送信を有効化します。

	コマンドまたはアクション	目的
		• retrans-timer time : ICMPv6 ルータ アドバタイズメントメッセージで、ネイバー送信要求メッセージ間の時間をアドバタイズします。範囲は 0 ～ 9000 秒です。 • suppress-ra : ICMPv6 ルータ アドバタイズメントメッセージの送信を無効にします。
ステップ 4	(任意) show ipv6 nd interface 例 : <pre>switch(config-if)# show ipv6 nd interface</pre>	IPv6 ネイバー検出に構成されたインターフェイスを表示します。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、IPv6 ネイバー探索到達可能時間を構成する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# ipv6 nd reachable-time 10
```

次に、IPv6 ネイバー探索インターフェイスを表示する例を示します。

```
switch(config-if)# show ipv6 nd interface ethernet 3/1
ICMPv6 ND Interfaces for VRF "default"
Ethernet3/1, Interface status: protocol-down/link-down/admin-down
IPv6 address: 0dc3:0dc3:0000:0000:0218:baff:fed8:239d
ICMPv6 active timers:
Last Neighbor-Solicitation sent: never
Last Neighbor-Advertisement sent: never
Last Router-Advertisement sent:never
Next Router-Advertisement sent in: 0.000000
Router-Advertisement parameters:
Periodic interval: 200 to 600 seconds
Send "Managed Address Configuration" flag: false
Send "Other Stateful Configuration" flag: false
Send "Current Hop Limit" field: 64
Send "MTU" option value: 1500
Send "Router Lifetime" field: 1800 secs
Send "Reachable Time" field: 10 ms
Send "Retrans Timer" field: 0 ms
Neighbor-Solicitation parameters:
NS retransmit interval: 1000 ms
ICMPv6 error message parameters:
Send redirects: false
Send unreachable: false
```

オプションの IPv6 ネイバー探索

次のオプションの IPv6 ネイバー探索コマンドを使用できます。

コマンド	目的
ipv6 nd hop-limit	ルータアドバタイズメントおよびルータから発信されるすべての IPv6 パケットで使用されるホップの最大数を構成します。
ipv6 nd managed-config-flag	「managed address configuration flag」フラグは、IPv6 ルータ アドバタイズメントで設定されません。
ipv6 nd mtu	各インターフェイスにおいて送信される IPv6 パケットの最大伝送単位 (MTU) サイズを設定します。
ipv6 nd ns-interval	インターフェイスで IPv6 ネイバー再送信要求メッセージが送信される時間間隔を設定します。
ipv6 nd other-config-flag	IPv6 ルータ アドバタイズメントに「other stateful configuration」フラグを構成します。
ipv6 nd ra-interval	インターフェイスで IPv6 ルータ アドバタイズメント (RA) メッセージが送信される時間間隔を構成します。
ipv6 nd ra-lifetime	インターフェイス上の IPv6 ルータ アドバタイズメントに含まれるルータのライフタイム値を構成します。
ipv6 nd reachable-time	到達可能性確認イベントがいくつか発生した後、リモート IPv6 ノードが到達可能と見なされる時間を構成します。
ipv6 nd redirects	ICMPv6 リダイレクト メッセージの送信を有効にします。
ipv6 nd retrans-timer	ルータアドバタイズメントのネイバー送信要求メッセージ間のアドバタイズ時間を構成します。
ipv6 nd suppress-ra	LAN インターフェイス上で IPv6 ルータ アドバタイズメントの送信を抑制します。

IPv6 パケット検証の構成

Cisco NX-OS は、IPv6 パケットの検証をチェックする侵入検知システム (IDS) をサポートしています。これらの IDS チェックは有効または無効にできます。



(注) Cisco Nexus 3600 プラットフォーム スイッチは、送信元 IP アドレスが 0.0.0.0 のパケットを除外しません。

IDS チェックを有効にするには、グローバル構成モードで次のコマンドを使用します。

コマンド	目的
hardware ip verify address { destination zero identical reserved source multicast }	IPv6 アドレスに対して次の IDS チェックを実行します。 • destination zero : 宛先 IP アドレスが :: である場合は IPv6 パケットをドロップします。 • identical : 送信元 IPv6 アドレスが宛先 IPv6 アドレスと同じである場合は IPv6 パケットをドロップします。 • reserved : IPv6 アドレスが ::1 である場合は、IPv6 パケットをドロップします。 • source multicast : 送信元 IPv6 アドレスが FF00::/8 の範囲内（マルチキャスト）である場合は IPv6 パケットをドロップします。
hardware ipv6 verify length { consistent maximum { max-frag max-tcp udp } }	IPv6 アドレスに対して次の IDS チェックを実行します。 • consistent : イーサネットフレームサイズが、IPv6 パケット長にイーサネットヘッダーを加えた値以上の場合には、IPv6 パケットをドロップします。 • maximum max-frag : 計算式（IPv6 ペイロード長 - IPv6 拡張ヘッダーバイト数） + （フラグメントオフセット * 8）の値が 65536 より大きい場合には、IPv6 パケットをドロップします。 • maximum max-tcp : TCP 長が IP ペイロード長より長い場合は、IP パケットをドロップします。 • maximum udp : IPv6 ペイロード長が UDP パケット長を下回る場合には、IPv6 パケットをドロップします。
hardware ipv6 verify tcp tiny-frag	IPv6 フラグメント オフセットが 1 の場合、または IPv6 フラグメント オフセットが 0 で IP ペイロード長が 16 未満の場合、TCP パケットをドロップします。
hardware ipv6 verify version	EtherType が 6（IPv6）に設定されていない場合、IPv6 パケットをドロップします。

IPv6 パケット検証の構成を表示するには、**show hardware forwarding ip verify** コマンドを使用します。

IPv6 設定の確認

IPv6 設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show hardware forwarding ip verify	IPv4 および IPv6 パケット検証の構成を表示します。
show ipv6 interface	IPv6-related インターフェイスの情報を表示します。
show ipv6 adjacency	隣接関係テーブルを表示します。
show ipv6 icmp	ICMPv6 情報を表示します。
show ipv6 nd	IPv6 ネイバー探索インターフェイス情報を表示します。
show ipv6 neighbor	IPv6 ネイバー エントリを表示します。

IPv6 の設定例

次に、IPv6 を構成する例を示します。

```
configure terminal
interface ethernet 3/1
ipv6 address 2001:db8::/64 eui64
ipv6 nd reachable-time 10
```




第 5 章

OSPFv2 の設定

この章では、Cisco NX-OS スイッチで IPv4 ネットワーク用の Open Shortest Path First version 2 (OSPFv2) を設定する方法について説明します。

この章は、次の項で構成されています。

- [OSPFv2 について \(75 ページ\)](#)
- [OSPFv2 の前提条件 \(87 ページ\)](#)
- [注意事項と制約事項 \(87 ページ\)](#)
- [デフォルト設定 \(88 ページ\)](#)
- [基本的な OSPFv2 の設定 \(88 ページ\)](#)
- [高度な OSPFv2 の設定 \(100 ページ\)](#)
- [OSPFv2 設定の確認 \(122 ページ\)](#)
- [OSPFv2 統計情報の表示 \(123 ページ\)](#)
- [OSPFv2 の設定例 \(123 ページ\)](#)
- [その他の参考資料 \(123 ページ\)](#)

OSPFv2 について

OSPFv2 は、IPv4 ネットワーク用 IETF リンクステートプロトコルです（「[リンクステートプロトコル](#)」の項を参照）。OSPFv2 ルータは、hello パケットと呼ばれる特別なメッセージを各 OSPF 対応インターフェイスに送信して、ほかの OSPFv2 隣接ルータを探索します。ネイバールータが発見されると、この 2 台のルータは hello パケットの情報を比較して、両者の設定に互換性のあるかどうかを判定します。これらのネイバールータは隣接を確立しようとします。つまり、両者のリンクステートデータベースを同期させて、確実に同じ OSPFv2 ルーティング情報を持つようにします。隣接ルータは、各リンクの稼働状態に関する情報、リンクのコスト、およびその他のあらゆるネイバー情報を含むリンクステートアドバタイズメント (LSA) を共有します。これらのルータはその後、受信した LSA をすべての OSPF 対応インターフェイスにフラッディングします。これにより、すべての OSPFv2 ルータのリンクステートデータベースが最終的に同じになります。すべての OSPFv2 ルータのリンクステートデータベースが同じになると、ネットワークは収束します（「[コンバージェンス](#)」を参照）。その後、各ルータは、ダイクストラの最短パス優先 (SPF) アルゴリズムを使用して、自身のルートテーブルを構築します。

OSPFv2 ネットワークは、複数のエリアに分割できます。ルータは、ほとんどの LSA を 1 つのエリア内だけに送信するため、OSPF 対応ルータの CPU とメモリの要件が緩やかになります。

OSPFv2 は IPv4 をサポートしています。

Hello パケット

OSPFv2 ルータは、すべての OSPF 対応インターフェイスに hello パケットを定期的送信します。ルータがこの hello パケットを送信する頻度は、インターフェイスごとに設定された hello 間隔により決定されます。OSPFv2 は、hello パケットを使用して、次のタスクを実行します。

- ネイバー探索
- キープアライブ
- 指定ルータの選定（「[指定ルータ](#)」セクションを参照してください）

hello パケットには、リンクの OSPFv2 コスト割り当て、hello 間隔、送信元ルータのオプション機能など、送信元の OSPFv2 インターフェイスとルータに関する情報が含まれます。これらの hello パケットを受信する OSPFv2 インターフェイスは、設定に受信インターフェイスの設定との互換性があるかどうかを判定します。互換性のあるインターフェイスはネイバーと見なされ、ネイバー テーブルに追加されます（「[ネイバー](#)」の項を参照してください）。

hello パケットには、送信元インターフェイスが通信したルータのルータ ID のリストも含まれます。受信インターフェイスが、このリストで自身の ID を見つけた場合は、2 つのインターフェイス間で双方向通信が確立されます。

OSPFv2 は、hello パケットをキープアライブメッセージとして使用して、ネイバーが通信を継続中であるかどうかを判定します。ルータが設定されたデッド間隔（通常は hello 間隔の倍数）の間、hello パケットを受信しない場合、そのネイバーはローカル ネイバー テーブルから削除されます。

ネイバー情報

ネイバーであると思なされるようにするには、リモートインターフェイスと互換性があるように、OSPFv2 インターフェイスを設定しておく必要があります。この 2 つの OSPFv2 インターフェイスで、次の基準が一致している必要があります。

- hello 間隔
- デッド間隔
- エリア ID（「[エリア](#)」の項を参照）
- 認証
- オプション機能

一致する場合は、次の情報がネイバー テーブルに入力されます。

- ネイバー ID：ネイバーのルータ ID。

- プライオリティ：ネイバーのプライオリティ。プライオリティは、指定ルータの選定（「[指定ルータ](#)」を参照）に使用されます。
- 状態：ネイバーから通信があったか、双方向通信の確立処理中であるか、リンクステート情報を共有しているか、または完全な隣接関係が確立されたかを示します。
- デッドタイム：このネイバーから最後の hello パケットを受信した後に経過した時間を示します。
- IP アドレス：ネイバーの IP アドレス。
- 指定ルータ：ネイバーが指定ルータ、またはバックアップ指定ルータとして宣言されたかどうかを示します（[指定ルータ](#)を参照）。
- ローカルインターフェイス：このネイバーの hello パケットを受信したローカルインターフェイス。

隣接関係

すべてのネイバーが隣接関係を確立するわけではありません。ネットワークタイプと確立された指定ルータに応じて、完全な隣接関係を確立して、すべてのネイバーと LSA を共有するものと、そうでないものがあります。詳細については、「[指定されたルータ](#)」セクションを参照してください。

隣接関係は、OSPF のデータベース説明パケット、リンク状態要求パケット、およびリンク状態更新パケットを使用して確立されます。データベース説明パケットには、ネイバーのリンクステートデータベースからの LSA ヘッダーだけが含まれます（「[リンク状態データベース](#)」のセクションを参照）。ローカルルータは、これらのヘッダーを自身のリンクステートデータベースと比較して、新規の LSA か、更新された LSA かを判定します。ローカルルータは、新規または更新の情報を必要とする各 LSA について、リンク状態要求パケットを送信します。これに対し、ネイバーはリンク状態更新パケットを返信します。このパケット交換は、両方のルータのリンクステート情報が同じになるまで続きます。

指定ルータ

複数のルータを含むネットワークは、OSPF 特有の状況です。すべてのルータがネットワークで LSA をフラッドした場合、同じリンクステート情報が複数の送信元から送信されます。ネットワークのタイプによっては、OSPFv2 は指定ルータ（DR）という 1 台のルータを使用して LSA のフラッドを制御し、OSPFv2 の残りの部分に対してネットワークを代表する役割をさせる場合があります（[エリア](#)のセクションを参照）。DR がダウンした場合、OSPFv2 はバックアップ指定ルータ（BDR）を選択します。DR がダウンすると、OSPFv2 はこの BDR を使用します。

ネットワークタイプは次のとおりです。

- ポイントツーポイント：2 台のルータ間にのみ存在するネットワーク。ポイントツーポイント ネットワーク上の全ネイバーは隣接関係を確立し、DR は存在しません。

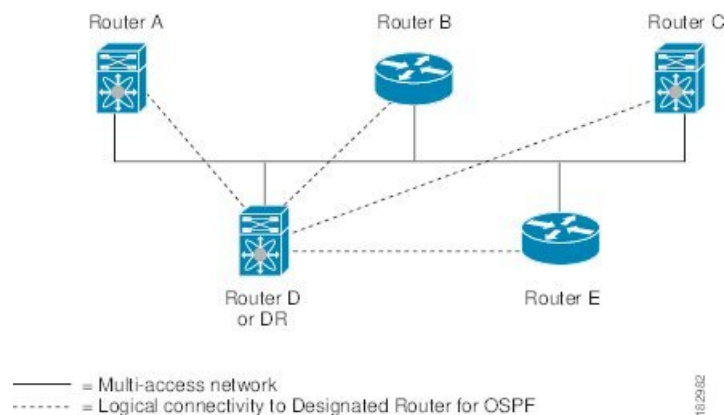
- **ブロードキャスト**：ブロードキャスト トラフィックが可能なイーサネットなどの共有メディア上で通信できる複数のルータを持つネットワーク。OSPFv2 ルータは DR および BDR を確立し、これらにより、ネットワーク上の LSA フラッドイングを制御します。OSPFv2 は、よく知られている IPv4 マルチキャスト アドレス 224.0.0.5 および MAC アドレス 0100.5300.0005 を使用して、ネイバーと通信します。

DR と BDR は、hello パケット内の情報に基づいて選択されます。インターフェイスは hello パケットの送信時に、どれが DR および BDR かわかっている場合は、優先フィールドと、DR および BDR フィールドを設定します。ルータは、hello パケットの DR および BDR フィールドで宣言されたルータと優先フィールドに基づいて、選定手順を実行します。最終的に OSPFv2 は、最も大きいルータ ID を DR および BDR として選択します。

他のルータはすべて DR および BDR と隣接関係を確立し、IPv4 マルチキャスト アドレス 224.0.0.6 を使用して、LSA 更新情報を DR と BDR に送信します。次の図は、すべてのルータと DR との隣接関係を示しています。

DR は、ルータ インターフェイスに基づいています。1 つのネットワークの DR であるルータは、別のインターフェイス上の他のネットワークの DR となることはできません。

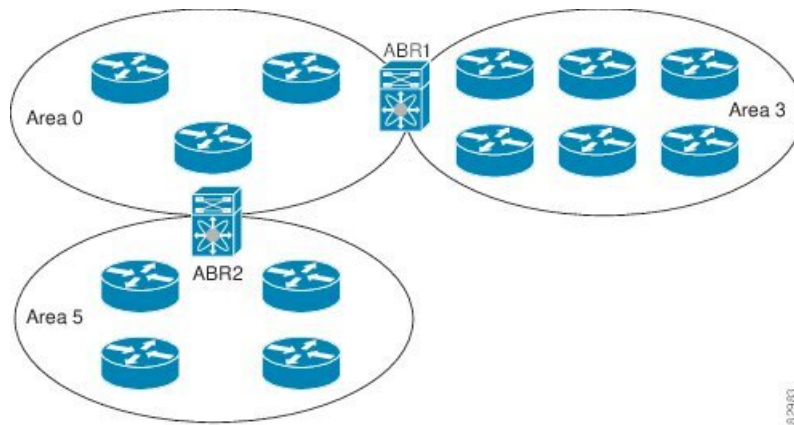
図 17: マルチアクセス ネットワークの DR



エリア

OSPFv2 ネットワークを複数のエリアに分割すると、ルータに要求される OSPFv2 の CPU とメモリに関する要件を制限できます。エリアとは、ルータの論理的な区分で、OSPFv2 ドメイン内にリンクして別のサブドメインを作成します。LSA フラッドイングはエリア内でのみ発生し、リンクステートデータベースはエリア内のリンクにのみ制限されます。定義されたエリア内のインターフェイスには、エリア ID を割り当てることができます。エリア ID は 32 ビット値で、数字またはドット付き 10 進表記 (10.2.3.1 など) で入力できます。Cisco NX-OS では、常にドット付き 10 進表記でエリアが表示されます。OSPFv2 ネットワークで、0 という予約されたエリア ID を持つバックボーンエリアも定義する必要があります。エリアが複数ある場合は、1 台以上のルータがエリア境界ルータ (ABR) となります。ABR は、バックボーンエリアと他の 1 つ以上の定義済みエリアの両方に接続します (次の図を参照)。

図 18: OSPFv2 エリア



ABR には、接続するエリアごとに個別のリンクステート データベースがあります。ABR は、接続したエリアの 1 つからバックボーンエリアにネットワーク集約（タイプ 3）LSA（「[ルート集約](#)」セクションを参照）を送信します。バックボーンエリアは、1 つのエリアに関する集約情報を別のエリアに送信します。OSPFv2 エリアの図では、エリア 0 が、エリア 5 に関する集約情報をエリア 3 に送信しています。

OSPFv2 では、自律システム境界ルータ（ASBR）という、もう 1 つのルータ タイプも定義されています。このルータは、OSPFv2 エリアを別の自律システムに接続します。自律システムとは、単一の技術的管理エンティティにより制御されるネットワークです。OSPFv2 は、そのルーティング情報を別の自律システムに再配布したり、再配布されたルートを実別の自律システムから受信したりできます。詳細については、「[詳細な機能](#)」のセクションを参照してください。

リンクステートアドバタイズメント

OSPFv2 はリンクステートアドバタイズメント（LSA）を使用して、固有のルーティングテーブルを構築します。

LSA タイプ

次の表に、Cisco NX-OS でサポートされる LSA タイプを示します。

表 9: LSA タイプ

タイプ	名前	説明
1	ルータ LSA	すべてのルータが送信する LSA。この LSA には、すべてのリンクの状態とコスト、およびリンク上のすべての OSPFv2 ネイバーの一覧が含まれます。ルータ LSA は SPF 再計算をトリガーします。ルータ LSA はローカル OSPFv2 エリアにフラッドイングされます。「 エリア 」の項を参照してください。
2	ネットワーク LSA	DR が送信する LSA。この LSA には、マルチアクセス ネットワーク内のすべてのルータの一覧が含まれます。ネットワーク LSA は SPF 再計算をトリガーします。「 指定ルータ 」のセクションを参照してください。
3	ネットワーク集約 LSA	エリア境界ルータが、ローカル エリア内の宛先ごとに外部エリアに送信する LSA。この LSA には、エリア境界ルータからローカルの宛先へのリンク コストが含まれます。「 エリア 」のセクションを参照してください。
4	ASBR 集約 LSA	エリア境界ルータが外部エリアに送信する LSA。この LSA は、リンク コストを ASBR のみにアドバタイズします。「 エリア 」の項を参照してください。

タイプ	名前	説明
5	AS 外部 LSA	ASBR が生成する LSA。この LSA には、外部自律システム宛先へのリンク コストが含まれます。AS 外部 LSA は、自律システム全体にわたってフラッドニングされます。「 エリア 」の項を参照してください。
7	NSSA 外部 LSA	ASBR が Not-So-Stubby Area (NSSA) 内で生成する LSA。この LSA には、外部自律システム宛先へのリンク コストが含まれます。NSSA 外部 LSA は、ローカル NSSA 内のみでフラッドニングされます。「 エリア 」のセクションを参照してください。
9-11	不透明 LSA	OSPF の拡張に使用される LSA。「 不透明 LSA 」のセクションを参照してください。

リンク コスト

各 OSPFv2 インターフェイスは、リンク コストを割り当てられています。このコストは任意の数字です。デフォルトでは、Cisco NX-OS が、設定された参照帯域幅をインターフェイス帯域幅で割った値をコストとして割り当てます。デフォルトでは、参照帯域幅は 40 Gbps です。リンク コストは各リンクに対して、LSA 更新情報で伝えられます。

フラッドニングと LSA グループ ペーシング

OSPFv2 ルータは LSA を受信すると、その LSA をすべての OSPF 対応インターフェイスに転送し、この情報を使用して OSPFv2 エリアをフラッドニングします。この LSA フラッドニングにより、ネットワーク内のすべてのルータが同じルーティング情報を持つことが保証されます。LSA フラッドニングは、OSPFv2 エリアの設定により異なります（「[エリア](#)」を参照）。LSA は、リンクステート リフレッシュ時間に基づいて（デフォルトでは 30 分ごとに）フラッドニングされます。各 LSA には、リンクステート リフレッシュ時間が設定されています。

ネットワークの LSA 更新情報のフラッドニング レートは、LSA グループ ペーシング機能を使用して制御できます。LSA グループ ペーシングにより、CPU またはバッファの使用率を低下させることができます。この機能により、同様のリンクステート リフレッシュ時間を持つ LSA がグループ化されるため、OSPFv2 で、複数の LSA を 1 つの OSPFv2 更新メッセージにまとめることが可能となります。

デフォルトでは、相互のリンクステート リフレッシュ時間が 4 分以内の LSA が同じグループに入れます。この値は、大規模なリンクステートデータベースでは低く、小規模のデータベースでは高くして、ネットワーク上の OSPFv2 負荷を最適化する必要があります。

リンクステート データベース

各ルータは、OSPFv2 ネットワーク用のリンクステートデータベースを保持しています。このデータベースには、収集されたすべての LSA が含まれ、ネットワークを通過するすべてのルートに関する情報が格納されます。OSPFv2 は、この情報を使用して、各宛先への最適パスを計算し、この最適パスをルーティング テーブルに入力します。

MaxAge と呼ばれる設定済みの時間間隔で受信された LSA 更新情報がまったくない場合は、リンクステート データベースから LSA が削除されます。ルータは、LSA を 30 分ごとに繰り返してフラッディングし、正確なリンクステート情報が期限切れで削除されるのを防ぎます。Cisco NX-OS は、すべての LSA が同時にリフレッシュされるのを防ぐために、LSA グループ機能をサポートしています。詳細については、「[フラッディングと LSA グループ ペーシング](#)」のセクションを参照してください。

不透明 LSA

不透明 LSA により、OSPF 機能の拡張が可能となります。不透明 LSA は、標準 LSA ヘッダーと、それに続くアプリケーション固有の情報で構成されます。この情報は、OSPFv2 または他のアプリケーションにより使用される場合があります。次のような 3 種類の不透明 LSA タイプが定義されています。

- LSA タイプ 9：ローカル ネットワークにフラッディングされます。
- LSA タイプ 10：ローカル エリアにフラッディングされます。
- LSA タイプ 11：ローカル自律システムにフラッディングされます。

OSPFv2 およびユニキャスト RIB

OSPFv2 は、リンクステートデータベースでダイクストラの SPF アルゴリズムを実行します。このアルゴリズムにより、パス上の各リンクのリンク コストの合計に基づいて、各宛先への最適なパスが選択されます。そして、選択された各宛先への最短パスが OSPFv2 ルートテーブルに入力されます。OSPFv2 ネットワークが収束すると、このルート テーブルはユニキャスト RIB にデータを提供します。OSPFv2 はユニキャスト RIB と通信し、次の動作を行います。

- ルートの追加または削除
- 他のプロトコルからのルートの再配布への対応
- 変更されていない OSPFv2 ルートの削除およびスタブ ルータ アドバタイズメントを行うためのコンバージェンス更新情報の提供（「[OSPFv2 スタブ ルータ アドバタイズメント](#)」セクションを参照）

さらに OSPFv2 は、変更済みダイクストラ アルゴリズムを実行して、集約および外部（タイプ 3、4、5、7）LSA の変更の高速再計算を行います。

認証

OSPFv2 メッセージに認証を設定して、ネットワークでの不正な、または無効なルーティング更新を防止できます。Cisco NX-OS は、次の 2 つの認証方式をサポートしています。

- 簡易パスワード認証
- MD5 認証ダイジェスト

OSPFv2 認証は、OSPFv2 エリアに対して、またはインターフェイスごとに設定できます。

簡易パスワード認証

簡易パスワード認証では、OSPFv2 メッセージの一部として送信された単純なクリアテキストのパスワードを使用します。受信 OSPFv2 ルータが OSPFv2 メッセージを有効なルート更新情報として受け入れるには、同じクリアテキストパスワードで構成されている必要があります。パスワードがクリアテキストであるため、ネットワーク上のトラフィックをモニタできるあらゆるユーザーがパスワードを入手できます。

暗号化認証

暗号化認証では、暗号化されたパスワードを OSPFv2 認証に使用します。トランスミッタは、送信するパケットとキー文字列を使用してコードを計算し、そのコードとキー ID をパケットに挿入して、パケットを送信します。受信側は、受信したパケットとローカルに設定されたキーストリング（パケット内のキー ID に対応）を使用してコードをローカルに計算することにより、パケット内のコードを検証します。

メッセージダイジェスト 5（MD5）とハッシュベースの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）暗号化認証の両方がサポートされています。

MD5 認証

OSPFv2 メッセージを認証するには、MD5 認証を使用する必要があります。そのためには、ローカル ルータとすべてのリモート OSPFv2 ネイバーが共有するパスワードを設定します。Cisco NX-OS は各 OSPFv2 メッセージに対して、メッセージと暗号化されたパスワードに基づく MD5 一方向メッセージダイジェストを作成します。インターフェイスはこのダイジェストを OSPFv2 メッセージとともに送信します。受信する OSPFv2 ネイバーは、同じ暗号化パスワードを使用して、このダイジェストを確認します。メッセージが変更されていない場合はダイジェストの計算が同一であるため、OSPFv2 メッセージは有効と見なされます。

MD5 認証には、ネットワークでのメッセージの再送を防ぐための、各 OSPFv2 メッセージのシーケンス番号が含まれます。

高度な機能

Cisco NX-OS は、ネットワークでの OSPFv2 の可用性やスケーラビリティを向上させる数多くの高度な OSPFv2 機能をサポートしています。

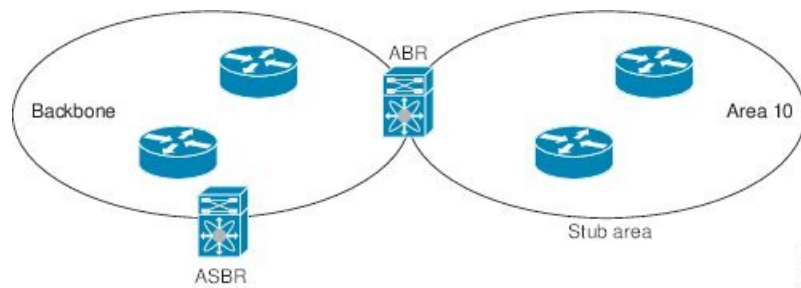
スタブエリア

エリアをスタブエリアにすると、エリアでフラッディングされる外部ルーティング情報の量を制限できます。スタブエリアとは、AS 外部（タイプ 5）LSA（[リンク ステート アドバタイズメント](#)）のセクションを参照）が許可されないエリアです。これらの LSA は通常、外部ルーティング情報を伝播するためにローカル自律システム全体でフラッディングされます。スタブエリアには、次の要件があります。

- スタブエリア内のすべてのルータはスタブルータです。「[スタブ ルーティング](#)」の項を参照してください。
- スタブエリアには ASBR ルータは存在しません。
- スタブエリアには仮想リンクを設定できません。

次の図には、外部 AS に到達するためにエリア 0.0.0.10 内のすべてのルータが ABR を通過する必要がある OSPFv2 AS の例を示します。エリア 0.0.0.10 はスタブエリアとして設定できます。

図 19: スタブエリア



スタブエリアは、外部自律システムへのバックボーンエリアを通過する必要があるすべてのトラフィックにデフォルトルートを使用します。IPv4 の場合のデフォルトルートは 0.0.0.0 です。

Not-So-Stubby Area

Not-So-Stubby Area (NSSA) は、スタブエリアに似ていますが、NSSA では、再配布を使用して NSSA 内で自律システム外部ルートをインポートできる点が異なります。NSSA ASBR はこれらのルートを再配布し、NSSA 外部（タイプ 7）LSA を生成して NSSA 全体でフラッディングします。または、NSSA を他のエリアに接続する ABR を設定することにより、この NSSA 外部 LSA を AS 外部（タイプ 5）LSA に変換することもできます。こうすると、エリア ボーダー ルータ（ABR）は、これらの AS 外部 LSA を OSPFv2 自律システム全体にフラッディングします。変換中は集約とフィルタリングがサポートされます。NSSA 外部 LSA の詳細については、[リンクステート アドバタイズメント](#)のセクションを参照してください。

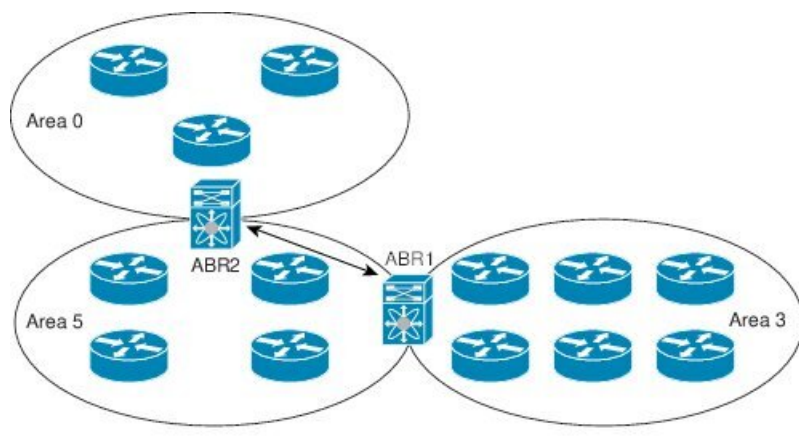
たとえば、OSPFv2 を使用する中央サイトを、異なるルーティング プロトコルを使用するリモートサイトに接続するときに NSSA を使用すると、管理作業を簡素化できます。リモートサイトへのルートはスタブエリア内に再配布できないため、NSSA を使用する前に、企業サイトの境界ルータとリモートルータの間の接続を OSPFv2 スタブエリアとして実行できません。

NSSA を使用すると、企業のルータとリモート ルータ間のエリアを NSSA として定義する（「[NSSA の設定](#)」を参照）ことで、OSPFv2 を拡張してリモート接続性をサポートできます。バックボーン エリア 0 を NSSA にできません。

仮想リンク

仮想リンクを使用すると、物理的に直接接続できない場合に、OSPFv2 エリア ABR をバックボーン エリア ABR に接続できます。次の図には、エリア 3 をエリア 5 経由でバックボーン エリアに接続する仮想リンクを示します。

図 20: 仮想リンク



また、仮想リンクを使用して、分割エリアから一時的に回復できます。分割エリアは、エリア内のリンクがダウンしたために隔離された一部のエリアで、ここからはバックボーンエリアへの代表 ABR に到達できません。

ルートの再配布

OSPFv2 は、ルート再配布を使用して、他のルーティングプロトコルからルートを学習できます。「[ルートの再配布 \(9 ページ\)](#)」の項を参照してください。リンク コストをこれらの再配布されたルートに割り当てるか、またはデフォルト リンク コストを再配布されたすべてのルートに割り当てるように、OSPFv2 を設定します。

ルート再配布では、ルート マップを使用して、再配布する外部ルートを管理します。ルートマップの構成の詳細については、[Route Policy Manager の設定 \(443 ページ\)](#) を参照してください。ルートマップを使用して、これらの外部ルートがローカル OSPFv2 自律システムでアドバタイズされる前に AS 外部 (タイプ 5) LSA および NSSA 外部 (タイプ 7) LSA のパラメータを変更できます。

ルート集約

OSPFv2 は、学習したすべてのルートを、すべての OSPF 対応ルータと共有するため、ルート集約を使用して、すべての OSPF 対応ルータにフラッドイングされる一意のルート数を削減した方がよい場合があります。ルート集約により、より具体的な複数のアドレスが、すべての具体的なアドレスを表す 1 つのアドレスに置き換えられるため、ルートテーブルが簡素化され

ます。たとえば、10.1.1.0/24、10.1.2.0/24、および10.1.3.0/24 というアドレスを1つの集約アドレス 10.1.0.0/16 に置き換えることができます。

一般的には、エリア境界ルータ（ABR）の境界ごとに集約します。集約は2つのエリアの間でも設定できますが、バックボーンの方に集約する方が適切です。こうすると、バックボーンがすべての集約アドレスを受信し、すでに集約されているそれらのアドレスを他のエリアに投入できるためです。集約には、次の2タイプがあります。

- エリア間ルート集約
- 外部ルート集約

エリア間ルート集約は ABR 上で設定し、自律システム内のエリア間のルートを集約します。集約の利点を生かすには、これらのアドレスを1つの範囲内にまとめることができるように、連続するネットワーク番号をエリア内で割り当てる必要があります。

外部ルート集約は、ルート再配布を使用して OSPFv2 に投入される外部ルートに特有のルート集約です。集約する外部の範囲が連続していることを確認する必要があります。異なる2台のルータからの重複範囲を集約すると、誤った宛先にパケットが送信される原因となる場合があります。外部ルート集約は、ルートを OSPF に再配布している ASBR で設定してください。

集約アドレスの設定時に Cisco NX-OS は、ルーティング ブラック ホールおよびルート ループを防ぐために、集約アドレスの廃棄ルートを自動的に設定します。

OSPFv2 スタブルータ アドバタイズメント

OSPFv2 スタブルータ アドバタイズメント機能を使用して、OSPFv2 インターフェイスをスタブルータとして機能するように構成できます。この機能は、ネットワークに新規ルータを機能制限付きで導入する場合や、過負荷になっているルータの負荷を制限する場合など、このルータ経由の OSPFv2 トラフィックを制限するときに使用します。また、この機能は、さまざまな管理上またはトラフィック エンジニアリング上の理由により使用する場合があります。

OSPFv2 スタブルータ アドバタイズメントは、OSPFv2 ルータをネットワーク トポロジから削除しませんが、他の OSPFv2 ルータがこのルータを使用して、ネットワークの他の部分にトラフィックをルーティングできないようにします。このルータを宛先とするトラフィック、またはこのルータに直接接続されたトラフィックだけが送信されます。

OSPFv2 スタブルータ アドバタイズメントは、すべてのスタブ リンク（ローカル ルータに直接接続された）を、ローカル OSPFv2 インターフェイスのコストとしてマークします。すべてのリモート リンクは、最大のコスト（0xFFFF）としてマークされます。

複数の OSPFv2 インスタンス

Cisco NX-OS は、同じノード上で動作する、OSPFv2 プロトコルの複数インスタンスをサポートしています。同一インターフェイスには複数のインスタンスを設定できません。デフォルトでは、すべてのインスタンスが同じシステム ルータ ID を使用します。複数のインスタンスが同じ OSPFv2 自律システムにある場合は、各インスタンスのルータ ID を手動で設定する必要があります。

SPF 最適化

Cisco NX-OS は、次の方法で SPF アルゴリズムを最適化します。

- ネットワーク（タイプ 2）LSA、ネットワーク集約（タイプ 3）LSA、および AS 外部（タイプ 5）LSA 用の部分的 SPF：これらの LSA のいずれかが変更されると、Cisco NX-OS は、全体的な SPF 計算ではなく、高速部分計算を実行します。
- SPF タイマー：さまざまなタイマーを設定して、SPF 計算を制御できます。これらのタイマーには、後続の SPF 計算の幾何バックオフが含まれます。幾何バックオフにより、複数の SPF 計算による CPU 負荷が制限されます。

BFD

この機能では、双方向フォワーディング検出（BFD）をサポートします。BFD は、転送パスの障害を高速で検出することを目的にした検出プロトコルです。BFD は 2 台の隣接デバイス間のサブセカンド障害を検出し、BFD の負荷の一部を、サポートされるモジュール上のデータプレーンに分散できるため、プロトコル hello メッセージよりも CPU を使いません。

仮想化のサポート

OSPFv2 は、仮想ルーティングおよび転送（VRF）インスタンスをサポートしています。デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS はユーザーをデフォルトの VRF に配置します。各 OSPFv2 インスタンスは、システム制限値の範囲で複数の VRF をサポートできます。詳細については、「[レイヤ 3 仮想化の設定](#)」を参照してください。

OSPFv2 の前提条件

OSPFv2 には、次の前提条件があります。

- OSPF を設定するための、ルーティングの基礎に関する詳しい知識がある。
- スイッチにログインしている。
- リモート OSPFv2 ネイバーと通信可能な IPv4 用インターフェイスが 1 つ以上設定されている。
- LAN Base Services ライセンスがインストールされている。
- OSPFv2 ネットワーク戦略と、ネットワークのプランニングが完成している。たとえば、複数のエリアが必要かどうかを決定します。
- OSPF 機能を有効にしてある（[OSPFv2 機能のイネーブル化](#)のセクションを参照）。

注意事項と制約事項

OSPFv2 設定時の注意事項および制約事項は、次のとおりです。

- Cisco NX-OS は、ユーザがエリアを 10 進表記で入力するか、ドット付き 10 進表記で入力するかに関係なく、ドット付き 10 進表記でエリアを表示します。
- Cisco NX-OS リリース 10.3(3)F 以降、OSPFv2 は Cisco NX-OS スイッチの OSPFv2 ユーザーパスワードのタイプ 6 キーチェーン暗号化をサポートします。

デフォルト設定

次の表に、OSPFv2 パラメータのデフォルト設定を示します。

表 10: OSPFv2 のデフォルト パラメータ

パラメータ	デフォルト
hello 間隔	10 秒
デッド間隔	40 秒
OSPFv2 機能	ディセーブル
スタブルータアドバタイズメントの宣言期間	600 秒
リンク コスト計算の参照帯域幅	40 Gbps
LSA 最小到着時間	1000 ミリ秒
LSA グループ ペーシング	240 秒
SPF 計算初期遅延時間	0 ミリ秒
SPF 計算ホールドタイム	5000 ミリ秒
SPF 計算初期遅延時間	0 ミリ秒

基本的な OSPFv2 の設定

OSPFv2 は、OSPFv2 ネットワークを設計した後に設定します。

OSPFv2の有効化

OSPFv2 を設定するには、その前に OSPFv2 機能を有効にする必要があります。

手順の概要

1. `configure terminal`
2. `feature ospf`

3. (任意) **show feature**
4. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	feature ospf 例 : switch(config)# feature ospf 例 :	OSPFv2 機能を有効にします。
ステップ 3	(任意) show feature 例 : switch(config)# show feature	有効および無効にされた機能を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	この設定変更を保存します。

例

no feature ospf コマンドを使用して、OSPFv2 機能を無効にし、関連する構成をすべて削除します。

コマンド	目的
no feature ospf 例 : switch(config)# no feature ospf	OSPFv2 機能を無効にして、関連付けられた構成をすべて削除します。

OSPFv2 インスタンスの作成

OSPFv2 を設定する最初のステップは、OSPFv2 インスタンスを作成することです。作成した OSPFv2 インスタンスには、一意のインスタンスタグを割り当てます。インスタンスタグは任意の文字列です。

OSPFv2 インスタンス パラメータの詳細については、[高度な OSPFv2 の設定](#)のセクションを参照してください。

始める前に

OSPF 機能を有効にしてあることを確認します（[OSPFv2 機能のイネーブル化](#)のセクションを参照）。

show ip ospf instance-tag コマンドを使用して、インスタンス タグが使用されていないことを確認します。

OSPFv2 がルータ ID（設定済みのループバック アドレスなど）を入手可能であるか、またはルータ ID オプションを設定する必要があります。

手順の概要

1. **configure terminal**
2. **router ospf instance-tag**
3. （任意） **router-id ip-address**
4. （任意） **show ip ospf instance-tag**
5. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router ospf instance-tag 例 : <pre>switch(config)# router ospf 201 switch(config-router)</pre>	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	（任意） router-id ip-address 例 : <pre>switch(config-router)# router-id 192.0.2.1</pre>	OSPFv2 ルータ ID を設定します。この IP アドレスにより、この OSPFv2 インスタンスが識別されます。このアドレスは、システムの設定済みインターフェイス上に存在する必要があります。
ステップ 4	（任意） show ip ospf instance-tag 例 : <pre>switch(config-router)# show ip ospf 201</pre>	OSPF 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 5	copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

例

OSPFv2 インスタンスと、関連付けられた構成をすべて削除するには、**no router ospf** コマンドを使用します。

コマンド	目的
no router ospf instance-tag 例 : <pre>switch(config)# no router ospf 201</pre>	OSPF インスタンスと、関連付けられた設定を削除します。



(注) このコマンドは、インターフェイス モードでは OSPF 設定を削除しません。インターフェイス モードで設定された OSPFv2 コマンドはいずれも、手動で削除する必要があります。

OSPFv2 インスタンスのオプションパラメータの設定

OSPF のオプション パラメータを設定できます。

OSPFv2 インスタンス パラメータの詳細については、[高度な OSPFv2 の設定](#)のセクションを参照してください。

始める前に

OSPF 機能を有効にしてあることを確認します ([OSPFv2 機能の有効化](#)のセクションを参照)。

OSPFv2 がルータ ID (設定済みのループバック アドレスなど) を入手可能であるか、またはルータ ID オプションを設定する必要があります。

手順の概要

1. **distance number**
2. **log-adjacency-changes [detail]**
3. **maximum-paths path-number**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	distance number 例 : <pre>switch(config-router)# distance 25</pre>	この OSPFv2 インスタンスのアドミニストレーティブ ディスタンスを設定します。範囲は 1 ～ 255 です。デフォルトは 110 です。
ステップ 2	log-adjacency-changes [detail] 例 : <pre>switch(config-router)# log-adjacency-changes</pre>	ネイバーの状態が変化するたびに、システム メッセージを生成します。
ステップ 3	maximum-paths path-number 例 : <pre>switch(config-router)# maximum-paths 4</pre>	ルートテーブル内の宛先への同じ OSPFv2 パスの最大数を設定します。このコマンドはロードバランシングに使用されます。指定できる範囲は 1 ～ 16 です。デフォルト値は 8 です。

例

次の例は、OSPFv2 インスタンスを作成する方法を示しています。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# copy running-config startup-config
```

OSPFv2でのネットワークの設定

ルータがこのネットワークへの接続に使用するインターフェイスを介して、OSPFv2 へのネットワークを関連付けることで、このネットワークを設定できます（[ネイバー](#)のセクションを参照）。すべてのネットワークをデフォルトバックボーンエリア（エリア 0）に追加したり、任意の 10 進数または IP アドレスを使用して新規エリアを作成したりできます。



(注) すべてのエリアは、バックボーンエリアに直接、または仮想リンク経由で接続する必要があります。



(注) インターフェイスに有効な IP アドレスを設定するまでは、OSPF はインターフェイス上でイネーブルにされません。

始める前に

OSPF 機能を有効にしてあることを確認します（[OSPFv2 機能の有効化](#)のセクションを参照）。

手順の概要

1. **configure terminal**
2. **interface interface-type slot/port**
3. **no switchport**
4. **ip address ip-prefix/length**
5. **ip router ospf instance-tag area area-id [secondaries none]**
6. （任意） **show ip ospf instance-tag interface interface-type slot/port**
7. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します
ステップ 2	interface interface-type slot/port 例 : <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 3	no switchport 例 : <pre>switch(config-if)# no switchport</pre>	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	ip address ip-prefix/length 例 : <pre>switch(config-if)# ip address 192.0.2.1/16</pre>	このインターフェイスに IP アドレスおよびサブネット マスクを割り当てます。
ステップ 5	ip router ospf instance-tag area area-id [secondaries none] 例 : <pre>switch(config-if)# ip router ospf 201 area 0.0.0.15</pre>	OSPFv2 インスタンスおよびエリアにインターフェイスを追加します。
ステップ 6	（任意） show ip ospf instance-tag interface interface-type slot/port	OSPF 情報を表示します。

	コマンドまたはアクション	目的
	例 : <pre>switch(config-if)# show ip ospf 201 interface ethernet 1/2</pre>	
ステップ 7	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

例

インターフェイス コンフィギュレーション モードで、省略可能な次の OSPFv2 パラメータを設定できます。

コマンド	目的
ip ospf cost number 例 : <pre>switch(config-if)# ip ospf cost 25</pre>	このインターフェイスの OSPFv2 コスト メトリックを設定します。デフォルトでは、参照帯域幅とインターフェイス帯域幅に基づいて、コスト メトリックが計算されます。有効な範囲は 1 ～ 65535 です。
ip ospf dead-interval seconds 例 : <pre>switch(config-if)# ip ospf dead-interval 50</pre>	OSPFv2 デッド間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトでは、hello 間隔の秒数の 4 倍です。
ip ospf hello-interval seconds 例 : <pre>switch(config-if)# ip ospf hello-interval 25</pre>	OSPFv2 hello 間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 10 秒です。
ip ospf mtu-ignore 例 : <pre>switch(config-if)# ip ospf mtu-ignore</pre>	OSPFv2 で、ネイバーとのあらゆる IP MTU 不一致が無視されるように設定します。デフォルトでは、ネイバー MTU がローカル インターフェイス MTU が不一致の場合には、隣接関係が確立されません。
ip ospf passive-interface 例 : <pre>switch(config-if)# ip ospf passive-interface</pre>	インターフェイス上でルーティングが更新されないようにします。
ip ospf priority number 例 : <pre>switch(config-if)# ip ospf priority 25</pre>	エリアの DR の決定に使用される OSPFv2 プライオリティを設定します。有効な範囲は 0 ～ 255 です。デフォルトは 1 です。「 指定ルータ 」の項を参照してください。

コマンド	目的
ip ospf shutdown 例 : switch(config-if)# ip ospf shutdown	このインターフェイス上の OSPFv2 インスタンスをシャットダウンします。

次に、OSPFv2 インスタンス 201 にネットワーク エリア 0.0.0.10 を追加する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip address 192.0.2.1/16
switch(config-if)# ip router ospf 201 area 0.0.0.10
switch(config-if)# copy running-config startup-config
```

show ip ospf interface コマンドを使用してインターフェイス設定を確認します。**show ip ospf neighbor** コマンドを使用してこのインターフェイスのネイバーを確認します。

エリアの認証の設定

エリア内のすべてのネットワーク、またはエリア内の個々のインターフェイスの認証を設定できます。インターフェイス認証設定を使用すると、エリア認証は無効になります。

始める前に

OSPF 機能を有効にしてあることを確認します ([OSPFv2 機能のイネーブル化](#)のセクションを参照)。

インターフェイス上のすべてのネイバーが、共有認証キーを含め、同じ認証設定を共有することを確認します。

この認証設定のためのキー チェーンを作成します。

手順の概要

1. **configure terminal**
2. **router ospf instance-tag**
3. **area area-id authentication [message-digest]**
4. **interface interface-type slot/port**
5. **no switchport**
6. (任意) **ip ospf authentication-key [0 | 3] key**
7. (任意) **ip ospf message-digest-key key-id md5 [0 | 3] key**
8. (任意) **show ip ospf instance-tag interface interface-type slot/port**
9. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	router ospf instance-tag 例 : switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	area area-id authentication [message-digest] 例 : switch(config-router)# area 0.0.0.10 authentication	エリアの認証モードを設定します。
ステップ 4	interface interface-type slot/port 例 : switch(config-router)# interface ethernet 1/2 switch(config-if)#	インターフェイス設定モードを開始します。
ステップ 5	no switchport 例 : switch(config-if)# no switchport	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 6	(任意) ip ospf authentication-key [0 3] key 例 : switch(config-if)# ip ospf authentication-key 0 mypass	(オプション) このインターフェイスに簡易パスワード認証を構成します。認証が、キーチェーンにもメッセージダイジェストにも設定されていない場合は、このコマンドを使用します。0 の場合は、パスワードをクリア テキストで設定します。3 の場合は、パスワードを 3DES 暗号化として設定します。
ステップ 7	(任意) ip ospf message-digest-key key-id md5 [0 3] key 例 : switch(config-if)# ip ospf message-digest-key 21 md5 0 mypass	このインターフェイスにメッセージダイジェスト認証を設定します。認証がメッセージダイジェストに設定されている場合は、このコマンドを使用します。key-id の範囲は 1 ～ 255 です。MD5 オプションが 0 の場合はパスワードがクリアテキストで構成され、3 の場合はパスワードが 3DES 暗号化として構成されます。
ステップ 8	(任意) show ip ospf instance-tag interface interface-type slot/port	

	コマンドまたはアクション	目的
	例 : <pre>switch(config-if)# show ip ospf 201 interface ethernet 1/2</pre>	
ステップ 9	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

インターフェイスの認証の設定

エリア内の個々のインターフェイスに認証を設定できます。インターフェイス認証設定を使用すると、エリア認証は無効になります。

始める前に

OSPF 機能を有効にしてあることを確認します ([OSPFv2 機能のイネーブル化](#)のセクションを参照)。

インターフェイス上のすべてのネイバーが、共有認証キーを含め、同じ認証設定を共有することを確認します。

この認証設定のためのキー チェーンを作成します。

OSPFv2 HMAC-SHA 認証を構成するには、キーに使用する HMAC-SHA アルゴリズムを指定する必要があります。暗号化アルゴリズムを選択せずにキーチェーンを使用した暗号化認証が構成されている場合、OSPFv2 は MD5 暗号化アルゴリズムを使用します。

手順の概要

1. **configure terminal**
2. **interface interface-type slot/port**
3. **no switchport**
4. **ip ospf authentication [message-digest]**
5. **ip ospf authentication keychain key-name**
6. **ip ospf authentication-key [0 | 3 | 7] key**
7. **ip ospf message-digest-key key-id md5 [0 | 3 | 7] key**
8. **show ip ospf instance-tag interface interface-type slot/port**
9. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します
ステップ 2	interface interface-type slot/port 例 : <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 3	no switchport 例 : <pre>switch(config-if)# no switchport</pre>	そのインターフェイスを、レイヤ3ルーテッドインターフェイスとして設定します。
ステップ 4	ip ospf authentication [message-digest] 例 : <pre>switch# configure terminal switch(config)#</pre>	OSPFv2 のインターフェイス認証モードをクリアテキストタイプとメッセージダイジェストタイプのどちらかでイネーブルにします。これにより、エリアに基づくこのインターフェイスの認証が無効となります。すべてのネイバーが、この認証タイプを共有する必要があります。
ステップ 5	ip ospf authentication keychain key-name 例 : <pre>switch(config-if)# ip ospf authentication keychain Test1</pre>	OSPFv2 のキーチェーンを使用するようにインターフェイス認証を構成します。
ステップ 6	ip ospf authentication-key [0 3 7] key 例 : <pre>switch(config-if)# ip ospf authentication-key 0 mypass</pre>	このインターフェイスに簡易パスワード認証を設定します。認証が、キーチェーンにもメッセージダイジェストにも設定されていない場合は、このコマンドを使用します。 オプションは次のとおりです。 • 0 の場合は、パスワードをクリアテキストで構成します。 • 3 : パス キーを 3DES 暗号化として設定します。 • 7 : パス キーを Cisco タイプ 7 暗号化として設定します。

	コマンドまたはアクション	目的
ステップ 7	ip ospf message-digest-key key-id md5 [0 3 7] key 例 : <pre>switch(config-if)# ip ospf message-digest-key 21 md5 0 mypass</pre>	このインターフェイスにメッセージダイジェスト認証を設定します。認証がメッセージダイジェストに設定されている場合は、このコマンドを使用します。 key-id の範囲は 1 ～ 255 です。MD5 オプションは次のとおりです。 • 0 の場合は、パスワードをクリア テキストで構成します。 • 3 : パス キーを 3DES 暗号化として設定します。 • 7 : パス キーを Cisco タイプ 7 暗号化として設定します。
ステップ 8	show ip ospf instance-tag interface interface-type slot/port 例 : <pre>switch(config-if)# show ip ospf 201 interface ethernet 1/2</pre>	OSPF 情報を表示します。
ステップ 9	copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、インターフェイスに暗号化されていない簡単なパスワードを設定し、イーサネット インターフェイス 1/2 のパスワードを設定する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# exit
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip router ospf 201 area 0.0.0.10
switch(config-if)# ip ospf authentication
switch(config-if)# ip ospf authentication-key 0 mypass
switch(config-if)# copy running-config startup-config
```

次に、OSPFv2 HMAC-SHA-1 および MD5 暗号化認証を設定する例を示します。

```
switch# configure terminal
switch(config)# key chain chain1
switch(config-keychain)# key 1
switch(config-keychain-key)# key-string 7 070724404206
switch(config-keychain-key)# accept-lifetime 01:01:01 Jan 01 2015 infinite
switch(config-keychain-key)# send-lifetime 01:01:01 Jan 01 2015 infinite
switch(config-keychain-key)# cryptographic-algorithm HMAC-SHA-1
switch(config-keychain-key)# exit
switch(config-keychain)# key 2
switch(config-keychain-key)# key-string 7 070e234f1f5b4a
switch(config-keychain-key)# accept-lifetime 10:51:01 Jul 24 2015 infinite
switch(config-keychain-key)# send-lifetime 10:51:01 Jul 24 2015 infinite
```

```

switch(config-keychain-key)# cryptographic-algorithm MD5
switch(config-keychain-key)# exit
switch(config-keychain)# exit

switch(config)# interface ethernet 1/1
switch(config-if)# ip router ospf 1 area 0.0.0.0
switch(config-if)# ip ospf authentication message-digest
switch(config-if)# ip ospf authentication key-chain chain1

switch(config-if)# show key chain chain1
Key-Chain chain1
Key 1 -- text 7 "070724404206"
cryptographic-algorithm HMAC-SHA-1
accept lifetime UTC (01:01:01 Jan 01 2015)-(always valid) [active]
send lifetime UTC (01:01:01 Jan 01 2015)-(always valid) [active]
Key 2 -- text 7 "070e234f1f5b4a"
cryptographic-algorithm MD5
accept lifetime UTC (10:51:00 Jul 24 2015)-(always valid) [active]
send lifetime UTC (10:51:00 Jul 24 2015)-(always valid) [active]

switch(config-if)# show ip ospf interface ethernet 1/1
Ethernet1/1 is up, line protocol is up
IP address 11.11.11.1/24
Process ID 1 VRF default, area 0.0.0.3
Enabled by interface configuration
State BDR, Network type BROADCAST, cost 40
Index 6, Transmit delay 1 sec, Router Priority 1
Designated Router ID: 33.33.33.33, address: 11.11.11.3
Backup Designated Router ID: 1.1.1.1, address: 11.11.11.1
2 Neighbors, flooding to 2, adjacent with 2
Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
Hello timer due in 00:00:08
Message-digest authentication, using keychain key1 (ready)
Sending SA: Key id 2, Algorithm MD5
Number of opaque link LSAs: 0, checksum sum 0

```

高度な OSPFv2 の設定

OSPFv2 は、OSPFv2 ネットワークを設計した後に設定します。

境界ルータのフィルタ リストの設定

OSPFv2 ドメインを関連ネットワークを含む一連のエリアに分割できます。すべてのエリアは、エリア境界ルータ（ABR）経由でバックボーンエリアに接続する必要があります。OSPFv2 ドメインは、自律システム境界ルータ（ASBR）を介して、外部ドメインに接続可能です。「[エリア](#)」の項を参照してください。

ABR には、省略可能な次の設定パラメータがあります。

- **Area range** : エリア間のルート集約を設定します。
- **Filter list** : ABR 上で、外部エリアから受信したネットワーク集約（タイプ 3）LSA をフィルタリングします。

ASBR もフィルタ リストをサポートしています。

始める前に

OSPF 機能を有効にしてあることを確認します ([OSPFv2 機能のイネーブル化](#)のセクションを参照)。

フィルタ リストが、着信または発信ネットワーク集約 (タイプ 3) LSA の IP プレフィックスのフィルタリングに使用するルート マップを作成します。[Route Policy Manager の設定 \(443 ページ\)](#) を参照してください。

手順の概要

1. **configure terminal**
2. **router ospf instance-tag**
3. **area area-id filter-list route-map map-name {in | out}**
4. (任意) **show ip ospf policy statistics area id filter-list {in | out}**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	router ospf instance-tag 例 : switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	area area-id filter-list route-map map-name {in out} 例 : switch(config-router)# area 0.0.0.10 filter-list route-map FilterLSAs in	ABR 上で着信または発信ネットワーク集約 (タイプ 3) LSA をフィルタリングします。
ステップ 4	(任意) show ip ospf policy statistics area id filter-list {in out} 例 : switch(config-router)# show ip ospf policy statistics area 0.0.0.10 filter-list in	OSPF ポリシー情報を表示します。
ステップ 5	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします

例

次に、エリア 0.0.0.10 でフィルタ リストを設定する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 filter-list route-map FilterLSAs in
switch(config-router)# copy running-config startup-config
```

スタブエリアの設定

OSPFv2 ドメインの外部トラフィックが不要な個所にスタブエリアを設定できます。スタブエリアは AS 外部（タイプ 5）LSA をブロックし、選択したネットワークへの往復の不要なルーティングを制限します。「[スタブエリア](#)」の項を参照してください。また、すべての集約ルートがスタブエリアを経由しないようブロックすることもできます。

始める前に

OSPF 機能を有効にしてあることを確認します（[OSPFv2 機能の有効化](#)のセクションを参照）。

設定されるスタブエリア内に、仮想リンクと ASBR のいずれも含まれないことを確認します。

手順の概要

1. **configure terminal**
2. **router ospf instance-tag**
3. **area area-id stub**
4. （任意） **area area-id default-cost cost**
5. （任意） **show ip ospf instance-tag**
6. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router ospf instance-tag 例 : <pre>switch(config)# router ospf 201 switch(config-router)#</pre>	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

	コマンドまたはアクション	目的
ステップ 3	area area-id stub 例 : <pre>switch(config-router)# area 0.0.0.10 stub</pre>	このエリアをスタブエリアとして作成します。
ステップ 4	(任意) area area-id default-cost cost 例 : <pre>switch(config-router)# area 0.0.0.10 default-cost 25</pre>	このスタブエリアに送信されるデフォルトサマリルートのコストメトリックを設定します。指定できる範囲は0～16777215です。デフォルトは1です。
ステップ 5	(任意) show ip ospf instance-tag 例 : <pre>switch(config-router)# show ip ospf 201</pre>	OSPF 情報を表示します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします

例

次に、スタブエリアを作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 stub
switch(config-router)# copy running-config startup-config
```

Totally Stubby エリアの設定

Totally Stubby エリアを作成して、すべての集約ルート更新がスタブエリアに入るのを防ぐことができます。

Totally Stubby エリアを作成するには、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
area area-id stub no-summary 例 : <pre>switch(config-router)# area 20 stub no-summary</pre>	このエリアを Totally Stubby エリアとして作成します。

NSSA の設定

OSPFv2 ドメインの一部で一定限度の外部トラフィックが必要な場合は、その部分に NSSA を設定できます。[Not-So-Stubby エリア](#) のセクションを参照してください。また、この外部トラフィックを AS 外部（タイプ 5）LSA に変換して、このルーティング情報で OSPFv2 ドメインをフラッディングすることもできます。NSSA は、省略可能な次のパラメータで設定できます。

- **No redistribution** : 再配布されたルートは、NSSA をバイパスして OSPFv2 自律システム内の他のエリアに再配布されます。このオプションは、NSSA ASBR が ABR も兼ねているときに使用します。
- **Default information originate** : 外部自律システムへのデフォルトルートの NSSA 外部（タイプ 7）LSA を生成します。このオプションは、ASBR のルーティングテーブルにデフォルトルートが含まれる場合に NSSA ASBR 上で使用します。このオプションは、ASBR のルーティングテーブルにデフォルトルートが含まれるかどうかに関係なく、NSSA ASBR 上で使用できます。
- **Route map** : 目的のルートだけが NSSA および他のエリア全体でフラッディングされるように、外部ルートをフィルタリングします。
- **Translate** : NSSA 外のエリア向けに、NSSA 外部 LSA を AS 外部 LSA に変換します。再配布されたルートを OSPFv2 自律システム全体でフラッディングするには、このコマンドを NSSA ABR 上で使用します。また、これらの AS 外部 LSA の転送アドレスを無効にすることもできます。このオプションを選択した場合は、転送アドレスが 0.0.0.0 に設定されます。
- **No summary** : すべての集約ルートが NSSA でフラッディングされないようにします。このオプションは NSSA ABR 上で使用します。

始める前に

OSPF 機能を有効にしてあることを確認します（[OSPFv2 機能のイネーブル化](#)のセクションを参照）。

設定する NSSA 上に仮想リンクがないことと、この NSSA がバックボーンエリアでないことを確認します。

手順の概要

1. **configure terminal**
2. **router ospf instance-tag**
3. **area area-id nssa [no-redistribution] [default-information-originate] originate [route-map map-name]] [no-summary] [translate type7 {always | never} [suppress-fa]]**
4. （任意） **area area-id default-cost cost**
5. （任意） **show ip ospf instance-tag**
6. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	router ospf instance-tag 例 : switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	area area-id nssa [no-redistribution] [default-information-originate] originate [route-map map-name] [no-summary] [translate type7 {always never} [suppress-fa]] 例 : switch(config-router)# area 0.0.0.10 nssa	このエリアを NSSA として作成します。
ステップ 4	(任意) area area-id default-cost cost 例 : switch(config-router)# area 0.0.0.10 default-cost 25	この NSSA に送信されるデフォルト集約ルートのコスト メトリックを設定します。
ステップ 5	(任意) show ip ospf instance-tag 例 : switch(config-router)# show ip ospf 201	OSPF 情報を表示します。
ステップ 6	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします

例

次に、すべての集約ルート更新をブロックする NSSA を作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 nssa no-summary
switch(config-router)# copy running-config startup-config
```

次に、デフォルト ルートを生成する NSSA を作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 nssa default-info-originate
switch(config-router)# copy running-config startup-config
```

次に、外部ルートをフィルタリングし、すべての集約ルート更新をブロックするNSSAを作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 nssa route-map ExternalFilter no-summary
switch(config-router)# copy running-config startup-config
```

次に、常にNSSA 外部（タイプ 5）LSA を AS 外部（タイプ 7）LSA に変換するNSSAを作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 nssa translate type 7 always
switch(config-router)# copy running-config startup-config
```

仮想リンクの設定

仮想リンクは、隔離されたエリアを中継エリアを介してバックボーン エリアに接続します。[\[仮想リンク\]](#)セクションを展開します。仮想リンクには、省略可能な次のパラメータを設定できます。

- **Authentication** : 簡単なパスワード認証または MD5 メッセージダイジェスト認証、および関連付けられたキーを設定します。
- **Dead interval** : ローカル ルータがデッドであることを宣言し、隣接関係を解消する前に、ネイバーが hello パケットを待つ時間を設定します。
- **Hello interval** : 連続する hello パケット間の時間間隔を設定します。
- **Retransmit interval** : 連続する LSA 間の推定時間間隔を設定します。
- **Transmit delay** : LSA をネイバーに送信する推定時間を設定します。



(注) リンクがアクティブになる前に、関与する両方のルータで仮想リンクを設定する必要があります。

スタブ エリアには仮想リンクを追加できません。

始める前に

OSPF 機能を有効にしてあることを確認します（[OSPFv2 機能のイネーブル化](#)のセクションを参照）。

手順の概要

1. configure terminal

2. **router ospf** *instance-tag*
3. **area** *area-id* **virtual link** *router-id*
4. (任意) **show ip ospf virtual-link** [**brief**]
5. (任意) **copy running-config startup-config**
6. (任意) **authentication** [**key-chain** *key-id* **message-digest** | **null**]
7. (任意) **authentication-key** [**0** | **3**] *key*
8. (任意) **dead-interval** *seconds*
9. (任意) **hello-interval** *seconds*
10. (任意) **message-digest-key** *key-id* **md5** [**0** | **3**] *key*
11. (任意) **retransmit-interval** *seconds*
12. (任意) **transmit-delay** *seconds*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router ospf <i>instance-tag</i> 例 : <pre>switch(config)# router ospf 201 switch(config-router)#</pre>	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	area <i>area-id</i> virtual link <i>router-id</i> 例 : <pre>switch(config-router)# area 0.0.0.10 virtual-link 10.1.2.3 switch(config-router-vlink)#</pre>	リモートルータへの仮想リンクの端を作成します。仮想リンクをリモートルータ上に作成して、リンクを完成させる必要があります。
ステップ 4	(任意) show ip ospf virtual-link [brief] 例 : <pre>switch(config-router-vlink)# show ip ospf virtual-link</pre>	OSPF 仮想リンク情報を表示します。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします

	コマンドまたはアクション	目的
ステップ 6	(任意) authentication [key-chain <i>key-id</i> message-digest null] 例 : <pre>switch(config-router-vlink)# authentication message-digest</pre>	エリアに基づくこの仮想リンクの認証がオーバーライドされます。
ステップ 7	(任意) authentication-key [0 3] <i>key</i> 例 : <pre>switch(config-router-vlink)# authentication-key 0 mypass</pre>	この仮想リンクに簡易パスワードを設定します。認証が、キーチェーンにもメッセージダイジェストにも設定されていない場合は、このコマンドを使用します。0 の場合は、パスワードをクリアテキストで設定します。3 の場合は、パスワードを 3DES 暗号化として設定します。
ステップ 8	(任意) dead-interval <i>seconds</i> 例 : <pre>switch(config-router-vlink)# dead-interval 50</pre>	OSPFv2 デッド間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトでは、hello 間隔の秒数の 4 倍です。
ステップ 9	(任意) hello-interval <i>seconds</i> 例 : <pre>switch(config-router-vlink)# hello-interval 25</pre>	OSPFv2 hello 間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 10 秒です。
ステップ 10	(任意) message-digest-key <i>key-id</i> md5 [0 3] <i>key</i> 例 : <pre>switch(config-router-vlink)# message-digest-key 21 md5 0 mypass</pre>	この仮想リンクにメッセージダイジェスト認証を設定します。認証がメッセージダイジェストに設定されている場合は、このコマンドを使用します。0 の場合は、パスワードをクリアテキストで設定します。3 の場合は、パスキーを 3DES 暗号化として設定します。
ステップ 11	(任意) retransmit-interval <i>seconds</i> 例 : <pre>switch(config-router-vlink)# retransmit-interval 50</pre>	OSPFv2 再送信間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 5 分です。
ステップ 12	(任意) transmit-delay <i>seconds</i> 例 : <pre>switch(config-router-vlink)# transmit-delay 2</pre>	OSPFv2 送信遅延を秒単位で設定します。指定できる範囲は 1 ～ 450 です。デフォルトは 1 です。

例

次に、2 つの ABR 間に簡単な仮想リンクを作成する例を示します。

ABR 1（ルータ ID 27.0.0.55）の設定は、次のとおりです。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 virtual-link 10.1.2.3
switch(config-router-vlink)# copy running-config startup-config
```

ABR 2（ルータ ID 10.1.2.3）の設定は、次のとおりです。

```
switch# configure terminal
switch(config)# router ospf 101
switch(config-router)# area 0.0.0.10 virtual-link 27.0.0.55
switch(config-router-vlink)# copy running-config startup-config
```

再配布の設定

他のルーティングプロトコルから学習したルートを、ASBR 経由で OSPFv2 自律システムに再配布できます。

OSPF でのルート再配布には、省略可能な次のパラメータを設定できます。

- **Default information originate** : 外部自律システムへのデフォルト ルートの AS 外部（タイプ 5）LSA を生成します。



(注) **Default information originate** はオプションのルートマップ内の **match** 文を無視します。

- **Default metric** : すべての再配布ルートに同じコスト メトリックを設定します。



(注) スタティックルートを再配布する場合、デフォルトのスタティックルートを正常に再配布するためには、Cisco NX-OS も **default-information originate** コマンドを必要とします。

始める前に

OSPF 機能を有効にしてあることを確認します（[OSPFv2 機能の有効化](#)のセクションを参照）。

再配布で使用する、必要なルート マップを作成します。

手順の概要

1. **configure terminal**
2. **router ospf instance-tag**
3. **redistribute {bgp id | direct | eigrp id | isis id | ospf id | rip id | static} route-map map-name**
4. **default-information originate [always] [route-map map-name]**
5. **default-metric [cost]**
6. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router ospf instance-tag 例 : <pre>switch(config)# router ospf 201 switch(config-router)#</pre>	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	redistribute {bgp id direct eigrp id isis id ospf id rip id static} route-map map-name 例 : <pre>switch(config-router)# redistribute bgp route-map FilterExternalBGP</pre>	設定したルートマップ経由で、選択したプロトコルを OSPF に再配布します。 (注) スタティック ルートを再配布する場合、デフォルトのスタティック ルートを正常に再配布するためには、Cisco NX-OS も default-information originate コマンドを必要とします。
ステップ 4	default-information originate [always] [route-map map-name] 例 : <pre>switch(config-router)# default-information-originate route-map DefaultRouteFilter</pre>	デフォルト ルートが RIB に存在する場合は、この OSPF ドメインにデフォルト ルートを作成します。次の省略可能なキーワードを使用します。 • always : ルートが RIB に存在しない場合でも、常にデフォルト ルート 0.0.0. を生成します。 • route-map : ルート マップが true を返す場合にデフォルト ルートを生成します。 (注) このコマンドは、ルート マップの match 文を無視します。
ステップ 5	default-metric [cost] 例 : <pre>switch(config-router)# default-metric 25</pre>	再配布されたルートのコストメトリックを設定します。このコマンドは、直接接続されたルートには適用されません。ルートマップを使用して、直接接続されたルートのデフォルトのメトリックを設定します。
ステップ 6	(任意) copy running-config startup-config 例 :	実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします

	コマンドまたはアクション	目的
	switch(config)# copy running-config startup-config	

例

次に、ボーダー ゲートウェイ プロトコル (BGP) を OSPF に再配布する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# redistribute bgp route-map FilterExternalBGP
switch(config-router)# copy running-config startup-config
```

再配布されるルート数の制限

ルートの再配布によって、OSPFv2 ルートテーブルに多くのルートが追加される可能性があります。外部プロトコルから受け取るルートの数の上限を設定できます。OSPFv2 には、再配布ルートの制限を設定するために次のオプションが用意されています。

- 上限固定：設定された最大値に OSPFv2 が達すると、メッセージをログに記録します。OSPFv2 は以降の再配布ルートを受け取りません。任意で、最大値のしきい値パーセンテージを設定して、OSPFv2 がこのしきい値を超えたときに警告を記録するようにすることもできます。
- 警告のみ：OSPFv2 が最大値に達したときのみ、警告のログを記録します。OSPFv2 は、再配布されたルートを受け入れ続けます。
- 取り消し：OSPFv2 が最大値に達したときにタイムアウト期間を開始します。このタイムアウト期間後、現在の再配布されたルート数が最大制限より少なければ、OSPFv2 はすべての再配布されたルートを要求します。再配布されたルートの現在数が最大数に達した場合、OSPFv2 はすべての再配布されたルートを取り消します。OSPFv2 が追加の再配布されたルートを受け付ける前に、この状況を解消する必要があります。
- 任意で、タイムアウト期間を設定できます。

始める前に

OSPF 機能を有効にしてあることを確認します ([OSPFv2 機能の有効化](#)のセクションを参照)。

手順の概要

1. **configure terminal**
2. **router ospf instance-tag**
3. **redistribute {bgp id | direct | eigrp id | isis id | ospf id | rip id | static} route-map map-name**
4. **redistribute maximum-prefix max [threshold] [warning-only | withdraw [num-retries timeout]]**
5. (任意) **show running-config ospf**

6. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router ospf instance-tag 例 : <pre>switch(config)# router ospf 201 switch(config-router)#</pre>	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	redistribute {bgp id direct eigrp id isis id ospf id rip id static} route-map map-name 例 : <pre>switch(config-router)# redistribute bgp route-map FilterExternalBGP</pre>	設定したルートマップ経由で、選択したプロトコルを OSPF に再配布します。
ステップ 4	redistribute maximum-prefix max [threshold] [warning-only withdraw [num-retries timeout]] 例 : <pre>switch(config-router)# redistribute maximum-prefix 1000 75 warning-only</pre>	OSPFv2 が配布するプレフィックスの最大数を指定します。指定できる範囲は 0 ～ 65536 です。任意で次のオプションを指定します。 • threshold : 警告メッセージをトリガーする最大プレフィックス数のパーセンテージ。 • warning-only : プレフィックスの最大数を超えた場合に警告メッセージを記録します。 • withdraw : 再配布されたすべてのルートを取り消します。任意で再配布されたルートを取得しようと試みます。num-retries の範囲は 1 ～ 12 です。timeout の範囲は 60 ～ 600 秒です。デフォルトは 300 秒です。clear ip ospf redistribution コマンドは、すべてのルートが取り消された場合に使用します。
ステップ 5	(任意) show running-config ospf 例 : <pre>switch(config-router)# show running-config ospf</pre>	OSPFv2 設定を表示します。

	コマンドまたはアクション	目的
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします

例

次に、OSPF に再配布されるルート数を制限する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# redistribute bgp route-map FilterExternalBGP
switch(config-router)# redistribute maximum-prefix 1000 75
```

ルート集約の設定

集約したアドレス範囲を設定することにより、エリア間ルートのルート集約を設定できます。また、ASBR 上のこれらのルートのサマリアドレスを設定して、外部の再配布されたルートのルート集約を設定することもできます。「[ルート集約](#)」の項を参照してください。

始める前に

OSPF 機能を有効にしてあることを確認します ([OSPFv2 機能のイネーブル化](#)のセクションを参照)。

手順の概要

1. **configure terminal**
2. **router ospf instance-tag**
3. **area area-id range ip-prefix/length [no-advertise] [cost cost]**
4. **summary-address ip-prefix/length [no-advertise | tag tag]**
5. (任意) **show ip ospf summary-address**
6. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 2	router ospf instance-tag 例 : <pre>switch(config)# router ospf 201 switch(config-router)#</pre>	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	area area-id range ip-prefix/length [no-advertise] [cost cost] 例 : <pre>switch(config-router)# area 0.0.0.10 range 10.3.0.0/16</pre>	一定の範囲のアドレスのサマリ アドレスを ABR 上に作成します。このサマリアドレスをネットワーク集約（タイプ 3）LSA にアドバタイズしないようにすることもできます。cost の範囲は 0 ～ 16777215 です。
ステップ 4	summary-address ip-prefix/length [no-advertise tag tag] 例 : <pre>switch(config-router)# summary-address 10.5.0.0/16 tag 2</pre>	一定の範囲のアドレスのサマリ アドレスを ABR 上に作成します。ルートマップによる再配布で使えるよう、このサマリアドレスにタグを割り当てることもできます。
ステップ 5	（任意） show ip ospf summary-address 例 : <pre>switch(config-router)# show ip ospf summary-address</pre>	OSPF サマリ アドレスに関する情報を表示します。
ステップ 6	（任意） copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします

例

次に、ABR 上のエリア間のサマリ アドレスを作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 range 10.3.0.0/16
switch(config-router)# copy running-config startup-config
```

次に、ASBR 上のサマリ アドレスを作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# summary-address 10.5.0.0/16
switch(config-router)# copy running-config startup-config
```

スタブルートアドバタイズメントの設定

短期間だけ、このルータ経由の OSPFv2 トラフィックを制限する場合は、スタブルートアドバタイズメントを使用します。「[OSPFv2 スタブルータアドバタイズメント](#)」のセクションを参照してください。

スタブルートアドバタイズメントは、省略可能な次のパラメータで設定できます。

- **On startup** : 指定した宣言期間だけ、スタブルートアドバタイズメントを送信します。
- **Wait for BGP** : BGP がコンバージェンスするまで、スタブルートアドバタイズメントを送信します。



- (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。

始める前に

OSPF 機能を有効にしてあることを確認します ([OSPFv2 機能の有効化](#)のセクションを参照)。

手順の概要

1. **configure terminal**
2. **router ospf instance-tag**
3. **max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup {seconds | wait-for bgp tag}] [summary-lsa [max-metric-value]]**
4. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router ospf instance-tag 例 : <pre>switch(config)# router ospf 201 switch(config-router)#</pre>	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

	コマンドまたはアクション	目的
ステップ 3	max-metric router-lsa [external-lsa [<i>max-metric-value</i>]] [include-stub] [on-startup {seconds wait-for bgp tag}] [summary-lsa [<i>max-metric-value</i>]] 例 : <pre>switch(config-router)# max-metric router-lsa</pre>	OSPFv2 スタブルートアドバタイズメントを設定します。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします

例

次に、起動時にスタブルートアドバタイズメントを、デフォルトの 600 秒間イネーブルにする例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# max-metric router-lsa on-startup
switch(config-router)# copy running-config startup-config
```

デフォルト タイマーの変更

OSPFv2 には、プロトコル メッセージの動作および最短パス優先 (SPF) の計算を制御する多数のタイマーが含まれています。OSPFv2 には、省略可能な次のタイマー パラメータが含まれます。

- **LSA arrival time** : ネイバーから着信する LSA 間で許容される最小間隔を設定します。この時間より短時間で到着する LSA はドロップされます。
- **Pacing LSAs** : LSA が集められてグループ化され、リフレッシュされて、チェックサムが計算される間隔、つまり期限切れとなる間隔を設定します。このタイマーは、LSA 更新が実行される頻度を制御し、LSA 更新メッセージで送信される LSA 更新の数を制御します（「[フラディングと LSA グループ ペーシング](#)」を参照）。
- **Throttle LSAs** : LSA 生成のレート制限を設定します。このタイマーは、トポロジが変更された後に LSA が生成される頻度を制御します。
- **Throttle SPF calculation** : SPF 計算の実行頻度を制御します。

インターフェイス レベルでは、次のタイマーも制御できます。

- **Retransmit interval** : 連続する LSA 間の推定時間間隔を設定します。
- **Transmit delay** : LSA をネイバーに送信する推定時間を設定します。

hello 間隔とデッド タイマーに関する情報の詳細については、「[OSPFv2 のネットワークの設定](#)」の項を参照してください。

始める前に

OSPF 機能を有効にしてあることを確認します（[OSPFv2 機能の有効化](#)のセクションを参照）。

手順の概要

1. **configure terminal**
2. **router ospf instance-tag**
3. **timers lsa-arrival msec**
4. **timers lsa-group-pacing seconds**
5. **timers throttle lsa start-time hold-interval max-time**
6. **timers throttle spf delay-time hold-time max-wait**
7. **interface type slot/port**
8. **no switchport**
9. **ip ospf hello-interval seconds**
10. **ip ospf dead-interval seconds**
11. **ip ospf retransmit-interval seconds**
12. **ip ospf transmit-delay seconds**
13. （任意） **show ip ospf**
14. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	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	router ospf instance-tag 例： switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	timers lsa-arrival msec 例： switch(config-router)# timers lsa-arrival 2000	LSA 到着時間をミリ秒で設定します。範囲は 10 ～ 600000 です。デフォルトは 1000 ミリ秒です。
ステップ 4	timers lsa-group-pacing seconds 例：	LSA がグループ化される間隔を秒で設定します。範囲は 1 ～ 1800 です。デフォルトは 240 秒です。

	コマンドまたはアクション	目的
	<pre>switch(config-router)# timers lsa-group-pacing 1800</pre>	
ステップ 5	timers throttle lsa start-time hold-interval max-time 例 : <pre>switch(config-router)# timers throttle lsa 3000 6000 6000</pre>	次のタイマーを使用して、LSA 生成のレート制限をミリ秒で設定します。 • start-time : 指定できる範囲は 50 ～ 5000 ミリ秒です。デフォルト値は 50 ミリ秒です。 • hold-interval : 指定できる範囲は 50 ～ 30,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。 • max-time : 指定できる範囲は 50 ～ 30,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
ステップ 6	timers throttle spf delay-time hold-time max-wait 例 : <pre>switch(config-router)# timers throttle spf 3000 2000 4000</pre>	SPF 最適パス スケジュール初期遅延時間と、各 SPF 最適パス計算間の最小ホールド タイム (秒単位) を設定します。指定できる範囲は 1 ～ 600000 です。デフォルトは、遅延時間なし、およびホールド タイム 5000 ミリ秒です。
ステップ 7	interface type slot/port 例 : <pre>switch(config)# interface ethernet 1/2 switch(config-if)</pre>	インターフェイス設定モードを開始します。
ステップ 8	no switchport 例 : <pre>switch(config-if)# no switchport</pre>	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 9	ip ospf hello-interval seconds 例 : <pre>switch(config-if)# ip ospf hello-interval 30</pre>	このインターフェイスの hello 間隔を設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 10 です。
ステップ 10	ip ospf dead-interval seconds 例 : <pre>switch(config-if)# ip ospf dead-interval 30</pre>	このインターフェイスのデッド間隔を設定します。有効な範囲は 1 ～ 65535 です。
ステップ 11	ip ospf retransmit-interval seconds 例 : <pre>switch(config-if)# ip ospf retransmit-interval 30</pre>	このインターフェイスから送信される各 LSA 間の推定時間間隔を設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 5 分です。

	コマンドまたはアクション	目的
ステップ 12	ip ospf transmit-delay seconds 例 : <pre>switch(config-if)# ip ospf transmit-delay 450 switch(config-if)#</pre>	LSA をネイバーに送信する推定時間間隔を秒で設定します。指定できる範囲は1～450です。デフォルトは1です。
ステップ 13	(任意) show ip ospf 例 : <pre>switch(config-if)# show ip ospf</pre>	OSPF に関する情報を表示します。
ステップ 14	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします

例

次に、lsa-group-pacing オプションで LSA フラッディングを制御する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# timers lsa-group-pacing 300
switch(config-router)# copy running-config startup-config
```

OSPFv2 インスタンスの再起動

OSPFv2 インスタンスを再起動できます。この処理では、インスタンスのすべてのネイバーが消去されます。

OSPFv2 インスタンスを再起動して、関連付けられたすべてのネイバーを削除するには、次のコマンドを使用します。

手順の概要

1. restart ospf instance-tag

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	restart ospf instance-tag 例 : <pre>switch(config)# restart ospf 201</pre>	OSPFv2 インスタンスを再起動して、すべてのネイバーを削除します。

仮想化による OSPFv2 の設定

複数の OSPFv2 インスタンスを作成することができます。また、複数の VRF を作成し、各 VRF で同じ OSPFv2 インスタンスまたは複数の OSPFv3 インスタンスを使用することもできます。VRF に OSPFv2 インスタンスを割り当てることができます。



(注) インターフェイスの VRF を設定した後に、インターフェイスの他のすべてのパラメータを設定します。インターフェイスの VRF を設定すると、そのインターフェイスのすべての設定が削除されます。

始める前に

OSPF 機能を有効にしてあることを確認します ([OSPFv2 機能の有効化](#)のセクションを参照)。

手順の概要

1. **configure terminal**
2. **vrf context vrf-name**
3. **router ospf instance-tag**
4. **vrf vrf-name**
5. (任意) **maximum-paths path**
6. **interface interface-type slot/port**
7. **no switchport**
8. **vrf member vrf-name**
9. **ip address ip-prefix/length**
10. **ip router ospf instance-tag area area-id**
11. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	vrf context vrf-name 例 : <pre>switch(config)# vrf context RemoteOfficeVRF switch(config-vrf)#</pre>	新しい VRF を作成し、VRF 設定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 instance-tag 例 : <pre>switch(config-vrf)# router ospf 201 switch(config-router)#</pre>	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 4	vrf vrf-name 例 : <pre>switch(config-router)# vrf RemoteOfficeVRF switch(config-router-vrf)#</pre>	VRF 設定モードを開始します。
ステップ 5	(任意) maximum-paths path 例 : <pre>switch(config-router-vrf)# maximum-paths 4</pre>	この VRF のルート テーブル内の宛先への、同じ OSPFv2 パスの最大数を設定します。この機能は、ロード バランシングに使用されます。
ステップ 6	interface interface-type slot/port 例 : <pre>switch(config-router-vrf)# interface ethernet 1/2 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 7	no switchport 例 : <pre>switch(config-if)# no switchport</pre>	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 8	vrf member vrf-name 例 : <pre>switch(config-if)# vrf member RemoteOfficeVRF</pre>	このインターフェイスを VRF に追加します。
ステップ 9	ip address ip-prefix/length 例 : <pre>switch(config-if)# ip address 192.0.2.1/16</pre>	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 10	ip router ospf instance-tag area area-id 例 : <pre>switch(config-if)# ip router ospf 201 area 0</pre>	このインターフェイスを OSPFv2 インスタンスおよび設定エリアに割り当てます。
ステップ 11	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします

例

次に、VRF を作成して、その VRF にインターフェイスを追加する例を示します。

```
switch# configure terminal
switch(config)# vrf context NewVRF
switch(config)# router ospf 201
switch(config)# interface ethernet 1/2
switch(config-if)# vrf member NewVRF
switch(config-if)# ip address 192.0.2.1/16
switch(config-if)# ip router ospf 201 area 0
switch(config-if)# copy running-config startup-config
```

OSPFv2 設定の確認

OSPFv2 設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ip ospf	OSPFv2 設定を表示します。
show ip ospf border-routers [vrf {vrf-name all default management}]	OSPFv2 境界ルータ設定を表示します。
show ip ospf database [vrf {vrf-name all default management}]	OSPFv2 リンクステート データベースの要約を表示します。
show ip ospf interface number [vrf {vrf-name all default management}]	OSPFv2 インターフェイス設定を表示します。
show ip ospf lsa-content-changed-list neighbor-id interface-type number [vrf {vrf-name all default management}]	変更された OSPFv2 LSA を表示します。
show ip ospf neighbors [neighbor-id] [detail] [interface-type number] [vrf {vrf-name all default management}] [summary]	OSPFv2 ネイバーの一覧を表示します。
show ip ospf request-list neighbor-id interface-type number [vrf {vrf-name all default management}]	OSPFv2 リンクステート要求の一覧を表示します。
show ip ospf retransmission-list neighbor-id interface-type number [vrf {vrf-name all default management}]	OSPFv2 リンクステート再送の一覧を表示します。
show ip ospf route [ospf-route] [summary] [vrf {vrf-name all default management}]	内部 OSPFv2 ルートを表示します。
show ip ospf summary-address [vrf {vrf-name all default management}]	OSPFv2 サマリ アドレスに関する情報を表示します。

コマンド	目的
show ip ospf virtual-links [brief] [vrf { <i>vrf-name</i> all default management }]	OSPFv2 仮想リンクに関する情報を表示します。
show ip ospf vrf { <i>vrf-name</i> all default management }	VRF ベースの OSPFv2 設定に関する情報を表示します。
show running-configuration ospf	現在実行中の OSPFv2 設定を表示します。

OSPFv2 統計情報の表示

OSPFv2 統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
show ip ospf policy statistics area <i>area-id</i> filter-list { in out } [vrf { <i>vrf-name</i> all default management }]	エリアの OSPFv2 ルート ポリシー統計情報を表示します。
show ip ospf policy statistics redistribute { bgp direct eigrp ospf rip static } vrf { <i>vrf-name</i> all default management }	OSPFv2 ルート ポリシー統計情報を表示します。
show ip ospf statistics [vrf { <i>vrf-name</i> all default management }]	OSPFv2 イベント カウンタを表示します。
show ip ospf traffic [interface - <i>type number</i>] [vrf { <i>vrf-name</i> all default management }]	OSPFv2 パケット カウンタを表示します。

OSPFv2 の設定例

次に、OSPFv2 を設定する例を示します。

```
feature ospf
router ospf 201
router-id 290.0.2.1

interface ethernet 1/2
no switchport
ip router ospf 201 area 0.0.0.10
ip ospf authentication
ip ospf authentication-key 0 mypass
```

その他の参考資料

OSPF の実装に関する詳細情報については、次のページ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
ルート マップ	Route Policy Manager の設定 (443 ページ)

MIB

MIB	MIB のリンク
• OSPF-MIB • ~~OSPF-TRAP~~MIB	MIBを検索してダウンロードするには、次の MIB ロケータ に移動します。



第 6 章

OSPFv3 の設定

この章では、Cisco NX-OS デバイスで IPv6 ネットワーク用の Open Shortest Path First version 3 (OSPFv3) を設定する方法について説明します。

この章は、次の項で構成されています。

- [OSPFv3 について \(125 ページ\)](#)
- [OSPFv3 の前提条件 \(140 ページ\)](#)
- [OSPFv3 の注意事項および制約事項 \(140 ページ\)](#)
- [デフォルト設定 \(141 ページ\)](#)
- [基本的なOSPFv3の設定 \(141 ページ\)](#)
- [高度なOSPFv3の設定 \(153 ページ\)](#)
- [暗号化および認証の構成 \(176 ページ\)](#)
- [OSPFv3 の設定の確認 \(189 ページ\)](#)
- [OSPFv3 のモニタリング \(190 ページ\)](#)
- [OSPFv3 の設定例 \(191 ページ\)](#)
- [関連項目 \(191 ページ\)](#)
- [その他の参考資料 \(191 ページ\)](#)

OSPFv3 について

OSPFv3 は、IETF リンクステート プロトコル ([概要 \(3 ページ\)](#) を参照) です。OSPFv3 ルータは、hello パケットと呼ばれる特別なメッセージを各 OSPF 対応インターフェイスに送信し、他の OSPFv3 隣接ルータを探索します。ネイバー ルータが発見されると、この 2 台のルータは hello パケットの情報を比較して、両者の設定に互換性のあるかどうかを判定します。これらのネイバー ルータは隣接を確立しようとします。つまり、両者のリンクステート データベースを同期させて、確実に同じ OSPFv3 ルーティング情報を持つようにします。隣接ルータは、各リンクの稼働状態に関する情報、リンクのコスト、およびその他のあらゆるネイバー情報を含むリンクステート アドバタイズメント (LSA) を共有します。これらのルータはその後、受信した LSA をすべての OSPF イネーブル インターフェイスにフラッドします。これにより、すべての OSPFv3 ルータのリンクステート データベースが最終的に同じになります。すべての OSPFv3 ルータのリンクステート データベースが同じになると、ネットワークは

収束します（「[コンバージェンス](#)」を参照）。その後、各ルータは、ダイクストラの最短パス優先（SPF）アルゴリズムを使用して、自身のルートテーブルを構築します。

OSPFv3 ネットワークは、複数のエリアに分割できます。ルータは、ほとんどの LSA を 1 つのエリア内だけに送信するため、OSPF 対応ルータの CPU とメモリの要件が緩やかになります。

OSPFv3 は IPv6 をサポートしています。IPv4 向けの OSPF の詳細については、[OSPFv2 の設定 \(75 ページ\)](#) を参照してください。

OSPFv3 と OSPFv2 の比較

OSPFv3 プロトコルの大半は OSPFv2 と同じです。OSPFv3 は RFC 2740 に記載されています。

OSPFv3 プロトコルと OSPFv2 プロトコルの重要な相違点は、次のとおりです。

- OSPFv2 を拡張した OSPFv3 では、IPv6 ルーティング プレフィックスとサイズの大きい IPv6 アドレスのサポートを提供しています。
- OSPFv3 の LSA は、アドレスとマスクではなく、プレフィックスとプレフィックス長として表現されます。
- ルータ ID とエリア ID は 32 ビット数で、IPv6 アドレスとは無関係です。
- OSPFv3 では、ネイバー探索およびその他の機能にリンクローカル IPv6 アドレスを使用します。
- OSPFv3 は、IPv6 認証トレーラ（RFC 6506）または IPSec（RFC 4552）を使用できます。ただし、Cisco NX-OS は RFC 6506 をサポートしておらず、Cisco NX-OS リリース 7.0(3)I3(1)以降の RFC 4552 の一部のみをサポートしています。
- OSPFv3 では、LSA タイプが再定義されています。

Hello パケット

OSPFv3 ルータは、すべての OSPF イネーブル インターフェイスに hello パケットを定期的に送信します。ルータがこの hello パケットを送信する頻度は、インターフェイスごとに設定された hello 間隔により決定されます。OSPFv3 は、hello パケットを使用して、次のタスクを実行します。

- ネイバー探索
- キープアライブ
- 双方向通信
- 指定ルータの選定（「[指定ルータ](#)」セクションを参照してください）

hello パケットには、リンクの OSPFv3 コスト割り当て、hello 間隔、送信元ルータのオプション機能など、送信元の OSPFv3 インターフェイスとルータに関する情報が含まれます。これらの hello パケットを受信する OSPFv3 インターフェイスは、設定に受信インターフェイスの設

定との互換性があるかどうかを判定します。互換性のあるインターフェイスはネイバーと見なされ、ネイバー テーブルに追加されます（「[ネイバー](#)」の項を参照してください）。

hello パケットには、送信元インターフェイスが通信したルータのルータ ID のリストも含まれます。受信インターフェイスが、このリストで自身の ID を見つけた場合は、2 つのインターフェイス間で双方向通信が確立されます。

OSPFv3 は、hello パケットをキープアライブメッセージとして使用して、ネイバーが通信を継続中であるかどうかを判定します。ルータが設定されたデッド間隔（通常は hello 間隔の倍数）で hello パケットを受信しない場合、そのネイバーはローカル ネイバー テーブルから削除されます。

ネイバー情報

ネイバーであるとは見なされるようにするには、リモートインターフェイスと互換性があるように OSPFv3 インターフェイスを設定しておく必要があります。この 2 つの OSPFv3 インターフェイスで、次の基準が一致している必要があります。

- hello 間隔
- デッド間隔
- エリア ID（「[エリア](#)」の項を参照）
- 認証
- オプション機能

一致する場合は、次の情報がネイバー テーブルに入力されます。

- ネイバー ID：ネイバー ルータのルータ ID
- 優先度：ネイバー ルータの優先度。プライオリティは、指定ルータの選定（「[指定ルータ](#)」を参照）に使用されます。
- 状態：ネイバーから通信があったか、双方向通信の確立処理中であるか、リンクステート情報を共有しているか、または完全な隣接関係が確立されたかを示します。
- デッドタイム：このネイバーから最後の hello パケットを受信したあとに経過した時間を示します。
- リンクローカル IPv6 アドレス：ネイバーのリンクローカル IPv6 アドレス
- 指定ルータ：ネイバーが指定ルータ、またはバックアップ指定ルータとして宣言されたかどうかを示します（「[指定ルータ](#)」の項を参照）。
- ローカルインターフェイス：このネイバーの hello パケットを受信したローカルインターフェイス。

最初の hello パケットが新規ネイバーから受信されると、そのネイバーは、初期化状態のネイバーテーブルに入力されます。いったん双方向通信が確立されると、ネイバー状態は双方向となります。2 つのインターフェイスが互いのリンクステートデータベースを交換するため、次

に ExStart および交換状態となります。これらがすべて完了すると、ネイバーは完全な状態へと移行し、これが完全な隣接関係となります。ネイバーは、デッド間隔で hello パケットをまったく送信しない場合は、ダウン状態に移行し、隣接とは見なされなくなります。

隣接関係

すべてのネイバーが隣接関係を確立するわけではありません。ネットワークタイプと確立された指定ルータに応じて、完全な隣接関係を確立して、すべてのネイバーと LSA を共有するものと、そうでないものがあります。詳細については、「[指定されたルータ](#)」セクションを参照してください。

隣接関係は、OSPFv3 のデータベース説明パケット、リンク状態要求パケット、およびリンク状態更新パケットを使用して確立されます。データベース説明パケットには、ネイバーのリンクステートデータベースからの LSA ヘッダーが含まれます（「[リンク状態データベース](#)」の項を参照）。ローカルルータは、これらのヘッダーを自身のリンクステートデータベースと比較して、新規の LSA か、更新された LSA かを判定します。ローカルルータは、新規または更新の情報を必要とする各 LSA について、リンク状態要求パケットを送信します。これに対し、ネイバーはリンク状態更新パケットを返信します。このパケット交換は、両方のルータのリンクステート情報が同じになるまで続きます。

指定ルータ

複数のルータを含むネットワークは、OSPFv3 特有の状況です。すべてのルータがネットワークで LSA をフラッドした場合は、同じリンクステート情報が複数の送信元から送信されます。ネットワークのタイプによっては、OSPFv3 は指定ルータ（DR）という 1 台のルータを使用して LSA のフラッドを制御し、OSPFv3 の残りの部分に対してネットワークを代表する役割をさせる場合があります（「[エリア](#)」の項を参照）。DR がダウンした場合、OSPFv3 はバックアップ指定ルータ（BDR）を選択します。DR がダウンすると、OSPFv3 はこの BDR を使用します。

ネットワークタイプは次のとおりです。

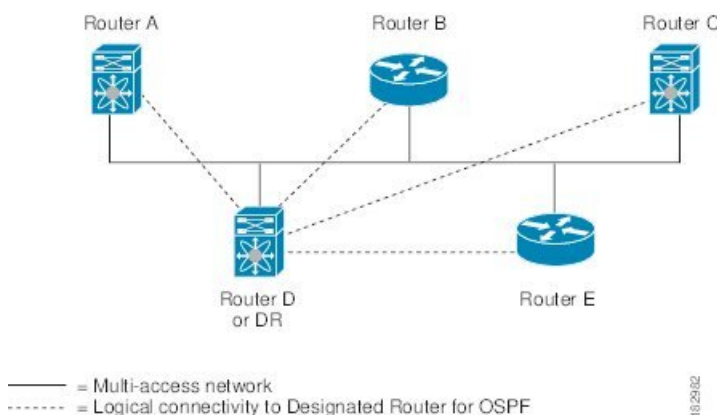
- ポイントツーポイント：2 台のルータ間にのみ存在するネットワーク。ポイントツーポイント ネットワーク上の全ネイバーは隣接関係を確立し、DR は存在しません。
- ブロードキャスト：ブロードキャストトラフィックが可能なイーサネットなどの共有メディア上で通信できる複数のルータを持つネットワーク。OSPFv3 ルータは DR および BDR を確立し、これらにより、ネットワーク上の LSA フラッドを制御します。OSPFv3 は、よく知られている IPv6 マルチキャストアドレス FF02::5 および MAC アドレス 0100.5300.0005 を使用して、ネイバーと通信します。

DR と BDR は、hello パケット内の情報に基づいて選択されます。インターフェイスは hello パケットの送信時に、どれが DR および BDR かわかっている場合は、優先フィールドと、DR および BDR フィールドを設定します。ルータは、hello パケットの DR および BDR フィールドで宣言されたルータと優先フィールドに基づいて、選定手順を実行します。最終的に OSPFv3 は、最も大きいルータ ID を DR および BDR として選択します。

他のルータはすべて DR および BDR と隣接関係を確立し、IPv6 マルチキャストアドレス FF02::6 を使用して、LSA 更新情報を DR と BDR に送信します。次の図は、すべてのルータと DR との隣接関係を示しています。

DR は、ルータ インターフェイスに基づいています。1 つのネットワークの DR であるルータは、別のインターフェイス上の他のネットワークの DR となることはできません

図 21: マルチアクセス ネットワークの DR



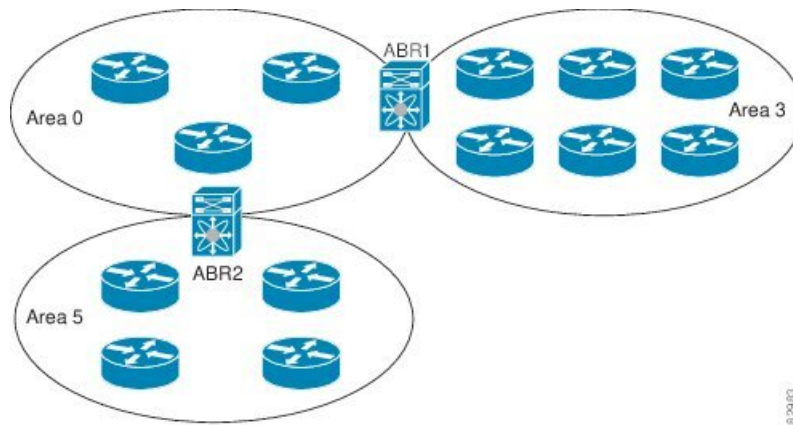
エリア

OSPFv3 ネットワークを複数のエリアに分割すると、ルータに要求される OSPFv3 の CPU とメモリに関する要件を制限できます。エリアとは、ルータの論理的な区分で、OSPFv3 ドメイン内にリンクして別のサブドメインを作成します。LSA フラッドイングはエリア内でのみ発生し、リンクステートデータベースはエリア内のリンクにのみ制限されます。定義されたエリア内のインターフェイスには、エリア ID を割り当てることができます。エリア ID は、10.2.3.1 などの、数字またはドット付き 10 進表記で表現される 32 ビット値です。

Cisco NX-OS はエリアを常にドット付き 10 進表記で表示します。

OSPFv3 ネットワーク内に複数のエリアを定義する場合は、0 という予約されたエリア ID を持つバックボーンエリアも定義する必要があります。エリアが複数ある場合は、1 台以上のルータがエリア境界ルータ (ABR) となります。ABR は、バックボーンエリアと他の 1 つ以上の定義済みエリアの両方に接続します (次の図を参照)。

図 22: OSPFv3 エリア



ABR には、接続するエリアごとに個別のリンクステートデータベースがあります。ABR は、接続したエリアの 1 つからバックボーン エリアにエリア間プレフィックス（タイプ 3）LSA（「[ルート集約](#)」セクションを参照）を送信します。バックボーンエリアは、1 つのエリアに関する集約情報を別のエリアに送信します。**OSPFv3 エリア**の図では、エリア 0 が、エリア 5 に関する集約情報をエリア 3 に送信しています。

OSPFv3 では、自律システム境界ルータ（ASBR）という、もう 1 つのルータ タイプも定義されています。このルータは、OSPFv3 エリアを別の自律システム（AS）に接続します。自律システムとは、単一の技術的管理エンティティにより制御されるネットワークです。OSPFv3 は、そのルーティング情報を別の自律システムに再配布したり、再配布されたルートを別の自律システムから受信したりできます。詳細については、「[詳細な機能](#)」のセクションを参照してください。

リンクステートアドバタイズメント

OSPFv3 はリンクステートアドバタイズメント（LSA）を使用して、固有のルーティングテーブルを構築します。

LSA タイプ

次のテーブルに、Cisco NX-OS でサポートされる LSA タイプを示します。

表 11: LSA タイプ

名前	名前	説明
1	ルータ LSA	すべてのルータが送信する LSA。この LSA には、すべてのリンクの状態とコストが含まれますが、プレフィックス情報は含まれません。ルータ LSA は SPF 再計算をトリガーします。ルータ LSA は 指定ルータ (77 ページ) ローカル OSPFv3 エリアにフラッディングされます。
2	ネットワーク LSA	DR が送信する LSA。この LSA には、マルチアクセス ネットワーク内のすべてのルータの一覧が含まれますが、プレフィックス情報は含まれません。ネットワーク LSA は SPF 再計算をトリガーします。 「 指定ルータ 」のセクションを参照してください。
3	エリア間プレフィックス LSA	ABR が、ローカルエリア内の宛先ごとに外部エリアに送信する LSA。この LSA には、境界ルータからローカルの宛先へのリンク コストが含まれます。「 エリア 」のセクションを参照してください。
4	エリア間ルータ LSA	エリア境界ルータが外部エリアに送信する LSA。この LSA は、リンク コストを ASBR のみにアドバタイズします。 「 エリア 」の項を参照してください。

名前	名前	説明
5	AS 外部 LSA	ASBR が生成する LSA。この LSA には、外部自律システム宛先へのリンク コストが含まれます。AS 外部 LSA は、自律システム全体にわたってフラッディングされます。「 エリア 」の項を参照してください。
7	タイプ 7 LSA	ASBR が NSSA 内で生成する LSA。この LSA には、外部自律システム宛先へのリンク コストが含まれます。タイプ 7 LSA は、ローカル NSSA 内のみでフラッディングされます。「 エリア 」の項を参照してください。
8	リンク LSA	リンクローカル フラッディング スコープを使用して、すべてのルータによって送信される LSA（「 フラッディングと LSA グループ ペーシング 」のセクションを参照してください）。この LSA には、このリンクのリンクローカル アドレスと IPv6 アドレスが含まれます。
9	エリア内プレフィックス LSA	すべてのルータが送信する LSA。この LSA には、プレフィックスまたはリンク状態へのあらゆる変更が含まれます。エリア内プレフィックス LSA はローカル OSPFv3 エリアにフラッディングされます。この LSA は SPF 再計算をトリガーしません。

名前	名前	説明
11	猶予 LSA	再起動されるルータが、リンクローカルフラッドディングスコープを使用して送信する LSA。この LSA は、OSPFv3 のグレースフル リスタートに使用されます。「 ハイ アベイラビリティおよびグレースフル リスタート 」を参照してください。

リンク コスト

各 OSPFv3 インターフェイスは、リンク コストを割り当てられています。このコストは任意の数字です。デフォルトでは、Cisco NX-OS が、設定された参照帯域幅をインターフェイス帯域幅で割った値をコストとして割り当てます。デフォルトでは、参照帯域幅は 40 Gbps です。リンク コストは各リンクに対して、LSA 更新情報で伝えられます。

フラッドディングと LSA グループ ペーシング

OSPFv3 は、LSA のタイプに応じて、ネットワークのさまざまなセクションに LSA の更新をフラッドディングします。OSPFv3 は、次のフラッドディング スコープを使用します

- **リンク ローカル** : LSA は、ローカル リンク上でのみフラッドディングされます。リンク LSA および猶予 LSA に使用されます。
- **エリアローカル** : LSA は、単一の OSPF エリア全体にのみフラッドディングされます。ルータ LSA、ネットワーク LSA、エリア間プレフィックス LSAs、エリア間ルータ LSA、およびエリア内プレフィックス LSA に使用されます。
- **AS スコープ** : LSA は、ルーティング ドメイン全体にフラッドディングされます。AS スコープは AS 外部 LSA に使用されます。

LSA フラッドディングにより、ネットワーク内のすべてのルータが同じルーティング情報を持つことが保証されます。LSA フラッドディングは、OSPFv3 エリアの設定により異なります（「[エリア](#)」の項を参照）。LSA は、リンクステート リフレッシュ時間に基づいて（デフォルトでは 30 分ごとに）フラッドディングされます。各 LSA には、リンクステート リフレッシュ時間が設定されています。

ネットワークの LSA 更新情報のフラッドディング レートは、LSA グループ ペーシング機能を使用して制御できます。LSA グループ ペーシングにより、CPU またはバッファの使用率を低下させることができます。この機能により、同様のリンクステート リフレッシュ時間を持つ LSA がグループ化されるため、OSPFv3 で、複数の LSA を 1 つの OSPFv3 更新メッセージにまとめることが可能となります。

デフォルトでは、相互のリンクステートリフレッシュ時間が 10 秒以内の LSA が、同じグループに入れられます。この値は、大規模なリンクステートデータベースでは低く、小規模のデータベースでは高くして、ネットワーク上の OSPFv3 負荷を最適化する必要があります。

リンクステート データベース

各ルータは、OSPFv3 ネットワーク用のリンクステートデータベースを保持しています。このデータベースには、収集されたすべての LSA が含まれ、ネットワークを通過するすべてのルートに関する情報が格納されます。OSPFv3 は、この情報を使用して、各宛先への最適なパスを計算し、この最適なパスをルーティングテーブルに入力します。

MaxAge と呼ばれる設定済みの時間間隔で受信された LSA 更新情報がまったくない場合は、リンクステートデータベースから LSA が削除されます。ルータは、LSA を 30 分ごとに繰り返してフラッドイングし、正確なリンクステート情報が期限切れで削除されるのを防ぎます。Cisco NX-OS は、すべての LSA が同時にリフレッシュされるのを防ぐために、LSA グループ機能をサポートしています。詳細については、「[フラッドイングと LSA グループ ペーシング](#)」のセクションを参照してください。

マルチエリア隣接関係 (Multi-Area Adjacency)

OSPFv3 マルチエリア隣接関係により、複数のエリアにあるプライマリ インターフェイス上にリンクを設定できます。このリンクは、それらのエリア内の優先されるエリア内リンクになります。マルチエリア隣接関係では、OSPFv3 エリアにポイントツーポイントの番号なしリンクを確立し、そのエリアにトポロジパスを提供します。プライマリ隣接関係はリンクを使用して、ネイバーステートが full の場合に、ルータ LSA で対応するエリアの番号なしポイントツーポイント リンクをアドバタイズします。

マルチエリア インターフェイスは、OSPF の既存のプライマリ 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ネイバー ルータ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。詳細については、[マルチエリアの隣接関係の設定 \(159 ページ\)](#) を参照してください。

OSPFv3 と IPv6 ユニキャスト RIB

OSPFv3 は、リンクステートデータベースでダイクストラの SPF アルゴリズムを実行します。このアルゴリズムにより、パス上の各リンクのリンクコストの合計に基づいて、各宛先への最適なパスが選択されます。選択された各宛先への最短パスが OSPFv3 ルートテーブルに入力されます。OSPFv3 ネットワークが収束すると、このルート テーブルは IPv6 ユニキャスト RIB にデータを提供します。OSPFv3 は IPv6 ユニキャスト RIB と通信し、次の動作を行います。

- ルートの追加または削除
- 他のプロトコルからのルートの再配布への対応

- 変更されていない OSPFv3 ルートの削除およびスタブ ルータ アドバタイズメントを行うためのコンバージェンス更新情報を提供します（「[複数の OSPFv3 インスタンス \(Multiple OSPFv3 Instances\)](#)」を参照）。

さらに OSPFv3 は、変更済みダイクストラ アルゴリズムを実行して、エリア間プレフィックス、エリア間ルータ、AS 外部、タイプ 7、およびエリア内プレフィックス（タイプ 3、4、5、7、8）の各 LSA の変更の高速再計算を行います。

アドレス ファミリのサポート

Cisco NX-OS は、ユニキャスト IPv6 やマルチキャスト IPv6 などの複数のアドレス ファミリをサポートしています。アドレス ファミリに特有の OSPFv3 機能は、次のとおりです。

- デフォルト ルート
- ルート集約
- ルートの再配布
- 境界ルータのフィルタ リスト
- SPF 最適化

これらの機能の設定時に IPv6 ユニキャスト 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 unicast** コマンドを使用します。

認証および暗号化

OSPFv3 メッセージに認証を設定して、ネットワークでの不正な、または無効なルーティング 更新を防止できます。

RFC 4552 は、IPv6 認証ヘッダー (AH) またはカプセル化セキュリティ ペイロード (ESP) 拡張ヘッダーを使用して、OSPFv3 への認証を提供します。Cisco NX-OS 7.0(3)I3(1) 以降、Cisco NX-OS は、IPv6 AH ヘッダーを使用して OSPFv3 パケットを認証することにより、RFC 4552 をサポートします。

Cisco NX-OS は、IP セキュリティ (IPSec) 認証方式と、メッセージダイジェスト 5 (MD5) またはセキュア ハッシュ アルゴリズム 1 (SHA1) アルゴリズムをサポートして、OSPFv3 パケットを認証します。OSPFv3 IPSec 認証は、コマンドを使用する静的キーのみをサポートします。

Cisco NX-OS は、OSPFv3 メッセージの暗号化と認証の両方に IPSec ESP 方式もサポートしています。暗号化は、ESP 暗号化の AES または 3DES アルゴリズムと、ESP 認証の SHA-1 または NULL をサポートします。

Cisco NX-OS リリース 10.4(1)F 以降、Cisco NX-OS は、キーチェーン オプションを使用した暗号化または認証アルゴリズムとキーの構成をサポートしています。

IPSec 暗号化または認証は、OSPFv3 プロセス、エリア、インターフェイス、あるいはその両方に対して構成可能です。認証設定は、プロセスからエリア、インターフェイス レベルに継承さ

れます。認証が3つのレベルすべてで構成されている場合、インターフェイス構成がプロセスおよびエリア構成よりも優先され、エリア構成はプロセスレベルよりも優先されます。

高度な機能

Cisco NX-OS は、ネットワークでの OSPFv3 の可用性やスケーラビリティを向上させる高度な OSPFv3 機能をサポートしています。

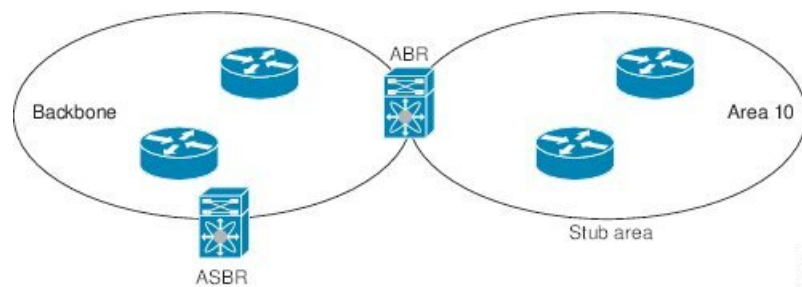
スタブエリア

エリアをスタブエリアにすると、エリアでフラッディングされる外部ルーティング情報の量を制限できます。スタブエリアとは、AS 外部（タイプ 5）LSA（「[リンク ステート アドバタイズメント](#)」のセクションを参照）が許可されないエリアです。これらの LSA は通常、外部ルーティング情報を伝播するためにローカル自律システム全体でフラッディングされます。スタブエリアには、次の要件があります。

- スタブエリア内のすべてのルータはスタブ ルータです。「[スタブ ルーティング](#)」の項を参照してください。
- スタブエリアには ASBR ルータは存在しません。
- スタブエリアには仮想リンクを設定できません。

次の図に示す OSPFv3 自律システムでは、エリア 0.0.0.10 内のルータはすべて、外部自律システムに到達するために ABR を通過しなければなりません。エリア 0.0.0.10 は、スタブエリアとして設定できます。

図 23: スタブエリア



スタブエリアは、外部自律システムへのバックボーンエリアを通過する必要があるすべてのトラフィックにデフォルトルートを使用します。デフォルトルートは、プレフィックス長がIPv6 向けに 0 に設定されたエリア間プレフィックス LSA です。

Not-So-Stubby Area

Not-So-Stubby Area (NSSA) は、スタブエリアに似ていますが、NSSA では、再配布を使用して NSSA 内で自律システム外部ルートをインポートできる点が異なります。NSSA ASBR はこれらのルートを実再配布し、タイプ 7 LSA を生成して NSSA 全体にフラッディングします。または、このタイプ 7 LSA を AS 外部（タイプ 5）LSA に変換するよう、NSSA を他のエリアに接続する ABR を設定することができます。こうすると、ABR は、これらの AS 外部 LSA を

OSPFv3 自律システム全体にフラッドイングします。変換中は集約とフィルタリングがサポートされます。type-7 LSA の詳細については、「[リンクステートアドバタイズ](#)」のセクションを参照してください。

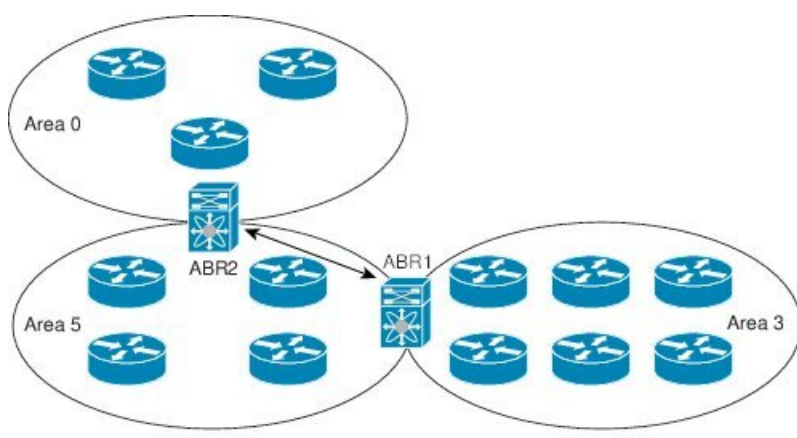
たとえば、OSPFv3 を使用する中央サイトを、異なるルーティングプロトコルを使用するリモートサイトに接続するときに NSSA を使用すると、管理作業を簡素化できます。NSSA を使用する前は、企業サイトの境界ルータとリモートルータの間の接続を OSPFv3 スタブエリアとして実行できませんでした。これは、リモートサイトへのルートはスタブエリア内に再配布できないためです。NSSA が実装されたことで、企業ルータとリモートルータ間のエリアを NSSA として定義することにより、NSSA で OSPFv3 を拡張してリモート接続をカバーできます（[NSSA の設定 \(157 ページ\)](#) セクションを参照）。

バックボーンエリア 0 を NSSA にできません。

仮想リンク

仮想リンクを使用すると、物理的に直接接続できない場合に、OSPFv3 エリア ABR をバックボーンエリア ABR に接続できます。次の図には、エリア 3 をエリア 5 経由でバックボーンエリアに接続する仮想リンクを示します。

図 24: 仮想リンク



また、仮想リンクを使用して、分割エリアから一時的に回復できます。分割エリアは、エリア内のリンクがダウンしたために隔離された一部のエリアで、ここからはバックボーンエリアへの代表 ABR に到達できません。

ルートの再配布

OSPFv3 は、ルート再配布を使用して、他のルーティングプロトコルからルートを学習できます。[ルートの再配布](#)のセクションを参照してください。リンクコストをこれらの再配布されたルートに割り当てるか、またはデフォルトリンクコストを再配布されたすべてのものに割り当てるよう、OSPFv3 を設定します。

ルート再配布では、ルートマップを使用して、再配布する外部ルートを管理します。再配布を指定したルートマップを設定して、どのルートが OSPFv2 に渡されるかを制御する必要があります。ルートマップを使用すると、宛先、送信元プロトコル、ルートタイプ、ルートタグな

どの属性に基づいて、ルートをフィルタリングできます。ルートマップを使用して、これらの外部ルートがローカル OSPFv3 AS でアドバタイズされる前に AS 外部（タイプ 5）LSA および NSSA 外部（タイプ 7）LSA のパラメータを変更できます。詳細については、「[Route Policy Manager の設定（443 ページ）](#)」を参照してください。

ルート集約

OSPFv3 は学習したすべてのルートをあらゆる OSPF 対応ルータと共有するので、ルート集約を使用して、それぞれの OSPF 対応ルータにフラッドされる固有のルート の数を削減した方がよい場合もあります。ルート集約により、より具体的な複数のアドレスが、すべての具体的なアドレスを表す 1 つのアドレスに置き換えられるため、ルートテーブルが簡素化されます。たとえば、2010:11:22:0:1000::1 と 2010:11:22:0:2000:679:1 を 1 つの集約アドレス 2010:11:22::/32 に置き換えることができます。

一般的には、エリア境界ルータ（ABR）の境界ごとに集約します。集約は 2 つのエリアの間でも設定できますが、バックボーンの方に集約する方が適切です。こうすると、バックボーンがすべての集約アドレスを受信し、すでに集約されているそれらのアドレスを他のエリアに投入できるためです。集約には、次の 2 タイプがあります。

- エリア間ルート集約
- 外部ルート集約

エリア間ルート集約は ABR 上で設定し、自律システム内のエリア間のルートを集約します。集約の利点を生かすには、これらのアドレスを 1 つの範囲内にまとめることができるように、連続するネットワーク番号をエリア内で割り当てます。

外部ルート集約は、ルート再配布を使用して OSPFv3 に投入される外部ルートに特有のルート集約です。集約する外部の範囲が連続していることを確認する必要があります。異なる 2 台のルータからの重複範囲を集約すると、誤った宛先にパケットが送信される原因となる場合があります。外部ルート集約は、ルートを OSPF に再配布している ASBR で設定してください。

集約アドレスの設定時に Cisco NX-OS は、ルーティング ブラック ホールおよびルート ループを防ぐために、集約アドレスの廃棄ルートを自動的に設定します。

高可用性およびグレースフル リスタート

Cisco NX-OS はハイ アベイラビリティをサポートしています。Cisco NX-OS システムでコールドリブートが発生した場合、ネットワークはシステムへのトラフィック転送を中止し、ネットワーク トポロジからシステムを削除します。このシナリオでは、OSPFv3 でステートレス リスタートが発生し、ローカルシステム上のすべての隣接関係が削除されます。Cisco NX-OS はスタートアップ構成を適用し、OSPFv3 がネイバーを再発見して隣接関係を再度確立します。

プロセスで問題が発生すると、OSPFv3 は自動的に再起動します。再起動後、プラットフォームがネットワーク トポロジから除外されないように、OSPFv3 はグレースフル リスタートを開始します。手動で OSPF を再起動すると、ステートフル スイッチオーバーと同様のグレースフル リスタートが実行されます。どちらの場合も、実行コンフィギュレーションが適用されます。

グレースフルリスタート、つまり、Nonstop Forwarding (NSF) では、処理の再起動中も OSPFv3 がデータ転送パス上に存在し続けます。OSPFv3 はリスタートの実行が必要になると、最初にリンクローカル猶予 (タイプ 11) LSA を送信します。この再起動中の OSPFv3 プラットフォームは NSF 対応と呼ばれます。

猶予 LSA には猶予期間が含まれます。猶予期間とは、ネイバー OSPFv3 インターフェイスは再起動中の OSPFv3 インターフェイスからの LSA を待つよう指定された時間です (通常、OSPFv3 は隣接関係を切断し、ダウン状態または再起動中の OSPFv3 インターフェイスからのすべての LSA を廃棄します)。参加するネイバーは、NSF ヘルパーと呼ばれ、再起動中の OSPFv3 インターフェイスから発信されたすべての LSA を、インターフェイスがまだ隣接しているかのように保持します。

再起動中の OSPFv3 インターフェイスが稼働を再開すると、ネイバーを再探索して隣接関係を確立し、LSA 更新情報の送信を再開します。この時点で、NSF ヘルパーは、グレースフルリスタートが完了したと認識します。



- (注) 再起動中の OSPFv3 インターフェイスが猶予期間の終了前に復旧しない場合、またはネットワークでトポロジの変更が発生した場合、OSPFv3 ネイバーは再起動中の OSPFv3 との隣接関係を切断し、通常の OSPFv3 再起動として扱います。



- (注) OSPFv3 のインサースビス ソフトウェア アップグレード (ISSU) をサポートするには、グレースフルリスタートを有効にする必要があります。グレースフルリスタートを無効にすると、この構成では ISSU をサポートできないことを伝える警告が Cisco NX-OS から出されます。

複数の OSPFv3 インスタンス

Cisco NX-OS は、OSPFv3 プロトコルの複数インスタンスをサポートしています。デフォルトでは、すべてのインスタンスが同じシステム ルータ ID を使用します。複数のインスタンスが同じ OSPFv3 自律システムにある場合は、各インスタンスのルータ ID を手動で設定する必要があります。

OSPFv3 ヘッダーには、特定の OSPFv3 インスタンスの OSPFv3 パケットを識別するためのインスタンス ID フィールドが含まれます。この OSPFv3 インスタンスを割り当てることができません。インターフェイスは、パケットヘッダーの OSPFv3 インスタンス ID が一致しない OSPFv3 パケットをすべてドロップします。

Cisco NX-OS では、インターフェイス上に 1 つの OSPFv3 インスタンスのみが許可されます。

SPF 最適化

Cisco NX-OS は、次の方法で SPF アルゴリズムを最適化します。

- ・ネットワーク (タイプ 2) LSA、エリア間プレフィックス (タイプ 3) LSA、および AS 外部 (タイプ 5) LSA 用部分 SPF: これらの LSA のいずれかが変更されると、Cisco NX-OS は、全体的な SPF 計算ではなく、高速部分計算を実行します。

- **SPF タイマー**：さまざまなタイマーを設定して、SPF 計算を制御できます。これらのタイマーには、後続の SPF 計算の幾何バックオフが含まれます。幾何バックオフにより、複数の SPF 計算による CPU 負荷が制限されます。

BFD

この機能では、双方向フォワーディング検出 (BFD) をサポートします。BFD は、転送パスの障害を高速で検出することを目的にした検出プロトコルです。BFD は 2 台の隣接デバイス間のサブセカンド障害を検出し、BFD の負荷の一部を、サポートされるモジュール上のデータプレーンに分散できるため、プロトコル hello メッセージよりも CPU を使いません。

仮想化のサポート

OSPFv3 は、仮想ルーティングおよび転送 (VRF) インスタンスをサポートしています。

OSPFv3 の前提条件

OSPFv3 の前提条件は次のとおりです。

- OSPFv3 を設定するための、ルーティングの基礎に関する詳しい知識がある。
- スイッチにログオンしている。
- リモート OSPFv3 ネイバーと通信可能な 1 つ以上の IPv6 用インターフェイスが設定されている。
- Enterprise Services ライセンスがインストールされている。
- OSPFv3 ネットワーク戦略と、ネットワークのプランニングが完成している。たとえば、複数のエリアが必要かどうかを決定します。
- OSPF が有効になっています ([OSPFv3 の有効化 \(142 ページ\)](#) セクションを参照)。
- Advanced Services ライセンスがインストールされている。
- IPv6 アドレス指定および基本設定に関する詳しい知識がある。IPv6 ルーティングおよびアドレス指定の詳細については、[IPv6 の設定 \(45 ページ\)](#) を参照してください。

OSPFv3 の注意事項および制約事項

OSPFv3 設定時の注意事項および制約事項は、次のとおりです。

- Cisco NX-OS は、ユーザがエリアを 10 進表記で入力するか、ドット付き 10 進表記で入力するかに関係なく、ドット付き 10 進表記でエリアを表示します。

- 仮想ポートチャネル (vPC) 環境で OSPFv3 を設定する場合は、コア スイッチ上のルータ コンフィギュレーション モードで次のタイマー コマンドを使用することにより、vPC ピアリンクがシャットダウンしたときに OSPF の高速コンバージェンスを実現します。

```
switch (config-router)# timers throttle spf 1 50 50
switch (config-router)# timers lsa-arrival 10
```

- Cisco NX-OS リリース 10.4(1)F 以降、Cisco NX-OS スイッチの OSPFv3 暗号化および認証 コマンドに対してキーチェーンのサポートが提供されます。

デフォルト設定

次の表に、OSPFv3 パラメータのデフォルト設定を示します。

表 12: **OSPFv3** のデフォルト パラメータ

パラメータ	デフォルト
hello 間隔	10 秒
デッド間隔	40 秒
グレースフル リスタートの猶予期間	60 秒
グレースフル リスタートの通知期間	15 秒
OSPFv3 機能	ディセーブル
スタブルータ アドバタイズメントの宣言期間	600 秒
リンク コスト計算の参照帯域幅	40 Gbps
LSA 最小到着時間	1000 ミリ秒
LSA グループ ペーシング	10 秒
SPF 計算初期遅延時間	0 ミリ秒
SPF 計算ホールド タイム	5000 ミリ秒
SPF 計算初期遅延時間	0 ミリ秒

基本的な OSPFv3 の設定

OSPFv3 は、OSPFv3 ネットワークを設計したあとに設定します。

OSPFv3の有効化

OSPFv3 を構成する前に、OSPFv3 を有効にする必要があります。

手順の概要

1. **configure terminal**
2. **feature ospfv3**
3. (任意) **show feature**
4. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	feature ospfv3 例 : switch(config)# feature ospfv3	OSPFv3 を有効にします。
ステップ 3	(任意) show feature 例 : switch(config)# show feature	有効および無効にされた機能を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	この設定変更を保存します。

例

OSPFv3 機能を無効にして、関連付けられている構成をすべて削除するには、構成モードで次のコマンドを使用します。

コマンド	目的
no feature ospfv3 例 : switch(config)# no feature ospfv3	OSPFv3 機能を無効にして、関連付けられた設定をすべて削除します。

OSPFv3 インスタンスの作成

OSPFv3 設定の最初のステップは、インスタンスまたは OSPFv3 インスタンスの作成です。作成した OSPFv3 インスタンスには、一意のインスタンス タグを割り当てます。インスタンス タグは任意の文字列です。各 OSPFv3 インスタンスには、省略可能な次のパラメータも設定できます。

- **Router ID** : この OSPFv3 インスタンスのルータ ID を設定します。このパラメータを使用しない場合は、ルータ ID 選択アルゴリズムが使用されます。詳細については、「[ルータ ID](#)」のセクションを参照してください。
- **Administrative distance** : ルーティング情報の送信元の信頼性をランク付けします。詳細については、「[アドミニストレーティブディスタンス](#)」のセクションを参照してください。
- **Log adjacency changes** : OSPFv3 ネイバーの状態が変化するたびにシステムメッセージを作成します。
- **Maximum paths** : OSPFv3 が、特定の宛先についてルート テーブルにインストールする同等パスの最大数を設定します。このパラメータは、複数パス間のロードバランシングに使用します。
- **Reference bandwidth** : ネットワークの算出 OSPFv3 コスト メトリックを制御します。算出コストは、参照帯域幅をインターフェイス帯域幅で割った値です。算出コストは、ネットワークが OSPFv3 インスタンスに追加されるときにリンクコストを割り当てると、無効にすることができます。詳細については、「[OSPFv3でのネットワークの設定 \(145ページ\)](#)」を参照してください。

OSPFv3 インスタンス パラメータの詳細については、「[高度な OSPFv3 の設定](#)」のセクションを参照してください。

始める前に

OSPFv3 機能が有効にされている必要があります ([OSPFv3の有効化 \(142ページ\)](#) のセクションを参照してください)。

使用する予定の OSPFv3 インスタンス タグが、このルータ上では使用されていないことを確認します。

`show ospfv3 instance-tag` コマンドを使用して、インスタンス タグが使用されていないことを確認します。

OSPFv3 がルータ ID (設定済みのループバック アドレスなど) を入手可能であるか、またはルータ ID オプションを設定する必要があります。

手順の概要

1. **configure terminal**
2. **router ospfv3 instance-tag**
3. (任意) **router-id ip-address**
4. (任意) **show ipv6 ospfv3 instance-tag**

5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	router ospfv3 instance-tag 例 : switch(config)# router ospfv3 201 switch(config-router)#	新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	(任意) router-id ip-address 例 : switch(config-router)# router-id 192.0.2.1	OSPFv3 ルータ ID を設定します。このドット付き 10 進表記の ID で、この OSPFv3 インスタンスが識別されます。この ID は、システムの設定済みインターフェイス上に存在する必要があります。
ステップ 4	(任意) show ipv6 ospfv3 instance-tag 例 : switch(config-router)# show ipv6 ospfv3 201	OSPFv3 情報を表示します。
ステップ 5	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	この設定変更を保存します。

例

OSPFv3 インスタンスと、関連付けられている構成をすべて削除するには、コンフィギュレーション モードで以下のコマンドを使用します。

コマンド	目的
no router ospfv3 instance-tag 例 : switch(config)# no router ospfv3 201	OSPFv3 インスタンスおよび関連付けられた構成をすべて削除します。



- (注) このコマンドは、インターフェイス モードでは OSPF 設定を削除しません。インターフェイス モードで設定された OSPFv3 コマンドはいずれも、手動で削除する必要があります。

ルータ コンフィギュレーション モードで、次の OSPFv3 用オプションパラメータを設定できます。

コマンド	目的
log-adjacency-changes [detail] 例 : <pre>switch(config-router)# log-adjacency-changes</pre>	ネイバーの状態が変化するたびに、システムメッセージを生成します。
passive-interface default 例 : <pre>switch(config-router)# passive-interface default</pre>	すべてのインターフェイス上でルーティングが更新されないようにします。このコマンドは、VRF またはインターフェイス コマンドモードの設定によって上書きされます。

アドレス ファミリ構成モードで、次の OSPFv3 用オプションパラメータを構成できます。

コマンド	目的
distance number 例 : <pre>switch(config-router-af)# distance 25</pre>	この OSPFv3 インスタンスのアドミニストレーティブ ディスタンスを設定します。範囲は 1 ～ 255 です。デフォルトは 110 です。
maximum-paths paths 例 : <pre>switch(config-router-af)# maximum-paths 4</pre>	すべてのインターフェイス上でルーティングが更新されないようにします。このコマンドは、VRF またはインターフェイス コマンドモードの設定によって上書きされます。

次の例は、OSPFv3 インスタンスを作成する方法を示しています。

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# copy running-config startup-config
```

OSPFv3でのネットワークの設定

ルータがこのネットワークへの接続に使用するインターフェイスを介して、OSPFv3 へのネットワークを関連付けることで、このネットワークを設定できます（「[ネイバー](#)」セクションを参照）。すべてのネットワークをデフォルトバックボーンエリア（エリア 0）に追加したり、任意の 10 進数または IP アドレスを使用して新規エリアを作成したりできます。



(注) すべてのエリアは、バックボーンエリアに直接、または仮想リンク経由で接続する必要があります。



(注) インターフェイスの有効な IPv6 アドレスを設定するまでは、インターフェイス上で OSPFv3 がイネーブルになりません。

始める前に

OSPFv3 機能が有効にされている必要があります ([OSPFv3の有効化 \(142 ページ\)](#) のセクションを参照してください)。

手順の概要

1. **configure terminal**
2. **interface interface-type slot/port**
3. **ipv6 address ipv6-prefix/length**
4. **ipv6 router ospfv3 instance-tag area area-id [secondaries none]**
5. (任意) **show ipv6 ospfv3 instance-tag interface interface-type slot/port**
6. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	interface interface-type slot/port 例 : <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 3	ipv6 address ipv6-prefix/length 例 : <pre>switch(config-if)# ipv6 address 2001:0DB8::1/48</pre>	このインターフェイスに IPv6 アドレスを割り当てます。

	コマンドまたはアクション	目的
ステップ 4	ipv6 router ospfv3 instance-tag area area-id [secondaries none] 例 : switch(config-if)# ipv6 router ospfv3 201 area 0	OSPFv3 インスタンスおよびエリアにインターフェイスを追加します。
ステップ 5	(任意) show ipv6 ospfv3 instance-tag interface interface-type slot/port 例 : switch(config-if)# show ipv6 ospfv3 201 interface ethernet 1/2	OSPFv3 情報を表示します。
ステップ 6	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	この設定変更を保存します。

例

インターフェイス コンフィギュレーション モードで、省略可能な次の OSPFv3 パラメータを設定できます。

コマンド	目的
ospfv3 cost number 例 : switch(config-if)# ospfv3 cost 25	このインターフェイスの OSPFv3 コスト メトリックを設定します。デフォルトでは、参照帯域幅とインターフェイス帯域幅に基づいて、コストメトリックが計算されます。有効な範囲は 1 ～ 65535 です。
ospfv3 dead-interval seconds 例 : switch(config-if)# ospfv3 dead-interval 50	OSPFv3 デッド間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトでは、hello 間隔の秒数の 4 倍です。
ospfv3 hello-interval seconds 例 : switch(config-if)# ospfv3 hello-interval 25	OSPFv3 hello 間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 10 秒です。
ospfv3 instance instance 例 : switch(config-if)# ospfv3 instance 25	OSPFv3 インスタンス ID を設定します。有効な範囲は 0 ～ 255 です。デフォルトは 0 です。インスタンス ID のスコープはリンクローカルです。

コマンド	目的
ospfv3 mtu-ignore 例 : <pre>switch(config-if)# ospfv3 mtu-ignore</pre>	OSPFv3 で、ネイバーとのあらゆる IP 最大伝送単位 (MTU) 不一致が無視されるよう設定します。デフォルトでは、ネイバー MTU がローカル インターフェイス MTU が不一致の場合には、隣接関係が確立されません。
ospfv3 network{ broadcast point-point } 例 : <pre>switch(config-if)# ospfv3 network broadcast</pre>	OSPFv3 ネットワーク タイプを設定します。
[default no] ospfv3 passive-interface 例 : <pre>switch(config-if)# ospfv3 passive-interface</pre>	インターフェイス上でルーティングが更新されないようにします。このコマンドによって、ルータまたは VRF コマンドモードの設定が上書きされます。 default オプションは、このインターフェイスモードコマンドを削除して、ルータまたは VRF の設定に戻します (設定がある場合)。
ospfv3 priority number 例 : <pre>switch(config-if)# ospfv3 priority 25</pre>	エリアの DR の決定に使用される OSPFv3 優先度を設定します。有効な範囲は 0 ~ 255 です。デフォルトは 1 です。「 指定ルータ 」の項を参照してください。
ospfv3 shutdown 例 : <pre>switch(config-if)# ospfv3 shutdown</pre>	このインターフェイス上の OSPFv3 インスタンスをシャットダウンします。

次に、OSPFv3 インスタンス 201 にネットワーク エリア 0.0.0.10 を追加する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ipv6 address 2001:0DB8::1/48
switch(config-if)# ipv6 ospfv3 201 area 0.0.0.10
switch(config-if)# copy running-config startup-config
```

OSPFv3IPSec 認証の設定

プロセス、エリア、またはインターフェイスに対して OSPFv3 IP セキュリティ (IPSec) 認証を設定できます。

認証設定は、プロセスからエリア、インターフェイス レベルに継承されます。認証が 3 つのレベルすべてで設定されている場合、インターフェイス設定がプロセスおよびエリア設定よりも優先されます。

始める前に

OSPF 機能がイネーブルにされていることを確認します（「[OSPFv3の有効化（142 ページ）](#)」セクションを参照）。

手順の概要

1. **configure terminal**
2. **[no] feature imp**
3. **router ospfv3 instance-tag**
4. **exit**
5. **authentication ipsec spi spi auth [0 | 3 | 7] key**
- 6.
7. （任意） **show ospfv3 process**
8. （任意） **show ospfv3 interface interface-type slot/port**
9. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	[no] feature imp 例 : <pre>switch(config)# feature imp</pre>	OSPFv3 認証に必要なインターネット メッセージング プログラム (IMP) を有効にします。
ステップ 3	router ospfv3 instance-tag 例 : <pre>switch(config)# router ospfv3 100 switch(config-router)#</pre>	新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 4	exit 例 : <pre>switch(config-router)# exit switch(config)#</pre>	OSPFv3 ルータ設定モードを終了します。
ステップ 5	authentication ipsec spi spi auth [0 3 7] key 例 :	プロセス（または VRF）レベルで OSPFv3 IPSec 認証を設定します。

	コマンドまたはアクション	目的
	<pre>switch(config)# authentication ipsec spi 475 md5 111111111111111111112222222222222222</pre>	spi 引数は、セキュリティ パラメータ インデックス (SPI) を指定します。指定できる範囲は 256 ～ 4294967295 です。 auth 引数は、認証のタイプを指定します。サポートされる値は md5 または sha1 です。 0 の場合は、パスワードをクリアテキストで設定します。3 の場合は、パス キーを 3DES 暗号化として設定します。7 パス キーを Cisco タイプ 7 暗号化として設定します。 cleartext オプション (0) を使用する場合、key 引数は md5 では 32 文字、sha1 では 40 文字にする必要があります。
ステップ 6	オプション	説明
	コマンド	目的
	area area authentication ipsec spi spi auth [0 3 7] key 例 : <pre>switch(config)# area 0 authenticationipsec spi 475 md5 111111111111111111112222222222222222</pre>	エリア レベルで OSPFv3 IPSec 認証を設定します。 spi 引数は、セキュリティ パラメータ インデックス (SPI) を指定します。指定できる範囲は 256 ～ 4294967295 です。 auth 引数は、認証のタイプを指定します。サポートされる値は md5 または sha1 です。 0 の場合は、パスワードをクリアテキストで設定します。3 の場合は、パス キーを 3DES 暗

コマンドまたはアクション		目的
オプション	説明	
	号化として設定します。7 パスキーを Cisco タイプ 7 暗号化として設定します。 cleartext オプション (0) を使用する場合、key 引数は md5 では 32 文字、sha1 では 40 文字にする必要があります。 (注) エリア レベルで OSPFv3 IPSec 認証を無効にするには、area area authentication disable コマンドを使用します。	
interface interface-type slot/port ospfv3 authentication ipsec spi spi auth [0 3 7] key 例 : <pre>switch(config)# interface ethernet 1/1 switch(config-if)# ospfv3 authentication ipsec spi 475 md5 111111111111111111112222222222222222</pre>	指定したインターフェイスの OSPFv3 IPSec 認証を設定します。 spi 引数は、セキュリティパラメータインデックス (SPI) を指定します。指定できる範囲は 256 ～ 4294967295 です。	

コマンドまたはアクション		目的
オプション	説明	
	<code>auth</code> 引数は、認証のタイプを指定します。サポートされる値は <code>md5</code> または <code>sha1</code> です。 <code>0</code> の場合は、パスワードをクリアテキストで設定します。<code>3</code> の場合は、パスワードを 3DES 暗号化として設定します。<code>7</code> パスワードを Cisco タイプ 7 暗号化として設定します。 <code>cleartext</code> オプション (<code>0</code>) を使用する場合、<code>key</code> 引数は <code>md5</code> では 32 文字、<code>sha1</code> では 40 文字にする必要があります。 (注) 指定したインターフェイスの OSPFv3 IPsec 認証をディセーブルにするには、<code>ospfv3 authentication disable</code> コマンドを使用します。	

	コマンドまたはアクション	目的
ステップ 7	(任意) show ospfv3 process 例 : <pre>switch(config)# show ospfv3 100</pre>	プロセス レベルの OSPFv3 認証設定を表示します。
ステップ 8	(任意) show ospfv3 interface interface-type slot/port 例 : <pre>switch(config)# show ospfv3 interface ethernet 1/1</pre>	インターフェイス レベルでの OSPFv3 認証設定を表示します。
ステップ 9	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

高度な OSPFv3 の設定

OSPFv3 は、OSPFv3 ネットワークを設計したあとに設定します。

境界ルータのフィルタ リストの設定

OSPFv3 ドメインを、関連性のある各ネットワークを含む一連のエリアに分離できます。すべてのエリアは、エリア境界ルータ (ABR) 経由でバックボーン エリアに接続している必要があります。OSPFv3 ドメインは、自律システム境界ルータ (ASBR) を介して、外部ドメインにも接続可能です。「[エリア](#)」の項を参照してください。

ABR には、省略可能な次の設定パラメータがあります。

- **Area range** : エリア間のルート集約を設定します。詳細については、「[ルート集約の設定 \(167 ページ\)](#)」を参照してください。
- **Filter list** : ABR 上で、外部エリアから受信したエリア間プレフィックス (タイプ 3) LSA をフィルタリングします。

ASBR もフィルタ リストをサポートしています。

始める前に

フィルタリストが、着信または発信エリア間プレフィックス (タイプ 3) LSA の IP プレフィックスのフィルタリングに使用するルート マップを作成します。[Route Policy Manager の設定 \(443 ページ\)](#) を参照してください。

OSPFv3 機能が有効にされている必要があります ([OSPFv3 の有効化 \(142 ページ\)](#) のセクションを参照してください)。

手順の概要

1. **configure terminal**
2. **router ospfv3 instance-tag**
3. **address-family ipv6 unicast**
4. **area area-id filter-list route-map map-name { in | out }**
5. (任意) **show ipv6 ospfv3 policy statistics area id filter-list { in | out }**
6. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router ospfv3 instance-tag 例 : <pre>switch(config)# router ospfv3 201 switch(config-router)#</pre>	新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	address-family ipv6 unicast 例 : <pre>switch(config-router)# address-family ipv6 unicast switch(config-router-af)#</pre>	IPv6 ユニキャスト アドレス ファミリ モードを開始します。
ステップ 4	area area-id filter-list route-map map-name { in out } 例 : <pre>switch(config-router-af)# area 0.0.0.10 filter-list route-map FilterLSAs in</pre>	ABR 上で着信または発信エリア間プレフィックス (タイプ 3) LSA をフィルタリングします。
ステップ 5	(任意) show ipv6 ospfv3 policy statistics area id filter-list { in out } 例 : <pre>switch(config-if)# show ipv6 ospfv3 policy statistics area 0.0.0.10 filter-list in</pre>	OSPFv3 ポリシー情報を表示します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config-router)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、無効にされているグレースフル リスタートを有効にする方法を示します。

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# area 0.0.0.10 filter-list route-map FilterLSAs in
switch(config-router-af)# copy running-config startup-config
```

スタブエリアの設定

OSPFv3 ドメインの外部トラフィックが不要な個所にスタブエリアを設定できます。スタブエリアはAS外部（タイプ5）LSAをブロックし、不要な、選択したネットワークへの往復のルーティングを制限します。「[スタブエリア](#)」の項を参照してください。また、すべての集約ルートがスタブエリアを経由しないようブロックすることもできます。

始める前に

OSPF を有効にする必要があります（[OSPFv3の有効化（142 ページ）](#) セクションを参照）。設定されるスタブエリア内に、仮想リンクと ASBR のいずれも含まれないことを確認します。

手順の概要

1. **configure terminal**
2. **router ospfv3 instance-tag**
3. **area area-id stub**
4. （任意） **address-family ipv6 unicast**
5. （任意） **area area-id default-cost cost**
6. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	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	router ospfv3 instance-tag 例： <pre>switch(config)# router ospfv3 201 switch(config-router)#</pre>	新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

	コマンドまたはアクション	目的
ステップ 3	area area-id stub 例 : switch(config-router)# area 0.0.0.10 stub	このエリアをスタブ エリアとして作成します。
ステップ 4	(任意) address-family ipv6 unicast 例 : switch(config-router)# address-family ipv6 unicast switch(config-router-af)#	IPv6 ユニキャスト アドレス ファミリ モードを開始します。
ステップ 5	(任意) area area-id default-cost cost 例 : switch(config-router-af)# area 0.0.0.10 default-cost 25	このスタブ エリアに送信されるデフォルト サマリ ルートのコストメトリックを設定します。指定できる範囲は 0 ～ 16777215 です。
ステップ 6	(任意) copy running-config startup-config 例 : switch(config-router)# copy running-config startup-config	この設定変更を保存します。

例

次に、すべてのサマリ ルート更新をブロックするスタブ エリアを作成する例を示します。

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# area 0.0.0.10 stub no-summary
switch(config-router)# copy running-config startup-config
```

Totally Stubby エリアの設定

Totally Stubby エリアを作成して、すべての集約ルート更新がスタブ エリアに入るのを防ぐことができます。

Totally Stubby エリアを作成するには、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. area area-id stub no-summary

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	area area-id stub no-summary 例 : <pre>switch(config-router)# area 20 stub no-summary</pre>	このエリアを Totally Stubby エリアとして作成します。

NSSA の設定

OSPFv3 ドメインの一部で一定限度の外部トラフィックが必要な場合は、その部分に NSSA を設定できます。また、この外部トラフィックを AS 外部（タイプ 5）LSA に変換して、このルーティング情報で OSPFv3 ドメインをフラッドニングすることもできます。NSSA は、省略可能な次のパラメータで設定できます。

- **No redistribution** : NSSA をバイパスして OSPFv3 AS 内の他のエリアに到達するルートを再配布します。このオプションは、NSSA ASBR が ABR も兼ねているときに使用します。
- **Default information originate** : 外部自律システムへのデフォルトルートのタイプ 7 LSA を生成します。このオプションは、ASBR のルーティングテーブルにデフォルトルートが含まれる場合に NSSA ASBR 上で使用します。このオプションは、ASBR のルーティングテーブルにデフォルトルートが含まれるかどうかに関係なく、NSSA ASBR 上で使用できます。
- **Route map** : 目的のルートのみが NSSA および他のエリア全体でフラッドニングされるよう、外部ルートをフィルタリングします。
- **Translate** : NSSA 外のエリア向けに、タイプ 7 LSA を AS 外部 LSA（タイプ 5）に変換します。再配布されたルートを OSPFv3 自律システム全体でフラッドニングするには、このコマンドを NSSA ABR 上で使用します。また、これらの AS 外部 LSA の転送アドレスを無効にすることもできます。
- **No summary** : すべての集約ルートが NSSA でフラッドニングされないようにします。このオプションは NSSA ABR 上で使用します。

始める前に

OSPF を有効にする必要があります（[OSPFv3 の有効化（142 ページ）](#) セクションを参照）。

設定する NSSA 上に仮想リンクがないことと、この NSSA がバックボーンエリアでないことを確認します。

手順の概要

1. **configure terminal**
2. **router ospfv3 instance-tag**

3. **area area-id nssa** [**no-redistribution**] [**default-information-originate**] [**route-map map-name**] [**no-summary**] [**translate type7 { always | never }**] [**suppress-fa**]]
4. (任意) **address-family ipv6 unicast**
5. (任意) **area area-id default-cost cost**
6. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router ospfv3 instance-tag 例 : <pre>switch(config)# router ospfv3 201 switch(config-router)#</pre>	新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	area area-id nssa [no-redistribution] [default-information-originate] [route-map map-name] [no-summary] [translate type7 { always never }] [suppress-fa]] 例 : <pre>switch(config-router)# area 0.0.0.10 nssa</pre>	このエリアを NSSA として作成します。
ステップ 4	(任意) address-family ipv6 unicast 例 : <pre>switch(config-router)# address-family ipv6 unicast switch(config-router-af)#</pre>	IPv6 ユニキャスト アドレス ファミリ モードを開始します。
ステップ 5	(任意) area area-id default-cost cost 例 : <pre>switch(config-router-af)# area 0.0.0.10 default-cost 25</pre>	この NSSA に送信されるデフォルト集約ルートのコスト メトリックを設定します。指定できる範囲は 0 ~ 16777215 です。
ステップ 6	copy running-config startup-config 例 : <pre>switch(config-router)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、すべての集約ルート更新をブロックする NSSA を作成する例を示します。

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# area 0.0.0.10 nssa no-summary
switch(config-router)# copy running-config startup-config
```

次に、デフォルト ルートを生成する NSSA を作成する例を示します。

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# area 0.0.0.10 nssa default-info-originate
switch(config-router)# copy running-config startup-config
```

次に、外部ルートをフィルタリングし、すべての集約ルート更新をブロックする NSSA を作成する例を示します。

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# area 0.0.0.10 nssa route-map ExternalFilter no-summary
switch(config-router)# copy running-config startup-config
```

この例では、常にタイプ 7 LSA を AS 外部 (タイプ 5) LSA に変換する NSSA を作成する方法を示します。

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# area 0.0.0.10 nssa translate type 7 always
switch(config-router)# copy running-config startup-config
```

次に、すべての集約ルート更新をブロックする NSSA を作成する例を示します。

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# area 0.0.0.10 nssa no-summary
switch(config-router)# copy running-config startup-config
```

マルチエリアの隣接関係の設定

既存の OSPFv3 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。

始める前に

OSPFv3 機能が有効にされている必要があります ([OSPFv3の有効化 \(142 ページ\)](#) のセクションを参照してください)。

インターフェイスにプライマリ エリアが構成されていることを確認します ([OSPFv3でのネットワークの設定 \(145 ページ\)](#) を参照してください)。

手順の概要

1. **configure terminal**
2. **interface interface-type slot/port**

3. **ipv6 router ospfv3 instance-tag multi-area area-id**
4. (任意) **show ipv6 ospfv3 instance-tag interface interface-type slot/port**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	グローバル設定モードを開始します
ステップ 2	interface interface-type slot/port 例 : switch(config)# interface ethernet 1/2 switch(config-if)#	インターフェイス設定モードを開始します。
ステップ 3	ipv6 router ospfv3 instance-tag multi-area area-id 例 : switch(config-if)# ipv6 router ospfv3 201 multi-area 3	別のエリアにインターフェイスを追加します。 (注) Cisco NX-OS リリース 7.0(3)I5(1) 以降では、 instance-tag 引数はオプションです。インスタンスを指定しない場合、マルチエリア構成は、そのインターフェイスのプライマリ エリアに構成されている同じインスタンスに適用されます。
ステップ 4	(任意) show ipv6 ospfv3 instance-tag interface interface-type slot/port 例 : switch(config-if)# show ipv6 ospfv3 201 interface ethernet 1/2	OSPFv3 情報を表示します。
ステップ 5	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	この設定変更を保存します。

例

次に、OSPFv3 インターフェイスに別のエリアを追加する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ipv6 address 2001:0DB8::1/48
switch(config-if)# ipv6 ospfv3 201 area 0.0.0.10
```



```
switch(config-if)# ipv6 ospfv3 201 multi-area 20
switch(config-if)# copy running-config startup-config
```

仮想リンクの設定

仮想リンクは、隔離されたエリアを中継エリアを介してバックボーン エリアに接続します。[\[仮想リンク\]](#) セクションを展開します。仮想リンクには、省略可能な次のパラメータを設定できます。

- **Dead interval** : ローカル ルータがデッドであることを宣言し、隣接関係を解消する前に、ネイバーが hello パケットを待つ時間を設定します。
- **Hello interval** : 連続する hello パケット間の時間間隔を設定します。
- **Retransmit interval** : 連続する LSA 間の推定時間間隔を設定します。
- **Transmit delay** : LSA をネイバーに送信する推定時間を設定します。



(注) リンクがアクティブになる前に、関与する両方のルータで仮想リンクを設定する必要があります。

始める前に

OSPF を有効にする必要があります ([OSPFv3の有効化 \(142 ページ\)](#) セクションを参照)。

手順の概要

1. **configure terminal**
2. **router ospfv3 instance-tag**
3. **area area-id virtual-link router-id**
4. (任意) **show ipv6 ospfv3 virtual-link [brief]**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 2	router ospfv3 instance-tag 例 : <pre>switch(config)# router ospfv3 201 switch(config-router)#</pre>	新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	area area-id virtual-link router-id 例 : <pre>switch(config-router)# area 0.0.0.10 virtual-link 2001:0DB8::1 switch(config-router-vlink)#</pre>	リモートルータへの仮想リンクの端を作成します。仮想リンクをリモートルータ上に作成して、リンクを完成させる必要があります。
ステップ 4	(任意) show ipv6 ospfv3 virtual-link [brief] 例 : <pre>switch(config-if)# show ipv6 ospfv3 virtual-link</pre>	OSPFv3 仮想リンク情報を表示します。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config-router)# copy running-config startup-config</pre>	この設定変更を保存します。

例

仮想リンク コンフィギュレーションモードで、省略可能な次のコマンドを設定できます。

コマンド	目的
dead-interval seconds 例 : <pre>switch(config-router-vlink)# dead-interval 50</pre>	OSPFv3 デッド間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトでは、hello 間隔の秒数の 4 倍です。
hello-interval seconds 例 : <pre>switch(config-router-vlink)# hello-interval 25</pre>	OSPFv3 hello 間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 10 秒です。
retransmit-interval seconds 例 : <pre>switch(config-router-vlink)# retransmit-interval 50</pre>	OSPFv3 再送信間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 5 分です。

コマンド	目的
transmit-delay seconds 例 : <pre>switch(config-router-vlink)# transmit-delay 2</pre>	OSPFv3 送信遅延を秒単位で設定します。指定できる範囲は 1 ～ 450 です。デフォルトは 1 です。

次に、2 つの ABR 間に簡単な仮想リンクを作成する例を示します。

ABR 1 (ルータ ID 2001:0DB8::1) の設定は、次のとおりです。

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# area 0.0.0.10 virtual-link 2001:0DB8::10
switch(config-router)# copy running-config startup-config
```

ABR 2 (ルータ ID 2001:0DB8::10) の設定は、次のとおりです。

```
switch# configure terminal
switch(config)# router ospf 101
switch(config-router)# area 0.0.0.10 virtual-link 2001:0DB8::1
switch(config-router)# copy running-config startup-config
```

再配布の設定

他のルーティングプロトコルから学習したルートを、ASBR 経由で OSPFv3 自律システムに再配布できます。

OSPF でのルート再配布には、省略可能な次のパラメータを設定できます。

- **Default information originate** : 外部自律システムへのデフォルト ルートの AS 外部 (タイプ 5) LSA を生成します。



(注) **Default information originate** はオプションのルート マップ内の **match** 文を無視します。

- **Default metric** : すべての再配布ルートに同じコスト メトリックを設定します。



(注) スタティック ルートを再配布する場合は、Cisco NX-OS でもデフォルト スタティック ルートが再配布されます。

始める前に

再配布で使用する、必要なルート マップを作成します。

OSPF を有効にする必要があります ([OSPFv3の有効化 \(142 ページ\)](#) セクションを参照)。

手順の概要

1. **configure terminal**
2. **router ospfv3 instance-tag**
3. **address-family ipv6 unicast**
4. **redistribute { bgp id | direct | isis id | rip id | static } route-map map-name**
5. **default-information originate [always] [route-map map-name]**
6. **default-metric cost**
7. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router ospfv3 instance-tag 例 : <pre>switch(config)# router ospfv3 201 switch(config-router)#</pre>	新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	address-family ipv6 unicast 例 : <pre>switch(config-router)# address-family ipv6 unicast switch(config-router-af)#</pre>	IPv6 ユニキャスト アドレス ファミリ モードを開始します。
ステップ 4	redistribute { bgp id direct isis id rip id static } route-map map-name 例 : <pre>switch(config-router-af)# redistribute bgp route-map FilterExternalBGP</pre>	設定したルートマップ経由で、選択したプロトコルを OSPFv3 に再配布します。 (注) スタティック ルートを再配布する場合は、Cisco NX-OS でもデフォルト スタティック ルートが再配布されます。
ステップ 5	default-information originate [always] [route-map map-name] 例 : <pre>switch(config-router-af)# default-information-originate route-map DefaultRouteFilter</pre>	デフォルトのルートが RIB に存在する場合、この OSPFv3 ドメインにデフォルトのルートを作成します。次の省略可能なキーワードを使用します。 • always : ルートが RIB に存在しない場合でも、常にデフォルト ルート 0.0.0. を生成します。 • route-map : ルート マップが true を返す場合にデフォルト ルートを生成します。

	コマンドまたはアクション	目的
		(注) このコマンドは、ルート マップの match 文を無視します
ステップ 6	default-metric cost 例 : switch(config-router-af)# default-metric 25	再配布されたルートのコストメトリックを設定します。指定できる範囲は 1 ～ 16777214 です。このコマンドは、直接接続されたルートには適用されません。ルートマップを使用して、直接接続されたルートのデフォルトのメトリックを設定します。
ステップ 7	copy running-config startup-config 例 : switch(config-router)# copy running-config startup-config	この設定変更を保存します。

例

次に、ボーダー ゲートウェイ プロトコル (BGP) を OSPFv3 に再配布する例を示します。

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# redistribute bgp route-map FilterExternalBGP
switch(config-router-af)# copy running-config startup-config
```

再配布されるルート数の制限

ルート再配布によって、OSPFv3 ルート テーブルに多数のルートを追加できます。外部プロトコルから受け取るルートの上限を設定できます。OSPFv3 には、再配布されるルート制限を設定するための次のオプションがあります。

- 上限固定：設定された最大値に OSPFv3 が達すると、メッセージをログに記録します。OSPFv3 はそれ以上の再配布されたルートを受け付けません。任意で、最大値のしきい値パーセンテージを設定して、OSPFv3 がこのしきい値を超えたときに警告を記録するようにすることもできます。
- 警告のみ：OSPFv3 が最大値に達したときのみ、警告のログを記録します。OSPFv3 は、再配布されたルートを受け入れ続けます。
- 取り消し：OSPFv3 が最大値に達したときに設定したタイムアウト期間を開始します。このタイムアウト期間後、現在の再配布されたルート数が最大制限より少なければ、OSPFv3 はすべての再配布されたルートを要求します。再配布されたルートの現在数が最大数に達した場合、OSPFv3 はすべての再配布されたルートを取り消します。OSPFv3 が追加の再配布されたルートを受け付ける前に、この状況を解消する必要があります。任意で、タイムアウト期間を設定できます。

始める前に

OSPF を有効にする必要があります ([OSPFv3の有効化 \(142 ページ\)](#) セクションを参照)。

手順の概要

1. **configure terminal**
2. **router ospfv3 instance-tag**
3. **address-family ipv6 unicast**
4. **redistribute { bgp id | direct | isis id | rip id | static } route-map map-name**
5. **redistribute maximum-prefix max [threshold] [warning-only | withdraw [num-retries timeout]]**
6. (任意) **show running-config ospfv3**
7. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router ospfv3 instance-tag 例 : <pre>switch(config)# router ospfv3 201 switch(config-router)#</pre>	新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	address-family ipv6 unicast 例 : <pre>switch(config-router)# address-family ipv6 unicast switch(config-router-af)#</pre>	IPv6 ユニキャスト アドレス ファミリ モードを開始します。
ステップ 4	redistribute { bgp id direct isis id rip id static } route-map map-name 例 : <pre>switch(config-router-af)# redistribute bgp route-map FilterExternalBGP</pre>	設定したルートマップ経由で、選択したプロトコルを OSPFv3 に再配布します。
ステップ 5	redistribute maximum-prefix max [threshold] [warning-only withdraw [num-retries timeout]] 例 : <pre>switch(config-router)# redistribute maximum-prefix 1000 75 warning-only</pre>	OSPFv2 が配布するプレフィックスの最大数を指定します。指定できる範囲は 0 ～ 65536 です。任意で次のオプションを指定します。 • threshold : 警告メッセージをトリガする最大プレフィックスの割合。

	コマンドまたはアクション	目的
		• warning-only : プレフィックスの最大数を超えた場合に警告メッセージを記録します。 • withdraw : 再配布されたすべてのルートを取り消し、任意で再配布されたルートを取得しようと試みます。<i>num-retries</i> の範囲は 1 ～ 12 です。<i>timeout</i> の範囲は 60 ～ 600 秒です。デフォルトは 300 秒です。
ステップ 6	(任意) show running-config ospfv3 例 : <pre>switch(config-router)# show running-config ospf</pre>	OSPFv3 設定を表示します。
ステップ 7	(任意) copy running-config startup-config 例 : <pre>switch(config-router)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、OSPF に再配布されるルート の数を制限する例を示します。

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# redistribute bgp route-map FilterExternalBGP
switch(config-router-af)# redistribute maximum-prefix 1000 75
```

ルート集約の設定

集約したアドレス範囲を設定することにより、エリア間ルートのルート集約を設定できます。また、ASBR 上のこれらのルートのサマリアドレスを設定して、外部の再配布されたルートのルート集約を設定することもできます。詳細については、「[ルート集約](#)」を参照してください。

始める前に

OSPF を有効にする必要があります ([OSPFv3 の有効化 \(142 ページ\)](#) セクションを参照)。

手順の概要

1. **configure terminal**
2. **router ospfv3 instance-tag**
3. **address-family ipv6 unicast**
4. **area area-id range ipv6-prefix/length [no-advertise] [cost cost]**

5. **summary-address** *ipv6-prefix/length* [**no-advertise**] [**tag** *tag*]
6. (任意) **show ipv6 ospfv3 summary-address**
7. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	router ospfv3 instance-tag 例 : switch(config)# router ospfv3 201 switch(config-router)#	新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	address-family ipv6 unicast 例 : switch(config-router)# address-family ipv6 unicast switch(config-router-af)#	IPv6 ユニキャスト アドレス ファミリ モードを開始します。
ステップ 4	area area-id range ipv6-prefix/length [no-advertise] [cost cost] 例 : switch(config-router-af)# area 0.0.0.10 range 2001:0DB8::/48 advertise	一定の範囲のアドレスのサマリ アドレスを ABR 上に作成します。このサマリ アドレスをエリア間プレフィックス (タイプ 3) LSA にアドバタイズすることもできます。cost の範囲は 0 ~ 16777215 です。
ステップ 5	summary-address ipv6-prefix/length [no-advertise] [tag tag] 例 : switch(config-router-af)# summary-address 2001:0DB8::/48 tag 2	一定の範囲のアドレスのサマリ アドレスを ABR 上に作成します。ルートマップによる再配布で使えるよう、このサマリ アドレスにタグを割り当てることもできます。
ステップ 6	(任意) show ipv6 ospfv3 summary-address 例 : switch(config-router)# show ipv6 ospfv3 summary-address	OSPFv3 サマリ アドレスに関する情報を表示します
ステップ 7	(任意) copy running-config startup-config 例 : switch(config-router)# copy running-config startup-config	この設定変更を保存します。

例

次に、ABR 上のエリア間のサマリ アドレスを作成する例を示します。

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# address-family ipv6 unicast
switch(config-router)# area 0.0.0.10 range 2001:0DB8::/48
switch(config-router)# copy running-config startup-config
```

次に、ASBR 上のサマリ アドレスを作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# address-family ipv6 unicast
switch(config-router)# summary-address 2001:0DB8::/48
switch(config-router)# copy running-config startup-config
```

デフォルト タイマーの変更

OSPFv3 には、プロトコル メッセージの動作および最短パス優先 (SPF) の計算を制御する多数のタイマーが含まれています。OSPFv3 には、省略可能な次のタイマー パラメータが含まれます。

- **LSA arrival time** : ネイバーから着信する LSA 間で許容される最小間隔を設定します。この時間より短時間で到着する LSA はドロップされます。
- **Pacing LSAs** : LSA が集められてグループ化され、リフレッシュされて、チェックサムが計算される間隔、つまり期限切れとなる間隔を設定します。このタイマーは、LSA 更新が実行される頻度を制御し、LSA 更新メッセージで送信される LSA 更新の数を制御します（「[フラiddiingと LSA グループ ペーシング](#)」を参照）。
- **Throttle LSAs** : LSA 生成のレート制限を設定します。このタイマーは、トポロジが変更された後に LSA が生成される頻度を制御します。
- **Throttle SPF calculation** : SPF 計算の実行頻度を制御します。

インターフェイス レベルでは、次のタイマーも制御できます。

- **Retransmit interval** : 連続する LSA 間の推定時間間隔を設定します。
- **Transmit delay** : LSA をネイバーに送信する推定時間を設定します。

hello 間隔とデッドタイマーに関する情報の詳細については、「[OSPFv3でのネットワークの設定 \(145 ページ\)](#)」の項を参照してください。

手順の概要

1. **configure terminal**
2. **router ospfv3 instance-tag**
3. **timers lsa-arrival**
4. **timers lsa-group-pacing seconds**

5. **timers throttle lsa start-time hold-interval max-time**
6. **address-family ipv6 unicast**
7. **timers throttle spf delay-time hold-time**
8. **interface interface type slot/port**
9. **ospfv3 retransmit-interval seconds**
10. **ospfv3 transmit-delay seconds**
11. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router ospfv3 instance-tag 例 : <pre>switch(config)# router ospfv3 201 switch(config-router)#</pre>	新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	timers lsa-arrival 例 : <pre>switch(config-router)# timers lsa-arrival 2000</pre>	LSA 到着時間をミリ秒で設定します。範囲は 10 ～ 600000 です。デフォルトは 1000 ミリ秒です。
ステップ 4	timers lsa-group-pacing seconds 例 : <pre>switch(config-router)# timers lsa-group-pacing 200</pre>	LSA がグループ化される間隔を秒で設定します。範囲は 1 ～ 1800 です。デフォルトは 10 秒です。
ステップ 5	timers throttle lsa start-time hold-interval max-time 例 : <pre>switch(config-router)# timers throttle lsa network 350 5000 6000</pre>	LSA 生成のレート制限をミリ秒で設定します。次のタイマーを設定できます。 start-time : 指定できる範囲は 50 ～ 5000 ミリ秒です。デフォルト値は 50 ミリ秒です。 hold-interval : 指定できる範囲は 50 ～ 30,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。 max-time : 指定できる範囲は 50 ～ 30,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
ステップ 6	address-family ipv6 unicast 例 :	IPv6 ユニキャストアドレスファミリ モードを開始します。

	コマンドまたはアクション	目的
	<pre>switch(config-router)# address-family ipv6 unicast switch(config-router-af)#</pre>	
ステップ 7	timers throttle spf delay-time hold-time 例 : <pre>switch(config-router)# timers throttle spf 3000 2000</pre>	SPF 最適パス スケジュール初期遅延時間と、各 SPF 最適パス計算間の最小ホールドタイム（秒単位）を設定します。指定できる範囲は1～600000です。デフォルトは、遅延時間なし、およびホールドタイム 5000 ミリ秒です。
ステップ 8	interface interface type slot/port 例 : <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 9	ospfv3 retransmit-interval seconds 例 : <pre>switch(config-if)# ospfv3 retransmit-interval 30</pre>	このインターフェイスから送信される各 LSA 間の推定時間間隔を設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 5 分です。
ステップ 10	ospfv3 transmit-delay seconds 例 : <pre>switch(config-if)# ospfv3 transmit-delay 600 switch(config-if)#</pre>	LSA をネイバーに送信する推定時間間隔を秒で設定します。指定できる範囲は1～450です。デフォルトは 1 です。
ステップ 11	（任意） copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、lsa-group-pacing オプションで LSA フラッディングを制御する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# timers lsa-group-pacing 300
switch(config-router)# copy running-config startup-config
```

グレースフル リスタートの設定

デフォルトでは、グレースフル リスタートは有効です。OSPFv3 インスタンスのグレースフル リスタートには、省略可能な次のパラメータを設定できます。

- **Grace period** : グレースフル リスタートの開始後に、ネイバーが隣接関係を解消するまでに待つ時間を設定します。

- **Helper mode disabled** : ローカル OSPFv3 インスタンスのヘルパー モードをディセーブルにします。OSPFv3 は、ネイバーのグレースフル リスタートには関与しません。
- **Planned graceful restart only** : 予定された再起動の場合にのみグレースフル リスタートがサポートされるよう、OSPFv3 を設定します。

始める前に

OSPFv3 機能が有効にされている必要があります ([OSPFv3の有効化 \(142 ページ\)](#) のセクションを参照してください)。

すべてのネイバーで、一致した省略可能なパラメーター式とともにグレースフルリスタートが設定されていることを確認します。

手順の概要

1. **configure terminal**
2. **router ospfv3 instance-tag**
3. **graceful-restart**
4. **graceful-restart grace-period seconds**
5. **graceful-restart helper-disable**
6. **graceful-restart planned-only**
7. (任意) **show ipv6 ospfv3 instance-tag**
8. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	router ospfv3 instance-tag 例 : <pre>switch(config)# router ospfv3 201 switch(config-router)#</pre>	新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	graceful-restart 例 : <pre>switch(config-router)# graceful-restart</pre>	グレースフルリスタートをイネーブルにします。グレースフルリスタートは、デフォルトで有効にされています。
ステップ 4	graceful-restart grace-period seconds 例 :	猶予期間を秒で設定します。指定できる範囲は 5 ～ 1800 です。デフォルトは 60 秒です。

	コマンドまたはアクション	目的
	<code>switch(config-router)# graceful-restart grace-period 120</code>	
ステップ 5	graceful-restart helper-disable 例 : <code>switch(config-router)# graceful-restart helper-disable</code>	ヘルパーモードを無効にします。デフォルトでは、イネーブルです。
ステップ 6	graceful-restart planned-only 例 : <code>switch(config-router)# graceful-restart planned-only</code>	予定された再起動時にのみグレースフルリスタートを設定します。
ステップ 7	(任意) show ipv6 ospfv3 instance-tag 例 : <code>switch(config-if)# show ipv6 ospfv3 201</code>	OSPFv3 情報を表示します。
ステップ 8	(任意) copy running-config startup-config 例 : <code>switch(config)# copy running-config startup-config</code>	この設定変更を保存します。

例

次に、無効にされているグレースフルリスタートを有効にし、猶予期間を 120 秒に設定する例を示します。

```
switch# configure terminal
switch(config)# router ospfv3 201
switch(config-router)# graceful-restart
switch(config-router)# graceful-restart grace-period 120
switch(config-router)# copy running-config startup-config
```

OSPFv3 インスタンスの再起動

OSPFv3 インスタンスを再起動できます。この処理では、インスタンスのすべてのネイバーが消去されます。

OSPFv3 インスタンスを再起動して、関連付けられたすべてのネイバーを削除するには、次のコマンドを使用します。

手順の概要

1. `restart ospfv3 instance-tag`

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	restart ospfv3 instance-tag 例 : <pre>switch(config)# restart ospfv3 201</pre>	OSPFv3 インスタンスを再起動して、すべてのネイバーを削除します。

仮想化による OSPFv3 の設定

各 VDC で複数 OSPFv3 インスタンスを構成できます。また、各 VDC で複数の VRF を作成し、各 VRF で同じ OSPFv2 インスタンスまたは複数の OSPFv3 インスタンスを使用することもできます。VRF には OSPFv3 インターフェイスを割り当てます。



(注) インターフェイスの VRF を設定した後に、インターフェイスの他のすべてのパラメータを設定します。インターフェイスの VRF を設定すると、そのインターフェイスのすべての設定が削除されます。

始める前に

VDC を作成します。

OSPF を有効にする必要があります ([OSPFv3 の有効化 \(142 ページ\)](#) セクションを参照)。

手順の概要

1. **configure terminal**
2. **vrf context vrf-name**
3. **router ospfv3 instance-tag**
4. **vrf vrf-name**
5. (任意) **maximum-paths paths**
6. **interface interface type slot/port**
7. **vrf member vrf-name**
8. **ipv6 address ipv6-prefix/length**
9. **ipv6 ospfv3 instance-tag area area-id**
10. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	vrf context vrf-name 例 : <pre>switch(config)# vrf context RemoteOfficeVRF switch(config-vrf)#</pre>	新しい VRF を作成し、VRF 設定モードを開始します。
ステップ 3	router ospfv3 instance-tag 例 : <pre>switch(config)# router ospfv3 201 switch(config-router)#</pre>	新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 4	vrf vrf-name 例 : <pre>switch(config-router)# vrf RemoteOfficeVRF switch(config-router-vrf)#</pre>	VRF 設定モードを開始します。
ステップ 5	(任意) maximum-paths paths 例 : <pre>switch(config-router-vrf)# maximum-paths 4</pre>	この VRF のルート テーブル内の宛先への、同じ OSPFv3 パスの最大数を設定します。このコマンドはロード バランシングに使用します。
ステップ 6	interface interface type slot/port 例 : <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 7	vrf member vrf-name 例 : <pre>switch(config-if)# vrf member RemoteOfficeVR</pre>	このインターフェイスを VRF に追加します。
ステップ 8	ipv6 address ipv6-prefix/length 例 : <pre>switch(config-if)# ipv6 address 2001:0DB8::1/48</pre>	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 9	ipv6 ospfv3 instance-tag area area-id 例 : <pre>switch(config-if)# ipv6 ospfv3 201 area 0</pre>	設定した OSPFv3 インスタンスおよびエリアに、このインターフェイスを割り当てます。

	コマンドまたはアクション	目的
ステップ 10	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、VRF を作成して、その VRF にインターフェイスを追加する例を示します。

```
switch# configure terminal

switch(config)# vrf context NewVRF

switch(config-vrf)# exit

switch(config)# router ospfv3 201

switch(config-router)# exit

switch(config)# interface ethernet 1/2

switch(config-if)# vrf member NewVRF

switch(config-if)# ipv6 address 2001:0DB8::1/48

switch(config-if)# ipv6 ospfv3 201 area 0

switch(config-if)# copy running-config startup-config
```

暗号化および認証の構成

Cisco Nexus リリース 10.2 (1) 以降では、ESP カプセル化を使用して OSPFv3 メッセージを暗号化および認証できます。OSPFv3 は、セキュア接続を IPSec に依存しています。IPSec は、次の 2 つのカプセル化タイプをサポートしています。

- 認証ヘッダー (AH)
- Encapsulating Security Payload (ESP)
- RFC4552 「Authentication/Confidentiality for OSPFv3」は、上記の両方の側面をカバーしています。

ESP設定は、OSPFv3 メッセージの暗号化と認証の両方を提供します。

Cisco Nexus リリース 10.4(1)F 以降では、キーチェーン オプションを使用して暗号化および認証アルゴリズムとキーを構成できます。

制限事項は次のとおりです。

1. IPSec トランスポートモードのみがサポートされ、トンネルモードはサポートされません。

2. AH と ESP の設定は、インターフェイス上では一緒に使用できません。ただし、2 つの異なるインターフェイスに AH と ESP を設定できます。
3. RFC 4552 のセクション 10 で定義されている中断のないキー再生成はサポートされていません。
4. 次の暗号化アルゴリズムが ESP でサポートされます。
 - AES-CBC (128 ビット)
 - AES 192 ビットと AES 256 ビットは、このリリースではサポートされません。
 - 3DES-CBC
 - NULL
5. ESP では次の認証がサポートされます。
 - SHA-1
 - NULL
6. 1 つの ESP CLI で暗号化アルゴリズムと認証アルゴリズムの両方を NULL に設定することはできません。
7. 複数のエリアの一部であるインターフェイスは、親と同じ ESP パラメータを使用します。
8. 設定中に SPI が競合すると、エラーがユーザにスローされ、設定は保存されません。そのため、ESP 構成を変更する場合は、ユーザーは新しい構成に異なる SPI を使用する必要があります。
9. 最大 128 の SA/SPI 値を OSPFv3 プロセスごとに設定できます。

次のレベルで ESP を設定できます。

- ルータ
- エリア
- インターフェイス
- 仮想リンク

ルータ レベルでの OSPFv3 暗号化の設定

次のコマンドを使用して、ルータ レベルで OSPFv3 パケットを暗号化および認証するように OSPFv3 ESP を設定できます。

始める前に

OSPFv3 機能を有効にします。

認証パッケージを有効にします。

手順

ステップ 1 グローバル設定モードを開始します。

```
switch# configure terminal
```

ステップ 2 OSPFv3 を有効にします。

```
switch(config)# feature ospfv3
```

ステップ 3 認証パッケージを有効にします。

```
switch(config)# feature imp
```

ステップ 4 インスタンスタグが設定された新しい OSPFv3 インスタンスを作成します。

```
switch(config)# router ospfv3 instance-tag
```

ステップ 5 IPsec ESP 暗号化を有効にします:

```
switch(config-router)# encryption ipsec spi spi_id esp [encrypt_algorithm [ 0 | 3 | 7 ] key | key-chain enc_keychain_name  
| null] authentication [auth_algorithm [ 0 | 3 | 7 ] key | key-chain auth_keychain_name | null]
```

spi_id を使用してセキュリティポリシーインデックスを指定し、*encrypt_algorithm* を使用して暗号化アルゴリズムを定義できます。3DES、AES 128、または null を指定できます。番号 0、3、および 7 は、*key* の形式を指定します。認証アルゴリズムは、*auth_algorithm* (SHA-1 または NULL) で定義できます。

key-chain オプションを使用して、キーとアルゴリズムも構成できます。

ステップ 6 (任意) OSPFv3 情報を表示します。

```
switch(config)# show running-config ospfv3
```

エリア レベルでの OSPFv3 暗号化の設定

次のコマンドを使用して、エリアレベルで OSPFv3 パケットを暗号化および認証するように OSPFv3 ESP を設定できます。

始める前に

OSPFv3 機能を有効にします。

認証パッケージを有効にします。

手順

ステップ 1 グローバル設定モードを開始します。

```
switch# configure terminal
```

ステップ 2 OSPFv3 を有効にします。

```
switch(config)# feature ospfv3
```

ステップ 3 認証パッケージを有効にします。

```
switch(config)# feature imp
```

ステップ 4 インスタンスタグが設定された新しい OSPFv3 インスタンスを作成します。

```
switch(config)# router ospfv3 instance-tag
```

ステップ 5 IPsec ESP 暗号化を有効にします:

```
switch(config-router)#area area-num encryption ipsec spi spi_val esp encrypt_algorithm [ 0 | 3 | 7 ] key | key-chain  
enc_keychain_name | null authentication auth_algorithm [ 0 | 3 | 7 ] key | key-chain auth_keychain_name | null
```

spi_id を使用してセキュリティポリシーインデックスを指定し、*encrypt_algorithm* を使用して暗号化アルゴリズムを定義できます。3DES、AES 128、または null を指定できます。番号 0、3、6 および 7 は、*key* の形式を指定します。認証アルゴリズムは、*auth_algorithm* (SHA-1 または NULL またはキーチェーン) で定義できます。

key-chain オプションを使用して、キーとアルゴリズムも構成できます。

ステップ 6 (任意) OSPFv3 情報を表示します。

```
switch(config)# show running-config ospfv3
```

インターフェイスレベルでの OSPFv3 暗号化の設定

次のコマンドを使用して、インターフェイス レベルで OSPFv3 パケットを暗号化および認証するように OSPFv3 ESP を設定できます。

始める前に

OSPFv3 をイネーブルにする必要があります。

認証パッケージを有効にします。

手順

ステップ 1 グローバル設定モードを開始します。

```
switch# configure terminal
```

ステップ 2 OSPFv3 を有効にします。

```
switch(config)# feature ospfv3
```

ステップ 3 認証モードをイネーブルにします。

```
switch(config)# feature imp
```

ステップ 4 イーサネット インターフェイス設定モードを開始します:

```
switch(config)# interface ethernet interface
```

ステップ 5 インターフェイスのOSPFv3インスタンスとエリアを指定します。

```
switch (config-if) # instance-tag area-id ipv6 router ospfv3 area
```

ステップ 6 IPsec ESP 暗号化を有効にします:

```
switch(config-if)# ospfv3 encryption ipsec spi spi_id esp encrypt_algorithm [ 0 | 3 | 7 ] key | key-chain  
enc_keychain_name | null authentication auth_algorithm [ 0 | 3 | 7 ] key | key-chain auth_keychain_name | null]
```

spi_id を使用してセキュリティポリシーインデックスを指定し、*encrypt_algorithm* を使用して暗号化アルゴリズムを定義できます。3DES、AES 128、または null を指定できます。番号 0、3、および 7 は、*key* の形式を指定します。認証アルゴリズムは、*auth_algorithm* (SHA-1 または NULL) で定義できます。

key-chain オプションを使用して、キーとアルゴリズムを構成することもできます。

ステップ 7 (オプション) インターフェイスの実行設定を表示します:

```
switch(config-if)#show run interface interface
```

設定例

次に、イーサネットインターネット 3/2 のセキュリティ を有効にする例を示します。

```
switch# configure terminal
switch(config)# feature ospfv3
switch(config)# feature imp
switch(config)# interface ethernet 3/2
switch(config-if)# ipv6 router ospfv3 1 area 0.0.0.0
switch(config-if)# ospfv3 encryption ipsec spi 444
    esp Specify encryption parameters
switch(config-if)# ospfv3 encryption ipsec spi 444 esp
    3des Use the triple DES algorithm
    aes Use the AES algorithm
    key-chain Encryption password key-chain
    null Use NULL authentication
switch(config-if)# ospfv3 encryption ipsec spi 444 esp aes
    128 Use the 128-bit AES algorithm
switch(config-if)# ospfv3 encryption ipsec spi 444 esp aes 128
    0 Specifies an UNENCRYPTED encryption key will follow
    3 Specifies an 3DES ENCRYPTED encryption key will follow
    7 Specifies a Cisco type 7 ENCRYPTED encryption key will follow
    WORD The UNENCRYPTED (cleartext) encryption key
switch(config-if)# ospfv3 encryption ipsec spi 444 esp aes 128
12345678123456781234567812345678 authentication null
switch(config-if)# sh ospfv3 interface
Ethernet3/2 is up, line protocol is up
IPv6 address 1:1:1:1::2/64
Process ID 1 VRF default, Instance ID 0, area 0.0.0.0
Enabled by interface configuration
State DOWN, Network type BROADCAST, cost 40
```

```
    ESP Encryption AES, Authentication NULL, SPI 444, ConnId 444
switch(config-if)#
```

仮想リンクの OSPFv3 暗号化の設定

次のコマンドを使用して、仮想リンクの OSPFv3 パケットを暗号化および認証するように OSPFv3 ESP を設定できます。

始める前に

OSPFv3 機能を有効にします。

認証パッケージを有効にします。

手順

ステップ 1 グローバル設定モードを開始します。

```
switch# configure terminal
```

ステップ 2 OSPFv3 を有効にします。

```
switch(config)# feature ospfv3
```

ステップ 3 認証パッケージを有効にします。

```
switch(config)# feature imp
```

ステップ 4 インスタスタグが設定された新しい OSPFv3 インスタンスを作成します。

```
switch(config)#router ospfv3 instance-tag
```

ステップ 5 リモートルータへの仮想リンクの端を作成します。仮想リンクをリモートルータ上に作成して、リンクを完成させる必要があります。

```
switch(config-router)# area area-id virtual-link router-id
```

ステップ 6 IPsec ESP 暗号化を有効にします:

```
switch(config-router-vlink)# encryption ipsec spi spi_id esp encrypt_algorithm [ 0 | 3 | 7 ] key | key-chain  
enc_keychain_name | null authentication auth_algorithm [ 0 | 3 | 7 ] key | key-chain auth_keychain_name | null]
```

spi_id を使用してセキュリティポリシーインデックスを指定し、*encrypt_algorithm* を使用して暗号化アルゴリズムを定義できます。3DES、AES 128、または null を指定できます。番号 0、3、および 7 は、*key* の形式を指定します。認証アルゴリズムは、*auth_algorithm*（SHA-1 または NULL）で定義できます。

key-chain オプションを使用して、キーとアルゴリズムも構成できます。

ステップ 7 （任意）OSPFv3 情報を表示します。

```
switch(config)# show running-config ospfv3
```

設定例

次に、仮想リンクを暗号化する例を示します。

```
switch(config)# feature ospfv3
switch(config)# feature imp
switch(config-if)# router ospfv3 1
switch(config-router)# area 0.0.0.1 virtual-link 3.3.3.3
switch(config-router-vlink)# encryption ipsec spi ?
<256-4294967295> SPI Value
switch(config-router-vlink)# encryption ipsec spi 256 esp ?
3des Use the triple DES algorithm
aes Use the AES algorithm
key-chain Encryption password key-chain
null Use NULL authentication
switch(config-router-vlink)# encryption ipsec spi 256 esp aes 128
123456789A123456789B123456789C12 authentication ?
null Use NULL authentication
sha1 Use the SHA1 algorithm
switch(config-router-vlink)# encryption ipsec spi 256 esp aes 128
123456789A123456789B123456789C12 authentication null
```



(注) 複数の OSPFv3 ネイバーに IPsec ESP を許可するには、次のポリシーマップをコントロールプレーンに適用する必要があります。

```
ipv6 access-list copp-acl-ipsec
10 permit ahp any any
20 permit esp any any

class-map type control-plane match-any copp-class-critical-customized-copp
match access-group name copp-acl-ipsec
policy-map type control-plane customized-copp
class copp-class-critical-customized-copp
police cir 36000 kbps bc 1280000 bytes conform transmit violate drop
control-plane
service-policy input customized-copp
```

ルータ レベルで OSPFv3 認証の構成

次のコマンドを使用して、ルータ レベルで OSPFv3 パケットを認証するように OSPFv3 ESP を構成できます。

始める前に

OSPFv3 が有効になっていることを確認してください。詳細は「[OSPFv3の有効化（142 ページ）](#)」を参照してください。

手順の概要

1. configure terminal
2. feature ospfv3
3. feature imp

4. **router ospfv3 instance-tag**
5. **[no] authentication {ipsec spi spi_id [auth_algorithm [0 | 3 | 7] key | key-chain auth_keychain_name | null]}**
6. (任意) **show running-config ospfv3**
7. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	feature ospfv3 例 : <pre>switch(config)# feature ospfv3</pre>	OSPFv3 を有効にします。
ステップ 3	feature imp 例 : <pre>switch(config)# feature imp</pre>	認証モードを有効にします。
ステップ 4	router ospfv3 instance-tag 例 : <pre>switch(config)# router ospfv3 100 switch(config-router)#</pre>	新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 5	[no] authentication {ipsec spi spi_id [auth_algorithm [0 3 7] key key-chain auth_keychain_name null]} 例 : 認証アルゴリズムおよびキー オプションの場合 : <pre>switch(config-router)# authentication ipsec spi 475 md5 11111111111111111222222222222222</pre> キーチェーンの場合 : <pre>switch(config-router)# authentication ipsec spi 333 key-chain test1</pre>	プロセス（または VRF）レベルで OSPFv3 IPsec 認証を設定します。 spi 引数は、セキュリティ パラメータ インデックス（SPI）を指定します。指定できる範囲は 256 ～ 4294967295 です。 auth 引数は、認証のタイプを指定します。サポートされる値は md5 または sha1 です。 0 の場合は、パスワードをクリア テキストで設定します。3 の場合は、パス キーを 3DES 暗号化として設定します。7 パス キーを Cisco タイプ 7 暗号化として設定します。 cleartext オプション（0）を使用する場合、key 引数は md5 では 32 文字、sha1 では 40 文字にする必要があります。

	コマンドまたはアクション	目的
		Cisco NX-OS リリース 10.4(1)F 以降では、 key-chain オプションはキーおよびアルゴリズムを構成するために提供されます。 このコマンドの no 形式を使用して、OSPFv3 IPsec 認証を無効にします。
ステップ 6	(任意) show running-config ospfv3 例 : switch(config)# show running-config ospfv3	OSPFv3 認証構成情報を表示します。
ステップ 7	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	この設定変更を保存します。

エリア レベルで OSPFv3 認証の構成

次のコマンドを使用して、エリア レベルで OSPFv3 パケットを認証するように OSPFv3 ESP を構成できます。

始める前に

OSPFv3 が有効になっていることを確認してください。詳細は「[OSPFv3の有効化（142 ページ）](#)」を参照してください。

手順の概要

1. **configure terminal**
2. **feature ospfv3**
3. **feature imp**
4. **router ospfv3 instance-tag**
5. **[no] area area-id-ip authentication {ipsec spi spi_id[auth_algorithm [0 | 3 | 7] key | key-chain auth_keychain_name | null]**
6. (任意) **show running-config ospfv3**
7. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	feature ospfv3 例 : <pre>switch(config)# feature ospfv3</pre>	OSPFv3 を有効にします。
ステップ 3	feature imp 例 : <pre>switch(config)# feature imp</pre>	認証モードを有効にします。
ステップ 4	router ospfv3 instance-tag 例 : <pre>switch(config)# router ospfv3 100 switch(config-router)#</pre>	新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 5	[no] area area-id-ip authentication {ipsec spi spi_id[auth_algorithm [0 3 7] key key-chain auth_keychain_name null] 例 : 認証アルゴリズムおよびキー オプションの場合 : <pre>switch(config-router)# area 0 authentication ipsec spi 475 md5 11111111111111112222222222222222</pre> キーチェーンの場合 : <pre>switch(config-router)# area 0 authentication ipsec spi 333 key-chain test1</pre>	エリア レベルで OSPFv3 IPsec 認証を設定します。 spi 引数は、セキュリティ パラメータ インデックス (SPI) を指定します。指定できる範囲は 256 ～ 4294967295 です。 auth 引数は、認証のタイプを指定します。サポートされる値は MD5 または SHA-1 です。 0 の場合は、パスワードをクリア テキストで設定します。3 の場合は、パス キーを 3DES 暗号化として設定します。7 : Cisco タイプ 7 暗号化としてキーを構成します。 cleartext オプション (0) を使用する場合、key 引数は MD5 では 32 文字、SHA-1 では 40 文字にする必要があります。 Cisco NX-OS リリース 10.4(1)F 以降では、key-chain オプションはキーおよびアルゴリズムを構成するために提供されます。 このコマンドの no 形式を使用して、OSPFv3 IPsec 認証を無効にします。

	コマンドまたはアクション	目的
ステップ 6	(任意) show running-config ospfv3 例 : switch(config)# show running-config ospfv3	OSPFv3 認証構成情報を表示します。
ステップ 7	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	この設定変更を保存します。

インターフェイス レベルで OSPFv3 認証の構成

次のコマンドを使用して、間隔レベルで OSPFv3 パケットを認証するように OSPFv3 ESP を構成できます。

始める前に

OSPFv3 が有効になっていることを確認してください。詳細は「[OSPFv3の有効化（142 ページ）](#)」を参照してください。

手順の概要

1. **configure terminal**
2. **interfaceinterface-type slot/port**
3. **[no] ospfv3 authentication {disable | ipsec spi spi_id {md5 akey | sha1 akey | key-chain keychain_ah}}**
4. (任意) **show running-config ospfv3**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	interfaceinterface-type slot/port 例 : switch(config)# interface ethernet 1/1 switch(config-if)#	インターフェイス設定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	[no] ospfv3 authentication {disable ipsec spi spi_id {md5 akey sha1 akey key-chain keychain_ah}} 例 : 認証アルゴリズムおよびキー オプションの場合 : <pre>switch(config-if)# ospfv3 authentication ipsec spi 475 md5 11111111111111111222222222222222</pre> キーチェーンの場合 : <pre>switch(config-if)# ospfv3 authentication ipsec spi 333 key-chain test1</pre>	指定したインターフェイスの OSPFv3 IPsec 認証を設定します。 spi 引数は、セキュリティ パラメータ インデックス (SPI) を指定します。指定できる範囲は 256 ~ 4294967295 です。 auth 引数は、認証のタイプを指定します。サポートされる値は MD5 または SHA-1 です。 0 の場合は、パスワードをクリア テキストで設定します。3 の場合は、パス キーを 3DES 暗号化として設定します。7 : Cisco タイプ 7 暗号化としてキーを構成します。 cleartext オプション (0) を使用する場合、key 引数は MD5 では 32 文字、SHA-1 では 40 文字にする必要があります。 Cisco NX-OS リリース 10.4(1)F 以降では、key-chain オプションはキーおよびアルゴリズムを構成するために提供されます。 このコマンドの no 形式を使用して、OSPFv3 IPsec 認証を無効にします。
ステップ 4	(任意) show running-config ospfv3 例 : <pre>switch(config)# show running-config ospfv3</pre>	OSPFv3 認証構成情報を表示します。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

仮想リンク レベルでの OSPFv3 認証の構成

次のコマンドを使用して、仮想リンク レベルで OSPFv3 パケットを認証するように OSPFv3 ESP を構成できます。

始める前に

OSPFv3 が有効になっていることを確認してください。詳細は「[OSPFv3の有効化 \(142 ページ\)](#)」を参照してください。

手順の概要

1. configure terminal

2. **feature ospfv3**
3. **feature imp**
4. **router ospfv3 instance-tag**
5. **area area-id virtual-link router-id**
6. **[no] authentication {ipsec spi spi_id [auth_algorithm [0 | 3 | 7] key | key-chain auth_keychain_name | null]**
7. (任意) **show running-config ospfv3**
8. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	feature ospfv3 例 : switch(config)# feature ospfv3	OSPFv3 を有効にします。
ステップ 3	feature imp 例 : switch(config)# feature imp	認証モードを有効にします。
ステップ 4	router ospfv3 instance-tag 例 : switch(config)# router ospfv3 100 switch(config-router)#	新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 5	area area-id virtual-link router-id 例 : switch(config-router)# area 0.0.0.10 virtual-link 2001:0DB8::1 switch(config-router-vlink)#	リモートルータへの仮想リンクの端を作成します。 仮想リンクをリモートルータ上に作成して、リンクを完成させる必要があります。
ステップ 6	[no] authentication {ipsec spi spi_id [auth_algorithm [0 3 7] key key-chain auth_keychain_name null] 例 : 認証アルゴリズムおよびキー オプションの場合 : switch(config-router-vlink)# authentication ipsec spi 475 md5 11111111111111112222222222222222	仮想リンク レベルで OSPFv3 IPsec 認証を構成します。 spi 引数は、セキュリティ パラメータ インデックス (SPI) を指定します。指定できる範囲は 256 ~ 4294967295 です。

	コマンドまたはアクション	目的
	キーチェーンの場合 : <pre>switch(config-router-vlink)# authentication ipsec spi 333 key-chain test1</pre>	auth 引数は、認証のタイプを指定します。サポートされる値は MD5 または SHA-1 です。 0 の場合は、パスワードをクリア テキストで設定します。3 の場合は、パス キーを 3DES 暗号化として設定します。7 : Cisco タイプ 7 暗号化としてキーを構成します。 cleartext オプション (0) を使用する場合、key 引数は MD5 では 32 文字、SHA-1 では 40 文字にする必要があります。 Cisco NX-OS リリース 10.4(1)F 以降では、key-chain オプションはキーおよびアルゴリズムを構成するために提供されます。 このコマンドの no 形式を使用して、OSPFv3 IPsec 認証を無効にします。
ステップ 7	(任意) show running-config ospfv3 例 : <pre>switch(config)# show running-config ospfv3</pre>	OSPFv3 認証構成情報を表示します。
ステップ 8	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

OSPFv3 の設定の確認

OSPFv3 の設定を表示するには、次のいずれかのタスクを実行します。

コマンド	目的
show ipv6 ospfv3	OSPFv3 設定を表示します。
show ipv6 ospfv3 border-routers	ABR および ASBR への内部 OSPF ルーティング テーブル エントリを表示します
show ipv6 ospfv3 database	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。
show ipv6 ospfv3 interface type number [vrf { vrf-name all default management }]	OSPFv3 インターフェイス設定を表示します。

コマンド	目的
show ipv6 ospfv3 neighbors	ネイバー情報を表示します。 clear ospfv3 neighbors コマンドを使用すると、すべてのネイバーとの隣接関係を削除できます。
show ipv6 ospfv3 request-list	ルータから要求されている LSA の一覧を表示します。
show ipv6 ospfv3 retransmission-list	再送を待っている LSA の一覧を表示します。
show ipv6 ospfv3 summary-address	OSPFv3 インスタンスで設定されている、すべての集約アドレス再配布情報の一覧を表示します。
show ospfv3 process	プロセス レベルの OSPFv3 認証設定を表示します。
show ospfv3 interface <i>interface-type slot/port</i>	インターフェイス レベルでの OSPFv3 認証設定を表示します。
show running-configuration ospfv3	現在実行中の OSPFv3 コンフィギュレーションを表示します。

OSPFv3のモニタリング

OSPFv3 統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
show ipv6 ospfv3 memory	OSPFv3 メモリ使用状況の統計情報を表示します。
show ipv6 ospfv3 policy statistics area <i>area-id</i> filter-list {in out} [vrf { <i>vrf-name</i> all default management}]	エリアの OSPFv3 ルート ポリシー統計情報を表示します。
show ipv6 ospfv3 policy statistics redistribute { bgp <i>id</i> direct isis <i>id</i> rip <i>id</i> static } vrf { <i>vrf-name</i> all default management}]	OSPFv3 ルート ポリシー統計を表示します。
show ipv6 ospfv3 statistics [vrf { <i>vrf-name</i> all default management}]	OSPFv3 イベント カウンタを表示します
show ipv6 ospfv3 traffic [<i>interface-type number</i>] [vrf { <i>vrf-name</i> all default management}]	OSPFv3 パケット カウンタを表示します。

OSPFv3 の設定例

次に、OSPFv3 を設定する例を示します。

```
feature ospfv3
router ospfv3 201
router-id 290.0.2.1

interface ethernet 1/2
ipv6 address 2001:0DB8::1/48

ipv6 ospfv3 201 area 0.0.0.10
```

key-chain オプションを使用して、OSPFv3 暗号を構成する例を示します。

```
switch(config-if)# ospfv3 encryption ipsec spi 333 esp ?
  3des      Use the triple DES algorithm
  aes       Use the AES algorithm
  key-chain Encryption password key-chain
  null      Use NULL authentication
switch(config-if)# ospfv3 encryption ipsec spi 333 esp key-chain ?
  WORD Encryption key-chain name (Max Size 63)
switch(config-if)# ospfv3 encryption ipsec spi 333 esp key-chain test1 ?
  authentication Specify authentication parameters
switch(config-if)# ospfv3 encryption ipsec spi 333 esp key-chain test1 authentication ?
  key-chain Authentication password key-chain
  null      Use NULL authentication
switch(config-if)# ospfv3 encryption ipsec spi 333 esp key-chain test1 authentication
key-chain ?
  WORD Authentication key-chain name (Max Size 63)
switch(config-if)# ospfv3 encryption ipsec spi 333 esp key-chain test1 authentication
key-chain test2 ?
  <CR>
switch(config-router)# sh ospfv3
Routing Process 2 with ID 20.20.10.2 VRF default
Routing Process Instance Number 1
Install discard route for summarized internal routes.
ESP Encryption 3DES, Authentication SHA1, SPI 334, ConnId 334
ESP keychains: Enchr test_key_chain_01(ready), Auth test1(ready)
Number of new LSAs originated : 3
Number of new LSAs received : 0
```

関連項目

次の項目には、OSPF に関する詳細情報が含まれています。

- [OSPFv2 の設定（75 ページ）](#)
- [Route Policy Manager の設定（443 ページ）](#)

その他の参考資料

OSPF の実装に関する詳細情報については、次のページを参照してください。

MIB

MIB	MIB のリンク
• OSPF-MIB • OSPF-TRAP-MIB	MIB を検索してダウンロードするには、次の MIB ロケータ に移動します。



第 7 章

EIGRP の設定

この章では、Cisco NX-OS スイッチで Enhanced Interior Gateway Routing Protocol (EIGRP) を設定する方法について説明します。

この章は、次の項で構成されています。

- [EIGRP に関する情報 \(193 ページ\)](#)
- [EIGRP の前提条件 \(200 ページ\)](#)
- [注意事項と制約事項 \(200 ページ\)](#)
- [デフォルト設定 \(201 ページ\)](#)
- [基本的な EIGRP の設定 \(202 ページ\)](#)
- [高度な EIGRP の設定 \(206 ページ\)](#)
- [EIGRP の仮想化の設定 \(219 ページ\)](#)
- [EIGRP の設定の確認 \(221 ページ\)](#)
- [EIGRP 統計情報の表示 \(222 ページ\)](#)
- [EIGRP の設定例 \(222 ページ\)](#)
- [関連項目 \(222 ページ\)](#)
- [その他の参考資料 \(223 ページ\)](#)

EIGRP に関する情報

EIGRP は、リンクステートプロトコルの機能にディスタンス ベクトル プロトコルの利点を組み合わせたプロトコルです。EIGRP は、定期的に Hello メッセージを送信してネイバーを探索します。EIGRP は、新規ネイバーを検出すると、すべてのローカル EIGRP ルートおよびルート メトリックに対する 1 回限りの更新を送信します。受信側の EIGRP ルータは、受信したメトリックと、その新規ネイバーにローカルで割り当てられたリンクのコストに基づいて、ルート ディスタンスを計算します。この最初の全面的なルート テーブルの更新後は、ルート変更の影響を受けるネイバーにのみ、差分更新が EIGRP により送信されます。この処理により、コンバージェンスにかかる時間が短縮され、EIGRP が使用する帯域幅が最小限になります。

EIGRP コンポーネント

EIGRP には、次の基本コンポーネントがあります。

- Reliable Transport Protocol
- ネイバー探索およびネイバー回復
- 拡散更新アルゴリズム

信頼性の高いトランスポート プロトコル

信頼性の高いトランスポート プロトコルは、すべてのネイバーに EIGRP パケットの順序付けされた配信を保証します。(「[ネイバー探索およびネイバー回復](#)」の項を参照してください。)
信頼性の高いトランスポート プロトコルは、マルチキャスト パケットとユニキャスト パケットの混合伝送をサポートしています。この転送は信頼性が高く、未確認パケットが保留されているときにも、マルチキャストパケットの迅速な送信が可能です。この方式により、さまざまな速度のリンクでも短いコンバージェンス時間が維持されるようになります。マルチキャストおよびユニキャストパケットの送信を制御するデフォルトタイマーの変更の詳細については、「[高度な EIGRP の構成](#)」を参照してください。

Reliable Transport Protocol には、次のメッセージ タイプが含まれます。

- **Hello** : ネイバー探索およびネイバー回復に使用されます。EIGRP はデフォルトでは、定期的なマルチキャスト Hello メッセージをローカル ネットワーク上に、設定された hello 間隔で送信します。デフォルトの hello 間隔は 5 秒です。
- **Acknowledgement** : 更新、照会、返信を確実に受信したことを確認します。
- **Updates** : ルーティング情報が変更されると、その影響を受けるネイバーに送信されます。更新には、ルート宛先、アドレス マスク、および遅延や帯域幅などのルート メトリックが含まれます。更新情報は EIGRP トポロジ テーブルに格納されます。
- **Queries and Replies** : 必要に応じて、EIGRP が使用する DUAL の一部として送信されます。

ネイバー探索およびネイバー回復

EIGRP は、Reliable Transport Protocol からの Hello メッセージを使用して、直接接続されたネットワーク上のネイバー EIGRP ルータを探索します。EIGRP により、ネイバー テーブルにネイバーが追加されます。ネイバー テーブルの情報には、ネイバー アドレス、検出されたインターフェイス、およびネイバー到達不能を宣言する前に EIGRP が待機する時間を示すホールド タイムが含まれています。デフォルトのホールド タイムは、hello 間隔の 3 倍または 15 秒です。

EIGRP は、ローカル EIGRP ルーティング情報を共有するために、一連の更新メッセージを新規ネイバーに送信します。このルート情報は EIGRP トポロジ テーブルに格納されます。このように EIGRP ルート情報全体を最初に送信した後は、ルーティングが変更されたときのみ、EIGRP により更新メッセージが送信されます。これらの更新メッセージは新情報または更新情

報のみを含んでおり、変更の影響を受けるネイバーにのみ送信されます。「[EIGRP ルートアップデート](#)」の項を参照してください。

EIGRP はまた、Hello メッセージをネイバーへのキープアライブのためにも使用します。Hello メッセージを受信している限り、Cisco NX-OS は、ネイバーがダウンせずに機能していると判定します。

拡散更新アルゴリズム

拡散更新アルゴリズム (DUAL) により、トポロジテーブルの宛先ネットワークに基づいてルーティング情報が計算されます。トポロジテーブルには、次の情報が含まれます。

- IPv4 アドレス/マスク：この宛先のネットワーク アドレスおよびネットワーク マスク。
- サクセサ：現在のフィジブルディスタンスよりも宛先まで短いディスタンスをアドバタイズする、すべてのフィジブルサクセサまたはネイバーの IP アドレスおよびローカルインターフェイス接続。
- フィージビリティディスタンス (FD)：計算された、宛先までの最短ディスタンス。フィジブルディスタンスは、ネイバーがアドバタイズした距離に、そのネイバーへのリンクコストを加えた合計です。

DUAL は、ディスタンス メトリックを使用して、ループが発生しない効率的なパスを選択します。DUAL はルートを選択し、フィジブルサクセサに基づいてユニキャストルーティング情報ベース (RIB) に挿入します。トポロジが変更されると、DUAL は、トポロジテーブルでフィジブルサクセサを探します。フィジブルサクセサが見つかった場合、DUAL は、最短のフィジブルディスタンスを持つフィジブルサクセサを選択して、それをユニキャスト RIB に挿入します。これにより、再計算が不要となります。

フィジブルサクセサが存在しないが、宛先をアドバタイズするネイバーが存在する場合は、DUAL がパッシブ状態からアクティブ状態へと移行し、新しいサクセサまたは宛先へのネクストホップルータを決定する再計算をトリガーします。ルートの再計算に必要な時間は、コンバージェンス時間に影響します。EIGRP は照会メッセージをすべてのネイバーに送信し、フィジブルサクセサを探します。フィジブルサクセサを持つネイバーは、その情報を含む返信メッセージを送信します。フィジブルサクセサを持たないネイバーは、DUAL の再計算をトリガーします。

EIGRP ルート更新

トポロジが変更されると、EIGRP は、変更されたルーティング情報のみを含む更新メッセージに影響を受けるネイバーに送信します。更新メッセージには、新規の、または更新されたネットワーク宛先へのディスタンス情報が含まれます。

EIGRP でのディスタンス情報は、帯域幅、遅延、負荷使用状況、リンクの信頼性などの使用可能なルートメトリックの組み合わせとして表現されます。各メトリックには重みが関連付けられており、これにより、メトリックがディスタンスの計算に含まれるかどうかが決まります。このメトリックの重みは設定することができます。特性を微調整して最適なパスを完成するこ

ともできますが、設定可能なメトリックの大部分でデフォルト設定を使用することを推奨します。

内部ルート メトリック

内部ルートとは、同じ EIGRP 自律システム内のネイバー間のルートです。これらのルートには、次のメトリックがあります。

- **ネクスト ホップ**：ネクスト ホップ ルータの IP アドレス。
- **遅延**：宛先ネットワークへのルートを形成するインターフェイス上で設定された遅延の合計。10 マイクロ秒単位で設定されます。
- **帯域幅**：宛先へのルートの一部であるインターフェイスで設定された最小帯域幅から計算されます。



(注) デフォルト帯域幅の値の使用を推奨します。この帯域幅パラメータは EIGRP でも使用されます。

- **MTU**：宛先へのルート上の最大伝送単位の最小値。
- **ホップカウント**：宛先までにルートが通過するホップまたはルータの数。このメトリックは、DUAL 計算で直接には使用されません。
- **信頼性**：宛先までのリンクの信頼性を示します。
- **負荷**：宛先までのリンク上のトラフィック量を示します。

デフォルトで EIGRP は、帯域幅と遅延のメトリックを使用して、宛先までのディスタンスを計算します。計算に他のメトリックが含まれるように、メトリックの重みを変更できます。

外部ルート メトリック

外部ルートとは、異なる EIGRP 自律システムにあるネイバー間のルートです。これらのルートには、次のメトリックがあります。

- **ネクスト ホップ**：ネクスト ホップ ルータの IP アドレス。
- **ルータ ID**：このルートを EIGRP に再配布したルータのルータ ID。
- **AS 番号**：宛先の自律システムの番号。
- **プロトコル ID**：宛先へのルートを学習したルーティング プロトコルを表すコード。
- **タグ**：ルート マップで使用可能な任意のタグ。
- **メトリック**：外部ルーティング プロトコルの、このルートのルート メトリック。

EIGRP とユニキャスト RIB

EIGRP は、すべての学習したルートを EIGRP トポロジテーブルとユニキャスト RIB に追加します。トポロジが変更されると、EIGRP は、これらのルートを使用してフィジブル サクセサを探します。EIGRP は、他のルーティングプロトコルから EIGRP に再配布されたあらゆるルートの変更についてのユニキャスト RIB からの通知も待ち受けます。

高度な EIGRP

EIGRP の高度な機能を使用して、EIGRP の設定を最適化できます。

アドレス ファミリ

EIGRP は、IPv4 アドレス ファミリをサポートします。

アドレス ファミリ コンフィギュレーション モードには、次の EIGRP 機能が含まれます。

- 認証
- AS 番号
- デフォルト ルート
- メトリック
- ディスタンス
- グレースフル リスタート
- ロギング
- ロード バランシング
- 再分配
- ルータ ID
- スタブ ルータ
- タイマー

複数のコンフィギュレーションモードで同じ機能を設定できません。たとえばルータコンフィギュレーションモードでデフォルトメトリックを設定すると、アドレスファミリモードでデフォルトメトリックを設定できません。

認証

EIGRP メッセージに認証を設定することで、ネットワークでの不正なルーティング更新や無効なルーティング更新を防止できます。EIGRP 認証は MD5 認証ダイジェストをサポートしています。

認証キーのキーチェーン管理を使用して、仮想ルーティング/転送 (VRF) インスタンスごと、またはインターフェイスごとに EIGRP 認証を設定できます。キーチェーン管理を使用すると、MD5 認証ダイジェストが使用する認証キーへの変更を管理できます。

MD5 認証を行うには、ローカル ルータとすべてのリモート EIGRP ネイバーで同一のパスワードを設定します。EIGRP メッセージが作成されると、Cisco NX-OS は、そのメッセージ自体と暗号化されたパスワードに基づいて MD5 一方方向メッセージダイジェストを作成し、このダイジェストを EIGRP メッセージとともに送信します。受信する EIGRP ネイバーは、同じ暗号化パスワードを使用して、このダイジェストを確認します。メッセージが変更されていない場合は計算が同一であるため、EIGRP メッセージは有効と見なされます。

MD5 認証には各 EIGRP メッセージのシーケンス番号も含まれており、これにより、ネットワークでのメッセージの再送が防止されます。

スタブ ルータ

EIGRP スタブ ルーティング機能を使用すると、ネットワークの安定性の向上、リソース使用量の削減、スタブ ルータ設定の簡易化を実現できます。スタブ ルータは、リモート ルータ経由で EIGRP ネットワークに接続します。「[スタブ ルーティング](#)」の項を参照してください。

EIGRP スタブ ルーティングを使用すると、EIGRP を使用するように配布とリモート ルータを設定し、リモート ルータのみをスタブ として設定する必要があります。EIGRP スタブ ルーティングで、分散 ルータでの集約が自動的にイネーブルになるわけではありません。ほとんどの場合、分散 ルータでの集約の設定が必要です。

EIGRP スタブ ルーティングを使用しない場合は、分散 ルータからリモート ルータに送信されたルートがフィルタリングまたは集約された後でも、問題が発生することがあります。たとえば、ルートが企業ネットワーク内のどこかで失われた場合に、EIGRP が分散 ルータに照会を送信することがあります。分散 ルータは、ルートが集約されている場合でも、リモート ルータに照会を送信することがあります。分散 ルータとリモート ルータの間の WAN リンク上の通信に問題が発生した場合は、EIGRP がアクティブ状態のままとなり、ネットワークの他の場所が不安定となる場合があります。EIGRP スタブ ルーティングを使用すると、リモート ルータに照会が送信されなくなります。

ルート集約

指定したインターフェイスにサマリー集約アドレスを設定できます。ルート集約を使用すると、固有性の強い一連のアドレスをすべての固有アドレスを代表する 1 つのアドレスに置き換えることによって、ルート テーブルを簡素化できます。たとえば、10.1.1.0/24、10.1.2.0/24、および 10.1.3.0/24 というアドレスを 1 つの集約アドレス 10.1.0.0/16 に置き換えることができます。

より具体的なアドレスがルーティング テーブルにある場合、EIGRP は、より具体的なルートの最小メトリックに等しいメトリックを持つインターフェイスからの集約アドレスをアドバタイズします。



(注) EIGRP は、自動ルート集約をサポートしていません。

ルートの再配布

EIGRP を使用して、ダイレクトルート、スタティックルート、他の EIGRP 自律システムから学習したルート、または他のプロトコルからのルートを再配布できます。再配布を含むルートマップを設定して、どのルートが EIGRP に渡されるかを制御します。ルートマップを使用すると、宛先、送信元プロトコル、ルートタイプ、ルートタグなどの属性に基づいて、ルートをフィルタリングできます。[Route Policy Manager の設定 \(443 ページ\)](#) を参照してください。

インポートされた EIGRP へのすべてのルートに使用されるデフォルトメトリックも設定できます。

ロードバランシング

ロードバランシングを使用すると、ルータは、宛先アドレスから等距離内にあるすべてのルータのネットワークポートにトラフィックを分散できます。ロードバランシングにより、ネットワークセグメントの使用率が向上し、それによってネットワーク帯域幅の効率も向上します。

Cisco NX-OS は、等コストマルチパス (ECMP) 機能をサポートします。EIGRP ルートテーブルおよびユニキャスト RIB の等コストパスは最大 16 です。これらのパスの一部または全部に対してトラフィックのロードバランスを行うよう、EIGRP を設定できます。



(注) Cisco NX-OS の EIGRP は、等コストでないロードバランシングはサポートしていません。

Split Horizon

スプリットホライズンを使用すると、ルートを学習したインターフェイスから EIGRP がルートをアドバタイズしないようにできます。

スプリットホライズンは、EIGRP 更新パケットおよび EIGRP 照会パケットの送信を制御する方式です。インターフェイスでスプリットホライズンをイネーブルにすると、Cisco NX-OS は、このインターフェイスから学習された宛先への更新パケットも照会パケットも送信しません。この方法でアップデートパケットとクエリーパケットを制御すると、ルーティングループが発生する可能性が低くなります。

ポイズンリバーによるスプリットホライズンにより、EIGRP は、EIGRP がルートを学習したインターフェイス経由で、そのルートを到達不能としてアドバタイズするよう設定されます。

EIGRP は、次のシナリオでスプリットホライズン、またはポイズンリバーによるスプリットホライズンを使用します。

- スタートアップモードで、2 台のルータ間で初めてトポロジテーブルを交換する。
- トポロジテーブルの変更をアドバタイズする。
- 照会メッセージを送信する。

デフォルトでは、スプリットホライズン機能がすべてのインターフェイスでイネーブルになっています。

仮想化のサポート

Cisco NX-OSは、同一システム上で動作する複数のEIGRPプロトコルインスタンスをサポートします。EIGRPは、仮想ルーティングおよび転送（VRF）インスタンスをサポートしています。デフォルトでは、特に別のVRFを設定しない限り、Cisco NX-OSはユーザーをデフォルトのVRFに配置します。「[レイヤ3 仮想化の構成](#)」を参照してください

デフォルトでは、すべてのインスタンスが同じシステム ルータ ID を使用します。インスタンスごとに一意のルータ ID を設定することもできます。

EIGRP の前提条件

EIGRP を使用するには、次の前提条件を満たしている必要があります。

- EIGRP 機能をイネーブルにする必要があります（[EIGRP 機能のイネーブル化](#)を参照）。

注意事項と制約事項

EIGRP 設定時の注意事項および制約事項は次のとおりです。

- 他のプロトコル、接続されたルータ、またはスタティックルートからの再配布には、メトリック設定（デフォルトメトリック設定オプションまたはルートマップによる）が必要です（[Route Policy Manager の設定（443 ページ）](#)を参照）。
- グレースフルスタートについては、NSF 認識ルータが動作中であり、ネットワークで完全に収束している場合にのみ、このルータが NSF 対応ルータのグレースフルリスタート動作を支援できます。
- グレースフルリスタートについては、グレースフルリスタートに関係する隣接スイッチが NSF 認識、または NSF 対応である必要があります。
- Cisco NX-OS の EIGRP は Cisco IOS ソフトウェアの EIGRP と互換性があります。
- 妥当な理由がない限り、メトリックの重みを変更しないでください。メトリックの重みを変更した場合は、同じ自律システム内のすべての EIGRP ルータに、それを適用する必要があります。
- 大規模ネットワークの場合は、スタブの使用を検討してください。
- EIGRP ベクトルメトリックは維持されないため、異なる EIGRP 自律システム間での再配布は避けてください。
- `no ip next-hop-self` コマンドは、ネクストホップの到達可能性を保証しません。
- `ip passive-interface eigrp` コマンドを使用すると、ネイバーが形成されなくなります。

- Cisco NX-OS は IGRP も、IGRP および EIGRP クラウドの接続もサポートしていません。
- 自動集約は、デフォルトではイネーブルにされていません。
- Cisco NX-OS は IP のみをサポートします。



(注) Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合がありますので注意してください。

デフォルト設定

次のテーブルは、各 EIGRP パラメータに対するデフォルト設定を示します。

表 13: テーブル 6-1 デフォルト EIGRP パラメータ

パラメータ	デフォルト
アドミニストレーティブ ディスタンス	• 内部ルート : 90 • 外部ルート : 170
帯域幅の割合	50%
再配布されたルートのデフォルトのメトリック	• bandwidth : 100000 kbps • delay : 100 (10 マイクロ秒単位) • reliability : 255 • loading : 1 • MTU : 1500
EIGRP 機能	ディセーブル
hello 間隔	5 秒
Hold time	15 秒
等コスト パス	8
メトリック重み	1 0 1 0 0
アドバタイズされたネクスト ホップ アドレス	ローカル インターフェイスの IP アドレス
NSF コンバージェンス時間	120

パラメータ	デフォルト
NSF ルート保留時間	240
NSF 信号送信時間	20
再分配	ディセーブル
スプリット ホライズン	有効 (Enabled)

基本的な EIGRP の設定

このセクションは、次のトピックで構成されています。

EIGRP 機能の有効化

EIGRP を設定するには、その前に EIGRP 機能をイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **feature eigrp**
3. (任意) **show feature**
4. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	feature eigrp 例 : <pre>switch(config)# feature eigrp</pre>	EIGRP 機能を有効にします。
ステップ 3	(任意) show feature 例 : <pre>switch(config)# show feature</pre>	有効にされた機能に関する情報を表示し。

	コマンドまたはアクション	目的
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

例

no feature eigrp コマンドを使用して、BFD 機能を無効にし、関連する構成をすべて削除します。

コマンド	目的
no feature eigrp 例 : <pre>switch(config)# no feature eigrp</pre>	EIGRP 機能をディセーブルにして、関連付けられたコンフィギュレーションをすべて削除します。

EIGRP インスタンスの作成

EIGRP インスタンスを作成して、そのインスタンスにインターフェイスを関連付けることができます。この EIGRP プロセスに一意の自律システム番号を割り当てます（「[自律システム](#)」の項を参照）。ルート再配布をイネーブルにしていない限り、他の自律システムからルートがアドバタイズされることも、受信されることもありません。

始める前に

EIGRP 機能を有効にしていることを確認します（[EIGRP 機能の有効化](#)のセクションを参照）。

EIGRP がルータ ID（設定済みのループバックアドレスなど）を入手可能であるか、またはルータ ID オプションを設定する必要があります。

AS 番号であると認められていないインスタンス タグを設定する場合は、AS 番号を明示的に設定する必要があります。そうしないと、この EIGRP インスタンスはシャットダウン状態のままになります。

手順の概要

1. **configure terminal**
2. **router eigrp instance-tag**
3. (任意) **autonomous-system as-number**
4. (任意) **log-adjacency-changes**
5. (任意) **log-neighbor-warnings [seconds]**
6. **interface interface-type slot/port**
7. **no switchport**
8. **ip router eigrp instance-tag**

9. **show ip eigrp interfaces**10. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router eigrp instance-tag 例 : <pre>switch(config)# router eigrp Test1 switch(config-router)#</pre>	インスタンス タグを設定して、新しい EIGRP プロセスを作成します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。 AS 番号であると認められていない <i>instance-tag</i> を構成する場合は、 autonomous-system コマンドを使用して AS 番号を明示的に構成する必要があります。そうしないと、この EIGRP インスタンスはシャットダウン状態のままになります。
ステップ 3	(任意) autonomous-system as-number 例 : <pre>switch(config-router)# autonomous-system 33</pre>	この EIGRP インスタンスに一意の AS 番号を設定します。有効な範囲は 1 ～ 65535 です。
ステップ 4	(任意) log-adjacency-changes 例 : <pre>switch(config-router)# log-adjacency-changes</pre>	隣接関係の状態が変化するたびに、システム メッセージを生成します。このコマンドは、デフォルトでイネーブルになっています。
ステップ 5	(任意) log-neighbor-warnings [seconds] 例 : <pre>switch(config-router)# log-neighbor-warnings</pre>	ネイバーの警告が発生するたびに、システム メッセージを生成します。警告メッセージの時間間隔を、1 ～ 65535 の秒数で設定できます。デフォルトは 10 秒です。このコマンドは、デフォルトでイネーブルになっています。
ステップ 6	interface interface-type slot/port 例 : <pre>switch(config-router)# interface ethernet 1/2 switch(config-if)#</pre>	インターフェイス設定モードを開始します。? を使用すると、スロットおよびポートの範囲を確認できます。
ステップ 7	no switchport 例 :	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。

	コマンドまたはアクション	目的
	<code>switch(config-if)# no switchport</code>	
ステップ 8	ip router eigrp instance-tag 例 : <code>switch(config-if)# ip router eigrp Test1</code>	このインターフェイスを、設定された EIGRP プロセスに関連付けます。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 9	show ip eigrp interfaces 例 : <code>switch(config-if)# show ip eigrp interfaces</code>	EIGRP インターフェイスに関する情報を表示します。
ステップ 10	(任意) copy running-config startup-config 例 : <code>switch(config)# copy running-config startup-config</code>	この設定変更を保存します。

例

EIGRP プロセスと、関連付けられた設定を削除するには、**no router eigrp** コマンドを使用します。

コマンド	目的
no router eigrp instance-tag 例 : <code>switch(config)# no router eigrp Test1</code>	EIGRP プロセスと、関連付けられたすべての設定を削除します。



(注) EIGRP プロセスを削除する場合は、インターフェイス モードで設定された EIGRP コマンドも削除する必要があります。

次に、EIGRP プロセスを作成し、EIGRP のインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# router eigrp Test1
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip router eigrp Test1
switch(config-if)# no shutdown
switch(config-if)# copy running-config startup-config
```

その他の EIGRP パラメータの詳細については、[高度な EIGRP の設定](#)のセクションを参照してください。

EIGRP インスタンスの再起動

EIGRP インスタンスを再起動できます。再起動すると、インスタンスのすべてのネイバーが消去されます。

EIGRP インスタンスを再起動して、関連付けられたすべてのネイバーを削除するには、次のコマンドを使用します。

コマンド	目的
flush-routes 例 : <pre>switch(config)# flush-routes</pre>	この EIGRP インスタンスを再起動するときに、ユニキャスト RIB のすべての EIGRP ルートをフラッシュします。
restart eigrp instance-tag 例 : <pre>switch(config)# restart eigrp Test1</pre>	EIGRP インスタンスを再起動して、すべてのネイバーを削除します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。

EIGRP インスタンスのシャットダウン

EIGRP インスタンスを正常にシャットダウンできます。これにより、すべてのルートと隣接関係は移動しますが、EIGRP 設定は保持されます。

EIGRP インスタンスをディセーブルにするには、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
shutdown 例 : <pre>switch(config-router)# shutdown</pre>	この EIGRP インスタンスをディセーブルにします。EIGRP ルータ設定は残ります。

高度な EIGRP の設定

このセクションは、次のトピックで構成されています。

EIGRP での認証の設定

EIGRP のネイバー間に認証を設定できます。「[認証 \(Authentication\)](#)」セクションを参照してください。

EIGRP プロセスまたは個々のインターフェイスに対応する EIGRP 認証を設定できます。インターフェイスの EIGRP 認証設定は、EIGRP プロセスレベルの認証設定よりも優先します。

始める前に

EIGRP 機能を有効にしていることを確認します（[EIGRP 機能の有効化](#)のセクションを参照）。

EIGRP プロセスのすべてのネイバーが、共有認証キーを含め、同じ認証設定を共有することを確認します。

この認証構成のためのキー チェーンを作成します。

手順の概要

1. **configure terminal**
2. **router eigrp instance-tag**
3. **address-family ipv4 unicast**
4. **authentication keychain keychain**
5. **authentication mode md5**
6. **interface interface-type slot/port**
7. **no switchport**
8. **ip router eigrp instance-tag**
9. **ip authentication keychain eigrp instance-tag keychain**
10. **ip authentication mode eigrp instance-tag md5**
11. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	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	router eigrp instance-tag 例： <pre>switch(config)# router eigrp Test1 switch(config-router)#</pre>	インスタンス タグを設定して、新しい EIGRP プロセスを作成します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。 AS 番号であると認められていない <i>instance-tag</i> を構成する場合は、 autonomous-system コマンドを使用して AS 番号を明示的に構成する必要があります。そうしないと、この EIGRP インスタンスはシャットダウン状態のままになります。

	コマンドまたはアクション	目的
ステップ 3	address-family ipv4 unicast 例 : <pre>switch(config-router)# address-family ipv4 unicast switch(config-router-af)#</pre>	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。IPv4 の場合、このコマンドはオプションです。
ステップ 4	authentication keychain keychain 例 : <pre>switch(config-router-af)# authentication keychain routeKeys</pre>	この VRF の EIGRP プロセスにキーチェーンを関連付けます。キー チェーン名は、大文字と小文字が区別される 20 文字以下の任意の英数字文字列にできます。
ステップ 5	authentication mode md5 例 : <pre>switch(config-router-af)# authentication mode md5</pre>	この VRF の MD5 メッセージダイジェスト認証モードを設定します。
ステップ 6	interface interface-type slot/port 例 : <pre>switch(config-router-af) interface ethernet 1/2 switch(config-if)#</pre>	インターフェイス設定モードを開始します。? を使用すると、サポートされているインターフェイスを調べることができます。
ステップ 7	no switchport 例 : <pre>switch(config-if)# no switchport</pre>	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 8	ip router eigrp instance-tag 例 : <pre>switch(config-if)# ip router eigrp Test1</pre>	このインターフェイスを、設定された EIGRP プロセスに関連付けます。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 9	ip authentication keychain eigrp instance-tag keychain 例 : <pre>switch(config-if)# ip authentication keychain eigrp Test1 routeKeys</pre>	このインターフェイスの EIGRP プロセスにキーチェーンを関連付けます。この設定は、ルータの VRF モードで設定された認証設定よりも優先します。 インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 10	ip authentication mode eigrp instance-tag md5 例 : <pre>switch(config-if)# ip authentication mode eigrp Test1 md5</pre>	このインターフェイスの MD5 メッセージダイジェスト認証モードを設定します。この設定は、ルータの VRF モードで設定された認証設定よりも優先します。 インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。

	コマンドまたはアクション	目的
ステップ 11	copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、EIGRP の MD5 メッセージ ダイジェスト 認証をイーサネット インターフェイス 1/2 上で設定する例を示します。

```
switch# configure terminal
switch(config)# router eigrp Test1
switch(config-router)# exit
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip router eigrp Test1
switch(config-if)# ip authentication keychain eigrp Test1 routeKeys
switch(config-if)# ip authentication mode eigrp Test1 md5
switch(config-if)# copy running-config startup-config
```

EIGRP スタブ ルーティングの設定

ルータで EIGRP スタブ ルーティングを設定するには、アドレス ファミリ 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
stub [direct receive-only redistributed [direct] leak-map map-name] 例 : <pre>switch(config-router-af)# eigrp stub redistributed</pre>	リモート ルータを EIGRP スタブ ルータとして設定します。リークマップのマップネーム名は、構成されたルートマップを参照します。複数のオプションを一度に構成して、目的のスタブ ルータ機能を有効にすることができます。

次に、直接接続され、再配布されるルートをアドバタイズするスタブ ルータを設定する例を示します。

```
switch# configure terminal

switch(config)# router eigrp Test1

switch(config-router)# address-family ipv4 unicast

switch(config-router-af)# stub direct redistributed

switch(config-router-af)# copy running-config startup-config
```

ルータがスタブ ルータとして設定されていることを確認するには、**show ip eigrp neighbor detail** コマンドを使用します。出力の最後の行は、リモート ルータまたはスポーク ルータのスタブ ステータスを示します。次に、**ip eigrp neighbor detail** コマンドの出力例を示します。

```
Router# show ip eigrp neighbor detail
IP-EIGRP neighbors for process 201
H Address Interface Hold Uptime SRTT RTO Q Seq Type
(sec) (ms) Cnt Num
0 10.1.1.2 Se3/1 11 00:00:59 1 4500 0 7
Version 12.1/1.2, Retrans: 2, Retries: 0
Stub Peer Advertising ( CONNECTED SUMMARY) Routes
```

EIGRP のサマリー アドレスの設定

指定したインターフェイスにサマリー集約アドレスを設定できます。ルーティングテーブルに他にも個別のルートがある場合、EIGRPは、他の個別ルートすべての中で最小のメトリックと等しいメトリックで、サマリーアドレスをインターフェイスからアドバタイズします。「[ルート集約](#)」の項を参照してください。

サマリー集約アドレスを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
ip summary-address eigrp <i>instance-tag ip-prefix/length [</i> <i>distance leak-map map-name</i> <i>]</i> 例 : <pre>switch(config-if)# ip summary-address eigrp Test1 192.0.2.0/8</pre>	サマリー集約アドレスを、IP プレフィックス/長さとして設定します。インスタンスタグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。リークマップのマップネーム名は、構成されたルートマップを参照します。 また、この集約アドレスのアドミニストレーティブ ディスタンスを設定することもできます。集約アドレスのデフォルトアドミニストレーティブ ディスタンスは 5 です。 (注) EIGRP がすでに実行されている場合を除き、プレフィックス/長さ形式をアドレスマスクの代わりに使用して IP アドレスを設定することを推奨します。EIGRP インスタンスが起動する前にアドレスマスク形式を使用すると、後でサマリーアドレスを削除または変更できなくなります。

次に、EIGRP によりネットワーク 192.0.2.0 がイーサネット 1/2 のみに集約されるようにする例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip summary-address eigrp Test1 192.0.2.0 255.255.255.0
```

EIGRP へのルートの再配布

他のルーティング プロトコルから EIGRP にルートを再配布できます。

始める前に

EIGRP 機能を有効にしていることを確認します ([EIGRP 機能の有効化](#)のセクションを参照)。

他のプロトコルから再配布されるルートには、メトリック（デフォルト メトリック 設定オプションまたはルート マップによる）を設定する必要があります。

ルートマップを作成して、EIGRP に再配布されるルートのタイプを管理する必要があります。
[Route Policy Manager の設定（443 ページ）](#) を参照してください。

手順の概要

1. **configure terminal**
2. **router eigrp instance-tag**
3. **address-family ipv4 unicast**
4. **redistribute { bgp as | { eigrp | ospf | ospfv3 | rip } instance-tag | direct | static } route-map name**
5. **default-metric bandwidth delay reliability loading mtu**
6. **show ip eigrp route-map statistics redistribute**
7. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router eigrp instance-tag 例 : <pre>switch(config)# router eigrp Test1 switch(config-router)#</pre>	インスタンス タグを設定して、新しい EIGRP プロセスを作成します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。 AS 番号であると認められていない <i>instance-tag</i> を設定する場合は、 autonomous-system コマンドを使用して AS 番号を明示的に設定する必要があります。そうしないと、この EIGRP インスタンスはシャットダウン状態のままになります。
ステップ 3	address-family ipv4 unicast 例 : <pre>switch(config-router)# address-family ipv4 unicast switch(config-router-af)#</pre>	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。IPv4 の場合、このコマンドはオプションです。
ステップ 4	redistribute { bgp as { eigrp ospf ospfv3 rip } instance-tag direct static } route-map name 例 : <pre>switch(config-router-af)# redistribute bgp 100 route-map BGPFilter</pre>	1 つのルーティング ドメインから EIGRP にルートを注入します。インスタンス タグおよびマップ名には最大 20 文字の英数字を使用できます。大文字と小文字は区別されます。

	コマンドまたはアクション	目的
ステップ 5	default-metric bandwidth delay reliability loading mtu 例 : <pre>switch(config-router-af)# default-metric 500000 30 200 1 1500</pre>	ルート再配布で学習したルートに割り当てられるメトリックを設定します。デフォルト値は次のとおりです。 • bandwidth : 100000 kbps • delay : 100 (10 マイクロ秒単位) • reliability : 255 • loading : 1 • MTU : 1492
ステップ 6	show ip eigrp route-map statistics redistribute 例 : <pre>switch(config-router-af)# show ip eigrp route-map statistics redistribute bgp</pre>	EIGRP ルート マップ統計に関する情報を表示します。
ステップ 7	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、BGP を IPv4 向けの EIGRP に再配布する例を示します。

```
switch# configure terminal

switch(config)# router eigrp Test1

switch(config-router)# redistribute bgp 100 route-map BGPFilter

switch(config-router)# default-metric 500000 30 200 1 1500

switch(config-router)# copy running-config startup-config
```

再配布されるルート数の制限

ルートの再配布では、多くのルートを EIGRP ルート テーブルに追加できます。外部プロトコルから受け取るルートの数の上限を設定できます。EIGRP では、再配布されるルートの上限を設定するために次のオプションが用意されています。

- 上限固定 : EIGRP が設定された最大値に達すると、メッセージをログに記録します。EIGRP は、それ以上の再配布されたルートを受け入れません。しきい値を超えたときに EIGRP が警告をログに記録する、最大値のしきい値に対する割合を設定することもできます。

- 警告のみ：EIGRP が最大値に達したときのみ、警告のログを記録します。EIGRP は、再配布されたルートを受け入れ続けます。
 - 取り消し：EIGRP が最大値に達すると、タイムアウト期間が開始します。タイムアウト期間の経過後、再配布されたルートの現在数が最大数よりも少ない場合、EIGRP はすべての再配布されたルートを要求します。再配布されたルートの現在数が最大数に達した場合、EIGRP はすべての再配布されたルートを取り消します。EIGRP が再配布されたルートをさらに受け入れられるように、この条件をクリアする必要があります。
- 任意で、タイムアウト期間を設定できます。

始める前に

EIGRP 機能を有効にしていることを確認します（[EIGRP 機能の有効化](#)のセクションを参照）。

手順の概要

1. **configure terminal**
2. **router eigrp instance-tag**
3. **redistribute { bgp id | direct | eigrp id | ospf id | rip id | static } route-map map-name**
4. **redistribute maximum-prefix max [threshold] [warning-only | withdraw [num-retries timeout]]**
5. （任意） **show running-config eigrp**
6. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	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	router eigrp instance-tag 例： <pre>switch(config)# router eigrp Test1 switch(config-router)#</pre>	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	redistribute { bgp id direct eigrp id ospf id rip id static } route-map map-name 例： <pre>switch(config-router)# redistribute bgp route-map FilterExternalBGP</pre>	設定したルートマップ経由で、選択したプロトコルを EIGRP に再配布します。

	コマンドまたはアクション	目的
ステップ 4	redistribute maximum-prefix <i>max</i> [<i>threshold</i>] [warning-only withdraw [<i>num-retries</i> <i>timeout</i>]] 例 : <pre>switch(config-router)# redistribute maximum-prefix 1000 75 warning-only</pre>	EIGRP が再配布するプレフィックスの最大数を指定します。指定できる範囲は 0 ～ 65536 です。任意で次のオプションを指定します。 • threshold : 警告メッセージをトリガする最大プレフィックスの割合。 • warning-only : プレフィックスの最大数を超えた場合に警告メッセージを記録します。 • withdraw : 再配布されたすべてのルートを取り消します。任意で再配布されたルートを取得しようと試みます。<i>num-retries</i> の範囲は 1 ～ 12 です。<i>timeout</i> は 60 ～ 600 秒です。デフォルトは 300 秒です。clear ip eigrp redistribution コマンドは、すべてのルートを取り消す場合に使用します。
ステップ 5	(任意) show running-config eigrp 例 : <pre>switch(config-router)# show running-config eigrp</pre>	EIGRP の設定を表示します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config-router)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、EIGRP に再配布されるルート の数を制限する例を示します。

```
switch# configure terminal
switch(config)# router eigrp Test1
switch(config-router)# redistribute bgp route-map FilterExternalBGP
switch(config-router)# redistribute maximum-prefix 1000 75
```

EIGRP でのロードバランスの設定

EIGRP でのロードバランスを設定できます。最大パス オプションを使用して、ECMP ルートの数を設定できます。

始める前に

EIGRP 機能を有効にしていることを確認します ([EIGRP 機能の有効化](#)のセクションを参照)。

手順の概要

1. **configure terminal**
2. **router eigrp instance-tag**
3. **address-family ipv4 unicast**
4. **maximum-paths num-paths**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	router eigrp instance-tag 例 : <pre>switch(config)# router eigrp Test1 switch(config-router)#</pre>	インスタンス タグを設定して、新しい EIGRP プロセスを作成します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。 AS 番号であると認められていない <i>instance-tag</i> を設定する場合は、autonomous-system コマンドを使用して AS 番号を明示的に設定する必要があります。そうしないと、この EIGRP インスタンスはシャットダウン状態のままになります。
ステップ 3	address-family ipv4 unicast 例 : <pre>switch(config-router)# address-family ipv4 unicast switch(config-router-af)#</pre>	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。IPv4 の場合、このコマンドはオプションです。
ステップ 4	maximum-paths num-paths 例 : <pre>switch(config-router-af)# maximum-paths 5</pre>	EIGRP がルート テーブルに受け入れる等コストパスの数を設定します。指定できる範囲は 1 ～ 16 です。デフォルト値は 8 です。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、6 つまでの等コストパスによる、EIGRP の等コストロードバランスを IPv4 上で設定する例を示します。

```
switch# configure terminal
switch(config)# router eigrp Test1
switch(config-router)# maximum-paths 6
switch(config-router)# copy running-config startup-config
```

hello パケット間のインターバルとホールドタイムの調整

Hello メッセージの間隔とホールドタイムは調整できます。

デフォルトでは、5 秒ごとに Hello メッセージが送信されます。ホールドタイムは Hello メッセージでアドバタイズされ、ネイバーに、送信者が有効であると見なすべき時間を示します。デフォルトの保留時間は、hello 間隔の 3 倍（15 秒）です。

hello パケットの間隔を変更するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
ip hello-interval eigrp instance-tag seconds 例 : <pre>switch(config-if)# ip hello-interval eigrp Test1 30</pre>	EIGRP ルーティング処理の hello 間隔を設定します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。範囲は 1 ～ 65535 秒です。デフォルトは 5 分です。

非常に輻輳した大規模なネットワークでは、デフォルトの保留時間では、全ルータがネイバーから hello パケットを受信するまでに十分な時間がない場合もあります。この場合は、ホールドタイムを増やすことを推奨します。

ホールドタイムを変更するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
ip hold-time eigrp instance-tag seconds 例 : <pre>switch(config-if)# ip hold-time eigrp Test1 30</pre>	EIGRP ルーティング処理のホールドタイムを設定します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。有効な範囲は 1 ～ 65535 です。

タイマー設定を確認するには、**show ip eigrp interface detail** コマンドを使用します。

スプリット ホライズンの無効化

スプリット ホライズンを使用すると、ルータによって情報元インターフェイスからルート情報がアドバタイズされないようにできます。通常はスプリット ホライズンにより、特にリンクに障害がある場合に、複数のルーティング スイッチ間での通信が最適化されます。

デフォルトでは、スプリット ホライズンはすべてのインターフェイスで有効になっています。

スプリット ホライズンを無効にするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
no ip split-horizon eigrp instance-tag 例 : switch(config-if)# no ip split-horizon eigrp Test1	スプリット ホライズンを無効にします。

EIGRP の調整

オプション パラメータを設定し、ネットワークに合わせて EIGRP を調整できます。

アドレス ファミリ コンフィギュレーション モードでは、次のオプション パラメータを設定できます。

コマンド	目的
default-information originate [always route-map map-name] 例 : switch(config-router-af)# default-information originate always	プレフィックス 0.0.0.0/0 を持つデフォルト ルートを発信するか、受け入れます。ルート マップが提供されると、ルート マップが true 状態となっている場合にのみデフォルト ルートが発信されます。マップ名には最大 20 文字の英数字を使用できます。大文字と小文字は区別されます。
distance internal external 例 : switch(config-router-af)# distance 25 100	この EIGRP プロセスのアドミニストレーティブ ディスタンスを設定します。範囲は 1 ～ 255 です。内部の値で、同じ自律システム内で学習したルートのディスタンスが設定されます（デフォルト値は 90 です）。外部の値で、外部自律システムから学習したルートのディスタンスが設定されます（デフォルト値は 170 です）。
metric maximum-hops hop-count 例 : switch(config-router-af)# metric maximum-hops 70	アドバタイズされるルートに許容される最大ホップ数を設定します。ホップ数がこの最大値を超えるルートは、到達不能としてアドバタイズされます。範囲は 1 ～ 255 です。デフォルトは 100 です。

コマンド	目的
metric weights tos k1 k2 k3 k4 k5 例 : <pre>switch(config-router-af)# metric weights 0 1 3 2 1 0</pre>	EIGRP メトリックまたは K 値を調整します。EIGRP は次の式を使用して、ネットワークへの合計メトリックを決定します。 $\text{metric} = [k1 \times \text{bandwidth} + (k2 \times \text{bandwidth}) / (256 - \text{load}) + k3 \times \text{delay}] \times [k5 / (\text{reliability} + k4)]$ デフォルト値と指定できる範囲は、次のとおりです。 • TOS : 0。指定できる範囲は 0 ～ 8 です。 • k1 : 1。有効な範囲は 0 ～ 255 です。 • k2 : 0。有効な範囲は 0 ～ 255 です。 • k3 : 1。有効な範囲は 0 ～ 255 です。 • k4 : 0。有効な範囲は 0 ～ 255 です。 • k5 : 0。有効な範囲は 0 ～ 255 です。
timers active-time { time-limit disabled } 例 : <pre>switch(config-router-af)# timers active-time 200.</pre>	(照会の送信後に) ルートがアクティブ (SIA) 状態のままとなっていることを宣言するまでに、ルータが待機する時間を分単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 3 です。

インターフェイス コンフィギュレーション モードで、省略可能な次のパラメータを設定できます。

コマンド	目的
ip band width eigrp instance-tag bandwidth 例 : <pre>switch(config-if)# ip bandwidth eigrp Test1 30000</pre>	インターフェイス上の EIGRP の帯域幅メトリックを設定します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。帯域幅の範囲は、1 ～ 2,560,000,000 kbps です。
ip band width-percent eigrp instance-tag percent 例 : <pre>switch(config-if)# ip bandwidth-percent eigrp Test1 30</pre>	EIGRP がインターフェイス上で使用する可能性のある帯域幅の割合を設定します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。 割合の範囲は 0 ～ 100 です。デフォルトは 50 です。
no ip delay eigrp instance-tag delay 例 : <pre>switch(config-if)# ip delay eigrp Test1 100</pre>	インターフェイス上の EIGRP の遅延メトリックを設定します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。遅延の範囲は、1 ～ 16777215 (10 マイクロ秒単位) です。

コマンド	目的
ip distribute-list eigrp instance-tag { prefix-list name route-map name} { in out } 例 : <pre>switch(config-if)# ip distribute-list eigrp Test1 route-map EigrpTest in</pre>	このインターフェイス上の EIGRP のルータ フィルタリング ポリシーを設定します。インスタンス タグ、プレフィックス リスト名、およびルート マップ名には最大 20 文字の英数字を使用できます。大文字と小文字は区別されます。
no ip next-hop-self eigrp instance-tag 例 : <pre>switch(config-if)# ip next-hop-self eigrp Test1</pre>	このインターフェイスのアドレスではなく、受信したネクストホップアドレスを使用するよう、EIGRP を設定します。デフォルトでは、このインターフェイスの IP アドレスをネクストホップアドレスに使用します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ip offset-list eigrp instance-tag { prefix-list name route-map name} { in out } offset 例 : <pre>switch(config-if)# ip offset-list eigrp Test1 prefix-list EigrpList in</pre>	EIGRP が学習したルートに、着信および発信メトリックへのオフセットを追加します。インスタンス タグ、プレフィックス リスト名、およびルート マップ名には最大 20 文字の英数字を使用できます。大文字と小文字は区別されます。
ip passive-interface eigrp instance-tag 例 : <pre>switch(config-if)# ip passive-interface eigrp Test1</pre>	EIGRP hello を抑制します。これにより、EIGRP インターフェイス上でネイバーがルーティングアップデートを形成および送信することを防ぎます。インスタンス タグには英数字を

EIGRP の仮想化の設定

EIGRP 機能を有効にしていることを確認します ([EIGRP 機能の有効化](#)のセクションを参照)。

始める前に

複数の VRF を作成して、各 VRF で同じまたは複数の EIGRP プロセスを使用することもできます。VRF にはインターフェイスを割り当てます。



- (注) インターフェイスの VRF を設定した後に、インターフェイスの他のすべてのパラメータを設定します。インターフェイスの VRF を設定すると、そのインターフェイスの他の設定がすべて削除されます。

手順の概要

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **router eigrp** *instance-tag*
4. **interface** *ethernet slot/port*
5. **no switchport**
6. **vrf member** *vrf-name*
7. **ip router eigrp** *instance-tag*
8. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	vrf context <i>vrf-name</i> 例 : <pre>switch(config)# vrf context RemoteOfficeVRF switch(config-vrf)#</pre>	新しい VRF を作成し、VRF 設定モードを開始します。VRN 名には最大 20 文字の英数字を使用できます。大文字と小文字は区別されます。
ステップ 3	router eigrp <i>instance-tag</i> 例 : <pre>switch(config)# router eigrp Test1 switch(config-router)#</pre>	インスタンス タグを設定して、新しい EIGRP プロセスを作成します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。 AS 番号であると認められていない <i>instance-tag</i> を設定する場合は、autonomous-system コマンドを使用して AS 番号を明示的に設定する必要があります。そうしないと、この EIGRP インスタンスはシャットダウン状態のままになります。
ステップ 4	interface <i>ethernet slot/port</i> 例 : <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>	インターフェイス設定モードを開始します。? を使用すると、スロットおよびポートの範囲を検索できます。
ステップ 5	no switchport 例 : <pre>switch(config-if)# no switchport</pre>	そのインターフェイスを、レイヤ 3 ルーテッドインターフェイスとして設定します。

	コマンドまたはアクション	目的
ステップ 6	vrf member vrf-name 例 : switch(config-if)# vrf member RemoteOfficeVRF	このインターフェイスを VRF に追加します。VRF 名には最大 20 文字の英数字を使用できます。大文字と小文字は区別されます。
ステップ 7	ip router eigrp instance-tag 例 : switch(config-if)# ip router eigrp Test1	このインターフェイスを EIGRP プロセスに追加します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 8	copy running-config startup-config 例 : switch(config-if)# copy running-config startup-config	この設定変更を保存します。

例

次に、VRF を作成して、その VRF にインターフェイスを追加する例を示します。

```
switch# configure terminal
switch(config)# vrf context NewVRF
switch(config-vrf)# router eigrp Test1
switch(config-router)# i nterface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip router eigrp Test1
switch(config-if)# vrf member NewVRF
switch(config-if)# copy running-config startup-config
```

EIGRP の設定の確認

EIGRP の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ip eigrp [instance-tag]	設定した EIGRP プロセスの要約を表示します。
show ip eigrp [instance-tag] interfaces [type number] [brief] [detail]	設定されているすべての EIGRP インターフェイスに関する情報を表示します。
show ip eigrp instance-tag neighbors [type number]	すべての EIGRP ネイバーに関する情報を表示します。EIGRP ネイバーの設定を確認するには、このコマンドを使用します。
show ip eigrp [instance-tag] route [ip-prefix/length] [active] [all-links] [detail-links] [pending] [summary] [zero-successors] [vrf vrf-name]	すべての EIGRP ルートに関する情報を表示します。

コマンド	目的
<code>show ip eigrp [instance-tag] topology [ip-prefix/length] [active] [all-links] [detail-links] [pending] [summary] [zero-successors] [vrf vrf-name]</code>	EIGRP トポロジ テーブルに関する情報を表示します。
<code>show running-configuration eigrp</code>	現在実行中の EIGRP コンフィギュレーションを表示します。

EIGRP 統計情報の表示

EIGRP 統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
<code>show ip eigrp [instance-tag] accounting [vrf vrf-name]</code>	EIGRP の課金統計情報を表示します。
<code>show ip eigrp [instance-tag] route-map statistics redistribute</code>	EIGRP の再配布統計情報を表示します。
<code>show ip eigrp [instance-tag] traffic [vrf vrf-name]</code>	EIGRP のトラフィック統計情報を表示します。

EIGRP の設定例

次に、EIGRP を設定する例を示します。

```
feature eigrp
interface ethernet 1/2
no switchport
ip address 192.0.2.55/24
ip router eigrp Test1
no shutdown
router eigrp Test1
router-id 192.0.2.1
```

関連項目

BGP の関連項目は、次のとおりです。

- [Route Policy Manager の設定](#) (443 ページ)

その他の参考資料

EIGRP の実装に関する詳細情報については、次のページを参照してください。

MIB

MIB	MIB のリンク
CISCO-EIGRP-MIB	MIB を検索してダウンロードするには、次の MIB を参照してダウンロードします。



第 8 章

IS-IS の設定

この章では、Cisco NX-OS デバイスの Integrated Intermediate System-to-Intermediate System (IS-IS) を設定する方法について説明します。

この章は、次の項で構成されています。

- [IS-IS について \(225 ページ\)](#)
- [IS-IS の前提条件 \(232 ページ\)](#)
- [IS-IS に関する注意事項および制限事項 \(233 ページ\)](#)
- [デフォルト設定 \(233 ページ\)](#)
- [IS-IS の設定 \(234 ページ\)](#)
- [IS-IS 設定の確認 \(259 ページ\)](#)
- [IS-IS の監視 \(260 ページ\)](#)
- [IS-IS の設定例 \(261 ページ\)](#)
- [関連項目 \(261 ページ\)](#)

IS-IS について

IS-IS は、ISO（国際標準化機構）/IEC（国際電気標準化会議）10589 に基づく IGP です。Cisco NX-OS は、インターネット プロトコル バージョン 4 (IPv4) および IPv6 をサポートします。IS-IS はネットワーク トポロジの変化を検出し、ネットワーク上の他のノードへのループフリー ルートを計算できる、ダイナミック リンクステート ルーティング プロトコルです。各ルータは、ネットワークの状態を記述するリンクステート データベースを維持し、設定された各リンクにパケットを送信してネイバーを検出します。IS-IS はネットワークを介して各ネイバーにリンクステート情報をフラッドします。ルータもすべての既存ネイバーを通じて、リンクステート データベースのアドバタイズメントおよびアップデートを送信します。

IS-IS の概要

IS-IS は、設定されている各インターフェイスに hello パケットを送信し、IS-IS ネイバー ルータを検出します。hello パケットには認証、エリア、サポート対象プロトコルなど、受信側インターフェイスが発信側インターフェイスとの互換性を判別するために使用する情報が含まれます。また、一致する最大転送ユニット (MTU) 設定を持つインターフェイスだけを使用して

IS-IS が隣接関係を確立できるように、**hello** パケットがパディングされます。互換インターフェイスは隣接関係を形成し、リンクステートアップデートメッセージ (LSP) を使用して、リンクステートデータベースのルーティング情報をアップデートします。ルータはデフォルトで、10 分間隔で定期的に LSP リフレッシュを送信し、LSP は 20 分間 (LSP ライフタイム) リンクステートデータベースに残ります。LSP ライフタイムが終了するまでにルータが LSP リフレッシュを受信しなかった場合、ルータはデータベースから LSP を削除します。

LSP 間隔は、LSP ライフタイムより短くする必要があります。そうしないと、リフレッシュ前に LSP がタイムアウトします。

IS-IS は、隣接ルータに定期的に **hello** パケットを送信します。**hello** パケットに対して一時モードを設定すると、IS-IS が隣接関係を確立する前に使用された余分なパディングがこれらの **hello** パケットに含まれなくなります。隣接ルータの MTU 値が変更された場合、IS-IS はこの変更を検出し、パディングされた **hello** パケットを一定期間送信できます。IS-IS はこの機能を使用して、隣接ルータ上の一致しない MTU 値を検出します。詳細については、「[Hello パディングの一時モードの設定](#)」の項を参照してください。

IS-IS エリア

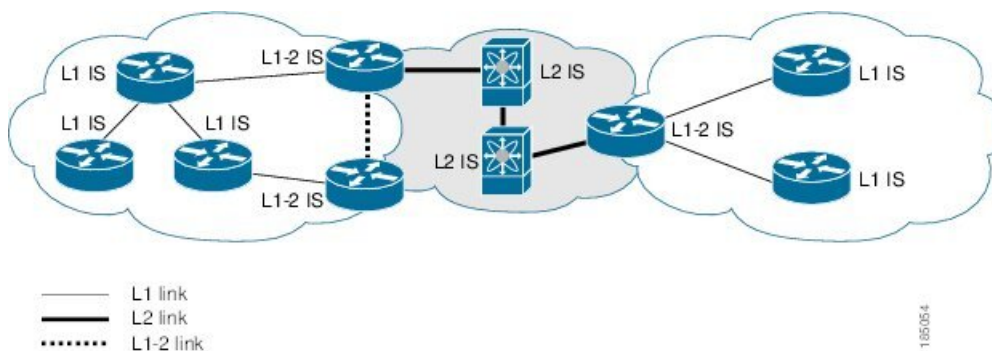
IS-IS ネットワークは、ネットワーク内のすべてのルータを含むシングルエリアとして設計することもできますし、バックボーンまたはレベル 2 エリアに接続する複数のエリアとして設計することもできます。非バックボーンエリアのルータはレベル 1 ルータで、ローカルエリア内で隣接関係を確立します (エリア内ルーティング)。レベル 2 エリアのルータは、他のレベル 2 ルータと隣接関係を確立し、レベル 1 エリア間のルーティングを実行します (エリア間ルーティング)。1 つのルータにレベル 1 エリアとレベル 2 エリアの両方を設定できます。これらのレベル 1/レベル 2 ルータは、エリア境界ルータとして動作し、ローカルエリアからレベル 2 バックボーンエリアに情報をルーティングします (図 7-1 を参照)。

レベル 1 エリア内のルータは、そのエリア内の他のすべてのルータに対する到達方法を認識します。レベル 2 ルータは、他のエリア境界ルータおよび他のレベル 2 ルータへの到達方法を認識します。レベル 1/レベル 2 ルータは 2 つのエリアの境界にまたがり、レベル 2 バックボーンエリアとの間で双方向にトラフィックをルーティングします。レベル 1/レベル 2 ルータはレベル 1 ルータの **Attached** (ATT) ビット信号を使用して、レベル 2 エリアに接続するため、このレベル 1/レベル 2 ルータへのデフォルトルートを設定します。

エリア内に 2 台以上のレベル 1/レベル 2 ルータがある場合など、場合によっては、レベル 1 ルータがレベル 2 エリアへのデフォルトルートとして使用するレベル 1/レベル 2 ルータを制御することもできます。**Attached** ビットを設定するレベル 1/レベル 2 ルータを設定できます。詳細については、「[IS-IS 設定の確認](#)」の項を参照してください。

Cisco NX-OS の IS-IS インスタンスは、レベル 1 またはレベル 2 エリアを 1 つだけサポートするか、またはそれぞれのエリアを 1 つずつサポートします。デフォルトでは、すべての IS-IS インスタンスが自動的にレベル 1 およびレベル 2 ルーティングをサポートします。

図 25: エリアに分割された IS-IS ネットワーク



ASBR（自律システム境界ルータ）は、IS-IS AS（自律システム）全体に外部宛先をアドバタイズします。外部ルートは、他のプロトコルから IS-IS に再配布されたルートです。

NET およびシステム ID

IS-IS インスタンスごとにネットワーク エンティティ タイトル（NET）が関連付けられています。NET は、その IS-IS インスタンスをエリア内で一意に特定する IS-IS システム ID とエリア ID からなります。たとえば、NET が 47.0004.004d.0001.0001.0c11.1111.00 の場合、システム ID は 0001.0c11.1111.00、エリア ID は 47.0004.004d.0001 です。

DIS

IS-IS はブロードキャストネットワーク内で代表中継システム（DIS）を使用することにより、各ルータがブロードキャストネットワーク上の他のルータと不要なリンクを形成しないようにします。IS-IS ルータは DIS に LSP を送信し、DIS がブロードキャストネットワークのあらゆるリンクステート情報を管理します。エリア内で DIS を選択するために IS-IS に使用させる IS-IS プライオリティをユーザ側で設定できます。



（注） ポイントツーポイント ネットワークでは DIS は不要です。

IS-IS 認証

隣接関係および LSP 交換を制御するために、認証を設定できます。ネイバーになろうとするルータは、設定されている認証レベルの同じパスワードを交換する必要があります。パスワードが無効なルータは、IS-IS によってブロックされます。IS-IS 認証はグローバルに設定することも、レベル 1、レベル 2、またはレベル 1/レベル 2 両方のルーティングに対応する個々のインターフェイスに設定することもできます。

IS-IS がサポートする認証方式は、次のとおりです。

- クリア テキスト：交換するすべてのパケットで、クリアテキストの 128 ビット パスワードが伝送されます。

- MD5 ダイジェスト：交換するすべてのパケットで、128 ビット キーに基づくメッセージ ダイジェストが伝送されます。

受動的攻撃から保護するために、IS-IS はネットワークを介してクリアテキストとして MD5 秘密キーを送信します。また、リプレイアタックから保護するために、IS-IS は各パケットにシーケンス番号を組み込みます。

hello および LSP 認証用のキーチェーンも使用できます。キーチェーン管理の詳細については、「Cisco Nexus 3600 NX-OS セキュリティ設定ガイド」を参照してください。

メッシュ グループ

メッシュグループは一連のインターフェイスであり、グループ内では、インターフェイスを介して到達可能なすべてのルータが他の各ルータとの間に 1 つ以上のリンクを持ちます。多数のリンクで障害が発生しても、ネットワークから 1 つまたは複数のルータが切り離されることはありません。

通常のフラッドイングでは、新しい LSP を受信したインターフェイスは、その LSP をルータ上の他のすべてのインターフェイスにフラッドイングします。メッシュグループを使用する場合、メッシュグループに含まれているインターフェイスは新しい LSP を受信しても、メッシュグループ内の他のインターフェイスには、新しい LSP をフラッドイングしません。



(注) 特定のメッシュ ネットワーク トポロジで、ネットワークのスケラビリティを向上させるために、LSP を制限しなければならない場合があります。LSP フラッドイングを制限すると、ネットワークの信頼性も下がります（障害発生時）。したがって、メッシュグループはどうしても必要な場合に限り、慎重にネットワークを設計したうえで使用することを推奨します。

ルータ間のパラレルリンクに、ブロックモードでメッシュグループを設定することもできます。このモードでは、各ルータがそれぞれリンクステート情報を最初に交換すると、それ以後はメッシュグループのそのインターフェイスですべての LSP がブロックされます。

過負荷ビット

IS-IS は過負荷ビットを使用して他のルータに指示を与え、それらのルータがトラフィックの転送にローカルルータを使用せずに、引き続きローカルルータ宛てのトラフィックをルーティングするようにします。

過負荷ビットを使用する状況は、次のとおりです。

- ルータがクリティカル条件下にある。
- ネットワークに対して通常手順でルータの追加および除去を行う。
- その他（管理上またはトラフィック エンジニアリング上）の理由。BGP コンバージェンスの待機中など。

ルート集約

サマリー集約アドレスを設定できます。ルート集約を使用すると、固有性の強い一連のアドレスをすべての固有アドレスを代表する1つのアドレスに置き換えることによって、ルートテーブルを簡素化できます。たとえば、10.1.1.0/24、10.1.2.0/24、および10.1.3.0/24というアドレスを1つの集約アドレス 10.1.0.0/16 に置き換えることができます。

IS-IS はルーティング テーブルに含まれている固有性の強いルートが多いほど、固有性の強いルートの最小メトリックと同じメトリックを指定して、サマリーアドレスをアドバタイズします。



(注) Cisco NX-OS は、自動ルート集約をサポートしていません。

再配布の設定

別のルーティング プロトコルからのルーティング情報を受け入れて、IS-IS ネットワークを通じてその情報を再配布するように、IS-IS を設定できます。任意で、再配布ルートのためのデフォルトルートを割り当てることができます。

始める前に

IS-IS を有効にする必要があります（「[IS-IS 機能の有効化](#)」の項を参照）。

手順の概要

1. **configure terminal**
2. **router isis instance-tag**
3. **address-family {ipv4 | ipv6} unicast**
4. **redistribute { bgp as | direct | { eigrp | isis | ospf | ospfv3 | rip } instance-tag | static } route-map map-name**
5. (任意) **default-information originate [always] [route-map map-name]**
6. (任意) **distribute { level-1 | level-2 } into { level-1 | level-2 } { route-map route-map | all }**
7. (任意) **show isis [vrf vrf-name] { ip | ipv6 } route ip-prefix [detail | longer-prefixes [summary | detail]]**
8. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 :	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
	switch# configure terminal switch(config)#	
ステップ 2	router isis instance-tag 例： switch(config)# router isis Enterprise switch(config-router)#	<i>instance tag</i> を設定して、新しい IS-IS インスタンスを作成します。
ステップ 3	address-family {ipv4 ipv6} unicast 例： switch(config-router)# address-family ipv4 unicast switch(config-router-af)#	アドレス ファミリ設定モードを開始します。
ステップ 4	redistribute { bgp as direct { eigrp isis ospf ospfv3 rip } instance-tag static } route-map map-name 例： switch(config-router-af)# redistribute eigrp 201 route-map ISISmap	他のプロトコルからのルートを IS-IS に再配布します。ルートマップの設定の詳細については、 ルートマップの設定 のセクションを参照してください。
ステップ 5	(任意) default-information originate [always] [route-map map-name] 例： switch(config-router-af)# default-information originate always	IS-IS へのデフォルト ルートを生成します。
ステップ 6	(任意) distribute { level-1 level-2 } into { level-1 level-2 } { route-map route-map all } 例： switch(config-router-af)# distribute level-1 into level-2 all	一方の IS-IS レベルから他方の IS-IS レベルへ、ルートを再配布します。
ステップ 7	(任意) show isis [vrf vrf-name] { ip ipv6 } route ip-prefix [detail longer-prefixes [summary detail]] 例： switch(config-if)# show isis ip summary-address	IS-IS ルートを表示します。
ステップ 8	(任意) copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	この設定変更を保存します。

例

次に、EIGRP を IS-IS に再配布する例を示します。

```
switch# configure terminal
switch(config)# router isis Enterprise
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# redistribute eigrp 201 route-map ISISmap
switch(config-router-af)# copy running-config startup-config
```

プレフィックスの抑制のリンク

デフォルトでは、IS-ISはシステムLSPの接続インターフェイスのアドレスをアドバタイズします。不要なインターフェイスアドレスのアドバタイズメントを抑制することで、LSPのサイズを削減し、IS-ISが維持するルート数を削減して、コンバージェンス時間を短縮できます。

LSPのルート数を減らすために、次の2つのプレフィックス抑制方式が提供されています。

- グローバルレベルでは、他の接続されたプレフィックスを除く、パッシブインターフェイスに属するプレフィックスだけをアドバタイズするように選択できます。[パッシブインターフェイスプレフィックスのみのアドバタイズ \(250 ページ\)](#) を参照してください。
- インターフェイスレベルで、接続されたプレフィックスのアドバタイズメントを無効にできます。「[インターフェイスでのプレフィックスの抑制 \(251 ページ\)](#)」を参照してください。

ロード バランシング

ロードバランシングを使用すると、ルータは、宛先アドレスから等距離内にあるすべてのルータのネットワークポートにトラフィックを分散できます。ロードバランシングは、ネットワークセグメントの使用率を向上させ、有効ネットワーク帯域幅を増加させます。

Cisco NX-OS は、等コスト マルチパス (ECMP) 機能をサポートします。IS-IS ルートテーブルおよびユニキャスト RIB の等コストパスは最大 64 です。これらのパスの一部または全部でトラフィックのロードバランシングが行われるように、IS-IS を設定できます。

BFD

この機能では、IPv4およびIPv6用の双方向フォワーディング検出 (BFD) をサポートします。BFD は、転送パスの障害を高速で検出することを目的にした検出プロトコルです。BFD は 2 台の隣接デバイス間のサブセカンド障害を検出し、BFD の負荷の一部を、サポートされるモジュール上のデータプレーンに分散できるため、プロトコル hello メッセージよりも CPU を使いません。詳細については、『[Cisco Nexus 3600 NX-OS Interfaces Configuration Guide](#)』を参照してください。

仮想化のサポート

Cisco NX-OS は、IS-IS の複数のプロセスインスタンスをサポートします。各 IS-IS インスタンスは、システム制限まで複数の仮想ルーティングおよび転送 (VRF) インスタンスをサポート

できます。サポートされる IS-IS インスタンスの数については、『[Cisco Nexus 3600 NX-OS Verified Scalability Guide](#)』を参照してください。

高可用性およびグレースフル リスタート

Cisco NX-OS は、マルチレベルのハイ アベイラビリティ アーキテクチャを提供します。IS-IS は、ステートフル リスタートをサポートしています。これは、ノンストップ ルーティング (NSR) とも呼ばれます。IS-IS で問題が発生した場合は、以前の実行時状態からの再起動を試みます。この場合、ネイバーはいずれのネイバーイベントも登録しません。最初の再起動が正常ではなく、別の問題が発生した場合、RFC 3847 のとおり、IS-IS はグレースフル リスタートを試みます。グレースフル リスタート、つまり、Nonstop Forwarding (NSF) では、処理の再起動中も IS-IS がデータ転送パス上に存在し続けます。再起動中の IS-IS インターフェイスが稼働を再開すると、ネイバーを再探索して隣接関係を確立し、更新情報の送信を再開します。この時点で、NSF ヘルパーは、グレースフル リスタートが完了したと認識します。

ステートフル リスタートは次のシナリオで使用されます。

- プロセスでの問題発生後の最初の回復試行
- **system switchover** コマンドを使用したユーザー開始スイッチオーバー

グレースフル リスタートは次のシナリオで使用されます。

- プロセスでの問題発生後の 2 回目の回復試行 (4 分以内)
- **restart isis** コマンドを使用したプロセスの手動再起動
- アクティブ スーパーバイザの削除
- **reload module active-sup** コマンドを使用したアクティブ スーパーバイザ リロード。



(注) グレースフルリスタートがデフォルトとなっており、ディセーブルにしないことを強く推奨します。

複数の IS-IS インスタンス

Cisco NX-OS は、同じノード上で動作する、IS-IS プロトコルの複数インスタンスをサポートしています。同一インターフェイスには複数のインスタンスを設定できません。すべてのインスタンスで同じシステム ルータ ID を使用します。サポートされる IS-IS インスタンスの数については、『[Cisco Nexus 3600 NX-OS Verified Scalability Guide](#)』を参照してください。

IS-IS の前提条件

IS-IS の前提条件は次のとおりです。

- IS-IS をイネーブルにする必要があります（「[IS-IS 機能のイネーブル化](#)」の項を参照）。

IS-IS に関する注意事項および制限事項

IS-IS 設定時の注意事項および制約事項は、次のとおりです。

- デフォルトの参照帯域幅が Cisco NX-OS と Cisco IOS では異なるため、アドバタイズされたトンネル IS-IS メトリックは、これら 2 つのオペレーティングシステムによって異なります。

デフォルト設定

次の表に、IS-IS パラメータのデフォルト設定値を示します。

表 14: デフォルトの IS-IS パラメータ

パラメータ	デフォルト
アドミニストレーティブ ディスタンス	115
エリア レベル	Level-1-2
DIS プライオリティ	64
グレースフル リスタート	イネーブル
hello 乗数	3
hello パディング	イネーブル
hello タイム	10 秒
IS-IS 機能	ディセーブル
LSP 間隔	33
LSP MTU	1492
最大 LSP ライフタイム	1200 秒
最大パス	8
メトリック	40
参照帯域幅	40 Gbps

IS-IS の設定

IS-IS コンフィギュレーション モード

この項では、各コンフィギュレーションモードの開始方法について説明します。現行のモードで ? コマンドを入力することで、そのモードで使用可能なコマンドを表示できます。

ルータ コンフィギュレーション モード

次に、ルータ コンフィギュレーション モードを開始する例を示します。

```
switch#: configure terminal
switch(config)# router isis isp
switch(config-router)#
```

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

次の例は、ネイバー アドレス ファミリ コンフィギュレーション モードの開始方法を示しています。

```
switch(config)# router isis isp
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)#
```

IS-IS 機能の有効化

IS-IS を設定する前に、IS-IS 機能を有効にする必要があります。

手順の概要

1. **configure terminal**
2. **feature isis**
3. (任意) **show feature**
4. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 2	feature isis 例 : <code>switch(config)# feature isis</code>	IS-IS 機能を有効にします。
ステップ 3	(任意) show feature 例 : <code>switch(config)# show feature</code>	有効および無効にされた機能を表示します。
ステップ 4	copy running-config startup-config 例 : <code>switch(config)# copy running-config startup-config</code>	この設定変更を保存します。

例

IS-IS 機能を無効にして、関連付けられている構成をすべて削除するには、構成モードで次のコマンドを使用します。

コマンド	目的
no feature isis 例 : <code>switch(config)# no feature isis</code>	IS-IS 機能を無効にして、関連するすべての構成を削除します。

IS-IS インスタンスの作成

IS-IS インスタンスを作成し、そのインスタンスのエリア レベルを設定できます。

始める前に

IS-IS を有効にする必要があります（「[IS-IS 機能の有効化](#)」の項を参照）。

手順の概要

1. **configure terminal**
2. **router isis instance-tag**
3. **net network-entity-title**
4. (任意) **is-type { level-1 | level-2 | level-1-2 }**
5. (任意) **show isis [vrf vrf-name] process**
6. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	router isis instance-tag 例 : switch(config)# router isis Enterprise switch(config-router)#	<i>instance tag</i> を設定して、新しい IS-IS インスタンスを作成します。
ステップ 3	net network-entity-title 例 : switch(config-router)# net 47.0004.004d.0001.0001.0c11.1111.00	この IS-IS インスタンスに対応する NET を設定します。
ステップ 4	(任意) is-type { level-1 level-2 level-1-2 } 例 : switch(config-router)# is-type level-2	この IS-IS インスタンスのエリア レベルを設定します。デフォルトは level-1-2 です。
ステップ 5	(任意) show isis [vrf vrf-name] process 例 : switch(config)# show isis process	すべての IS-IS インスタンスについて、IS-IS 要約情報を表示します。
ステップ 6	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	この設定変更を保存します。

例

IS-IS インスタンスおよび関連する構成を削除するには、構成モードで次のコマンドを使用します。

コマンド	目的
no router isis instance-tag	IS-IS インスタンスおよびすべての関連付けられている構成を削除します。



- (注) IS-IS インスタンスに関するすべての設定を完全に削除するには、インターフェイスモードで設定した IS-IS コマンドも削除する必要があります。

IS-IS の省略可能な次のパラメータを構成できます。

コマンド	目的
distance value 例 : <pre>switch(config-router)# distance 30</pre>	IS-IS のアドミニストレーティブ ディスタンスを設定します。範囲は 1 ～ 255 です。デフォルトは 115 です。
log-adjacency-changes 例 : <pre>switch(config-router)# log-adjacency-changes</pre>	IS-IS ネイバーのステートが変化するたびに、システムメッセージを送信します。
lsp-mtu size 例 : <pre>switch(config-router)# lsp-mtu 600</pre>	この IS-IS インスタンスにおける LSP の MTU を設定します。指定できる範囲は 128 ～ 4352 バイトです。デフォルトは 1492 です。
maximum-paths number 例 : <pre>switch(config-router)# maximum-paths 6</pre>	IS-IS がルートテーブルで維持する等コストパスの最大数を設定します。範囲は 1 ～ 64 です。デフォルト値は 8 です。
reference-bandwidth bandwidth-value { Mbps Gbps } 例 : <pre>switch(config-router)# reference-bandwidth 100 Gbps</pre>	IS-IS コストメトリックの計算に使用する、デフォルトの基準帯域幅を設定します。指定できる範囲は 1 ～ 4000 Gbps です。デフォルトは 40 Gbps です。

レベル 2 エリアで IS-IS インスタンスを作成する例を示します。

```
switch# configure terminal
switch(config)# router isis Enterprise
switch(config-router)# net 47.0004.004d.0001.0001.0c11.1111.00
switch(config-router)# is-type level 2
switch(config-router)# copy running-config startup-config
```

ネイバーの統計情報をクリアし、隣接関係を削除するには、ルータ構成モードで次のコマンドを使用します。

コマンド	目的
clear isis [<i>instance-tag</i>] adjacency [* <i>system-id</i> <i>interface</i>] 例 : switch(config-if)# clear isis adjacency *	ネイバーの統計情報を消去し、この IS-IS インスタンスの隣接関係を削除します。

IS-IS インスタンスの再起動

IS-IS インスタンスを再起動できます。この処理では、インスタンスのすべてのネイバーが消去されます。

IS-IS インスタンスを再起動し、関連付けられたすべてのネイバーを削除するには、次のコマンドを使用します。

手順の概要

1. restart isis instance-tag

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	restart isis instance-tag 例 : switch(config)# restart isis Enterprise	IS-IS インスタンスを再起動し、すべてのネイバーを削除します。

IS-IS のシャットダウン

IS-IS インスタンスをシャットダウンできます。シャットダウンすると、その IS-IS インスタンスがディセーブルになり、設定が保持されます。

IS-IS インスタンスをシャットダウンするには、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. shutdown

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	shutdown 例 : <pre>switch(config-router)# shutdown</pre>	IS-IS インスタンスをディセーブルにします。

エリアでの IS-IS 認証の設定

エリアで LSP を認証するように IS-IS を設定できます。

始める前に

IS-IS を有効にする必要があります。 [「IS-IS の有効化」](#) を参照してください。

キーチェーンを IS-IS 設定から参照する場合は、グローバル設定モードでキーチェーンを設定する必要があります。キーチェーン管理の詳細については、[「Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイド」](#) を参照してください。

手順の概要

1. `configure terminal`
2. `router isis instance-tag`
3. `authentication-type { cleartext | md5 } { level-1 | level-2 }`
4. `authentication key-chain key { level-1 | level-2 }`
5. (任意) `authentication-check { level-1 | level-2 }`
6. (任意) `copy running-config startup-config`

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	<code>configure terminal</code> 例 : <pre>switch# configure terminal switch(config)#</pre>	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	<code>router isis instance-tag</code> 例 : <pre>switch(config)# router isis Enterprise switch(config-router)#</pre>	<code>instance tag</code> を設定して、新しい IS-IS インスタンスを作成します。

	コマンドまたはアクション	目的
ステップ 3	authentication-type { cleartext md5 } { level-1 level-2 } 例 : <pre>switch(config-router)# authentication-type cleartext level-2</pre>	クリアテキストまたは MD5 認証ダイジェストとして、レベル 1 またはレベル 2 エリアに使用する認証方式を設定します。
ステップ 4	authentication key-chain key { level-1 level-2 } 例 : <pre>authentication key-chain key { level-1 level-2 }</pre>	IS-IS エリア レベル認証に使用する認証キーを設定します。
ステップ 5	(任意) authentication-check { level-1 level-2 } 例 : <pre>switch(config-router)# authentication-check level-2</pre>	受信パケットの認証パラメータチェックを有効にします。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config-router)# copy running-config startup-config</pre>	この設定変更を保存します。

例

IS-IS インスタンスにクリアテキスト認証を設定する例を示します。

```
switch# configure terminal
switch(config)# router isis Enterprise
switch(config-router)# authentication-type cleartext level-2
switch(config-router)# authentication key-chain ISISKey level-2
switch(config-router)# copy running-config startup-config
```

インターフェイスでの IS-IS 認証の設定

インターフェイスで Hello パケットを認証するように IS-IS を設定できます。

始める前に

IS-IS を有効にする必要があります（「[IS-IS 機能の有効化](#)」の項を参照）。

手順の概要

1. **configure terminal**
2. **interface interface-type slot/port**
3. **isis authentication-type { cleartext | md5 } { level-1 | level-2 }**
4. **isis authentication key-chain key { level-1 | level-2 }**

5. (任意) **isis authentication-check { level-1 | level-2 }**
6. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	グローバル設定モードを開始します
ステップ 2	interface interface-type slot/port 例 : switch(config)# interface ethernet 1/2 switch(config-if)#	インターフェイス設定モードを開始します。
ステップ 3	isis authentication-type { cleartext md5 } { level-1 level-2 } 例 : switch(config-if)# isis authentication-type cleartext level-2	クリアテキストまたは MD5 認証ダイジェストとして、このインターフェイスにおける IS-IS 認証タイプを設定します。
ステップ 4	isis authentication key-chain key { level-1 level-2 } 例 : switch(config-if)# isis authentication key-chain ISISKey level-2	このインターフェイス上で IS-IS に使用する認証キーを設定します。
ステップ 5	(任意) isis authentication-check { level-1 level-2 } 例 : switch(config-if)# isis authentication-check	受信パケットの認証パラメータチェックを有効にします。
ステップ 6	(任意) copy running-config startup-config 例 : switch(config-if)# copy running-config startup-config	この設定変更を保存します。

例

IS-IS インスタンスにクリアテキスト認証を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# isis authentication-type cleartext level-2
```

```
switch(config-if)# isis authentication key-chain ISISKey
switch(config-if)# copy running-config startup-config
```

メッシュ グループの設定

メッシュ グループにインターフェイスを追加することによって、そのメッシュ グループ内のインターフェイスに対する LSP フラッドイングの量を制限できます。任意で、メッシュグループ内のインターフェイスに対して、すべての LSP フラッドイングをブロックすることもできます。

メッシュグループにインターフェイスを追加するには、インターフェイス設定モードで次のコマンドを使用します。

手順の概要

1. **isis mesh-group { blocked | mesh-id }**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	isis mesh-group { blocked mesh-id } 例 : <pre>switch(config-if)# isis mesh-group 1</pre>	メッシュ グループにこのインターフェイスを追加します。範囲は 1 ～ 4294967295 です。

指定中継システムの設定

インターフェイス プライオリティを設定することによって、ルータがマルチアクセス ネットワークの代表中継システム (DIS) になるように設定できます。

DIS を設定するには、インターフェイス設定モードで次のコマンドを使用します。

手順の概要

1. **isis priority number { level-1 | level-2 }**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	isis priority number { level-1 level-2 } 例 : <pre>switch(config-if)# isis priority 100 level-1</pre>	DIS 選択のためのプライオリティを設定します。指定できる範囲は 0 ～ 127 です。デフォルトは 64 です。

ダイナミック ホスト交換の設定

ダイナミック ホスト交換を使用してシステム ID とルータのホスト名をマッピングするように、IS-IS を設定できます。

ダイナミック ホスト交換を設定するには、ルータ設定モードで次のコマンドを使用します。

手順の概要

1. hostname dynamic

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	hostname dynamic 例 : <pre>switch(config-router)# hostname dynamic</pre>	ダイナミック ホスト交換をイネーブルにします。

過負荷ビットの設定

最短パス優先（SPF）の計算で中間ホップとしてこのルータを使用しないことを他のルータに通知するように、ルータを設定できます。任意で、起動時に BGP がコンバージェンスするまで、一時的に過負荷ビットを設定することもできます。

過負荷ビットを設定する以外に、レベル 1 またはレベル 2 トラフィックに関して、LSP からの特定タイプの IP プレフィックスアドバタイズメントを抑制することが必要な場合もあります。

過負荷ビットを設定するには、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. **set-overload-bit** { **always** | **on-startup** { *seconds* | **wait-for bgp as-number** } } [**suppress** [*interlevel* | *external*]]

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	set-overload-bit { always on-startup { <i>seconds</i> wait-for bgp as-number } } [suppress [<i>interlevel</i> <i>external</i>]] 例 : <pre>switch(config-router)# set-overload-bit on-startup 30</pre>	IS-IS に過負荷ビットを設定します。seconds の範囲は 5 ～ 86400 です。

接続ビットの設定

Attached ビットを設定すると、レベル 1 ルータがレベル 2 エリアへのデフォルトルートとして使用するレベル 1/レベル 2 ルータを制御できます。Attached ビットの設定をディセーブルにすると、レベル 1 ルータはこのレベル 1/レベル 2 ルータを使用してレベル 2 エリアに接続しなくなります。

レベル 1/レベル 2 ルータの Attached ビットを設定するには、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. [**no**] **attached-bit**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	[no] attached-bit 例 : <pre>switch(config-router)# no attached-bit</pre>	Attached ビットを設定するようにレベル 1/レベル 2 ルータを設定します。この機能は、デフォルトでイネーブルにされています。

hello パディングの一時モードの設定

hello パディングの一時モードを設定すると、IS-IS が隣接関係を確立するときに hello パケットをパディングし、IS-IS が隣接関係を確立したあとでそのパディングを削除できます。

hello パディングのモードを構成するには、ルータ構成モードで次のコマンドを使用します。

コマンド	目的
[no] isis hello-padding 例 : <pre>switch(config-if)# no isis hello-padding</pre>	完全な最大伝送単位 (MTU) に hello パケットをパディングします。デフォルトではイネーブルになっています。パディングの一時モードを設定するには、このコマンドの no 形式を使用します。

サマリーアドレスの設定

ルーティングテーブルでサマリーアドレスによって表されるサマリアドレスを作成できます。1つのサマリーアドレスに、特定のレベルのアドレスグループを複数含めることができます。Cisco NX-OS は固有性の強いすべてのルートのうち、最小メトリックをアドバタイズします。

始める前に

IS-IS を有効にする必要があります（「[IS-IS 機能の有効化](#)」の項を参照）。

手順の概要

1. **configure terminal**
2. **router isis instance-tag**
3. **address-family {ipv4 | ipv6} unicast**
4. **summary-address ip-prefix/mask-len { level-1 | level-2 | level-1-2 }**
5. （任意） **show isis [vrf vrf-name] { ip | ipv6 } summary-address ip-prefix [longer-prefixes]**
6. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router isis instance-tag 例 : <pre>switch(config)# router isis Enterprise switch(config-router)#</pre>	<i>instance tag</i> を設定して、新しい IS-IS インスタンスを作成します。
ステップ 3	address-family {ipv4 ipv6} unicast 例 :	アドレス ファミリ設定モードを開始します。

	コマンドまたはアクション	目的
	<pre>switch(config-router)# address-family ipv4 unicast switch(config-router-af)#</pre>	
ステップ 4	summary-address ip-prefix/mask-len { level-1 level-2 level-1-2 } 例 : <pre>switch(config-router-af)# summary-address 192.0.2.0/24 level-2</pre>	IPv4 アドレスまたは IPv6 アドレスに対応する、IS-IS エリア用のサマリー アドレスを設定します。
ステップ 5	(任意) show isis [vrf vrf-name] { ip ipv6 } summary-address ip-prefix [longer-prefixes] 例 : <pre>switch(config-if)# show isis ip summary-address</pre>	IS-IS IPv4 または IPv6 サマリー アドレス情報を表示します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、IS-IS の IPv4 ユニキャスト サマリー アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# router isis Enterprise
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# summary-address 192.0.2.0/24 level-2
switch(config-router-af)# copy running-config startup-config
```

再配布の設定

別のルーティングプロトコルからのルーティング情報を受け入れて、IS-IS ネットワークを通じてその情報を再配布するように、IS-IS を設定できます。任意で、再配布ルートのためのデフォルト ルートを割り当てることができます。

始める前に

IS-IS を有効にする必要があります（「[IS-IS 機能の有効化](#)」の項を参照）。

手順の概要

1. **configure terminal**
2. **router isis instance-tag**
3. **address-family { ipv4 | ipv6 } unicast**
4. **redistribute { bgp as | direct | { eigrp | isis | ospf | ospfv3 | rip } instance-tag | static } route-map map-name**

5. (任意) **default-information originate** [**always**] [**route-map map-name**]
6. (任意) **distribute** { **level-1** | **level-2** } **into** { **level-1** | **level-2** } { **route-map route-map** | **all** }
7. (任意) **show isis** [**vrf vrf-name**] { **ip** | **ipv6** } **route ip-prefix** [**detail** | **longer-prefixes** [**summary** | **detail**]]
8. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router isis instance-tag 例 : <pre>switch(config)# router isis Enterprise switch(config-router)#</pre>	<i>instance tag</i> を設定して、新しい IS-IS インスタンスを作成します。
ステップ 3	address-family {ipv4 ipv6} unicast 例 : <pre>switch(config-router)# address-family ipv4 unicast switch(config-router-af)#</pre>	アドレス ファミリ 設定モードを開始します。
ステップ 4	redistribute { bgp as direct { eigrp isis ospf ospfv3 rip } instance-tag static } route-map map-name 例 : <pre>switch(config-router-af)# redistribute eigrp 201 route-map ISISmap</pre>	他のプロトコルからのルートを IS-IS に再配布します。ルートマップの設定の詳細については、 ルートマップの設定 のセクションを参照してください。
ステップ 5	(任意) default-information originate [always] [route-map map-name] 例 : <pre>switch(config-router-af)# default-information originate always</pre>	IS-IS へのデフォルト ルートを生成します。
ステップ 6	(任意) distribute { level-1 level-2 } into { level-1 level-2 } { route-map route-map all } 例 : <pre>switch(config-router-af)# distribute level-1 into level-2 all</pre>	一方の IS-IS レベルから他方の IS-IS レベルへ、ルートを再配布します。
ステップ 7	(任意) show isis [vrf vrf-name] { ip ipv6 } route ip-prefix [detail longer-prefixes [summary detail]]	IS-IS ルートを表示します。

	コマンドまたはアクション	目的
	例 : switch(config-if)# show isis ip summary-address	
ステップ 8	(任意) copy running-config startup-config 例 : switch(config-if)# copy running-config startup-config	この設定変更を保存します。

例

次に、EIGRP を IS-IS に再配布する例を示します。

```
switch# configure terminal
switch(config)# router isis Enterprise
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# redistribute eigrp 201 route-map ISISmap
switch(config-router-af)# copy running-config startup-config
```

再配布されるルート数の制限

ルートの再配布によって、IS-IS ルート テーブルに多くのルートが追加される可能性があります。外部プロトコルから受け取るルートの数の上限を設定できます。IS-IS には、再配布ルートの制限を設定するために次のオプションが用意されています。

- 上限固定 : IS-IS が設定された最大値に達すると、メッセージをログに記録します。IS-IS は以降の再配布ルートを受け取りません。任意で、最大値のしきい値パーセンテージを設定して、IS-IS がこのしきい値を超えたときに警告を記録するようにすることもできます。
- 警告のみ : IS-IS が最大値に達したときのみ、警告のログを記録します。IS-IS は引き続き再配布ルートを受け取ります。
- 取り消し : IS-IS が最大値に達したときにタイムアウト期間を開始します。タイムアウト期間の経過後、現在の再配布ルートの数が最大制限より少ない場合、IS-IS はすべての再配布ルートを要求します。現在の再配布ルートの数が最大制限に達している場合、IS-IS はすべての再配布ルートを取り消します。IS-IS が以降の再配布ルートを受け取るには、この状態を解消する必要があります。任意で、タイムアウト期間を設定できます。

始める前に

IS-IS をイネーブルにする必要があります（「[IS-IS 機能のイネーブル化](#)」の項を参照）。

手順の概要

1. **configure terminal**
2. **router isis instance-tag**
3. **redistribute { bgp id | direct | eigrp id | isis id | ospf id | rip id | static } route-map map-name**

4. **redistribute maximum-prefix** *max* [*threshold*] [**warning-only** | **withdraw** [*num-retries timeout*]]
5. (任意) **show running-config isis**
6. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router isis instance-tag 例 : <pre>switch(config)# router isis Enterprise switch(config-router)#</pre>	instance tag を設定して、新しい IS-IS インスタンスを作成します。
ステップ 3	redistribute { bgp id direct eigrp id isis id ospf id rip id static } route-map map-name 例 : <pre>switch(config-router)# redistribute bgp route-map FilterExternalBGP</pre>	設定したルートマップ経由で、選択したプロトコルを IS-IS に再配布します。
ステップ 4	redistribute maximum-prefix <i>max</i> [<i>threshold</i>] [warning-only withdraw [<i>num-retries timeout</i>]] 例 : <pre>switch(config-router)# redistribute maximum-prefix 1000 75 warning-only</pre>	IS-IS が配布するプレフィックスの最大数を指定します。有効な範囲は 1 ～ 65535 です。次の項目を任意で指定できます。 • threshold : 警告メッセージをトリガする最大プレフィックス数のパーセンテージ。 • warning-only : プレフィックスの最大数を超えた場合に警告メッセージを記録します。 • withdraw : 再配布されたすべてのルートを取り消します。オプション選択で、再配布されたルートの取得を試みることができます。 <i>num-retries</i> の範囲は 1 ～ 12 です。<i>timeout</i> は 60 ～ 600 秒です。デフォルトは 300 秒です。clear isis redistribution コマンドは、すべてのルートが取り消された場合に使用します。
ステップ 5	(任意) show running-config isis 例 :	IS-IS の設定を表示します。

	コマンドまたはアクション	目的
	<code>switch(config-router)# show running-config isis</code>	
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config-router)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、IS-IS に再配布されるルートの数制限する例を示します。

```
switch# configure terminal
switch(config)# router isis Enterprise
switch(config-router)# redistribute bgp route-map FilterExternalBGP
switch(config-router)# redistribute maximum-prefix 1000 75
```

パッシブインターフェイスプレフィックスのみのアドバタイズ

パッシブインターフェイスに属するプレフィックスだけがシステムリンクステートパケット (LSP) でアドバタイズされるように指定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router isis instance-tag 例 : <pre>switch(config)# router isis 200 switch(config-router)#</pre>	instance tag を設定して、新しい IS-IS インスタンスを作成します。
ステップ 3	address-family {ipv4 ipv6} unicast 例 : <pre>switch(config-router)# address-family ipv4 unicast switch(config-router-af)#</pre>	アドレス ファミリ設定モードを開始します。
ステップ 4	[no] advertise passive-only {level-1 level-2} 例 :	パッシブインターフェイスに属するプレフィックスのみのアドバタイズメントをイネーブルにします。

	コマンドまたはアクション	目的
	<pre>switch(config-router-af)# advertise passive-only level-1 switch(config-router-af)#</pre>	

例

次に、パッシブインターフェイスに属するプレフィックスのアドバタイズのみをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# address-family ipv4 unicast
switch(config-router-af)# advertise passive-only level-1
```

インターフェイスでのプレフィックスの抑制

IS-IS インターフェイスがシステムリンクステートパケット（LSP）内の接続されたプレフィックスをアドバタイズせずに隣接の形成に参加できるようにします。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します
ステップ 2	interface interface-type slot/port 例 : <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 3	[no] isis suppress 例 : <pre>switch(config-if)# isis suppress switch(config-if)#</pre>	インターフェイスで接続されているプレフィックスのアドバタイズメントを無効にします。

例

次に、システムリンクステートパケット（LSP）でインターフェイスの接続されたプレフィックスのアドバタイズを抑制する例を示します。

```
switch# configure terminal
```

```
switch(config)# interface ethernet 1/2
switch(config-if)# isis suppress
```

厳密な隣接モードのディセーブル化

IPv4 と IPv6 の両方のアドレス ファミリがイネーブルの場合、厳格な隣接モードはデフォルトでイネーブルです。このモードでは、デバイスが両方のアドレス ファミリにイネーブルでない任意のルータとの隣接関係を形成しません。厳格な隣接モードは、`no adjacency-check` コマンドを使用して無効にできます。

始める前に

IS-IS を有効にする必要があります（「[IS-IS 機能の有効化](#)」の項を参照）。

手順の概要

1. **configure terminal**
2. **router isis instance-tag**
3. **address-family ipv4 unicast**
4. **no adjacency-check**
5. **exit**
6. **address-family ipv6 unicast**
7. （任意） **no adjacency-check**
8. **show running-config isis**
9. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router isis instance-tag 例 : <pre>switch(config)# router isis Enterprise switch(config-router)#</pre>	instance tag を設定して、新しい IS-IS インスタンスを作成します。
ステップ 3	address-family ipv4 unicast 例 : <pre>switch(config-router)# address-family ipv4 switch(config-router-af)#</pre>	アドレス ファミリ設定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	no adjacency-check 例 : <code>switch(config-router-af)# no adjacency-check</code>	IPv4 アドレス ファミリに関する厳格な隣接モードをディセーブルにします。
ステップ 5	exit 例 : <code>switch(config-router-af)# exit</code> <code>switch(config-router)#</code>	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 6	address-family ipv6 unicast 例 : <code>switch(config-router)# address-family ipv6 unicast</code> <code>switch(config-router-af)#</code>	アドレス ファミリ 設定モードを開始します。
ステップ 7	(任意) no adjacency-check 例 : <code>switch(config-router-af)# no adjacency-check</code>	IPv6 アドレス ファミリに関する厳格な隣接モードをディセーブルにします。
ステップ 8	show running-config isis 例 : <code>switch(config-router-af)# show running-config isis</code>	IS-IS の設定を表示します。
ステップ 9	(任意) copy running-config startup-config 例 : <code>switch(config-router-af)# copy running-config startup-config</code>	この設定変更を保存します。

グレースフル リスタートの設定

IS-IS のグレースフル リスタートを設定できます。

始める前に

IS-IS を有効にする必要があります（「[IS-IS 機能の有効化](#)」の項を参照）。

手順の概要

1. **configure terminal**
2. **router isis instance-tag**
3. **graceful-restart**
4. **graceful-restart t3 manual time**
5. (任意) **show running-config isis**
6. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	router isis instance-tag 例 : switch(config)# router isis Enterprise switch(config-router)#	名前を設定して、新しい IS-IS プロセスを作成します。
ステップ 3	graceful-restart 例 : switch(config-router)# graceful-restart	グレースフルリスタート T3 タイマーを設定します。有効な範囲は 30 ～ 65535 秒です。デフォルトは 60 秒です。
ステップ 4	graceful-restart t3 manual time 例 : switch(config-router)# graceful-restart t3 manual 300	グレースフルリスタート T3 タイマーを設定します。有効な範囲は 30 ～ 65535 秒です。デフォルトは 60 秒です。
ステップ 5	(任意) show running-config isis 例 : switch(config-router)# show running-config isis	IS-IS の設定を表示します。
ステップ 6	(任意) copy running-config startup-config 例 : switch(config-router)# copy running-config startup-config	この設定変更を保存します。

例

次に、グレースフル リスタートを有効にする例を示します。

```
switch# configure terminal
switch(config)# router isis Enterprise
switch(config-router)# graceful-restart
switch(config-router)# copy running-config startup-config
```

仮想化の設定

複数の IS-IS インスタンスと複数の VRF を設定できます。また、各 VRF で同じまたは複数の IS-IS インスタンスを使用することもできます。VRF に IS-IS インターフェイスを割り当てます。

設定した VRF に NET を設定する必要があります。



- (注) インターフェイスの VRF を設定した後に、インターフェイスの他のすべてのパラメータを設定します。インターフェイスの VRF を設定すると、そのインターフェイスのすべての設定が削除されます。

始める前に

IS-IS を有効にする必要があります（「[IS-IS 機能の有効化](#)」の項を参照）。

手順の概要

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **exit**
4. **router isis** *instance-tag*
5. **vrf** *vrf-name*
6. **net** *network-entity-title*
7. **exit**
8. **interface** *ethernet slot/port*
9. **vrf member** *vrf-name*
10. { **ip** | **ipv6** } **address** *ip-prefix/length*
11. { **ip** | **ipv6** } **router isis** *instance-tag*
12. (任意) **show isis** [**vrf** *vrf-name*] [*instance-tag*] **interface** [*interface-type slot/port*]
13. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 2	vrf context <i>vrf-name</i> 例 : switch(config)# vrf context RemoteOfficeVRF switch(config-vrf)#	新しい VRF を作成し、VRF 設定モードを開始します。
ステップ 3	exit 例 : switch(config-vrf)# exit switch(config)#	VRF設定モードを終了します。
ステップ 4	router isis <i>instance-tag</i> 例 : switch(config)# router isis Enterprise switch(config-router)#	instance tag を設定して、新しい IS-IS インスタンスを作成します。
ステップ 5	vrf <i>vrf-name</i> 例 : switch(config-router)# vrf RemoteOfficeVRF switch(config-router-vrf)#	VRF 設定モードを開始します。
ステップ 6	net <i>network-entity-title</i> 例 : switch(config-router-vrf)# net 47.0004.004d.0001.0001.0c11.1111.00	この IS-IS インスタンスに対応する NET を設定します。
ステップ 7	exit 例 : switch(config-router-vrf)# exit switch(config-router)#	ルータ VRF 設定モードを終了します。
ステップ 8	interface <i>ethernet slot/port</i> 例 : switch(config)# interface ethernet 1/2 switch(config-if)#	インターフェイス設定モードを開始します。
ステップ 9	vrf member <i>vrf-name</i> 例 : switch(config-if)# vrf member RemoteOfficeVRF	このインターフェイスを VRF に追加します。
ステップ 10	{ ip ipv6 } address <i>ip-prefix/length</i> 例 : switch(config-if)# ip address 192.0.2.1/16	このインターフェイスの IP アドレスを設定します。 このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 11	{ ip ipv6 } router isis <i>instance-tag</i> 例 :	この IPv4 または IPv6 インターフェイスを IS-IS インスタンスに関連付けます。

	コマンドまたはアクション	目的
	<code>switch(config-if)# ip router isis Enterprise</code>	
ステップ 12	(任意) show isis [vrf vrf-name] [instance-tag] interface [interface-type slot/port] 例 : <pre>switch(config-if)# show isis Enterprise ethernet 1/2</pre>	VRF のインターフェイスに関する IS-IS 情報を表示します。
ステップ 13	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、VRF を作成して、その VRF にインターフェイスを追加する例を示します。

```
switch# configure terminal
switch(config)# vrf context NewVRF
switch(config-vrf)# exit
switch(config)# router isis Enterprise
switch(config-router)# vrf NewVRF
switch(config-router-vrf)# net 47.0004.004d.0001.0001.0c11.1111.00
switch(config-router-vrf)# interface ethernet 1/2
switch(config-if)# vrf member NewVRF
switch(config-if)# ip address 192.0.2.1/16
switch(config-if)# ip router isis Enterprise
switch(config-if)# copy running-config startup-config
```

IS-IS の調整

ネットワーク要件に合わせて IS-IS を調整できます。

IS-IS を調整するには、ルータ構成モードで次のオプション コマンドを使用します。

コマンド	目的
lsp-gen-interval [level-1 level-2] lsp-max-wait [lsp-initial-wait lsp-second-wait] 例 : <pre>switch(config-router)# lsp-gen-interval level-1 500 500 500</pre>	LSP 発生に関する IS-IS スロットルを設定します。オプション パラメータは次のとおりです。 • lsp-max-wait : トリガーから LSP 発生までの最大待ち時間。指定できる範囲は 500 ～ 65535 ミリ秒です。 • lsp-initial-wait : トリガーから LSP 発生までの初期待ち時間。指定できる範囲は 50 ～ 65535 ミリ秒です。 • lsp-second-wait : バックオフ時の LSP スロットルに使用する第 2 待ち時間。指定できる範囲は 50 ～ 65535 ミリ秒です。

コマンド	目的
max-lsp-lifetime ライフタイム 例: <pre>switch(config-router)# max-lsp-lifetime 500</pre>	LSP の最大ライフタイムを秒数で設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 1200 です。
metric-style transition 例: <pre>switch(config-router)# metric-style transition</pre>	IS-IS がナロー メトリック スタイルのタイプ、長さ、値 (TLV) オブジェクトとワイドメトリック スタイルの TLV オブジェクトの両方を生成して受け取ることができるようにします。デフォルトではディセーブルになっています。
spf-interval [level-1 level-2] spf-max-wait [spf-initial-wait spf-second-wait] 例 : <pre>switch(config-router)# spf-interval level-2 500 500 500</pre>	LSA 到着までのインターバルを設定します。オプションパラメータは次のとおりです。 • lsp-max-wait : トリガーから SPF 計算までの最大待ち時間。指定できる範囲は 500 ～ 65535 ミリ秒です。 • lsp-initial-wait : トリガーから SPF 計算までの初期待ち時間。指定できる範囲は 50 ～ 65535 ミリ秒です。 • lsp-second-wait : バックオフ時の SPF 計算に使用する第 2 待ち時間。指定できる範囲は 50 ～ 65535 ミリ秒です。

ルータ アドレス構成モードで次のオプション コマンドを使用します。

コマンド	目的
adjacency-check 例 : <pre>switch(config-router-af)# adjacency-check</pre>	隣接関係チェックを実行し、IS-IS インスタンスが同じアドレスファミリをサポートするリモート IS-IS エンティティに限って隣接関係を形成していることを確認します。このコマンドは、デフォルトでイネーブルになっています。

IS-IS を調整するには、インターフェイス コンフィギュレーション モードで次のオプション コマンドを使用します。

コマンド	目的
isis csnp-interval seconds [level-1 level-2] 例 : <pre>switch(config-if)# isis csnp-interval 20</pre>	IS-IS に Complete Sequence Number PDU (CSNP) インターバルを秒数で設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 10 です。

コマンド	目的
isis hello-interval seconds [level-1 level-2] 例 : <pre>switch(config-if)# isis hello-interval 20</pre>	IS-IS に hello 間隔を秒数で設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 10 です。
isis hello-multiplier num [level-1 level-2] 例 : <pre>switch(config-if)# isis hello-multiplier 20</pre>	ルータが隣接関係を破棄するまでに、ネイバーが見逃さなければならない IS-IS hello パケットの数を指定します。指定できる範囲は 3 ～ 1000 です。デフォルトは 3 です。 。
isis lsp-interval milliseconds 例: <pre>switch(config-if)# isis lsp-interval 20</pre>	フラッディング時にこのインターフェイスで LSP が送信される間隔をミリ秒数で設定します。指定できる範囲は 10 ～ 65535 です。デフォルトは 33 です。

IS-IS 設定の確認

IS-IS の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show isis [<i>instance-tag</i>] adjacency [interface] [detail summary] [vrf vrf-name]	IS-IS の隣接関係を表示します。 clear isis adjacency コマンドを使用して、これらの統計情報をクリアします。 (注) ホスト名が 14 文字未満の場合、 show isis adjacency コマンドはホスト名を表示します。それ以外の場合は、システム ID が表示されます。
show isis [<i>instance-tag</i>] database [level-1 level-2] [detail summary] [LSP ID] [{ ip ipv6 } prefix ip-prefix] [{ router-id router-id } [adjacency node-id] [zero-sequence] } [vrf vrf-name]	IS-IS LSP データベースを表示します。
show isis [<i>instance-tag</i>] hostname [vrf vrf-name]	ダイナミック ホスト交換情報を表示します。
show isis [<i>instance-tag</i>] interface [brief interface] [level-1 level-2] [vrf vrf-name]	IS-IS インターフェイス情報を表示します。
show isis [<i>instance-tag</i>] mesh-group [<i>mesh-id</i>] [vrf vrf-name]	メッシュ グループ情報を表示します。

コマンド	目的
show isis [<i>instance-tag</i>] protocol [vrf <i>vrf-name</i>]	IS-IS プロトコルに関する情報を表示します。
show isis [<i>instance-tag</i>] { ip ipv6 } redistribute route [ip-address summary] [[<i>ip-prefix</i>] [longer-prefixes [summary]] [vrf <i>vrf-name</i>]	IS-IS のルート再配布情報を表示します。
show isis [<i>instance-tag</i>] { ip ipv6 } route [ip-address summary] [<i>ip-prefix</i> [longer-prefixes [summary]] [detail]] [vrf <i>vrf-name</i>]	IS-IS ルート テーブルを表示します。
show isis [<i>instance-tag</i>] rrm [<i>interface</i>] [vrf <i>vrf-name</i>]	IS-IS インターフェイスの再送信情報を表示します。
show isis [<i>instance-tag</i>] srm [<i>interface</i>] [vrf <i>vrf-name</i>]	IS-IS インターフェイスのフラッドイング情報を表示します。
show isis [<i>instance-tag</i>] ssn [<i>interface</i>] [vrf <i>vrf-name</i>]	IS-IS インターフェイスの PSNP 情報を表示します。
show isis [<i>instance-tag</i>] { ip ipv6 } summary-address [<i>ip-address</i>] [<i>ip-prefix</i>] [vrf <i>vrf-name</i>]	IS-IS のサマリーアドレス情報を表示します。
show running-configuration isis	現在の実行中の IS-IS 設定を表示します。
show tech-support isis [detail]	IS-IS のテクニカル サポートの詳細情報を表示します。

IS-IS の監視

IS-IS の統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
show isis [<i>instance-tag</i>] adjacency [interface] [system-ID] [detail] [summary] [vrf <i>vrf-name</i>]	IS-IS 隣接関係の統計情報を表示します。
show isis [<i>instance-tag</i>] database [level-1 level-2] [detail summary] [<i>lsip</i>] { [adjacency id] { ip ipv6 } prefix <i>prefix</i>] [router-id id] [zero-sequence] [vrf <i>vrf-name</i>]	IS-IS データベースの統計情報を表示します。
show isis [<i>instance-tag</i>] statistics [<i>interface</i>] [vrf <i>vrf-name</i>]	IS-IS インターフェイスの統計情報を表示します。
show isis { ip ipv6 } route-map statistics redistribute { bgp id eigrp id isis id ospf id rip id static } [vrf <i>vrf-name</i>]	IS-IS 再配布の統計情報を表示します。

コマンド	目的
show isis route-map statistics distribute { level-1 level-2 } into { level-1 level-2 } [vrf vrf-name]	レベル間で配布されたルートに関する、IS-IS 配布統計情報を表示します。
show isis [instance-tag] spf-log [detail] [vrf vrf-name]	IS-IS SPF 計算の統計情報を表示します。
show isis [instance-tag] traffic [interface] [vrf vrf-name]	IS-IS トラフィックの統計情報を表示します。

IS-IS 設定の統計情報を消去するには、次のいずれかのタスクを実行します。

コマンド	目的
clear isis [instance-tag] adjacency [* [interface] [system-id id]] [vrf vrf-name]	IS-IS 隣接関係の統計情報を消去します。
clear isis { ip ipv6 } route-map statistics redistribute { bgp id direct eigrp id isis id ospf id rip id static } [vrf vrf-name]	IS-IS 再配布の統計情報を消去します。
clear isis route-map statistics distribute { level-1 level-2 } into { level-1 level-2 } [vrf vrf-name]	レベル間で配布されたルートに関する、IS-IS 配布統計情報を消去します。
clear isis [instance-tag] statistics [* interface] [vrf vrf-name]	IS-IS インターフェイスの統計情報を消去します。
clear isis [instance-tag] traffic [* interface] [vrf vrf-name]	IS-IS トラフィックの統計情報を消去します。

IS-IS の設定例

IS-IS を設定する例を示します。

```
router isis Enterprise
is-type level-1
net 49.0001.0000.0000.0003.00
graceful-restart
address-family ipv4 unicast
default-information originate

interface ethernet 2/1
ip address 192.0.2.1/24
isis circuit-type level-1
ip router isis Enterprise
```

関連項目

ルートマップの詳細については、[Route Policy Manager の設定（443 ページ）](#) を参照してください。



第 9 章

基本的 BGP の設定

この章では、Cisco NX-OS スイッチでボーダー ゲートウェイ プロトコル (BGP) を設定する方法について説明します。

この章は、次の項で構成されています。

- [基本的な BGP について \(263 ページ\)](#)
- [基本 BGP の前提条件 \(271 ページ\)](#)
- [BGP に関する注意事項と制約事項 \(271 ページ\)](#)
- [CLI コンフィギュレーション モード \(272 ページ\)](#)
- [デフォルト設定 \(274 ページ\)](#)
- [基本的 BGP の設定 \(275 ページ\)](#)
- [ベーシック BGP の設定の確認 \(292 ページ\)](#)
- [BGP 統計情報の表示 \(294 ページ\)](#)
- [ベーシック BGP の設定例 \(294 ページ\)](#)
- [関連項目 \(295 ページ\)](#)
- [次の作業 \(295 ページ\)](#)
- [その他の参考資料 \(295 ページ\)](#)

基本的な BGP について

Cisco NX-OS は BGP バージョン 4 をサポートします。BGP v4 に組み込まれているマルチプロトコル拡張機能を使用すると、IP マルチキャスト ルートおよび複数のレイヤ 3 プロトコル アドレス ファミリーに関するルーティング情報を BGP に伝送させることができます。BGP では、他の BGP 対応スイッチとの間で TCP セッションを確立するための、信頼できるトランスポート プロトコルとして TCP を使用します。

BGP ではパセクトルルーティングアルゴリズムを使用して、BGP 対応ネットワーク スイッチまたは BGP スピーカ間でルーティング情報を交換します。各 BGP スピーカはこの情報を使用して、特定の宛先までのパスを判別し、なおかつルーティンググループを伴うパスを検出して回避します。ルーティング情報には、宛先の実際のルートプレフィックス、宛先に対する自律システムのパス、およびその他のパス属性が含まれます。

BGPはデフォルトで、宛先ホストまたはネットワークへのベストパスとして、1つだけパスを選択します。各パスは、BGP ベストパス分析で使用する well-known mandatory、well-known discretionary、optional transitive の各属性を伝送します。BGP ポリシーを設定し、これらの属性の一部を変更することによって、BGP パス選択を制御できます。詳細については、[ルート ポリシーおよび BGP セッションのリセット \(298 ページ\)](#) を参照してください。

BGP は、ロード バランシングまたは等コスト マルチパス (ECMP) もサポートします。詳細については、「[ロード シェアリングとマルチパス](#)」の項を参照してください。

BGP 自律システム

自律システム (AS) とは、単一の管理エンティティにより制御されるネットワークです。自律システムは1つまたは複数の IGP および整合性のある一連のルーティング ポリシーを使用して、ルーティング ドメインを形成します。BGP は 16 ビットおよび 32 ビットの自律システム番号をサポートします。詳細については、「[自律システム](#)」を参照してください。

個々の BGP 自律システムは外部 BGP (eBGP) ピアリングセッションを通じて、ルーティング情報をダイナミックに交換します。同じ自律システム内の BGP スピーカは、内部 BGP (iBGP) を通じて、ルーティング情報を交換できます。

4 バイトの AS 番号のサポート

BGP では、2 バイトまたは 4 バイトの AS 番号をサポートしています。Cisco NX-OS は、プレーンテキスト表記で 4 バイト (つまり 32 ビットの整数) の AS 番号を表示します。4 バイトの AS 番号は、プレーンテキスト表記 (たとえば 1 ~ 4294967295) または AS ドット表記 (たとえば 1.0) で設定できます。詳細については、「[自律システム](#)」を参照してください。

アドミニストレーティブ ディスタンス

アドミニストレーティブ ディスタンスは、ルーティング情報源の信頼性を示す評価基準です。デフォルトで、BGP は次の表に示されたアドミニストレーティブ ディスタンスを使用します。

表 15: デフォルトの BGP アドミニストレーティブ ディスタンス

ディスタンス	デフォルト値	機能
外部	20	eBGP から学習したルートに適用されます。
内部	200	iBGP から学習したルートに適用されます。
ローカル	200	ルータを起点とするルートに適用されます。



- (注) アドミニストレーティブ ディスタンスが BGP パス選択アルゴリズムに影響を与えることはありませんが、BGP で学習されたルートが IP ルーティングテーブルに組み込まれるかどうかを左右します。

詳細については、「[アドミニストレーティブ ディスタンス](#)」のセクションを参照してください。

BGP ピア

BGP スピーカーは他の BGP スピーカーを自動的に検出しません。ユーザ側で BGP スピーカ間の関係を設定する必要があります。BGP ピアは、別の BGP スピーカへのアクティブな TCP 接続を持つ BGP スピーカです。

BGP セッション

BGP は TCP ポート 179 を使用して、ピアとの TCP セッションを作成します。ピア間で TCP 接続が確立されると、各 BGP ピアは最初に相手と、それぞれのすべてのルートを交換し、BGP ルーティングテーブルを完成させます。初期交換以後、BGP ピアはネットワーク トポロジが変化したとき、またはルーティングポリシーが変更されたときに、差分アップデートだけを送信します。更新と更新の間の非アクティブ期間には、ピアは「キープアライブ」と呼ばれる特別なメッセージを交換します。ホールドタイムは、次の BGP アップデートまたはキープアライブ メッセージを受信するまでに経過することが許容される、最大時間限度です。

Cisco NX-OS では、次のピア設定オプションをサポートしています。

- 個別の IPv4 または IPv6 アドレス : BGP は、リモートアドレスと AS 番号が一致する BGP スピーカとのセッションを確立します。
- 単一 AS 番号の IPv4 または IPv6 プレフィックス ピア : BGP は、プレフィックスおよび AS 番号が一致する BGP スピーカとのセッションを確立します。
- ダイナミック AS 番号プレフィックス ピア : BGP は、プレフィックスと、設定済み AS 番号のリストに載っている AS 番号と一致する BGP スピーカとのセッションを確立します。

プレフィックス ピアおよびインターフェイス ピアのダイナミック AS 番号

Cisco NX-OS では、BGP セッションを確立する AS 番号の範囲またはリストを受け入れます。たとえば IPv4 プレフィックス 192.0.2.0/8 および AS 番号 33、66、99 を使用するように BGP を設定する場合、BGP は 192.0.2.1 および AS 番号 66 を使用してセッションを確立しますが、192.0.2.2 および AS 番号 50 からのセッションは拒否します。

Cisco NX-OS リリース 9.3(6) 以降、ダイナミック AS 番号のサポートは、プレフィックス ピアに加えてインターフェイス ピアにも拡張されています。[IPv4 および IPv6 アドレス ファミリ向け IPv6 リンク ローカル経由の BGP インターフェイス ピアリングの設定 \(322 ページ\)](#) を参照してください。

Cisco NX-OS では、セッションが確立されるまで内部 BGP (iBGP) または外部 BGP (eBGP) セッションとして、プレフィックス ピアをダイナミック AS 番号と関連付けません。iBGP および eBGP の詳細については、を参照してください。



(注) ダイナミック AS 番号プレフィックス ピア設定は、BGP テンプレートから継承した個々の AS 番号の設定よりも優先します。詳細については、の章を参照してください。

BGP ルータ ID

ピア間で BGP セッションを確立するには、BGP セッションの確立時に、OPEN メッセージで BGP ピアに送信されるルータ ID を BGP に設定する必要があります。BGP ルータ ID は 32 ビット値であり、IPv4 アドレスで表すことがよくあります。ルータ ID はユーザ側で設定できます。デフォルトでは、Cisco NX-OS によって、ルータのループバック インターフェイスの IPv4 アドレスにルータ ID が設定されます。ルータ上でループバック インターフェイスが設定されていない場合は、BGP ルータ ID を表すためにルータ上の物理インターフェイスに設定されている最上位の IPv4 アドレスがソフトウェアによって選択されます。BGP ルータ ID は、ネットワーク内の BGP ピアごとに一意である必要があります。

BGP にルータ ID が設定されていない場合、BGP ピアとのピアリングセッションを確立できません。

BGP パスの選択

BGP は複数の送信元から、同じルートのアドバタイズメントを受信する可能性があります。BGP はベストパスとして、パスを 1 つだけ選択します。BGP は、そのパスを IP ルーティングテーブルに格納し、ピアにパスを伝達します。

所定のネットワークでパスが追加または削除されるたびに、ベストパスアルゴリズムが実行されます。ベストパスアルゴリズムは、ユーザが BGP 設定を変更した場合にも実行されます。BGP は所定のネットワークで使用できる一連の有効パスの中から、最適なパスを選択します。

Cisco NX-OS は次の手順で、BGP ベストパスアルゴリズムを実行します。

手順

- ステップ 1 2 つのパスを比較し、どちらが適切かを判別します（「ステップ 1 - 「[パスの比較ペア](#)」セクションを参照）。
- ステップ 2 すべてのパスについて繰り返し、全体として最適なパスを選択するためにパスを比較する順序を決定します（ステップ 2：「[比較順序の決定](#)」のセクションを参照してください）。
- ステップ 3 新しいベストパスを使用するに足るだけの差が新旧のベストパスにあるかどうかを判別します（ステップ 3：「[ベストパス変更抑制の決定](#)」セクションを参照）。

例



- (注) 重要なのは、パート 2 で決定される比較順序です。3 つのパス A、B、C があり、Cisco NX-OS が A と B を比較して A を選択し、Cisco NX-OS が B と C を比較して B を選択したとします。しかし、Cisco NX-OS が A と C を比較したときには、A を選択しないかもしれません。これは一部の BGP メトリックが同じネイバー自律システムからのパスだけに適用され、すべてのパスにわたっては適用されないからです。

パス選択には、BGP AS パス属性が使用されます。AS パス属性には、アドバタイズされたパスでたどる自律システム番号 (AS 番号) のリストが含まれます。BGP 自律システムを自律システムの集合または連合に細分化する場合は、AS パスにローカル定義の自律システムを指定した連合セグメントが含まれます。

ステップ 1: パス ペアの比較

BGP ベストパス アルゴリズムの最初のステップでは、より適切なパスを判別するために 2 つのパスを比較します。次に、Cisco NX-OS が 2 つのパスを比較して、より適切なパスを判別する基本的なステップについて説明します。

1. Cisco NX-OS は、比較する有効なパスを選択します (たとえば、到達不能なネクストホップがあるパスは無効です)。
2. Cisco NX-OS は、重み値が最大のパスを選択します。
3. Cisco NX-OS は、ローカル プリファレンスが最大のパスを選択します。
4. パスの一方がローカル起点の場合、Cisco NX-OS はそのパスを選択します。
5. Cisco NX-OS は、AS パスが短い方のパスを選択します。



- (注) AS パス長を計算するときに、Cisco NX-OS は連合セグメントを無視し、AS セットを 1 として数えます。詳細については、「[AS 連合](#)」の項を参照してください。

6. Cisco NX-OS は、オリジンが低い方のパスを選択します。内部ゲートウェイプロトコル (IGP) は EGP よりも低いと見なされます。
7. Cisco NX-OS は、multi exit discriminator (MED) が小さい方のパスを選択します。

このステップが実行されるされないを左右する、一連のオプションを選択できます。Cisco NX-OS が両方のパスの MED を比較するのは、通常、同じ自律システムのピアからそれらのパスを受け取った場合です。それ以外の場合、Cisco NX-OS は MED の比較を省略します。

パスのピア自律システムに関係なく、ベストパス アルゴリズムの MED 比較が必ず実行されるように、Cisco NX-OS を設定することもできます。詳細については、「[最適パス](#)」

[アルゴリズムの調整](#)」を参照してください。この設定を行わなかった場合、MED 比較が実行されるかどうかは、次のように比較する 2 つのパスの AS パス属性によって決まります。

- a. パスに AS パスがない、または AS_SET から始まる AS パスがある場合、パスは内部であり、Cisco NX-OS は他の内部パスに対して MED を比較します。
- b. AS パスが AS_SEQUENCE から始まる場合、ピア自律システムがシーケンスで最初の AS 番号になり、Cisco NX-OS は同じピア自律システムを持つ他のパスに対して MED を比較します。
- c. AS パ스에連合セグメントだけが含まれている場合、または連合セグメントで始まり、AS_SET が続いている場合、パスは内部であり、Cisco NX-OS は他の内部パスに対して MED を比較します。
- d. AS パスが連合セグメントで始まり、AS_SEQUENCE が続いている場合、ピア自律システムが AS_SEQUENCE で最初の AS 番号になり、Cisco NX-OS は同じピア自律システムを持つ他のパスに対して MED を比較します。



(注) Cisco NX-OS がパスで指定された MED 属性を受信しなかった場合、Cisco NX-OS は欠落 MED が使用可能な最大値になるようにユーザーがベストパスアルゴリズムを設定していない限り、MED を 0 と見なします。詳細については、「[最適パス アルゴリズムの調整](#)」を参照してください。

- e. 非決定性の MED 比較機能がイネーブルの場合、ベストパス アルゴリズムでは Cisco IOS スタイルの MED 比較が使用されます。詳細については、「[最適パス アルゴリズムの調整](#)」を参照してください。
8. 一方のパスが内部ピアから、他方のパスが外部ピアからの場合、Cisco NX-OS は外部ピアからのパスを選択します。
9. ネクストホップアドレスへの IGP メトリックが異なるパスの場合、Cisco NX-OS は IGP メトリックが小さい方のパスを選択します。
10. Cisco NX-OS は、最後に実行したベストパス アルゴリズムによって選択されたパスを使用します。

ステップ 1 ~ 9 のすべてのパス パラメータが同じ場合、ルータ ID を比較するようにベストパスアルゴリズムを設定できます。詳細については、「[最適パスアルゴリズムの調整](#)」を参照してください。パスに発信元属性が含まれている場合、Cisco NX-OS はその属性をルータ ID として使用して比較します。発信もと属性が含まれていない場合、Cisco NX-OS はパスを送信したピアのルータ ID を使用します。パス間でルータ ID が異なる場合、Cisco NX-OS はルータ ID が小さい方のパスを選択します。

属性の送信元をルータ ID として使用する場合は、2 つのパスに同じルータ ID を設定することができます。また、同じピアルータとの 2 つの BGP セッションが可能です。したがって、同じルータ ID で 2 つのパスを受信できます。

11. Cisco NX-OS は、クラスタ長が短いほうのパスを選択します。クラスタ リスト属性の指定されたパスを受け取らなかった場合、クラスタ長は 0 です。
12. Cisco NX-OS は、IP アドレスが小さい方のピアから受信したパスを選択します。ローカル発生 of パス（再配布のパスなど）は、ピア IP アドレスが 0 になります。

ステップ 9 以降が同じパスは、マルチパスを設定している場合、マルチパスに使用できません。詳細については、「[ロードシェアリングとマルチパス](#)」の項を参照してください。

ステップ 2：比較順序の決定

BGP ベストパス アルゴリズム実装の 2 番めのステップでは、Cisco NX-OS がパスを比較する順序を決定します。

1. Cisco NX-OS は、パスをグループに分けます。各グループ内で、Cisco NX-OS はすべてのパスにわたって MED を比較します。Cisco NX-OS は、[ステップ 1：パス ペアの比較](#)と同じルールを使用して、2 つのパス間で MED を比較できるかどうかを判断します。この比較では通常、ネイバー自律システムごとに 1 つずつグループが選択されます。**bgp bestpath med always** コマンドを設定すると、Cisco NX-OS はすべてのパスが含まれた 1 グループだけを選択します。
2. Cisco NX-OS は、常に最適な方を維持しながら、グループのすべてのパスを反復することによって、各グループのベストパスを決定します。Cisco NX-OS は、各パスをそれまでの一時的なベストパスと比較します。それまでのベストパスよりも適切な場合は、そのパスが新しく一時的なベストパスになり、Cisco NX-OS はグループの次のパスと比較します。
3. Cisco NX-OS は、ステップ 2 の各グループで選択されたベストパスからなる、パスセットを形成します。Cisco NX-OS は、このパスセットでもステップ 2 と同様にそれぞれの比較を繰り返すことによって、全体としてのベストパスを選択します。

ステップ 3：ベストパス変更の抑制の決定

実装の次のパートでは、Cisco NX-OS が新しいベストパスを使用するのか抑制するのかを決定します。新しいベストパスが古いパスとまったく同じ場合、ルータは引き続き既存のベストパスを使用できます（ルータ ID が同じ場合）。Cisco NX-OS では引き続き既存のベストパスを使用することによって、ネットワークにおけるルート変更を回避できます。

抑制機能をオフにするには、ルータ ID を比較するようにベストパスアルゴリズムを設定します。詳細については、「[最適パスアルゴリズムの調整](#)」を参照してください。この機能を設定すると、新しいベストパスが常に既存のベストパスよりも優先されます。

次の条件が発生した場合に、ベストパス変更を抑制できません。

- 既存のベストパスが無効になった。
- 既存または新しいベストパスを内部（または連合）ピアから受信したか、またはローカルに発生した（再配布などによって）。

- 同じピアからパスを受信した（パスのルータ ID が同じ）。
- パス間で重み値、ローカルプリファレンス、オリジン、またはネクストホップアドレスに対する IGP メトリックが異なっている。
- パス間で MED が異なっている。

BGP およびユニキャスト RIB

BGP はユニキャスト RIB（ルーティング情報ベース）と通信して、ユニキャストルーティングテーブルに IPv4 ルートを格納します。ベストパスの選択後、ベストパスの変更をルーティングテーブルに反映させる必要があると BGP が判別した場合、BGP はユニキャスト RIB にルートアップデートを送信します。

BGP はユニキャスト RIB における BGP ルートの変更に関して、ルート通知を受け取ります。さらに、再配布をサポートする他のプロトコルルートに関するルート通知を受け取ります。

BGP はネクストホップの変更に関する通知も、ユニキャスト RIB から受け取ります。BGP はこれらの通知を使用して、ネクストホップアドレスへの到達可能性および IGP メトリックを追跡します。

ユニキャスト RIB でネクストホップ到達可能性または IGP メトリックが変更されるたびに、BGP は影響を受けるルートについて、ベストパス再計算を開始させます。

BGP プレフィックス独立コンバージェンス

BGP プレフィックス独立コンバージェンス（PIC）エッジ機能は、リンク障害が発生した場合に、BGP バックアップパスへの BGP IP ルートのコンバージェンスを高速化します。

BGP PIC エッジ機能により、ネットワーク障害後の BGP コンバージェンスが向上します。このコンバージェンスは、IP ネットワークのエッジ障害に適用されます。この機能は、ルーティング情報ベース（RIB）と転送情報ベース（FIB）にバックアップパスを作成して保存します。これによって、プライマリパスの障害が発生した場合に、ただちにバックアップパスが引き継ぐことができ、フォワーディングプレーンの迅速なフェールオーバーが可能になります。BGP PIC エッジは、IPv4 アドレスファミリのみをサポートします。

BGP PIC エッジが設定されている場合、BGP は、プライマリベストパスに加えて、2 番目のベストパス（バックアップパス）も計算します。BGP は、PIC サポートを持つプレフィックスのベストパスとバックアップパスの両方を BGP RIB にインストールします。また BGP は、API を介してリモートの次のホップとともにバックアップパスを URIB にダウンロードし、その後バックアップとしてマークされたネクストホップで FIB を更新します。バックアップパスにより、単一のネットワーク障害に対処する高速再ルーティング機能が提供されます。

この機能は、ローカルインターフェイスとリモートインターフェイス/リンクの両方の障害を検出して、バックアップパスが使用されるようにします。

BGP PIC エッジは、ユニパスとマルチパスの両方をサポートします。

BGP の仮想化

BGP は、仮想ルーティングおよび転送（VRF）インスタンスをサポートします。デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS はユーザーをデフォルトの VRF に配置します。詳細については、「[レイヤ 3 仮想化の設定](#)」を参照してください。

基本 BGP の前提条件

BGP を使用するには、次の前提条件を満たしている必要があります。

- BGP 機能を有効にする必要があります（[BGP 機能のイネーブル化](#)のセクションを参照）。
- システムに有効なルータ ID を設定しておく必要があります。
- Regional Internet Registry（RIR）によって割り当てられたか、またはローカル管理の AS 番号を取得しておく必要があります。
- 再帰ネクストホップ解決に対応できる IGP を 1 つ以上設定する必要があります。
- BGP セッションを確立するネイバー環境で、アドレス ファミリを設定する必要があります。

BGP に関する注意事項と制約事項

BGP 設定時の注意事項および制約事項は、次のとおりです。

- ダイナミック AS 番号プレフィックスピア設定は、BGP テンプレートから継承した個々の AS 番号の設定よりも優先します。
- AS 連合でプレフィックスピアにダイナミック AS 番号を設定した場合、BGP はローカル連合の AS 番号のみでセッションを確立します。
- ダイナミック AS 番号プレフィックスピアで作成された BGP セッションは、設定済みの外部 BGP（eBGP）マルチホップ存続可能時間（TTL）値や直接接続ピアに対するディセーブル済みのチェックを無視します。
- ルータ ID の自動変更およびセッションフラップを避けるために、BGP 用のルータ ID を設定する必要があります。
- ピアごとに最大プレフィックス設定オプションを使用し、受信するルート数および使用するシステムリソース数を制限する必要があります。
- update-source を設定し、BGP/eBGP マルチホップセッションでセッションを確立する必要があります。
- 再配布を設定する場合、BGP ポリシーを指定する必要があります。
- VRF 内で BGP ルータ ID を定義する必要があります。

- キープアライブおよびホールド タイマーの値を小さくすると、BGP セッション フラップが発生する可能性があります。
- VRF を構成する場合は、望ましい VRF を入力します（「[レイヤ 3 仮想化の設定](#)」を参照）。
- BGP PIC エッジ機能には、次のようなガイドラインと制約事項が適用されます。
 - Cisco NX-OS リリース 9.2(2) 以降、BGP PIC エッジは Cisco Nexus 3600 プラットフォーム スイッチでサポートされます。
 - BGP PIC エッジは、IPv4 アドレス ファミリのみをサポートします。
 - BGP PIC エッジは、VXLAN EVPN および MPLS セグメント ルーティングではサポートされていません。
 - BGP PIC エッジは、1 つの修復（バックアップ）パスのみをサポートします。
 - BGP PIC エッジが設定されている場合、BGP は最大 63 のアクティブ パスをサポートします。アクティブ パスが 64 個ある場合、バックアップ パスは追加されません。

CLI コンフィギュレーション モード

以下の項では、BGP に対応する各 CLI コンフィギュレーション モードの開始方法について説明します。現行のモードで ? コマンドを入力すると、そのモードで使用可能なコマンドを表示できます。

グローバル コンフィギュレーション モード

グローバルコンフィギュレーションモードは、BGP プロセスを作成したり、AS 連合、ルート ダンプニングなどの拡張機能を設定したりする場合に使用します。詳細については、[高度な BGP の設定（297 ページ）](#) を参照してください。

次に、ルータ コンフィギュレーション モードを開始する例を示します。

```
switch# configuration
switch(config)# router bgp 64496
switch(config-router)#
```

BGP は仮想ルーティングおよび転送（VRF）をサポートします。ネットワークで VRF を使用する場合は、適切な VRF 内で BGP を設定できます。設定の詳細については、「[仮想化の設定](#)」の項を参照してください。

次に、VRF コンフィギュレーション モードを開始する例を示します。

```
switch(config)# router bgp 64497
switch(config-router)# vrf vrf_A
switch(config-router-vrf)#
```


アドレス ファミリ設定モード

任意で、BGP がサポートするアドレス ファミリを設定できます。アドレス ファミリ用の機能を設定する場合は、ルータ設定モードで **address-family** コマンドを使用します。ネイバーに対応する特定のアドレス ファミリを設定する場合は、ネイバー設定モードで **address-family** コマンドを使用します。

ルータ再配布、アドレス集約、ロードバランシングなどの拡張機能を使用する場合は、アドレス ファミリを設定する必要があります。

この例は、ルータ設定モードからアドレス ファミリ設定モードを開始する例を示します。

```
switch(config)# router bgp 64496
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)#
```

この例は、VRF を使用している場合に、VRF アドレス ファミリ設定モードを開始する例を示します。

```
switch(config)# router bgp 64497
switch(config-router)# vrf vrf_A
switch(config-router-vrf)# address-family ipv6 unicast
switch(config-router-vrf-af)#
```

ネイバー コンフィギュレーション モード

Cisco NX-OS には、BGP ピアを設定するためのネイバー コンフィギュレーション モードがあります。ネイバー コンフィギュレーション モードを使用して、ピアのあらゆるパラメータを設定できます。

次に、ネイバー コンフィギュレーション モードを開始する例を示します。

```
switch(config)# router bgp 64496
switch(config-router)# neighbor 192.0.2.1
switch(config-router-neighbor)#
```

次に、VRF ネイバー コンフィギュレーション モードを開始する例を示します。

```
switch(config)# router bgp 64497
switch(config-router)# vrf vrf_A
switch(config-router-vrf)# neighbor 192.0.2.1
switch(config-router-vrf-neighbor)#
```

ネイバー アドレス ファミリ コンフィギュレーション モード

アドレス ファミリ固有のネイバー設定を入力し、ネイバーのアドレス ファミリをイネーブルにするには、ネイバー コンフィギュレーション サブモード内のアドレス ファミリ コンフィギュレーションサブモードを使用できます。このモードは、所定のネイバーに認められるプレフィックス数の制限、eBGP のプライベート AS 番号の削除といった拡張機能に使用します。

RFC 5549 が導入されているため、IPv6 アドレスを持つネイバーに IPv4 アドレス ファミリを設定できます。

この例は、IPv4 アドレスでネイバーのための IPv4 ネイバー アドレス ファミリ設定モードを入力する方法を示します。

```
switch(config)# router bgp 64496
switch(config-router)# neighbor 192.0.2.1
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)#
```

この例は、IPv6 アドレスでネイバーのための IPv4 ネイバー アドレス ファミリ設定モードを入力する方法を示します。

```
switch(config)# router bgp 64496
switch(config-router)# neighbor 2001:db8::/64 eui64
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)#
```

この例は、IPv4 アドレスでネイバーのための VRF IPv4 ネイバー アドレス ファミリ構成モードを入力する方法を示します。

```
switch(config)# router bgp 64497
switch(config-router)# vrf vrf_A
switch(config-router-vrf)# neighbor 209.165.201.1
switch(config-router-vrf-neighbor)# address-family ipv4 unicast
switch(config-router-vrf-neighbor-af)#
```

この例は、IPv6 アドレスでネイバーのための VRF IPv4 ネイバー アドレス ファミリ設定モードを入力する方法を示します。

```
switch(config)# router bgp 64497
switch(config-router)# vrf vrf_A
switch(config-router-vrf)# neighbor 2001:db8::/64 eui64
switch(config-router-vrf-neighbor)# address-family ipv4 unicast
switch(config-router-vrf-neighbor-af)#
```

デフォルト設定

次の表に、BFD パラメータのデフォルト設定をリストします。

表 16: デフォルトの BGP パラメータ

パラメータ	デフォルト
BGP 機能	ディセーブル
キープアライブインターバル	60 秒
ホールド タイマー	180 秒
BGP PIC エッジ	無効化

基本的 BGP の設定

ベーシック BGP を設定するには、BGP をイネーブルにして、BGP ピアを設定する必要があります。ベーシック BGP ネットワークの設定は、いくつかの必須作業と多数の任意の作業からなります。BGP ルーティングプロセスおよび BGP ピアの設定は必須です。

BGP 機能のイネーブル化

始める前に

BGP を設定する前に、BGP 機能をイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **feature bgp**
3. (任意) **show feature**
4. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	feature bgp 例 : <pre>switch(config)# feature bgp</pre>	BGP 機能をイネーブルにします。
ステップ 3	(任意) show feature 例 : <pre>switch(config)# show feature</pre>	有効および無効にされた機能を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

例

no feature bgp コマンドを使用して、BGP 機能をディセーブルにし、関連するコンフィギュレーションをすべて削除します。

コマンド	目的
no feature bgp 例 : <pre>switch(config)# no feature bgp</pre>	BGP 機能をディセーブルにして、関連するすべての設定を削除します。

BGP インスタンスの作成

BGP インスタンスを作成し、BGP インスタンスにルータ ID を割り当てることができます。「[BGP ルータ ID](#)」のセクションを参照してください。Cisco NX-OS は、2 バイトまたは 4 バイトのプレーンテキスト表記または AS ドット表記による自律システム (AS) 番号をサポートします。詳細については、[4 バイト AS 番号のサポート](#)のセクションを参照してください。

始める前に

BGP 機能を有効にしていることを確認します ([BGP 機能の有効化](#)のセクションを参照してください)。

BGP はルータ ID (設定済みループバック アドレスなど) を取得できなければなりません。

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. (任意) **router-id** *ip-address*
4. (任意) **address-family** { *ipv4* | *ipv6* } { *unicast* | *multicast* }
5. (任意) **network** *ip-prefix* [*route-map map-name*]
6. (任意) **show bgp all**
7. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 2	router bgp <i>autonomous-system-number</i> 例 : switch(config)# router bgp 64496 switch(config-router)#	BGP を有効にして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による <i>xx.xx</i> という形式です。
ステップ 3	(任意) router-id <i>ip-address</i> 例 : switch(config-router)# router-id 192.0.2.255	BGP ルータ ID を設定します。この IP アドレスによって、この BGP スピーカを特定します。このコマンドによって、BGP ネイバーセッションの自動通知およびセッション リセットが開始されます。
ステップ 4	(任意) address-family { <i>ipv4</i> <i>ipv6</i> } { <i>unicast</i> <i>multicast</i> } 例 : switch(config-router)# address-family ipv4 unicast switch(config-router-af)#	指定されたアドレスファミリーに対応するグローバルアドレス ファミリ コンフィギュレーション モードを開始します。このコマンドによって、すべての BGP ネイバーセッションの自動通知およびセッション リセットが開始されます。
ステップ 5	(任意) network <i>ip-prefix</i> [<i>route-map map-name</i>] 例 : switch(config-router-af)# network 192.0.2.0	ネットワークを、この自律システムに対してローカルに設定し、BGP ルーティングテーブルに追加します。 エクステリア プロトコルの場合、 network コマンドでアドバタイズするネットワークを制御します。インテリア プロトコルでは、 network コマンドを使用して、アップデートの送信先を決定します。
ステップ 6	(任意) show bgp all 例 : switch(config-router-af)# show bgp all	すべての BGP アドレス ファミリに関する情報を表示します。
ステップ 7	(任意) copy running-config startup-config 例 : switch(config-router-af)# copy running-config startup-config	この設定変更を保存します。

例

BGP プロセスおよび関連するすべての設定を削除するには、**no router bgp** コマンドを使用します。

コマンド	目的
no router bgp <i>autonomous-system-number</i> 例 : switch(config)# no router bgp 201	BGP プロセスおよび関連する設定を削除します。

次に、IPv4 ユニキャスト アドレス ファミリを指定して BGP をイネーブルに設定し、アドバタイズするネットワークを 1 つ追加する例を示します。

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# network 192.0.2.0
switch(config-router-af)# copy running-config startup-config
```

BGP インスタンスの再起動

BGP インスタンスを再起動し、そのインスタンスのすべてのピア セッションをクリアできます。

BGP インスタンスを再起動し、関連付けられたすべてのピアを削除するには、次のコマンドを使用します。

コマンド	目的
restart bgp instance-tag 例 : switch(config)# restart bgp 201	BGP インスタンスを再起動し、すべてのピアリング セッションをリセットまたは再確立します。

BGP のシャットダウン

BGP プロトコルをシャットダウンして BGP を正常にディセーブルし、設定を保持できます。

BGP をシャットダウンするには、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
shutdown 例 : switch(config-router)# shutdown	BGP を正常にシャットダウンします。

BGP ピア設定

BGP プロセス内で BGP ピアを設定できます。BGP ピアごとに、関連付けられたキープアライブ タイマーとホールド タイマーがあります。これらのタイマーは、グローバルに設定することも、BGP ピアごとに設定することもできます。ピア設定はグローバル設定を上書きします。



(注) ピアごとに、ネイバー コンフィギュレーション モードでアドレス ファミリを設定する必要があります。

始める前に

BGP 機能を有効にしていることを確認します（[BGP 機能のイネーブル化](#)のセクションを参照してください）。

手順の概要

1. **configure terminal**
2. **router bgp autonomous-system-number**
3. **neighbor ip-address { ipv4 | ipv6 } remote-as as-number**
4. （任意） **description text**
5. （任意） **timers keepalive-time hold-time**
6. （任意） **shutdown**
7. **address-family { ipv4 | ipv6 } { unicast | multicast }**
8. （任意） **show bgp { ipv4 | ipv6 } { unicast | multicast } neighbors**
9. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router bgp autonomous-system-number 例 : <pre>switch(config)# router bgp 64496 switch(config-router)#</pre>	BGP を有効にして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。
ステップ 3	neighbor ip-address { ipv4 ipv6 } remote-as as-number 例 : <pre>switch(config-router)# neighbor 209.165.201.1 remote-as 64497 switch(config-router-neighbor)#</pre>	リモート BGP ピアの指定アドレス タイプと AS 番号を構成します。The <i>ip-address</i> 形式は x.x.x.x です。IPv6 <i>address-format</i> の形式は A:B::C:D です。
ステップ 4	（任意） description text 例 : <pre>switch(config-router-neighbor)# description Peer Router B switch(config-router-neighbor)#</pre>	ネイバーの説明を追加します。最大 80 文字の英数字ストリングを使用できます。
ステップ 5	（任意） timers keepalive-time hold-time 例 :	ネイバーのキープアライブおよびホールドタイムを表す BGP タイマー値を追加します。指定できる範囲

	コマンドまたはアクション	目的
	<code>switch(config-router-neighbor)# timers 30 90</code>	は 0 ～ 3600 秒です。デフォルトは、キープアライブ タイムで 60 秒、ホールド タイムで 180 秒です。 (注) ホールドタイマーが 10 秒以下の BGP セッションは、BGP セッションが 60 秒以上稼働するまで有効になりません。セッションが 60 秒間稼働すると、ホールドタイマーは構成どおりに動作します。
ステップ 6	(任意) shutdown 例 : <code>switch(config-router-neighbor)# shutdown</code>	この BGP ネイバーを管理目的でシャットダウンします。このコマンドによって、BGP ネイバーセッションの自動通知およびセッションリセットが開始されます。
ステップ 7	address-family { ipv4 ipv6 } { unicast multicast } 例 : <code>switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#</code>	ユニキャスト指定のアドレスファミリーに対応したネイバー アドレス ファミリー構成モードを開始します。
ステップ 8	(任意) show bgp { ipv4 ipv6 } { unicast multicast } neighbors 例 : <code>switch(config-router-neighbor-af)# show bgp ipv4 unicast neighbors</code>	BGP ピアに関する情報を表示します。
ステップ 9	copy running-config startup-config 例 : <code>switch(config-router-neighbor-af) copy running-config startup-config</code>	この設定変更を保存します。

例

次に、BGP ピアを設定する例を示します。

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# neighbor 192.0.2.1 remote-as 64497
switch(config-router-neighbor)# description Peer Router B
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# copy running-config startup-config
```

デフォルトスタティック ルートをすべての BGP VRF に配布

BGP 機能が有効になっていることを確認します

始める前に

新しい CLI `default-information originate` が追加され、デフォルトのスタティック ルートをデフォルト以外の VRF からすべての BGP (VRF) 仮想ルータ コンテキストに配布し、そのルートをすべての BGP VRF のローカル BGP ルート テーブルにインストールします。

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. **vrf** *vrf-name*
4. **address-family** { *ipv4* | *ipv6* } { *unicast* | *multicast* }
5. **redistribute static route-map** *map-name*
6. **default-information originate**
7. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router bgp <i>autonomous-system-number</i> 例 : <pre>switch(config)# router bgp 64496 switch(config-router)#</pre>	BGP を有効にして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による <i>xx.xx</i> という形式です。
ステップ 3	vrf <i>vrf-name</i> 例 : <pre>switch(config-router)# vrf vrf1</pre>	VRF 名を構成します。
ステップ 4	address-family { <i>ipv4</i> <i>ipv6</i> } { <i>unicast</i> <i>multicast</i> } 例 : <pre>switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#</pre>	指定されたアドレス ファミリに対応するグローバル アドレス ファミリ コンフィギュレーション モードを開始します。このコマンドによって、すべての BGP ネイバーセッションの自動通知およびセッション リセットが開始されます。
ステップ 5	redistribute static route-map <i>map-name</i> 例 : <pre>switch(config-router-neighbor-af)# redistribute static route-map test</pre>	スタティック ルート マップを再配布します。

	コマンドまたはアクション	目的
ステップ 6	default-information originate 例 : <pre>switch(config-router-neighbor-af) # default-information originate</pre>	デフォルトのスタティック ルートをデフォルト以外の VRF からすべての BGP (VRF) 仮想ルータ コンテキストに配布し、そのルートをすべての BGP VRF のローカル BGP ルート テーブルにインストールします。
ステップ 7	copy running-config startup-config 例 : <pre>switch(config-router-neighbor-af) # copy running-config startup-config</pre>	この設定変更を保存します。

例

デフォルトのスタティック ルートをデフォルト以外の VRF からすべての BGP (VRF) 仮想ルータ コンテキストに配布し、そのルートをすべての BGP VRF のローカル BGP ルート テーブルにインストールする方法の例を示します。

```
switch# configure terminal
switch(config)# router bgp 100
switch(config-router)# vrf green
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-vrf-af)# redistribute static route-map test
switch(config-router-vrf-af)# default-information originate
switch(config-router-vrf-af)# exit
switch(config)# copy running-config startup-config
```

次に、デフォルト以外の VRF グリーンから、別のデフォルト以外の VRF 共有にデフォルトのルート リークを構成する方法の例を示します。

```
router bgp 100
address-family ipv4 unicast
redistribute static route-map test
vrf Green
address-family ipv4 unicast
redistribute static route-map test
default-information originate
vrf Shared
address-family ipv4 unicast
redistribute static route-map test
```

更新アナウンス遅延タイマーの構成

`advertisement-interval` コマンドを使用すると、BGP ルーティング アップデートを送信する最小 ルート アドバタイズメント インターバル (MRAI) を設定できます。ルート アップデートがトリガされるとすぐに通知するのではなく、BGP はアドバタイズメント間隔が満了するまで待ってから、アップデートを送信します。この間隔中に他の変更が発生した場合、BGP はそれらすべての変更を効率的にアナウンスできます。

この遅延タイマーは、新しいルートアナウンスメントに対してのみ設定され、ルート取り消しアナウンスメントには設定されません。ルートの取り消しはすぐにアナウンスする必要があります。

始める前に

BGP 機能が有効になっていることを確認します

手順の概要

1. **configure terminal**
2. **router bgp autonomous-system-number**
3. **neighbor prefix remote-as route-map map-name**
4. **address-family { ipv4 | ipv6 } { unicast | multicast }**
5. **advertisement-interval seconds**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router bgp autonomous-system-number 例 : <pre>switch(config)# router bgp 64496 switch(config-router)#</pre>	BGP を有効にして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。
ステップ 3	neighbor prefix remote-as route-map map-name 例 : <pre>switch(config-router)# neighbor 192.0.2.0/8 remote-as routemap BGPPeers switch(config-router-neighbor)#</pre>	IPv4 プレフィックス、およびリモート BGP ピアの受け付けられた AS 番号のリストのルートマップを構成します。IPv4 の <i>prefix</i> 形式は、x.x.x.x/長さです。長さの範囲は 1 ～ 32 です。 <i>map-name</i> には最大 63 文字の英数字を使用できます。大文字と小文字は区別されます。
ステップ 4	address-family { ipv4 ipv6 } { unicast multicast } 例 : <pre>switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#</pre>	指定されたアドレスファミリに対応するグローバル アドレス ファミリ コンフィギュレーション モードを開始します。このコマンドによって、すべての BGP ネイバーセッションの自動通知およびセッション リセットが開始されます。
ステップ 5	advertisement-interval seconds 例 :	新しいルートアップデートの通知を遅らせる間隔を構成します。

BGP 再接続間隔の構成

	コマンドまたはアクション	目的
	<pre>switch(config-router-neighbor-af)# advertisement-interval 300</pre>	(注) この間隔は、ただちに行う必要があるルート取り消しの通知には適用されません。 間隔は、1 ～ 600 秒の範囲にすることができます。

例

次に、アップデート アナウンスメント遅延タイマーを構成する例を示します。

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# neighbor 192.0.2.0/8 remote-as route-map BGPPeers
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# advertisement-interval 300
```

BGP 再接続間隔の構成

BGP セッションが再接続できるまでの間隔を構成できます。

始める前に

BGP 機能が有効になっていることを確認します

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. **reconnect-interval** *interval*
4. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router bgp <i>autonomous-system-number</i> 例 : <pre>switch(config)# router bgp 64496 switch(config-router)#</pre>	BGP を有効にして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。

	コマンドまたはアクション	目的
ステップ 3	reconnect-interval interval 例 : <pre>switch(config-router)# reconnect-interval 20</pre>	ドロップされた BGP 接続を自動的に再接続できるようになるまでの間隔を構成します。間隔の範囲は 1 ～ 60 秒です。 間隔のデフォルト値は 30 秒です。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config-router)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、BGP 再接続感覚を構成する例を示します。

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# reconnect-interval 20
switch(config-router)# copy running-config startup-config
```

プレフィックス ピアのダイナミック AS 番号の設定

BGP プロセス内で複数の BGP ピアを設定できます。BGP セッションの確立をルートマップの単一の AS 番号または複数の AS 番号に制限できます。

プレフィックス ピアのダイナミック AS 番号を介して設定された BGP セッションは、**ebgp-multihop** コマンドおよび **disable-connected-check** コマンドを無視します

ルートマップの AS 番号のリストは変更できますが、ルートマップ名を変更するには **no neighbor** コマンドを使用する必要があります。設定されたルートマップの AS 番号に変更を加えた場合、新しいセッションのみに影響します。

始める前に

BGP 機能が有効になっていることを確認します

手順の概要

1. **configure terminal**
2. **router bgp autonomous-system-number**
3. **neighbor prefix remote-as route-map map-name**
4. (任意) **show bgp { ipv4 { unicast | multicast } neighbors**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	router bgp autonomous-system-number 例 : switch(config)# router bgp 64496 switch(config-router)#	BGP を有効にして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。
ステップ 3	neighbor prefix remote-as route-map map-name 例 : switch(config-router)# neighbor 192.0.2.0/8 remote-as routemap BGPPeers switch(config-router-neighbor)#	IPv4 プレフィックス、およびリモート BGP ピアの受け付けられた AS 番号のリストのルート マップを構成します。IPv4 の <i>prefix</i> 形式は、x.x.x.x/長さ長さの範囲は 1 ～ 32 です。 <i>map-name</i> には最大 63 文字の英数字を使用できます。大文字と小文字は区別されます。
ステップ 4	(任意) show bgp { ipv4 { unicast multicast } neighbors 例 : switch(config-router-neighbor)# show bgp ipv4 unicast neighbors	BGP ピアに関する情報を表示します。
ステップ 5	(任意) copy running-config startup-config 例 : switch(config-router-neighbor) copy running-config startup-config	この設定変更を保存します。

例

次に、プレフィックス ピアのダイナミック AS 番号を設定する例を示します。

```
switch# configure terminal
switch(config)# route-map BGPPeers
switch(config-route-map)# match as-number 64496, 64501-64510
switch(config-route-map)# match as-number as-path-list List1, List2
switch(config-route-map)# exit
switch(config)# router bgp 64496
switch(config-router)# neighbor 192.0.2.0/8 remote-as route-map BGPPeers
switch(config-router-neighbor)# description Peer Router B
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# copy running-config startup-config
```

BGP PIC エッジの設定

BGP PIC エッジを設定するには、次の手順に従います。



(注) BGP PIC エッジ機能は、IPv4 アドレス ファミリのみをサポートします。

始める前に

BGP をイネーブルにする必要があります（「[BGP のイネーブル化](#)」の項を参照）。

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. **neighbor** *ip-address*
4. **remote-as** *as-number*
5. **address-family** *ipv4 unicast*
6. **additional-paths** *install backup*
7. (任意) **copy** *running-config startup-config*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	router bgp <i>autonomous-system-number</i> 例 : <pre>switch(config)# router bgp 64496 switch(config-router)#</pre>	BGP を有効にして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による <i>xx.xx</i> という形式です。
ステップ 3	neighbor <i>ip-address</i> 例 : <pre>switch(config-router)# neighbor 209.165.201.1 switch(config-router-neighbor)#</pre>	リモート BGP ピアの IPv4 アドレスを設定します。 <i>ip-address</i> の形式は <i>x.x.x.x</i> です。
ステップ 4	remote-as <i>as-number</i> 例 : <pre>switch(config-router-neighbor)# remote-as as-number switch(config-router-neighbor-remote-as)#</pre>	リモート BGP ピアの AS 番号を設定します。

	コマンドまたはアクション	目的
	<code>switch(config-router-neighbor)# remote-as 64497</code>	
ステップ 5	address-family ipv4 unicast 例 : <pre>switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#</pre>	IPv4 アドレス ファミリのネイバー アドレス ファミリ設定を開始します。
ステップ 6	additional-paths install backup 例 : <pre>switch(config-router-neighbor-af)# additional-paths install backup</pre>	ルーティング テーブルにバックアップ パスをインストールする BGP をイネーブルにします。
ステップ 7	(任意) copy running-config startup-config 例 : <pre>switch(config-router-neighbor-af)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次の例は、IPv4 ネットワークで BGP PIC エッジをサポートするように、デバイスを設定する方法を示しています。

```
interface Ethernet2/2 ip address 1.1.1.5/24 no shutdown

interface Ethernet2/3 ip address 2.2.2.5/24 no shutdown

router bgp 100
neighbor 1.1.1.6
remote-as 200
address-family ipv4 unicast additional-paths install backup
address-family ipv4 unicast neighbor 2.2.2.6
remote-as 100
address-family ipv4 unicast
```

BGP が 2 つのネイバー (1.1.1.6 と 2.2.2.6) から同じプレフィックス (99.0.0.0/24 など) を受信した場合、両方のパスが URIB にインストールされます。一方はプライマリ パスになり、もう一方はバックアップ パスになります。

BGP 出力 :

```
switch(config)# show ip bgp 99.0.0.0/24
BGP routing table information for VRF default, address family IPv4 Unicast BGP routing
table entry
for 99.0.0.0/24, version 4
Paths: (2 available, best #2)
Flags: (0x00001a) on xmit-list, is in urib, is best urib route

Path type: internal, path is valid, not best reason: Internal path, backup path AS-Path:
  200 , path
sourced external to AS
```



```
2.2.2.6 (metric 0) from 2.2.2.6 (2.2.2.6)
Origin IGP, MED not set, localpref 100, weight 0
```

```
Advertised path-id 1
Path type: external, path is valid, is best path AS-Path: 200 , path sourced external
to AS
1.1.1.6 (metric 0) from 1.1.1.6 (99.0.0.1)
Origin IGP, MED not set, localpref 100, weight 0

Path-id 1 advertised to peers: 2.2.2.6
```

URIB 出力 :

```
switch(config)# show ip route 99.0.0.0/24
IP Route Table for VRF "default" '*' denotes best ucast next-hop '*' denotes best mcast
next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>
99.0.0.0/24, ubest/mbest: 1/0
*via 1.1.1.6, [20/0], 14:34:51, bgp-100, external, tag 200
via 2.2.2.6, [200/0], 14:34:51, bgp-100, internal, tag 200 (backup)
```

UFIB 出力 :

```
switch# show forwarding route 123.1.1.0 detail module 8
Prefix 123.1.1.0/24, No of paths: 1, Update time: Wed Jul 11 19:00:12 2018
Vobj id: 141 orig_as: 65002 peer_as: 65100 rnh: 10.3.0.2
10.4.0.2 Ethernet8/4 DMAC: 0018.bad8.4dfd
packets: 2 bytes: 3484 Repair path 10.3.0.2 Ethernet8/3 DMAC: 0018.bad8.4dfd
packets: 0
bytes: 1
```

BGP 情報の消去

BGP 情報を消去するには、次のコマンドを使用します。

コマンド	目的
clear bgp all { <i>neighbor</i> * <i>as-number</i> peer-template <i>name</i> <i>prefix</i> } [vrf <i>vrf-name</i>]	すべてのアドレス ファミリから 1 つ以上のネイバーをクリアします。* を指定すると、すべてのアドレス ファミリのすべてのネイバーが消去されます。引数は次のとおりです。 • <i>neighbor</i> : ネイバーの IPv4 アドレス。 • <i>as-number</i> : 自律システム番号。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。 • <i>name</i> : ピア テンプレート名。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • <i>prefix</i> : IPv4 プレフィックス。そのプレフィックス内のすべてのネイバーがクリアされます • <i>vrf-name</i> : VRF 名。その VRF 内のすべてのネイバーがクリアされます。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
clear bgp all dampening [vrf <i>vrf-name</i>]	すべてのアドレス ファミリのルートフラップ ダンプニング ネットワークをクリアします。 <i>vrf-name</i> には最大 64 文字の英数字文字列を指定します。大文字と小文字は区別されます。
clear bgp all flap-statistics [vrf <i>vrf-name</i>]	すべてのアドレスファミリのルートフラップ統計情報をクリアします。 <i>vrf-name</i> には最大 64 文字の英数字文字列を指定します。大文字と小文字は区別されます。
clear bgp ipv4 { unicast multicast } dampening [vrf <i>vrf-name</i>]	選択したアドレス ファミリのルートフラップ ダンプニング ネットワークをクリアします。 <i>vrf-name</i> には最大 64 文字の英数字文字列を指定します。大文字と小文字は区別されます。
clear bgp ipv4 { unicast multicast } flap-statistics [vrf <i>vrf-name</i>]	選択したアドレスファミリのルートフラップ統計情報をクリアします。 <i>vrf-name</i> には最大 64 文字の英数字文字列を指定します。大文字と小文字は区別されます。

コマンド	目的
<pre>clear bgp { ipv4 ipv6 } { unicast multicast } { neighbor * as-number peer-template name prefix } [vrf vrf-name]</pre>	選択したアドレス ファミリから 1 つ以上のネイバーをクリアします。* を指定すると、そのアドレス ファミリのすべてのネイバーが消去されます。引数は次のとおりです。 • neighbor : ネイバーの IPv4 アドレス。 • as-number : 自律システム番号。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。 • name : ピア テンプレート名。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • prefix : IPv4 プレフィックス。そのプレフィックス内のすべてのネイバーがクリアされます。 • vrf-name : VRF 名。その VRF 内のすべてのネイバーがクリアされます。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します
<pre>clear ip bgp { ip { unicast multicast } } { neighbor * as-number peer-template name prefix } [vrf vrf-name]</pre>	1 つ以上のネイバーをクリアします。* を指定すると、そのアドレス ファミリのすべてのネイバーが消去されます。引数は次のとおりです。 • neighbor : ネイバーの IPv4 アドレス。 • as-number : 自律システム番号。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。 • name : ピア テンプレート名。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • prefix : IPv4 プレフィックス。そのプレフィックス内のすべてのネイバーがクリアされます。 • vrf-name : VRF 名。その VRF 内のすべてのネイバーがクリアされます。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。

コマンド	目的
clear ip bgp dampening [<i>ip-neighbor</i> <i>ip-prefix</i>] [<i>vrf vrf-name</i>]	1 つ以上のネットワークのルートフラップダンプニングをクリアします。引数は次のとおりです。 • <i>neighbor</i> : ネイバーの IPv4 または IPv6 アドレス。 • <i>ip-prefix</i> : IPv4 または IPv6。そのプレフィックス内のすべてのネイバーがクリアされます。 • <i>vrf-name</i> : VRF 名。その VRF 内のすべてのネイバーがクリアされます。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
clear ip bgp flap-statistics [<i>ip-neighbor</i> <i>ip-prefix</i>] [<i>vrf vrf-name</i>]	1 つ以上のネットワークのルートフラップ統計情報をクリアします。引数は次のとおりです。 • <i>neighbor</i> : ネイバーの IPv4 または IPv6 アドレス。 • <i>ip-prefix</i> : IPv4 または IPv6。そのプレフィックス内のすべてのネイバーがクリアされます。 • <i>vrf-name</i> : VRF 名。その VRF 内のすべてのネイバーがクリアされます。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。

ベーシック BGP の設定の確認

BGP の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show bgp all [<i>summary</i>] [<i>vrf vrf-name</i>]	すべてのアドレスファミリについて、BGP 情報を表示します。
show bgp convergence [<i>vrf vrf-name</i>]	すべてのアドレスファミリについて、BGP 情報を表示します。
show bgp { <i>ipv4</i> { <i>unicast</i> <i>multicast</i> } [<i>ip-address</i>] <i>community</i> { <i>regex</i> <i>expression</i> [<i>community</i>] [<i>no-advertise</i>] [<i>no-export</i>] [<i>no-export-subconfed</i>] } [<i>vrf vrf-name</i>]	BGP コミュニティと一致する BGP ルートを表示します。
show bgp [<i>vrf vrf-name</i>] { <i>ip</i> <i>ipv6</i> } { <i>unicast</i> <i>multicast</i> } [<i>ip-address</i>] <i>community-list list-name</i> [<i>vrf vrf-name</i>]	BGP コミュニティリストと一致する BGP ルートを表示します。

コマンド	目的
show bgp ip { unicast multicast } [ip-address] extcommunity { regexp <i>expression</i> generic [non-transitive transitive] <i>aa4:nn</i> [exact-match]} [vrf <i>vrf-name</i>]	BGP 拡張コミュニティと一致する BGP ルートを表示します。
show bgp ip { unicast multicast } [ip-address] extcommunity-list <i>list-name</i> [exact-match] [vrf <i>vrf-name</i>]	BGP 拡張コミュニティ リストと一致する BGP ルートを表示します。
show bgp ip { unicast multicast } [ip-address] { dampening <i>dampened-paths</i> [regexp <i>expression</i>]} [vrf <i>vrf-name</i>]	BGP ルート ダンプニングの情報を表示します。ルート フラップ ダンプニング情報を消去するには、 clear bgp dampening コマンドを使用します。
show bgp ip { unicast multicast } [ip-address] history-paths [regexp <i>expression</i>] [vrf <i>vrf-name</i>]	BGP ルート ヒストリ パスを表示します。
show bgp ip { unicast multicast } [ip-address] filter-list <i>list-name</i> [vrf <i>vrf-name</i>]	BGP フィルタ リストの情報を表示します。
show bgp ip { unicast multicast } [ip-address] neighbors [ip-address] [vrf <i>vrf-name</i>]	BGP ピアの情報を表示します。これらのネイバーを消去するには、 clear bgp neighbors コマンドを使用します。
show bgp ip { unicast multicast } [ip-address] { nexthop nexthop-database } [vrf <i>vrf-name</i>]	BGP ルート ネクスト ホップの情報を表示します。
show bgp paths	BGP パス情報を表示します。
show bgp ip { unicast multicast } [ip-address] policy <i>name</i> [vrf <i>vrf-name</i>]	BGP ポリシー情報を表示します。ポリシー情報を消去するには、 clear bgp policy コマンドを使用します。
show bgp ip { unicast multicast } [ip-address] prefix-list <i>list-name</i> [vrf <i>vrf-name</i>]	プレフィックス リストと一致する BGP ルートを表示します。
show bgp ip { unicast multicast } [ip-address] received-paths [vrf <i>vrf-name</i>]	ソフト再構成用に保管されている BGP パスを表示します。
show bgp ip { unicast multicast } [ip-address] regexp <i>expression</i> [vrf <i>vrf-name</i>]	AS_path 正規表現と一致する BGP ルートを表示します。
show bgp ip { unicast multicast } [ip-address] route-map <i>map-name</i> [vrf <i>vrf-name</i>]	ルート マップと一致する BGP ルートを表示します。
show bgp peer-policy <i>name</i> [vrf <i>vrf-name</i>]	BGP ピア ポリシー情報を表示します。
show bgp peer-session <i>name</i> [vrf <i>vrf-name</i>]	BGP ピア セッション情報を表示します。

コマンド	目的
show bgp peer-template name [vrf vrf-name]	BGP ピア テンプレート情報を表示します。ピア テンプレートのすべてのネイバーを消去するには、 clear bgp peer-template コマンドを使用します。
show bgp process	BGP プロセス情報を表示します。
show ip bgp options	BGP のステータスと構成情報を表示します。このコマンドには複数のオプションがあります。
show running-configuration bgp	現在実行中の BGP コンフィギュレーションを表示します。

BGP 統計情報の表示

BGP の統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
show bgp ip { unicast multicast } [ip-address] flap-statistics [vrf vrf-name]	BGP ルート フラップの統計情報を表示します。これらの統計情報をクリアするには、 clear bgp flap-statistics コマンドを使用します。
show bgp sessions [vrf vrf-name]	すべてのピアの BGP セッションを表示します。これらの統計情報をクリアするには、 clear bgp sessions コマンドを使用します。
show bgp sessions [vrf vrf-name]	すべてのピアの BGP セッションを表示します。これらの統計情報をクリアするには、 clear bgp sessions コマンドを使用します。
show bgp statistics	BGP 統計情報を表示します。

ベーシック BGP の設定例

次に、ベーシック BGP 設定の例を示します。

```
feature bgp
router bgp 64496
neighbor 192.0.2.1 remote-as 64496
address-family ipv4 unicast
next-hop-self
```

関連項目

BGP の関連項目は、次のとおりです。

- [Route Policy Manager の設定](#)（443 ページ）

次の作業

次の機能の詳細については、[高度な BGP の設定](#)（297 ページ）を参照してください。

- ピア テンプレート
- ルートの再配布
- ルート マップ

その他の参考資料

BGP の実装に関連する詳細情報については、次の項を参照してください。

MIB

MIB	MIB のリンク
BGP4-MIB CISCO-BGP4-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://tools.cisco.com/ITDIT/MIBS/servlet/index



第 10 章

高度な BGP の設定

この章では、Cisco NX-OS スイッチでボーダー ゲートウェイ プロトコル (BGP) の拡張機能を設定する方法について説明します。

この章は、次の項で構成されています。

- [拡張 BGP の概要 \(297 ページ\)](#)
- [拡張 BGP の前提条件 \(307 ページ\)](#)
- [拡張 BGP に関する注意事項と制限事項 \(308 ページ\)](#)
- [BGP のデフォルト設定 \(311 ページ\)](#)
- [高度な BGP の設定 \(311 ページ\)](#)
- [BGP 向け BFD の構成例 \(341 ページ\)](#)
- [BGP 属性フィルタリングの設定とエラー処理 \(341 ページ\)](#)
- [独自の自律システムを含む自律システム パスの設定 \(344 ページ\)](#)
- [BGP グレースフル シャットダウン \(360 ページ\)](#)
- [グレースフル リスタートの設定 \(374 ページ\)](#)
- [拡張 BGP の設定の確認 \(377 ページ\)](#)
- [BGP 統計情報の表示 \(379 ページ\)](#)
- [関連項目 \(379 ページ\)](#)
- [その他の参考資料 \(380 ページ\)](#)

拡張 BGP の概要

BGP は、組織または自律システム間のループフリー ルーティングを実現する、インタードメインルーティングプロトコルです。Cisco NX-OS は BGP バージョン 4 をサポートします。BGP v4 に組み込まれているマルチプロトコル拡張機能を使用すると、IP ルートおよび複数のレイヤ 3 プロトコル アドレス ファミリに関するルーティング情報を BGP に伝送させることができます。BGP では、他の BGP 対応スイッチ (BGP ピア) との間で TCP セッションを確立するために、信頼できるトランスポート プロトコルとして TCP を使用します。外部組織に接続するときには、ルータが外部 BGP (eBGP) ピアリングセッションを作成します。同じ組織内の BGP ピアは、内部 BGP (iBGP) ピアリングセッションを通じて、ルーティング情報を交換します。

ピア テンプレート

BGP ピア テンプレートを使用すると、類似した BGP ピア間で再利用できる共通のコンフィギュレーションブロックを作成できます。各ブロックでは、ピアに継承させる一連の属性を定義できます。継承した属性の一部を上書きすることもできるので、非常に柔軟性のある方法で、繰り返しの多い BGP の設定を簡素化できます。

Cisco NX-OS は、3 種類のピア テンプレートを実装します。

- **peer-session** テンプレートでは、トランスポートの詳細、ピアのリモート自律システム番号、セッションタイマーなど、BGP セッション属性を定義します。peer-session テンプレートは、別の peer-session テンプレートから属性を継承することもできます（ローカル定義の属性によって、継承した peer-session 属性は上書きされます）。
- **peer-policy** テンプレートでは、着信ポリシー、発信ポリシー、フィルタ リスト、プレフィックス リストを含め、アドレス ファミリに依存する、ピアのポリシー要素を定義します。peer-policy テンプレートは、一連の peer-policy テンプレートからの継承が可能です。Cisco NX-OS は、継承設定のプリファレンス値で指定された順序で、これらの peer-policy テンプレート进行评估します。最小値が大きい値よりも優先されます。
- **peer** テンプレートは、peer-session および peer-policy テンプレートからの継承が可能であり、ピアの定義を簡素化できます。peer テンプレートの使用は必須ではありませんが、peer テンプレートによって再利用可能なコンフィギュレーションブロックが得られるので、BGP の設定を簡素化できます。

認証

BGP ネイバー セッションに認証を設定できます。この認証方式によって、ネイバーに送られる各 TCP セグメントに MD5 認証ダイジェストが追加され、不正なメッセージや TCP セキュリティ アタックから BGP が保護されます。



(注) MD5 パスワードは、BGP ピア間で一致させる必要があります。

ルート ポリシーおよび BGP セッションのリセット

BGP ピアにルート ポリシーを関連付けることができます。ルート ポリシーではルート マップを使用して、BGP が認識するルートを制御または変更します。着信または発信ルート アップデートに関するルート ポリシーを設定できます。ルート ポリシーはプレフィックス、AS_path 属性など、さまざまな条件で一致が必要であり、ルートを選択して受け付けるかまたは拒否します。ルート ポリシーでパス属性を変更することもできます。

BGP ピアに適用するルート ポリシーを変更する場合は、そのピアの BGP セッションをリセットする必要があります。Cisco NX-OS は、BGP ピアリングセッションのリセット方法として、次の 3 種類をサポートします。

- **ハードリセット**：ハードリセットでは、指定されたピアリングセッションが TCP 接続を含めて切断され、指定のピアからのルートが削除されます。このオプションを使用すると、BGP ネットワーク上のパケットフローが中断します。ハードリセットは、デフォルトでディセーブルです。
- **ソフト再構成着信**：ソフト再構成着信によって、セッションをリセットすることなく、指定されたピアのルーティングアップデートが開始されます。このオプションを使用できるのは、着信ルートポリシーを変更する場合です。ソフト再構成着信の場合、ピアから受け取ったすべてのルートのコピーを保存したあとで、着信ルートポリシーを介してルートが処理されます。着信ルートポリシーを変更する場合、Cisco NX-OS は変更された着信ルートポリシーを介して保存ルートを渡し、既存のピアリングセッションを切断することなく、ルートテーブルをアップデートします。ソフト再構成着信の場合、まだフィルタリングされていない BGP ルートの保存に、大量のメモリリソースを使用する可能性があります。ソフト再構成着信は、デフォルトでディセーブルです。
- **ルートリフレッシュ**：ルートリフレッシュでは、着信ルートポリシーの変更時に、サポートするピアにルートリフレッシュ要求を送信することによって、着信ルーティングテーブルがダイナミックにアップデートされます。リモート BGP ピアは新しいルートコピーで応答し、ローカル BGP スピーカが変更されたルートポリシーでそれを処理します。Cisco NX-OS はピアに、プレフィックスの発信ルートリフレッシュを自動的に送信します。
- BGP ピアは、BGP ピアセッションの確立時に、BGP 機能ネゴシエーションの一部として、ルートリフレッシュ機能をアドバタイズします。ルートリフレッシュは優先オプションであり、デフォルトでイネーブルです。



(注) BGP はさらに、ルート再配布、ルート集約、ルートダンプニングなどの機能にルートマップを使用します。ルートマップの詳細については、[Route Policy Manager の設定 \(443 ページ\)](#) を参照してください。

eBGP

eBGP を使用すると、異なる AS からの BGP ピアを接続し、ルーティングアップデートを交換できます。外部ネットワークへの接続によって、自分のネットワークから他のネットワークへ、またインターネットを介して、トラフィックを転送できます。

eBGP ピアリングセッションの確立には、ループバックインターフェイスを使用します。ループバックインターフェイスは、インターフェイスフラップが発生する可能性が小さいからです。インターフェイスフラップが発生するのは、障害またはメンテナンスが原因で、インターフェイスが管理上アップまたはダウンになったときです。マルチホップ、高速外部フォールオーバー、AS パス属性のサイズ制限については、「[eBGP の構成](#)」のセクションを参照してください。

eBGP ネクストホップ変更なし

外部 BGP (eBGP) セッションでは、デフォルトで、デバイスがルートの送信時に BGP ルートのネクストホップ属性を（自身のアドレスに）変更します。eBGP ネクストホップ非変更機能が設定されている場合、BGP はネクストホップ属性を変更せずに eBGP マルチホップピアにルートを送信します。ネクストホップ属性は変更されません。BGP ネクストホップ非変更機能により、ネットワークの設計および移行を柔軟に実効できます。これは、マルチホップとして設定された eBGP ピア間だけで使用できます。

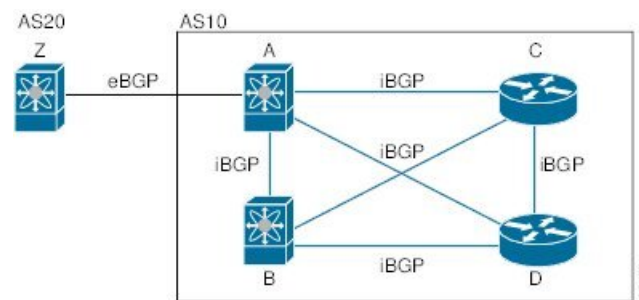
たとえば、デバイス A、B、C 間の eBGP 接続を持つネットワークを考えてみます。デバイス A がデバイス B に 100 のプレフィックスをアナウンスするとします。デバイス B にはデバイス C へのアウトバウンドルートマップが構成され、`match ip prefix list` と `set ip next-hop` がルートマップで設定されています。デバイス B は、プレフィックスリストに一致するルートに対してだけ、変更されていないネクストホップアドレスを伝播します。他のプレフィックスについては、自身をネクストホップアドレスとします。

iBGP

内部 BGP (iBGP) を使用すると、同じ自律システム内の BGP ピアを接続できます。iBGP はマルチホーム BGP ネットワーク（同じ外部自律システムに対して複数の接続があるネットワーク）に使用できます。

次の図に、より大きな BGP ネットワークの中の iBGP ネットワークを示します。

図 26: iBGP ネットワーク



iBGP ネットワークはフルメッシュです。各 iBGP ピアは、ネットワーク ループを防止するために、他のすべての iBGP ピアに対して直接接続されています。



(注) iBGP ネットワークでは別個のインテリア ゲートウェイ プロトコルを設定する必要があります。

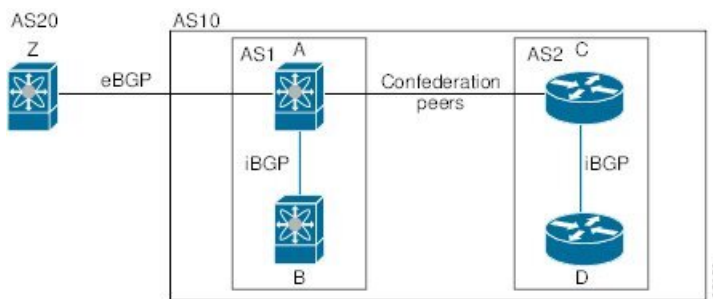
AS 連合

フルメッシュの iBGP ネットワークは、iBGP ピア数が増えるにしたがって複雑になります。自律システムを複数のサブ自律システムに分割し、それを 1 つの連合としてまとめることによっ

て、iBGP メッシュを緩和できます。連合は、同じ自律システム番号を使用して外部ネットワークと通信する、iBGP ピアからなるグループです。各サブ AS はその中ではフルメッシュであり、同じ連合内の他のサブ AS に対する少数の接続があります。

図には、BGP ネットワークが2つのサブ自律システムと1つのコンフェデレーションに分けられて表示されています。

図 27: AS 連合



この例では、AS10 が 2 つの AS (AS1 および AS2) に分割されています。各サブ AS はフルメッシュですが、サブ AS 間のリンクは 1 つだけです。AS コンフェデレーションを使用することによって、図「AS 連合」のフルメッシュ自律システムに比べて、リンク数を少なくできます。

ルート リフレクタ

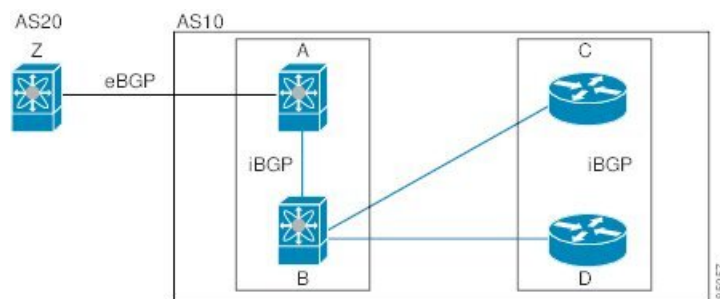
ルート リフレクタ構成を使用することによって、iBGP メッシュを緩和することもできます。ルート リフレクタは学習したルートをネイバーに渡すことで、すべての iBGP ピアをフルメッシュにしなくてもすむようにします。

図 iBGP ネットワークに、メッシュの iBGP スピーカーを 4 つ使用する (ルータ A、B、C、D)、単純な iBGP 構成を示します。ルート リフレクタを使用しなかった場合、外部ネイバーからルートを受け取ったルータ A は、3 つの iBGP ネイバーのすべてにルートをアドバタイズします。

ある iBGP ピアをルート リフレクタとして設定すると、そのピアが iBGP で学習したルートを一連の iBGP ネイバーに渡す役割を担います。

次の図では、ルータ B がルート リフレクタです。ルート リフレクタは、ルータ A からアドバタイズされたルートを受信すると、ルータ C と D へのルートをアドバタイズ (リフレクト) します。ルータ A は、ルータ C と D の両方にアドバタイズする必要がなくなります。

図 28: ルート リフレクタ



ルート リフレクタおよびそのクライアント ピアは、クラスタを形成します。ルート リフレクタのクライアント ピアとして動作するように、すべての iBGP ピアを設定する必要はありません。ただし、完全な BGP アップデートがすべてのピアに届くように、非クライアント ピアはフルメッシュとして設定する必要があります。

機能ネゴシエーション

BGP スピーカは機能ネゴシエーション機能を使用することによって、ピアがサポートする BGP 拡張機能について学習できます。機能ネゴシエーションによって、リンクの両側の BGP ピアがサポートする機能セットだけを BGP に使用させることができます。

BGP ピアが機能ネゴシエーションをサポートしない場合で、なおかつアドレスファミリが IPv4 として設定されている場合、Cisco NX-OS は機能ネゴシエーションを行わずに、ピアとの新規セッションを試みます。

ルート ダンプニング

ルート ダンプニングは、インターネットワーク上でのフラッピング ルートの伝搬を最小限に抑える BGP 機能です。ルート フラップが発生するのは、使用可能ステートと使用不能ステートが短時間で次々切り替わる場合です。

AS1、AS2、および AS3 という 3 つの BGP 自律システムからなるネットワークの場合について考えてみます。AS1 のルートがフラップした（使用不能になった）とします。ルート ダンプニングを使用しない場合、AS1 は AS2 に回収メッセージを送信します。AS2 は AS3 にその回収メッセージを伝達します。フラッピング ルートが再び発生すると、AS1 から AS2 にアドバタイズメント メッセージを送信し、AS2 は AS3 にそのアドバタイズメントを送信します。ルートの使用不能と使用可能が繰り返されると、AS1 は多数の回収メッセージおよびアドバタイズメント メッセージを送信することになり、それが他の自律システムに伝播します。

ルート ダンプニングによって、フラッピングを最小限に抑えることができます。ルート フラップが発生したとします。（ルート ダンプニングがイネーブルの）AS2 がルートにペナルティとして 1000 を割り当てます。AS2 は引き続き、ネイバーにルートの状態をアドバタイズします。ルート フラップが発生するたびに、AS2 がペナルティ値を追加します。ルート フラップが頻繁に発生して、ペナルティが設定可能な抑制限度を超えると、AS2 はフラップ回数に関係なく、ルートのアドバタイズを中止します。その結果、ルートが減衰（ダンプニング）します。

ルートに与えられたペナルティは、再使用限度に達するまで減衰します。その時点で、AS2 は再びルートをアドバタイズします。再使用限度が 50% になると、AS2 はそのルートのダンプニング情報を削除します。



- (注) ルートダンプニングがイネーブルの場合は、ピアのリセットによってルートが回収されても、リセット中の BGP にはペナルティは適用されません。

ロードシェアリングおよびマルチパス

BGP はルーティングテーブルに、同じ宛先プレフィックスに到達する複数の等コスト eBGP または iBGP パスを組み込むことができます。その場合、宛先プレフィックスへのトラフィックは、組み込まれたすべてのパス間で共有されます。

BGP ベストパス アルゴリズムでは、次の属性が同じ場合に、等コストパスと見なされます。

- 重量
- ローカルプリファレンス
- AS_path
- オリジンコード
- Multi-Exit Discriminator (MED)
- BGP ネクストホップまでの IGP コスト

BGP はこれら複数のパスの中から、ベストパスとして 1 つだけ選択し、そのパスを BGP ピアにアドバタイズします。



- (注) 異なる AS 連合から受け取ったパスは、外部 AS_path 値およびその他の属性が同じ場合に、等コストパスと見なされます。



- (注) iBGP マルチパスに関してルートリフレクタを設定すると、ルートリフレクタが、選択されたベストパスをピアにアドバタイズします。そのパスのネクストホップは変更されません。

ルート集約

集約アドレスを設定できます。ルート集約を使用すると、固有性の強い一連のアドレスをすべての固有アドレスを代表する 1 つのアドレスに置き換えることによって、ルートテーブルを簡素化できます。たとえば、10.1.1.0/24、10.1.2.0/24、および 10.1.3.0/24 という固有性の強い 3 つのアドレスを 1 つの集約アドレス 10.1.0.0/16 に置き換えることができます。

アドバタイズされるルートが少なくなるように、BGP ルート テーブル内には集約プレフィックスが存在します。



(注) Cisco NX-OS は、自動ルート集約をサポートしていません。

ルート集約はフォワーディンググループにつながる可能性があります。この問題を回避するために、集約アドレスのアドバタイズメントを生成するときに、BGP はローカルルーティングテーブルに、その集約アドレスに対応するサマリー廃棄ルートを自動的に組み込みます。BGP はサマリー廃棄のアドミニストレーティブ ディスタンスを 220 に設定し、ルート タイプを廃棄に設定します。BGP はネクストホップ解決に廃棄ルートを使用しません。

BGP 条件付きアドバタイズメント

BGP 条件付きアドバタイズメントを使用すると、プレフィックスが BGP テーブルに存在するかどうかに基づいてルートをアドバタイズまたは撤回するように BGP を設定できます。この機能は、たとえば、BGP でいずれかのプロバイダーにプレフィックスをアドバタイズするようなマルチホーム ネットワーク（他のプロバイダーからの情報が存在しない場合のみ）で便利です。

AS1、AS2、および AS3 という 3 つの BGP 自律システムからなるネットワークの例について考えてみます。この例で、AS1 と AS3 はインターネットと AS2 に接続しています。条件付きアドバタイズメントを使用しない場合、AS2 はすべてのルートを AS1 と AS3 の両方にプロパゲートします。条件付きアドバタイズメントを使用すれば、AS1 からのルートが存在しない場合のみ（たとえば AS1 へのリンクがダウンした場合）、特定のルートを AS3 にアドバタイズするように AS2 を設定できます。

BGP 条件付きアドバタイズメントでは、設定されたルート マップに一致する各ルートに、存在テストまたは非存在テストが追加されます。「[BGP 条件付きアドバタイズメントの設定](#)」を参照してください。

BGP ネクスト ホップ アドレス トラッキング

BGP は、インストールされているルートのネクスト ホップ アドレスをモニタして、ネクスト ホップの到達可能性の確認、および BGP ベストパスの選択、インストール、検証を行います。BGP ネクストホップアドレスのトラッキングを行うと、ネクストホップの到達可能性に影響を及ぼす可能性のあるルート変更が RIB で行われたときに確認プロセスをトリガーすることで、このようなネクストホップ到達可能性テストの速度が向上します。

ネクストホップ情報が変更されると、BGP は RIB から通知を受信します（イベント駆動型の通知）。BGP は、次のいずれかのイベントが発生したときに通知を受け取ります。

- ネクスト ホップが到達不能になった。
- ネクスト ホップが到達可能になった。
- ネクスト ホップへの完全な繰り返し IGP メトリックが変更される。

- ファースト ホップの IP アドレスまたはファースト ホップのインターフェイスが変更される。
- ネクスト ホップが接続された。
- ネクスト ホップが接続解除された。
- ネクスト ホップがローカル アドレスになった。
- ネクスト ホップが非ローカル アドレスになった。



(注) 到達可能性および再帰メトリック イベントは、最適パスの再計算をトリガーします。

RIB からのイベント通知は、クリティカルおよび非クリティカルとして分類されます。クリティカルおよび非クリティカルイベントの通知は、別々のバッチで送信されます。ただし、非クリティカルイベントが保留中であり、クリティカルイベントを読み込む要求がある場合は、非クリティカルイベントがクリティカルイベントとともに送信されます。

- クリティカルイベントは、ネクスト ホップの到達可能性（到達可能と到達不能）、接続性（接続と非接続）、および局在性（ローカルと非ローカル）に関係があります。これらのイベントの通知は遅延しません。
- 非クリティカルイベントには、IGP メトリックの変更のみが含まれます。

詳細については、「[BGP ネクスト ホップ アドレス トラッキングの設定](#)」を参照してください。

Site of Origin

発信元サイトは、マルチホーム VPN サイトがある場合にルーティング ループを防止します。同じサイトから学習したルートには、同じサイトへのすべての PE-CE リンクの PE で構成されている、同じ `site-of-origin` 値を使用してタグ付けされます。特定の `Site-of-Origin` 値を持つルートが、PE-CE リンクに構成されている同じ `Site-of-Origin` 値を持つ CE に再アドバタイズされることはありません。このプロセスにより、CE ルータは同じサイトから発信されたルートを再学習できなくなります。BGP と EIGRP は、ループを防ぐために `Site of Origin` を使用します。

サイトの自律システム番号 (ASN) をプロバイダの ASN でオーバーライドできます。この機能は、ルートの発信元サイトを識別し、VPN 内のルータ間でのルーティング ループを防ぐために、発信元サイトと併用することがよくあります。

ルートの再配布

スタティック ルートまたは他のプロトコルからのルートを再配布するように、BGP を設定できます。再配布を指定してルート ポリシーを設定し、BGP に渡されるルートを制御します。ルート ポリシーを使用すると、宛先、送信元プロトコル、ルート タイプ、ルート タグなどの

属性に基づいて、ルートをフィルタリングできます。詳細については、[Route Policy Manager の設定（443 ページ）](#)を参照してください。

BFD

この機能では、双方向フォワーディング検出（BFD）をサポートします。BFDは、転送パスの障害を高速で検出することを目的にした検出プロトコルです。BFDは2台の隣接デバイス間のサブセカンド障害を検出し、BFDの負荷の一部を、サポートされるモジュール上のデータプレーンに分散できるため、プロトコル hello メッセージよりも CPU を使いません。

BGP の BFD は eBGP シングルホップ ピアおよび iBGP シングルホップ ピアでサポートされます。BFD を使用している iBGP シングルホップ ピアの場合、ネイバー コンフィギュレーション モードで `update-source` オプションを構成する必要があります。BFD は、その他の iBGP ピアまたはマルチホップ eBGP ピアでサポートされません。

BFD は以下のタイプのインターフェイスでサポートされます。

- レイヤ 3 物理およびサブインターフェイス
- レイヤ 3 ポート チャンネルおよびサブインターフェイス
- スイッチ仮想インターフェイス（SVI）

BGP の BFD は、ポート チャンネル上の認証またはリンクごとの BFD セッションはサポートしません。

Cisco NX-OS リリース 9.3(3) 以降では、BGP の BFD は BGP IPv4 と IPv6 のプレフィックスピアでもサポートされます。このサポートにより、BGP はマルチホップ BFD を使用できるようになり、BGP コンバージェンス時間が改善されます。プレフィックスピアでは、シングルホップ BGP とマルチホップ BGP の両方がサポートされます。

詳細については、[双方向フォワーディング検出の設定（467 ページ）](#)を参照してください。

BGP の調整

BGP タイマーによって、さらにベストパス アルゴリズムの調整によって、BGP のデフォルト動作を変更できます。

BGP タイマー

BGP では、ネイバー セッションおよびグローバル プロトコル イベントにさまざまなタイプのタイマーを使用します。確立されたセッションごとに、最低限2つのタイマーがあります。定期的にキープアライブメッセージを送信するためのタイマー、さらに想定時間内にピアのキープアライブが届かなかった場合に、セッションをタイムアウトさせるためのタイマーです。また、個々の機能を処理するための、その他のタイマーがあります。これらのタイマーは通常、秒単位で設定します。タイマーには、異なる BGP ピアで同じタイマーが異なるタイミングでスタートするように、ランダム アジャストメントが組み込まれています。

ベストパス アルゴリズムの調整

オプションの構成パラメータによって、ベストパスアルゴリズムのデフォルト動作を変更できます。たとえば、アルゴリズムでの Multi-Exit Discriminator 属性およびルータ ID の扱い方を変更できます。

マルチプロトコル BGP

Cisco NX-OS の BGP は、複数のアドレス ファミリをサポートします。マルチプロトコル BGP (MP-BGP) は、アドレス ファミリに応じて異なるルート セットを伝送します。BGP ではたとえば、IPv4 ユニキャスト ルーティング用のルートと IPv4 マルチキャスト ルーティング用のルート セットを伝送できます。IP マルチキャスト ネットワークではリバース パス フォワーディング (RPF) のチェックに MP-BGP を使用できます。



(注) マルチキャスト BGP ではマルチキャスト状態情報をプロパゲートしないため、プロトコル独立マルチキャスト (PIM) などのマルチキャスト プロトコルが必要です。

マルチプロトコル BGP 設定をサポートするには、ルータ アドレスファミリおよびネイバー アドレス ファミリの各コンフィギュレーション モードを使用します。MP-BGP では、設定されたアドレス ファミリごとに別々の RIB が維持されます (ユニキャスト RIB と、BGP のマルチキャスト RIB など)。

マルチプロトコル BGP ネットワークは下位互換性がありますが、マルチプロトコル拡張機能をサポートしない BGP ピアは、アドレスファミリ ID 情報など、マルチプロトコル拡張機能が伝送するルーティング情報を転送できません。

RFC 5549

Cisco NX-OS リリース 9.2(2) 以降、BGP は RFC 5549 をサポートしており、IPv4 プレフィックスを IPv6 ネクスト ホップで伝送できます。BGP はすべてのホップで実行され、すべてのルータが IPv4 および IPv6 トラフィックを転送できるため、各ルータ間で IPv6 トンネルをサポートする必要はありません。BGP は、IPv6 ルートを介した IPv4 を Unicast Route Information Base (URIB) にインストールします。

拡張 BGP の前提条件

BGP を使用するには、次の前提条件を満たしている必要があります。

- BGP 機能を有効にする必要があります ([BGP 機能のイネーブル化](#)のセクションを参照)。
- システムに有効なルータ ID を設定しておく必要があります。
- Regional Internet Registry (RIR) によって割り当てられたか、またはローカル管理の AS 番号を取得しておく必要があります。

- ネイバー関係を作成しようとするピアに到達可能でなければなりません（Interior Gateway Protocol（IGP）、スタティック ルート、直接接続など）。
- BGP セッションを確立するネイバー環境で、アドレス ファミリを明示的に設定する必要があります。

拡張 BGP に関する注意事項と制限事項

BGP 設定時の注意事項および制約事項は、次のとおりです。

- プレフィックス ピアリングは、パッシブ TCP モードでのみ動作します。ピア アドレスがプレフィックス内にある場合、リモート ピアからの着信接続を受け入れます。
- ダイナミック AS 番号プレフィックス ピア構成は、BGP テンプレートから継承した個々の AS 番号の構成よりも優先します。
- AS 連合でプレフィックス ピアにダイナミック AS 番号を設定した場合、BGP はローカル連合の AS 番号のみでセッションを確立します。
- ダイナミック AS 番号プレフィックス ピアで作成された BGP セッションは、設定済みの eBGP マルチホップ存続可能時間（TTL）値や直接接続ピアに対するディセーブル済みのチェックを無視します。
- ルータ ID の自動変更およびセッション フラップを避けるために、BGP 用のルータ ID を設定します。
- ピアごとに最大プレフィックス構成オプションを使用し、受信するルート数および使用するシステム リソース数を制限してください。
- update-source を設定し、eBGP マルチホップ セッションでセッションを確立します。
- 再配布を設定する場合は、BGP ルート マップを指定します。
- VRF 内で BGP ルータ ID を設定します。
- キープアライブおよびホールドタイマーの値を小さくすると、ネットワークでセッションフラップが発生する可能性があります。
- 次の注意事項および制約事項が remove-private-as コマンドに適用されます。
 - デバイスのローカル AS 番号がプライベート AS 番号である場合、同じデバイス上の他のネイバーに対しては remove-private-as 構成コマンドを使用できません。回避策として、パブリック ローカル AS 番号を持つ各ネイバーで local-as コマンドを使用できます。
 - デバイスの実際の AS 番号がプライベート AS 番号で、パブリックな local-as 番号を持つネイバーに対して remove-private-as all コマンドが構成されている場合は、local-as number [no-prepend [replace-as]] コマンドを使用して、実際のプライベート AS 番号が AS パスに付加されていないことを確認します。

- デバイスの実際の AS 番号がパブリック AS 番号であり、ネイバーに対して `remove-private-as all` コマンドが構成されている場合は、同じネイバーに対してプライベート `local-as` 番号を構成できません。回避策として、既存の構成を削除して続行する必要があります。
- `remove-private-as` コマンドでは、AS パスにパブリックとプライベートの両方の AS 番号が含まれている場合でも、AS パスからプライベート AS 番号が削除されます。
- `remove-private-as` コマンドでは、AS パスにプライベート AS 番号のみが含まれている場合でも、AS パスからプライベート AS 番号が削除されます。このコマンドは eBGP ピアのみに適用され、その場合、eBGP ピアではローカルデバイスの AS 番号が AS パスに付加されるため、長さ 0 の AS パスにはなることはありません。
- `remove-private-as` コマンドでは、AS パスでコンフェデレーションセグメントの前にプライベート AS 番号が出現する場合でも、プライベート AS 番号が削除されます。
- AS パスからプライベート AS 番号を削除すると、送信されるプレフィックスのパス長が減少します。AS パス長は BGP 最良パス選択の重要な要素であるため、パス長を保持するために必要な場合があります。`replace-as` キーワードは、削除されたすべての AS 番号をローカルルータの AS 番号で置き換えることでパス長が維持されるようにします。
- Cisco NX-OS リリース 9.3(3) 以降では、BGP の BFD は BGP IPv4 と IPv6 のプレフィックスピアでサポートされます。
- Cisco NX-OS リリース 9.3(3) 以降、BGP プレフィックスピアはグレースフルリスタートをサポートします。BGP プレフィックスピアのタイムアウト値（秒単位）を設定するには、ルータ構成モードで `timers prefix-peer-timeout` コマンドを使用します。デフォルト値は 90 秒です。
- IPv4 および IPv6 アドレスファミリの IPv6 リンクローカルを介した BGP インターフェイスピアリングには、次の注意事項と制限事項が適用されます。
 - この機能は、複数のインターフェイス間で同じリンクローカルアドレスを設定することをサポートしていません。
 - この機能は、論理インターフェイス（ループバック）ではサポートされていません。イーサネットインターフェイス、ポートチャネルインターフェイス、サブインターフェイス、およびブレイクアウトインターフェイスのみがサポートされます。
 - Cisco NX-OS リリース 9.3(6) 以降では、VLAN インターフェイスがサポートされます。
 - この機能は、リンクローカルアドレスを持つ IPv6 対応インターフェイスでのみサポートされます。
 - この機能は、設定されたプレフィックスピアとインターフェイスのリモートピアが同じ場合はサポートされません。
 - 次のコマンドはネイバーインターフェイスコンフィギュレーションモードではサポートされていません。

- **disable-connected-check**
 - **maximum-peers**
 - **update-source**
 - **ebgp-multihop**
- BFD マルチホップおよび次のコマンドは、IPv4 および IPv6 アドレス ファミリの IPv6 リンクローカルを介した BGP インターフェイス ピアリングではサポートされません。

- **bfd-multihop**
- **bfd multihop interval**
- **bfd multihop authentication**

- BGP では、ルートアドバタイズメントのコンバージェンス時間が短縮されます。ルートアドバタイズメント (RA) リンクレベル プロトコルの検出を高速化するには、IPv4 および IPv6 アドレス ファミリの IPv6 リンクローカル経由 BGP インターフェイス ピアリングを使用する各 IPv6 対応インターフェイスで次のコマンドを入力します。

```
interface Ethernet port/slot
ipv6 nd ra-interval 4 min 3
ipv6 nd ra-lifetime 10
```

- Cisco NX-OS リリース 10.3(3)F 以降、BGP パスワードのタイプ 6 暗号化は、次の制限付きで Cisco NX-OS スイッチでサポートされます。
 - タイプ 6 暗号化が構成されている場合、既存のタイプ 6 暗号化パスワードをタイプ 0/タイプ 3/タイプ 7 パスワードに変更することはできません。
 - タイプ 6 暗号化がサポートされていない古いイメージでコールドリブートによってシステムをダウングレードする場合は、タイプ 6 構成を削除して、それからコールドリブートを実行してください。そうしないと、構成が失われ、ネイバーの構成がなくなります。
 - プライマリ キーの設定は、スイッチに対してローカルです。あるスイッチからタイプ 6 に構成された実行データを取得し、別のプライマリ キーが構成されている別のスイッチに適用すると、新しいスイッチでの復号化は失敗します。
 - ISSU 中に、古いイメージ (タイプ 0/タイプ 3/タイプ 7 暗号化キーが構成に存在する) から新しいイメージ (タイプ 6 暗号化がサポートされている) に移行する場合、BGP は既存 **encryption re-encrypt obfuscated** のコマンドを使用して再暗号化が適用されるまで、または適用されない限り、タイプ 6 の暗号化に既存のキーを変換しません。
 - BGP タイプ 6 パスワードは、非 DME プラットフォームではサポートされません。
 - ネイバーまたはテンプレートのパスワードをプログラム (RESTCONF、NETCONF など) で設定する場合は、パスワードのタイプとパスワードを指定することを強くお勧めします。プログラム コールでいずれかのプロパティが欠落している場合、BGP は欠落しているプロパティのすでに使用可能な (またはデフォルトの) 値を使用して、ネイバーまたはテンプレートのパスワードを構成します。

ユーザーがプロパティを指定せずに構成する必要がある場合、ユーザーは両方のピアルータで同じ手順を実行する必要があります。

BGP のデフォルト設定

次の表に、BGP パラメータのデフォルト設定値を示します。

表 17: デフォルトの BGP パラメータ

パラメータ	デフォルト
BGP 機能	無効
キープアライブ インターバル	60 秒
ホールド タイマー	180 秒

高度な BGP の設定



(注) Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合がありますので注意してください。

インターフェイスでの IP 転送の有効化

RFC 5549 を使用するには、少なくとも 1 つの IPv4 アドレスを設定する必要があります。IPv4 アドレスを構成しない場合は、RFC 5549 を使用するよう IP 転送機能を有効にする必要があります。

手順の概要

1. **configure terminal**
2. **interface type slot/port**
3. **ip forward**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 type slot/port 例 : <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 3	ip forward 例 : <pre>switch(config-if)# ip forward switch(config-if)#</pre>	インターフェイスに IP アドレスが設定されていない場合でも、そのインターフェイスで IPv4 トラフィックを許可します。

例

次の例は、インターフェイスで IP 転送機能にを有効にする方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ip forward
```

BGP セッション テンプレートの設定

BGP セッション テンプレートを使用すると、類似した設定が必要な複数の BGP ピアで、BGP の設定を簡素化できます。BGP テンプレートによって、共通のコンフィギュレーション ブロックを再利用できます。先に BGP テンプレートを設定し、その後で BGP ピアにテンプレートを適用します。

BGP セッション テンプレートでは、継承、パスワード、タイマー、セキュリティなどのセッション属性を設定できます。

peer-session テンプレートは、別の peer-session テンプレートからの継承が可能です。第 3 のテンプレートから継承するように第 2 テンプレートを設定できます。さらに最初のテンプレートもこの第 3 のテンプレートから継承させることができます。この間接継承を続けることができる peer-session テンプレートの数は、最大 7 つです。

ネイバーに設定した属性は、ネイバーが BGP テンプレートから継承した属性よりも優先されます。

始める前に

BGP 機能を有効にしていることを確認します (BGP 機能のイネーブル化のセクションを参照してください)。

テンプレートを編集するときには、ピアまたはテンプレートのレベルで **no** 形式のコマンドを使用すると、テンプレートの設定を明示的に上書きできます。属性をデフォルトの状態にリセットするには、**default** 形式のコマンドを使用する必要があります。

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. **template peer-session** *template-name*
4. (任意) **password** *number password*
5. (任意) **timers** *keepalive hold*
6. **exit**
7. **neighbor** *ip-address remote-as as-number*
8. **inherit peer-session** *template-name*
9. (任意) **description** *text*
10. (任意) **show bgp peer-session** *template-name*
11. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router bgp <i>autonomous-system-number</i> 例 : <pre>switch(config)# router bgp 65536 switch(config-router)#</pre>	BGP を有効にして、ローカル BGP スピーカに自律システム番号を割り当てます。
ステップ 3	template peer-session <i>template-name</i> 例 : <pre>switch(config-router)# template peer-session BaseSession switch(config-router-stmp)#</pre>	peer-session テンプレート 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	(任意) password number password 例 : <pre>switch(config-router-stmp)# password 0 test</pre>	ネイバーにクリアテキストのパスワード「test」を追加します。パスワードは 3DES (タイプ 3 暗号形式) で保存および表示されます。
ステップ 5	(任意) timers keepalive hold 例 : <pre>switch(config-router-stmp)# timers 30 90</pre>	peer-session テンプレートに BGP キープアライブおよびホールドタイマー値を追加します。 デフォルトのキープアライブインターバルは 60 です。デフォルトのホールドタイムは 180 です。
ステップ 6	exit 例 : <pre>switch(config-router-stmp)# exit switch(config-router)#</pre>	peer-session テンプレート 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	neighbor ip-address remote-as as-number 例 : <pre>switch(config-router)# neighbor 192.168.1.2 remote-as 65536 switch(config-router-neighbor)#</pre>	BGP ルーティング用のネイバー コンフィギュレーション モードを開始し、ネイバー IP アドレスを設定します。
ステップ 8	inherit peer-session template-name 例 : <pre>switch(config-router-neighbor)# inherit peer-session BaseSession switch(config-router-neighbor)</pre>	ピアに peer-session テンプレートを適用します。
ステップ 9	(任意) description text 例 : <pre>switch(config-router-neighbor)# description Peer Router A switch(config-router-neighbor)</pre>	ネイバーの説明を追加します。
ステップ 10	(任意) show bgp peer-session template-name 例 : <pre>switch(config-router-neighbor)# show bgp peer-session BaseSession</pre>	peer-policy テンプレートを表示します。
ステップ 11	(任意) copy running-config startup-config 例 : <pre>switch(config-router-neighbor)# copy running-config startup-config</pre>	この設定変更を保存します。

例

show bgp neighbor コマンドを実行して、適用されたテンプレートを確認します。テンプレートで利用できるすべてのコマンドの詳細については、[Cisco Nexus 3000 シリーズ コマンド リファレンス](#)を参照してください。

BGP peer-session テンプレートを設定して、BGP ピアに適用する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# template peer-session BaseSession
switch(config-router-stmp)# timers 30 90
switch(config-router-stmp)# exit
switch(config-router)# neighbor 192.168.1.2 remote-as 65536
switch(config-router-neighbor)# inherit peer-session BaseSession
switch(config-router-neighbor)# description Peer Router A
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor)# copy running-config startup-config
```

BGP peer-policy テンプレートの設定

peer-policy テンプレートを設定すると、特定のアドレスファミリに対応する属性を定義できます。各 peer-policy テンプレートにプリファレンスを割り当て、指定した順序でテンプレートが継承されるようにします。ネイバー アドレス ファミリでは最大 5 つの peer-policy テンプレートを使用できます。

Cisco NX-OS は、プリファレンス値を使用して、アドレス ファミリの複数のピア ポリシーを評価します。プリファレンス値が最小のものが最初に評価されます。ネイバーに設定した属性は、ネイバーが BGP テンプレートから継承した属性よりも優先されます。

peer-policy テンプレートでは、AS-path フィルタリスト、プレフィックスリスト、ルートリフレクション、ソフト再構成など、アドレス ファミリ固有の属性を設定できます。

始める前に

BGP 機能を有効にしていることを確認します ([BGP 機能の有効化](#)のセクションを参照)。



- (注) テンプレートを編集するときには、ピアまたはテンプレートのレベルで **no** 形式のコマンドを使用すると、テンプレートの設定を明示的に上書きできます。属性をデフォルトの状態にリセットするには、**default** 形式のコマンドを使用する必要があります。

手順の概要

1. **configure terminal**
2. **router bgp autonomous-system-number**
3. **template peer-policy template-name**
4. (任意) **advertise-active-only**
5. (任意) **maximum-prefix number**

6. **exit**
7. **neighbor ip-address remote-as as-number**
8. **address-family { ipv4 | ipv6 } { multicast | unicast }**
9. **inherit peer-policy template-name preference**
10. (任意) **show bgp peer-policy template-name**
11. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	router bgp autonomous-system-number 例 : switch(config)# router bgp 65536 switch(config-router)#	BGP を有効にして、ローカル BGP スピーカに自律システム番号を割り当てます。
ステップ 3	template peer-policy template-name 例 : switch(config-router)# template peer-policy BasePolicy switch(config-router-ptmp)#	peer-policy テンプレートを作成します。
ステップ 4	(任意) advertise-active-only 例 : switch(config-router-ptmp)# advertise-active-only	アクティブ ルートのみをピアにアドバタイズします。
ステップ 5	(任意) maximum-prefix number 例 : switch(config-router-ptmp)# maximum-prefix 20	このピアに認めるプレフィックスの最大数を設定します。
ステップ 6	exit 例 : switch(config-router-ptmp)# exit switch(config-router)#	peer-policy テンプレート 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	neighbor ip-address remote-as as-number 例 : switch(config-router)# neighbor 192.168.1.2 remote-as 65536 switch(config-router-neighbor)#	BGP ルーティング用のネイバー設定モードを開始し、ネイバー 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 8	address-family { ipv4 ipv6 } { multicast unicast } 例 : <pre>switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#</pre>	指定されたアドレス ファミリに対応する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ます。
ステップ 9	inherit peer-policy template-name preference 例 : <pre>switch(config-router-neighbor-af)# inherit peer-policy BasePolicy 1</pre>	ピア アドレス ファミリ設定に peer-policy テンプレートを適用し、このピア ポリシーのプリファレンス値を割り当てます。
ステップ 10	(任意) show bgp peer-policy template-name 例 : <pre>switch(config-router-neighbor-af)# show bgp peer-policy BasePolicy</pre>	peer-policy テンプレートを表示します。
ステップ 11	(任意) copy running-config startup-config 例 : <pre>switch(config-router-neighbor-af)# copy running-config startup-config</pre>	この設定変更を保存します。

例

show bgp neighbor コマンドを実行して、適用されたテンプレートを確認します。テンプレートで利用できるすべてのコマンドの詳細については、[Cisco Nexus 3000 シリーズ コマンド リファレンス](#)を参照してください。

BGP peer-session テンプレートを設定して、BGP ピアに適用する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# template peer-session BasePolicy
switch(config-router-ptmp)# maximum-prefix 20
switch(config-router-ptmp)# exit
switch(config-router)# neighbor 192.168.1.1 remote-as 65536
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# inherit peer-policy BasePolicy
switch(config-router-neighbor-af)# copy running-config startup-config
```

BGP peer テンプレートの設定

BGP peer テンプレートを設定すると、1 つの再利用可能なコンフィギュレーションブロックで、セッション属性とポリシー属性を結合することができます。peer テンプレートも、peer-session または peer-policy テンプレートを継承できます。ネイバーに設定した属性は、ネイバーが BGP テンプレートから継承した属性よりも優先されます。ネイバーに設定できる peer テンプレートは1つだけですが、peer テンプレートは peer-session および peer-policy テンプレートを継承できます。

peer テンプレートは、eBGP マルチホップ TTL、最大プレフィックス数、ネクストホップセルフ、タイマーなど、セッション属性およびアドレス ファミリ属性をサポートします。

始める前に

BGP 機能を有効にしていることを確認します (BGP 機能のイネーブル化のセクションを参照してください)。



(注) テンプレートを編集するときには、ピアまたはテンプレートのレベルで **no** 形式のコマンドを使用すると、テンプレートの設定を明示的に上書きできます。属性をデフォルトの状態にリセットするには、**default** 形式のコマンドを使用する必要があります。

手順の概要

- 1. **configure terminal**
- 2. **router bgp** *autonomous-system-number*
- 3. **template peer** *template-name*
- 4. (任意) **inherit peer-session** *template-name*
- 5. (任意) **address-family** { **ipv4** | **ipv6** } { **multicast** | **unicast** }
- 6. (任意) **inherit peer** *template-name*
- 7. **exit**
- 8. (任意) **timers** *keepalive hold*
- 9. **exit**
- 10. **neighbor** *ip-address* **remote-as** *as-number*
- 11. **inherit peer** *template-name*
- 12. (任意) **timers** *keepalive hold*
- 13. (任意) **show bgp peer-template** *template-name*
- 14. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	router bgp <i>autonomous-system-number</i> 例 : switch(config)# router bgp 65536	BGP モードを開始し、ローカル BGP スピーカに自律システム番号を割り当てます。

	コマンドまたはアクション	目的
ステップ 3	template peer <i>template-name</i> 例 : <pre>switch(config-router)# template peer BasePeer switch(config-router-neighbor)#</pre>	peer テンプレート コンフィギュレーション モードを開始します。
ステップ 4	(任意) inherit peer-session <i>template-name</i> 例 : <pre>switch(config-router-neighbor)# inherit peer-session BaseSession</pre>	peer テンプレートで peer-session テンプレートを継承します。
ステップ 5	(任意) address-family { ipv4 ipv6 } { multicast unicast } 例 : <pre>switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#</pre>	指定のアドレス ファミリに対しグローバルアドレスファミリ コンフィギュレーション モードを設定します。
ステップ 6	(任意) inherit peer <i>template-name</i> 例 : <pre>switch(config-router-neighbor-af)# inherit peer BasePolicy</pre>	ネイバー アドレス ファミリ 設定に peer-policy テンプレートを適用します。
ステップ 7	exit 例 : <pre>switch(config-router-neighbor-af)# exit switch(config-router-neighbor)#</pre>	BGP ネイバー アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 8	(任意) timers <i>keepalive hold</i> 例 : <pre>switch(config-router-neighbor)# timers 45 100</pre>	ピアに BGP タイマー値を追加します。 これらの値によって、peer-session テンプレート、BaseSession のタイマー値が上書きされます。
ステップ 9	exit 例 : <pre>switch(config-router-neighbor)# exit switch(config-router)#</pre>	BGP peer テンプレート コンフィギュレーション モードを終了します。
ステップ 10	neighbor <i>ip-address remote-as as-number</i> 例 : <pre>switch(config-router)# neighbor 192.168.1.2 remote-as 65536 switch(config-router-neighbor)#</pre>	BGP ルーティング用のネイバー設定モードを開始し、ネイバー IP アドレスを設定します。
ステップ 11	inherit peer <i>template-name</i> 例 : <pre>switch(config-router-neighbor)# inherit peer BasePeer</pre>	peer テンプレートを継承します。

	コマンドまたはアクション	目的
ステップ 12	(任意) timers keepalive hold 例 : <pre>switch(config-router-neighbor)# timers 60 120</pre>	このネイバーに BGP タイマー値を追加します。 これらの値によって、peer テンプレートおよび peer-session テンプレートのタイマー値が上書きされます。
ステップ 13	(任意) show bgp peer-template template-name 例 : <pre>switch(config-router-neighbor-af)# show bgp peer-template BasePeer</pre>	peer テンプレートを表示します。
ステップ 14	(任意) copy running-config startup-config 例 : <pre>switch(config-router-neighbor-af)# copy running-config startup-config</pre>	この設定変更を保存します。

例

show bgp neighbor コマンドを実行して、適用されたテンプレートを確認します。テンプレートで利用できるすべてのコマンドの詳細については、[Cisco Nexus 3600 シリーズ コマンド リファレンス](#)を参照してください。

BGP peer テンプレートを設定して、BGP ピアに適用する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# template peer BasePeer
switch(config-router-neighbor)# inherit peer-session BaseSession
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# inherit peer-policy BasePolicy 1
switch(config-router-neighbor-af)# exit
switch(config-router-neighbor)# exit
switch(config-router)# neighbor 192.168.1.2 remote-as 65536
switch(config-router-neighbor)# inherit peer BasePeer
switch(config-router-neighbor)# copy running-config startup-config
```

プレフィックス ピアリングの設定

BGP では、IPv4 と IPv6 の両方のプレフィックスを使用してピアセットを定義できます。この機能を使用すると、各ネイバーを設定に追加する必要がありません。

プレフィックス ピアリングを定義する場合は、プレフィックスとともにリモート AS 番号を指定する必要があります。プレフィックス ピアリングが設定されている許容最大ピア数を超えない場合、BGP はプレフィックスおよび自律システムから接続するピアを受け付けます。

プレフィックス ピアリングに含まれている BGP ピアが切断されると、Cisco NX-OS は定義されているプレフィックス ピア タイムアウト値まで、ピア構造を維持します。この場合、その

プレフィックス ピアリングのすべてのスロットを他のピアが使い果たした結果、ブロックされるという危険性を伴わずに、確立されたピアのリセットまたは再接続が可能になります。

BGP プレフィックス ピアリングのタイムアウト値を構成するには、ルータ コンフィギュレーション モードで以下のコマンドを使用します。

コマンド	目的
timers prefix-peer-timeout value 例： <pre>switch(config-router)# timers prefix-peer-timeout 120</pre>	プレフィックス ピアのタイムアウト値を構成します。有効な範囲は 0 ～ 1200 秒です。デフォルト値は 30 です。 (注) プレフィックス ピアの場合は、プレフィックス ピア タイムアウトを、設定されたグレースフル リスタート タイマーよりも大きく設定します。プレフィックス ピア タイムアウトがグレースフル リスタート タイマーよりも大きければ、ピアのルートは再起動中に保持されます。プレフィックス ピア タイムアウトがグレースフル リスタート タイマーよりも小さいと、ピアのルートはプレフィックス ピアタイムアウトによって消去されます。これは、再起動が完了する前に発生する可能性があります。
timers prefix-peer-wait interval 例： <pre>switch(config-router)# timers prefix-peer-wait 50</pre>	VRF ごとまたはデフォルト VRF で BGP プレフィックス ピアリング 待機タイマーを構成します。timers prefix-peer-wait コマンドを使用して、ピアプレフィックスの待機時間を無効にし、BGP プレフィックスがルーティング情報ベース (RIB) に挿入されるまで遅延がないようにできます。 間隔の範囲は 0 ～ 1200 秒です。デフォルト値は 90 秒です。 (注) このタイマーは、BGP ダイナミック ネイバーにのみ適用されます。これは、BGP が再起動したとき、またはダイナミック BGP ネイバーで初めて起動するときのみ設定されます。

ピアの最大数を構成するには、ネイバー構成モードで以下のコマンドを使用します。

コマンド	目的
maximum-peers value 例： <pre>switch(config-router-neighbor)# maximum-peers 120</pre>	このプレフィックス ピアリングの最大ピア数を構成します。範囲は 1 ～ 1000 です。

最大 10 のピアを受け付けるプレフィックス ピアリングの設定例を示します。

```
switch(config)# router bgp 65536
switch(config-router)# timers prefix-peer-timeout 120
switch(config-router)# neighbor 10.100.200.0/24 remote-as 65536
switch(config-router-neighbor)# maximum-peers 10
```

```
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)#
```

次に、ピア プレフィックス待機時間を無効にする例を示します。

```
switch(config)# router bgp 100
switch(config-router)# timers prefix-peer-wait 50
switch(config-router)#
```

show ip bgp neighbors コマンドを使用すると、所定のプレフィックス ピアリングの構成の詳細とともに、現在受け付けられているインスタンスのリスト、アクティブ ピア数、最大同時ピア数、および受け付けたピアの合計数を表示できます。

IPv4 および IPv6 アドレス ファミリ向け IPv6 リンク ローカル経由の BGP インターフェイス ピアリングの設定

アンナナンバード インターフェイスを使用した自動 BGP ネイバー探索のために、IPv4 および IPv6 アドレス ファミリの IPv6 リンクローカルを経由して、BGP インターフェイス ピアリングを設定できます。これにより、インターフェイス名を（インターフェイススコープのアドレスではなく）BGP ピアとして使用する BGP セッションを設定できます。この機能は、ICMPv6 ネイバー探索（ND）のルート アドバタイズメント（RA）を使用して自動ネイバー探索を行い、RFC 5549 を使用して IPv6 ネクスト ホップで IPv4 ルートを送信します。

始める前に

BGP を有効にする必要があります。

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. **neighbor** *interface-name* **remote-as** {*as-number* | **route-map** *map-name*}
4. **inherit peer** *template-name*
5. （任意） **maximum-peers** *value*
6. **address-family** {*ipv4* | *ipv6*} **unicast**
7. （任意） **show bgp** {*ipv4* | *ipv6*} **unicast neighbors** *interface*
8. （任意） **show ip bgp neighbors** *interface-name*
9. （任意） **show ipv6 routers** [*interface interface*]
10. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal</pre>	コンフィギュレーション モードに入ります。
ステップ 2	router bgp autonomous-system-number 例 : <pre>switch(config)# router bgp 65535 switch(config-router)#</pre>	BGP を有効にして、ローカル BGP スピーカに自律システム番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。
ステップ 3	neighbor interface-name remote-as {as-number route-map map-name} 例 : <pre>switch(config-router)# neighbor Ethernet1/1 remote-as route-map Testmap switch(config-router-neighbor)#</pre>	BGP ルーティングのためにルータをネイバー設定モードにして、インターフェイスを BGP ピア用に設定します。 (注) 指定できるのは、イーサネット インターフェイス、ポートチャネル インターフェイス、サブインターフェイス、およびブレイクアウト インターフェイスだけです。 Cisco NX-OS リリース 9.3(6) 以降では、ルートマップを指定でき、AS リストを含められるルートマップを指定できます。ダイナミック AS 番号の使用の詳細については、プレフィックス ピアおよびインターフェイス ピアのダイナミック AS 番号 (265 ページ) を参照してください。 設定を複数のインターフェイスに適用する必要がある場合、<i>interface-name</i> は範囲にすることができます。
ステップ 4	inherit peer template-name 例 : <pre>switch(config-router-neighbor)# inherit peer PEER</pre>	peer テンプレートを継承します。
ステップ 5	(任意) maximum-peers value 例 : <pre>switch(config-router-neighbor)# maximum-peers 120</pre>	ネイバー設定モードのこのプレフィックス ピアリングの最大ピア数を設定します。範囲は 1 ～ 1000 です。 (注) 単一のインターフェイス ピアによって起動できるセッションのデフォルト数は 1 です。

	コマンドまたはアクション	目的
ステップ 6	address-family {ipv4 ipv6} unicast 例 : <pre>switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#</pre>	指定のアドレス ファミリーに対しグローバル アドレス ファミリー設定モードを開始します。
ステップ 7	(任意) show bgp {ipv4 ipv6} unicast neighbors interface 例 : <pre>switch(config-router-neighbor-af)# show bgp ipv4 unicast neighbors e1/25</pre> 例 : <pre>switch(config-router-neighbor-af)# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11</pre>	BGP ピアに関する情報を表示します。
ステップ 8	(任意) show ip bgp neighbors interface-name 例 : <pre>switch(config-router-neighbor-af)# show ip bgp neighbors Ethernet1/1</pre>	BGP ピアとして使用されるインターフェイスを表示します。
ステップ 9	(任意) show ipv6 routers [interface interface] 例 : <pre>switch(config-router-neighbor-af)# show ipv6 routers interface Ethernet1/1</pre>	IPv6 ICMP ルータ アドバタイズメントによって学習されたリモート IPv6 ルータのリンク ローカルアドレスを表示します。
ステップ 10	(任意) copy running-config startup-config 例 : <pre>switch(config-router-neighbor-af)# copy running-config startup-config</pre>	この設定変更を保存します。

例

この例は、ルート マップを使用して、IPv4 および IPv6 アドレス ファミリーの IPv6 リンク ローカル経由で、BGP インターフェイス ピアリングを設定する例を示します。

リーフ 1 の iBGP インターフェイス ピアリング設定 :

```
switch# configure terminal
switch(config)# route-map Testmap permit 10
switch(config-route-map)# match as-number 100-200, 300, 400
switch(config-route-map)# exit
switch(config)# router bgp 65000
switch(config-router)# neighbor Ethernet1/1 remote-as route-map Testmap
switch(config-router-neighbor)# inherit peer PEER
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor)# address-family ipv6 unicast
switch(config-router-neighbor-af)# copy running-config startup-config
```

次に、IPv4 および IPv6 アドレス ファミリーの IPv6 リンクローカル経由での、BGP インターフェイス ピアリングのサンプル出力例を示します。

```
switch(config-router-neighbor)# show bgp ipv4 unicast neighbors e1/15.1
BGP neighbor is fe80::2, remote AS 100, ibgp link, Peer index 4
Peer is an instance of interface peering Ethernet1/15.1
BGP version 4, remote router ID 5.5.5.5
Neighbor previous state = OpenConfirm
BGP state = Established, up for 2d16h
Neighbor vrf: default
Peer is directly attached, interface Ethernet1/15.1
Last read 00:00:54, hold time = 180, keepalive interval is 60 seconds
Last written 00:00:08, keepalive timer expiry due 00:00:51
Received 3869 messages, 0 notifications, 0 bytes in queue
Sent 3871 messages, 0 notifications, 0(0) bytes in queue
Enhanced error processing: On
0 discarded attributes
Connections established 2, dropped 1
Last reset by peer 2d16h, due to session closed
Last error length received: 0
Reset error value received 0
Reset error received major: 104 minor: 0
Notification data received:
Last reset by us never, due to No error
Last error length sent: 0
Reset error value sent: 0
Reset error sent major: 0 minor: 0
--More--
```

インターフェイス コンフィギュレーション：

次のいずれかのコマンドを使用して、対応するインターフェイスで IPv6 を有効にする必要があります。

- **ipv6 address *ipv6-address***
- **ipv6 address use-link-local-only**
- **ipv6 link-local *link-local-address***

```
switch# configure terminal
switch(config)# interface Ethernet1/1
switch(config-if)# ipv6 address use-link-local-only
```



- (注) インターフェイスで IPv4 アドレスが設定されていない場合は、**ip forward** コマンドをインターフェイスで設定して IPv4 転送を有効にする必要があります。



- (注) IPv6 ND タイマーを調整して、ネイバー探索を高速化し、BGP のルートコンバージェンスを高速化できます。

```
switch(config-if)# ipv6 nd ra-interval 4 min 3
switch(config-if)# ipv6 nd ra-lifetime 10
```



(注) Cisco NX-OS リリース 9.3(6) 以降で、パラレルリンクを使用するカスタマーの導入では、インターフェイスモードで次のコマンドを追加する必要があります。

```
switch(config-if)# ipv6 link-local use-bia
```

このコマンドは、異なるインターフェイス間での IPv6 LLA を一意にします。

BGP 認証の設定

MD5 ダイジェストを使用してピアからのルート更新を認証するように、BGP を設定できます。

または、Cisco NX-OS リリース 10.4(2)F 以降では、TCP 認証オプション (TCP AO) を使用してピアからのルートアップデートを認証するように BGP を構成できます。

Cisco NX-OS リリース 10.3(3)F 以降では、BGP パスワードのタイプ 6 暗号化が Cisco NX-OS スイッチでサポートされています。次の暗号化タイプがサポートされています。

- AES ベースの暗号化
- 秘密の暗号化と復号には、プライマリキーと呼ばれる構成可能な暗号キーが使用されます。

MD5 ダイジェストまたは TCP AO を使用するように BGP を構成するには、ネイバー 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。

始める前に

- プライマリキーが Cisco NX-OS スイッチで **key config-key ascii <primary_key>** コマンドを使用して構成されていることを確認します。
- タイプ 6 暗号化を適切に機能させるには、Cisco NX-OS スイッチで **feature password encryption aes** が有効になっていることを確認します。
- BGP ネイバーセッション認証に TCP キーチェーン認証オプションを構成して使用するには、「TCP 認証オプションの構成」を参照してください。<https://www.cisco.com/content/en/us/td/docs/dcn/nx-os/nexus9000/104x/configuration/security/cisco-nexus-9000-series-nx-os-security-configuration-guide-release-104x/chapter.html>

手順の概要

1. **key config-key ascii <primary_key>**
2. **configure terminal**
3. **feature password encryption aes**
4. **router bgp** AS 番号
5. **template peer** テンプレート名
6. **password {0 | 3 | 7 | 6} string**
7. (任意) **encryption re-encrypt obfuscated**

- ## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	key config-key ascii <primary_key> 例： switch# key config-key ascii 0123456789012345	プライマリキーを構成します。 (注) - このコマンドは、プライマリ キーが構成されていない場合にのみ入力します。 - プライマリ キーがすでに構成されている場合にこのコマンドを入力すると、実際には既存のプライマリ キー値が変更されます。新しい値に変更するには、プロンプトが表示されたら既存のプライマリ キー値を入力します。
ステップ 2	configure terminal 例： switch# 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	feature password encryption aes 例： switch(config)# feature password encryption aes	AES パスワード暗号化を有効にします。
ステップ 4	router bgp AS 番号 例： switch(config-router)# router bgp 1	BGP ルータ モードを開始します。
ステップ 5	template peer テンプレート名 例： switch(config-router-neighbor)# template peer abc	BGP ネイバー モードを開始します。
ステップ 6	password {0 3 7 6} string 例： switch(config-router-neighbor)# password 6 Jk5L8Zn7WvYQ2c3mQz1ZnkRPNjy6GynJrHwscQdEP0r8DQiscXVTCF=	MGP ネイバー セッションの MD5 パスワードを設定します。 (注) タイプ 0/タイプ 3/タイプ 7 を新しく構成する場合、プライマリ キーが構成されていて feature password encryption aes が有効になっている場合、タイプ

	コマンドまたはアクション	目的
		0/3/7 はタイプ 6 パスワードに自動的に暗号化されます。
ステップ 7	(任意) encryption re-encrypt obfuscated 例 : switch# encryption re-encrypt obfuscated	既存のタイプ 0/タイプ 3/タイプ 7 パスワードをタイプ 6 パスワードに暗号化します。
ステップ 8	(任意) encryption delete type-6 例 : switch# encryption delete type-6	タイプ 6 暗号化パスワードを削除します。
ステップ 9	(任意) ao <Keychain-name> [include-tcp-options]	パケットの MAC ダイジェストの計算中に TCP オプション ヘッダー (TCP AO オプション以外) を含めるかどうかを指定するオプションを構成します。

BGP セッションのリセット

BGP のルート ポリシーを変更した場合は、関連付けられた BGP ピアセッションをリセットする必要があります。BGP ピアがルート リフレッシュをサポートしない場合は、着信ポリシー変更に関するソフト再構成を設定できます。Cisco NX-OS は自動的に、セッションのソフトリセットを試みます。

ソフト再構成着信を設定するには、ネイバー アドレス ファミリ設定モードで次のコマンドを使用します。

コマンド	目的
soft-reconfiguration inbound always 例 : switch(config-router-neighbor-af)# soft-reconfiguration inbound always	着信 BGP ルート アップデートを格納するために、ソフト再構成をイネーブルにします。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。

BGP ネイバー セッションをリセットするには、任意のモードで次のコマンドを使用します。

コマンド	目的
clear bgp ip { unicast multicast } ip-address soft { in out } 例 : switch# clear bgp ip unicast 192.0.2.1 soft in	TCP セッションを切断しないで、BGP セッションをリセットします。

ネクストホップアドレスの変更

次の方法で、ルートアドバタイズメントで使用するネクストホップアドレスを変更できます。

- ネクストホップ計算をディセーブルにして、ローカル BGP スピーカ アドレスをネクストホップ アドレスとして使用します。
- ネクストホップ アドレスをサードパーティ アドレスとして設定します。この機能は、元のネクスト ホップ アドレスがルートの送り先のピアと同じサブネット上にある場合に使用します。この機能を使用すると、フォワーディング時に余分なホップを節約できます。

ネクストホップアドレスを変更するには、コマンドアドレス ファミリ コンフィギュレーション モードで次のパラメータを使用します。

コマンド	目的
next-hop-self 例 : <pre>switch(config-router-neighbor-af) # next-hop-self</pre>	ルートアップデートのネクストホップアドレスとして、ローカル BGP スピーカ アドレスを使用します。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。
next-hop-third-party 例 : <pre>switch(config-router-neighbor-af) # next-hop-third-party</pre>	ネクストホップ アドレスをサードパーティ アドレスとして設定します。このコマンドは、 next-hop-self を構成されていないシングルホップEBGP ピアに使用します。

BGP ネクスト ホップ アドレス トラッキングの設定

BGP ネクスト ホップ アドレス トラッキングはデフォルトで有効であり、無効にすることができません。

BGP ネクスト ホップ トラッキングのパフォーマンスを向上するために、RIB チェック間の遅延インターバルを変更できます。BGP ネクストホップの到達可能性に影響を及ぼすルートのクリティカル タイマーを設定したり、BGP テーブルのその他のルートすべての非クリティカル タイマーを設定したりできます。

BGP ネクストホップアドレス トラッキングを変更するには、アドレスファミリ 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
nexthop trigger-delay {critical non-critical } milliseconds 例 : <pre>switch(config-router-af) # nexthop trigger-delay critical 5000</pre>	クリティカルなネクスト ホップの到達可能性ルートおよび非クリティカルなルートについて、ネクストホップ アドレス トラッキングの遅延タイマーを指定します。指定できる範囲は1～4294967295 ミリ秒です。クリティカル タイマーのデフォルトは3000です。非クリティカル タイマーのデフォルトは 10000 です。

コマンド	目的
nexthop route-map name 例 : <pre>switch(config-router-af)# nexthop route-map nextHopLimits</pre>	BGP ネクストホップアドレスが一致するルートマップを指定します。63 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。

ネクストホップフィルタリングの設定

BGP ネクストホップフィルタリングを使用すると、RIB でネクストホップアドレスがチェックされるときにそのネクストホップアドレスの基盤となるルートがルートマップを経由します。ルートマップでそのルートが拒否されると、ネクストホップアドレスは到達不能として扱われます。

BGP は、ルートポリシーによって拒否されたすべてのネクストホップを無効であるとマークし、無効なネクストホップアドレスを使用するルートについてベストパスを計算しません。

BGP ネクストホップフィルタリングを設定するには、アドレスファミリ 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
nexthop route-map name 例 : <pre>switch(config-router-af)# nexthop route-map nextHopLimits</pre>	BGP ネクストホップルートが一致するルートマップを指定します。63 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。

ネクストホップセルフによるリフレクトルートの制御

NX-OS では、**next-hop-self [all]** 引数を使用して特定のピアに送信する際の iBGP ルートを制御できます。これらの引数を使用すると、ルートのリフレクトが実施されている場合でも、ルートのネクストホップを選択的に変更できます。

コマンド	目的
next-hop-self [all] 例 : <pre>switch(config-router-af)# next-hop-self all</pre>	ルートアップデートのネクストホップアドレスとして、ローカル BGP スピーカアドレスを使用します。 all キーワードはオプションです。 all を指定すると、すべてのルートが next-hop-self を使用するピアに送信されます。 all を指定しなかった場合、リフレクトしたルートのネクストホップは変更されません。

セッションがダウンした場合のネクストホップグループの縮小

セッションがダウンしたときに迅速な方法で ECMP グループを縮小するように BGP を設定できます。

この機能は、次の BGP パス障害イベントに適用されます。

- 1 つまたは複数のレイヤ 3 リンクの障害
- BGP ネイバーの BFD 障害検出
- BGP ネイバーの管理上のシャットダウン (shutdown コマンドを使用)

レイヤ 3 リンク障害の迅速な処理はデフォルトで有効になっており、有効にするための構成コマンドは必要ありません。

最後の 2 つのイベントの迅速な処理を構成するには、ルータ構成モードで次のコマンドを使用します。

コマンド	目的
neighbor-down fib-accelerate 例 : <pre>switch(config-router)# neighbor-down fib-accelerate</pre>	BGP セッションがダウンするたびに、すべてのネクストホップグループ (ECMP グループと単一のネクストホップルート) から対応する次のネクストホップを取り消します。 (注) このコマンドは、IPv4 と IPv6 の両方のアドレスファミリルートに適用され、すべての非直接ルートが BGP によってインストールされる BGP 専用環境でのみサポートされます。

機能ネゴシエーションのディセーブル化

機能ネゴシエーションをディセーブルにすると、機能ネゴシエーションをサポートしない古い BGP ピアとの相互運用が可能です。

機能ネゴシエーションをディセーブルにするには、ネイバー 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
dont-capability-negotiate 例 : <pre>switch(config-router-neighbor)# dont-capability-negotiate</pre>	機能ネゴシエーションをディセーブルにします。このコマンドの設定後、BGP セッションを手動でリセットする必要があります。

BGP 追加パスの設定

GP は、プレフィックスごとの複数パスの送受信と、このパスのアドバタイジングをサポートします。

追加パスの送受信機能のアドバタイズ

BGP ピア間の追加パスの送受信機能を実装するように BGP を設定できます。これを行うには、ネイバー アドレス ファミリ設定モードで次のコマンドを使用します。

手順の概要

1. `[no] capability additional-paths send [disable]`
2. `[no] capability additional-paths receive [disable]`
3. `show bgp neighbor`

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	<code>[no] capability additional-paths send [disable]</code> 例 : <pre>switch(config-router-neighbor-af) # capability additional-paths send</pre>	BGP ピアに追加パスを送信する機能をアドバタイズします。 disable オプションは、追加パス送信機能のアドバタイズをディセーブルにします。 このコマンドの no 形式を使用すると、追加パスの送信機能がディセーブルになります。
ステップ 2	<code>[no] capability additional-paths receive [disable]</code> 例 : <pre>switch(config-router-neighbor-af) # capability additional-paths receive</pre>	BGP ピアから追加パスを受信する機能をアドバタイズします。 disable オプションは、追加パス受信機能のアドバタイズをディセーブルにします。 このコマンドの no 形式は、追加パスの受信機能をディセーブルにします。
ステップ 3	<code>show bgp neighbor</code> 例 : <pre>switch(config-router-neighbor-af) # show bgp neighbor</pre>	ローカル ピアがリモート ピアへの追加パス送受信機能をアドバタイズしたかを表示します。

例

BGP ピアに追加のパスを送受信する機能をアドバタイズする BGP の設定例を示します。

```
switch# configure terminal
switch(config)# router bgp 100
```

```
switch(config-router)# neighbor 10.131.31.2 remote-as 100
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# capability additional-paths send
switch(config-router-neighbor-af)# capability additional-paths receive
```

追加パスの送受信の設定

BGP ピア間の追加パスの送受信機能を設定できます。これを行うには、アドレス ファミリ設定モードで次のコマンドを使用します。

手順の概要

1. **[no] additional-paths send**
2. **[no] additional-paths receive**
3. **show bgp neighbor**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	[no] additional-paths send 例 : <pre>switch(config-router-af)# additional-paths send</pre>	機能が無効になっていないこのアドレス ファミリで、すべてのネイバーの追加パスの送信機能を有効にします。 このコマンドの no 形式を使用すると、送信機能が無効になります。
ステップ 2	[no] additional-paths receive 例 : <pre>switch(config-router-af)# additional-paths receive</pre>	機能が無効になっていないこのアドレス ファミリで、すべてのネイバーの追加パスの受信機能を有効にします。 このコマンドの no 形式を使用すると、受信機能が無効になります。
ステップ 3	show bgp neighbor 例 : <pre>switch(config-router-af)# show bgp neighbor</pre>	ローカル ピアがリモート ピアへの追加パス送受信機能をアダプタイズしたものとして表示します。

例

機能が無効になっていない指定されたアドレス ファミリで、すべてのネイバーの追加パスの受信機能を有効にする例を示します。

```
switch# configure terminal
switch(config)# router bgp 100
switch(config-router)# address-family ipv4 unicast
```

```
switch(config-router-af)# additional-paths send
switch(config-router-af)# additional-paths receive
```

アドバタイズされるパスの設定

BGP にアドバタイズされたパスを指定できます。これを行うには、ルートマップ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. **[no] set ip next-hop unchanged**
2. **[no] set path-selection { all | backup | best2 | multipaths } | advertise**
3. **show bgp { ipv4 | ipv6 } unicast [ip-address | ipv6-prefix] [vrf vrf-name]**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	[no] set ip next-hop unchanged 例 : <pre>switch(config-route-map)# set ip next-hop unchanged</pre>	不変のネクストホップ IP アドレスを指定します。
ステップ 2	[no] set path-selection { all backup best2 multipaths } advertise 例 : <pre>switch(config-route-map)# set path-selection all advertise</pre>	すべてのパスが指定されたプレフィックスにアドバタイズされるように指定します。次のいずれかのオプションを選択できます。 • all : 使用可能なすべての有効なパスをアドバタイズします。 • backup : バックアップパスとしてマークされたパスをアドバタイズします。このオプションでは、additional-path install backup コマンドを使用してバックアップパスを有効にする必要があります。 • best2 : 2 番目に最適なパスをアドバタイズします。これは、すでに計算されているベストパスを除き、残りの使用可能なパスのベストパスです。 • multipaths : すべてのマルチパスをアドバタイズします。このオプションでは、maximum-paths コマンドを使用してマルチパスを有効にする必要があります。 (注)

	コマンドまたはアクション	目的
		マルチパスがない場合、backup オプションと best2 オプションは同じです。マルチパスがある場合、best2 はマルチパスのリストの最初のパスで、バックアップは計算されたベストパスとマルチパスを除くすべての使用可能なパスのベストパスです。 このコマンドの no 形式は、最適パスだけがアドバタイズされるように指定します。
ステップ 3	show bgp {ipv4 ipv6} unicast [ip-address ipv6-prefix] [vrf vrf-name] 例 : <pre>switch(config-route-map)# show bgp ipv4 unicast</pre>	プレフィックスの追加パスのパス ID とこれらのパスのアドバタイズメント情報を表示します。

例

すべてのパスがプレフィックス リスト p1 にアドバタイズされるよう指定する例を示します。

```
switch# configure terminal
switch(config)# route-map PATH_SELECTION_RMAP
switch(config-route-map)# match ip address prefix-list p1
switch(config-route-map)# set path-selection all advertise
```

追加パス選択の設定

プレフィックスに追加のパスを選択する機能を設定できます。これを行うには、アドレスファミリー 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. **[no] additional-paths selection route-map map-name**
2. **{|} [ip-address | ipv6-prefix] [vrf-name] show bgpipv4ipv6unicastvrf**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	[no] additional-paths selection route-map map-name 例 : <pre>switch(config-router-af)# additional paths selection route-map map1</pre>	プレフィックスに追加のパスを選択する機能を設定します。 このコマンドの no 形式は、追加パス選択機能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 2	<pre>{ } [ip-address ipv6-prefix] [vrf-name] show bgpipv4ipv6unicastvrf</pre> 例 : <pre>switch(config-route-af) # show bgp ipv4 unicast</pre>	プレフィックスの追加パスのパス ID とこれらのパスのアドバタイズメント情報を表示します。

例

指定されたアドレス ファミリで追加パス選択を設定する例を示します。

```
switch# configure terminal
switch(config)# router bgp 100
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# additional-paths selection route-map PATH_SELECTION_RMAP
```

eBGP の設定

このセクションは、次のトピックで構成されています。

eBGP ネクストホップ変更なしの構成

ネクスト ホップ アドレスを変更せずに eBGP マルチホップ ピアにルートを送信するように eBGP を設定できます。デフォルトでは、デバイスはルートの送信時に BGP ルートのネクスト ホップアドレスを自身のアドレスに変更します。

	コマンド	目的
ステップ 1	disable-connected-check 例 : <pre>switch(config-router-neighbor) # disable-connected-check</pre>	シングルホップ eBGP ピアが直接接続されているかどうかのチェックを無効にします。このコマンドの使用後、BGP セッションを手動でリセットする必要があります。
ステップ 2	configure terminal 例 : <pre>switch# configure terminal</pre>	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 route-map name 例 : <pre>switch(config) # route-map route</pre>	ルート マップ 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	set ip next-hop unchanged 例 : <pre>switch(config-route-map) # set ip next-hop unchanged</pre>	ネクスト ホップ アドレスを変更せずに指定された eBGP ピアに BGP アップデートを送信するようにデバイスを構成します。

	コマンド	目的
ステップ 5	exit 例 : switch(config-route-map)# exit	ルート マップ コンフィギュレーション モードを終了します。

次に、eBGP ネクスト ホップを変更せずに設定し、ネクスト ホップ アドレスを変更せずにルートを送信する例を示します。

```
switch# configure terminal
switch(config)# route-map route
switch(config-route-map)# set ip next-hop unchanged
switch(config-route-map)# exit
switch(config)#
```

eBGP シングルホップ チェックの無効化

シングルホップ eBGP ピアがローカルルータに直接接続されているかどうかのチェック機能を無効にするように、eBGP を設定できます。このオプションは、直接接続されたスイッチ間のシングルホップ ループバック eBGP セッションの設定に使用します。

シングルホップ eBGP ピアが直接接続されているかどうかのチェックを無効にするには、ネイバー設定モードで次のコマンドを使用します。

コマンド	目的
disable-connected-check 例 : switch(config-router-neighbor)# disable-connected-check	シングルホップ eBGP ピアが直接接続されているかどうかのチェックを無効にします。このコマンドの使用後、BGP セッションを手動でリセットする必要があります。

eBGP マルチホップの設定

eBGP マルチホップをサポートする eBGP 存続可能時間 (TTL) 値を設定できます。eBGP ピアは状況によって、別の eBGP ピアに直接接続されず、リモート eBGP ピアに到達するために複数のホップを必要とします。ネイバーセッションに eBGP TTL 値を設定すると、このようなマルチホップセッションが可能になります。

eBGP マルチホップを設定するには、ネイバー 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
ebgp-multihop ttl-value 例 : switch(config-router-neighbor)# ebgp-multihop 5	eBGP マルチホップの eBGP TTL を設定します。有効な範囲は2～255です。このコマンドの使用後、BGP セッションを手動でリセットする必要があります。

同じ自律システムで eBGP ルートの構成

リモート自律システム (AS) から学習した eBGP ルートを、同じ AS 内の別の eBGP ピアにアドバタイズするように構成できます。



(注) 同じ AS 番号内のピア間でルート更新が送信される場合、**allowas-in** コマンドを入力しない限り、これらの更新は破棄されます。

AS ピア チェックを無効にするには、ネイバー 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
ステップ 1	router bgp autonomous-system-number 例 : <code>switch(config)# router bgp 64496</code>	BGP を有効にして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。
ステップ 2	neighbor ipv4 remote-as as-number 例 : <code>switch (config-router)# neighbor 209.165.201.1 remote-as 64497</code>	リモート BGP ピアの指定アドレス タイプと AS 番号を構成します。ip-address の形式は x.x.x.x です。IPv6 address-format の形式は A:B::C:D です。
ステップ 3	address family ipv4 unicast 例 : <code>switch(config-router)# address family ip4 unicast</code>	ユニキャスト指定のアドレスファミリーに対応したネイバーアドレスファミリー構成モードを開始します。
ステップ 4	disable-peer-as-check 例 : <code>switch(config-router-neighbor-af)# disable-peer-as-check</code>	同じ AS 内のピア間でルートが更新されるように、AS チェックを無効にします。
ステップ 5	show bgp neighbor 例 : <code>switch(config-router-neighbor-af)# show bgp ipv4 unicast neighbors</code>	BGP ピアに関する情報を表示します。

次に、BGP ピア情報を表示する例を示します。

```
switch(config)# show bgp neighbor 1.222.222.2
bgp neighbor is 1.222.222.2, remote as 2222, ebgp link, peer index 1
bgp version 4, remote router id1.100.1.2 ####output truncated####
for address family:ipv4 unicast
bgp table version 54, neighbor version 54
3 accepted paths consume 108 bytes of memory
```

```
10 sent paths
peer asn check is disabled

#####output omitted#####
```

高速外部フェールオーバーのディセーブル化

通常、BGP ルータと直接接続 eBGP ピア間の接続が失われると、ピアとの eBGP セッションをリセットすることによって、BGP が高速外部フェールオーバーを開始します。この高速外部フェールオーバーをディセーブルにすると、リンク フラップが原因の不安定さを制限できます。

高速外部フェールオーバーを無効にするには、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
no fast-external-fallover 例 : switch(config-router)# no fast-external-fallover	eBGP ピアの高速外部フェールオーバーをディセーブルにします。このコマンドは、デフォルトでイネーブルになっています。

AS パス属性の制限

AS パス属性で自律システム番号が高いルートを廃棄するように eBGP を設定できます。

AS パス属性で AS 番号の多いルートを廃棄するには、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
maxas-limit number 例 : switch(config-router)# maxas-limit 50	AS パス セグメントの番号が指定された上限を超えている eBGP ルートを廃棄します。範囲は 1 ～ 2000 です。

ローカル AS サポートの設定

ローカル AS 機能では、ルータが実際の AS に加えて、2 番目の自律システム (AS) のメンバーであるように見せることができます。ローカル AS を使用すると、ピアリングの調整を変更せずに 2 つの ISP をマージできます。マージされた ISP 内のルータは、新しい自律システムのメンバになりますが、使用者に対しては古い自律システム番号を使用し続けます。

ローカル AS は正しい eBGP ピアにしか使用できません。別のコンフェデレーションのサブ自律システムのメンバである 2 ピアに対しては、この機能は使用できません。

eBGP ローカル AS のサポートを設定するには、ネイバー 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
local-as number [no-prepend [replace-as [dual-as]]] 例 : <pre>switch(config-router-neighbor) # local-as 1.1</pre>	AS_PATH 属性にローカル AS の <i>number</i> を付加するよう eBGP を設定します。 local-as number としては 16 ビット整数または 32 ビット整数が可能です。32 ビットの場合、上位 16 ビット 10 進数と下位 16 ビット 10 進数による <i>xx.xx</i> という形式にします。 no-prepend キーワードは、local-as number とピアリングしているパートナーを除き、local-asnumber がダウンストリーム BGP ネイバーの前に付加されないようにします。 replace-as キーワードは、ピアリングセッションの local-as number だけが AS_PATH 属性の前に付加されるようにします。ローカル BGP ルーティングプロセスからの自律システム番号は、プリペンドされません。 dual-as キーワードは、eBGP ネイバーを構成し、実際の自律システム番号（ローカルの BGP ルーティングプロセスからのもの）またはローカル AS として構成された自律システム番号を使用して、ピアリングセッションを確立するようにします。

AS 連合の設定

AS 連合を設定するには、連合識別情報を指定する必要があります。AS 連合内の自律システムグループは、自律システム番号として連合 ID を持つ、1 つの自律システムとして認識されます。

BGP 連合 ID 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。

コマンド	目的
confederation identifier as-number 例 : <pre>switch(config-router) # confederation identifier 64512</pre>	AS 連合を表す連合 ID を設定します。 各連合には別のサブ自律システム番号があり、通常は専用番号です（64512 ～ 65534）。 このコマンドによって、BGP ネイバー セッションの自動通知およびセッションリセットが開始されます。

AS 連合に所属する自律システムを設定するには、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。

コマンド	目的
bgp confederation peers as-number [as-number2...] 例 : <pre>switch(config-router)# bgp confederation peers 5 33 44</pre>	連合に所属する自律システムのリストを指定します。 このコマンドによって、BGP ネイバーセッションの自動通知およびセッションリセットが開始されます。

BGP 向け BFD の構成例

この例は、個々の BGP ネイバーの BFD をイネーブルにする方法を示します。

```
router bgp 400
  router-id 2.2.2.2
  neighbor 172.16.2.3
    bfd
    remote-as 400
    update-source Vlan1002
    address-family ipv4 unicast
```

この例は、BGP プレフィックス ピアの BFD をイネーブルにする方法を示します。

```
router bgp 400
  router-id 1.1.1.1
  neighbor 172.16.2.0/24
    bfd
    remote-as 400
    update-source Vlan1002
    address-family ipv4 unicast
```

BGP 属性フィルタリングの設定とエラー処理

Cisco NX-OS リリース 9.3(3) 以降では、BGP属性フィルタリングとエラー処理を設定して、セキュリティレベルを向上させることができます。次の機能を利用でき、次の順序で実装されます。

- **パス属性 treat-as-withdraw:** アップデートに指定した属性タイプが含まれている場合に、指定したネイバーから受け取った BGP アップデートを **treat-as-withdraw** とすることを許可します。アップデートに含まれるプレフィックスは、ルーティングテーブルから削除されます。
- **パス属性 discard:** BGP アップデートの特定のパス属性を特定のネイバーから削除できます。
- **拡張属性エラー処理:** 形式が誤っているアップデートに起因するピアセッションのフラッピングを防止します。

属性タイプ 1、2、3、4、8、14、15、16 は、パス属性 `treat-as-withdraw` とパス属性 `discard` に対して設定できません。属性タイプ 9 (Originator)、タイプ 10 (Cluster-id) は、eBGP ネイバーでのみ設定できます。

BGP 更新メッセージからのパス属性の取り消しとしての処理

特定のパス属性を含む BGP 更新を「扱うように」処理するには、ルータネイバー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

	コマンドまたはアクション	目的
ステップ 1	[no] path-attribute treat-as-withdraw [value range start end] in 例 : <pre>switch#(config-router)# neighbor 10.20.30.40 switch(config-router-neighbor)# path-attribute treat-as-withdraw 100 in</pre> 例 : <pre>switch#(config-router)# neighbor 10.20.30.40 switch(config-router-neighbor)# path-attribute treat-as-withdraw range 21 255 in</pre>	指定されたパス属性またはパス属性の範囲を含む着信 BGP 更新メッセージをすべて取り消すものとして扱い、ルーティングテーブルが最新であることを確認するために着信ルートリフレッシュをトリガーします。<code>treat-as-withdraw</code> である BGP 更新のプレフィックスは、BGP ルーティングテーブルから削除されます。 このコマンドは、BGP テンプレートピアおよび BGP テンプレートピアセッションでもサポートされます。

BGP 更新メッセージからのパス属性の破棄

特定のパス属性を含む BGP アップデートを廃棄するには、ルータ ネイバー 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

	コマンドまたはアクション	目的
ステップ 1	[no] path-attribute discard [value range start end] in 例 : <pre>switch#(config-router)# neighbor 10.20.30.40 switch(config-router-neighbor)# path-attribute discard 100 in</pre> 例 : <pre>switch#(config-router)# neighbor 10.20.30.40 switch(config-router-neighbor)# path-attribute discard range 100 255 in</pre>	指定されたネイバーの BGP アップデート メッセージ内の指定されたパス属性をドロップし、ルーティングテーブルが最新であることを確認するために着信ルートリフレッシュをトリガーします。特定の属性または不要な属性の範囲全体を設定できます。 このコマンドは、BGP テンプレートピアおよび BGP テンプレートピアセッションでもサポートされます。 (注)

	コマンドまたはアクション	目的
		discard と treat-as-withdraw の両方に同じパス属性が設定されている場合、treat-as-withdraw の優先順位が高くなります。

拡張属性エラー処理のイネーブル化またはディセーブル化

BGP 拡張属性エラー処理はデフォルトで有効になっていますが、無効にすることもできます。この機能は、RFC 7606 に準拠しており、不正な更新によるピアセッションのフラッピングを防止します。デフォルトの動作は、eBGP ピアと iBGP ピアの両方に適用されます。

拡張エラー処理を無効または再度有効にするには、ルータ設定モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	[no] enhanced-error 例： switch(config)# router bgp 1000 switch(config-router)# enhanced-error	BGP 拡張属性エラー処理をイネーブルまたはディセーブルにします。

取り消されたパス属性または破棄されたパス属性の表示

廃棄または不明なパス属性に関する情報を表示するには、次のいずれかのタスクを実行します。

コマンド	目的
show bgp {ipv4 ipv6} unicast path-attribute discard]	属性が破棄されたすべてのプレフィックスを表示します。
show bgp {ipv4 ipv6} unicast path-attribute unknown]	不明な属性を持つすべてのプレフィックスを表示します。
show bgp {ipv4 ipv6} unicast ip-address	プレフィックスに関連付けられている不明な属性および破棄された属性を表示します。

次の例は、属性が廃棄されたプレフィックスを示しています。

```
switch# show bgp ipv4 unicast path-attribute discard
Network                Next Hop
1.1.1.1/32              20.1.1.1
1.1.1.2/32              20.1.1.1
```

```
1.1.1.3/32      20.1.1.1
```

次の例は、不明な属性を持つプレフィックスを示しています。

```
switch# show bgp ipv4 unicast path-attribute unknown
Network      Next Hop
2.2.2.2/32   20.1.1.1
2.2.2.3/32   20.1.1.1
```

次の例は、プレフィックスに関連付けられている不明な属性および破棄された属性を表示します。

```
switch# show bgp ipv4 unicast 2.2.2.2
BGP routing table entry for 2.2.2.2/32, version 6241
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1
  1000
    20.1.1.1 from 20.1.1.1 (20.1.1.1)
      Origin IGP, localpref 100, valid, external, best
      unknown transitive attribute: flag 0xE0 type 0x62 length 0x64
        value 0000 0000 0100 0000 0200 0000 0300 0000
              0400 0000 0500 0000 0600 0000 0700 0000
              0800 0000 0900 0000 0A00 0000 0B00 0000
              0C00 0000 0D00 0000 0E00 0000 0F00 0000
              1000 0000 1100 0000 1200 0000 1300 0000
              1400 0000 1500 0000 1600 0000 1700 0000
              1800 0000
      rx pathid: 0, tx pathid: 0x0
      Updated on Jul 20 2019 07:50:43 PST
```

独自の自律システムを含む自律システムパスの設定

独自の自律システムを含む自律システム（AS）パスを受け入れる機能を BGP でイネーブルにします。

始める前に

BGP 機能を有効にしていることを確認します（[BGP 機能のイネーブル化](#)のセクションを参照してください）。

手順の概要

1. **configure terminal**
2. **router bgp as-number**
3. **neighbor ip-address remote-as as-number**
4. **address-family { ipv4 | ipv6 } { multicast | unicast }**
5. **[no | default] allowas-in [allowas-in-cnt]**
6. **end**
7. （任意） **show running-config bgp**
8. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	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	router bgp <i>as-number</i>	BGP モードを開始し、ローカル BGP スピーカに自律システム番号を割り当てます。 <i>as-number</i> の値の範囲は 1 ～ 65535 です。
ステップ 3	neighbor <i>ip-address</i> remote-as <i>as-number</i>	BGP ルーティング用のネイバー コンフィギュレーション モードを開始し、ネイバー IP アドレスを設定します。
ステップ 4	address-family { ipv4 ipv6 } { multicast unicast }	指定のアドレス ファミリに対応するルータ 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 5	[no default] allowas-in [<i>allowas-in-cnt</i>]	BGP の allowas-in 機能をイネーブルにし、自律システム番号の発生回数を設定します。 allowas-in-cnt の場合、1 ～ 10 の整数を入力します。デフォルトでは、自律システム番号の発生回数は 3 に設定されます。
ステップ 6	end	ルータ アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 7	(任意) show running-config bgp	BGP の設定を表示します。
ステップ 8	copy running-config startup-config	リブートおよびリスタート時に実行構成をスタートアップ構成にコピーして、変更を継続的に保存します。

例

次に、BGP の **allowas-in** 機能を設定し、ユニキャスト IPv4 アドレス ファミリ用に設定する例を示します。

```
switch# configure terminal
switch(config)# router bgp 77
switch(config-router)# neighbor 6.20.1.1 remote-as 66
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# allowas-in 5
switch(config-router-neighbor-af)# end
```

ルートリフレクタの設定

ルートリフレクタとして動作するローカル BGP スピーカに対するルートリフレクタクライアントとして、iBGP ピアを設定できます。ルートリフレクタとそのクライアントがともにクラスタを形成します。クライアントからなるクラスタには通常、ルートリフレクタが1つ存在します。このような状況では、ルートリフレクタのルータ ID でクラスタを識別します。ネットワークの冗長性を高め、シングルポイント障害を回避するために、複数のルートリフレクタからなるクラスタを設定できます。クラスタ内のすべてのルートリフレクタは、同じ4バイトクラスタ ID で設定する必要があります。これは、ルートリフレクタが同じクラスタ内のルートリフレクタからのアップデートを認識できるようにするためです。

始める前に

BGP 機能を有効にしていることを確認します（[BGP 機能の有効化](#)のセクションを参照）。

手順の概要

1. **configure terminal**
2. **router bgp *as-number***
3. **cluster-id *cluster-id***
4. **address-family {*ipv4* | *ipv6*} { *unicast* | *multicast* }**
5. （任意） **client-to-client reflection**
6. **exit**
7. **neighbor *ip-address* remote-as *as-number***
8. **address-family { *ipv4* | *ipv6* } { *unicast* | *multicast* }**
9. **route-reflector-client**
10. （任意） **show bgp ip { *unicast* | *multicast* } neighbors**
11. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router bgp <i>as-number</i> 例 : <pre>switch(config)# router bgp 65536 switch(config-router)#</pre>	BGP モードを開始し、ローカル BGP スピーカに自律システム番号を割り当てます。

	コマンドまたはアクション	目的
ステップ 3	cluster-id cluster-id 例 : <pre>switch(config-router)# cluster-id 192.0.2.1</pre>	クラスタに対応するルート リフレクタの 1 つとして、ローカル ルータを設定します。クラスタを識別するクラスタ ID を指定します。このコマンドによって、BGP ネイバーセッションの自動ソフト クリアまたはリフレッシュが開始されます。
ステップ 4	address-family {ipv4 ipv6} { unicast multicast} 例 : <pre>switch(config-router)# address-family ipv4 unicast switch(config-router-af)#</pre>	指定のアドレス ファミリに対応するグローバル アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	(任意) client-to-client reflection 例 : <pre>switch(config-router-af)# client-to-client reflection</pre>	クライアント間のルート リフレクションを設定します。この機能は、デフォルトでイネーブルになっています。このコマンドによって、BGP ネイバーセッションの自動ソフト クリアまたはリフレッシュが開始されます。
ステップ 6	exit 例 : <pre>switch(config-router-neighbor)# exit switch(config-router)#</pre>	ルータ アドレス コンフィギュレーション モードを終了します。
ステップ 7	neighbor ip-address remote-as as-number 例 : <pre>switch(config-router)# neighbor 192.0.2.10 remote-as 65536 switch(config-router-neighbor)#</pre>	リモート BGP ピアの IP アドレスおよび AS 番号を設定します。
ステップ 8	address-family { ipv4 ipv6 } { unicast multicast } 例 : <pre>switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#</pre>	指定のアドレス ファミリに対応しネイバー 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 9	route-reflector-client 例 : <pre>switch(config-router-neighbor-af)# route-reflector-client</pre>	BGP ルート リフレクタとしてスイッチを設定し、そのクライアントとしてネイバーを設定します。このコマンドによって、BGP ネイバーセッションの自動通知およびセッション リセットが開始されます。
ステップ 10	(任意) show bgp ip { unicast multicast } neighbors 例 : <pre>switch(config-router-neighbor-af)# show bgp ip unicast neighbors</pre>	BGP ピアを表示します。

	コマンドまたはアクション	目的
ステップ 11	(任意) copy running-config startup-config 例 : <pre>switch(config-router-neighbor-af)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、ルート リフレクタとしてルータを設定し、クライアントとしてネイバーを 1 つ追加する例を示します。

```
switch(config)# router bgp 65536
switch(config-router)# neighbor 192.0.2.10 remote-as 65536
switch(config-router-neighbor)# address-family ip unicast
switch(config-router-neighbor-af)# route-reflector-client
switch(config-router-neighbor-af)# copy running-config startup-config
```

ルート ダンプニングの設定

iBGP ネットワーク上での eBGP ルート フラップの伝播を最小限に抑えるために、ルート ダンプニングを構成できます。

ルート ダンプニングを設定するには、アドレス ファミリまたは VRF アドレス ファミリ 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
dampening [{ <i>half-life reuse-limit suppress-limit max-suppress-time</i> route-map <i>map-name</i> }] 例 : <pre>switch(config-router-af)# dampening route-map bgpDamp</pre>	機能ネゴシエーションをディセーブルにします。パラメータ値は次のとおりです。 • half-life : 指定できる範囲は 1 ～ 45 です。 • reuse-limit : 指定できる範囲は 1 ～ 20000 です。 • suppress-limit : 指定できる範囲は 1 ～ 20000 です。 • max-suppress-time : 指定できる範囲は 1 ～ 255 です。

ロード シェアリングおよび ECMP の設定

等コスト マルチパス ロード バランシング用に BGP がルート テーブルに追加するパスの最大数を設定できます。

パスの最大数を設定するには、ルータ アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
maximum-paths [ibgp] maxpaths 例 : <pre>switch(config-router-af) # maximum-paths 12</pre>	ロードシェアリング用の等コストパスの最大数を設定します。指定できる範囲は1～16です。デフォルトは1です。

最大プレフィックス数の設定

BGP が BGP ピアから受け取ることのできるプレフィックスの最大数を設定できます。任意で、プレフィックス数がこの値を超えた場合に、BGP に警告メッセージを生成させる、またはピアとの BGP セッションを切断させることを設定できます。

BGP ピアに認めるプレフィックスの最大数を設定するには、ネイバー アドレス ファミリ 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
maximum-prefix maximum [threshold] [restart time warming-only] 例 : <pre>switch(config-router-neighbor-af) # maximum-prefix 12</pre>	ピアからのプレフィックスの最大数を設定します。パラメータの範囲は次のとおりです。 • maximum : 指定できる範囲は 1 ～ 300000 です。 • threshold : 指定できる範囲は 1 ～ 100 % です。デフォルトは 75% です。 • time : 指定できる範囲は 1 ～ 65535 分です。 このコマンドによって、プレフィックス限度を超えた場合に、BGP ネイバー セッションの自動通知およびセッションリセットが開始されます。

ダイナミック機能の設定

BGP ピアのダイナミック機能を設定できます。

ダイナミック機能を設定するには、ネイバー 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
dynamic-capability 例 : <pre>switch(config-router-neighbor) # dynamic-capability</pre>	ダイナミック機能をイネーブルにします。このコマンドによって、BGP ネイバー セッションの自動通知およびセッションリセットが開始されます。 このコマンドは、デフォルトでイネーブルになっています。

集約アドレスの設定

BGP ルート テーブルの集約アドレス エントリを設定できます。

集約アドレスを設定するには、ルータ アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
aggregate-address <code>ip-prefix/length [as-set] [summary-only] [advertise-map map-name] [attribute-map map-name] [suppress-map map-name]</code> 例 : <pre>switch(config-router-af)# aggregate-address 192.0.2.0/8 as-set</pre>	集約アドレスを作成します。このルートに関してアドバタイズされるパスは、集約されているすべてのパスに含まれるすべての要素からなる、自律システム セットです。 • as-set キーワードは、関係するパスから自律システム セットパス情報およびコミュニティ情報を生成します。 • summary-only キーワードは、アップデートから具体的なルートをすべてフィルタリングします。 • advertise-map キーワードおよび引数では、選択されたルートから属性情報を選択するためのルート マップを指定します。 • attribute-map キーワードおよび引数では、集約から属性情報を選択するためのルート マップを指定します。 • suppress-map キーワードおよび引数では、固有性の強いルートを条件付きでフィルタ処理します。

BGP ルートの抑制

新しく学習された BGP ルートが転送情報ベース (FIB) により確認され、ハードウェアでプログラミングされた後にのみ、これらのルートをアドバタイズするように Cisco NX-OS を設定できます。ルートがプログラミングされた後は、これらのルートに対する以降の変更にはこのハードウェア プログラミングのチェックは必要ありません。BGP ルート抑制はデフォルトでは有効ではありません。



- (注) スイッチ上で、ハードウェアテーブルの枯渇が原因でハードウェアでローカルにプログラミングされていないルートに対して `fib-suppression` を有効にすると、BGP は、ハードウェアでローカルにプログラミングされていない場合でも、これらの失敗したルートをアドバタイズします。

BGP ルートを抑制するには、ルータ構成モードで次のコマンドを使用します。

コマンド	目的
suppress-fib-pending 例 : <pre>switch(config-router)# suppress-fib-pending</pre>	新しく学習された BGP ルート（IPv4 または IPv6）がハードウェアでプログラミングされるまで、ダウンストリームの BGP ネイバーにアドバタイズされることを抑制します。

BGP 条件付きアドバタイズメントの設定

BGP がプロパゲートするルートを制限するように BGP 条件付きアドバタイズメントを設定できます。次の 2 つのルート マップを定義します。

- **アドバタイズ マップ** : BGP が条件付きアドバタイズメントを考慮する前にルートが一致する必要のある条件を指定します。このルートマップには、適切な **match** 文を含めることができます。
- **存在マップまたは非存在マップ** : BGP がアドバタイズ マップに一致するルートをプロパゲートする前に BGP テーブルに存在する必要があるプレフィックスを定義します。非存在マップは、BGP がアドバタイズ マップに一致するルートをプロパゲートする前に BGP テーブルに存在してはならないプレフィックスを定義します。BGP は、これらのルートマップでプレフィックス リストの **match** 文内にある **permit** 文のみを処理します。

ルートが条件を渡さない場合、そのルートが BGP テーブルにあれば BGP によってルートが取り消されます。

始める前に

BGP 機能を有効にしていることを確認します（[BGP 機能のイネーブル化](#)のセクションを参照してください）。

手順の概要

1. **configure terminal**
2. **router bgp as-number**
3. **neighbor ip-address remote-as as-number**
4. **address-family { ipv4 | ipv6 } { unicast | multicast }**
5. **advertise-map adv-map { exist-map exist-rmap | non-exist-map nonexist-rmap }**
6. （任意） **show ip bgp neighbor**
7. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router bgp as-number 例 : <pre>switch(config)# router bgp 65536 switch(config-router)#</pre>	BGP モードを開始し、ローカル BGP スピーカに自律システム番号を割り当てます。
ステップ 3	neighbor ip-address remote-as as-number 例 : <pre>switch(config-router)# neighbor 192.168.1.2 remote-as 65537 switch(config-router-neighbor)#</pre>	BGP ルーティング用のネイバー設定モードを開始し、ネイバー IP アドレスを設定します。
ステップ 4	address-family { ipv4 ipv6 } { unicast multicast } 例 : <pre>switch(config-router-neighbor)# address-family ipv4 multicast switch(config-router-neighbor-af)#</pre>	アドレス ファミリ設定モードを開始します。
ステップ 5	advertise-map adv-map { exist-map exist-rmap non-exist-map nonexist-rmap } 例 : <pre>switch(config-router-neighbor-af)# advertise-map advertise exist-map exist</pre>	2 つの設定済みルート マップに従い、ルートを条件付きでアドバタイズするように BGP を設定します。 • adv-map : BGP がルートを次のルート マップに渡す前に、そのルートが渡す必要のある match 文を含むルート マップを指定します。adv-map は、大文字と小文字が区別される 63 文字以下の英数字文字列です。 • exist-rmap : プレフィックス リストの match ステートメントを使用してルートマップを指定します。BGP テーブル内のプレフィックスは、BGP がルートをアドバタイズする前に、プレフィックスリスト内のプレフィックスと一致する必要があります。exist-rmap は、大文字と小文字が区別される 63 文字以下の英数字文字列です。 • nonexist-rmap : プレフィックス リストの match ステートメントを使用してルートマップを指定します。BGP テーブル内のプレフィックスは、

	コマンドまたはアクション	目的
		BGP がルートをアドバタイズする前に、プレフィックスリスト内のプレフィックスと一致してはいけません。nonexist-rmap は、大文字と小文字が区別される 63 文字以下の英数字文字列です。
ステップ 6	(任意) show ip bgp neighbor 例 : <pre>switch(config-router-neighbor-af)# show ip bgp neighbor</pre>	BGP に関する情報、および設定した条件付きアドバタイズメントのルートマップに関する情報を表示します。
ステップ 7	(任意) copy running-config startup-config 例 : <pre>switch(config-router-neighbor-af)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、BGP 条件付きアドバタイズメントを設定する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# neighbor 192.0.2.2 remote-as 65537
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# advertise-map advertise exist-map exist
switch(config-router-neighbor-af)# exit
switch(config-router-neighbor)# exit
switch(config-router)# exit
switch(config)# route-map advertise
switch(config-route-map)# match as-path pathList
switch(config-route-map)# exit
switch(config)# route-map exit
switch(config-route-map)# match ip address prefix-list plist
switch(config-route-map)# exit
switch(config)# ip prefix-list plist permit 209.165.201.0/27
```

ルートの再配布の設定

別のルーティングプロトコルからのルーティング情報を受け入れて、BGP ネットワークを通じてその情報を再配布するように、BGP を設定できます。任意で、再配布ルートのためのデフォルトルートを割り当てることができます。

始める前に

BGP 機能を有効にしていることを確認します (BGP 機能のイネーブル化のセクションを参照してください)。

手順の概要

1. **configure terminal**
2. **router bgp as-number**
3. **address-family { ipv4 | ipv6 } { unicast | multicast }**
4. **redistribute { direct | { eigrp | ospf | ospfv3 | rip } instance-tag | static } route-map map-name**
5. (任意) **default-metric value**
6. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router bgp as-number 例 : <pre>switch(config)# router bgp 65536 switch(config-router)#</pre>	BGP モードを開始し、ローカル BGP スピーカに自律システム番号を割り当てます。
ステップ 3	address-family { ipv4 ipv6 } { unicast multicast } 例 : <pre>switch(config-router)# address-family ipv4 unicast switch(config-router-af)#</pre>	アドレス ファミリ設定モードを開始します。
ステップ 4	redistribute { direct { eigrp ospf ospfv3 rip } instance-tag static } route-map map-name 例 : <pre>switch(config-router-af)# redistribute eigrp 201 route-map Eigrpmap</pre>	他のプロトコルからのルートを BGP に再配布します。ルートマップの設定の詳細については、 ルートマップの設定 のセクションを参照してください。
ステップ 5	(任意) default-metric value 例 : <pre>switch(config-router-af)# default-metric 33</pre>	BGP へのデフォルト ルートを生成します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config-router-af)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、EIGRP を BGP に再配布する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# redistribute eigrp 201 route-map Eigrpmap
switch(config-router-af)# copy running-config startup-config
```

再分配による BGP 減衰の無効化

BGP に再配布されたルートの IGP メトリックが変更された場合、BGP の内部ダンプニングが発生し、BGP ピアへの即時ルート アップデートが行われなくなります。これは、再配布されたルートについて報告された IGP メトリック変更を BGP が処理する方法に影響します。BGP は、10 分間の遅延でバッチ プロセスを通してこれらの変更を抑制します。このコマンドを使用すると、その遅延を調整したり、遅延をなくしたりして、その変化への対応を迅速化することができます。

手順の概要

1. **configure terminal**
2. **router bgp *as-number***
3. **address-family { *ipv4* | *ipv6* } { *unicast* | *multicast* }**
4. **dampen-igp-metric *seconds***

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router bgp <i>as-number</i> 例 : <pre>switch(config)# router bgp 65536 switch(config-router)#</pre>	BGP モードを開始し、ローカル BGP スピーカに自律システム番号を割り当てます。
ステップ 3	address-family { <i>ipv4</i> <i>ipv6</i> } { <i>unicast</i> <i>multicast</i> } 例 : <pre>switch(config-router)# address-family ipv4 unicast switch(config-router-af)#</pre>	アドレス ファミリ設定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	dampen-igp-metric seconds 例 : <pre>switch(config-router-af)# dampen-igp-metric 100</pre>	再配布されたルートの IGP メトリック関連変更のダンプニングを構成します。

例

次に、再配布ルートに BGP ダンプニングを構成する例を示します。

```
switch# configure terminal
switch(config)# router bgp 100
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# dampen-igp-metric 100
switch(config-router-af)#
```

マルチプロトコル BGP の設定

複数のアドレスファミリ（IPv4 のユニキャストおよびマルチキャストルートを含む）をサポートするように MP-BGP を構成できます。

始める前に

BGP 機能を有効にしていることを確認します（[BGP 機能のイネーブル化](#)のセクションを参照してください）。

手順の概要

1. **configure terminal**
2. **router bgp as-number**
3. **neighbor ip-address remote-as as-number**
4. **address-family { ipv4 | ipv6 } { unicast | multicast }**
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router bgp as-number 例 :	BGP モードを開始し、ローカル BGP スピーカに自律システム番号を割り当てます

	コマンドまたはアクション	目的
	<pre>switch(config)# router bgp 65536 switch(config-router)#</pre>	
ステップ 3	neighbor ip-address remote-as as-number 例 : <pre>switch(config-router)# neighbor 192.168.1.2 remote-as 65537 switch(config-router-neighbor)#</pre>	BGP ルーティング用のネイバー設定モードを開始し、ネイバー IP アドレスを設定します。
ステップ 4	address-family { ipv4 ipv6 } { unicast multicast } 例 : <pre>switch(config-router-neighbor)# address-family ipv4 multicast switch(config-router-neighbor-af)#</pre>	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	(任意) copy running-config startup-config 例 : <pre>switch(config-router-neighbor-af)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、ネイバーのマルチキャスト RPF に対して IPv4 ルートのアドバタイズおよび受信をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ipv6 address 2001:0DB8::1
switch(config-if)# router bgp 65536
switch(config-router)# neighbor 192.168.1.2 remote-as 35537
switch(config-router-neighbor)# address-family ipv4 multicast
switch(config-router-neighbor-af)# exit
switch(config-router-neighbor)# address-family ipv6 multicast
switch(config-router-neighbor-af)# copy running-config startup-config
```

元の BGP 拡張コミュニティ サイトの構成

BGP 拡張コミュニティの Site of Origin を構成するには、次のコマンドを使用します。

コマンド	目的
router bgp as-number 例 : <pre>switch(config)# router bgp 1 switch(config-router)#</pre>	BGP 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。

コマンド	目的
vrf vrf-name 例 : <pre>switch(config-router)# vrf 450 switch(config-router-vrf)#</pre>	ルータ VRF 設定モードを開始し、この BGP インスタンスと VRF を関連付けます。
neighbor ip-address remote-as as-number 例: <pre>switch(config-router-vrf)# neighbor 1::1 remote-as 2 switch(config-router-vrf-neighbor)#</pre>	リモート BGP ピアの IP アドレスおよび AS 番号を設定します。
address-family { ipv4 ipv6 } { multicast unicast } 例 : <pre>switch(config-router-vrf-neighbor)# address-family ipv6 unicast switch(config-router-vrf-neighbor-af)#</pre>	指定されたアドレス ファミリに対応する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ます。
soo value 例 : <pre>switch(config-router-vrf-neighbor-af)# soo 22:14</pre>	元の BGP 拡張コミュニティ値のサイトを構成します。 この値は、次のいずれかの形式です。 • asn:number • IP address:number 番号の範囲は、2 バイトの ASN の場合は 0 ～ 65535、4 バイトの ASN の場合は 0 ～ 4294967295 です。

BGP の調整

BGP タイマーによって、さらにベストパス アルゴリズムの調整によって、BGP のデフォルト動作を変更できます。

仮想化の設定

始める前に

BGP 機能を有効にしていることを確認します（[BGP 機能の有効化](#)のセクションを参照してください）。

手順の概要

1. configure terminal

2. **vrf context** *vrf-name*
3. **exit**
4. **router bgp** *as-number*
5. **vrf** *vrf-name*
6. **neighbor** *ip-address* **remote-as** *as-number*
7. (任意) **bestpath as-path multipath-relax**
8. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	vrf context <i>vrf-name</i> 例 : <pre>switch(config)# vrf context RemoteOfficeVRF switch(config-vrf)#</pre>	新しい VRF を作成し、VRF 設定モードを開始します。
ステップ 3	exit 例 : <pre>switch(config-vrf)# exit switch(config)#</pre>	VRF設定モードを終了します。
ステップ 4	router bgp <i>as-number</i> 例 : <pre>switch(config)# router bgp 65536 switch(config-router)#</pre>	自律システム番号を設定して、新しい BGP プロセスを作成します。
ステップ 5	vrf <i>vrf-name</i> 例 : <pre>switch(config-router)# vrf RemoteOfficeVRF switch(config-router-vrf)#</pre>	ルータ VRF設定モードを開始し、この BGP インスタンスと VRF を関連付けます。
ステップ 6	neighbor <i>ip-address</i> remote-as <i>as-number</i> 例 : <pre>switch(config-router-vrf)# neighbor 209.165.201.1 remote-as 65536 switch(config-router--vrf-neighbor)#</pre>	リモート BGP ピアの IP アドレスおよび AS 番号を設定します。

	コマンドまたはアクション	目的
ステップ 7	(任意) bestpath as-path multipath-relax 例 : <pre>switch(config-router-vrf)# bestpath as-path multipath-relax</pre>	自律パスの長さが同じで、他のマルチパスの条件を満たしている場合、別の自律システムから受け取ったパスをマルチパスとして扱えるようにします。
ステップ 8	(任意) copy running-config startup-config 例 : <pre>switch(config-router-neighbor)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、VRF を作成し、VRF でルータ ID を設定する例を示します。

```
switch# configure terminal
switch(config)# vrf context NewVRF
switch(config-vrf)# exit
switch(config)# router bgp 65536
switch(config-router)# vrf NewVRF
switch(config-router-vrf)# neighbor 209.165.201.1 remote-as 65536
switch(config-router-vrf-neighbor)# copy running-config startup-config
```

BGP グレースフル シャットダウン

BGP グレースフル シャットダウンに関する情報

リリース 9.3(1) 以降、BGP はグレースフル シャットダウン機能をサポートしています。この BGP 機能は、BGP **shutdown** コマンドと連携して次のことを行います。

- ルータまたはリンクがオフラインになったときのネットワーク コンバージェンス時間を大幅に短縮します。
- ルータまたはリンクがオフラインになったときに、転送中のドロップされたパケットを削減または排除します。

名前にかかわらず、BGP グレースフル シャットダウンは実際にはシャットダウンを引き起こしません。代わりに、ルータまたはリンクが間もなくダウンすることを、接続されているルータに通知します。

グレースフル シャットダウン機能は、GRACEFUL_SHUTDOWN ウェルノウン コミュニティ (0xFFFF0000 または 65535:0) を使用します。これは、IANA および IETF によって RFC 8326 によって識別されます。この既知のコミュニティは任意のルートにアタッチでき、ルートの他の属性と同様に処理されます。

この機能は、ルータまたはリンクがダウンすることを通知するため、メンテナンス時間帯または計画停止の準備に役立ちます。トラフィックへの影響を制限するには、BGP をシャットダウンする前にこの機能を使用します。

グレースフル シャットダウンの認識とアクティブ化

BGP ルータは、すべてのルートの優先事項を、GRACEFUL SHUTDOWN 対応というコンセプトを通し、GRACEFUL_SHUTDOWN コミュニティによって制御できます。グレースフルシャットダウン対応は、デフォルトでイネーブルになっています。これにより、受信側ピアは、GRACEFUL_SHUTDOWN コミュニティを伝える着信ルートを優先しなくなります。一般的な使用例ではありませんが、**graceful-shutdown aware** コマンドを使用して、グレースフルシャットダウン対応を無効にしてから再度有効にすることもできます。

グレースフル シャットダウン対応は、BGP グローバル コンテキストでのみ適用されます。コンテキストの詳細については、[グレースフルシャットダウンのコンテキスト \(361 ページ\)](#) を参照してください。対応のためのオプションは、**activate** という別のオプションと一緒に動作します。このオプションをルートマップに割り当てると、グレースフルシャットダウンのルートをより詳細に制御できます。

グレースフル シャットダウン対応オプションとアクティブ化オプションの協同作用

グレースフル シャットダウンがアクティブな場合、**activate** キーワードを指定した場合にのみ、GRACEFUL_SHUTDOWN コミュニティがルート更新に追加されます。この時点で、コミュニティを含む新しいルート更新が生成され、送信されます。**graceful-shutdown aware** コマンドが設定されると、コミュニティを受信するすべてのルータは、アップデート内のルートの優先を解除します（そのルート優先度を下げます）。**graceful-shutdown aware** コマンドを使用しなかった場合、BGP は GRACEFUL_SHUTDOWN コミュニティの設定されたルートの優先度を下げません。

この機能がアクティブになり、ルータがグレースフルシャットダウンの対応状態になった場合でも、BGP は引き続き、GRACEFUL_SHUTDOWN コミュニティが有効だとしてルートを考慮します。ただし、これらのルートには、最適パスの計算で最低の優先度が与えられます。代替パスが使用可能な場合は、新しい最適パスが選択され、まもなくダウンするルータまたはリンクに対応するためのコンバージェンスが行われます。

グレースフル シャットダウンのコンテキスト

BGP のグレースフルシャットダウン機能には、機能の影響と使用可能な機能を決定する 2 つのコンテキストがあります。

コンテキスト	影響	コマンド
グローバル	スイッチ全体と、スイッチによって処理されるすべてのルート。たとえば、GRACEFUL_SHUTDOWN コミュニティを持つすべてのルートを再アドバタイズします。	graceful-shutdown activate [route-map ルート マップ] graceful-shutdown aware
Peer	BGP ピアまたはネイバー間のリンク。たとえば、ピア間のリンクを 1 つだけ GRACEFUL_SHUTDOWN コミュニティでアドバタイズします。	graceful-shutdown activate [route-map ルート マップ]

ルート マップによるグレースフル シャットダウン

グレースフル シャットダウンは、ルート ポリシー マネージャ (RPM) 機能と連携して、スイッチの BGP ルータが GRACEFUL_SHUTDOWN コミュニティを使用してルートを送受信する方法を制御します。ルート マップは、インバウンドおよびアウトバウンド方向でコミュニティとのルート更新を処理できます。通常、ルートマップは必要ありません。ただし、必要に応じて、グレースフルシャットダウンルートの制御をカスタマイズするために使用できます。

通常のインバウンドルート マップ

通常のインバウンドルート マップは、BGP ルータに着信するルートに影響します。ルータはデフォルトでグレースフルシャットダウンを認識するため、通常のインバウンドルート マップはグレースフル シャットダウン機能では一般的に使用されません。

Cisco NX-OS リリース 9.3 (1) 以降を実行している Cisco Nexus スイッチでは、グレースフルシャットダウン機能のインバウンドルート マップは必要ありません。Cisco NX-OS リリース 9.3

(1) 以降には、BGP ルータがグレースフルシャットダウン対応である場合に GRACEFUL_SHUTDOWN コミュニティを持つすべてのルートを自動的に非優先にする、暗黙のインバウンドルート マップがあります。

通常のインバウンドルート マップは、既知の GRACEFUL_SHUTDOWN コミュニティと一致するように設定できます。これらの着信ルートマップは一般的ではありませんが、使用される場合があります。

- スイッチが 9.3 (1) よりも前の Cisco NX-OS リリースを実行している場合、NX-OS 9.3 (1) には暗黙的なインバウンドルート マップがありません。これらのスイッチでグレースフルシャットダウン機能を使用するには、グレースフルシャットダウンインバウンドルート マップを作成する必要があります。ルートマップは、既知の GRACEFUL_SHUTDOWN コミュニティを持つインバウンドルートと一致し、それらを許可し、それらを非優先にする必要があります。着信ルート マップが必要な場合は、9.3 (1) より前のバージョンの

NX-OS を実行し、グレースフル シャットダウン ルートを受信している BGP ピアで作成します。

- グレースフル シャットダウン 認識をディセーブルにし、一部の BGP ネイバーからの `GRACEFUL_SHUTDOWN` コミュニティを持つ着信ルートでルータを動作させる場合は、それぞれのピアでインバウンド ルート マップを設定できます。

通常のアウトバウンド ルート マップ

通常のアウトバウンド ルート マップは、BGP ルータが送信するルートの転送を制御します。通常のアウトバウンド ルート マップは、グレースフル シャットダウン 機能に影響を与える可能性があります。たとえば、`GRACEFUL_SHUTDOWN` コミュニティで一致するようにアウトバウンド ルート マップを設定し、属性を設定できます。これは、グレースフル シャットダウン アウトバウンド ルート マップよりも優先されます。

グレースフル シャットダウン アウトバウンド ルート マップ

アウトバウンド グレースフル シャットダウン ルート マップは、グレースフル シャットダウン 機能のアウトバウンド ルート マップの特定のタイプです。これらはオプションですが、ルート マップに関連付けられているコミュニティ リストがすでにある場合に役立ちます。通常のグレースフル シャットダウン アウトバウンド ルート マップには、特定の属性を設定または変更するための `set` 句のみが含まれています。

アウトバウンド ルート マップは、次の方法で使用できます。

- 既存のアウトバウンド ルート マップをすでに持っている顧客の場合は、より大きいシーケンス番号を持つ新しいエントリを追加し、`GRACEFUL_SHUTDOWN` ウェルノウン コミュニティで照合し、必要な属性を追加できます。
- **`graceful-shutdown activate route-map name`** オプションを使用してグレースフル シャットダウン アウトバウンド ルート マップを使用することもできます。これが一般的な使用例です。

このルート マップには `match` 句が必要ないため、ルート マップはネイバーに送信されるすべてのルートで一致します。

ルート マップの優先順位

同じルータ上に複数のルート マップが存在する場合は、次の優先順位が適用されて、コミュニティとのルートの処理方法が決定されます。次の例を考慮してください。60 のローカル設定を設定する標準の発信ルート マップ名 `Red` があるとします。また、`Blue` という名前のピア グレースフル シャットダウン ルート マップがあり、`local-pref` が 30 に設定されているとします。ルート更新が処理されると、`Red` は `Blue` を上書きするため、ローカル プリファレンスは 60 に設定されます。

- 通常の発信ルート マップは、ピア グレースフル シャットダウン マップよりも優先されます。

- ピア グレースフル シャットダウン マップは、グローバル グレースフル シャットダウン マップよりも優先されます。

注意事項と制約事項

BGP グローバル シャットダウンの制限事項と注意事項は、次のとおりです。

- グレースフルシャットダウン機能は、影響を受けるルータの代替ルートがネットワークに存在する場合にのみ、トラフィック損失を回避するのに役立ちます。ルータに代替ルートがない場合は、GRACEFUL_SHUTDOWN コミュニティを伝送するルートが使用可能な唯一のルートであるため、最適パスの計算に使用されます。この状況では、機能の目的が失われます。
- GRACEFUL_SHUTDOWN コミュニティを送信するには、BGP 送信コミュニティの設定が必要です。
- ルート マップの場合:
 - グローバルルートマップとネイバールートマップが設定されている場合、ネイバー単位のルートマップが優先されます。
 - 発信ルートマップは、グレースフル シャットダウン用に設定されたグローバル ルートマップよりも優先されます。
 - 発信ルートマップは、グレースフル シャットダウン用に設定されたピアルートマップよりも優先されます。
 - レガシー（既存の）インバウンドルートマップにグレースフル シャットダウン機能を追加するには、次の手順を実行します。
 1. graceful shutdown match 句をルートマップの先頭に追加します。これには、句に低いシーケンス番号（たとえば、シーケンス番号 0）を設定します。
 2. graceful shutdown 句の後に continue ステートメントを追加します。continue ステートメントを省略すると、graceful shutdown 句と一致するルートマップ処理が停止します。シーケンス番号が大きい他の句（たとえば、1 以上）は処理されません。

グレースフル シャットダウン タスクの概要

グレースフル シャットダウン機能を使用するには、通常、すべての Cisco Nexus スイッチでグレースフル シャットダウン対応をイネーブルにし、機能をイネーブルのままにします。BGP ルータをオフラインにする必要がある場合は、graceful-shutdown activate を設定します。

次の詳細に、グレースフル シャットダウン機能を使用するためのベスト プラクティスを示します。

ルータまたはリンクをダウンさせるには、次の手順を実行します。

1. グレースフル シャットダウン機能を設定します。

2. ネイバーでベスト パスを確認します。
3. 最適パスが再計算されたら、BGP を無効にする **shutdown** コマンドを発行します。
4. ルータまたはリンクをシャットダウンする必要がある作業を実行します。

ルータまたはリンクをオンラインに戻すには、次の手順を実行します。

1. シャットダウンが必要な作業が完了したら、BGP を再度イネーブルにします (**no shutdown**)。
2. グレースフル シャットダウン機能を無効にします (config モードの **no graceful-shutdown activate**)。

リンクのグレースフル シャットダウンの設定

この作業では、2 つの BGP ルータ間の特定のリンクでグレースフル シャットダウンを設定できます。

始める前に

BGP をまだ有効にしていない場合は、ここで有効にします (**feature bgp**)。

手順の概要

1. **config terminal**
2. **router bgp autonomous-system-number**
3. **neighbor { ipv4-address|ipv6-address } remote-as as-number**
4. **graceful-shutdown activate [route-map map-name]**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	config terminal 例 : switch-1# configure terminal switch-1(config)#	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	router bgp autonomous-system-number 例 : switch-1(config)# router bgp 110 switch-1(config-router)#	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成または設定します。

	コマンドまたはアクション	目的
ステップ 3	neighbor { ipv4-address ipv6-address } remote-as as-number 例 : <pre>switch-1(config-router)# neighbor 10.0.0.3 remote-as 200 switch-1(config-router-neighbor)#</pre>	ネイバーが属する自律システム (AS) を設定します。
ステップ 4	graceful-shutdown activate [route-map map-name] 例 : <pre>switch-1(config-router-neighbor)# graceful-shutdown activate route-map gshutPeer switch-1(config-router-neighbor)#</pre>	ネイバーへのリンクでグレースフルシャットダウンを設定します。また、既知の GRACEFUL_SHUTDOWN コミュニティを使用してルートをアドバタイズし、アウトバウンドルート更新にルートマップを適用します。 ルートは、デフォルトでグレースフルシャットダウンコミュニティでアドバタイズされます。この例では、ルートは gshutPeer という名前のルートマップを使用して、グレースフルシャットダウンコミュニティを持つネイバーにアドバタイズされます。 gshut コミュニティを受信したデバイスは、ルートのコミュニティを確認し、オプションでコミュニティを使用してルーティングポリシーを適用します。

GRACEFUL_SHUTDOWN コミュニティに基づく BGP ルートのフィルタリングとローカルプリファレンスの設定

まだ 9.3(1) を実行していないスイッチには、GRACEFUL_SHUTDOWN コミュニティ名と一致するインバウンドルートマップがありません。したがって、正しいルートを識別して先送りする方法はありません。

9.3(1) よりも前のリリースの NX-OS を実行しているスイッチでは、グレースフルシャットダウン (65535:0) のコミュニティ値と一致するインバウンドルートマップを設定し、ルートを非優先にする必要があります。

スイッチが 9.3(1) 以降を実行している場合、着信ルートマップを設定する必要はありません。

手順の概要

1. **configure terminal**
2. **ip community list standard community-list-name seq sequence-number { permit | deny } value**
3. **route map map-tag {deny | permit} sequence-number**
4. **match community community-list-name**
5. **set local-preference local-pref-value**
6. **exit**
7. **router bgp community-list-name**

8. **neighbor** { *ipv4-address|ipv6-address* }
9. **address-family** { *address-family sub family* }
10. **send community**
11. **route map** *map-tag* **in**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch-1# configure terminal switch-1(config)#</pre>	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	ip community list standard community-list-name seq sequence-number { permit deny } value 例 : <pre>switch-1(config)# ip community-list standard GSHUT seq 10 permit 65535:0 switch-1(config)#</pre>	コミュニティリストを設定し、よく知られたグレースフルシャットダウン コミュニティ値を持つルートを許可または拒否します。
ステップ 3	route map map-tag {deny permit} sequence-number 例 : <pre>switch-1(config)# route-map RM_GSHUT permit 10 switch-1(config-route-map)#</pre>	ルート マップをシーケンス 10 として設定し、GRACEFUL_SHUTDOWN コミュニティを持つルートを許可します。
ステップ 4	match community community-list-name 例 : <pre>switch-1(config-route-map)# match community GSHUT switch-1(config-route-map)#</pre>	IP コミュニティ リスト GSHUT に一致するルートがルート ポリシー マネージャ (RPM) により処理されるように設定します。
ステップ 5	set local-preference local-pref-value 例 : <pre>switch-1(config-route-map)# set local-preference 10 switch-1(config-route-map)#</pre>	IP コミュニティ リスト GSHUT に一致するルートに、指定されたローカル プリファレンスが与えられるように設定します。
ステップ 6	exit 例 : <pre>switch-1(config-route-map)# exit switch-1(config)#</pre>	ルート マップ設定モードを終了し、グローバル設定モードに戻ります。
ステップ 7	router bgp community-list-name 例 : <pre>switch-1(config)# router bgp 100 switch-1(config-router)#</pre>	ルータ設定モードを開始し、BGP インスタンスを作成します。

すべての BGP ネイバーのグレースフル シャットダウンの設定

	コマンドまたはアクション	目的
ステップ 8	neighbor { ipv4-address ipv6-address } 例 : <pre>switch-1(config-router)# neighbor 10.0.0.3 switch-1(config-router-neighbor)#</pre>	指定したネイバーのルート BGP ネイバー モードを開始します。
ステップ 9	address-family { address-family sub family } 例 : <pre>nxosv2(config-router-neighbor)# address-family ipv4 unicast nxosv2(config-router-neighbor-af)#</pre>	ネイバーをアドレス ファミリ (AF) 設定モードにします。
ステップ 10	send community 例 : <pre>nxosv2(config-router-neighbor-af)# send-community nxosv2(config-router-neighbor-af)#</pre>	ネイバーとの BGP コミュニティ交換を可能にします。
ステップ 11	route map map-tag in 例 : <pre>nxosv2(config-router-neighbor-af)# route-map RM_GSHUT in nxosv2(config-router-neighbor-af)#</pre>	ネイバーからの着信ルートにルート マップを適用します。この例では、RM_GSHUT という名前のルート マップは、ネイバーからの GRACEFUL_SHUTDOWN コミュニティを持つルートを許可します。

すべての BGP ネイバーのグレースフル シャットダウンの設定

グレースフル シャットダウン イニシエータのすべてのネイバーに GRACEFUL_SHUTDOWN ウェルノウン コミュニティを手動で適用できます。

すべての BGP ネイバーに対して、グローバル レベルでグレースフル シャットダウンを設定できます。

始める前に

BGP をまだ有効にしていない場合は、ここで有効にします (**feature bgp**)。

手順の概要

1. **configure terminal**
2. **router bgp autonomous-system-number**
3. **graceful-shutdown activate [route-map map-name]**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch-1# configure terminal switch-1(config)#</pre>	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	router bgp autonomous-system-number 例 : <pre>switch-1(config)# router bgp 110 switch-1(config-router)#</pre>	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 3	graceful-shutdown activate [route-map map-name] 例 : <pre>switch-1(config-router-neighbor)# graceful-shutdown activate route-map gshutPeer switch-1(config-router-neighbor)#</pre>	すべてのネイバーへのリンクのグレースフルシャットダウン ルート マップを設定します。また、既知の GRACEFUL_SHUTDOWN コミュニティを持つすべてのルートをアドバタイズし、ルートマップをアウトバウンド ルート アップデートに適用します。 ルートはデフォルトで GRACEFUL_SHUTDOWN コミュニティでアドバタイズされます。この例では、ルートが gshutPeer という名前のルートマップを持つコミュニティを持つすべてのネイバーにアドバタイズされます。ルートマップには set 句のみを含める必要があります。 GRACEFUL_SHUTDOWN コミュニティを受信したデバイスは、ルートのコミュニティを確認し、オプションでコミュニティを使用してルーティング ポリシーを適用します。

GRACEFUL_SHUTDOWN コミュニティを使用したすべてのルートのプリファレンスの制御

Cisco NX-OS では、GRACEFUL_SHUTDOWN コミュニティを持つ着信ルートの優先順位を下げるができます。 **graceful shutdown aware** が有効になっている場合、最適パス計算時に、BGP はコミュニティを伝送するルートを最も低い優先順位と見なします。デフォルトでは、プリファレンスの引き下げが有効になっていますが、このオプションを選択的に無効にすることもできます。

このオプションをイネーブルまたはディセーブルにするたびに、BGP のベストパス計算がトリガーされます。このオプションを使用すると、グレースフルシャットダウンのウェルノウンコミュニティにおける BGP のベストパス計算の動作を柔軟に制御できます。

始める前に

BGPを有効にしていない場合は、ここで有効にします（**feature bgp**）。

手順の概要

1. **configure terminal**
2. **router bgp autonoums-system**
3. （任意） **no graceful-shutdown aware**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch-1(config)# config terminal switch-1(config)#</pre>	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	router bgp autonoums-system 例 : <pre>switch-1(config)# router bgp 100 switch-1(config-router)#</pre>	ルータ コンフィギュレーション モードを開始し、BGP ルーティング プロセスを設定します。
ステップ 3	（任意） no graceful-shutdown aware 例 : <pre>switch-1(config-router)# no graceful-shutdown aware switch-1(config-router)#</pre>	このBGPルータでは、GRACEFUL_SHUTDOWN コミュニティを持つすべてのルートに低い優先順位を指定しないという意味です。グレースフルシャットダウン認識機能がディセーブルになっている場合、デフォルトアクションはルートを非優先にします。そのため、コマンドには no 形式というオプションが存在しており、これを使用すると、グレースフルシャットダウン ルートは非優先になりません。

GRACEFUL_SHUTDOWN コミュニティのピアへの送信の防止

発信ルート更新にルート属性として追加された GRACEFUL_SHUTDOWN コミュニティが不要になった場合は、コミュニティを削除して、指定されたネイバーに送信なくなります。1つの使用例は、ルータが自律システム境界にあり、グレースフルシャットダウン機能が自律システム境界の外部に伝播しないようにする場合です。

GRACEFUL_SHUTDOWN がピアに送信されないようにするには、**send community** オプションを無効にするか、コミュニティを発信ルート マップから削除します。

次の方法の中から 1 つを選択してください。

- 実行コンフィギュレーションで **send-community** を無効にします。

例：

```
nxosv2(config-router-neighbor-af)# no send-community standard
nxosv2(config-router-neighbor-af)#
```

このオプションを使用すると、スイッチは GRACEFUL_SHUTDOWN コミュニティを受信しますが、発信ルート マップを介してダウンストリーム ネイバーに送信されません。すべての標準コミュニティも送信されません。

- 次の手順に従って、発信ルートマップを介して GRACEFUL_SHUTDOWN コミュニティを削除します。
 1. GRACEFUL_SHUTDOWN コミュニティと一致する IP コミュニティ リストを作成します。
 2. GRACEFUL_SHUTDOWN コミュニティと照合する発信ルート マップを作成します。
 3. **set community-list delete** 句を使用して GRACEFUL_SHUTDOWN コミュニティを削除します。

このオプションを使用すると、コミュニティ リストは GRACEFUL_SHUTDOWN コミュニティと一致し、許可されます。その後、発信ルートマップはコミュニティと照合され、発信ルートマップから削除されます。他のすべてのコミュニティは、問題なく発信ルートマップを通過します。

グレースフル シャットダウン情報の表示

グレースフル シャットダウン機能に関する情報は、次の **show** コマンドで確認できます。

コマンド	アクション
show ip bgp community-list graceful-shutdown	GRACEFUL_SHUTDOWN コミュニティを持つ BGP ルーティング テーブル内のすべてのエントリを表示します。
show running-config bgp	実行中の BGP のデフォルト設定を示します。
show running-config bgp all	グレースフル シャットダウン機能に関する情報など、実行中の BGP 設定のすべての情報を表示します。
show bgp address-family neighbors neighbor-address	機能がピアに設定されている場合、次のように表示されます。 • 指定されたネイバーの graceful-shutdown-activate 機能の状態 • 指定されたネイバーに設定されたグレースフルシャットダウンルートマップの名前

コマンド	アクション
show bgp process	コンテキストに応じて異なる情報を表示します。 graceful-shutdown-activate オプションがピア コンテキストで設定されている場合、graceful-shutdown-active を介して機能の有効または無効状態を示します。 graceful-shutdown-activate オプションがグローバル コンテキストで設定され、graceful-shutdown ルートマップがある場合は、次のように機能の有効状態が表示されます。 • graceful-shutdown-active • graceful-shutdown-aware • graceful-shutdown route-map
show ip bgp address	指定されたアドレスについて、次を含む BGP ルーティング テーブル情報を表示します。 • 最適パスとして指定されたアドレスの状態 • 指定されたアドレスが GRACEFUL_SHUTDOWN コミュニティの一部であるかどうか

グレースフル シャットダウンの設定例

次に、グレースフル シャットダウン機能を使用するための設定例を示します。

BGP リンクのグレースフル シャットダウンの設定

次に、ローカルプリファレンスとコミュニティを設定しながらグレースフル シャットダウンを設定する例を示します。

- 指定されたネイバーへのリンクのグレースフル シャットダウン アクティブ化の設定
- ルートへの **GRACEFUL_SHUTDOWN** コミュニティの追加
- コミュニティとのアウトバウンドルートに対して **set** 句のみを使用して **gshutPeer** という名前のルートマップを設定します。

```
router bgp 100
  neighbor 20.0.0.3 remote-as 200
  graceful-shutdown activate route-map gshutPeer
  address-family ipv4 unicast
    send-community
```

```
route-map gshutPeer permit 10
  set local-preference 0
  set community 200:30
```

All-Neighbor BGP リンクのグレースフル シャットダウンの設定

次に例を示します。

- ローカル ルータとそのすべてのネイバーを接続するすべてのリンクに対してグレースフルシャットダウン アクティブ化を設定します。
- GRACEFUL_SHUTDOWN コミュニティをルートに追加しています。
- すべての発信ルートに対して set 句のみを使用して gshutAall という名前のルートマップを設定します。

```
router bgp 200
  graceful-shutdown activate route-map gshutAll

route-map gshutAll permit 10
  set as-path prepend 10 100 110
  set community 100:80

route-map Red permit 10
  set local-pref 20

router bgp 100
  graceful-shutdown activate route-map gshutAll
  router-id 2.2.2.2
  address-family ipv4 unicast
  network 2.2.2.2/32
  neighbor 1.1.1.1 remote-as 100
  update-source loopback0
  address-family ipv4 unicast
  send-community
  neighbor 20.0.0.3 remote-as 200
  address-family ipv4 unicast
  send-community
  route-map Red out
```

この例では、ネイバー 1.1.1.1 に対して gshutAll ルート マップが有効になりますが、ネイバー 20.0.0.3 で設定された発信ルートマップ Red が優先されるため、ネイバー 20.0.0.3 に対しては有効になりません。

ピアテンプレートでのグレースフル シャットダウンの設定

この例では、ピアセッションテンプレートでグレースフルシャットダウン機能を設定します。これはネイバーによって継承されます。

```
router bgp 200
  template peer-session p1
    graceful-shutdown activate route-map gshut_out
  neighbor 1.1.1.1 remote-as 100
  inherit peer-session p1
  address-family ipv4 unicast
  send-community
```

GRACEFUL_SHUTDOWN コミュニティの使用およびインバウンドルートマップに基づく BGP ルートのフィルタリングとローカル プリファレンスの設定

次に、コミュニティ リストを使用して、GRACEFUL_SHUTDOWN コミュニティを持つ着信ルートをフィルタリングする例を示します。この設定は、Cisco NX-OS 9.3(1) を最小バージョンとして実行していないレガシー スイッチに役立ちます。

次に例を示します。

- GRACEFUL_SHUTDOWN コミュニティを持つルートを許可する IP コミュニティ リスト。
- RM_GSHUT という名前のルート マップは、GSHUT という名前の標準コミュニティ リストに基づいてルートを許可します。
- また、ルートマップは、処理するルートの優先順位を 0 に設定します。これにより、ルータがオフラインになったときに、それらのルートに最適パス計算の優先順位が低くなります。ネイバー (20.0.0.2) からの着信 IPv4 ルートにルート マップが適用されます。

```
ip community-list standard GSHUT permit 65535:0

route-map RM_GSHUT permit 10
  match community GSHUT
  set local-preference 0

router bgp 200
  neighbor 20.0.0.2 remote-as 100
  address-family ipv4 unicast
    send-community
    route-map RM_GSHUT in
```

グレースフル リスタートの設定

グレースフル リスタートを設定し、BGP に対してグレースフル リスタート ヘルパー機能をイネーブルにできます。



- (注) Cisco NX-OS リリース 10.1(1) は、より多くの BFD セッションをサポートします。BGP セッションが BFD に関連付けられている場合、ISSU 中にピア接続を維持するために BGP **restart-time** を増やす必要が生じることがあります。

始める前に

BGP をイネーブルにする必要があります（「BGP のイネーブル化」の項を参照）。

VRF を作成します。

手順の概要

1. **configure terminal**
2. **router bgp as-number**

3. (任意) **timers prefix-peer-timeout** *timeout*
4. **graceful-restart**
5. **graceful-restart** {**restart-time** *time*|**stalepath-time** *time*}
6. **graceful-restart-helper**
7. (任意) **show running-config** **bgp**
8. (任意) **copy running-config** **startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	router bgp <i>as-number</i> 例 : <pre>switch(config)# router bgp 65535 switch(config-router)#</pre>	自律システム番号を設定して、新しい BGP プロセスを作成します。
ステップ 3	(任意) timers prefix-peer-timeout <i>timeout</i> 例 : <pre>switch(config-router)# timers prefix-peer-timeout 20</pre>	BGP プレフィックス ピアのタイムアウト値を設定します (秒単位)。デフォルト値は 90 秒です。 (注) このコマンドは、Cisco NX-OS リリース 9.3(3) 以降でサポートされます。
ステップ 4	graceful-restart 例 : <pre>switch(config-router)# graceful-restart</pre>	グレースフル リスタートおよびグレースフル リスタートヘルパー機能をイネーブルにします。このコマンドは、デフォルトでイネーブルになっています。 このコマンドによって、BGP ネイバーセッションの自動通知およびセッション リセットが開始されます。
ステップ 5	graceful-restart { restart-time <i>time</i> stalepath-time <i>time</i> } 例 : <pre>switch(config-router)# graceful-restart restart-time 300</pre>	グレースフル リスタート タイマーを設定します。 オプション パラメータは次のとおりです。 • restart-time : BGP ピアに送信されたリスタートの最大時間。有効な範囲は 1 ~ 3600 秒です。デフォルトは 120 です。 (注)

	コマンドまたはアクション	目的
		Cisco NX-OS リリース 10.1(1) は、より多くの BFD セッションをサポートします。BGP セッションが BFD に関連付けられている場合、ISSU 中にピア接続を維持するために BGP restart-time を増やす必要が生じることがあります。 • stalepath-time : BGP が再起動中の BGP ピアからの古いルートを維持する最大時間有効な範囲は 1 ～ 3600 秒です。デフォルトは 300 です。 NX-OS ソフトウェア リリース 9.3(3) より前では、BGP セッションがグレースフルリスタート機能をアドバタイズするには、BGP セッションの手動リセットが必要でした。NX-OS ソフトウェア リリース 9.3(3) 以降では、このコマンドが有効になっている場合、BGP セッションは、BGP セッションを再起動する必要なく、グレースフルリスタート機能を動的にアドバタイズします。
ステップ 6	graceful-restart-helper 例 : <pre>switch(config-router)# graceful-restart restart-time 300</pre>	BGP GR が無効になっている場合、SSO や BGP プロセスの再起動などの特定の GR 対応イベントが N9K でローカルに発生している間、N9K 自体は必ずしも自身の転送状態を保持しません。ただし、GR ヘルパーとして、GR 機能をアドバタイズして再起動しているピアをサポートします。つまり、N9K は、ピアリングがダウンしたことを検出すると（ホールドタイマーの期限切れまたは通知メッセージの受信以外）、ピアを指すルートを失効させ、ピアの EOR（または失効パスタイムアウト）を待機します。ピアが再起動して N9K とのピアリングを再確立すると、ピアは自身のすべてのルートを再アドバタイズし、N9K は BGP およびルーティングテーブルでこれらのルートを更新します。ピアから EOR を受信するか、または古いパスタイムアウト（どちらか先に発生した方）を受信すると、N9K はそのピアから残りの古いルートをフラッシュします。ヘルパーモードがない場合、N9K は再起動中のリモートピアから学習したルートを即座にクリアし、トラフィック損失につながる可能性があります。
ステップ 7	（任意） show running-config bgp 例 : <pre>switch(config-router)# show running-config bgp</pre>	BGP の設定を表示します。

	コマンドまたはアクション	目的
ステップ 8	(任意) copy running-config startup-config 例 : <pre>switch(config-router)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、グレースフル リスタートを有効にする例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# graceful-restart
switch(config-router)# graceful-restart restart-time 300
switch(config-router)# copy running-config startup-config
```

拡張 BGP の設定の確認

BGP の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show bgp all [summary] [vrf vrf-name]	すべてのアドレスファミリについて、BGP 情報を表示します。
show bgp convergence [vrf vrf-name]	すべてのアドレスファミリについて、BGP 情報を表示します。
show bgp ip {unicast} [ip-address] community {regex expression [community] [no-advertise] [no-export] [no-export-subconfed]} [vrf vrf-name]	BGP コミュニティと一致する BGP ルートを表示します。
show bgp [vrf vrf-name] ip {unicast} [ip-address] community-list list-name [vrf vrf-name]	BGP コミュニティ リストと一致する BGP ルートを表示します。
show bgp ip {unicast} [ip-address] extcommunity {regex expression generic [non-transitive transitive] aa4:nn [exact-match]} [vrf vrf-name]	BGP 拡張コミュニティと一致する BGP ルートを表示します。
show bgp ip {unicast} [ip-address] extcommunity-list list-name [exact-match] [vrf vrf-name]	BGP 拡張コミュニティ リストと一致する BGP ルートを表示します。

コマンド	目的
show bgp ip {unicast} [ip-address] {dampening dampened-paths [regex expression]} [vrf vrf-name]	BGP ルート ダンプニングの情報を表示します。ルート フラップ ダンプニング情報を消去するには、 clear bgp dampening コマンドを使用します。
show bgp ip {unicast} [ip-address] history-paths [regex expression] [vrf vrf-name]	BGP ルート ヒストリ パスを表示します。
show bgp ip {unicast} [ip-address] filter-list list-name [vrf vrf-name]	BGP フィルタ リストの情報を表示します。
show bgp ip {unicast} [ip-address] neighbors [ip-address] [vrf vrf-name]	BGP ピアの情報を表示します。これらのネイバーを消去するには、 clear bgp neighbors コマンドを使用します。
show bgp ip {unicast} [ip-address] {nexthop nexthop-database} [vrf vrf-name]	BGP ルート ネクスト ホップの情報を表示します。
show bgp paths	BGP パス情報を表示します。
show bgp ip {unicast} [ip-address] policy name [vrf vrf-name]	BGP ポリシー情報を表示します。ポリシー情報を消去するには、 clear bgp policy コマンドを使用します。
show bgp ip {unicast} [ip-address] prefix-list list-name [vrf vrf-name]	プレフィックス リストと一致する BGP ルートを表示します。
show bgp ip {unicast} [ip-address] received-paths [vrf vrf-name]	ソフト再構成用に保管されている BGP パスを表示します。
show bgp ip {unicast} [ip-address] regex expression [vrf vrf-name]	AS_path 正規表現と一致する BGP ルートを表示します。
show bgp ip {unicast} [ip-address] route-map map-name [vrf vrf-name]	ルート マップと一致する BGP ルートを表示します。
show bgp peer-policy name [vrf vrf-name]	BGP ピア ポリシー情報を表示します。
show bgp peer-session name [vrf vrf-name]	BGP ピア セッション情報を表示します。
show bgp peer-template name [vrf vrf-name]	BGP ピア テンプレート情報を表示します。ピア テンプレートのすべてのネイバーを消去するには、 clear bgp peer-template コマンドを使用します。
show bgp process	BGP プロセス情報を表示します。

コマンド	目的
show ip bgp options	BGP のステータスと構成情報を表示します。このコマンドには複数のオプションがあります。詳細については、 Cisco Nexus 3000 シリーズ コマンド リファレンス を参照してください。
show ip mbgp options	BGP のステータスと構成情報を表示します。このコマンドには複数のオプションがあります。詳細については、 Cisco Nexus 3000 シリーズ コマンド リファレンス を参照してください。
show running-configuration bgp	現在実行中の BGP コンフィギュレーションを表示します。

BGP 統計情報の表示

BGP の統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
show bgp ip {unicast} [ip-address] flap-statistics [vrf vrf-name]	BGP ルートフラップの統計情報を表示します。これらの統計情報をクリアするには、 clear bgp flap-statistics コマンドを使用します。
show bgp sessions [vrf vrf-name]	すべてのピアの BGP セッションを表示します。これらの統計情報をクリアするには、 clear bgp sessions コマンドを使用します。
show bgp sessions [vrf vrf-name]	すべてのピアの BGP セッションを表示します。これらの統計情報をクリアするには、 clear bgp sessions コマンドを使用します。
show bgp statistics	BGP 統計情報を表示します。

関連項目

BGP の詳細については、次の項目を参照してください。

- [Route Policy Manager の設定](#) (443 ページ)

その他の参考資料

BGP の実装に関連する詳細情報については、次の項を参照してください。

MIB

MIB	MIB のリンク
BGP4-MIB CISCO-BGP4-MIB	MIB を検索してダウンロードするには、次の MIB ロケータ に移動します。



第 11 章

RIP の設定

この章は、次の項で構成されています。

- [RIP について](#) (381 ページ)
- [RIP のライセンス要件](#) (384 ページ)
- [RIP の前提条件](#) (384 ページ)
- [RIP に関する注意事項と制約事項](#) (384 ページ)
- [RIP パラメータのデフォルト設定](#) (385 ページ)
- [RIP の設定](#) (385 ページ)
- [RIP の設定の確認](#) (400 ページ)
- [RIP 統計情報の表示](#) (400 ページ)
- [RIP の設定例](#) (400 ページ)
- [関連項目](#) (401 ページ)

RIP について

RIP の概要

RIP はユーザデータグラムプロトコル (UDP) データパケットを使用して、小規模なインターネットワークでルーティング情報を交換します。RIPv2 は IPv4 をサポートしています。RIPv2 は RIPv2 プロトコルがサポートするオプションの認証機能を使用します (「[RIPv2 の認証](#)」の項を参照)。

RIP では次の 2 種類のメッセージを使用します。

- 要求：他の RIP 対応ルータからのルート アップデートを要求するためにマルチキャストアドレス 224.0.0.9 に送信されます。
- 応答：デフォルトでは 30 秒間隔で送信されます (「[RIP 設定の検証](#)」の項を参照)。ルータも、要求メッセージの受信後に応答メッセージを送信します。応答メッセージには、RIP ルート テーブル全体が含まれます。RIP ルーティング テーブルが 1 つの応答パケットに収まらない場合、RIP は 1 つの要求に対して複数の応答パケットを送信します。

RIP はルーティング メトリックとして、ホップ カウントを使用します。ホップ カウントは、パケットが宛先に到達するまでに、通過できるルータの数です。直接接続されているネットワークのメトリックは 1 です。到達不能ネットワークのメトリックは 16 です。RIP はこのようにメトリックの範囲が小さいので、大規模なネットワークに適したルーティングプロトコルではありません。

RIPv2 認証

RIP メッセージに認証を設定して、ネットワークでの不正な、または無効なルーティング更新を防止できます。Cisco NX-OS は簡易パスワードまたは MD5 認証ダイジェストをサポートしています。

認証キーのキーチェーン管理を使用することによって、インターフェイスごとに RIP 認証を設定できます。キーチェーン管理によって、MD5 認証ダイジェストまたは単純テキストパスワード認証で使用される認証キーの変更を制御できます。キーチェーンの作成の詳細については、『[Cisco Nexus 3600 Series NX-OS Security Configuration Guide](#)』を参照してください。

MD5 認証ダイジェストを使用するには、ローカル ルータとすべてのリモート RIP ネイバーで共有されるパスワードを設定します。Cisco NX-OS は、メッセージ自体と暗号化されたパスワードに基づいて MD5 の一方方向メッセージダイジェストを作成し、このダイジェストを RIP メッセージ（要求または応答）とともに送信します。受信側の RIP ネイバーは、同じ暗号パスワードを使用して、ダイジェストを検証します。メッセージが変更されていない場合は、計算が一致し、RIP メッセージは有効と見なされます。

MD5 認証ダイジェストの場合はさらに、ネットワークでメッセージが再送されないように、各 RIP メッセージにシーケンス番号が組み込まれます。

Split Horizon

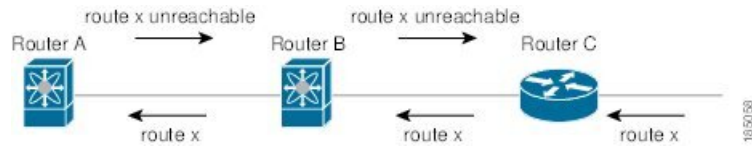
スプリット ホライズンを使用すると、ルートを学習したインターフェイスから RIP がルートをアドバタイズしないようにできます。

スプリット ホライズンは、RIP アップデートおよびクエリー パケットの送信を制御する方法です。インターフェイス上でスプリットホライズンがイネーブルの場合、Cisco NX-OS はそのインターフェイスから学習した宛先にはアップデート パケットを送信しません。この方法でアップデート パケットを制御すると、ルーティング ループの発生する可能性が小さくなります。

ポイズンリバー스를指定してスプリットホライズンを使用すると、ルートを学習したインターフェイス経由では到達不能であると RIP が学習したルートをアドバタイズするように、インターフェイスを設定できます。

次の図に、ポイズンリバー스를イネーブルにしてスプリットホライズンを指定した、RIP ネットワークの例を示します。

図 29: スプリット ホライズン ポイズンリバー스를指定した RIP



ルータ C はルート X について学習し、そのルートをルータ B にアドバタイズします。ルータ B はルート X をルータ A にアドバタイズしますが、ルート X の到達不能アップデートをルータ C に送り返します。

デフォルトでは、スプリットホライズンはすべてのインターフェイスでイネーブルになっています。

ルートのフィルタリング

RIP 対応インターフェイスでルート ポリシーを設定すれば、RIP アップデートをフィルタリングすることができます。Cisco NX-OS は、ルート ポリシーが許可するルートのみでルートテーブルを更新します。

ルート集約

指定したインターフェイスに複数のサマリー集約アドレスを設定できます。ルート集約を使用すると、固有性の強い一連のアドレスをすべての固有アドレスを代表する 1 つのアドレスに置き換えることによって、ルートテーブルを簡素化できます。たとえば、10.1.1.0/24、10.1.2.0/24、および 10.1.3.0/24 というアドレスを 1 つの集約アドレス 10.1.0.0/16 に置き換えることができます。

RIP はルーティング テーブルに含まれている固有性の強いルートが多いほど、固有性の強いルートの最大メトリックと同じメトリックのインターフェイスからのサマリーアドレスをアドバタイズします。



(注) Cisco NX-OS は、自動ルート集約をサポートしていません。

ルートの再配布

RIP を使用すると、スタティックルートや他のプロトコルからのルートを再配布できます。再配布を指定したルート マップを設定して、どのルートが RIP に渡されるかを制御する必要があります。ルート ポリシーを使用すると、宛先、送信元プロトコル、ルート タイプ、ルート タグなどの属性に基づいて、ルートをフィルタリングできます。詳細については、[Route Policy Manager の設定 \(443 ページ\)](#) を参照してください。

RIP ルーティング ドメインにルートを再配布しても、デフォルトでは Cisco NX-OS がそのつど、RIP ルーティング ドメインにデフォルトルートを再配布することはありません。RIP にデフォルトルートを生成し、ルート ポリシーでそのルートを制御できます。

RIP にインポートされたすべてのルートに使用する、デフォルトのメトリックも設定できます。

ロード バランシング

ロードバランシングを使用すると、ルータは、宛先アドレスから等距離内にあるすべてのルータのネットワーク ポートにトラフィックを分散できます。ロードバランシングは、ネットワーク セグメントの使用率を向上させ、有効ネットワーク帯域幅を増加させます。

Cisco NX-OS は、等コスト マルチパス (ECMP) 機能をサポートします。RIP ルート テーブル およびユニキャスト RIB の等コスト パスは最大 16 です。これらのパスの一部または全部でトラフィックのロード バランシングが行われるように、RIP を設定できます。

RIP のハイ アベイラビリティ

Cisco NX-OS は、RIP のステートレス リスタートをサポートします。リブートまたはスーパーバイザ スイッチオーバー後に、Cisco NX-OS が実行コンフィギュレーションを適用し、RIP がただちに要求パケットを送信して、ルーティング テーブルに再入力します。

RIP 仮想化のサポート

Cisco NX-OS は、同一システム上で動作する複数の RIP プロトコル インスタンスをサポートします。RIP は、仮想ルーティングおよび転送 (VRF) インスタンスをサポートします。

RIP のライセンス要件

製品	ライセンス要件
Cisco NX-OS	RIP にライセンスは必要ありません。ライセンス パッケージに含まれていない機能は nx にバンドルされており、無料で提供されます。Cisco NX-OS ライセンス方式の詳細について NX-OS Licensing Guide 』を参照してください。

RIP の前提条件

- RIP をイネーブルにします (「[RIP のネーブル化](#)」セクションを参照)。

RIP に関する注意事項と制約事項

RIP には、次の注意事項および制限事項があります。

- Cisco NX-OS は、RIPv1 をサポートしません。RIPv1 パケットを受信した Cisco NX-OS は、メッセージを記録してパケットをドロップします。
- Cisco NX-OS は、RIPv1 ルータとの隣接関係を確立しません。
- RIP では IPv6 はサポートされていません。

RIP パラメータのデフォルト設定

次の表に、RIP パラメータのデフォルト設定値を示します。

デフォルトの RIP パラメータ

パラメータ	デフォルト
ロード バランシングを行う最大パス数	16
RIP 機能	ディセーブル
スプリット ホライズン	有効 (Enabled)

RIP の設定

RIP のイネーブル化

RIP を設定するには、その前に RIP を有効にする必要があります。

手順の概要

1. **configure terminal**
2. **[no] feature rip**
3. (任意) **show feature**
4. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定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 2	[no] feature rip 例 : <code>switch(config)# feature rip</code>	RIP 機能を有効にします。
ステップ 3	(任意) show feature 例 : <code>switch(config)# show feature</code>	有効および無効にされた機能を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : <code>switch(config)# copy running-config startup-config</code>	この設定変更を保存します。

RIP インスタンスの作成

RIP インスタンスを作成し、そのインスタンスのアドレス ファミリを設定できます。

始める前に

RIP をイネーブルにします（「[RIP のネーブル化](#)」セクションを参照）。

手順の概要

1. **configure terminal**
2. **[no] router rip instance-tag**
3. **address-family ipv4 unicast**
4. (任意) **show ip rip [instance instance-tag] [vrf vrf-name]**
5. (任意) **distance value**
6. (任意) **maximum-paths number**
7. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <code>switch# configure terminal</code> <code>switch(config)#</code>	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 2	[no] router rip instance-tag 例 : switch(config)# router RIP Enterprise switch(config-router)#	<i>instance tag</i> を設定して、新しい RIP インスタンスを作成します。
ステップ 3	address-family ipv4 unicast 例 : switch(config-router)# address-family ipv4 unicast switch(config-router-af)#	この RIP インスタンスのアドレス ファミリを設定し、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 4	(任意) show ip rip [instance instance-tag] [vrf vrf-name] 例 : switch(config-router-af)# show ip rip	すべての RIP インスタンスの RIP 要約情報を表示します。
ステップ 5	(任意) distance value 例 : switch(config-router-af)# distance 30	RIP のアドミニストレーティブ ディスタンスを設定します。範囲は 1 ～ 255 です。デフォルトは 120 です。「 アドミニストレーティブ ディスタンス 」のセクションを参照してください。
ステップ 6	(任意) maximum-paths number 例 : switch(config-router-af)# maximum-paths 6	RIP がルート テーブルで維持する等コストパスの最大数を設定します。有効な範囲は 1 ～ 64 です。デフォルトは 16 です。
ステップ 7	(任意) copy running-config startup-config 例 : switch(config-router-af)# copy running-config startup-config	この設定変更を保存します。

例

次に、IPv4 に対応する RIP インスタンスを作成し、ロード バランシングのための等コスト パス数を設定する例を示します。

```
switch# configure terminal
switch(config)# router rip Enterprise
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# max-paths 10
switch(config-router-af)# copy running-config startup-config
```

RIP インスタンスの再起動

RIP インスタンスを再起動し、インスタンスに関連付けられているすべてのネイバーを削除できます。

RIP インスタンスを再起動し、関連付けられたすべてのネイバーを削除するには、グローバル設定モードで次のコマンドを使用します。

手順の概要

1. **restart rip instance-tag**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	restart rip instance-tag 例 : <pre>switch(config)# restart rip Enterprise</pre>	RIP インスタンスを再起動し、すべてのネイバーを削除します。

インターフェイスでの RIP の設定

始める前に

RIP をイネーブルにします（「[RIP のネーブル化](#)」セクションを参照）。

手順の概要

1. **configure terminal**
2. **interface interface-type slot/port**
3. **ip router rip instance-tag**
4. （任意） **show ip rip [instance instance-tag] interface [interface-type slot/port] [vrf vrf-name] [detail]**
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します
ステップ 2	interface interface-type slot/port 例 :	インターフェイス設定モードを開始します。

	コマンドまたはアクション	目的
	switch(config)# interface ethernet 1/2 switch(config-if)#	
ステップ 3	ip router rip instance-tag 例 : switch(config-if)# ip router rip Enterprise	このインターフェイスを RIP インスタンスに関連付けます。
ステップ 4	(任意) show ip rip [instance instance-tag] interface [interface-type slot/port] [vrf vrf-name] [detail] 例 : switch(config-if)# show ip rip Enterprise ethernet 1/2	インターフェイスの RIP 情報を表示します。
ステップ 5	(任意) copy running-config startup-config 例 : switch(config-if)# copy running-config startup-config	この設定変更を保存します。

例

次に、RIP インスタンスに Ethernet 1/2 インターフェイスを追加する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ip router rip Enterprise
switch(config)# copy running-config startup-config
```

RIP 認証の設定

インターフェイスに RIP パケットの認証を設定できます。

始める前に

RIP をイネーブルにします（「[RIP のネーブル化](#)」セクションを参照）。

認証をイネーブルにする前に、必要に応じてキーチェーンを設定します。キーチェーンの実装の詳細については、『[Cisco Nexus 3600 Series NX-OS Security Configuration Guide](#)』を参照してください。

手順の概要

1. **configure terminal**
2. **interface interface-type slot/port**
3. **ip rip authentication mode {text | md5}**
4. **ip rip authentication key-chain key**

5. (任意) `copy running-config startup-config`

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <code>switch# configure terminal</code> <code>switch(config)#</code>	グローバル設定モードを開始します
ステップ 2	interface interface-type slot/port 例 : <code>switch(config)# interface ethernet 1/2</code> <code>switch(config-if)#</code>	インターフェイス設定モードを開始します。
ステップ 3	ip rip authentication mode {text md5} 例 : <code>switch(config-if)# ip rip authentication mode md5</code>	クリアテキストまたは MD5 認証ダイジェストとして、このインターフェイスにおける RIP 認証タイプを設定します。
ステップ 4	ip rip authentication key-chain key 例 : <code>switch(config-if)# ip rip authentication key-chain RIPKey</code>	このインターフェイス上で RIP に使用する認証キーを設定します。
ステップ 5	(任意) copy running-config startup-config 例 : <code>switch(config-if)# copy running-config startup-config</code>	この設定変更を保存します。

例

次に、キーチェーンを作成し、RIP インターフェイス上で MD5 認証を設定する例を示します。

```
switch# configure terminal
switch(config)# key chain RIPKey
switch(config-keychain)# key 2
switch(config-keychain-key)# accept-lifetime 00:00:00 Jan 01 2000 infinite
switch(config-keychain-key)# send-lifetime 00:00:00 Jan 01 2000 infinite
switch(config-keychain-key)# exit
switch(config-keychain)# exit
switch(config)# interface ethernet 1/2
switch(config-if)# ip rip authentication mode md5
switch(config-if)# ip rip authentication key-chain RIPKey
switch(config-if)# copy running-config startup-config
```

パッシブインターフェイスの設定

インターフェイスを受動モードに設定することによって、ルートを受信するが、ルートアップデータの送信は行わないように RIP インターフェイスを設定できます。

受動モードで RIP インターフェイスを設定するには、インターフェイス設定モードで次のコマンドを使用します。

手順の概要

1. ip rip passive-interface

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	ip rip passive-interface 例 : <pre>switch(config-if)# ip rip passive-interface</pre>	インターフェイスを受動モードに設定します。

ポイズン リバースを指定したスプリット ホライズンの設定

インターフェイスの設定でポイズンリバースをイネーブルにすると、RIP が学習したルートについて、ルートを学習したインターフェイス経由では到達不能であることをアドバタイズできます。

インターフェイス上で、ポイズンリバースを指定してスプリット ホライズンを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. ip rip poison-reverse

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	ip rip poison-reverse 例 : <pre>switch(config-if)# ip rip poison-reverse</pre>	ポイズン リバースを指定してスプリット ホライズンをイネーブルにします。ポイズンリバースを指定したスプリット ホライズンは、デフォルトでディセーブルです。

ルート集約の設定

ルーティング テーブルでサマリー アドレスによって表される集約アドレスを作成できます。Cisco NX-OS は、固有性の強いすべてのルートの中でメトリックが最小のサマリー アドレス メトリックをアドバタイズします。

インターフェイス上でサマリーアドレスを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. **ip rip summary-address ip-prefix/mask-len**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	ip rip summary-address ip-prefix/mask-len 例 : <pre>switch(config-if)# ip rip summary-address 1.1.1.1/32</pre>	IPv4 アドレスに対応する、RIP 用のサマリー アドレスを設定します。

ルートの再配布の設定

別のルーティングプロトコルからのルーティング情報を受け入れて、RIP ネットワークを通じてその情報を再配布するように、RIP を設定できます。再配布されたルートを任意で、デフォルト ルートとして割り当てることができます。

始める前に

RIP を有効にします（「[RIP の有効化](#)」セクションを参照）。

再配布を設定する前に、ルートマップを設定します。ルートマップの設定の詳細については、「[ルート マップの設定](#)」セクションを参照してください。

手順の概要

1. **configure terminal**
2. **router rip instance-tag**
3. **address-family ipv4 unicast**
4. **redistribute {bgp as | direct | {eigrp | isis | ospf | ospfv3 | rip} instance-tag | static} route-map map-name**
5. （任意） **default-information originate [always] [route-map map-name]**
6. （任意） **default-metric value**
7. （任意） **show ip rip route [ip-prefix [longer-prefixes | shorter-prefixes]] [vrf vrf-name] [summary]**

8. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router rip instance-tag 例 : <pre>switch(config)# router rip Enterprise switch(config-router)#</pre>	<i>instance tag</i> を設定して、新しい RIP インスタンスを作成します。
ステップ 3	address-family ipv4 unicast 例 : <pre>switch(config-router)# address-family ipv4 unicast switch(config-router-af)#</pre>	アドレスファミリ コンフィギュレーション モードに入ります。
ステップ 4	redistribute {bgp as direct {eigrp isis ospf ospfv3 rip} instance-tag static} route-map map-name 例 : <pre>switch(config-router-af)# redistribute eigrp 201 route-map RIPmap</pre>	他のプロトコルからのルートを RIP に再配布します。
ステップ 5	(任意) default-information originate [always] [route-map map-name] 例 : <pre>switch(config-router-af)# default-information originate always</pre>	RIP にデフォルト ルートを生成し、必要に応じてルート マップにより制御します。
ステップ 6	(任意) default-metric value 例 : <pre>switch(config-router-af)# default-metric 2</pre>	再配布されたすべてのルートにデフォルトメトリックを設定します。有効な範囲は1～15です。デフォルトは1です。
ステップ 7	(任意) show ip rip route [ip-prefix [longer-prefixes shorter-prefixes]] [vrf vrf-name] [summary] 例 : <pre>switch(config-router-af)# show ip rip route</pre>	RIP のルートを表示します。

	コマンドまたはアクション	目的
ステップ 8	(任意) copy running-config startup-config 例 : <pre>switch(config-router-af)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、EIGRP を RIP に再配布する例を示します。

```
switch# configure terminal
switch(config)# router rip Enterprise
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# redistribute eigrp 201 route-map RIPmap
switch(config-router-af)# copy running-config startup-config
```

Cisco IOS RIP との互換性のため、Cisco NX-OS RIP を設定

Cisco NX-OS RIP を、ルートがアドバタイズされ、処理される方法で Cisco IOS RIP のように動作するよう設定できます。

直接接続されたルートが、Cisco NX-OS RIP ではコスト 1 として処理され、Cisco IOS RIP ではコスト 0 として処理されます。ルートが Cisco NX-OS RIP でアドバタイズされる場合、受信デバイスはすべての受信ルートに +1 の最小のコストを増加し、ルーティング テーブルにルートをインストールします。Cisco IOS RIP において、このコストの増加は送信側ルータで実行され、受信側ルータは変更なしでルートをインストールします。Cisco NX-OS および Cisco IOS デバイスの両方が連携しているときに、この動作の違いにより問題が発生する可能性があります。Cisco IOS RIP など、ルートをアドバタイズし、処理するために、Cisco NX-OS RIP の設定に応じて、次の互換性の問題を回避できます。

始める前に

RIP をイネーブルにします（「[RIP のネーブル化](#)」セクションを参照）。

手順の概要

1. **configure terminal**
2. **router rip instance-tag**
3. **[no] metric direct 0**
4. (任意) **show running-config rip**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router rip instance-tag 例 : <pre>switch(config)# router rip 100 switch(config-router)#</pre>	instance tag を設定して、新しい RIP インスタンスを作成します。インスタンス タグには 100、201、または 20 文字までの英数字を入力できます。
ステップ 3	[no] metric direct 0 例 : <pre>switch(config-router)# metric direct 0</pre>	ルートがアドバタイズされ、処理される方法で Cisco IOS RIP と Cisco NX-OS RIP が互換性を持つようにするため、直接接続するルータすべてをデフォルトであるコスト 1 の代わりにコスト 0 で設定します。 (注) このコマンドは、Cisco IOS デバイスを含む RIP ネットワークに存在するすべての Cisco NX-OS デバイスで設定する必要があります。
ステップ 4	(任意) show running-config rip 例 : <pre>switch(config-router)# show running-config rip</pre>	現在実行中の RIP コンフィギュレーションを表示します。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config-router)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、すべての直接ルートをコスト 0 からコスト 1 に返すことによって、Cisco IOS RIP と Cisco NX-OS RIP の互換性をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# router rip 100
switch(config-router)# no metric direct 0
switch(config-router)# show running-config rip
switch(config-router)# copy running-config startup-config
```

仮想化の設定

複数の RIP インスタンスを設定し、複数の VRF を作成し、同じまたは複数の RIP インスタンスを各 VRF で使用するようにできます。VRF に RIP インターフェイスを割り当てます。



(注) インターフェイスの VRF を設定した後に、インターフェイスの他のすべてのパラメータを設定します。インターフェイスの VRF を設定すると、そのインターフェイスのすべての設定が削除されます。

始める前に

RIP をイネーブルにします（「[RIP のネーブル化](#)」セクションを参照）。

手順の概要

1. **configure terminal**
2. **vrf context vrf-name**
3. **exit**
4. **router rip instance-tag**
5. **vrf vrf-name**
6. (任意) **address-family ipv4 unicast**
7. (任意) **redistribute {bgp as | direct | {eigrp | isis | ospf | ospfv3 | rip} instance-tag | static} route-map map-name**
8. **interface ethernet slot/port**
9. **vrf member vrf-name**
10. **ip-address ip-prefix/length**
11. **ip router rip instance-tag**
12. (任意) **show ip rip [instance instance-tag] interface [interface-type slot/port] [vrf vrf-name]**
13. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	vrf context vrf-name 例 :	新しい VRF を作成し、VRF 設定モードを開始します。

	コマンドまたはアクション	目的
	<code>switch(config)# vrf context RemoteOfficeVRF</code> <code>switch(config-vrf)#</code>	
ステップ 3	exit 例 : <code>switch(config-vrf)# exit</code> <code>switch(config)#</code>	VRF設定モードを終了します。
ステップ 4	router rip instance-tag 例 : <code>switch(config)# router rip Enterprise</code> <code>switch(config-router)#</code>	instance tag を設定して、新しい RIP インスタンスを作成します。
ステップ 5	vrf vrf-name 例 : <code>switch(config-router)# vrf RemoteOfficeVRF</code> <code>switch(config-router-vrf)#</code>	新しい VRF を作成します。
ステップ 6	(任意) address-family ipv4 unicast 例 : <code>switch(config-router-vrf)# address-family ipv4 unicast</code> <code>switch(config-router-vrf-af)#</code>	この RIP インスタンスの VRF アドレス ファミリを設定します。
ステップ 7	(任意) redistribute {bgp as direct {eigrp isis ospf ospfv3 rip} instance-tag static} route-map map-name 例 : <code>switch(config-router-vrf-af)# redistribute eigrp 201 route-map RIPmap</code>	他のプロトコルからのルートを RIP に再配布します。 ルート マップの設定の詳細については、「ルート マップの設定」を参照してください。
ステップ 8	interface ethernet slot/port 例 : <code>switch(config-router-vrf-af)# interface ethernet 1/2</code> <code>switch(config-if)#</code>	インターフェイス設定モードを開始します。
ステップ 9	vrf member vrf-name 例 : <code>switch(config-if)# vrf member RemoteOfficeVRF</code>	このインターフェイスを VRF に追加します。
ステップ 10	ip-address ip-prefix/length 例 : <code>switch(config-if)# ip address 192.0.2.1/16</code>	このインターフェイスの IP アドレスを設定します。 このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 11	ip router rip instance-tag 例 :	このインターフェイスを RIP インスタンスに関連付けます。

	コマンドまたはアクション	目的
	switch(config-if)# ip router rip Enterprise	
ステップ 12	(任意) show ip rip [instance instance-tag] interface [interface-type slot/port] [vrf vrf-name] 例 : <pre>switch(config-if)# show ip rip Enterprise ethernet 1/2</pre>	VRF のインターフェイスに関する RIP 情報を表示します。
ステップ 13	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、VRF を作成して、その VRF にインターフェイスを追加する例を示します。

```
switch# configure terminal
switch(config)# vrf context RemoteOfficeVRF
switch(config-vrf)# exit
switch(config)# router rip Enterprise
switch(config-router)# vrf RemoteOfficeVRF
switch(config-router-vrf)# address-family ipv4 unicast
switch(config-router-vrf-af)# redistribute eigrp 201 route-map RIPmap
switch(config-router-vrf-af)# interface ethernet 1/2
switch(config-if)# vrf member RemoteOfficeVRF
switch(config-if)# ip address 192.0.2.1/16
switch(config-if)# ip router rip Enterprise
switch(config-if)# copy running-config startup-config
```

RIP の調整

ネットワーク要件に適合するように RIP を調整できます。RIP では複数のタイマーを使用して、ルーティングアップデート間隔、ルートが無効になるまでの時間の長さ、およびその他のパラメータを決定します。これらのタイマーを調整すると、インターネットワークのニーズに適合するように、ルーティングプロトコルのパフォーマンスを調整できます。



(注) ネットワーク上のすべての RIP 対応ルータで、RIP タイマーに同じ値を設定する必要があります。

RIP を調整するには、アドレス ファミリ コンフィギュレーション モードで次のオプション コマンドを使用します。

コマンド	目的
timers basic update timeout holddown garbage-collection 例 : <pre>switch(config-router-af)# timers basic 40 120 120 100</pre>	RIP タイマーを秒数で設定します。パラメータは次のとおりです。 • update : 指定できる範囲は5～任意の正の整数。デフォルトは 30 です。 • timeout : ルートの無効を宣言するまでに、Cisco NX-OS が待機する時間。タイムアウト インターバルが終了するまでに、このルートのアップデート情報を Cisco NX-OS が受信しなかった場合、Cisco NX-OS はルートの無効を宣言します。指定できる範囲は1～任意の正の整数です。デフォルトは 180 です。 • holddown : 無効ルートに関するよりよいルート情報を Cisco NX-OS が無視する時間。指定できる範囲は 0 ～任意の正の整数です。デフォルトは 180 です。 • garbage-collection : Cisco NX-OS がルートを無効として表示してから、Cisco NX-OS がそのルートをルーティング テーブルから削除するまでの時間。指定できる範囲は 1 ～任意の正の整数です。デフォルトは 120 です。

RIP を調整するには、インターフェイス コンフィギュレーション モードで次のオプション コマンドを使用します。

コマンド	目的
ip rip metric-offset value 例 : <pre>switch(config-if)# ip rip metric-offset 10</pre>	このインターフェイスで受信する各ルートのメトリックに値を追加します。有効な範囲は 1 ～ 15 です。デフォルトは 1 です。
ip rip route-filter {prefix-list list-name route-map map-name [in out]} 例 : <pre>switch(config-if)# ip rip route-filter route-map InputMap in</pre>	着信または発信 RIP アップデートをフィルタリングするための、ルート マップを指定します。

RIP の設定の確認

RIP の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ip rip instance [<i>instance-tag</i>] [vrf <i>vrf-name</i>]	RIP インスタンスの状態を表示します。
show ip rip [instance <i>instance-tag</i>] interface <i>slot/port</i> detail [vrf <i>vrf-name</i>]	インターフェイスの RIP ステータスを表示します。
show ip rip [instance <i>instance-tag</i>] neighbor [<i>interface-type</i> <i>number</i>] [vrf <i>vrf-name</i>]	RIP ネイバー テーブルを表示します。
show ip rip [instance <i>instance-tag</i>] route [<i>ip-prefix/length</i>] [longer-prefixes shorter-prefixes] [summary] [vrf <i>vrf-name</i>]	RIP ルート テーブルを表示します。
show running-configuration rip	現在実行中の RIP コンフィギュレーションを表示します。

RIP 統計情報の表示

RIP の統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
show ip rip [instance <i>instance-tag</i>] policy statistics redistribute { bgp as direct { eigrp isis ospf ospfv3 rip } [<i>instance-tag</i> static] [vrf <i>vrf-name</i>]	RIP ポリシー統計情報を表示します。
show ip rip [instance <i>instance-tag</i>] statistics <i>interface-type</i> <i>number</i> [vrf <i>vrf-name</i>]	RIP の統計情報を表示します。

clear rip policy statistics redistribute protocol process-tag コマンドを使用して、ポリシー統計情報をクリアします。

clear ip rip statistics コマンドを使用し、して、RIP 統計情報をクリアします。

RIP の設定例

VRF で Enterprise RIP インスタンスを作成し、その RIP インスタンスにイーサネット インターフェイス 1/2 の例を示します。さらに、**ethernet interface 1/2** の認証を設定し、この RIP ドメインに EIGRP を再配布する例も示します

```
vrf context NewVRF
!
feature rip
```



```
router rip Enterprise
  vrf NewVRF
    address-family ipv4 unicast
      redistribute eigrp 201 route-map RIPmap
      maximum-paths 10
!
interface ethernet 1/2
  vrf member NewVRF
  ip address 192.0.2.1/16
  ip router rip Enterprise
  ip rip authentication mode md5
  ip rip authentication key-chain RIPKey
```

関連項目

ルート マップの詳細については、ルート ポリシー マネージャの構成を参照してください。



第 12 章

スタティック ルーティングの設定

この章では、ルータでスタティック ルートとデフォルト ルートを構成する方法について説明します。

この章は、次の項で構成されています。

- [スタティック ルーティングについて \(403 ページ\)](#)
- [スタティック ルーティングの前提条件 \(405 ページ\)](#)
- [注意事項と制約事項 \(406 ページ\)](#)
- [デフォルト設定 \(406 ページ\)](#)
- [スタティック ルーティングの設定 \(406 ページ\)](#)
- [スタティック ルーティングの設定確認 \(409 ページ\)](#)
- [設定：スタティック スタティック ルーティングの例 \(409 ページ\)](#)

スタティック ルーティングについて

ルータは、ユーザーが手動で設定したルート テーブル エントリのルート情報を使用するか、またはダイナミック ルーティング アルゴリズムで計算されたルート情報を使用して、パケットを転送します。

スタティック ルートは、2つのルータ間の明示パスを定義するものであり、自動的にアップデイトされません。ネットワークに変更があった場合は、ユーザーが手動でスタティック ルートを再設定する必要があります。スタティック ルートは、ダイナミック ルートに比べて使用する帯域幅が少なくなります。ルーティング アップデイトの計算や分析に CPU サイクルを使用しません。

必要に応じて、スタティック ルートでダイナミック ルートを補うことができます。スタティック ルートをダイナミック ルーティング アルゴリズムに再配布することはできますが、ダイナミック ルーティング アルゴリズムで計算されたルーティング情報をスタティック ルーティング テーブルに再配布することはできません。

スタティック ルートは、ネットワーク トラフィックが予測可能で、ネットワーク設計が単純な環境で使用します。スタティック ルートはネットワークの変化に対応できないので、大規模でたえず変化しているネットワークでは、スタティック ルートを使用すべきではありません。大部分のネットワークは、ルータ間の通信にダイナミック ルートを使用しますが、特殊な状況

でスタティック ルートを1つか2つ設定する場合があります。スタティック ルートは、最終手段としてのゲートウェイ（ルーティング不能なすべてのパケットの送信先となるデフォルト ルータ）を指定する場合にも便利です。

アドミニストレーティブ ディスタンス

アドミニストレーティブ ディスタンスは、2つの異なるルーティングプロトコルから同じ宛先に、2つ以上のルートが存在する場合に、最適なパスを選択するために、ルータが使用するメトリックです。複数のプロトコルがユニキャスト ルーティング テーブルに同じルートを追加した場合に、アドミニストレーティブ ディスタンスを手がかりに、他のルーティング プロトコル（またはスタティック ルート）ではなく、特定のルーティング プロトコル（またはスタティック ルート）が選択されます。各ルーティング プロトコルは、アドミニストレーティブ ディスタンス値を使用して、信頼性の高い順にプライオリティが与えられます。

スタティック ルートのデフォルトのアドミニストレーティブ ディスタンスは1です。ルータは値の小さいルートが最短であると見なすので、スタティック ルートがダイナミック ルートより優先されます。ダイナミック ルートでスタティック ルートを上書きする場合は、スタティック ルートにアドミニストレーティブ ディスタンスを指定します。たとえば、アドミニストレーティブ ディスタンスが120のダイナミック ルートが2つある場合に、ダイナミック ルートでスタティック ルートを上書きするには、スタティック ルートに120より大きいアドミニストレーティブ ディスタンスを指定します。

直接接続のスタティック ルート

直接接続のスタティック ルートで指定しなければならないのは、出力インターフェイス（あらゆるパケットを宛先ネットワークに送り出すインターフェイス）だけです。ルータは宛先が出力インターフェイスに直接接続されているものと見なし、パケットの宛先をネクスト ホップ アドレスとして使用します。ネクストホップは、ポイントツーポイントインターフェイスの場合に限り、インターフェイスにできます。ブロードキャストインターフェイスの場合は、ネクストホップをIPv4 アドレスにする必要があります。

完全指定のスタティック ルート

完全指定のスタティック ルートでは、出力インターフェイス（あらゆるパケットを宛先ネットワークに送り出すインターフェイス）およびネクスト ホップ アドレスを指定する必要があります。完全指定のスタティック ルートを使用できるのは、出力インターフェイスがマルチアクセスインターフェイスで、ネクストホップ アドレスを特定する必要がある場合です。ネクストホップ アドレスは、指定された出力インターフェイスに直接接続する必要があります。

フローティング スタティック ルート

フローティング スタティック ルートは、ダイナミック ルートをバックアップするためにルータが使用するスタティック ルートです。フローティング スタティック ルートには、バックアップするダイナミック ルートより大きいアドミニストレーティブ ディスタンスを設定する必要

があります。この場合、ルータはフローティング スタティック ルートよりダイナミック ルートを優先させます。フローティング スタティック ルートは、ダイナミック ルートが失われた場合の代用として使用できます。



- (注) デフォルトでは、ルータはダイナミック ルートよりスタティック ルートを優先させます。スタティック ルートの方がダイナミック ルートより、アドミニストレーティブ ディスタンスが小さいからです。

スタティック ルートのリモート ネクスト ホップ

リモート（非直接接続）ネクスト ホップを指定したスタティック ルートの場合、ルータに直接接続されていない隣接ルータのネクストホップアドレスを指定できます。データ転送時に、スタティック ルートにリモート ネクストホップがあると、そのネクスト ホップがユニキャスト ルーティング テーブルで繰り返し使用され、リモート ネクストホップに到達可能な、対応する直接接続のネクストホップ（複数可）が特定されます。

BFD

この機能では、双方向フォワーディング検出（BFD）をサポートします。BFDは、転送パスの障害を高速で検出することを目的にした検出プロトコルです。BFDは2台の隣接デバイス間のサブセカンド障害を検出し、BFD の負荷の一部を、サポートされるモジュール上のデータ プレーンに分散できるため、プロトコル hello メッセージよりも CPU を使いません。

BGP の BFD は eBGP シングルホップ ピアおよび iBGP シングルホップ ピアでサポートされます。BFD を使用している iBGP シングル ホップ ピアの場合、ネイバー コンフィギュレーション モードで `update-source` オプションを構成する必要があります。BFD は、その他の iBGP ピアまたはマルチホップ eBGP ピアでサポートされません。

仮想化のサポート

スタティック ルートは、仮想ルーティングおよび転送（VRF）インスタンスをサポートしています。デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS はユーザーをデフォルトの VRF に配置します。詳細については、「[レイヤ3仮想化の設定](#)」を参照してください。

スタティック ルーティングの前提条件

スタティック ルーティングの前提条件は、次のとおりです。

- スタティック ルートのネクストホップアドレスは到達可能である必要があります。そうでないと、そのスタティック ルートはユニキャスト ルーティング テーブルに追加されません。

注意事項と制約事項

スタティック ルーティング設定時の注意事項および制約事項は、次のとおりです。

- スタティック ルートのネクストホップ アドレスとしてインターフェイスを指定できるのは、GRE トンネルなどのポイントツーポイント インターフェイスの場合に限られます。

デフォルト設定

次の表にスタティック ルーティング パラメータのデフォルト設定を示します。

表 18: デフォルトのスタティック ルーティング パラメータ

パラメータ	デフォルト
アドミニストレーティブ ディスタンス	1

スタティック ルーティングの設定

このセクションは、次のトピックで構成されています。

スタティック ルーティングの設定

ルータ上でスタティック ルートを設定できます。

手順の概要

1. **configure terminal**
2. **ip route** { *ip-prefix* | *ip-addr ip-mask* } {[*next-hop* | *nh-prefix*] |[*interface next-hop* | *nh-prefix*]} [*name nexthop-name*] [*tag tag-value* [*pref*] [*track*] [*vrf*]
3. (任意) **show ip static-route**
4. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	ip route { ip-prefix ip-addr ip-mask } { [next-hop nh-prefix] [interface next-hop nh-prefix] } [name nexthop-name] [tag tag-value [pref] [track] [vrf] } 例 : <pre>switch(config)# ip route 192.0.2.0/8 ethernet 1/2 192.0.2.4</pre>	スタティック ルートおよびこのスタティック ルート用のインターフェイスを設定します。任意でネクストホップアドレスを設定できます。 <i>pref</i> 値で管理上の距離を設定します。範囲は 1 ～ 255 です。デフォルトは 1 です。
ステップ 3	(任意) show ip static-route 例 : <pre>switch(config)# show ip static-route</pre>	スタティック ルート情報を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

例

スタティック ルートの設定例を示します。

```
switch# configure terminal
switch(config)# ip route 192.0.2.0/8 192.0.2.10
switch(config)# copy running-config startup-config
```

no ip static-route コマンドを使用すれば、スタティック ルートを削除できます。

仮想化の設定

VRF でスタティック ルートを設定できます。

手順の概要

1. **configure terminal**
2. **vrf context vrf-name**
3. **ip route { ip-prefix | ip-addr ip-mask } { next-hop | nh-prefix | interface } [tag tag-value [pref]]**
4. (任意) **show ip static-route vrf vrf-name**

5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	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	vrf context vrf-name 例： switch(config)# vrf context StaticVrf	スタティック ルートおよびこのスタティック ルート用のインターフェイスを設定します。任意でネクストホップアドレスを設定できます。 <i>pref</i> 値で管理上の距離を設定します。範囲は1～255です。デフォルトは1です。
ステップ 3	ip route { ip-prefix ip-addr ip-mask } { next-hop nh-prefix interface } [tag tag-value [pref]] 例： switch(config-vrf)# ip route 192.0.2.0/8 ethernet 1/2	スタティック ルートおよびこのスタティック ルート用のインターフェイスを設定します。任意でネクストホップアドレスを設定できます。 <i>pref</i> 値で管理上の距離を設定します。範囲は1～255です。デフォルトは1です。
ステップ 4	(任意) show ip static-route vrf vrf-name 例： switch(config-vrf)# show ip static-route	スタティック ルートの情報を表示します。
ステップ 5	(任意) copy running-config startup-config 例： switch(config-vrf)# copy running-config startup-config	この設定変更を保存します。

例

スタティック ルートの設定例を示します。

```
switch# configure terminal
switch(config)# vrf context StaticVrf
switch(config-vrf)# ip route 192.0.2.0/8 192.0.2.10
switch(config-vrf)# copy running-config startup-config
```


スタティック ルーティングの設定確認

スタティック ルーティングの設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
show ip static-route	設定されているスタティックルートを表示します。

設定：スタティック スタティック ルーティングの例

次に、スタティック ルーティングの設定例を示します。

```
configure terminal
ip route 192.0.2.0/8 192.0.2.10
copy running-config startup-config
```




第 13 章

レイヤ 3 仮想化の設定

この章では、レイヤ 3 仮想化の設定手順について説明します。

この章は、次の項で構成されています。

- [レイヤ 3 仮想化について \(411 ページ\)](#)
- [VRF の注意事項と制約事項 \(414 ページ\)](#)
- [VRF-Lite の注意事項と制限事項 \(415 ページ\)](#)
- [VRF ルート リークの注意事項と制約事項 \(415 ページ\)](#)
- [デフォルト設定 \(416 ページ\)](#)
- [VRF の設定 \(416 ページ\)](#)
- [VRF の設定の確認 \(423 ページ\)](#)
- [VRF の設定例 \(423 ページ\)](#)

レイヤ 3 仮想化について

レイヤ 3 仮想化の概要

Cisco NX-OS は、仮想ルーティングおよび転送 (VRF) インスタンスをサポートしています。各 VRF には、IPv4 に対応するユニキャストおよびマルチキャストルートテーブルを備えた、独立したアドレス空間が 1 つずつあり、他の VRF と無関係にルーティングを決定できます。

ルータごとに、デフォルト VRF および管理 VRF があります。すべてのレイヤ 3 インターフェイスおよびルーティング プロトコルは、ユーザが別の VRF に割り当てない限り、デフォルト VRF に存在します。mgmt0 インターフェイスは、管理 VRF 内に存在します。スイッチは、VRF-Lite 機能を使用して、カスタマー エッジ (CE) スイッチで複数の VRF をサポートします。VRF-Lite によって、サービス プロバイダーは 1 つのインターフェイスを使用して、重複する IP アドレスを持つ複数の仮想プライベート ネットワーク (VPN) をサポートできます。



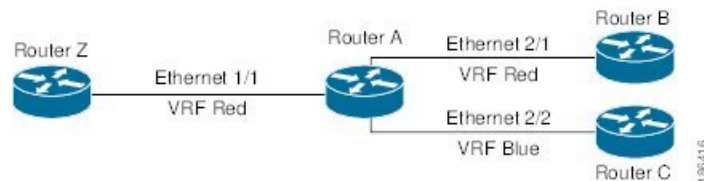
(注) スイッチでは、VPN のサポートのためにマルチプロトコル ラベル スイッチング (MPLS) が使用されません。

VRF およびルーティング

すべてのユニキャストおよびマルチキャストルーティングプロトコルはVRFをサポートします。VRFでルーティングプロトコルを設定する場合は、同じルーティングプロトコルインスタンスの別のVRFのルーティングパラメータに依存しないルーティングパラメータをそのVRFに設定します。

VRFにインターフェイスおよびルーティングプロトコルを割り当てることによって、仮想レイヤ3ネットワークを作成できます。インターフェイスが存在するVRFは1つだけです。次の図は、1つの物理ネットワークが2つのVRFからなる2つの仮想ネットワークに分割されている例を示しています。ルータZ、A、およびBは、VRF Redにあり、1つのアドレスドメインを形成しています。これらのルータは、ルータCが含まないルートアップデートを共有します。ルータCは別のVRFで設定されているからです。

図 30: ネットワーク内の VRF



デフォルトで、着信インターフェイスのVRFを使用して、ルート検索に使用するルーティングテーブルを選択します。ルートポリシーを設定すると、この動作を変更し、Cisco NX-OSが着信パケットに使用するVRFを設定できます。

VRFはVRF間のルートリーク（インポートまたはエクスポート）をサポートします。いくつかの制限が、VRF-Liteのルートリークに適用されます。詳細については、[VRF ルートリーキングの注意事項および制約事項](#)のセクションを参照してください。

VRF-Lite

VRF-Liteの機能によって、サービスプロバイダーは、VPN間で重複したIPアドレスを使用できる複数のVPNをサポートできます。VRF-Liteは入力インターフェイスを使用して異なるVPNのルートを区別し、各VRFに1つまたは複数のレイヤ3インターフェイスを対応付けて仮想パケット転送テーブルを形成します。VRFのインターフェイスは、イーサネットポートなどの物理インターフェイス、またはVLAN SVIなどの論理インターフェイスにすることができますが、レイヤ3インターフェイスは、一度に複数のVRFに属することはできません。



(注) VRF-Liteの実装では、マルチプロトコルラベルスイッチング（MPLS）およびMPLSコントロールプレーンはサポートされません。



(注) VRF-Liteインターフェイスは、レイヤ3インターフェイスである必要があります。

VRF 認識サービス

Cisco NX-OS アーキテクチャの基本的な特徴として、すべての IP ベースの機能が VRF を認識することがあげられます。

次の VRF 認識サービスは、特定の VRF を選択することにより、リモート サーバへの接続や、選択した VRF に基づいた情報のフィルタリングを可能にします。

- AAA
- Call Home
- HSRP
- HTTP
- ライセンス
- NTP
- RADIUS
- Ping と トレースルート
- SSH
- SNMP
- Syslog
- TACACS+
- TFTP
- VRRP

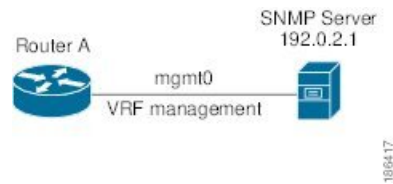
各サービスで VRF サポートを設定する詳細については、各サービスの適切なコンフィギュレーション ガイドを参照してください。

Reachability

到達可能性は、サービスを提供するサーバに到達するために必要なルーティング情報がどの VRF にあるかを示します。たとえば、管理 VRF で到達可能な SNMP サーバを設定できます。ルータにサーバアドレスを設定する場合は、サーバに到達するために Cisco NX-OS が使用すべき VRF も設定します。

次の図は、管理 VRF を介して到達可能な SNMP サーバを示しています。SNMP サーバ ホスト 192.0.2.1 には管理 VRF を使用するよう、ルータ A を設定します。

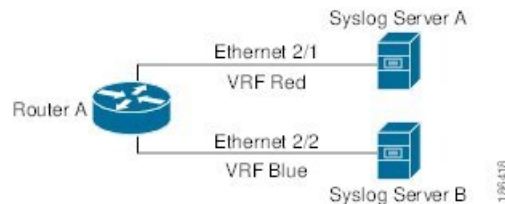
図 31: サービス VRF の到達可能性



フィルタリング

フィルタリングにより、VRF に基づいて VRF 認識サービスに渡される情報のタイプを制限できます。たとえば、Syslog サーバが特定の VRF をサポートするように設定できます。次の図は、それぞれが 1 つの VRF をサポートしている 2 つの syslog サーバを示しています。syslog サーバ A は VRF Red で設定されているので、Cisco NX-OS は VRF Red で生成されたシステムメッセージだけを syslog サーバ A に送信します。

図 32: サービス VRF のフィルタリング

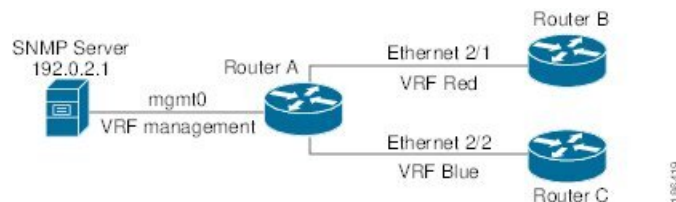


到達可能性とフィルタリングの組み合わせ

VRF 認識サービスの到達可能性とフィルタリングを組み合わせることができます。サービスに接続するために Cisco NX-OS が使用する VRF とともに、そのサービスがサポートする VRF も設定できます。デフォルト VRF でサービスを設定する場合は、任意で、すべての VRF をサポートするようにサービスを設定できます。

次の図は、管理 VRF を介して到達可能な SNMP サーバを示しています。たとえば、SNMP サーバが VRF Red からの SNMP 通知だけをサポートするように設定できます。

図 33: サービス VRF の到達可能性とフィルタリング



VRF の注意事項と制約事項

VRF には VRF Lite のシナリオにおいて次の設定の注意事項と制約事項があります:

- インターフェイスを既存の VRF のメンバにすると、Cisco NX-OS はあらゆるレイヤ 3 設定を削除します。VRF にインターフェイスを追加したあとで、すべてのレイヤ 3 パラメータを設定する必要があります。
- 管理 VRF に `mgmt0` インターフェイスを追加し、そのあとで `mgmt0` の IP アドレスおよびその他のパラメータを設定します。
- VRF が存在しないうちに VRF のインターフェイスを設定した場合は、VRF を作成するまで、そのインターフェイスは運用上のダウンになります。
- Cisco NX-OS はデフォルトで、デフォルトと管理 VRF を作成します。`mgmt0` は管理 VRF のメンバにする必要があります。
- **write erase boot** コマンドを実行しても、管理 VRF の設定は削除されません。**write erase** コマンドを使用してから **write erase boot** コマンドを使用する必要があります。

VRF-Lite の注意事項と制限事項

VRF-lite には、次の注意事項と制限事項があります。

- VRF-lite を備えたスイッチは、各 VRF に対してそれぞれ、グローバル ルーティング テーブルとは異なる IP ルーティング テーブルを持ちます。
- VRF-lite が異なる VRF テーブルを使用するため、同じ IP アドレスを再利用できます。別々の VPN では IP アドレスの重複が許可されます。
- VRF-Lite では、一部の MPLS-VRF 機能（ラベル交換、またはラベル付きパケット）がサポートされていません。
- 複数の仮想レイヤ 3 インターフェイスを VRF-lite スイッチに接続できます。
- スイッチでは、物理ポートか VLAN SVI、またはその両方の組み合わせを使用して、VRF を設定できます。SVI は、アクセス ポートまたはトランク ポートで接続できます。
- VRF-lite は、BGP、スタティック ルーティングをサポートします。
- VRF-lite は、Enhanced Interior Gateway Routing Protocol (EIGRP) をサポートしません。
- VRF-Lite は、パケット スイッチング レートに影響しません。
- マルチキャストを同時に同一のレイヤ 3 インターフェイス上に設定することはできません。

VRF ルート リークの注意事項と制約事項

VRF ルート リークには次の注意事項と制約事項があります。

- ルート リークはデフォルト以外の 2 つの VRF 間でサポートされます。また、デフォルト VRF と任意の他の VRF 間でもサポートされます。
- デフォルト VRF へのルート リークは、グローバル VRF であるため使用できません。
- 指定した IP アドレスにマッチするルート マップのフィルタを使用して、特定のルートに対してルート リークを制限できます。
- デフォルトでは、リークできる IP プレフィックスの最大数は 1000 ルートに設定されています。この数値は 0 から 1000 までの任意の値に設定できます。
- VRF ルート リークには Enterprise ライセンスが必要で、BGP をイネーブルにする必要があります。

デフォルト設定

次の表は、VRF パラメータのデフォルト設定をまとめたものです。

表 19: デフォルトの VRF パラメータ

パラメータ	デフォルト
設定されている VRF	デフォルト、管理
ルーティング コンテキスト	デフォルト VRF

VRF の設定

VRF の作成

スイッチに VRF を作成できます。

手順の概要

1. **configure terminal**
2. **vrf context name**
3. **ip route { ip-prefix | ip-addr ip-mask } {[next-hop | nh-prefix] | [interface next-hop | nh-prefix]} [tag tag-value [pref]]**
4. (任意) **show vrf [vrf-name]**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	vrf context name 例 : switch(config)# vrf context Enterprise switch(config-vrf)#	新しい VRF を作成し、VRF 設定モードを開始します。 name は、32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
ステップ 3	ip route { ip-prefix ip-addr ip-mask } {[next-hop nh-prefix]} [tag tag-value [pref] 例 : switch(config-vrf)# ip route 192.0.2.0/8 ethernet 1/2 192.0.2.4	スタティック ルートおよびこのスタティック ルート用のインターフェイスを設定します。任意でネクスト ホップ アドレスを設定できます。 preference 値でアドミニストレーティブディスタンスを設定します。範囲は 1 ～ 255 です。デフォルトは 1 です。
ステップ 4	（任意） show vrf [vrf-name] 例 : switch(config-vrf)# show vrf Enterprise	VRF 情報を表示します。
ステップ 5	（任意） copy running-config startup-config 例 : switch(config-vrf)# copy running-config startup-config	この設定変更を保存します。

例

VRF および関連する設定を削除するには、**no vrf context** コマンドを使用します。

コマンド	目的
no vrf context name 例 : switch(config)# no vrf context Enterprise	VRF および関連するすべての設定を削除します。

グローバル設定モードで使用できるコマンドはすべて、VRF 設定モードでも使用できます。

次に、VRF を作成し、VRF にスタティック ルートを追加する例を示します。

```
switch# configure terminal
switch(config)# vrf context Enterprise
switch(config-vrf)# ip route 192.0.2.0/8 ethernet 1/2
switch(config-vrf)# exit
switch(config)# copy running-config startup-config
```

インターフェイスへの VRF メンバーシップの割当て

インターフェイスを VRF のメンバにできます。

始める前に

VRF 用のインターフェイスを設定したあとで、インターフェイスに IP アドレスを割り当てます。

手順の概要

1. **configure terminal**
2. **interface interface-type slot/port**
3. **vrf member vrf-name**
4. **ip address ip-prefix/length**
5. **show vrf vrf-name interface interface-type number**
6. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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 interface-type slot/port 例 : switch(config)# interface ethernet 1/2 switch(config-if)#	インターフェイス設定モードを開始します。
ステップ 3	vrf member vrf-name 例 : switch(config-if)# vrf member RemoteOfficeVRF	このインターフェイスを VRF に追加します。
ステップ 4	ip address ip-prefix/length 例 : switch(config-if)# ip address 192.0.2.1/16	このインターフェイスの IP アドレスを設定します。 このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。

	コマンドまたはアクション	目的
ステップ 5	show vrf vrf-name interface interface-type number 例 : <pre>switch(config-if)# show vrf Enterprise interface ethernet 1/2</pre>	VRF 情報を表示します。
ステップ 6	copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、VRF にインターフェイスを追加する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# vrf member RemoteOfficeVRF
switch(config-if)# ip address 192.0.2.1/16
switch(config-if)# copy running-config startup-config
```

ルーティング プロトコル用の VRF パラメータの設定

1 つまたは複数の VRF にルーティング プロトコルを関連付けることができます。ルーティング プロトコルに関する VRF の設定については、該当する章を参照してください。ここでは、詳細な設定手順の例として、OSPFv2 プロトコルを使用します。

手順の概要

1. **configure terminal**
2. **router ospf instance-tag**
3. **vrf vrf-name**
4. (任意) **maximum-paths paths**
5. **interface interface-type slot/port**
6. **vrf member vrf-name**
7. **ip address ip-prefix/length**
8. **ip router ospf instance-tag area area-id**
9. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	router ospf instance-tag 例 : switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	vrf vrf-name 例 : switch(config-router)# vrf RemoteOfficeVRF switch(config-router-vrf)#	VRF 設定モードを開始します。
ステップ 4	(任意) maximum-paths paths 例 : switch(config-router-vrf)# maximum-paths 4	この VRF のルート テーブル内の宛先への、同じ OSPFv2 パスの最大数を設定します。ロード バランシングに使用されます。
ステップ 5	interface interface-type slot/port 例 : switch(config)# interface ethernet 1/2 switch(config-if)#	インターフェイス設定モードを開始します。
ステップ 6	vrf member vrf-name 例 : switch(config-if)# vrf member RemoteOfficeVRF	このインターフェイスを VRF に追加します。
ステップ 7	ip address ip-prefix/length 例 : switch(config-if)# ip address 192.0.2.1/16	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 8	ip router ospf instance-tag area area-id 例 : switch(config-if)# ip router ospf 201 area 0	このインターフェイスを OSPFv2 インスタンスおよび設定エリアに割り当てます。
ステップ 9	(任意) copy running-config startup-config 例 : switch(config-if)# copy running-config startup-config	この設定変更を保存します。

例

次に、VRF を作成して、その VRF にインターフェイスを追加する例を示します。

```
switch# configure terminal
switch(config)# vrf context RemoteOfficeVRF
switch(config-vrf)# exit
switch(config)# router ospf 201
switch(config-router)# vrf RemoteOfficeVRF
switch(config-router-vrf)# maximum-paths 4
switch(config-router-vrf)# interface ethernet 1/2
switch(config-if)# vrf member RemoteOfficeVRF
switch(config-if)# ip address 192.0.2.1/16
switch(config-if)# ip router ospf 201 area 0
switch(config-if)# exit
switch(config)# copy running-config startup-config
```

VRF 認識サービスの設定

VRF 認識サービスの到達可能性とフィルタリングを設定できます。VRF 用サービスの設定手順を扱っている、該当する章またはコンフィギュレーションガイドへのリンクについては、[VRF 認識サービス](#)のセクションを参照してください。ここでは、サービスの詳細な設定手順の例として、SNMP および IP ドメイン リストを使用します。

手順の概要

1. **configure terminal**
2. **snmp-server host ip-address [filter-vrf vrf-name] [use-vrf vrf-name]**
3. **vrf context vrf-name**
4. **ip domain-list domain-name [all-vrfs][use-vrf vrf-name]**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	snmp-server host ip-address [filter-vrf vrf-name] [use-vrf vrf-name] 例 : <pre>switch(config)# snmp-server host 192.0.2.1 use-vrf Red</pre>	グローバル SNMP サーバを設定し、サービスに到達するために Cisco NX-OS が使用する VRF を設定します。選択した VRF からこのサーバへの情報をフィルタリングするには、 filter-vrf キーワードを使用します。

	コマンドまたはアクション	目的
ステップ 3	vrf context vrf-name 例 : <pre>switch(config)# vrf context Blue switch(config-vrf)#</pre>	新しい VRF を作成します。
ステップ 4	ip domain-list domain-name [all-vrfs][use-vrf vrf-name] 例 : <pre>switch(config-vrf)# ip domain-list List all-vrfs use-vrf Blue</pre>	VRF でドメインリストを設定し、必要に応じて、リスト内のドメイン名に到達するために Cisco NX-OS が使用する VRF を設定します。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config-vrf)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次の例は、VRF Red 上の到達可能な SNMP ホスト 192.0.2.1 に、すべての VRF の SNMP 情報を送信する方法を示しています。

```
switch# configure terminal
switch(config)# snmp-server host 192.0.2.1 for-all-vrfs use-vrf Red
switch(config)# copy running-config startup-config
```

次に、VRF Red で到達可能な SNMP ホスト 192.0.2.12 に対して、VRF Blue の SNMP 情報をフィルタリングする例を示します。

```
switch# configure terminal
switch(config)# vrf definition Blue
switch(config-vrf)# snmp-server host 192.0.2.12 use-vrf Red
switch(config)# copy running-config startup-config
```

VRF スコープの設定

すべての EXEC コマンド (**show** コマンドなど) には、対応する VRF スコープを設定できます。VRF スコープを設定すると、EXEC コマンド出力のスコープが設定された VRF に自動的に限定されます。このスコープは、一部の EXEC コマンドで利用できる VRF キーワードによって上書きできます。

VRF スコープを設定するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
routing-context vrf vrf-name 例 : <pre>switch# routing-context vrf redswitch%red#</pre>	すべての EXEC コマンドに対応するルーティング コンテキストを設定します。デフォルトのルーティング コンテキストはデフォルト VRF です。

デフォルトの VRF スコープに戻すには、EXEC モードで次のコマンドを使用します。

コマンド	目的
routing-context vrf default 例 : <pre>switch# routing-context vrf default</pre>	デフォルトのルーティングコンテキストを設定します。

VRF の設定の確認

VRF の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show vrf [vrf-name]	すべてまたは 1 つの VRF の情報を表示します。
show vrf [vrf-name] detail	すべてまたは 1 つの VRF の詳細情報を表示します。
show vrf [vrf-name] [interface interface-type slot/port]	インターフェイスの VRF ステータスを表示します。

VRF の設定例

次に、VRF Red を設定して、その VRF に SNMP サーバを追加し、VRF Red に OSPF インスタンスを追加する例を示します。

```
vrf context Red
snmp-server host 192.0.2.12 use-vrf Red
router ospf 201
interface ethernet 1/2

vrf member Red
ip address 192.0.2.1/16
ip router ospf 201 area 0
```

次に、VRF Red および Blue を設定し、各 VRF に OSPF インスタンスを追加して、各 OSPF インスタンスの SNMP コンテキストを作成する例を示します。

```
vrf context Red
vrf context Blue
```

```

feature ospf
router ospf Lab
vrf Red
router ospf Production
vrf Blue

interface ethernet 1/2
vrf member Red
ip address 192.0.2.1/16
ip router ospf Lab area 0
no shutdown

interface ethernet 10/2
vrf member Blue
ip address 192.0.2.1/16
ip router ospf Production area 0
no shutdown

snmp-server user admin network-admin auth md5 nbv-12345
snmp-server community public ro

```

各 VRF の SNMP コンテキストの作成

```

snmp-server context lab instance Lab vrf Red
snmp-server context production instance Production vrf Blue

```

この前の例で、VRF Red の OSPF インスタンス Lab の OSPF-MIB 値にアクセスするには、SNMP コンテキスト **lab** を使用します。

次に、デフォルト以外の 2 つの VRF 間、およびデフォルト VRF からデフォルト以外の VRF にルート リークを設定する例を示します。

```

feature bgp
vrf context Green
ip route 33.33.33.33/32 35.35.1.254
address-family ipv4 unicast
route-target import 3:3
route-target export 2:2
export map test
import map test
import vrf default map test
interface Ethernet1/7

vrf member Green
ip address 35.35.1.2/24
vrf context Shared
ip route 44.44.44.44/32 45.45.1.254

address-family ipv4 unicast
route-target import 1:1
route-target import 2:2
route-target export 3:3
export map test
import map test
import vrf default map test
interface Ethernet1/11
vrf member Shared
ip address 45.45.1.2/24
router bgp 100

address-family ipv4 unicast
redistribute static route-map test
vrf Green
address-family ipv4 unicast

```



```

redistribute static route-map test
vrf Shared
address-family ipv4 unicast
redistribute static route-map test
ip prefix-list test seq 5 permit 0.0.0.0/0 le 32
route-map test permit 10
match ip address prefix-list test
ip route 100.100.100.100/32 55.55.55.1

nexus# show ip route vrf all
IP Route Table for VRF "default"
 '*' denotes best ucast next-hop
  *** denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]
 '%<string>' in via output denotes VRF <string>
55.55.55.0/24, ubest/mbest: 1/0, attached
*via 55.55.55.5, Lo0, [0/0], 00:07:59, direct
55.55.55.5/32, ubest/mbest: 1/0, attached
*via 55.55.55.5, Lo0, [0/0], 00:07:59, local
100.100.100.100/32, ubest/mbest: 1/0
*via 55.55.55.1, [1/0], 00:07:42, static

IP Route Table for VRF "management"
 '*' denotes best ucast next-hop
  *** denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]
 '%<string>' in via output denotes VRF <string>
0.0.0.0/0, ubest/mbest: 1/0
*via 10.29.176.1, [1/0], 12:53:54, static
10.29.176.0/24, ubest/mbest: 1/0, attached
*via 10.29.176.233, mgmt0, [0/0], 13:11:57, direct
10.29.176.233/32, ubest/mbest: 1/0, attached
*via 10.29.176.233, mgmt0, [0/0], 13:11:57, local

IP Route Table for VRF "Green"
 '*' denotes best ucast next-hop
  *** denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]
 '%<string>' in via output denotes VRF <string>
33.33.33.33/32, ubest/mbest: 1/0
*via 35.35.1.254, [1/0], 00:23:44, static
35.35.1.0/24, ubest/mbest: 1/0, attached
*via 35.35.1.2, Eth1/7, [0/0], 00:26:46, direct
35.35.1.2/32, ubest/mbest: 1/0, attached
*via 35.35.1.2, Eth1/7, [0/0], 00:26:46, local
44.44.44.44/32, ubest/mbest: 1/0
*via 45.45.1.254%Shared, [20/0], 00:12:08, bgp-100, external, tag 100
100.100.100.100/32, ubest/mbest: 1/0
*via 55.55.55.1%default, [20/0], 00:07:41, bgp-100, external, tag 100

IP Route Table for VRF "Shared"
 '*' denotes best ucast next-hop
  *** denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]
 '%<string>' in via output denotes VRF <string>
33.33.33.33/32, ubest/mbest: 1/0
*via 35.35.1.254%Green, [20/0], 00:12:34, bgp-100, external, tag 100
44.44.44.44/32, ubest/mbest: 1/0
*via 45.45.1.254, [1/0], 00:23:16, static
45.45.1.0/24, ubest/mbest: 1/0, attached
*via 45.45.1.2, Eth1/11, [0/0], 00:25:53, direct
45.45.1.2/32, ubest/mbest: 1/0, attached
*via 45.45.1.2, Eth1/11, [0/0], 00:25:53, local
100.100.100.100/32, ubest/mbest: 1/0

```

```
*via 55.55.55.1%default, [20/0], 00:07:41, bgp-100, external, tag 100
nexus(config)#
```



第 14 章

ユニキャスト RIB および FIB の設定

この章では、Cisco Nexus スイッチのユニキャストルーティング情報ベース（RIB）および転送情報ベース（FIB）のルートを設定し、管理する方法について説明します。

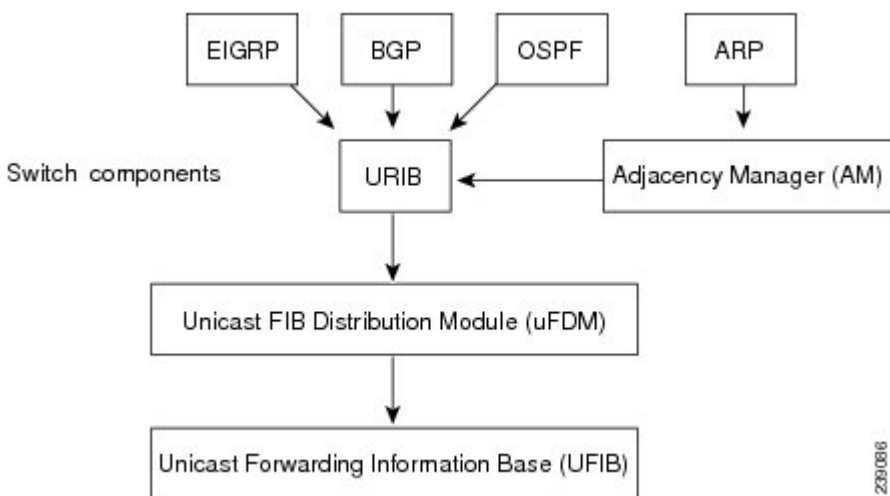
この章は、次の項で構成されています。

- [ユニキャスト RIB および FIB について（427 ページ）](#)
- [ユニキャスト RIB および FIB の管理（429 ページ）](#)
- [ユニキャスト RIB および FIB の確認（440 ページ）](#)

ユニキャスト RIB および FIB について

ユニキャスト RIB（IPv4 RIB）および FIB は、次の図に示すように、Cisco NX-OS の転送アーキテクチャの一部です。

図 34 : Cisco NX-OS 転送アーキテクチャ



ユニキャスト RIB は、直接接続のルート、スタティックルート、ダイナミックユニキャストルーティングプロトコルで検出されたルートを含むルーティングテーブルを維持しています。また、アドレス解決プロトコル（ARP）などの送信元から、隣接情報を収集します。ユニキャスト

スト RIB は、ルートに最適なネクストホップを決定し、さらにユニキャスト FIB 分散モジュール (FDM) のサービスを使用して、ユニキャスト転送情報ベース (FIB) にデータを入力します。

各ダイナミック ルーティング プロトコルは、タイムアウトしたあらゆるルートについて、ユニキャスト RIB を更新する必要があります。その後、ユニキャスト RIB はそのルートを削除し、そのルートに最適なネクストホップを再計算します (代わりに使用できるパスがある場合)。

レイヤ 3 整合性チェッカー

まれな事例として、各モジュールのユニキャスト RIB と FIB の間に不整合が発生することがあります。Cisco NX-OS は、レイヤ 3 整合性チェッカーをサポートします。この機能は、各インターフェイス モジュールのユニキャスト IPv4 RIB と FIB の間の不整合を検出します。不整合には次のようなものがあります。

- 欠落したプレフィックス
- 余分なプレフィックス
- ネクストホップ アドレスの誤り
- ARP またはネイバー探索 (ND) キャッシュ内の不正なレイヤ 2 リライト文字列

レイヤ 3 整合性チェッカーは、FIB のエントリと隣接マネージャ (AM) から取得した最新の隣接情報を比較し、不整合があれば記録します。次に整合性チェッカーは、ユニキャスト RIB のプレフィックスをモジュールの FIB と比較し、不整合があればログに記録します。「[レイヤ 3 整合性チェッカーのトリガー](#)」の項を参照してください。

不整合は手動で解消できます。「[FIB 内の転送情報の消去](#)」の項を参照してください。

FIB テーブル

次に、スイッチが通常の転送モードで設定されている場合の Cisco Nexus 3500 プラットフォーム スイッチのユニキャスト ルーティング テーブルの容量を示します。

- ユニキャスト ルーティング ホスト テーブル = 64,000 ハッシュ テーブル エントリ
- ユニキャスト ルーティング LPM テーブル = 16,000 TCAM エントリ
- ECMP メンバー テーブル サイズ : 16,000 エントリ

次に、スイッチがワープ モードで設定されている場合の Cisco Nexus 3500 プラットフォーム スイッチのユニキャスト ルーティング テーブルの容量を示します。

- L3 ユニキャスト ホスト テーブル = 8000 TCAM エントリ
- L3 ユニキャスト LPM テーブル = 4000 TCAM エントリ



(注) ECMP はワープ モードではサポートされません。



(注) ワープ モードでは、2 つの等コスト パスが RIB で受信されると、パスの 1 つがハードウェアにインストールされます。ルーティングプロトコル構成で、最大パスを 1 に構成することをお勧めします。

仮想化のサポート

ユニキャスト RIB および FIB は、仮想ルーティングおよび転送 (VRF) インスタンスをサポートします。詳細については、「[レイヤ 3 仮想化の設定](#)」を参照してください。

ユニキャスト RIB および FIB の管理



(注) Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合がありますので注意してください。

モジュールの FIB 情報の表示

スイッチの FIB 情報を表示できます。

手順の詳細

スイッチの FIB 情報を表示するには、任意のモードで次のコマンドを使用します。

コマンド	目的
show ip fib adjacency 例 : <pre>switch# show ip fib adjacency</pre>	FIB の隣接情報を表示します。
show forwarding ipv4 adjacency 例 : <pre>switch# show forwarding ipv4 adjacency</pre>	IPv4 の隣接情報を表示します。
show ip fib interfaces 例 : <pre>switch# show ip fib interfaces</pre>	IPv4 の FIB インターフェイス情報を表示します。

コマンド	目的
show ip fib route 例 : <pre>switch# show ip fib route</pre>	IPv4 のルート テーブルを表示します。
show forwarding ipv4 route 例 : <pre>switch# show forwarding ipv4 route</pre>	IPv4 のルート テーブルを表示します。

次に、スイッチの FIB の内容を表示する例を示します。

```
switch# show ip fib route
```

```
IPv4 routes for table default/base
```

```

-----+-----+-----
Prefix | Next-hop | Interface
-----+-----+-----
0.0.0.0/32 Drop Null0
255.255.255.255/32 Receive sup-eth1

```

ユニキャスト FIB でのロードシェアリングの設定

OSPF（Open Shortest Path First）などのダイナミック ルーティング プロトコルは、等コスト マルチパス（ECMP）によるロードシェアリングをサポートしています。ルーティング プロトコルは、そのプロトコルに設定されたメトリックに基づいて最適なルートを決定制し、そのプロトコルに設定された最大数までのパスをユニキャスト RIB に組み込みます。ユニキャスト RIB は、RIB に含まれるすべてのルーティング プロトコル パスのアドミニストレーティブ ディスタンスを比較し、ルーティング プロトコルによって組み込まれたすべてのパス セットから最適なパス セットを選択します。ユニキャスト RIB は、この最適なパス セットを FIB に組み込み、フォワーディング プレーンで使用できるようにします。

フォワーディング プレーンは、ロードシェアリングのアルゴリズムを使用して、FIB に組み込まれたパスのいずれかを選択し、それを特定のデータ パケットに使用します。

ロードシェアリングの次の設定項目をグローバルに設定できます。

- ロードシェアリング モード：宛先のアドレスとポート、または送信元と宛先のアドレスとポートに基づいて、最適なパスを選択します。
- 汎用 ID：ハッシュ アルゴリズムのランダム シードを設定します。汎用 ID を設定する必要はありません。ユーザが設定しなかった場合は、Cisco NX-OS が汎用 ID を選択します。

ロードシェアリングでは、特定のフローに含まれるすべてのパケットに対して s srkuyo;pame パスが使用されます。フローは、ユーザが設定したロードシェアリング方式によって定義されます。たとえば、送信元/宛先のロードシェアリングを設定すると、送信元 IP アドレスと宛先 IP アドレスのペアが同じであるすべてのパケットが同じパスをたどります。

ユニキャスト FIB のロード シェアリング アルゴリズムを設定するには、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。

コマンド	目的
ip load-sharing address {destination port destination source-destination [port source-destination] source } hardware lb-keyshift value lb-2nd-heir-keyshift value [universal-id seed] [rotate rotate] [concatenation] 例 : <pre>ip load-sharing address source-destination port source-destination hardware lb-keyshift 1 lb-2nd-hier-keyshift 10</pre>	

コマンド	目的
	データ トラフィックに対するユニキャスト FIB のロードシェアリング アルゴリズムを設定します。 Cisco NX-OS リリース 10.3(3)F 以降では、Cisco Nexus 9600-R/RX ラインカードでのみ、IHB_ECMP_LB_KEY_CFG テーブルの次のパラメータをサポートするために hardware キーワードが追加されています。 • lb-keyshift : ロードバランシングの ECMP_LB_KEY_SHIFT 値を設定します。指定できる範囲は、1 ～ 10 です。 • lb-2nd-hier-keyshift : ロードバランシングの ECMP_2ND_HIER_LB_KEY_SHIFT 値を設定します。指定できる範囲は、1 ～ 10 です。 次のオプションは、すべての IP ロードシェアリング設定で使用できます。 • universal-id オプションは、ハッシュ アルゴリズムのランダム シードを設定することにより、フローをあるリンクから別のリンクにシフトします。 汎用 ID を設定する必要はありません。ユーザが設定しなかった場合は、Cisco NX-OS が汎用 ID を選択します。universal-id の範囲は 1 ～ 4294967295 です。 • rotate オプションを使用すると、ハッシュ アルゴリズムは、リンク ピッキングの選択をローテーションさせます。これは、ネットワーク内のすべてのノードが同じリンクを継続的に選択しないようにするためです。これは、ハッシュ アルゴリズムのビットパターンに影響を与えることによって機能します。このオプションは、あるリンクから別のリンクにフローをシフトし、最初の ECMP レベルからすでにロードバランシング（極性化）されているトラフィックのロードバランシングを複数のリンク間で行います。 rotate 値を指定すると、64 ビットのストリームが、循環回転でのそのビット位置から解釈されます。rotate 値の範囲は 1 ～ 63 で、デフォルトは 32 です。 (注) 多層レイヤ3 トポロジでは、極性が発生する可能性があります。極性を回避するには、トポロジの各層で異なる循環ビットを使用します。 (注) ポートチャネルの rotation 値を設定するには、port-channel load-balance src-dst ip-l4port rotate rotate コマンドを使用しま

コマンド	目的
	す。このコマンドの詳細については、『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide』を参照してください。 • concatenation オプションを使用すると、ECMP のハッシュ タグ値とポート チャネルのハッシュ タグ値がひとつに結合され、より強力な 64 ビットのハッシュを使用できるようになります。このオプションを使用しない場合、ECMP のロード バランシング およびポート チャネルのロード バランシングを個別に制御できます。デフォルトではディセーブルになっています。

ハッシュ オフセットの構成

多層 ECMP セッションで ECMP 極性を回避するには、各層で異なる ECMP ハッシュ オフセットを構成する必要があります。リリース 6.0(2)U5(1) 以降、ECMP ハッシュ 連結の新しい CLI が導入され、16 の ECMP パスでトラフィックを均等に分散できます。更新された CLI サポートは、Cisco Nexus 3000 シリーズ スイッチではなく、Cisco Nexus 3100 プラットフォーム スイッチに存在します。ハッシュ オフセットは、非連結モードでは <0-15> の範囲、連結モードでは <0-63> の範囲で構成できます。

連結モードで、ハッシュ オフセットが 0 に設定されていて、連結が設定されている場合、**show running-config** コマンドは **hardware ecmp hash-offset 0 connotationation** を表示します。ハッシュ オフセットは値ごとにプログラムされます。ダウングレード時に、連結が構成されている場合、CAP チェックは構成を削除するように求めます。

非連結モードでは、ハッシュ オフセットが 0 に構成されて連結がリセットされた場合、**show running-config** コマンドは **hardware ecmp hash-offset 0** を表示しません。ハッシュ オフセット値が 0 ～ 15 の範囲にある場合、ハッシュ オフセットは値に従ってプログラムされます。ハッシュ オフセットでは、値が 16 ～ 63 の範囲の場合、CLI エラーが表示されます（非連結モードでは、0 ～ 15 の範囲のハッシュ オフセットがサポートされます）。

show running-config のハッシュ オフセットは、構成された値に従って表示されます。

ECMP ハッシュ オフセットを構成するには、グローバル構成モードで以下のコマンドを使用します。

コマンド	目的
# hardware ecmp hash-offset ?	ECMP ハッシュ オフセットを構成します。範囲は 0 ～ 63 です。範囲 <0-15> のハッシュ オフセットは、非連結モード用です。範囲 <0-63> のハッシュ オフセットは、連結モード用です。

コマンド	目的
#hardware ecmp hash-offset number 例 : <pre>switch(config)# hardware ecmp hash-offset 5</pre>	非連結モードで ECMP ハッシュオフセットを構成します。範囲は 0 ～ 15 です。デフォルト値は 0 です。
#hardware ecmp hash-offset <0-63> concatenation 例: <pre>switch(config)# hardware ecmp hash-offset 63 concatenation</pre>	連結モードで ECMP ハッシュオフセットを構成します。 (注) 連結サポートは、Cisco Nexus 3000 シリーズ スイッチではなく、Cisco Nexus 3100 プラットフォーム スイッチにあります。この CLI は Cisco Nexus 3000 シリーズ スイッチでエラーを生成します。

hardware ecmp hash-offset コマンドを使用して設定された ECMP ハッシュ オフセットを、ip load-sharing address コマンドを使用して設定されたさまざまなユニバーサル ID とともに使用して、負荷分散アルゴリズムでさまざまなハッシュ結果を生成できます。

ハッシュ多項式の構成

リリース 6.0(2)U5(1) 以降、CRC 構成に新しい CLI が追加されました。

コマンド	目的
switch# config t	コンフィギュレーション モードを開始します。
switch(config)# hardware ecmp ? hash-offset Configure hash offsethash-polynomial Configure hash polynomial	ハードウェア ECMP の構成オプションとしてハッシュオフセットとハッシュ多数項を表示します。
switch config)# hardware ecmp hash-polynomial ? CRC16 Hash polynomial CRC16CRC32HI Hash polynomial CRC32 HI	ハッシュ多項式の構成オプションとして CRC16 および CRC32HI を表示します。
switch config)#show running-config	実行設定を表示します。

ユニキャスト FIB のロードシェアリングアルゴリズムを表示するには、任意のモードで次のコマンドを使用します。

コマンド	目的
show ip load-sharing 例 : <pre>switch(config)# show ip load-sharing</pre>	データトラフィックに対するユニキャスト FIB のロードシェアリング アルゴリズムを表示します。

次に、show ip load-sharing コマンドの出力例を示します。

```
hardware lb-keyshift 1 lb-2nd-hier-keyshift 10
switch(config)# ip load-sharing address source-destination port source-destination
switch(config)# show ip load-sharing
```

```
IPv4/IPv6 ECMP load sharing:
Universal-id (Random Seed): 251533739
Load-share mode : address source-destination port source-destination
GRE-Outer hash is disabled
Concatenation is disabled
Rotate: 32
```

```
Lbkeyshift: 1
2ndHeirLbkeyshift: 10
switch(config)#
```

ユニキャスト RIB および FIB が特定の送信元アドレス/宛先アドレスに使用するルートを表示するには、任意のモードで次のコマンドを使用します。

コマンド	目的
show routing hash source-addr dest-addr [ip-protocol ip-protocol] [source-l4-port dest-l4-port] [vrf vrf-name] 例: switch# show routing hash 1.1.1.6.5.5 5.3 ip-protocol 0x11 10 234	ユニキャスト RIB および FIB が特定の送信元/宛先アドレスペアに使用するルートを表示します。送信元アドレスと宛先アドレスの形式はx.x.x.xです。送信元ポートと宛先ポートの範囲は 1 ～ 65535 です。VRF 名には最大 64 文字の英数字文字列を指定します。大文字と小文字は区別されます。ip-protocol オプションは、IP ヘッダーのプロトコルフィールドに対応します。

次に、送信元/宛先ペアのために選択されたルートを表示する例を示します。

```
switch# show routing hash 1.1.1.6.5.5.5.3 ip-protocol 0x11 10 234
Load-share parameters used for software forwarding:
load-share mode: address source-destination port source-destination
Universal-id seed: 0xe05e2e85
Invoking pc_ic_ecmp_resolution
Hash for VRF "default"
Hashing to path *Eth1/29%
For route:
5.5.5.0/24 ubest/mbest: 3/0
*via 2.2.2.1, Eth1/18, [1/0], 00:14:14, static
*via 3.3.3.1, Eth1/29, [1/0], 00:14:14, static
*via 4.4.4.1, Eth1/34, [1/0], 00:14:14, static
```

ルーティング情報と隣接情報の表示

ユーザーは、ルーティング情報と隣接情報を表示できます。

ルーティング情報と隣接情報を表示するには、任意のモードで次のコマンドを使用します。

コマンド	目的
show ip route [route-type interface int-type number next-hop] 例: switch# show ip route	ユニキャスト ルート テーブルを表示します。route-type 引数には、1 つのルートプレフィックス、直接、静的、またはダイナミック ルーティング プロトコルを指定します。? キーワードを使用して、サポートされるインターフェイスを表示します。

コマンド	目的
show ip adjacency [<i>prefix</i> <i>interface number</i> [summary] non-best] [detail] [<i>vrf vrf-id</i>] 例 : switch# show ip adjacency	隣接関係テーブルを表示します。引数の範囲は次のとおりです。 • <i>prefix</i> : 任意の IPv4 プレフィックスアドレス。 • <i>interface-type number</i> : ? コマンドを使用して、サポートされるインターフェイスを表示します。 • <i>vrf-id</i> : 最大 32 文字の英数字文字列。大文字と小文字は区別されます。
show ip routing [<i>route-type</i> <i>interface int-type number</i> next-hop recursive-next-hop summary updated { <i>since</i> <i>until</i> } <i>time</i>] 例 : switch# show routing summary	ユニキャスト ルート テーブルを表示します。 <i>route-type</i> 引数には、1 つのルート プレフィックス、直接、静的、またはダイナミック ルーティング プロトコルを指定します。? キーワードを使用して、サポートされるインターフェイスを表示します。

次に、ユニキャスト ルート テーブルを表示する例を示します。

```
switch# show ip route
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
*** denotes best mcast next-hop
'[x/y]' denotes [preference/metric]

192.168.0.2/24, ubest/mbest: 1/0, attached
*via 192.168.0.32, Eth1/5, [0/0], 22:34:09, direct
192.168.0.32/32, ubest/mbest: 1/0, attached
*via 192.168.0.32, Eth1/5, [0/0], 22:34:09, local
```

次に、隣接情報を表示する例を示します。

```
switch# show ip adjacency

IP Adjacency Table for VRF default
Total number of entries: 2
Address Age MAC Address Pref Source Interface Best
10.1.1.1 02:20:54 00e0.b06a.71eb 50 arp mgmt0 Yes
10.1.1.253 00:06:27 0014.5e0b.81d1 50 arp mgmt0 Yes
```

レイヤ3 整合性チェッカーのトリガー

レイヤ3 整合性チェッカーを手動でトリガーできます。

レイヤ3 整合性チェッカーを手動でトリガーするには、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。

コマンド	目的
test [ipv4] [unicast] forwarding inconsistency [vrf vrf-name] [module { slot all }] 例 : <pre>switch(config)# test forwarding inconsistency</pre>	レイヤ 3 整合性チェックを開始します。 <i>vrf-name</i> には最大 32 文字の英数字文字列を指定します。大文字と-小文字は区別されます。 <i>slot</i> の範囲は 1 ～ 10 です。

レイヤ 3 整合性チェッカーを停止するには、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。

コマンド	目的
test forwarding [ipv4] [unicast] inconsistency [vrf vrf-name] [module { slot all }] stop 例 : <pre>switch(config)# test forwarding inconsistency stop</pre>	レイヤ 3 整合性チェックを停止します。 <i>vrf-name</i> には最大 64 文字の英数字文字列を指定します。大文字と-小文字は区別されます。 <i>slot</i> の範囲は 1 ～ 10 です。

レイヤ 3 の不整合を表示するには、任意のモードで次のコマンドを使用します。

コマンド	目的
show forwarding [ipv4] inconsistency [vrf vrf-name] [module { slot all }] 例 : <pre>switch(config)# show forwarding inconsistency</pre>	レイヤ 3 整合性チェックの結果を表示します。 <i>vrf-name</i> には最大 32 文字の英数字文字列を指定します。大文字と-小文字は区別されます。 <i>slot</i> の範囲は 1 ～ 10 です。

FIB 内の転送情報の消去

FIB 内の 1 つまたは複数のエントリを消去できます。



(注) **clear forwarding** コマンドを実行すると、スイッチ上の転送は中断されます。

FIB 内のエントリ（レイヤ 3 の不整合を含む）を消去するには、任意のモードで次のコマンドを使用します。

コマンド	目的
clear forwarding { ipv4 } route { * prefix } [vrf vrf-name] [module { slot all }] 例 : <pre>switch(config)# clear forwarding ipv4 route *</pre>	FIB から 1 つまたは複数のエントリを消去します。ルートのオプションは次のとおりです。 • * : すべてのルート。 • prefix : 任意の IP プレフィックス。 vrf-name には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。 slot の範囲は 1 ～ 10 です。



(注) FIB エントリをクリアした後は、RIB エントリをクリアしてください。

ルートのメモリ要件の見積もり

一連のルートおよびネクストホップアドレスが使用するメモリを見積もることができます。ルートのメモリ要件を見積もるには、任意のモードで次のコマンドを使用します。

コマンド	目的
show routing memory estimate routes num-routes next-hops num-nexthops 例 : <pre>switch# show routing memory estimate routes 1000 next-hops 1</pre>	ルートのメモリ要件を表示します。 num-routes の範囲は 1000 ～ 1000000 です。 num-nexthops の範囲は 1 ～ 16 です。

ユニキャスト RIB 内のルートの消去

ユニキャスト RIB から 1 つまたは複数のルートを消去できます。



注意 * キーワードを使用すると、ルーティングが著しく妨害されます。

ユニキャスト RIB 内の 1 つまたは複数のエントリを消去するには、任意のモードで次のコマンドを使用します。

コマンド	目的
clear iproute { * { <i>route</i> <i>prefix/length</i> } [<i>next-hop interface</i>] } [vrf <i>vrf-name</i>] 例 : <pre>switch(config)# clear ip route 10.2.2.2</pre>	ユニキャスト RIB とすべてのモジュール FIB から 1 つまたは複数のルートを消去します。ルートのオプションは次のとおりです。 • * : すべてのルート。 • route : 個々の IP ルート。 • prefix/length : 任意の IP プレフィックス。 • next-hop : ネスクトホップ アドレス。 • interface : ネスクトホップ アドレスに到達するためのインターフェイス <i>vrf-name</i> には最大 32 文字の英数字文字列を指定します。大文字と-小文字は区別されます。
clear routing unicast [ip ipv4] { * { <i>route</i> <i>prefix/length</i> } [<i>next-hop interface</i>] } [vrf <i>vrf-name</i>] 例 : <pre>switch(config)# clear routing ip 10.2.2.2</pre>	ユニキャスト RIB から 1 つまたは複数のルートを消去します。ルートのオプションは次のとおりです。 • * : すべてのルート。 • route : 個々の IP ルート。 • prefix/length : 任意の IP プレフィックス。 • next-hop : ネスクトホップ アドレス。 • interface : ネスクトホップ アドレスに到達するためのインターフェイス <i>vrf-name</i> には最大 32 文字の英数字文字列を指定します。大文字と-小文字は区別されます。

ユニキャスト RIB および FIB の確認

ユニキャスト RIB および FIB の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show forwarding adjacency	モジュールの隣接関係テーブルを表示します。
show forwarding distribution { clients fib-state }	FIB の分散情報を表示します。
show forwarding interfaces module slot	モジュールの FIB 情報を表示します。

コマンド	目的
show forwarding ipv4route	FIB 内のルートを表示します。
show ip adjacency	隣接関係テーブルを表示します。
show ip route	ユニキャスト RIB から受け取った IPv4 ルートを表示します。
show routing	ユニキャスト RIB から受け取ったルートを表示します。



第 15 章

Route Policy Manager の設定

この章では、Cisco NX-OS スイッチで Route Policy Manager を設定する方法について説明します。

この章は、次の項で構成されています。

- [Route Policy Manager について \(443 ページ\)](#)
- [Route Policy Manager の注意事項と制約事項 \(448 ページ\)](#)
- [デフォルト設定 \(449 ページ\)](#)
- [Route Policy Manager の設定 \(449 ページ\)](#)
- [Route Policy Manager の設定の確認 \(465 ページ\)](#)
- [関連項目 \(465 ページ\)](#)

Route Policy Manager について

Route Policy Manager は、ルート マップおよび IP プレフィックス リストをサポートしています。この機能は、ルート再配布に使用されます。プレフィックスリストには、1つまたは複数の IPv4 ネットワーク プレフィックスおよび関連付けられたプレフィックス長の値を指定します。プレフィックスリストは、ボーダーゲートウェイプロトコル (BGP) テンプレート、ルートフィルタリング、またはルーティング ドメイン間で交換されるルートの再配布などの機能で、単独で使用できます。

ルート マップは、ルートおよび IP パケットの両方に適用できます。ルート フィルタリングおよび再配布は、ルート マップを使用してルートを渡します。

プレフィックス リスト

プレフィックスリストを使用すると、アドレスまたはアドレス範囲を許可または拒否することができます。プレフィックスリストによるフィルタリングでは、ルートまたはパケットのプレフィックスと、プレフィックスリストに指定されているプレフィックスの照合が行われます。特定のプレフィックスがプレフィックスリストのどのエントリとも一致しなかった場合、実質的に拒否されたものと見なされます。

プレフィックスリストに複数のエントリを設定し、エントリと一致したプレフィックスを許可または拒否できます。各エントリにはシーケンス番号が関連付けられています。この番号はユーザが設定できます。シーケンス番号が設定されていない場合は、Cisco NX-OS によって自動的にシーケンス番号が設定されます。Cisco NX-OS はシーケンス番号が最も小さいエントリから順番にプレフィックスリストを評価します。Cisco NX-OS は、所定のプレフィックスと最初に一致したエントリを処理します。一致すると、Cisco NX-OS は `permit` 文または `deny` 文を処理し、プレフィックスリストの残りのエントリは評価しません。



(注) プレフィックス リストが空の場合は、すべてのルートが許可されます。

プレフィックス リストのマスク

マスクはプレフィックスリストに使用できます。マスクでは、数値1と数値0を使用して、対応する IP アドレス ビットをどのように扱うかを指定します。

- マスク ビット 0 は、対応するビット値を無視することを示します。
- マスク ビット 1 は、対応するビット値が正確に一致しているかどうかを確認することを示します。

プレフィックス リストを使用してルート マップの IP アドレスを照合できます。この IP アドレスは再配布時にルーティング プロトコルで使用されます。IP アドレスは、マスク ビット 1 に対応するビットがプレフィックスリストで指定されたサブネットと同じであるプレフィックス リストと照合されます。

マスクを慎重に設定することにより、許可または拒否のテストに 1 つまたは複数の IP アドレスを選択できます。

プレフィックスリストのマスクを使用すると、マスクに非連続ビットを指定し、偶数または奇数の IP アドレスの範囲を定義できます。

MAC リスト

MAC リストを使用すると、MAC アドレスまたはアドレス範囲を許可または拒否できます。MAC リストは MAC アドレスとオプションの MAC マスクのリストです。MAC マスクはワイルドカードマスクで、ルートマップが MAC リストのエントリと一致すると論理的に MAC アドレスと AND 結合されます。MAC リストによるフィルタリングでは、パケットの MAC アドレスと MAC リスト内の MAC リストが照合されます。特定の MAC アドレスが MAC リストのどのエントリとも一致しなかった場合、実質的に拒否されたものと見なされます。

MAC リストに複数のエントリを設定し、エントリと一致した MAC アドレスを許可または拒否できます。各エントリにはシーケンス番号が関連付けられています。この番号はユーザが設定できます。シーケンス番号が設定されていない場合は、Cisco NX-OS によって自動的にシーケンス番号が設定されます。Cisco NX-OS はシーケンス番号が最も小さいエントリから順番に MAC リストを評価します。Cisco NX-OS は指定された MAC アドレスと最初に一致するエン

リを処理します。一致すると、Cisco NX-OS は **permit** 文または **deny** 文を処理し、MAC リストの残りのエントリは評価しません。

ルートマップ

ルートマップは、ルートの再配布に使用できます。ルートマップ エントリは、一致基準および設定基準のリストからなります。一致基準では、着信ルートまたはパケットの一致条件を指定します。設定基準では、一致基準を満たした場合のアクションを指定します。

同じルートマップに複数のエントリを設定できます。これらのエントリには、同じルートマップ名を指定し、シーケンス番号で区別します。

一意のルートマップ名の下に1つまたは複数のルートマップ エントリをシーケンス番号に従って並べ、ルートマップを作成します。ルートマップ エントリのパラメータは、次のとおりです。

- シーケンス番号
- アクセス権：許可または拒否
- 一致基準
- 設定変更

ルートマップではデフォルトで、最小のシーケンス番号から順にルートまたは IP パケットが処理されます。**continue** 文を使用すると、次に処理するルートマップ エントリを決定できるので、別の順序で処理するようにルートマップを設定できます。

一致基準

さまざまな基準を使用して、ルートマップでルートや IP パケットを照合できます。BGP コミュニティ リストのように、特定のルーティング プロトコルだけに適用できる基準もありますが、IP 送信元または宛先アドレスなど、その他の基準はあらゆるルートまたは IP パケットに使用できます。

ルートマップに従ってルートまたはパケットを処理する場合、Cisco NX-OS は設定されている個々の **match** 文とルートまたはパケットを比較します。ルートまたはパケットが設定されている基準と一致した場合、Cisco NX-OS はルートマップ内で一致するエントリに対する許可または拒否設定、および設定されている設定基準に基づいて、このルートやパケットを処理します。

一致のカテゴリおよびパラメータは、次のとおりです。

- BGP パラメータ：AS 番号、AS パス、コミュニティ属性、または拡張コミュニティ属性に基づく一致
- プレフィックス リスト：アドレスまたはアドレス範囲に基づく一致
- マルチキャスト パラメータ：ランデブー ポイント、グループ、または送信元に基づく一致

- その他のパラメータ：IP ネクストホップ アドレスまたはパケット長に基づく一致

設定変更

ルートまたはパケットがルート マップのエントリと一致したら、設定済みの 1 つ以上の set 文に基づいて、そのルートまたはパケットを変更できます。

設定変更は次のとおりです。

- BGP パラメータ：AS パス、タグ、コミュニティ、拡張コミュニティ、ダンプニング、ローカル プリファレンス、オリジン、または重み値属性の変更
- メトリック：ルート メトリック、ルート タグ、またはルート タイプの変更
- その他のパラメータ：フォワーディングアドレスまたは IP ネクストホップアドレスの変更

アクセス リスト

IP アクセス リストでは、次のような IP パケット フィールドとパケットを照合できます。

- 送信元または宛先 IPv4 アドレス
- プロトコル
- Precedence
- ToS

BGP の AS 番号

BGP ピアとの照合に使用する AS 番号のリストを設定できます。BGP ピアがリスト内の AS 番号と一致し、さらに他の BGP ピア設定と一致する場合、BGP はセッションを作成します。BGP ピアがリスト内の AS 番号と一致しない場合は、BGP はピアを無視します。AS 番号は AS 番号の範囲のリストとして設定できます。また、AS パス リストを使用して AS 番号を正規表現と比較することもできます。

BGP の AS パス リスト

AS パス リストを設定すると、着信または発信 BGP ルートのアップデートをフィルタリングできます。ルート アップデートに AS パス リストのエントリと一致する AS パス属性が含まれている場合、ルータは設定されている許可または拒否条件に基づいてルート进行处理します。ルート マップの中で AS パス リストを設定できます。

同じ AS パス リスト名を使用することによって、AS パス リストで複数の AS パス エントリを設定できます。ルータは最初に一致したエントリ进行处理します。

BGP のコミュニティ リスト

ルートマップのコミュニティ リストを使用すると、BGP コミュニティに基づいて BGP ルート アップデートをフィルタリングできます。コミュニティ属性はコミュニティ リストに基づいて照合できます。また、コミュニティ属性はルート マップを使用して設定できます。

コミュニティ リストには、1 つまたは複数のコミュニティ属性を指定します。同じコミュニティ リスト エントリに複数のコミュニティ属性を設定した場合、BGP ルートが一致と見なされるには、指定されたすべてのコミュニティ属性と一致しなければなりません。

同じコミュニティ リスト名を使用することによって、コミュニティ リストのそれぞれ個別のエントリとして、複数のコミュニティ属性を設定することもできます。この場合、ルータは最初に BGP ルートと一致したコミュニティ属性を、そのエントリの許可または拒否設定に基づいて処理します。

コミュニティ リストのコミュニティ属性は、次の形式のいずれか 1 つで設定できます。

- 名前付きのコミュニティ属性 (**internet** や **no-export** など)。
- **aa:nn** 形式 (最初の 2 バイトは 2 バイトの自律システム番号、最後の 2 バイトはユーザが定義するネットワーク番号を表します)。
- 正規表現。

BGP の拡張コミュニティ リスト

拡張コミュニティ リストでは 4 バイトの AS 番号がサポートされています。拡張コミュニティ リストのコミュニティ属性は、次のいずれかの形式で設定できます。

- **aa4:nn** 形式 (最初の 4 バイトは 4 バイトの AS 番号、最後の 2 バイトはユーザが定義するネットワーク番号を表します)。
- 正規表現。

Cisco NX-OS は汎用の特定拡張コミュニティ リストをサポートしています。このリストを使用すると、4 バイトの AS 番号に対して通常のコミュニティ リストと同様の機能を使用できます。汎用の特定拡張コミュニティ リストには次のプロパティを設定できます。

- **Transitive** : BGP はコミュニティ属性を自律システム間に伝達します。
- **Nontransitive** : BGP はコミュニティ属性を削除してからルートを他の自律システムに伝達します。

ルートの再配布およびルート マップ

ルート マップを使用すると、ルーティング ドメイン間でのルートの再配布を制御できます。ルートマップではルートの属性を照合し、一致基準を満たすルートだけを再配布します。設定変更を使用することによって、再配布時に、ルートマップでルート属性を変更することもできます。

ルータは再配布されたルートを各ルートマップエントリと照合します。**match** 文が複数ある場合は、ルートがすべての一致基準を満たしている必要があります。ルートがルートマップエントリで定義されている一致基準を満たす場合は、エントリで定義されているアクションが実行されます。ルートが基準と一致しなかった場合、ルータは後続のルートマップエントリとルートを比較します。ルートの処理は、ルートがルートマップのいずれかのエントリと一致するか、どのエントリとも一致せずすべてのエントリによる処理が完了するまで続きます。ルータがルートマップの全エントリとルートを比較しても一致しなかった場合、ルータはそのルートを受け付けるか（着信ルートマップ）またはルートを転送します（発信ルートマップ）。

Route Policy Manager の注意事項と制約事項

Route Policy Manager 設定時の注意事項および制約事項は、次のとおりです。

- CLI は **route-tag** では **set** または **match** が有効になっていますが、サポートされておらず、その特定のルートマップシーケンスに対して意図しない動作が発生します。
- プレフィックスリスト内の名前は、大文字と小文字が区別されません。一意の名前を使用することを推奨します。大文字と小文字を変更しただけの名前は使用しないでください。たとえば、CTCPPrimaryNetworks と CtcPrimaryNetworks は 2 つの異なるエントリではありません。
- ルートマップが存在しない場合、すべてのルートが拒否されます。
- プレフィックス リストが存在しない場合は、すべてのルートが許可されます。
- ルートマップエントリに **match** 文がない場合、ルートマップエントリのアクセス権（許可または拒否）によって、すべてのルートまたはパケットの処理結果が決まります。
- ルートマップエントリの **match** 文の中で参照されたポリシー（プレフィックス リストなど）から **no-match** または **deny-match** が戻った場合、は **match** 文を Cisco NX-OS 失敗として、次のルートマップエントリを処理します。
- ルートマップを変更しても、ルートマップコンフィギュレーションサブモードを終了するまでは、Cisco NX-OS によりすべての変更が保留されます。その後、Cisco NX-OS がすべての変更をプロトコルクライアントに送信すると、変更が有効になります。
- 同じルートマップシーケンスに IPv4 と IPv6 の両方の **match** ステートメントを含めないことを推奨します。両方が必要な場合は、同じルートマップの異なるシーケンスで指定する必要があります。
- ルートマップは定義する前に使用できるので、設定変更を終えるときには、すべてのルートマップが存在していることを確認してください。
- 再配布およびフィルタリングを行う場合、ルートマップの使用状況を確認できます。各ルーティングプロトコルには、これらの統計情報を表示する機能があります。
- BGP を IGP に再配布するとき、iBGP も再配布されます。この動作を無効にするには、ルートマップに追加 **deny** 文を挿入します。

- Route Policy Manager は MAC リストをサポートしていません。
- `ip access-list name` コマンドの ACL 名の最大文字数は 64 です。ただし、RPM コマンドに関連付けられている ACL 名 (`ip prefix-list` や `match ip address` など) は、最大 63 文字しか使用できません。
- BGP は特定の **match** コマンドのみをサポートします。詳細については、[ルートマップの設定 \(458 ページ\)](#) セクションの **match** コマンドの表を参照してください。
- 「prefix-list」という名前の ACL を作成する場合、`match ip address` コマンドを使用して作成されたルート マップに関連付けることはできません。RPM コマンドの `match ip address prefix-list` は、前のコマンド (「prefix-list」 ACL 名) をあいまいにします。
- `match ip address` コマンドを使用する場合、設定できる ACL は 1 つだけです。

デフォルト設定

次は Route Policy Manager のデフォルト設定をリストします。

表 20: デフォルトの *Route Policy Manager* パラメータ

パラメータ	デフォルト
Route Policy Manager	有効 (Enabled)

Route Policy Manager の設定

IP プレフィックス リストの設定

IP プレフィックス リストでは、プレフィックスおよびプレフィックス長のリストに対して IP パケットまたはルートを照合します。IPv4 の IP プレフィックス リストを作成できます。

指定したプレフィックス長と完全に一致するプレフィックス リスト エントリのみを対象とするよう設定できます。また、指定したプレフィックス長の範囲に該当するすべてのプレフィックスを対象とすることもできます。

ge キーワードと **lt** キーワードを使用すると、プレフィックス長の範囲を指定できます。着信パケットまたはルートがプレフィックスリストと一致すると判定されるのは、プレフィックスが一致し、プレフィックス長が **ge** キーワードの値 (設定されている場合) 以上かつ **lt** キーワードの値 (設定されている場合) 以下の場合です。キーワード **eq** を使用する場合、設定する値はプレフィックスのマスク長より大きくする必要があります。

プレフィックス アドレスとの比較に使用できる連続または非連続ルートの範囲を定義するには、**mask** キーワードを使用します。

手順の概要

1. **configure terminal**
2. (任意) **ip prefix-list name description string**
3. **ip prefix-list name [seq number] [{ permit | deny } prefix { [eq prefix-length] | [ge prefix-length] | [le prefix-length] }] [mask mask]**
4. (任意) **show ip prefix-list name**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	(任意) ip prefix-list name description string 例 : <pre>switch(config)# ip prefix-list AllowPrefix description allows engineering server</pre>	プレフィックスリストについての情報ストリングを追加します。
ステップ 3	ip prefix-list name [seq number] [{ permit deny } prefix { [eq prefix-length] [ge prefix-length] [le prefix-length] }] [mask mask] 例 : <pre>switch(config)# ip prefix-list AllowPrefix seq 10 permit 192.0.2.0/23 eq 24 switch(config)# ip prefix-list even permit 0.0.0.0/32 mask 0.0.0.1</pre>	IPv4 プレフィックスリストを作成するか、または既存のプレフィックスリストにプレフィックスを追加します。プレフィックス長の照合は次のように行われます。 • eq : <i>prefix length</i> の値と完全に一致するものが対象。この値は、マスク長より大きくする必要があります。 • ge : 設定された <i>prefix length</i> 以上のプレフィックス長が対象。 • le : 設定された <i>prefix length</i> 以下のプレフィックス長が対象。 • マスク : 再配布中にルーティングプロトコルで使用されるプレフィックスアドレスのビットと比較する、プレフィックスリストのプレフィックスアドレスのビットを指定します。
ステップ 4	(任意) show ip prefix-list name 例 :	プレフィックス リストについての情報を表示します。

	コマンドまたはアクション	目的
	switch(config)# show ip prefix-list AllowPrefix	
ステップ 5	(任意) copy running-config startup-config 例 : switch# copy running-config startup-config	この設定変更を保存します。

例

次に、2つのエントリからなる IPv4 プレフィックス リストを作成し、BGP ネイバーにプレフィックス リストを適用する例を示します。

```
switch# configure terminal
switch(config)# ip prefix-list allowprefix seq 10 permit 192.0.2.0/23 eq 24
switch(config)# ip prefix-list allowprefix seq 20 permit 209.165.201.0/27 eq 28
switch(config)# router bgp 65536:20
switch(config-router)# neighbor 192.0.2.1/16 remote-as 65535:20
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# prefix-list allowprefix in
```

次に、奇数 IP アドレスの一致マスクを使用して IPv4 プレフィックス リストを作成する例を示します。

```
switch# configure terminal
switch(config)# ip prefix-list odd permit 0.0.0.1/32 mask 0.0.0.1
```

MAC リストの設定

MAC リストを設定すると、特定の範囲の MAC アドレスを許可または拒否できます。

手順の概要

1. **configure terminal**
2. **mac-list name [seq number] { } mac-address {mac-mask}**
3. (任意) **show mac- list name**
4. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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 2	mac-list name [seq number] { } mac-address {mac-mask} 例 : <pre>switch(config)# mac-list AllowMac seq 1 permit 0022.5579.a4c1 ffff.ffff.0000</pre>	MAC リストを作成するか、既存の MAC リストに MAC アドレスを追加します。 <i>seq</i> の範囲は 1 ~ 4294967294 です。 <i>mac-mask</i> は照合する MAC アドレスの部分を表します。MAC アドレス形式である必要があります。
ステップ 3	(任意) show mac- list name 例 : <pre>switch(config)# show mac-list AllowMac</pre>	MAC リストに関する情報を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

AS パス リストの設定

発信と着信の両方の BGP ルートに AS パス リスト フィルタを指定できます。各フィルタは、正規表現を使用するアクセス リストです。正規表現が ASCII ストリングとして表されたルートの AS パス属性と一致した場合は、許可または拒否条件が適用されます。

手順の概要

1. **configure terminal**
2. **ip as-path access-list name { deny | permit } expression**
3. (任意) **show ip as-path-access-list name**
4. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	ip as-path access-list name { deny permit } expression 例 : <pre>switch(config)# ip as-path access-list Allow40 permit 40</pre>	正規表現を使用して BGP AS パス リストを作成します。

	コマンドまたはアクション	目的
ステップ 3	(任意) show ip as-path-access-list name 例 : <pre>switch(config)# show ip as-path-access-list Allow40</pre>	as-path アクセス リストの情報を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、2つのエントリからなる AS パス リストを作成し、BGP ネイバーに AS パス リストを適用する例を示します。

```
switch# configure terminal
switch(config)# ip as-path access-list AllowAS permit 64510
switch(config)# ip as-path access-list AllowAS permit 64496
switch(config)# copy running-config startup-config
switch(config)# router bgp 65536:20
switch(config-router)# neighbor 192.0.2.1/16 remote-as 65535:20
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# filter-list AllowAS in
```

BGP AS-path 属性の置き換え

次の手順では、着信および発信ルート マップの BGP as-path 属性を変更することにより、BGP ルーティング ポリシーを操作できます。

BGP as-path 属性を置き換えるときは、次のガイドラインを考慮してください。

- この機能は、アドレス ファミリ識別子 (AFI) ごとに eBGP ネイバーにのみ適用されます。iBGP ネイバーで機能を設定しようとしても、構成は無視されます。
- この機能を備えたルート マップは、BGP ネイバーのインバウンド側とアウトバウンド側の両方に適用できます。
- この機能は、AS_SET、AS_SEQUENCE、CONFED_SET、および CONFED_SEQUENCE の任意の組み合わせをサポートします。
- 2 バイト AS のみをサポートする BGP スピーカーと対話する場合、4 バイト AS 番号は予約済みの 2 バイト AS 番号 23456 に置き換えられます。
- コンフェデレーション識別子が設定されている場合は、コンフェデレーションの外部にあるピアと対話するときに、CLI でローカル ASN としてコンフェデレーション識別子を使用することを検討してください。同じコンフェデレーションに属するピアと対話する場合は、**router bgp asn** コマンドでプロセス ASN を使用することを検討してください。

- BGP **local-as** 機能が設定されている場合、設定された **local-as** は CLI でローカル ASN と見なされます。
- アウトバウンドルート マップの場合、ローカル ASN は常に CLI からの結果の **as_path** に付加されます。
- **set as-path** または **set as-path replace** コマンドでは、最大 32 個の AS 番号を設定できます。
- 1 つのルート マップ シーケンスの下では、**set as-path**、**set as-path prepend**、および **set as-path replace** のオプションのうち 1 つだけを設定できます。
- **remove-private-as** が設定されている場合、アウトバウンド側で新しいルート マップ コマンドを適用する前に適用されます。
- **as-override** が設定されている場合、アウトバウンド側で新しいルート マップ コマンドを適用した後に適用されます。
- **AS_PATH** ループ チェックは、新しいルート マップ コマンドが着信側と発信側の両方に適用される前に、元の **AS_PATH** で実行されます。これらのチェックは、インバウンド側で **allow-as in** とアウトバウンド側で **disable-peer-as-check** を使用することで緩和できます。

完全な AS パスの置き換え

この手順を使用して、着信または発信 BGP アップデートの AS パスをカスタム AS パスに変更します。AS パスを完全に削除することもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	route-map map-name [permit deny] [seq] 例 : <pre>switch(config)# route-map Testmap permit 10 switch(config-route-map)#</pre>	ルート マップを作成するか、または既存のルート マップに対応するルートマップ設定モードを開始します。ルートマップのエントリを順序付けるには、 seq を使用します。
ステップ 3	[no] set as-path { none {as-number remote-as local-as}+] } 例 : <pre>switch(config-route-map)# set as-path 11 local-as remote-as 13</pre>	AS_PATH をカスタム ASN のリストに置き換えるか、 AS_PATH をクリアします。コマンド オプションは次のとおりです。 • as-number: 指定された AS 番号。 • remote-as: BGP ピアの AS 番号。 • local-as: ローカル AS 番号。

	コマンドまたはアクション	目的
		none キーワードは、AS パスを完全に削除します。

例

次の例では、これらの値が想定されています。

- 元の AS_PATH は **10 20 30 40 50 60** です。
- local-as は **100** です。
- remote-as は **200** です。

この例は、カスタム AS パスを指定する方法を示しています。このコマンドは、AS パスを **11 100 200 13 200 10.10 65535** に変更します。

```
switch# configure terminal
switch(config)# route-map Testmap permit 10
switch(config-route-map)# set as-path 11 local-as remote-as 13 remote-as 10.10 65535
```

この例は、AS パスをクリアする方法を示しています。このコマンドにより、AS パスが空になります。

```
switch# configure terminal
switch(config)# route-map Testmap permit 10
switch(config-route-map)# set as-path none
```

AS パスでの選択した AS 番号の置き換え

この手順を使用して、AS パス内の特定の AS 番号を置き換え、着信または発信 BGP 更新でそれらをカスタム AS 番号に置き換えます。**private-as** をマッチ キーワードとして指定することもできます。この場合、**private-as** の任意のインスタンスが一致し、置換または削除できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	route-map map-name [permit deny] [seq] 例 : switch(config)# route-map Testmap permit 10 switch(config-route-map)#	ルート マップを作成するか、または既存のルート マップに対応するルートマップ設定モードを開始します。ルートマップのエントリを順序付けるには、 seq を使用します。

	コマンドまたはアクション	目的
ステップ 3	[no] set as-path replace {asn_list private-as} [with {as-number remote-as none}] 例 : <pre>switch(config-route-map)# set as-path replace 1, 2, private-as with remote-as</pre>	with キーワードが指定されていない場合は、コンマで区切られた <i>asn_list</i> で示されている ASN のインスタンスを local-as に置き換えます。private-as キーワードが指定されている場合は、private-as を置き換えます。 with キーワードが指定されている場合は、一致した ASN の with キーワードの後の値、または private-as キーワードが指定されている場合は private-as を置き換えます。 with キーワードに続くコマンドオプションは次のとおりです。 • as-number: 一致した値は、指定された AS 番号に置き換えられます。 • remote-as: 一致した値は、BGP ピアの AS 番号に置き換えられます。 • none: 一致した値は AS-path から削除されます。

例

次の例では、これらの値が想定されます。

- 元の AS_PATH は **1 5 2 10.10 65534 20** です。
- **local-as** は **100** です。
- **remote-as** は **200** です。

この例は、2 つの特定の ASN と、**private-as** を **local-as** に置き換える方法を示しています。このコマンドは、AS パスを **100 5 100 10.10 100 20** に変更します。

```
switch# configure terminal
switch(config)# route-map Testmap permit 10
switch(config-route-map)# set as-path replace 1, 2, private-as
```

この例は、2 つの特定の ASN と、**private-as** をネイバーの ASN (**remote-as**) に置き換える方法を示しています。このコマンドは、AS パスを **200 5 200 10.10 200 20** に変更します。

```
switch# configure terminal
switch(config)# route-map Testmap permit 10
switch(config-route-map)# set as-path replace 1, 2, private-as with remote-as
```


この例は、2 つの特定の ASN と private-as を削除する方法を示しています。このコマンドは、AS パスを **5 10.10 20** に変更します。

```
switch# configure terminal
switch(config)# route-map Testmap permit 10
switch(config-route-map)# set as-path replace 1, 2, private-as with none
```

コミュニティ リストの設定

コミュニティ リストを使用すると、コミュニティ属性に基づいて BGP ルートをフィルタリングできます。コミュニティ番号は *aa:nn* 形式の 4 バイト値です。最初の 2 バイトは自律システム番号を表し、最後の 2 バイトはユーザ定義のネットワーク番号です。

同じコミュニティ リスト文で複数の値を設定した場合、コミュニティ リストフィルタを満足させるには、すべてのコミュニティ値が一致しなければなりません。複数の値をそれぞれ個別のコミュニティ リスト文で設定した場合は、最初に条件が一致したリストが処理されます。

コミュニティリストを *match* 文で使用すると、コミュニティ属性に基づいて BGP ルートをフィルタリングできます。

手順の概要

1. **configure terminal**
- 2.
3. (任意) **show ip community-list name**
4. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション		目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>		グローバル設定モードを開始します。
ステップ 2	オプション	説明	
	コマンド	説明	
	ip community-list standard list-name { deny permit } [community-list] [internet] [local-AS] [	標準 BGP コミュニティ リストを作成します。 list-name は 63 文字以内の英数字のストリング	

	コマンドまたはアクション		目的
	オプション	説明	
	no-advertise][no-export] 例 : switch(config)# ip community-list standard BGPCommunity permit no-advertise 65536:20	(大文字と小文字を区別) で指定します。 <i>community-list</i> には、1つ以上のコミュニティを <i>aa:nn</i> 形式で指定できます。	
	ip community-list expanded <i>list-name</i> { deny permit } <i>expression</i> 例 : switch(config)# ip community-list expanded BGPComplex deny 50000:[0-9][0-9]_	正規表現を使用して拡張 BGP AS コミュニティリストを作成します。	
ステップ 3	(任意) show ip community-list name 例 : switch(config)# show ip community-list BGPCommunity		コミュニティ リストの情報を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config		この設定変更を保存します。

例

次に、2つのエントリからなるコミュニティ リストの作成例を示します。

```
switch# configure terminal
switch(config)# ip community-list standard BGPCommunity permit no-advertise 65536:20
switch(config)# ip community-list standard BGPCommunity permit local-AS no-export
switch(config)# copy running-config startup-config
```

ルート マップの設定

ルート マップを使用して、ルートの再配布やルート フィルタリングを行うことができます。ルート マップには、複数の一致基準と複数の設定基準を含めることができます。

BGPにルートマップを設定すると、BGP ネイバーセッションの自動ソフトクリアまたはリフレッシュのトリガーになります。

手順の概要

1. **configure terminal**
2. **route-map map-name [permit | deny] [seq]**
3. (任意) **continue seq**
4. (任意) **exit**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	route-map map-name [permit deny] [seq] 例 : <pre>switch(config)# route-map Testmap permit 10 switch(config-route-map)#</pre>	ルートマップを作成するか、または既存のルートマップに対応するルートマップ設定モードを開始します。 <i>seq</i> を使用して、ルートマップ エントリを順序付けます。
ステップ 3	(任意) continue seq 例 : <pre>switch(config-route-map)# continue 10</pre>	ルートマップで次処理するシーケンス文を決定します。使用するのは、フィルタリングおよび再配布の場合だけです。
ステップ 4	(任意) exit 例 : <pre>switch(config-route-map)# exit</pre>	ルートマップ コンフィギュレーション モードを終了します。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch# copy running-config startup-config</pre>	この設定変更を保存します。

例

ルートマップ コンフィギュレーション モードで、ルートマップに対して次のオプションの **match** パラメータを設定できます。



(注) **default-information originate** コマンドでは、オプションのルートマップの **match** 文は無視されます。

コマンド	目的
match as-path <i>name</i> [<i>name...</i>] 例 : <pre>switch(config-route-map)# match as-path Allow40</pre>	1 つまたは複数の AS パス リストと照合。AS パス リストは、 ip as-path access-list コマンドで作成します。
match as-number { <i>number</i> [, <i>number...</i>] as-path-list <i>name</i> [<i>name...</i>] } 例 : <pre>switch(config-route-map)# match as-number 33,50-60</pre>	1 つまたは複数の AS 番号または AS パス リストと照合。AS パス リストは、 ip as-path access-list コマンドで作成します。指定できる範囲は 1 ～ 65535 です。AS パス リスト名には最大 63 文字の英数字を使用できます。大文字と小文字は区別されます。
match community <i>name</i> [<i>name...</i>] [exact-match] 例 : <pre>switch(config-route-map)# match community BGPCommunity</pre>	1 つまたは複数のコミュニティリストと照合。コミュニティ リストは、 ip community-list コマンドで作成します。
match extcommunity <i>name</i> [<i>name...</i>] [exact-match] 例 : <pre>switch(config-route-map)# match extcommunity BGPextCommunity</pre>	1 つまたは複数の拡張コミュニティ リストと照合。コミュニティ リストは、 ip extcommunity-list コマンドで作成します。
match interface <i>interface-type</i> <i>number</i> [<i>interface-type</i> <i>number...</i>] 例 : <pre>switch(config-route-map)# match interface e 1/2</pre>	設定済みのインターフェイスのいずれかからのネクスト ホップと照合。? を使用すると、サポートされているインターフェイスタイプのリストを検索できます。
match ip address prefix-list <i>name</i> [<i>name...</i>] 例 : <pre>switch(config-route-map)# match ip address prefix-list AllowPrefix</pre>	1 つまたは複数の IPv4 プレフィックス リストと照合。プレフィックス リストは ip prefix-list コマンドを使用して作成します。
match ip next-hop prefix-list <i>name</i> [<i>name...</i>] 例 : <pre>switch(config-route-map)# match ip next-hop prefix-list AllowPrefix</pre>	1 つまたは複数の IP プレフィックス リストに対して、ルートの IPv4 ネクストホップアドレスを照合。プレフィックス リストは ip prefix-list コマンドを使用して作成します。

コマンド	目的
match ip route-source prefix-list name [name ...] 例 : <pre>switch(config-route-map)# match ip route-source prefix-list AllowPrefix</pre>	1 つまたは複数の IP プレフィックス リストに対して、ルートの IPv4 ルート送信元アドレスを照合。プレフィックス リストは ip prefix-list コマンドを使用して作成します。
match mac-list name [name...] 例 : <pre>switch(config-route-map)# match mac-list AllowMAC</pre>	1 つまたは複数の MAC リストと照合。MAC リストは mac-list コマンドを使用して作成します。
match metric value [+-deviation] [value..] 例 : <pre>switch(config-route-map)# match mac-list AllowMAC</pre>	ルート メトリック 値を 1 つまたは複数のメトリック 値または値の範囲と照合。メトリック範囲は +-deviation 引数を使用して設定します。ルートマップは次の範囲に該当するすべてのルートメトリックと照合されます。 <i>value - deviation to value + deviation.</i>
match route-type route-type 例 : <pre>switch(config-route-map)# match route-type level 1 level 2</pre>	ルート タイプと照合。 <i>route-type</i> は、次のうちの 1 つまたは複数にできます。 • external • internal • level-1 • level-2 • ローカル (local) • nssa-external • type-1 • type-2
match tag tagid [tagid.. .] 例 : <pre>switch(config-route-map)# match tag 2</pre>	フィルタリングまたは再配布に関する 1 つまたは複数のタグとルートを照合。
match vlan vlan-id [vlan-range] 例 : <pre>switch(config-route-map)# match vlan 3, 5-10</pre>	VLAN と照合。

ルート マップ設定モードで、オプションとして、ルート マップに次の **set** パラメータを設定できます。

コマンド	目的
set as-path { tag prepend { last-as number as-1 [as-2..] }} 例 : <pre>switch(config-route-map)# set as-path prepend 10 100 110</pre>	BGP ルートの AS パス属性を変更します。最後の AS 番号として設定された <i>number</i> または特定の AS パス値としてのストリング (<i>as-1 as-2...as-n</i>) を前に付加できます。
set comm-list name delete 例 : <pre>switch(config-route-map)# set comm-list BGPCommunity delete</pre>	着信または発信 BGP ルート アップデートのコミュニティ属性から、コミュニティを削除します。コミュニティ リストは ip community-list コマンドを使用して作成します。
set community { none additive local-AS no-advertise no-export community-1 [community-2. ...] } 例 : <pre>switch(config-route-map)# set community local-AS</pre>	BGP ルート アップデートのコミュニティ属性を設定します。 (注) ルートマップ属性の同じシーケンスで、 set community コマンドと set comm-list delete コマンドを両方使用すると、設定処理より先に削除処理が実行されます。 (注) send-community コマンドを BGP ネイバー アドレス ファミリ コンフィギュレーション モードで使用して、BGP コミュニティ属性を BGP ピアにプロパゲートします。
set dampening halflife reuse suppress duration 例 : <pre>switch(config-route-map)# set dampening 30 1500 10000 120</pre>	BGP ルート ダンプニング パラメータを設定します。 • <i>halflife</i> : 指定できる範囲は 1 ～ 45 分です。デフォルトは 15 です。 • <i>reuse</i> : 指定できる範囲は 1 ～ 20000 秒です。デフォルトは 750 です。 • <i>suppress</i> : 指定できる範囲は 1 ～ 20000 です。デフォルトは 2000 です。 • <i>duration</i> : 指定できる範囲は 1 ～ 255 分です。デフォルトは 60 です。
set extcomm-list name delete 例 : <pre>switch(config-route-map)# set extcomm-list BGPextCommunity delete</pre>	着信または発信 BGP ルート アップデートの拡張コミュニティ属性から、コミュニティを削除します。拡張コミュニティ リストは ip extcommunity-list コマンドを使用して作成します。

コマンド	目的
set extcommunity generic { transitive nontransitive } { none additive } community-1 [community-2...] 例 : <pre>switch(config-route-map)# set extcommunity generic transitive 1.0:30</pre>	BGP ルート アップデートの拡張コミュニティ属性を設定します。 (注) ルート マップ属性の同じシーケンスで、 set extcommunity コマンドと set extcomm-list delete コマンドを両方使用すると、設定処理より先に削除処理が実行されます。 (注) send-community コマンドを BGP ネイバーアドレスファミリ コンフィギュレーションモードで使用して、BGP コミュニティ属性を BGP ピアにプロパゲートします。
set forwarding-address 例 : <pre>switch(config-route-map)# set forwarding-address</pre>	OSPF のフォワーディング アドレスを設定します。
set level { backbone level-1 level-1-2 level-2 } 例 : <pre>switch(config-route-map)# set level backbone</pre>	IS-IS 用にルートをインポートするエリアを設定します。IS-IS のオプションは level-1、level-1-2、または level-2 です。デフォルトは level-1 です。
set local-preference value 例 : <pre>switch(config-route-map)# set local-preference 4000</pre>	BGP ローカル プリファレンス値を設定します。範囲は 0 ～ 4294967295 です。
set metric [+ -] bandwidth-metric 例 : <pre>switch(config-route-map)# set metric +100</pre>	既存のメトリック値を増減します。メトリックは Kb/s 単位です。範囲は 0 ～ 4294967295 です。

コマンド	目的
set metric bandwidth [delay reliability load mtu] 例 : <pre>switch(config-route-map)# set metric 33 44 100 200 1500</pre>	ルート メトリック値を設定します。 メトリックは次のとおりです。 • metric0 : 帯域幅 (Kb/s) 。 範囲は 0 ～ 4294967295 です。 • metric1 : 遅延 (10 マイクロ秒単位) 。 • metric2 : 信頼性。指定できる範囲は 0 ～ 255 (100% の信頼性) です。 • metric3 : ロード中。指定できる範囲は 1 ～ 200 (100% のロード) です。 • metric4 : パスの MTU。値の範囲は 1 ～ 4294967295 です。
set metric-type { external internal type-1 type-2 } 例 : <pre>switch(config-route-map)# set metric-type internal</pre>	宛先ルーティング プロトコルのメトリック タイプを設定します。オプションは次のとおりです。 external : IS-IS 外部メトリック internal : BGP の MED として IGP メトリックを使用 type-1 : OSPF 外部タイプ 1 メトリック type-2 : OSPF 外部タイプ 2 メトリック
set origin { egp as-number igp incomplete } 例 : <pre>switch(config-route-map)# set origin incomplete</pre>	BGP オリジン属性を設定します。EGP <i>as-number</i> の範囲は 0 ～ 65535 です。
set tag name 例 : <pre>switch(config-route-map)# set tag 33</pre>	宛先ルーティング プロトコルのタグ値を設定します。 name パラメータは符号なし整数です。
set weight count 例 : <pre>switch(config-route-map)# set weight 33</pre>	BGP ルートの重み値を設定します。範囲は 0 ～ 65535 です。

set metric-type internal コマンドは、発信ポリシーと eBGP ネイバーにのみ作用します。同じ BGP ピア発信ポリシーに **metric** コマンドと **metric-type internal** コマンドを両方設定した場合、Cisco NX-OS は **metric-type internal** コマンドを無視します。

Route Policy Manager の設定の確認

Route Policy Manager の設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show ip community-list <i>[name]</i>	コミュニティ リストの情報を表示します。
show ip ext community-list <i>[name]</i>	拡張コミュニティ リストの情報を表示します。
show [ip] prefix-list <i>[name]</i>	IPv4プレフィックス リストの情報を表示します。
show route-map <i>[name]</i>	ルート マップの情報を表示します。

関連項目

Route Policy Manager の詳細については、次の項目を参照してください。

- [基本的 BGP の設定 \(263 ページ\)](#)



第 16 章

双方向フォワーディング検出の設定

この章では、双方向フォワーディング検出（BFD）を設定する方法について説明します。

この章は、次の項で構成されています。

- [BFD に関する情報（467 ページ）](#)
- [BFD の前提条件（469 ページ）](#)
- [注意事項と制約事項（469 ページ）](#)
- [デフォルト設定（471 ページ）](#)
- [BFD マルチホップ（471 ページ）](#)
- [BFD マルチホップのホップ数（472 ページ）](#)
- [BFD マルチホップの注意事項と制約事項（472 ページ）](#)
- [BFD の設定（472 ページ）](#)
- [IPv6 の BFD を構成する（485 ページ）](#)
- [TCAM リージョンサイズの設定（493 ページ）](#)
- [BFD マルチホップセッショングローバルインターバルパラメータの設定（494 ページ）](#)
- [マルチホップセッション単位の BFD パラメータの設定（495 ページ）](#)
- [BFD 設定の確認（496 ページ）](#)
- [BFD のモニタリング（496 ページ）](#)

BFD に関する情報

BFD は、メディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルの転送パス障害を高速で検出するように設計された検出プロトコルです。BFD を使用することで、さまざまなプロトコルの Hello メカニズムにより、変動速度ではなく一定速度で転送パス障害を検出できます。BFD はプロファイリングおよびプランニングを簡単にし、再コンバージェンス時間の一貫性を保ち、予測可能にします。

BFD では、2 台の隣接デバイス間のサブセカンド障害を検出します。

非同期モード

Cisco NX-OS は、BFD 非同期モードをサポートします。BFD 非同期モードでは、2 個の隣接するデバイス間で BFD 制御パケットが送信され、デバイス間の BFD ネイバーセッションがアクティベートされ、維持されます。両方のデバイス（または BFD ネイバー）で BFD を設定できます。適切なプロトコルで一度 BFD がイネーブルになると、Cisco NX-OS は BFD セッションを作成し、BFD セッションパラメータをネゴシエートし、BFD 制御パケットをネゴシエートされた間隔で各 BFD ネイバーに送信し始めます。BFD セッションパラメータは、次のとおりです。

- 目的の最小送信間隔：このデバイスが BFD Hello メッセージを送信する間隔。
- 必要最小受信間隔：このデバイスが別の BFD デバイスからの BFD Hello メッセージを受け付ける最小間隔。
- 検出乗数：転送パスの障害を検出するまでに喪失した、別の BFD デバイスからの BFD Hello メッセージの数。

BFD の障害検出

一度 BFD セッションが確立され、タイマー ネゴシエーションが終了すると、BFD ネイバーは、より速い速度の場合を除き IGP Hello プロトコルと同じ動作をする BFD 制御パケットを送信し、活性度を検出します。BFD は障害を検出しますが、プロトコルが障害の発生したピアをバイパスするための処置を行う必要があります。

BFD は転送パスに障害を検出したとき、障害検出通知を BFD 対応プロトコルに送信します。ローカルデバイスは、プロトコル再計算プロセスを開始してネットワーク全体の収束時間を削減できます。

ネットワークで障害が発生すると、次のことが発生します。

1. BFD 隣接ルータでの BFD ネイバー セッションが停止します。
2. BFD はローカル BFD プロセスに BFD ネイバーに接続できなくなったことを通知します。
3. ローカル BFD プロセスは BFD ネイバー関係を解除します。
4. 代替パスが使用可能な場合、ルータはただちにそのパスでコンバージェンスを開始します。



(注) BFD 障害検出は 1 秒未満で行われます。

BFD エコー機能

BFD エコー機能は、転送エンジンからリモート BFD ネイバーにエコー パケットを送信します。BFD ネイバーは検出を実行するために同じパスに沿ってエコー パケットを返送します。BFD ネイバーは、エコー パケットの実際の転送に参加しません。エコー機能および転送エンジンが検出の処理を行います。BFD はエコー機能がイネーブルになっている場合に非同期セッションの速度を低下させ、2 台の BFD ネイバー間で送信される BFD 制御パケット数を減らすために、slow timer を使用できます。また、転送エンジンは、リモートシステムを含めないでリモート（ネイバー）システムの転送パスをテストするので、パケット間遅延の変動が少なくなり、障害検出時間が短縮されます。

BFD ネイバーの両方がエコー機能を実行している場合、エコー機能は非対称になります。

セキュリティ

Cisco NX-OS は BFD パケットを隣接する BFD ピアから受信したことを確認するためにパケットの存続可能時間（TTL）値を使用します。すべての非同期およびエコー要求パケットの場合、BFD ネイバーは TTL 値を 255 に設定し、ローカル BFD プロセスは着信パケットを処理する前に TTL 値を 255 として確認します。エコー応答パケットの場合、BFD は TTL 値を 254 に設定します。

仮想化のサポート

BFD は、仮想ルーティングおよび転送（VRF）インスタンスをサポートしています。

BFD の前提条件

BFD には、次の前提条件があります。

- BFD 機能を有効にする必要があります（[BFD 機能の有効化](#)のセクションを参照）。
- クライアント プロトコル上で BFD を有効にする場合は、そのクライアント プロトコルの BFD を有効にします。「[BFD for IPv6 の構成](#)」セクションを参照してください。
- BFD 対応インターフェイスでインターネット制御メッセージプロトコル（ICMP）リダイレクト メッセージをディセーブルにします。
- 設定作業とともに一覧表示されているその他の詳細な前提条件を参照してください。
- BFD は BGP および PIM でサポートされます。

注意事項と制約事項

BFD 設定時のガイドラインと制約事項は次のとおりです。

- BFD は BFD バージョン 1 をサポートします。
- BFD は、IPv4、IPv6、OSPFv2、BGPv4 およびスタティック ルートをサポートします。
- BFD は、シングルホップ BFD をサポートします。
- BGP の BFD は、送信元更新でシングル ホップ eBGP および iBGP をサポートします。
- BFD は、レイヤ 3 インターフェイスとして、物理インターフェイス、ポートチャネル、サブインターフェイス、および VLAN インターフェイス (SVI) をサポートします。
- BFD は、すべてのインターフェイスの認証をサポートしています。
- BFD はレイヤ 3 隣接情報に応じて、レイヤ 2 のトポロジ変更を含むトポロジ変更を検出します。レイヤ 3 隣接情報が使用できない場合、VLAN インターフェイス (SVI) の BFD セッションはレイヤ 2 トポロジのコンバージェンス後に稼働しない可能性があります。
- ポート チャネル設定の制限事項

BFD で使用されるレイヤ 3 ポート チャネルでは、ポート チャネルの Link Aggregation Control Protocol (LACP) を有効にする必要があります。

SVI セッションで使用されるレイヤ 2 ポートチャネルでは、ポートチャネルの LACP を有効にする必要があります。

- SVI の制限事項

トポロジを変更すると（たとえば、VLAN へのリンクの追加または削除、レイヤ 2 ポートチャネルからのメンバの削除など）、SVI セッションが影響を受ける場合があります。SVI セッションはダウンした後、トポロジ ディスカバリの終了後に起動する場合があります。



ヒント SVI のセッションがフラップしないようにし、トポロジを変更する必要がある場合は、変更を加える前に BFD 機能をディセーブルにして、変更後、BFD を再度イネーブルにできます。また、大きな値（たとえば、5 秒）になるように BFD タイマーを設定し、上記のイベントの完了後に高速なタイマーに戻すこともできます。

- Cisco NX-OS は、BFD パケット処理の CPU 負荷軽減のための、互換モジュールへの BFD 動作の分散は行いません。
- BFD はステートレス リスタートおよびインサービスソフトウェアアップグレード (ISSU) をサポートしません。
- ポート チャネル経由で到達可能なピアに対して BFD を有効にする場合は、ポートチャネルで LACP を設定することをお勧めします。
- BFD エコー モードとユニキャスト リバース パス転送 (URPF) は相互に排他的であり、BFD インターフェイスで両方を有効にすることはできません。BFD のインターフェイスを構成する場合は、BFD エコーモードまたは URPF のいずれかを無効にする必要があります。

- スタティック IPv6 ルートは、BFD でサポートされています。
- BFD は、IPv6 エコー モードをサポートしません。BFD は IPv6 リンク ローカル アドレスのみを使用します。

デフォルト設定

次の表に、BFD パラメータのデフォルト設定値を示します。

表 21: デフォルトの BFD パラメータ

パラメータ	デフォルト
BFD 機能	ディセーブル
必要最小受信間隔	250 ミリ秒
目的の最小送信間隔	250 ミリ秒
BFD セッションのエコー Rx 間隔	50 ミリ秒
検出乗数	3
エコー機能	イネーブル
モード	非同期
ポート チャネル	論理モード (送信元/宛先ペアのアドレスごとに 1 セッション)
slow timer	2000 ミリ秒
起動タイマー	5 秒

BFD マルチホップ

IPv4 用の BFD マルチホップと IPv6 用の BFD マルチホップは、RFC 5883 に準拠した Cisco Nexus 36180YC-R および 3636C-R スイッチでサポートされています。マルチホップルート上に IPv4 または IPv6 BFD セッションを設定できます。BFD マルチホップセッションは、固有のソースと宛先アドレス ペア間で設定されます。マルチホップ BFD セッションは、シングルホップ BFD セッションの場合のようなインターフェイスではなく、送信元と宛先間のリンクに関連付けられます。

BFD マルチホップのホップ数

BFD マルチホップはTTLフィールドを最大制限に設定し、受信時に値をチェックしません。BFD コードは、BFD マルチホップ パケットが通過できるホップ数には影響しません。ただし、ほとんどのシステムでは、ホップ数が 255 に制限されています。

BFD マルチホップの注意事項と制約事項

BFD マルチホップ設定時の注意事項と制約事項は次のとおりです。

- BFD マルチホップは、Cisco Nexus 36180YC-R および 3636C-R スイッチでのみサポートされます。
- BFD マルチホップ は、UDP 宛先ポート 4784 で識別されます。
- エコー モードは BFD マルチホップではサポートされません。
- サポートされる最小タイマーとセッション数は異なる場合があります。デフォルト タイマーは 250 ミリ秒です。
- セグメント ルーティング アンダーレイによるマルチホップはサポートされていません。
- 既存の BFD 認証サポートは、マルチホップ セッション用にも拡張されています。
- BFD マルチホップは、IPv4 または IPv6 アドレスをサポートします。
- サポートされていないプラットフォームでは、BGPv6 マルチホップ ネイバーを設定するときに BFD コマンドが受け入れられます。ただし、セッションは作成またはインストールされません。
- サポートされる BFD マルチホップ セッションの最大数はプラットフォームにより決まります。
- Cisco Nexus 36180YC-R および 3636C-R スイッチでは、BFD マルチホップ セッションを有効にするために TCAM スペースを手動で分割する必要があります。TCAM スペースの切り分け後には、スイッチをリロードする必要があります。

BFD の設定

このセクションは、次のトピックで構成されています。

設定階層

BFD は、グローバル レベル、VRF のレベル、インターフェイスまたはポート チャネル レベル、またはサブインターフェイス レベルで設定できます（物理インターフェイスとポートチャ

ネルの場合)。VRF の設定はグローバル設定よりも優先されます。インターフェイスまたはポート チャンネルの設定は、VRF またはグローバル設定よりも優先されます。サポートされているインターフェイス上での、サブインターフェイス レベルの設定は、サブインターフェイスの最適化がイネーブルになっていない限りインターフェイスまたはポートチャンネル設定よりも優先されます。詳細については、サブインターフェイスの BFD の最適化のセクションを参照してください。

ポート チャンネルのメンバである物理ポートについては、メンバ ポートはプライマリ ポートチャンネルの BFD 設定を継承します。メンバー ポート サブインターフェイスは、サブインターフェイスの最適化がイネーブルになっていない限り、マスター ポートチャンネルの BFD 設定よりも優先させることができます。

BFD 設定のタスク フロー

BFD の設定には、次の作業を行います。

手順

ステップ 1 [BFD機能のイネーブル化](#)

ステップ 2 [グローバルな BFD パラメータの設定またはインターフェイスでの BFD の設定](#)

BFD 機能のイネーブル化

インターフェイスとプロトコルの BFD を設定する前に、BFD 機能をイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **feature bfd**
3. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定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 2	feature bfd 例： switch(config)# feature bfd	BFD 機能をイネーブルにします。
ステップ 3	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	この設定変更を保存します。

グローバルな BFD パラメータの設定

デバイスのすべての BFD セッションの BFD セッションパラメータを設定できます。BFD セッションパラメータは、スリーウェイ ハンドシェイクの BFD ピア間でネゴシエートされます。

インターフェイスでこれらのグローバルなセッションパラメータを上書きするには、[インターフェイスでの BFD の設定](#)のセクションを参照してください。

始める前に

BFD 機能をイネーブルにします。[BFD 機能のイネーブル化](#)のセクションを参照してください。

手順の概要

1. **configure terminal**
2. **bfd interval *mintx* min_rx msec multiplier value**
3. **bfd slow-timer interval**
4. **exit**
5. (任意) **show running-config bfd**
6. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	bfd interval <i>mintx</i> min_rx msec multiplier value 例： switch(config)# bfd interval 250 min_rx 250 multiplier 3	デバイスのすべての BFD セッションの BFD セッションパラメータを設定します。インターフェイスで BFD セッションパラメータを設定することにより、これらの値を上書きすることができます。 <i>mintx</i> お

	コマンドまたはアクション	目的
		よび msec の範囲は 250 ～ 999 ミリ秒で、デフォルトは 250 です。乗数の範囲は 3 ～ 50 です。乗数のデフォルトは 3 です。 デフォルト設定に戻すには、no bfd interval コマンドを使用します。
ステップ 3	bfd slow-timer interval 例 : <pre>switch(config)# bfd slow-timer 2000</pre>	スロー タイマーを設定します。この値は BFD が新しいセッションを開始する速度を決定し、BFD エコー機能がイネーブルの場合に非同期セッションの速度を低下させるために使用されます。指定できる範囲は 1000 ～ 30000 ミリ秒です。デフォルトは 2000 です。 デフォルト設定に戻すには、no bfd slow-timer コマンドを使用します。
ステップ 4	exit 例 : <pre>switch(config)# exit switch#</pre>	EXEC モードに戻ります。
ステップ 5	(任意) show running-config bfd 例 : <pre>switch# show running-config bfd</pre>	BFD の実行構成を表示します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch# copy running-config startup-config</pre>	この設定変更を保存します。

インターフェイス上での BFD の設定

BFD 機能をイネーブルにします。 [BFD 機能のイネーブル化](#) のセクションを参照してください。

始める前に

インターフェイスのすべての BFD セッションの BFD セッションパラメータを設定できます。BFD セッションパラメータは、スリーウェイ ハンドシェイクの BFD ピア間でネゴシエートされます。

この設定は、設定されたインターフェイスのグローバルセッション パラメータより優先されます。

手順の概要

1. configure terminal

2. **interface** *int-if*
3. **no ip redirect**
4. **bfd interval** *mintx min_rx msec multiplier value*
5. **exit**
6. **exit**
7. (任意) **show running-config bfd**
8. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 <i>int-if</i> 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	インターフェイス設定モードを開始します。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 3	no ip redirect 例 : <pre>switch(config-if)# no ip redirect</pre>	Internet Control Message Protocol (ICMP) リダイレクト メッセージを無効にします。
ステップ 4	bfd interval <i>mintx min_rx msec multiplier value</i> 例 : <pre>switch(config-if)# bfd interval 250 min_rx 250 multiplier 3</pre>	インターフェイスのすべての BFD セッションの BFD セッションパラメータを設定します。このコマンドはグローバルな BFD セッションパラメータより優先されます。 <i>mintx</i> および <i>msec</i> の範囲は 250 ～ 999 ミリ秒で、デフォルトは 250 です。乗数の範囲は 3 ～ 50 です。乗数のデフォルトは 3 です。 デフォルト設定に戻すには、 no bfd interval コマンドを使用します。
ステップ 5	exit 例 : <pre>switch(config-if)# exit switch (config)#</pre>	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 6	exit 例 : <pre>switch (config)# exit switch#</pre>	コンフィギュレーション モードを終了し、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 7	(任意) show running-config bfd 例 : <pre>switch# show running-config bfd</pre>	BFD の実行構成を表示します。
ステップ 8	(任意) copy running-config startup-config 例 : <pre>switch# copy running-config startup-config</pre>	この設定変更を保存します。

ポートチャネルの BFD の設定

ポートチャネルのすべての BFD セッションの BFD セッションパラメータを設定できます。たとえば、ポートチャネルの 1 つのリンクの BFD セッションが稼働している場合、BGP などのクライアントプロトコルにポートチャネルが稼働していることが通知されます。BFD セッションパラメータは、スリーウェイハンドシェイクの BFD ピア間でネゴシエートされます。

この設定は、設定されたポートチャネルのグローバルセッションパラメータより優先されます。ポートチャネルのメンバーポートは、メンバーポートのサブインターフェイスレベルで BFD パラメータを設定しない限り、ポートチャネルの BFD セッションパラメータを継承します。その場合、サブインターフェイス最適化がイネーブルにされていないと、メンバーポートサブインターフェイスはサブインターフェイス BFD コンフィギュレーションを使用します。詳細については、サブインターフェイスの BFD の最適化のセクションを参照してください。

始める前に

BFD をイネーブルにする前に、ポートチャネルの Link Aggregation Control Protocol (LACP) がイネーブルにされていることを確認します。

BFD 機能をイネーブルにします。[BFD 機能のイネーブル化](#)のセクションを参照してください。

手順の概要

1. **configure terminal**
2. **interface port-channel *number***
3. (任意) **bfd interval *mintx min_rx msec multiplier value***
4. **exit**
5. **exit**
6. (任意) **show running-config bfd**
7. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 port-channel number 例 : <pre>switch(config)# interface port-channel 2 switch(config-if)#</pre>	ポート チャネル コンフィギュレーション モードを開始します。? キーワードを使用して、サポートされる数値の範囲を表示します。
ステップ 3	(任意) bfd interval mintx min_rx msec multiplier value 例 : <pre>switch(config-if)# bfd interval 250 min_rx 250 multiplier 3</pre>	インターフェイスのすべての BFD セッションの BFD セッションパラメータを設定します。このコマンドはグローバルな BFD セッションパラメータより優先されます。mintx および msec の範囲は 250 ～ 999 ミリ秒で、デフォルトは 250 です。乗数の範囲は 3 ～ 50 です。乗数のデフォルトは 3 です。 デフォルト設定に戻すには、no bfd interval コマンドを使用します。
ステップ 4	exit 例 : <pre>switch(config-if)# exit switch (config)#</pre>	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 5	exit 例 : <pre>switch (config)# exit switch#</pre>	コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 6	(任意) show running-config bfd 例 : <pre>switch# show running-config bfd</pre>	BFD の実行構成を表示します。
ステップ 7	(任意) copy running-config startup-config 例 : <pre>switch# copy running-config startup-config</pre>	この設定変更を保存します。

BFD エコー機能の設定

BFD モニタ対象リンクの一端または両端で BFD エコー機能を設定できます。エコー機能は設定された `slow timer` に基づいて必要最小受信間隔を遅くします。`[RequiredMinEchoRx]` BFD セッションパラメータは、エコー機能がディセーブルの場合、ゼロに設定されます。`slow timer` は、エコー機能がイネーブルの場合、必要最小受信間隔になります。

始める前に

BFD 機能をイネーブルにします。[BFD 機能のイネーブル化](#)のセクションを参照してください。

BFD セッションパラメータを設定します。「[グローバルな BFD パラメータの設定](#)」のセクションまたは「[インターフェイスでの BFD の設定](#)」のセクションを参照してください。

インターネット制御メッセージプロトコル (ICMP) のリダイレクトメッセージが BFD 対応インターフェイスでディセーブルであることを確認します。インターフェイスで `no ip redirects` コマンドを使用します。

手順の概要

1. **configure terminal**
2. **bfd slow-timer echo-interval**
3. **interface int-if**
4. **bfd echo**
5. **exit**
6. **exit**
7. (任意) **show running-config bfd**
8. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	bfd slow-timer echo-interval 例 : <pre>switch(config)# bfd slow-timer 2000</pre>	エコー機能で使用する <code>slow timer</code> を設定します。この値は BFD が新しいセッションを開始する速度を決定し、BFD エコー機能がイネーブルの場合に非同期セッションの速度を低下させるために使用されます。この値は、エコー機能がイネーブルの場合、必要最小受信間隔より優先されます。指定できる範囲

	コマンドまたはアクション	目的
		は 1000 ～ 30000 ミリ秒です。デフォルトは 2000 です。 デフォルト設定に戻すには、no bfd slow-timer コマンドを使用します。
ステップ 3	interface int-if 例： switch(config)# interface ethernet 2/1 switch(config-if)#	インターフェイス設定モードを開始します。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 4	bfd echo 例： switch(config-if)# bfd echo	エコー機能をイネーブルにします。デフォルトではイネーブルになっています。 エコー機能をディセーブルにするには、no bfd echo コマンドを使用します。
ステップ 5	exit 例： switch(config-if)# exit switch (config)#	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 6	exit 例： switch (config)# exit switch#	コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 7	(任意) show running-config bfd 例： switch# show running-config bfd	BFD の実行構成を表示します。
ステップ 8	(任意) copy running-config startup-config 例： switch# copy running-config startup-config	この設定変更を保存します。

BGP での BFD の設定

ボーダー ゲートウェイ プロトコル (BGP) の BFD を設定できます。

始める前に

BFD 機能をイネーブルにします。[BFD 機能のイネーブル化](#)のセクションを参照してください。

BFD セッション パラメータを設定します。[グローバルな BFD パラメータの設定](#)のセクション、または[インターフェイスでの BFD の設定](#)のセクションを参照してください。

手順の概要

1. **configure terminal**
2. **router bgp as-number**
3. **neighbor { ip-address } remote-as as-number**
4. **bfd**
5. (任意) **show running-config bfd**
6. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router bgp as-number 例 : <pre>switch(config)# router bgp 64496 switch(config-router)#</pre>	BGP を有効にして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。
ステップ 3	neighbor { ip-address } remote-as as-number 例 : <pre>switch(config-router)# neighbor 209.165.201.1 remote-as 64497 switch(config-router-neighbor)#</pre>	リモート BGP ピアの IPv4 アドレスおよび AS 番号を設定します。The <i>ip-address</i> 形式は x.x.x.x です。
ステップ 4	bfd 例 : <pre>switch(config-router-neighbor)# bfd</pre>	この BGP ピアの BFD をイネーブルにします。
ステップ 5	(任意) show running-config bfd 例 : <pre>switch# show running-config bfd</pre>	BFD の実行構成を表示します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch# copy running-config startup-config</pre>	この設定変更を保存します。

PIM (Protocol Independent Multicast) での BFD の設定

PIM (Protocol Independent Multicast) プロトコルの BFD を設定できます。

始める前に

BFD機能をイネーブルにします。BFD機能のイネーブル化のセクションを参照してください。

PIM機能をイネーブルにします。詳細については、『Cisco Nexus 3600 スイッチ NX-OS マルチキャストルーティング構成ガイド』を参照してください。

手順の概要

1. **configure terminal**
2. **ip pim bfd**
3. **interface type slot/port**
4. (任意) **ip pim bfd-instance [disable]**
5. (任意) **show running-config pim**
6. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	ip pim bfd 例 : switch(config)# ip pim bfd	PIM の BFD をイネーブルにします。
ステップ 3	interface type slot/port 例 : switch(config)# interface ethernet 2/1 switch(config-if)#	インターフェイス設定モードを開始します。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 4	(任意) ip pim bfd-instance [disable] 例 : switch(config-if)# ip pim bfd-instance	PIM インターフェイスの BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 5	(任意) show running-config pim 例 :	PIM の実行コンフィギュレーションを表示します。

	コマンドまたはアクション	目的
	switch(config)# show running-config pim	
ステップ 6	(任意) copy running-config startup-config 例 : switch# copy running-config startup-config	この設定変更を保存します。

OSPFv2 での BFD の設定

Open Shortest Path First Protocol (OSPFv2) で BFD を設定できます。

始める前に

BFD 機能をイネーブルにします。[BFD 機能のイネーブル化](#)のセクションを参照してください。

BFD セッションパラメータを設定します。[グローバルな BFD パラメータの設定](#)のセクション、または[インターフェイスでの BFD の設定](#)のセクションを参照してください。

OSPFv2 機能を有効にします。

手順の概要

1. **configure terminal**
2. **router ospf process-id**
3. **bfd**
4. (任意) **show running-config ospf**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	router ospf process-id 例 : switch(config)# router ospf 64496 switch(config-router)#	設定された ID で新しい OSPFv2 プロセスを作成します。
ステップ 3	bfd 例 :	この OSPFv2 ピアの BFD を有効にします。デフォルト値は [無効 (Disabled)] です。

	コマンドまたはアクション	目的
	<code>switch(config-router)# bfd</code>	
ステップ 4	(任意) show running-config ospf 例 : <code>switch(config)# show running-config ospf</code>	OSPFv2 実行設定を表示します。
ステップ 5	(任意) copy running-config startup-config 例 : <code>switch# copy running-config startup-config</code>	この設定変更を保存します。

スタティック ルートの BFD の設定

インターフェイスのスタティック ルータの BFD を設定できます。Virtual Routing and Forwarding (VRF) インスタンス内のスタティック ルートでの BFD を任意で設定できます。

始める前に

BFD 機能をイネーブルにします。[BFD 機能のイネーブル化](#)のセクションを参照してください。

手順の概要

1. **configure terminal**
2. (任意) **vrf context vrf-name**
3. **ip route route interface { nh-address | nh-prefix }**
4. **ip route static bfd interface {nh-address | nh-prefix}**
5. (任意) **show ip route static [vrf vrf-name]**
6. (任意) **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <code>switch# configure terminal</code> <code>switch(config)#</code>	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	(任意) vrf context vrf-name 例 : <code>switch(config)# vrf context Red</code> <code>switch(config-vrf)#</code>	VRF 設定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	ip route route interface { nh-address nh-prefix } 例 : <pre>switch(config-vrf)# ip route 192.0.2.1 ethernet 2/1 192.0.2.4</pre>	スタティック ルートを作成します。 ? キーワードを使用して、サポートされているインターフェイスを表示します。
ステップ 4	ip route static bfd interface {nh-address nh-prefix} 例 : <pre>switch(config-vrf)# ip route static bfd ethernet 2/1 192.0.2.4</pre>	インターフェイスのすべてのスタティック ルートの BFD をイネーブルにします。 ? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 5	(任意) show ip route static [vrf vrf-name] 例 : <pre>switch(config-vrf)# show ip route static vrf Red</pre>	スタティック ルートを表示します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch# copy running-config startup-config</pre>	この設定変更を保存します。

IPv6 の BFD を構成する

IPv6 のグローバルな BFD パラメータの構成

1. configure terminal
2. bfd [ipv4 | ipv6] interval [interval min_rx milliseconds multiplier interval-multiplier]

始める前に

BFD パラメータを構成する際に、IPv4 または IPv6 アドレス ファミリを指定できます。

手順の概要

1. configure terminal
2. bfd [ipv4 | ipv6] interval [interval min_rx milliseconds multiplier interval-multiplier]

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	bfd [ipv4 ipv6] interval [interval min_rx milliseconds multiplier interval-multiplier] 例 : <pre>switch(config)# bfd ipv6 interval 50 min_rx 50 multiplier 3</pre>	デバイスの指定されたアドレスファミリで、すべての BFD セッションの BFD セッション パラメータを構成します。 Tx および Rx 間隔の範囲は 50 ～ 999 ミリ秒です。 乗数の範囲は 3 ～ 50 です。

IPv6 のインターフェイス BFD パラメータの構成

始める前に

デバイスで BFD を有効にする必要があります。

手順の概要

1. **configure terminal**
2. **interface interface**
3. **bfd [ipv4 | ipv6] interval [interval min_rx milliseconds multiplier interval-multiplier]**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 interface 例 : <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>	インターフェイス設定モードを開始します。 ? キーワードを使用して、サポートされるインターフェイスを表示します。

	コマンドまたはアクション	目的
ステップ 3	bfd [ipv4 ipv6] interval [interval min_rx milliseconds multiplier interval-multiplier] 例 : <pre>switch(config-if)# bfd ipv6 interval 50 min_rx 50 multiplier 3</pre>	デバイスの指定されたアドレスファミリで、すべての BFD セッションの BFD セッションパラメータを構成します。 Tx および Rx 間隔の範囲は 50 ～ 999 ミリ秒です。 乗数の範囲は 3 ～ 50 です。

OSPFv3 での IPv6 用 BFD の構成

Open Shortest Path First Protocol (OSPFv3) で IPv6 の BFD を構成できます。

始める前に

- BFD 機能をイネーブルにします。 [BFD 機能のイネーブル化](#)のセクションを参照してください。
- OSPFv3 機能を有効にします。
- BFD セッションパラメータを設定します。「[IPv6 のグローバル BFD パラメータの構成](#)」のセクションまたは「[IPv6 のインターフェイス BFD パラメータの構成](#)」のセクションを参照してください。
- OSPFv3 機能を有効にします。

手順の概要

1. **configure terminal**
2. **router ospfv3 process-id**
3. **bfd**
4. (任意) **show running-config ospfv3**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 2	router ospfv3 <i>process-id</i> 例 : <pre>switch(config)# router ospfv3 201 switch(config-router)#</pre>	設定された ID で新しい OSPFv2 プロセスを作成します。
ステップ 3	bfd 例 : <pre>switch(config-router)# bfd</pre>	この OSPFv3 ピアの BFD を有効にします。デフォルト値は [無効 (Disabled)] です。
ステップ 4	(任意) show running-config ospfv3 例 : <pre>switch(config-router)# show running-config ospfv3</pre>	OSPFv3 実行設定を表示します。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config-router)# copy running-config startup-config</pre>	この設定変更を保存します。

IPv6 スタティックルートの BFD の構成

インターフェイスのすべての IPv6 スタティック ルートの BFD を構成できます。

始める前に

- スタティックルートの両端にあるデバイスで BFD が有効になっていることを確認します。
- BFD セッション パラメータを構成していることを確認します。

手順の概要

1. **configure terminal**
2. (任意) **vrf context *vrf-name***
3. **ipv6 route *route* interface { *nh-address* | *nh-prefix* }**
4. **ipv6 route static bfd *network-interface* {*nh-address* | *nh-prefix* }**
5. (任意) **show bfd neighbors**
6. (任意) **show ipv6 route static**
7. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	(任意) vrf context vrf-name 例 : <pre>switch(config)# vrf context Red switch(config-vrf)#</pre>	VRF コンフィギュレーション モードを開始して、IPv6 スタティック ルート上で BFD を構成します。 トラッキングするルートの VRF を指定します。
ステップ 3	ipv6 route route interface { nh-address nh-prefix } 例 : <pre>switch(config-vrf)# ipv6 route 1::5/64 ethernet 1/3 2::2</pre>	IPv6 スタティック ルートを作成します。 - ルート引数に IPv6 アドレスを指定します。 ? キーワードを使用して、サポートされるインターフェイスを表示します。 - このスタティック ルートのネクストホップ (nh) アドレスまたはプレフィックスを指定します。
ステップ 4	ipv6 route static bfd network-interface {nh-address nh-prefix } 例 : <pre>switch(config-vrf)# ipv6 route static bfd ethernet 1/3 2::2</pre>	インターフェイスのすべての IPv6 スタティック ルートの BFD を有効にします。 ? キーワードを使用して、サポートされるインターフェイスを表示します。 - このスタティック ルートのネクストホップ (nh) アドレスまたはプレフィックスを指定します。
ステップ 5	(任意) show bfd neighbors 例 : <pre>switch(config-vrf)# show bfd neighbors</pre>	BFD ネイバーに関する情報を表示します。
ステップ 6	(任意) show ipv6 route static 例 : <pre>switch(config-vrf)# show ipv6 route static vrf Red</pre>	スタティック ルートを表示します。
ステップ 7	(任意) copy running-config startup-config 例 :	この設定変更を保存します。

	コマンドまたはアクション	目的
	switch(config-vrf)# copy running-config startup-config	

BFD エコー モードの設定

エコー機能はデフォルトで有効になっています。必要に応じて無効にできます。

手順の概要

1. **configure terminal**
2. **interface type slot/port**
3. **[no] bfd ipv4 echo**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 type slot/port 例 : <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>	インターフェイス設定モードを開始します。 ? キーワード を使用して、サポートされるインターフェイスを表示します。
ステップ 3	[no] bfd ipv4 echo 例 : <pre>switch(config-if)# bfd ipv4 echo</pre>	エコー機能をイネーブルにします。デフォルトではイネーブルになっています。 指定されたアドレスファミリのエコー機能を無効にするには、このコマンドの no 形式を使用します。

BFD セッション エコー間隔の構成

BFD セッションのエコー Rx 間隔を構成できます。

手順の概要

1. **configure terminal**
2. **interface interface**
3. **[no] bfd ipv4 echo-rx-interval interval**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 interface 例 : <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>	インターフェイス設定モードを開始します。 ? キーワード を使用して、サポートされるインターフェイスを表示します。
ステップ 3	[no] bfd ipv4 echo-rx-interval interval 例 : <pre>switch(config-if)# bfd ipv4 echo-rx-interval 500</pre>	BFD セッションのエコー Rx 間隔を構成します。この間隔は、50～999 ミリ秒の範囲で設定できます。 エコー間隔をデフォルト値の 50 ミリ秒に戻すには、このコマンドの no 形式を使用します。

BFD エコー インターフェイスの構成

ループバック インターフェイスをエコー フレームの送信元アドレスとして構成するには、次の作業を実行します。

手順の概要

1. **configure terminal**
2. **interface loopback number**
3. **ip address ip-address mask**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 2	interface loopback number 例 : <pre>switch(config)# interface loopback 50 switch(config-if)#</pre>	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	ip address ip-address mask 例 : <pre>switch(config-if)# ip address 192.108.1.27 255.255.255.0</pre>	IP アドレスをすべてのエコー フレームの送信元アドレスとして構成します。

BFD 低速タイマーの設定

エコーモードはデフォルトでイネーブルになっています。アドレスファミリに対して slow-timer 値を構成し、エコー モードを無効または有効にできます。

手順の概要

1. **configure terminal**
2. **interface interface**
3. **bfd ipv4 slow-timer [interval]**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 interface 例 : <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>	インターフェイス設定モードを開始します。 ? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 3	bfd ipv4 slow-timer [interval] 例 : <pre>switch(config-if)# bfd ipv4 slow-timer 6000</pre>	指定されたアドレスファミリのエコー機能で使用するスロータイマー（ミリ秒単位）を構成します。

TCAM リージョン サイズの設定

ACL Ternary Content Addressable Memory (TCAM) リージョンのサイズを変更できます。



(注) 単一のバンクを使用するには、`redirect_v4` リージョンと `bfd-multihop` リージョンのエントリの合計は 2048 である必要があります。次の構成を行った後、スイッチをリロードする必要があります。この構成は、Cisco Nexus 36180YC-R および 3636C-R スイッチにのみ適用されます。

手順の概要

1. `configure terminal`
2. `[no] hardware access-list tcam region bfd-multihop tcam_size`
3. `[no] hardware access-list tcam region redirect_v4 tcam_size`
4. `[optional] show running-config | include hardware region tcam_size`
5. `reload`

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	<code>configure terminal</code> 例 : <pre>switch# configure terminal switch(config)#</pre>	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	<code>[no] hardware access-list tcam region bfd-multihop tcam_size</code> 例 : <pre>switch(config)# hardware access-list tcam region bfd-multihop 100 switch(config-if)#</pre>	BFD マルチホップの ACL TCAM リージョン サイズを変更します。
ステップ 3	<code>[no] hardware access-list tcam region redirect_v4 tcam_size</code> 例 : <pre>switch(config)# hardware access-list tcam region redirect_v4 1948 switch(config-if)#</pre>	<code>redirect_v4</code> の ACL TCAM リージョン サイズを変更します。
ステップ 4	<code>[optional] show running-config include hardware region tcam_size</code> 例 :	(オプション) 実行構成と TCAM サイズを表示します。

	コマンドまたはアクション	目的
	<pre>switch(config)# show running-config include hardware hardware access-list tcam region redirect_v4 1948 hardware access-list tcam region bfd-multihop 100 switch(config)#</pre>	
ステップ 5	reload 例 : <pre>switch(config)# reload</pre>	デバイスがリロードされます。

BFD マルチホップセッション グローバル インターバル パラメータの設定

デバイスのすべての BFD セッションの BFD セッションパラメータを設定できます。セッションごとに異なる BFD セッションパラメータを設定するには、セッション単位の設定コマンドを使用します。

手順の概要

1. **configure terminal**
2. **[no] bfd interval milliseconds min_rx millisecondsmultiplier interval-multiplier**
3. **end**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	[no] bfd interval milliseconds min_rx millisecondsmultiplier interval-multiplier 例 : <pre>switch(config)# switch(config)# bfd multihop interval 250 min_rx 250 multiplier 3</pre>	デバイスのすべての BFD セッションの BFD セッションパラメータを設定します。このコマンドは、デフォルトの動作を上書きします。Required Minimum Received Interval と Desired Minimum Transmit Interval は 250 です。乗数のデフォルトは 3 です。
ステップ 3	end 例 : <pre>switch(config)# end</pre>	設定の変更を保存し、設定セッションを終了します。

マルチホップセッション単位の BFD パラメータの設定

マルチホップセッション単位の BFD パラメータを設定できます。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」を参照してください。

手順の概要

1. **configure terminal**
2. **router bgp as-number**
3. **neighbor {ip-address | ipv6-address} remote-as as-number**
4. **update-source interface**
5. **bfd**
6. **bfd multihop interval mintx min_rx msecmultiplier value**
7. **bfd multihop authentication keyed-sha1 keyid id id key ascii_key**
8. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	router bgp as-number 例 : <pre>switch(config)# router bgp 64496 switch(config-router)#</pre>	BGP を有効にして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。
ステップ 3	neighbor {ip-address ipv6-address} remote-as as-number 例 : <pre>switch(config-router)# neighbor 209.165.201.1 remote-as 64497 switch(config-router-neighbor)#</pre>	リモート BGP ピアの IPv4 アドレスまたは IPv6 アドレスおよび AS 番号を設定します。The <i>ip-address</i> 形式は x.x.x.x です。ipv6-address の形式は A:B::C:D です。
ステップ 4	update-source interface 例 : Example: <pre>switch(config-router-neighbor)# update-source</pre>	インターフェイスから BFD セッションの送信元 IP アドレスを取得します。

	コマンドまたはアクション	目的
	Ethernet1/4 switch(config-router-neighbor)#	
ステップ 5	bfd 例： switch(config-router-neighbor)# bfd	この BGP ピアの BFD をイネーブルにします。
ステップ 6	bfd multihop interval mintx min_rx msec multiplier value 例： Example: switch(config-router-neighbor)# bfd multihop interval 250 min_rx 250 multiplier 3	このネイバーのマルチホップ BFD 間隔値を設定します。mintx および msec の範囲は 250 ～ 999 ミリ秒で、デフォルトは 250 です。乗数の範囲は 1 ～ 50 です。乗数のデフォルトは 3 です。
ステップ 7	bfd multihop authentication keyed-sha1 keyid id id key ascii_key 例： Example: switch(config-router-neighbor)# bfd multihop authentication keyed-sha1 keyid 1 ascii_key cisco123	このネイバー上のマルチホップ BFD セッションで BFD の SHA-1 認証を設定します。ascii_key 文字列は BFD ピア間で共有される秘密キーです。0 ～ 255 の数値の id 値が、この特定の ascii_key に割り当てられます。BFD パケットは id でキーを指定し、複数のアクティブ キーが使用できます。 インターフェイスの SHA-1 認証を無効にするには、コマンドの形式を使用しません。
ステップ 8	(任意) copy running-config startup-config 例： switch# copy running-config startup-config	この設定変更を保存します。

BFD 設定の確認

BFD 設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show running-config bfd	実行 BFD コンフィギュレーションを表示します。
show startup-config bfd	次のシステム起動時に適用される BFD コンフィギュレーションを表示します。

BFD のモニタリング

BFD を表示するには、次のコマンドを使用します。

コマンド	目的
show bfd neighbors [application <i>name</i>] [details]	BGP などのサポートされるアプリケーションの BFD に関する情報を表示します。
show bfd neighbors [interface <i>int-if</i>] [details]	インターフェイスの BGP セッションに関する情報を表示します。
show bfd neighbors [dest-ip <i>ip-address</i>] [src-ip <i>ip-address</i>] [details]	インターフェイス上の指定された BGP セッションに関する情報を表示します。
show bfd neighbors [vrf <i>vrf-name</i>] [details]	VRF の BFD に関する情報を表示します。

これらのコマンドの出力フィールドの詳細については、[Cisco Nexus 3548 スイッチ コマンド リファレンス](#)を参照してください。



第 17 章

ポリシーベース ルーティングの設定

この章では、Cisco NX-OS デバイスでポリシー ベース ルーティングを設定する方法について説明します。

この章は、次の項で構成されています。

- [ポリシーベース ルーティングについて \(499 ページ\)](#)
- [ポリシーベース ルーティングの前提条件 \(502 ページ\)](#)
- [ポリシーベース ルーティングの注意事項と制約事項 \(502 ページ\)](#)
- [デフォルト設定 \(503 ページ\)](#)
- [ポリシーベース ルーティングの設定 \(503 ページ\)](#)
- [ポリシーベース ルーティングの設定の確認 \(508 ページ\)](#)
- [ポリシーベース ルーティングの設定例 \(508 ページ\)](#)

ポリシーベース ルーティングについて

ポリシーベース ルーティングを使用すると、IPv4 および IPv6 トラフィックフローに定義済みのポリシーを設定し、ルーティングプロトコルから派生したルートへの依存を弱めることができます。ポリシーベース ルーティングがイネーブルのインターフェイスで受信するすべてのパケットは、拡張パケット フィルタまたはルート マップを経由して渡されます。ルート マップでは、パケットの転送先を決定するポリシーを記述します。

ポリシーベース ルーティングには、次の機能が含まれます。

- 送信元ベース ルーティング：異なるユーザセットを起点とするトラフィックをポリシー ルータ上のそれぞれ異なる接続を使用してルーティングします。
- QoS (Quality of Service)：ネットワークの周辺で IP パケット ヘッダーに優先または ToS (タイプ オブ サービス) 値を設定することによって、またはキューイング メカニズムを利用して、ネットワークのコアまたはバックボーンでトラフィックにプライオリティを設定することによって、トラフィックを差別化します (『[Cisco Nexus 3600 NX-OS Quality of Service Configuration Guide](#)』を参照)。
- ロードシェアリング：トラフィックの特性に基づいて、複数のパスにトラフィックを分散します。

ポリシー ルート マップ

ルート マップのエントリごとに、**match** 文と **set** 文の組み合わせが 1 つずつ含まれています。**match** 文では、該当するパケットが特定のポリシーを満たす基準（つまり、満たすべき条件）を定義します。**set** 文節で、**match** 基準を満たしたパケットをどのようにルーティングするかを説明します。

ルート マップ文を許可または拒否として指定できます。文の解釈は次のとおりです。

- 文に許可が指定されていて、なおかつパケットが一致基準を満たしている場合は、の **set** 文節が適用されます。そのアクションの 1 つに、ネクスト ホップの選択が含まれます。
- 文に拒否が指定されている場合、一致基準を満たすパケットは標準のフォワーディング チャンネルを通じて送り返され、宛先ベース ルーティングが実行されます。
- 文が **permit** とマークされ、パケットがいずれのルート -マップ文にも一致しない場合、そのパケットは通常の転送チャンネルを介して返送され、宛先ベースのルーティングが実行されます。



(注) ポリシールーティングは、パケットの送信元となるインターフェイスではなく、パケットを受信するインターフェイス上で指定します。

ポリシーベース ルーティングの **set** 基準

Cisco Nexus 3600 プラットフォーム スイッチは、ポリシーベース ルーティングで使用されるルートマップに対して次の **set** コマンドをサポートしています。

- **set {ip | ipv6} next-hop address1 [address2...] [load-share]**
- **set interface null0**

これらの **set** コマンドは、ルートマップ シーケンス内では相互に排他的です。

最初のコマンドで、IP アドレスでは、パケットの転送先である宛先へのパス上の隣接ネクスト ホップルータを指定します。その時点でアップの接続インターフェイスに関連付けられた最初の IP アドレスがパケットのルーティングに使用されます。



(注) 任意に、最大 32 の IP アドレスにバランシング トラフィックをロードするように、ネクスト ホップアドレスのこのコマンドを設定できます。この場合、Cisco NX-OS は各 IP フローのすべてのトラフィックを特定の IP ネクスト ホップ アドレスに送信します。

パケットが定義された一致基準のいずれにも一致しない場合、そのパケットは標準の宛先ベース ルーティング プロセスを使用してルーティングされます。

ルート マップ処理ロジック

ルートマップが設定されたインターフェイスでパケットが受信されると、転送ロジックはシーケンス番号に従って各ルート マップ ステートメントを処理します。

ルート マップ文が `route-map...permit` 文の場合、パケットは `match` コマンドの基準と照合されます。このコマンドは、1つ以上のアクセスコントロールエントリ (ACE) を持つACLを参照する場合があります。パケットがACL内の許可ACEと一致する場合、ポリシーベース ルーティング ロジックはパケットに対して `set` コマンドで指定されたアクションを実行します。

ルート マップ文に `route-map...` 拒否文がある場合、パケットは一致コマンドの基準と照合されます。このコマンドは、1つ以上のACEを持つACLを参照する場合があります。パケットがACLの許可ACEに一致すると、ポリシーベース ルーティング プロセスが停止し、パケットはデフォルト IP ルーティング テーブルを使用してルーティングされます。



(注) `set` コマンドは、`route-map... deny` 文内部に影響しません。

- ルートマップ設定に `match` 文が含まれていない場合、ポリシーベース ルーティング ロジックは `set` コマンドで指定されているアクションをパケットに対して実行します。すべてのパケットは、ポリシーベース ルーティングを使用してルーティングされます。
- ルートマップコンフィギュレーションが `match` ステートメントを参照し、`match` ステートメントがアクセスコントロールエントリ (ACE) のない既存のACLまたは既存のACLを参照する場合、パケットはデフォルトルーティングテーブルを使用してルーティングされます。
- `set {ip | ipv6} next-hop` コマンドで指定されているネクスト ホップがダウンしているか、アクセス不能であるか、削除されている場合、パケットはデフォルト ルーティング テーブルを使用してルーティングされます。

Cisco NX-OS リリース 9.2(3) 以降では、`next-hop ip-address load-share` コマンドを使用して、ネクストホップが ECMP パス上で再帰的である場合、Cisco Nexus 36180YC-R スイッチ上でポリシーベース ルーティング トラフィックを分散できます。すべてのネクストホップルーティング要求については、ルーティングプロファイルマネージャ (RPM) がユニキャストルーティング情報ベース (uRIB) を使用してそれらを解決し、すべての ECMP パスをプログラムします。これにより、すべての ECMP パスの負荷が均一に分散されます。PMP over ECMP は IPv4 でのみサポートされます。

ポリシーベース ルーティング フィルタリング オプション

追加のオプションを使用してトラフィックを識別できます。次のリストには、ほとんどの追加フィルタリングオプションが含まれていますが、すべてを網羅しているわけではありません。

ポリシーベースのルーティング ACL は、次の追加フィルタリング オプションをサポートしています。

- レイヤ 3 送信元アドレスおよび/または宛先アドレス
- TCP/UDP ポート

ポリシーベース ルーティングの前提条件

追加のオプションを使用してトラフィックを識別できます。次のリストには、ほとんどの追加フィルタリングオプションが含まれていますが、すべてを網羅しているわけではありません。

ポリシーベースのルーティング ACL は、次の追加フィルタリング オプションをサポートしています。

- レイヤ 3 送信元アドレスおよび/または宛先アドレス
- TCP/UDP ポート

ポリシーベース ルーティングの注意事項と制約事項

ポリシーベース ルーティングに関する注意事項および制約事項は、次のとおりです。

- Cisco NX-OS リリース 7.0(3)F3(3) 以降、Cisco Nexus 3600 プラットフォーム スイッチは IPv4 および IPv6 ポリシーベース ルーティングをサポートします。これらのスイッチの場合、PBR ポリシーは、接続されているルートおよびローカル ルートよりも高い優先度を持ちます。プロトコルネイバーが直接接続されている場合は、明示的な許可リストが必要になることがあります。
- ポリシーベース ルーティングのルート マップでは、1 つのルート マップ文に `match` 文を 1 つだけ指定できます。
- `match` コマンドで、ポリシーベース ルーティング用ルート マップの複数の ACL を参照できません。
- インターフェイスが同じ仮想ルーティング/転送 (VRF) インスタンスに所属している場合は、ポリシーベース ルーティング対応のさまざまなインターフェイス間で、同じルート マップを共有できます。
- 一致基準としてプレフィックスリストを使用することはサポートされていません。ポリシーベース ルーティングルートマップではプレフィックスリストを使用しないでください。
- ポリシーベース ルーティングは、ユニキャストトラフィックのみをサポートします。マルチキャストトラフィックはサポートされていません。
- レイヤ 3 ポート チャネル サブインターフェイスによるポリシーベース ルーティングがサポートされます。
- ポリシーベース ルーティングのルート マップで使用する ACL には拒否アクセス コントロール エントリ (ACE) 含めることができません。

- ポリシーベースルーティングは、デフォルトのシステムルーティングモードでのみサポートされます。
- ネクストホップが ECMP パス上で再帰的である場合、ポリシーベース ルーティング トラフィックのバランスをとることはできません。代わりに、**set {ip | ipv6} next-hop ip-address load-share** コマンドを使用して隣接ネクスト ホップを指定します。
- ポリシーベース ルーティングは、VXLAN ではサポートされていません
- ポリシーベース ルーティング ポリシー統計情報はサポートされていません。

デフォルト設定

下の表に、ポリシーベース ルーティング パラメータのデフォルト設定を示します。

表 22: デフォルトのポリシーベース ルーティング パラメータ

パラメータ	デフォルト
ポリシーベース ルーティング	無効化

ポリシーベース ルーティングの設定

ポリシーベース ルーティング機能のイネーブル化

ルート ポリシーを設定する前に、ポリシーベース ルーティング機能をイネーブルにしておく必要があります。

手順の概要

1. **configure terminal**
2. **[no] feature pbr**
3. (任意) **show feature**
4. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	[no] feature pbr 例 : switch(config)# feature pbr	ポリシーベースルーティング機能をイネーブルにします。 ポリシーベース ルーティング機能を無効にするには、このコマンドの no 形式を使用します。 (注) no feature pbr コマンドは、インターフェイスに適用されているポリシーを削除します。ACL またはルートマップ設定は削除されず、システムチェックポイントも作成されません。
ステップ 3	(任意) show feature 例 : switch(config)# show feature	有効および無効にされた機能を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	この設定変更を保存します。

ECMP 上のポリシーベース ルーティングの有効化

ECMP を介した PBR は、デフォルトでは有効になっていません。ルート ポリシーを設定する前に、ポリシーベース ルーティング機能をイネーブルにしておく必要があります。

手順の概要

1. **configure terminal**
2. **[no] feature pbr**
3. (任意) **show feature**
4. **[no] hardware profile pbr ecmp paths max-paths**
5. **show system internal rpm state**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	[no] feature pbr 例 : <pre>switch(config)# feature pbr</pre>	ポリシーベースルーティング機能をイネーブルにします。 ポリシーベース ルーティング機能を無効にするには、このコマンドの no 形式を使用します。 (注) no feature pbr コマンドは、インターフェイスに適用されているポリシーを削除します。ACL またはルートマップ設定は削除されず、システムチェックポイントも作成されません。
ステップ 3	(任意) show feature 例 : <pre>switch(config)# show feature</pre>	有効および無効にされた機能を表示します。
ステップ 4	[no] hardware profile pbr ecmp paths max-paths 例 : <pre>switch(config)# hardware profile pbr ecmp paths max-paths 12 Warning!!: The pbr ecmp path limits have been changed. Please reload the switch now for the change to take effect. switch(config)# switch(config)# no hardware profile pbr ecmp paths max-paths 12 Warning!!: The pbr ecmp path limits have been changed. Please reload the switch now for the change to take effect. switch(config)#</pre>	IP ネクスト ホップの ECMP パスの数を設定します。ただし、設定された IP ネクスト ホップでロードシェアを明示的に設定しない限り、トラフィックはすべてのパスを通過しない可能性があります。PBRECMPPパスを削除または変更すると、その変更は次のリロード後にのみ有効になります。範囲は 1 ～ 64 です。
ステップ 5	show system internal rpm state	PBR ECMP パスの現在設定されている値と動作値を表示します。

ルート ポリシーの設定

ポリシーベースルーティングでルートマップを使用すると、着信インターフェイスにルーティング ポリシーを割り当てることができます。Cisco NX-OS はネクスト ホップおよびインターフェイスを検出するときに、パケットをルーティングします。

手順の概要

1. **configure terminal**
2. **interface type slot/port**
3. **{ ip | ipv6 } policy route-map map-name**
4. **route-map map-name [permit | deny] [seq]**
5. **match {ip | ipv6} address access-list-name name [name...]**
6. (任意) **set ip next-hop address1 [address2...] [load-share] [drop-on-fail]**
7. **set ipv6 next-hop address1 [address2...][load-share] [drop-on-fail]**
8. (任意) **set ip next-hop verify-availability**
9. (任意) **set interface null0**
10. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 type slot/port 例 : <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 3	{ ip ipv6 } policy route-map map-name 例 : <pre>switch(config-if)# ip policy route-map Testmap</pre>	IPv4 または IPv6 ポリシーベース ルーティング用のルートマップをインターフェイスに割り当てます。
ステップ 4	route-map map-name [permit deny] [seq] 例 : <pre>switch(config-if)# route-map Testmap switch(config-route-map)#</pre>	ルートマップを作成するか、または既存のルートマップに対応するルートマップ設定モードを開始します。seq を使用して、ルートマップ エントリを順序付けます。

	コマンドまたはアクション	目的
ステップ 5	match {ip ipv6} address access-list-name name [name...] 例 : <pre>switch(config-route-map)# match ip address access-list-name ACL1</pre>	1 つまたは複数の IPv4 または IPv6 アクセス コントロール リスト (ACL) に対して IP または IPv6 アドレスを照合します。このコマンドはポリシーベース ルーティング用であり、ルート フィルタリング または再配布では無視されます。
ステップ 6	(任意) set ip next-hop address1 [address2...] [load-share] [drop-on-fail] 例 : <pre>switch(config-route-map)# set ip next-hop 192.0.2.1</pre>	ポリシーベース ルーティング用の IPv4 ネクスト ホップアドレスを設定します。このコマンドでは、複数のアドレスが設定されている場合に、最初の有効なネクスト ホップアドレスが使用されます。 任意の load-share キーワードを使用して、最大 32 のネクスト ホップアドレスにトラフィックのロード バランシングを行います。 設定されたネクスト ホップが到達不能になったときに、デフォルト ルーティングを使用する代わりに、オプションの drop-on-fail キーワードを使用してパケットをドロップできます。
ステップ 7	set ipv6 next-hop address1 [address2...][load-share] [drop-on-fail] 例 : <pre>switch(config-route-map)# set ipv6 next-hop 2001:0DB8::1</pre>	ポリシーベース ルーティング用の IPv6 ネクスト ホップアドレスを設定します。このコマンドでは、複数のアドレスが設定されている場合に、最初の有効なネクスト ホップアドレスが使用されます。 任意の load-share キーワードを使用して、最大 32 のネクスト ホップアドレスにトラフィックのロード バランシングを行います。 設定されたネクスト ホップが到達不能になったときに、デフォルト ルーティングを使用する代わりに、オプションの drop-on-fail キーワードを使用してパケットをドロップできます。
ステップ 8	(任意) set ip next-hop verify-availability	<pre>switch(config-route-map)# set ip next-hop verify-availability</pre> スイッチがそのネクスト ホップへのポリシールーティングを実行する前に、ルート マッピングのネクストホップの到達可能性を確認するポリシールーティングを設定するには、このコマンドを使用します。
ステップ 9	(任意) set interface null0 例 : <pre>switch(config-route-map)# set interface null0</pre>	ルーティングに使用するインターフェイスを設定します。パケットをドロップするには null0 インターフェイスを使用します。

	コマンドまたはアクション	目的
ステップ 10	(任意) copy running-config startup-config 例 : <pre>switch(config-route-map)# copy running-config startup-config</pre>	この設定変更を保存します。

ポリシーベース ルーティングの設定の確認

ポリシーベース ルーティングの設定情報を表示するには、次のいずれかのタスクを実行します。

コマンド	目的
show [ip ipv6] policy [name]	IPv4 または IPv6 ポリシーに関する情報を表示します。

ポリシーベース ルーティングの設定例

インターフェイス上で単純なルート ポリシーを設定する例を示します。

```
ip access-list pbr-sample
permit tcp host 10.1.1.1 host 192.168.2.1 eq 80
!
route-map pbr-sample
match ip address pbr-sample
set ip next-hop 192.168.1.1
!
route-map pbr-sample
interface ethernet 1/2
ip policy route-map pbr-sample
```

次の出力で、この設定を確認します。

```
switch# show route-map pbr-sample
route-map pbr-sample, permit, sequence 10
Match clauses:
```

```
ip address (access-lists): pbr-sample
Set clauses:
```

```
ip next-hop 192.168.1.1
switch# show ip policy
Interface Route-map Status VRF-Name
Ethernet1/2 pbr-sample Active --
```

この例は、ECMP パスと非 ECMP パス間のロードシェアリングを示しています。

```
switch# show run rpm
!Command: show running-config rpm
!Running configuration last done at: Sun Dec 23 16:02:32 2018
!Time: Sun Dec 23 16:06:13 2018

version 9.2(3) Bios:version 08.35
```

```
feature pbr

route-map policy1 pbr-statistics
route-map policy1 permit 10
  match ip address acl2
  set ip next-hop 131.1.1.2 load-share
route-map policy2 pbr-statistics
route-map policy2 permit 10
  match ip address acl2
  set ip next-hop verify-availability 131.1.1.2 track 1
  set ip next-hop verify-availability 30.1.1.2 track 2 load-share

interface Ethernet1/31
  ip policy route-map policy2
```

この例は、ネクスト ホップ ルーティング要求に関する情報を表示しています。

```
switch# show system internal rpm pbr ip nexthop
PBR IPv4 nexthop table for vrf default

30.1.1.2 Usable
  via 28.1.1.2 Ethernet1/18 a46c.2ae3.02a7

131.1.1.2 Usable
  via 111.1.1.2 Vlan81 8478.ac58.afc1
Usable
  via 112.1.1.2 Vlan82 8478.ac58.afc1
Usable
  via 113.1.1.2 Vlan83 8478.ac58.afc1
Usable
  via 114.1.1.2 Vlan84 8478.ac58.afc1
Usable
  via 115.1.1.2 Vlan85 8478.ac58.afc1
Usable
  via 116.1.1.2 Vlan86 8478.ac58.afc1
Usable
  via 117.1.1.2 Vlan87 8478.ac58.afc1
Usable
  via 118.1.1.2 Vlan88 8478.ac58.afc1
```

この例は、ユニキャスト RIB から受け取ったルートを表示しています。

```
switch# show ip route 130.1.1.2
IP Route Table for VRF "default"
'!' denotes best ucast next-hop
'***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

130.1.1.0/24, ubest/mbest: 8/0
  *via 111.1.1.2, Vlan81, [110/120], 00:07:57, ospf-1, inter
  *via 112.1.1.2, Vlan82, [110/120], 00:07:57, ospf-1, inter
  *via 113.1.1.2, Vlan83, [110/120], 00:07:57, ospf-1, inter
  *via 114.1.1.2, Vlan84, [110/120], 00:07:57, ospf-1, inter
  *via 115.1.1.2, Vlan85, [110/120], 00:07:57, ospf-1, inter
  *via 116.1.1.2, Vlan86, [110/120], 00:07:57, ospf-1, inter
  *via 117.1.1.2, Vlan87, [110/120], 00:07:57, ospf-1, inter
  *via 118.1.1.2, Vlan88, [110/120], 00:07:57, ospf-1, inter
```

```
switch# show ip route 30.1.1.2
IIP Route Table for VRF "default"
'*' denotes best ucast next-hop
***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

30.1.1.0/24, ubest/mbest: 1/0
    *via 28.1.1.2, [1/0], 00:38:36, static
```



第 18 章

『Configuring HSRP』

この章では、Cisco NX-OS スイッチでホットスタンバイ ルータ プロトコル (HSRP) を設定する方法について説明します。

この章は、次の項で構成されています。

- [HSRP について \(511 ページ\)](#)
- [HSRP の前提条件 \(517 ページ\)](#)
- [HSRP の注意事項と制約事項 \(517 ページ\)](#)
- [HSRP のデフォルト設定 \(518 ページ\)](#)
- [『Configuring HSRP』 \(518 ページ\)](#)
- [HSRP 設定の確認 \(529 ページ\)](#)
- [HSRP の設定例 \(529 ページ\)](#)
- [その他の参考資料 \(530 ページ\)](#)

HSRP について

HSRP はファーストホップ冗長プロトコル (FHRP) であり、ファーストホップ IP ルータの透過的なフェールオーバーを可能にします。HSRP は、デフォルト ルータの IP アドレスを指定して設定された、イーサネット ネットワーク上の IP ホストにファーストホップ ルーティングの冗長性を提供します。ルータ グループでは HSRP を使用して、アクティブ ルータおよびスタンバイルータを選択します。ルータ グループでは、アクティブルータはパケットをルーティングするルータです。スタンバイ ルータは、アクティブ ルータで障害が発生した場合、または事前に設定された条件が満たされた場合に、引き継ぐルータです。

大部分のホストの実装では、ダイナミックなルータ ディスカバリ メカニズムをサポートしていませんが、デフォルトのルータを設定することはできます。すべてのホスト上でダイナミックなルータ ディスカバリ メカニズムを実行するのは、管理上のオーバーヘッド、処理上のオーバーヘッド、セキュリティ上の問題など、さまざまな理由で適切ではありません。HSRP は、そうしたホスト上にフェールオーバー サービスを提供します。

HSRP の概要

HSRP を使用する場合、HSRP の仮想 IP アドレスを（実際のルータの IP アドレスではなく）ホストのデフォルト ルータとして設定します。仮想 IP アドレスは、HSRP が動作するルータのグループで共有される IPv4 アドレスです。

ネットワーク セグメントに HSRP を設定する場合は、HSRP グループ用の仮想 MAC アドレスと仮想 IP アドレスを設定します。グループの各 HSRP 対応インターフェイス上で、同じ仮想アドレスを指定します。各インターフェイス上で、実アドレスとして機能する固有の IP アドレスおよび MAC アドレスも設定します。HSRP はこれらのインターフェイスのうちの 1 つをアクティブ ルータにするために選択します。アクティブ ルータは、グループの仮想 MAC アドレス宛てのパケットを受信してルーティングします。

指定されたアクティブ ルータで障害が発生すると、HSRP によって検出されます。その時点で、選択されたスタンバイ ルータが HSRP グループの MAC アドレスおよび IP アドレスの制御を行うことになります。HSRP はこの時点で、新しいスタンバイ ルータの選択も行います。

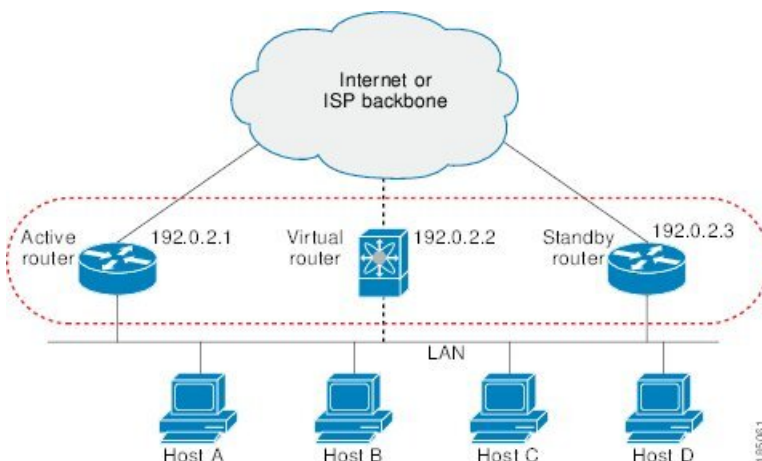
HSRP ではプライオリティメカニズムを使用して、デフォルトのアクティブ ルータにする HSRP 設定インターフェイスを決定します。アクティブ ルータとしてインターフェイスを設定するには、グループ内の他のすべての HSRP 設定インターフェイスよりも高いプライオリティを与えます。デフォルトのプライオリティは 100 なので、それよりもプライオリティが高いインターフェイスを 1 つ設定すると、そのインターフェイスがデフォルトのアクティブ ルータになります。

HSRP が動作するインターフェイスは、マルチキャストユーザデータグラムプロトコル (UDP) ベースの hello メッセージを送受信して、障害を検出し、アクティブおよびスタンバイ ルータを指定します。アクティブ ルータが設定された時間内に hello メッセージを送信できなかった場合は、最高のプライオリティのスタンバイ ルータがアクティブ ルータになります。アクティブ ルータとスタンバイ ルータ間のパケット フォワーディング機能の移動は、ネットワーク上のすべてのホストに対して完全に透過的です。

1 つのインターフェイス上で複数の HSRP グループを設定できます。

次の図に、HSRP 用に設定されたネットワークのセグメントを示します。仮想 MAC アドレスおよび仮想 IP アドレスの共有によって、2 つ以上のインターフェイスが単一の仮想ルータのように動作できます。

図 35: 2 台の対応ルータを含む HSRP トポロジ



仮想ルータは物理的には存在しませんが、相互にバックアップするように設定されたインターフェイスにとって、共通のデフォルトルータになります。アクティブルータの IP アドレスを使用して、LAN 上でホストを設定する必要はありません。代わりに、デフォルトルータとして仮想ルータの IP アドレス（仮想 IP アドレス）を使用して、ホストを設定します。アクティブルータが設定時間内に hello メッセージを送信できなかった場合は、スタンバイルータが引き継いで仮想アドレスに応答し、アクティブルータになってアクティブルータの役割を引き受けます。ホストの観点からは、仮想ルータは同じままです。



- (注) ルーテッドポートで受信した HSRP 仮想 IP アドレス宛のパケットは、ローカルルータ上で終端します。そのルータがアクティブ HSRP ルータであるのかスタンバイ HSRP ルータであるのかは関係ありません。これには ping トラフィックと Telnet トラフィックが含まれます。レイヤ 2 (VLAN) インターフェイスで受信した HSRP 仮想 IP アドレス宛のパケットは、アクティブルータ上で終端します。

HSRP for IPv4

HSRP ルータは、HSRP hello パケットを交換することによって相互に通信します。これらのパケットは、UDP ポート 1985 上の宛先 IP マルチキャストアドレス 224.0.0.2（すべてのルータと通信するための予約済みマルチキャストアドレス）に送信されます。アクティブルータは設定 IP アドレスおよび HSRP 仮想 MAC アドレスから hello パケットを得るのに対して、スタンバイルータは設定 IP アドレスおよびインターフェイス MAC アドレスから hello パケットを取得します。インターフェイス MAC アドレスは、バーンドインアドレス (BIA) のこともあれば、そうではないこともあります。BIA は、MAC アドレスの下位 6 バイトで、ネットワークカード (NIC) の製造元によって割り当てられます。

ホストはデフォルトルータが HSRP 仮想 IP アドレスとして設定されているので、HSRP 仮想 IP アドレスに関連付けられた MAC アドレスと通信する必要があります。この MAC アドレスは、仮想 MAC アドレス 0000.0C07.ACxy です。この場合、xy はそれぞれのインターフェイスに基づく、16 進数の HSRP グループ番号です。たとえば、HSRP グループ 1 は 0000.0C07.AC01

という HSRP 仮想 MAC アドレスを使用します。隣接 LAN セグメント上のホストは、標準のアドレス解決プロトコル（ARP）プロセスを使用して、関連付けられた MAC アドレスを解決します。

HSRP バージョン 2 では新しい IP マルチキャスト アドレス 224.0.0.102 を使用して hello パケットを送信します。バージョン 1 では、このマルチキャストアドレスが 224.0.0.2 です。バージョン 2 では、拡張グループ番号範囲 0 ～ 4095 を使用できます。また、新しい MAC アドレス範囲 0000.0C9F.F000 ～ 0000.0C9F.FFFF を使用します。

HSRP のバージョン

Cisco NX-OS は、デフォルトでは HSRP バージョン 1 をサポートしています。HSRP バージョン 2 を使用するようにインターフェイスを設定できます。

HSRP バージョン 2 では、HSRP バージョン 1 から次のように拡張されています。

- グループ番号の範囲が拡大されました。HSRP バージョン 1 がサポートするグループ番号は 0 ～ 255 です。HSRP バージョン 2 がサポートするグループ番号は 0 ～ 4095 です。
- IPv4 では IPv4 マルチキャスト アドレス 224.0.0.102 を使用して hello パケットを送信します。HSRP バージョン 1 では、このマルチキャストアドレスが 224.0.0.2 です。
- MAC アドレス範囲 0000.0C9F.F000 ～ 0000.0C9F.FFFF を使用します。HSRP バージョン 1 で使用する MAC アドレス範囲は、0000.0C07.AC00 ～ 0000.0C07.ACFF です。
- MD 5 認証のサポートが追加されました。

HSRP のバージョンを変更すると、Cisco NX-OS がグループを再初期化します。新しい仮想 MAC アドレスがグループに与えられるからです。

HSRP バージョン 2 では HSRP バージョン 1 とは異なるパケットフォーマットを使用します。パケットフォーマットは Type-Length-Value (TLV) です。HSRP バージョン 1 ルータは、HSRP バージョン 2 パケットを受信しても無視します。

HSRP サブネット VIP

Cisco NX-OS Release 7.0(3)F3(3) 以降、インターフェイス IP アドレスとは異なるサブネットに HSRP サブネット仮想 IP (VIP) アドレスを構成できます。

この機能を使用すると、パブリック IP アドレスとして VIP を使用し、プライベート IP アドレスとしてインターフェイス IP を使用して、パブリック IPv4 アドレスを節約できます。IPv6 アドレスには、より大きな IPv6 アドレスプールが使用可能であり、ルーティング可能な IPv6 アドレスを SVI で設定して通常の HSRP で使用できるため、IPv6 アドレスには HSRP サブネット VIP は必要ありません。

また、この機能により、vPC ピアへの定期的な ARP 同期が可能になり、VIP サブネット内のホストに対して HSRP サブネット VIP が設定されている場合に、ARP が VIP をソースとして使用できるようになります。

詳細については、「[HSRP の注意事項と制限事項](#)」および「[HSRP の設定例](#)」を参照してください。

HSRP 認証

HSRP のメッセージダイジェスト 5 (MD5) アルゴリズム認証は、HSRP スプーフィングソフトウェアから保護し、業界標準の MD5 アルゴリズムを使用して信頼性とセキュリティを向上させています。HSRP は IPv4 アドレスを認証 TLV に含めます。

HSRP メッセージ

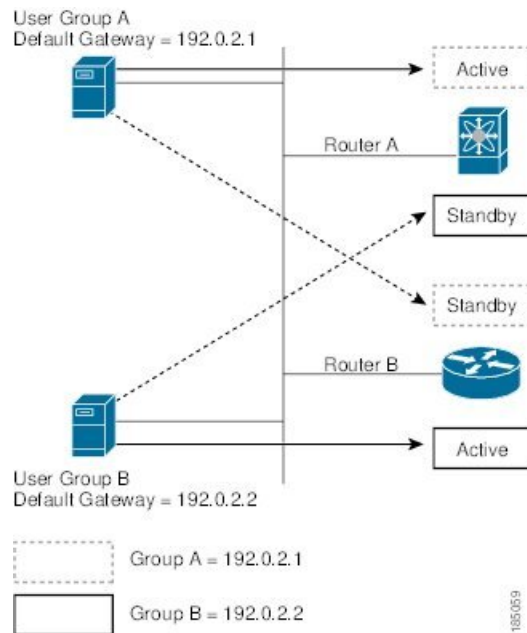
HSRP が設定されたルータは、次の 3 種類のマルチキャストメッセージを交換できます。

- **hello** : hello メッセージは、ルータの HSRP プライオリティおよびステート情報を他の HSRP ルータに伝えます。
- **coup** : スタンバイ ルータがアクティブ ルータの機能を引き受けるときに、coup メッセージを送信します。
- **resign** : アクティブ ルータは、アクティブ ルータとして機能する必要がなくなったときに、このメッセージを送信します。

HSRP ロードシェアリング

HSRP では、1 つのインターフェイスに複数のグループを設定できます。オーバーラップする 2 つの IPv4 HSRP グループを設定すると、期待されるデフォルトルータの冗長性を HSRP から提供しながら、接続ホストからのトラフィックのロードシェアリングが可能です。下の図に、ロードシェアリングが行われる HSRP IPv4 構成の例を示します。

図 36: HSRP ロードシェアリング



HSRP ロードシェアリングの図には、2 台のルータ（A および B）と 2 つの HSRP グループが示されています。ルータ A はグループ A のアクティブルータですが、グループ B のスタンバイルータです。同様に、ルータ B はグループ B のアクティブルータであり、グループ A のスタンバイルータです。両方のルータがアクティブのままの場合、HSRP は両方のルータにまたがるホスト。どちらかのルータで障害が発生すると、残りのルータが引き続き、両方のホストのトラフィックを処理します。

オブジェクトトラッキングおよび HSRP

オブジェクトトラッキングを使用すると、別のインターフェースの動作状態に基づいて、HSRP インターフェースのプライオリティを変更できます。オブジェクトトラッキングによって、メインネットワークへのインターフェースで障害が発生した場合に、スタンバイルータにルーティングできます。

トラッキング可能なオブジェクトは、インターフェースのラインプロトコルステートまたは IP ルートの到達可能性の 2 種類です。指定したオブジェクトがダウンすると、設定された値だけ Cisco NX-OS が HSRP プライオリティを引き下げます。詳細については、「[HSRP オブジェクトトラッキングの設定](#)」の項を参照してください。

仮想化のサポート

HSRP は仮想ルーティングおよび転送（VRF）インスタンスをサポートします。デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS はユーザーをデフォルトの VRF に配置します。

インターフェイスの VRF メンバーシップを変更すると、Cisco NX-OS によって HSRP を含め、すべてのレイヤ 3 構成が削除されます。

詳細については、「[レイヤ 3 仮想化の設定](#)」を参照してください。

HSRP の前提条件

HSRP の前提条件は、次のとおりです。

- HSRP グループを設定してイネーブルにするには、その前に HSRP 機能をスイッチでイネーブルにする必要があります。

HSRP の注意事項と制約事項

HSRP 設定時の注意事項および制約事項は、次のとおりです。

- 最小 hello タイマー値は 250 ミリ秒です。
- 最小ホールド タイマー値は 750 ミリ秒です。
- HSRP を設定するインターフェイスに IP アドレスを設定し、そのインターフェイスをイネーブルにしてからでなければ、HSRP はアクティブになりません。
- IPv4 では、仮想 IP アドレスは、インターフェイス IP アドレスと同じサブネットになければなりません。
- 同一インターフェイス上では、複数のファーストホップ冗長プロトコルを設定しないことを推奨します。
- HSRP バージョン 2 は HSRP バージョン 1 と相互運用できません。どちらのバージョンも相互に排他的なので、インターフェイスはバージョン 1 およびバージョン 2 の両方を運用できません。しかし、同一ルータの異なる物理インターフェイス上であれば、異なるバージョンを実行できます。
- バージョン 1 で認められるグループ番号範囲（0 ～ 255）を超えるグループを設定している場合は、バージョン 2 からバージョン 1 への変更はできません。
- Cisco NX-OS では、VDC、インターフェイス VRF メンバーシップ、ポート チャネル メンバーシップを変更したり、ポート モードをレイヤ 2 に変更した場合は、インターフェイス上のすべてのレイヤ 3 設定が削除されます。
- Cisco NX-OS リリース 7.0(3)F3(3) で導入された HSRP サブネット VIP 機能には、次のガイドラインと制限事項があります。
 - この機能は、IPv4 アドレスおよび vPC トポロジでのみサポートされます。
 - プライマリまたはセカンダリ VIP をサブネット VIP にすることはできますが、サブネット VIP がインターフェイス サブネットと重複してはなりません。

- - 通常のホスト VIP は 0 または 32 のマスク長を使用します。サブネット VIP のマスク長を指定する場合は、0 より大きく、32 未満にする必要があります。
- - uRPF はこの機能ではサポートされていません。
- - VIP を使用した DHCP ソースもサポートされていません。
- - この機能では、DHCP リレー エージェントを使用して、VIP を送信元として DHCP パケットをリレーすることはできません。
- - VIP 直接ルートは、redistribute コマンドとルート マップを使用して、ルーティング プロトコルに明示的にアドバタイズする必要があります。
- - スーパーバイザが生成したトラフィック（ping、トレースルートなど）は、VIP サブネットではなく、SVI IP アドレスを使用して送信されます。
- - サブネットVIPの長さが /32で設定されている場合は、/32を指定して no コマンドを使用し、IPアドレスを削除する必要があります（例えば no ip ip-address/32）。

HSRP のデフォルト設定

次の表に、HSRP パラメータのデフォルト設定値を示します。

表 23: デフォルトの HSRP パラメータ

パラメータ	デフォルト
HSRP	ディセーブル
認証	バージョン1の場合はテキストとしてイネーブル、パスワードは cisco
HSRP バージョン	バージョン 1
プリエンプション	無効
プライオリティ	100
仮想 MAC アドレス	HSRP グループ番号から生成

『Configuring HSRP』

HSRP 機能のイネーブル化

HSRP グループを設定してイネーブルにするには、その前に HSRP 機能をグローバルでイネーブルにする必要があります。

手順の詳細

HSRP 機能をイネーブルにするには、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。

コマンド	目的
feature hsrp 例： switch(config)# feature hsrp	HSRP をイネーブルにします。

HSRP 機能をディセーブルにして、関連付けられている設定をすべて削除するには、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。

コマンド	目的
no feature hsrp 例： switch(config)# no feature hsrp	HSRP をディセーブルにします。

HSRP バージョン設定

HSRP のバージョンを設定できます。既存グループのバージョンを変更すると、仮想 MAC アドレスが変更されるので、Cisco NX-OS がそれらのグループの HSRP を再初期化します。HSRP のバージョンは、インターフェイス上のすべてのグループに適用されます。

HSRP のバージョンを設定するには、インターフェイスコンフィギュレーションモードで次のコマンドを使用します。

コマンド	目的
hsrp version { 1 2 } 例： switch(config-if)# hsrp version 2	HSRP バージョンを設定します。デフォルトはバージョン 1 です。

IPv4 の HSRP グループの設定

IPv4 インターフェイスに HSRP グループを設定し、その HSRP グループに仮想 IP アドレスと仮想 MAC アドレスを設定できます。

始める前に

HSRP 機能が有効になっていることを確認します ([HSRP 機能の有効化](#)のセクションを参照)。

グループのいずれかのメンバインターフェイス上で仮想IPアドレスを設定すると、Cisco NX-OS によって HSRP がイネーブルになります。HSRP グループをイネーブルにする前に、認証、タイマー、プライオリティなどの HSRP 属性を設定する必要があります。

手順の概要

1. **configure terminal**
2. **interface type number**
3. **no switchport**
4. **ip address ip-address/length**
5. **hsrp group-number [ipv4]**
6. **ip [ip-address [secondary]]**
7. **exit**
8. **no shutdown**
9. (任意) **show hsrp [group group-number] [ipv4]**
10. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	interface type number 例： switch(config)# interface ethernet 1/2 switch(config-if)#	インターフェイス設定モードを開始します。
ステップ 3	no switchport 例： switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	ip address ip-address/length 例： switch(config-if)# ip address 192.0.2.2/8	インターフェイスの IPv4 アドレスを設定します。
ステップ 5	hsrp group-number [ipv4] 例： switch(config-if)# hsrp 2 switch(config-if-hsrp)	HSRP グループを作成し、HSRP コンフィギュレーションモードを開始します。HSRP バージョン 1 で指定できる範囲は 0 ～ 255 です。HSRP バージョン 2 で指定できる範囲は 0 ～ 4095 です。デフォルト値は 0 です

	コマンドまたはアクション	目的
ステップ 6	ip [ip-address [secondary]] 例 : switch(config-if-hsrp)# ip 192.0.2.1	HSRP グループの仮想 IP アドレスを設定し、グループを有効にします。このアドレスは、インターフェイスの IPv4 アドレスと同じサブネットになければなりません。
ステップ 7	exit 例 : switch(config-if-hsrp)# exit	HSRP 設定モードを終了します。
ステップ 8	no shutdown 例 : switch(config-if)# no shutdown	インターフェイスを有効にします。
ステップ 9	(任意) show hsrp [group group-number] [ipv4] 例 : switch(config-if)# show hsrp group 2	HSRP 情報を表示します。
ステップ 10	(任意) copy running-config startup-config 例 : switch(config-if)# copy running-config startup-config	この設定変更を保存します。

例



(注) 設定完了後にインターフェイスを有効にするには、**no shutdown** コマンドを使用する必要があります。

次に Ethernet 1/2 上で HSRP グループを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip 192.0.2.2/8
switch(config-if)# hsrp 2
switch(config-if-hsrp)# ip 192.0.2.1
switch(config-if-hsrp)# exit
switch(config-if)# no shutdown
switch(config-if)# copy running-config startup-config
```

HSRP 仮想 MAC アドレスの設定

設定されているグループ番号から HSRP が導き出したデフォルトの仮想 MAC アドレスを変更できます。

HSRP グループの仮想 MAC アドレスを手動で設定するには、HSRP 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
mac-address string 例： <pre>switch(config-if-hsrp)# mac-address 5000.1000.1060</pre>	HSRP グループの仮想 MAC アドレスを設定します。ストリングには標準の MAC アドレス フォーマット (xxxx.xxxx.xxxx) を使用します。

仮想 MAC アドレスに BIA (バーンドイン MAC アドレス) を使用するように HSRP を設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
hsrp use-bia [scope interface] 例： <pre>switch(config-if)# hsrp use-bia</pre>	HSRP 仮想 MAC アドレスにインターフェイスの BIA を使用するように、HSRP を設定します。 scope interface キーワードを使用すると、このインターフェイス上のすべてのグループに焼き込み MAC アドレスを使用するように HSRP を設定できます。

HSRP の認証

クリアテキストまたは MD5 ダイジェスト認証を使用してプロトコルを認証するように、HSRP を設定できます。MD5 認証ではキー チェーンが使用されます。

始める前に

HSRP 機能が有効になっていることを確認します ([HSRP 機能の有効化](#)のセクションを参照)。

HSRP グループのすべてのメンバに同じ認証およびキーを設定する必要があります。

MD5 認証を使用する場合は、キーチェーンが作成してあることを確認します。

手順の概要

1. **configure terminal**
2. **interface interface type slot/port**
3. **no switchport**
4. **hsrp group-number [ipv4]**
- 5.
6. (任意) **show hsrp [group group-number]**
7. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション		目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>		コンフィギュレーション モードに入ります。
ステップ 2	interface interface type slot/port 例 : <pre>switch(config)# interface ethernet 1/2 switch(config-if)#</pre>		インターフェイス構成モードを開始します。
ステップ 3	no switchport 例 : <pre>switch(config-if)# no switchport</pre>		そのインターフェイスを、レイヤ 3 ルーテッドインターフェイスとして設定します。
ステップ 4	hsrp group-number [ipv4] 例 : <pre>switch(config-if)# hsrp 2 switch(config-if-hsrp)</pre>		HSRP グループを作成し、HSRP 設定モードを開始します。
ステップ 5	オプション	説明	
	コマンド	目的	
	authentication text string 例 : <pre>switch(config-if-hsrp)# authentication text mypassword</pre>	このインターフェイス上で、HSRP のクリアテキスト認証を設定します。	
	authentication md5 { key-chain key-chain key-string { 0 7 } text [timeout seconds] } 例 : <pre>switch(config-if-hsrp)# authentication md5 key-chain hsrp-keys</pre>	このインターフェイス上で、HSRP の MD5 認証を設定します。キーチェーンまたはキー スtring を使用できます。キー スtring を使用する場合は、HSRP が新しいキーだけを受け付けるように、任意でタイムアウトを設定できます。指定できる範囲は 0 ～ 32767 秒です。	

	コマンドまたはアクション	目的
ステップ 6	(任意) show hsrp [group group-number] 例 : <pre>switch(config-if-hsrp)# show hsrp group 2</pre>	HSRP 情報を表示します。
ステップ 7	(任意) copy running-config startup-config 例 : <pre>switch(config-if-hsrp)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、キーチェーン作成後に HSRP の MD5 認証を Ethernet 1/2 上で設定する例を示します。

```
switch# configure terminal
switch(config)# key chain hsrp-keys
switch(config-keychain)# key 0
switch(config-keychain-key)# key-string 7 zqdest
switch(config-keychain-key) accept-lifetime 00:00:00 Jun 01 2008 23:59:59 Sep 12 2008
switch(config-keychain-key) send-lifetime 00:00:00 Jun 01 2008 23:59:59 Aug 12 2008
switch(config-keychain-key) key 1
switch(config-keychain-key) key-string 7 uaeqdyito
switch(config-keychain-key) accept-lifetime 00:00:00 Aug 12 2008 23:59:59 Dec 12 2008
switch(config-keychain-key) send-lifetime 00:00:00 Sep 12 2008 23:59:59 Nov 12 2008
switch(config-keychain-key)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# hsrp 2
switch(config-if-hsrp)# authenticate md5 key-chain hsrp-keys
switch(config-if-hsrp)# copy running-config startup-config
```

HSRP オブジェクト トラッキングの設定

他のインターフェイスまたはルータの可用性に基づいて、プライオリティが調整されるように HSRP グループを設定できます。スイッチがオブジェクトトラッキング対応として設定されていて、なおかつトラッキング対象のオブジェクトがダウンした場合、スイッチのプライオリティはダイナミックに変更されます。トラッキングプロセスはトラッキング対象オブジェクトに定期的にポーリングを実行し、値の変化をすべて記録します。値が変化すると、HSRP がプライオリティを再計算します。HSRP インターフェイスにプリエンブションを設定している場合は、プライオリティの高い HSRP インターフェイスがアクティブ ルータになります。

HSRP では、トラッキング対象のオブジェクトおよびトラック リストをサポートします。トラック リストの詳細については、[オブジェクト トラッキングの設定](#)を参照してください。

始める前に

HSRP 機能が有効になっていることを確認します ([HSRP 機能の有効化](#)のセクションを参照)。

手順の概要

1. **configure terminal**
- 2.
3. **interface** *interface-type slot/port*
4. **no switchport**
5. **hsrp group-number** [**ipv4**]
6. **priority** [*value*]
7. **track object-number** [**decrement value**]
8. **preempt** [**delay** [*minimum seconds*] [**reload seconds**] [**sync seconds**]]
9. (任意) **show hsrp interface** *interface-type number*
10. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション		目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>		コンフィギュレーション モードに入ります。
ステップ 2	オプション	説明	
	コマンド	目的	
	track object-id interface <i>interface-type number</i> { ip routing line-protocol } 例 : <pre>switch(config)# track 1 interface ethernet 2/2 line-protocol switch(config-track#</pre>	この HSRP インターフェイスが追跡するインターフェイスを設定します。インターフェイスのステート変化は次のように、この HSRP のプライオリティを左右します。 • HSRP コンフィギュレーション モードで、track コマンドで使用するインターフェイスおよび対応するオブジェクト番号を設定します。 • line-protocol キーワードを指定すると、インターフェイスがアップ状態かどうかを追跡さ	

	コマンドまたはアクション		目的
	オプション	説明	
		れます。 ip キーワードを指定すると、インターフェイス上で IP ルーティングがイネーブルであり、IP アドレスが設定されているかどうかもチェックされます。	
	track object-id ip route ip-prefix/length reachability 例： switch(config)# track 2 ip route 192.0.2.0/8 reachability switch(config-track)#	ルートのトラッキング対象オブジェクトを作成し、トラッキング コンフィギュレーション モードを開始します。 object-id の範囲は 1 ～ 500 です。	
ステップ 3	interface interface-type slot/port 例： switch(config)# interface ethernet 1/2 switch(config-if)#		インターフェイス設定モードを開始します。
ステップ 4	no switchport 例： switch(config-if)# no switchport		そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 5	hsrp group-number [ipv4] 例： switch(config-if)# hsrp 2 switch(config-if-hsrp)#		HSRP グループを作成し、HSRP 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	priority [value] 例： switch(config-if-hsrp)# priority 254		HSRP グループでのアクティブ ルータ選択に使用するプライオリティ レベルを設定します。有効な範囲は 0 ～ 255 です。デフォルトは 100 です。
ステップ 7	track object-number [decrement value] 例： switch(config-if-hsrp)# track 1 decrement 20		HSRP インターフェイスの重み付けを左右する、トラッキング対象のオブジェクトを指定します。 value 引数には、トラッキング対象のオブジェクトで障害が発生した場合に、HSRP インターフェイスのプライオリティから差し引く値を指定します。範囲は 1 ～ 255 です。デフォルトは 10 です。

	コマンドまたはアクション	目的
ステップ 8	preempt [delay [minimum seconds] [reload seconds] [sync seconds]] 例 : <pre>switch(config-if-hsrp)# preempt delay minimum 60</pre>	現在のアクティブ ルータよりプライオリティが高い場合に、HSRP グループのアクティブ ルータとして引き継ぐようにルータを設定します。このコマンドは、デフォルトでディセーブルになっています。指定できる範囲は 0 ～ 3600 秒です。
ステップ 9	(任意) show hsrp interface interface-type number 例 : <pre>switch(config-if-hsrp)# show hsrp interface ethernet 1/2</pre>	インターフェイスの HSRP 情報を表示します。
ステップ 10	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、Ethernet 1/2 上で HSRP オブジェクト トラッキングを設定する例を示します。

```
switch# configure terminal
switch(config)# track 1 interface ethernet 2/2 line-protocol
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# hsrp 2
switch(config-if-hsrp)# track 1 decrement 20
switch(config-if-hsrp)# copy running-config startup-config
```

HSRP プライオリティの設定

インターフェイス上で HSRP プライオリティを設定できます。HSRP では、プライオリティを使用して、アクティブ ルータとして動作する HSRP グループ メンバを決定します。

HSRP プライオリティを設定するには、インターフェイス コンフィギュレーションモードで次のコマンドを使用します。

コマンド	目的
priority level [forwarding-threshold lower lower-value upper upper-value] 例 : <pre>switch(config-if-hsrp)# priority 60 forwarding-threshold lower 40 upper 50</pre>	HSRP グループでのアクティブ ルータ選択に使用するプライオリティ レベルを設定します。 <i>level</i> の範囲は 0 ～ 255 です。デフォルトは 100 です。

HSRP のカスタマイズ

必要に応じて、HSRPの動作をカスタマイズできます。仮想IPアドレスを設定することによって、HSRP グループをイネーブルにすると、そのグループがただちに動作可能になることに注意してください。HSRP をカスタマイズする前に HSRP グループをイネーブルにした場合、機能のカスタマイズが完了しないうちに、ルータがグループの制御を引き継いでアクティブルータになる可能性があります。HSRP のカスタマイズを予定している場合は、HSRP グループをイネーブルにする前に行ってください。

HSRP をカスタマイズするには、HSRP 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
name string 例 : <pre>switch(config-if-hsrp)# name HSRP-1</pre>	HSRP グループの IP 冗長名を指定します。 <i>string</i> は 1 ～ 255 文字です。デフォルト スtring のフォーマットは hsrp-interface-short-name-group-id です。 たとえば、 hsrp-Eth2/1-1
preempt [delay [minimum seconds] [reload seconds] [sync seconds]] のようになります。 例 : <pre>switch(config-if-hsrp)# preempt delay minimum 60</pre>	現在のアクティブルータよりもプライオリティが高い場合に、HSRP グループのアクティブルータとして引き継ぐようにルータを設定します。このコマンドは、デフォルトでディセーブルになっています。指定できる範囲は 0 ～ 3600 秒です。
timers [msec] hellotime [msec] holdtime 例 : <pre>switch(config-if-hsrp)# timers 5 18</pre>	次のように、この HSRP メンバーの hello タイムおよびホールドタイムを設定します。 オプションの <i>msec</i> キーワードは、引数がデフォルトの秒単位ではなく、ミリ秒単位で表されることを指定します。タイマーの範囲（ミリ秒）は次のとおりです。 • <i>hellotime</i> : hello パケットを送信してから、次の hello パケットを送信するまでのインターバル。指定できる範囲は 255 ～ 999 ミリ秒です。 • <i>holdtime</i> : hello パケットの情報が無効と見なされるまでのインターバル。指定できる範囲は 750 ～ 3000 ミリ秒です。

HSRP をカスタマイズするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
hsrp delay minimum seconds 例 : <pre>switch(config-if)# hsrp delay minimum 30</pre>	グループがイネーブルになってから、グループに参加するまでに HSRP が待機する最小時間を指定します。指定できる範囲は 0 ～ 10000 秒です。デフォルトは 0 です。
hsrp delay reload seconds 例 : <pre>switch(config-if)# hsrp delay reload 30</pre>	リロード後、グループに参加するまでに HSRP が待機する最小時間を指定します。指定できる範囲は 0 ～ 10000 秒です。デフォルトは 0 です。

HSRP 設定の確認

HSRP の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show hsrp [group group-number]	すべてのグループまたは特定のグループの HSRP ステータスを表示します。
show hsrp delay [interface interface-type slot/port]	すべてのインターフェイスまたは特定のインターフェイスの HSRP 遅延値を表示します。
show hsrp [interface interface-type slot/port]	インターフェイスの HSRP ステータスを表示します。
show hsrp [group group-number] [interface interface-type slot/port] [active] [all] [init] [learn] [listen] [speak] [standby]	ステータスが active、init、listen、または standby の仮想フォワーダについて、グループまたはインターフェイスの HSRP ステータスを表示します。disabledを含めてすべてのステータスを表示する場合は、 all キーワードを使用します。
show hsrp [group group-number] [interface interface-type slot/port] active [all] [init] [learn] [listen] [speak] [standby] brief	ステータスが active、init、listen、または standby の仮想フォワーダについて、グループまたはインターフェイスの HSRP ステータスの要約を表示します。disabledを含めてすべてのステータスを表示する場合は、 all キーワードを使用します。

HSRP の設定例

次に、MD5 認証およびインターフェイストラッキングを指定して、インターフェイス上で HSRP をイネーブルにする例を示します。

```

key chain hsrp-keys
key 0
key-string 7 zqdest
accept-lifetime 00:00:00 Jun 01 2008 23:59:59 Sep 12 2008
send-lifetime 00:00:00 Jun 01 2008 23:59:59 Aug 12 2008
key 1
key-string 7 uaeqdyito
accept-lifetime 00:00:00 Aug 12 2008 23:59:59 Dec 12 2008
send-lifetime 00:00:00 Sep 12 2008 23:59:59 Nov 12 2008
feature hsrp
track 2 interface ethernet 2/2 ip
interface ethernet 1/2
no switchport
ip address 192.0.2.2/8
hsrp 1
authenticate md5 key-chain hsrp-keys
priority 90
track 2 decrement 20
ip-address 192.0.2.10
no shutdown

```

次に、インターフェイス IP アドレスのサブネットとは異なるサブネットに設定された HSRP サブネット VIP アドレスを設定する例を示します。

```

switch# configure terminal
switch(config)# feature hsrp
switch(config)# feature interface-vlan
switch(config)# interface vlan 2
switch(config-if)# ip address 192.0.2.1/24
switch(config-if)# hsrp 2
switch(config-if-hsrp)# ip 209.165.201.1/24

```

この例は、HSRP サブネットなし VIP アドレスがインターフェイス IP アドレスと異なるサブネットに設定されている場合の VIP の不一致エラーを示しています。

```

switch# configure terminal
switch(config)# feature hsrp
switch(config)# feature interface-vlan
switch(config)# interface vlan 2
switch(config-if)# ip address 192.0.2.1/24
switch(config-if)# hsrp 2
switch(config-if-hsrp)# ip 209.165.201.1
!ERROR: VIP subnet mismatch with interface IP!

```

次の例は、HSRP サブネットの VIP アドレスがインターフェイス IP アドレスと同じサブネットに設定されている場合の VIP の不一致エラーを示しています。

```

switch# configure terminal
switch(config)# feature hsrp
switch(config)# feature interface-vlan
switch(config)# interface vlan 2
switch(config-if)# ip address 192.0.2.1/24
switch(config-if)# hsrp 2
switch(config-if-hsrp)# ip 192.0.2.10/24
!ERROR: Subnet VIP cannot be in same subnet as interface IP!

```

その他の参考資料

HSRP の実装に関する詳細は、次の各項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
VRRP の設定	『Configuring VRRP』

MIB

MIB	MIB のリンク
CISCO-HSRP-MIB	MIB を検索してダウンロードするには、次の MIB ロケータ に移動します。



第 19 章

VRRP の設定

この章では、Cisco NX-OS スイッチ上で仮想ルータ冗長プロトコル（VRRP）を設定する方法について説明します。

この章は、次の項で構成されています。

- [VRRP の概要（533 ページ）](#)
- [VRRP の注意事項と制約事項（538 ページ）](#)
- [VRRP のデフォルト設定（539 ページ）](#)
- [VRRP の設定（540 ページ）](#)
- [VRRPv3 の設定（551 ページ）](#)
- [VRRPv2 設定の確認（556 ページ）](#)
- [VRRPv3 設定の確認（556 ページ）](#)
- [VRRP 統計情報の表示（557 ページ）](#)
- [VRRPv2 の設定例（557 ページ）](#)
- [VRRPv3 の構成例（559 ページ）](#)
- [その他の参考資料（559 ページ）](#)

VRRP の概要

VRRP を使用すると、仮想 IP アドレスを共有するルータ グループを設定することによって、ファーストホップ IP ルータで透過的フェールオーバーが可能になります。VRRP はそのグループのプライマリ ルータを選択して、仮想 IP アドレスへのすべてのパケットが処理できるようにします。残りのルータはスタンバイになり、プライマリ ルータで障害が発生した場合に処理を引き継ぎます。

VRRP の動作

LAN クライアントは、ダイナミック プロセスまたはスタティック設定を使用することによって、特定のリモート宛先へのファーストホップにするルータを決定できます。ダイナミック ルータ ディスカバリの例を示します。

- プロキシ ARP：クライアントはアドレス解決プロトコル（ARP）を使用して到達すべき宛先を取得します。ルータは独自の MAC アドレスで ARP 要求に応答します。
- ルーティング プロトコル：クライアントはダイナミック ルーティング プロトコルのアップデートを（ルーティング情報プロトコル（RIP）などから）受信し、独自のルーティング テーブルを形成します。
- ICMP Router Discovery Protocol（IRDP）クライアント：クライアントはインターネット制御メッセージプロトコル（ICMP）ルータ ディスカバリ クライアントを実行します。

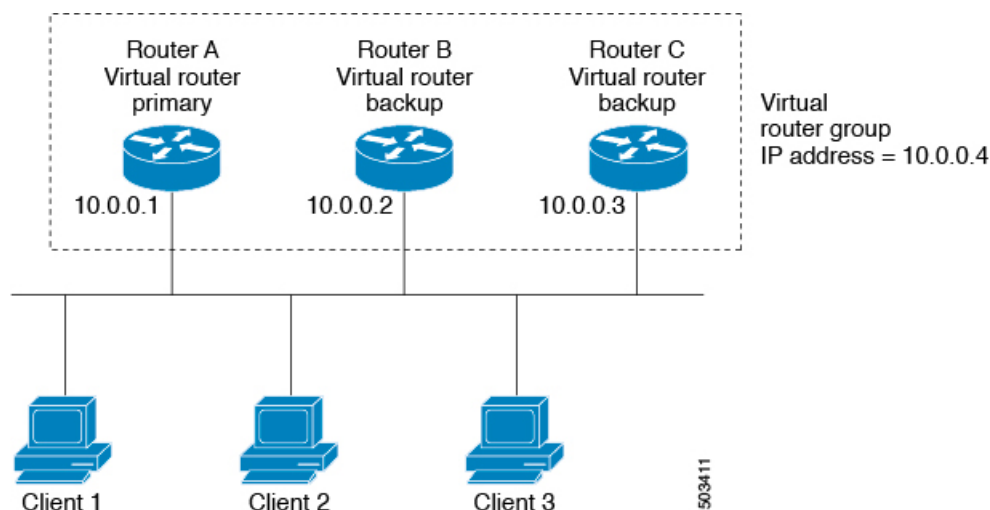
ダイナミック ディスカバリ プロトコルのデメリットは、LAN クライアントにある程度、設定および処理のオーバーヘッドが発生することです。また、ルータが故障した場合、他のルータに切り替えるプロセスも遅くなる場合があります。

ダイナミック ディスカバリ プロトコルの代わりに、クライアント上でデフォルト ルータをスタティックに設定することもできます。このアプローチでは、クライアントの設定および処理が簡素化されますが、シングルポイント障害が生じます。デフォルトゲートウェイで障害が発生した場合、LAN クライアントの通信はローカル IP ネットワーク セグメントに限定され、ネットワークの他の部分から切り離されます。

VRRP では、ルータ グループ（VRRP グループ）が単一の仮想 IP アドレスを共有できるようにすることによって、スタティック設定に伴う問題を解決できます。さらに、デフォルトゲートウェイとして仮想 IP アドレスを指定して、LAN クライアントを設定できます。

次の図は、基本的な VLAN トポロジです。この例では、ルータ A、B、および C が VRRP グループを形成します。グループの IP アドレスは、ルータ A のインターフェイス インターフェイスに設定されているアドレス（10.0.0.1）と同じです。

図 37: 基本的な VRRP トポロジ



仮想 IP アドレスにルータ A の物理イーサネット インターフェイスの IP アドレスが使用されるので、ルータ A がプライマリ（「IP アドレス オーナー」）になります。ルータ A はプライマリとして、VRRP グループ ルータの仮想 IP アドレスを所有し、送信されたパケットをこの IP

アドレスに転送します。クライアント 1～3 には、デフォルト ゲートウェイの IP アドレス 10.0.0.1 が設定されています。

ルータ B および C の役割はバックアップです。プライマリで障害が発生すると、プライオリティが最も高いバックアップルータがプライマリになり、仮想 IP アドレスを引き継いで、LAN ホストへのサービスが途切れないようにします。ルータ A が回復すると、これが再びプライマリ ルータになります。詳細については、「VRRP ルータのプライオリティおよびプリエンブション」のセクションを参照してください。



- (注) ルーテッドポートで受信した VRRP 仮想 IP アドレス宛のパケットは、ローカルルータ上で終了します。そのルータがプライマリ VRRP ルータであるのかバックアップ VRRP ルータであるのかは関係ありません。これには ping トラフィックと Telnet トラフィックが含まれます。レイヤ 2 (VLAN) インターフェイスで受信した、VRRP 仮想 IP アドレス宛のパケットは、プライマリ ルータに届きます。

VRRP の利点

VRRP の利点は、次のとおりです。

- 冗長性：複数のルータをデフォルト ゲートウェイ ルータとして設定できるので、ネットワークにシングル ポイント障害が発生する確率が下がります。
- ロード シェアリング：複数のルータで LAN クライアントとの間のトラフィックを分担できます。トラフィックの負荷が使用可能なルータ間でより公平に分担されます。
- マルチ VRRP グループ：プラットフォームがマルチ MAC アドレスをサポートする場合、ルータの物理インターフェイス上で、最大 255 の VRRP グループをサポートします。マルチ VRRP グループによって、LAN トポロジで冗長性およびロード シェアリングを実現できます。
- マルチ IP アドレス：セカンダリ IP アドレスを含めて、複数の IP アドレスを管理できます。イーサネットインターフェイス上で複数のサブネットを設定している場合は、各サブネットに VRRP を設定できます。
- プリエンブト：障害プライマリを引き継いでいたバックアップルータより、さらにプライオリティが高いバックアップルータが使用可能になったときに、プライオリティが高い方を優先させることができます。
- アドバタイズメント プロトコル：VRRP アドバタイズメントに、専用の Internet Assigned Numbers Authority (IANA) 規格マルチキャスト アドレス (224.0.0.18) を使用します。このアドレッシング方式によって、マルチキャストを提供するルータ数が最小限になり、テスト機器でセグメント上の VRRP パケットを正確に識別できるようになります。IANA は VRRP に IP プロトコル番号 112 を割り当てています。
- VRRPv3 の利点は次のとおりです。
 - マルチベンダー環境での相互運用性

- IPv4 および IPv6 アドレス ファミリをサポートします。

複数の VRRP グループ

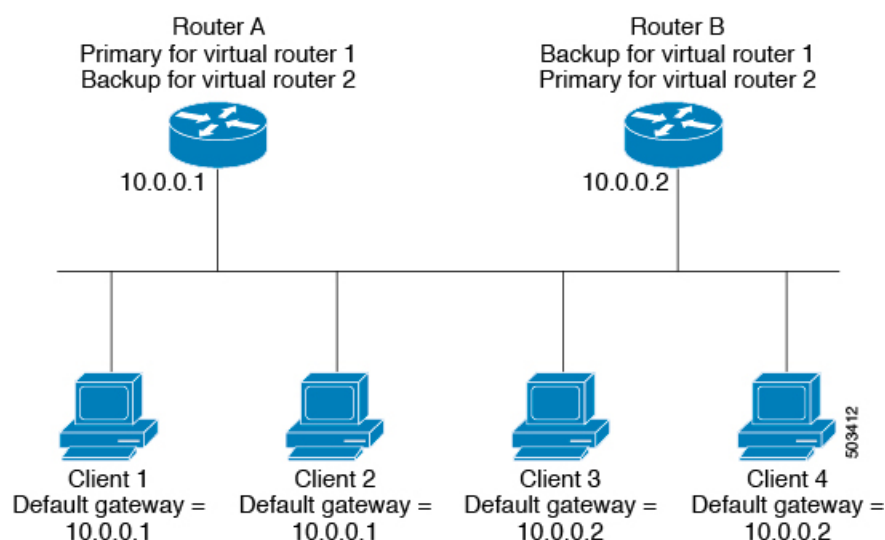
物理インターフェイス上で、最大255のVRRPグループを設定できます。ルータインターフェイスがサポートできるVRRPグループの実際数は、次の要因によって決まります。

- ルータの処理能力
- ルータのメモリの能力

ルータインターフェイス上で複数のVRRPグループが設定されたトポロジでは、インターフェイスはあるVRRPグループのプライマリ、および他の1つまたは複数のVRRPグループのバックアップとして動作可能です。

次の図のLAN トポロジでは、ルータ A と B がクライアント 1～4 のトラフィックを共有するように、VRRP が構成されています。ルータ A と B の一方で障害が発生した場合、もう一方がバックアップとして機能します。

図 38: ロードシェアリングおよび冗長構成の VRRP トポロジ



このトポロジには、オーバーラップする2つのVRRPグループに対応する2つの仮想IPアドレスが含まれています。VRRPグループ1では、ルータAがIPアドレス10.0.0.1のオーナーであり、プライマリです。ルータBはルータAのバックアップです。クライアント1と2には、デフォルトゲートウェイのIPアドレス10.0.0.1が設定されています。

VRRPグループ2では、ルータBがIPアドレス10.0.0.2のオーナーであり、プライマリです。ルータAはルータBをバックアップします。クライアント3と4には、デフォルトゲートウェイのIPアドレス10.0.0.2が設定されています。

VRRP ルータのプライオリティおよびプリエンブション

VRRP 冗長構成の重要な側面は、VRRP ルータのプライオリティです。各 VRRP ルータが果たす役割やプライマリルータで障害が発生した場合のアクションは、プライオリティによって決まるからです。

VRRP ルータが仮想 IP アドレスおよび物理インターフェイスの IP アドレスを所有する場合、そのルータはプライマリとして機能します。プライマリのプライオリティは 255 です。

プライオリティによって、VRRP ルータがバックアップルータとして動作するかどうかが決まり、さらに、プライマリで障害が発生した場合にプライマリになる順序も決まります。

たとえば、ルータ A が LAN トポロジにおけるプライマリであり、そのルータ A で障害が発生した場合、VRRP はバックアップ B が引き継ぐのか、バックアップ C が引き継ぐのかを判断する必要があります。ルータ B にプライオリティ 101 が設定されていて、ルータ C がデフォルトのプライオリティ 100 の場合、VRRP はルータ B をプライマリになるべきルータとして選択します。ルータ B の方がプライオリティが高いからです。ルータ B および C にデフォルトのプライオリティ 100 が設定されている場合は、VRRP は IP アドレスが大きい方のバックアップをプライマリになるべきルータとして選択します。

VRRP ではプリエンブションを使用して、VRRP バックアップルータがプライマリになってからのアクションを決定します。プリエンブションはデフォルトでイネーブルなので、VRRP は新しいプライマリよりプライオリティの高いバックアップがオンラインになると、バックアップに切り替えます。たとえば、ルータ A がプライマリであり、そのルータ A で障害が発生した場合、VRRP は（プライオリティの順位が次である）ルータ B を選択します。ルータ C がルータ B より高いプライオリティでオンラインになると、ルータ B で障害が発生していなくても、VRRP はルータ C を新しいプライマリとして選択します。

プリエンブションを無効にした場合、VRRP が切り替わるのは、元のプライマリが回復した場合、または新しいプライマリで障害が発生した場合に限られます。

VRRP のアドバタイズメント

VRRP プライマリは、同じグループ内の他の VRRP ルータに VRRP アドバタイズメントを送信します。アドバタイズメントでは、プライマリの優先順位と状態が伝達されます。Cisco NX-OS は VRRP アドバタイズメントを IP パケットにカプセル化して、VRRP グループに割り当てられた IP マルチキャスト アドレスに送信します。Cisco NX-OS がアドバタイズメントを送信する間隔はデフォルトでは 1 秒ですが、ユーザ側で別のアドバタイズインターバルを設定できます。

VRRP 認証

VRRP は、次の認証方式をサポートします。

- 認証なし
- プレーン テキスト認証

VRRP は次の場合に、パケットを拒否します。

- 認証方式がルータと着信パケットで異なる。
- テキスト認証文字列がルータと着信パケットで異なる。

VRRPv3

VRRP のバージョン 3 (VRRPv3) では、スイッチのグループで単一の仮想スイッチを形成して、冗長性を実現し、ネットワーク内のシングルポイント障害が生じる可能性を減らすことができます。これにより、仮想スイッチをデフォルトゲートウェイとして使用するよう、LAN クライアントを設定できます。スイッチのグループを表す仮想スイッチは、VRRPv3 グループとも呼ばれます。

仮想化のサポート

VRRP は仮想ルーティングおよび転送 (VRF) インスタンスをサポートします。デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS はユーザーをデフォルトの VRF に配置します。

インターフェイスの VRF メンバーシップを変更すると、Cisco NX-OS によって VRRP を含め、すべてのレイヤ 3 設定が削除されます。

詳細については、「[レイヤ 3 仮想化の設定](#)」を参照してください。

VRRP の注意事項と制約事項

VRRP には、次の注意事項および制限事項があります。

- 管理インターフェイス上で VRRP を設定できません。
- VRRP がイネーブルの場合は、ネットワーク上のスイッチ全体で VRRP 設定を複製する必要があります。
- VRRPv3 ピアのグレースフルフェールオーバーを実行する場合は、まずプロトコルをシャットダウンしてからインターフェイスをシャットダウンします。インターフェイスをシャットダウンしても、インターフェイスがシャットダウンする前にピア間の迅速な移行が保証されるわけではありません。したがって、ホールド時間の期限切れに基づいて VRRPv3 フェールオーバーが発生する可能性があります。
- 同一インターフェイス上では、複数のファーストホップ冗長プロトコルを設定しないことを推奨します。
- VRRP を設定するインターフェイスに IP アドレスを設定し、そのインターフェイスをイネーブルにしてからでなければ、VRRP はアクティブになりません。

- Cisco NX-OS では、VDC、インターフェイス VRF メンバーシップ、ポートチャネル メンバーシップを変更したり、ポートモードをレイヤ2に変更した場合は、インターフェイス上のすべてのレイヤ3 設定が削除されます。
- VRRP でレイヤ2 インターフェイスを追跡するよう設定した場合、レイヤ2 をシャットダウンしてからインターフェイスを再度イネーブル化することにより、VRRP プライオリティを更新してレイヤ2 インターフェイスのステートを反映させる必要があります。
- VRRPv3 設定時の注意事項および制約事項は、次のとおりです。
 - VRRPv3 は既存のダイナミック プロトコルの代替にはなりません。VRRPv3 は、マルチアクセス、マルチキャスト、またはブロードキャスト対応イーサネット LAN で使用するために設計されています。
 - VRRPv3 は、イーサネットおよびファストイーサネットインターフェイス、ブリッジグループ仮想インターフェイス (BVI)、ギガビットイーサネットインターフェイス、マルチプロトコルラベルスイッチング (MPLS) 仮想プライベートネットワーク (VPN)、VRF 認識 MPLS、VLAN のみでサポートされます。
 - VRRPv3 が使用中の場合、VRRPv2 は使用できません。VRRPv3 を設定するには、VRRPv2 設定を無効にする必要があります。
 - VRRPv3 ミリ秒タイマーは、絶対に必要な場合以外は使用しないようにし、使用する場合は慎重な検討とテストが必要です。ミリ秒の値は望ましい状況でのみ動作します。ミリ秒のタイマー値は、VRRPv3 も含めてサポートしている限り、サードパーティベンダーと互換性があります。

VRRP のデフォルト設定

次の表に、VRRP パラメータのデフォルト設定値を示します。

表 24: デフォルトの VRRP パラメータ

パラメータ	デフォルト
advertisement interval	1 秒
認証	認証なし
プリエンプション	有効
プライオリティ	100
VRRP 機能	無効
VRRPv3	無効

パラメータ	デフォルト
VRRPv3 セカンダリ アドレスの一致	有効 (Enabled)
VRRPv3 アドバタイズメントタイマー	1000 ミリ秒

VRRP の設定

VRRP 機能のイネーブル化

VRRP グループを設定してイネーブルにするには、その前に VRRP 機能をグローバルでイネーブルにする必要があります。

VRRP 機能をイネーブルにするには、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。

コマンド	目的
feature vrrp 例 : switch(config)# feature vrrp	VRRP をイネーブルにします。

VRRP 機能をディセーブルにして、関連付けられている設定をすべて削除するには、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。

コマンド	目的
no feature vrrp 例 : switch(config)# no feature vrrp	VRRP 機能をディセーブルにします。

VRRP グループの設定

VRRP グループを作成し、仮想 IP アドレスを割り当て、グループを有効にすることができます。

VRRP グループに設定できる仮想 IPv4 アドレスは 1 つです。プライマリ VRRP ルータはデフォルトで、仮想 IP アドレスを直接宛先とするパケットをドロップします。これは、VRRP プライマリがパケットを転送するネクストホップルータとしてのみ想定されているからです。アプリケーションによっては、Cisco NX-OS が仮想ルータ IP 宛のパケットを受け付けるようにする必要があります。仮想 IP アドレスに **secondary** オプションを使用すると、ローカル ルータが VRRP マスターの場合、これらのパケットを受け付けるようになります。

VRRP グループを設定した場合は、そのグループをアクティブにするために、グループを明示的に有効にする必要があります。

始める前に

インターフェイスに IP アドレスを設定していることを確認します（[IPv4 アドレッシングの設定](#)のセクションを参照）。

手順の概要

1. **configure terminal**
2. **interface interface -type slot/port**
3. **no switchport**
4. **vrrp number**
5. **address ip-address [secondary]**
6. **no shutdown**
7. （任意） **show vrrp**
8. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	interface interface -type slot/port 例 : <pre>switch(config)# switch(config-if)# interface ethernet 2/1</pre>	インターフェイス設定モードを開始します。
ステップ 3	no switchport 例 : <pre>switch(config-if)# no switchport</pre>	そのインターフェイスを、レイヤ 3 ルーテッドインターフェイスとして設定します。
ステップ 4	vrrp number 例 : <pre>switch(config-if)# vrrp 250 switch(config-if-vrrp)#</pre>	仮想ルータ グループを作成します。範囲は 1 ～ 255 です。
ステップ 5	address ip-address [secondary] 例 : <pre>switch(config-if-vrrp)# address 192.0.2.8</pre>	指定の VRRP グループに仮想 IPv4 アドレスを設定します。このアドレスは、インターフェイスの IPv4 アドレスと同じサブネットになければなりません。

	コマンドまたはアクション	目的
		secondary オプションは、VRRP ルータが仮想ルータの IP アドレスに送信されたパケットを受け付けて、アプリケーションに配信することをアプリケーションが要求する場合に限られます。
ステップ 6	no shutdown 例： switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#	VRRP グループを有効にします。デフォルトでは、ディセーブルです。
ステップ 7	(任意) show vrrp 例： switch(config-if-vrrp)# show vrrp	VRRP 情報を表示します。
ステップ 8	(任意) copy running-config startup-config 例： switch(config-if-vrrp)# copy running-config startup-config	この設定変更を保存します。

VRRP プライオリティの設定

仮想ルータの有効なプライオリティ範囲は 1 ～ 254 です（1 が最下位、254 が最上位のプライオリティ）。バックアップのデフォルトのプライオリティ値は 100 です。インターフェイスアドレスがプライマリ仮想 IP アドレスと同じスイッチ（プライマリ）の場合、デフォルト値は 255 です。

始める前に

VRRP 機能が有効になっていることを確認します（[VRRP の設定](#)のセクションを参照）。

インターフェイス上で IP アドレスを設定していることを確認します（[IPv4 アドレスの設定](#)のセクションを参照）。

手順の概要

1. **configure terminal**
2. **interface interface -type slot/port**
3. **no switchport**
4. **vrrp number**
5. **shutdown**
6. **priority level [forwarding-threshold lower lower-value upper upper-value]**
7. **no shutdown**
8. (任意) **show vrrp**
9. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	interface interface -type slot/port 例 : <pre>switch(config)# switch(config-if)# interface ethernet 2/1</pre>	インターフェイス設定モードを開始します。
ステップ 3	no switchport 例 : <pre>switch(config-if)# no switchport</pre>	そのインターフェイスを、レイヤ 3 ルーテッドインターフェイスとして設定します。
ステップ 4	vrrp number 例 : <pre>switch(config-if)# vrrp 250 switch(config-if-vrrp)#</pre>	仮想ルータ グループを作成します。範囲は 1 ～ 255 です。
ステップ 5	shutdown 例 : <pre>switch(config-if-vrrp)# shutdown switch(config-if-vrrp)#</pre>	VRRP グループを無効にします。デフォルトでは、ディセーブルです。
ステップ 6	priority level [forwarding-threshold lower lower-value upper upper-value] 例 : <pre>switch(config-if-vrrp)# priority 60 forwarding-threshold lower 40 upper 50</pre>	VRRP グループでのアクティブルータ選択に使用するプライオリティ レベルを設定します。レベルの範囲は 1 ～ 254 です。バックアップの場合、デフォルトは 100 です。インターフェイス IP アドレスが仮想 IP アドレスと等しいプライマリの場合は 255 です。
ステップ 7	no shutdown 例 : <pre>switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#</pre>	VRRP グループを有効にします。デフォルトでは、ディセーブルです。
ステップ 8	(任意) show vrrp 例 : <pre>switch(config-if-vrrp)# show vrrp</pre>	VRRP 情報を表示します。
ステップ 9	(任意) copy running-config startup-config 例 :	この設定変更を保存します。

	コマンドまたはアクション	目的
	<code>switch(config-if-vrrp)# copy running-config startup-config</code>	

VRRP 認証の設定

VRRP グループに単純なテキスト認証を設定できます。

始める前に

ネットワークのすべての VRRP スイッチで認証設定が同じであることを確認します。

VRRP 機能が有効になっていることを確認します ([VRRP の設定](#)のセクションを参照)。

インターフェイス上で IP アドレスを設定していることを確認します ([IPv4 アドレスの設定](#)のセクションを参照)。

手順の概要

1. **configure terminal**
2. **interface interface -type slot/port**
3. **no switchport**
4. **vrrp number**
5. **shutdown**
6. **authentication text password**
7. **no shutdown**
8. (任意) **show vrrp**
9. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	interface interface -type slot/port 例 : <code>switch(config)#</code> <code>switch(config-if)# interface ethernet 2/1</code>	インターフェイス設定モードを開始します。
ステップ 3	no switchport 例 :	そのインターフェイスを、レイヤ 3 ルーテッドインターフェイスとして設定します。

	コマンドまたはアクション	目的
	<code>switch(config-if)# no switchport</code>	
ステップ 4	vrrp number 例 : <code>switch(config-if)# vrrp 250</code> <code>switch(config-if-vrrp)#</code>	仮想ルータ グループを作成します。範囲は 1 ～ 255 です。
ステップ 5	shutdown 例 : <code>switch(config-if-vrrp)# shutdown</code> <code>switch(config-if-vrrp)#</code>	VRRP グループを無効にします。デフォルトでは、ディセーブルです。
ステップ 6	authentication text password 例 : <code>switch(config-if-vrrp)# authentication text cisco123</code>	単純なテキスト認証オプションを指定し、キーネーム パスワードを指定します。キーネームの範囲は 1 ～ 255 文字です。16 文字以上を推奨します。テキスト パスワードは、英数字で最大 8 文字です。
ステップ 7	no shutdown 例 : <code>switch(config-if-vrrp)# no shutdown</code> <code>switch(config-if-vrrp)#</code>	VRRP グループを有効にします。デフォルトでは、ディセーブルです。
ステップ 8	(任意) show vrrp 例 : <code>switch(config-if-vrrp)# show vrrp</code>	VRRP 情報を表示します。
ステップ 9	(任意) copy running-config startup-config 例 : <code>switch(config-if-vrrp)# copy running-config startup-config</code>	この設定変更を保存します。

例

アドバタイズメント パケットのタイム インターバルの設定

アドバタイズメント パケットのタイム インターバルを設定できます。

始める前に

VRRP 機能が有効になっていることを確認します ([VRRP の設定](#)のセクションを参照)。

インターフェイス上で IP アドレスを設定していることを確認します ([IPv4 アドレスの設定](#)のセクションを参照)。

手順の概要

1. **configure terminal**
2. **interface interface -type slot/port**
3. **no switchport**
4. **vrrp number**
5. **shutdown**
6. **advertisement-interval seconds**
7. **no shutdown**
8. (任意) **show vrrp**
9. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	interface interface -type slot/port 例 : <pre>switch(config)# switch(config-if)# interface ethernet 2/1</pre>	インターフェイス設定モードを開始します。
ステップ 3	no switchport 例 : <pre>switch(config-if)# no switchport</pre>	そのインターフェイスを、レイヤ3ルーテッドインターフェイスとして設定します。
ステップ 4	vrrp number 例 : <pre>switch(config-if)# vrrp 250 switch(config-if-vrrp)#</pre>	仮想ルータ グループを作成します。範囲は 1 ～ 255 です。
ステップ 5	shutdown 例 : <pre>switch(config-if-vrrp)# shutdown switch(config-if-vrrp)#</pre>	VRRP グループを無効にします。デフォルトでは、ディセーブルです。
ステップ 6	advertisement-interval seconds 例 : <pre>switch(config-if-vrrp)# advertisement-interval 15</pre>	アドバタイズメントフレームの送信間隔を秒数で設定します。有効な範囲は 1 ～ 254 です。デフォルト値は 1 秒です。

	コマンドまたはアクション	目的
ステップ 7	no shutdown 例 : <pre>switch(config-if-vrrp) # no shutdown switch(config-if-vrrp) #</pre>	VRRP グループを有効にします。デフォルトでは、ディセーブルです。
ステップ 8	(任意) show vrrp 例 : <pre>switch(config-if-vrrp) # show vrrp</pre>	VRRP 情報を表示します。
ステップ 9	(任意) copy running-config startup-config 例 : <pre>switch(config-if-vrrp) # copy running-config startup-config</pre>	この設定変更を保存します。

例

プリエンブションのディセーブル化

VRRP グループメンバーのプリエンブションをディセーブルにできます。プリエンブションをディセーブルにした場合は、プライオリティのより高いバックアップルータが、プライオリティのより低いプライマリルータを引き継ぐことはありません。プリエンブションはデフォルトでイネーブルです。

始める前に

VRRP 機能が有効になっていることを確認します ([VRRP の設定](#)のセクションを参照)。

インターフェイス上で IP アドレスを設定していることを確認します ([IPv4 アドレスの設定](#)のセクションを参照)。

手順の概要

1. **configure terminal**
2. **interface interface -type slot/port**
3. **no switchport**
4. **vrrp number**
5. **shutdown**
6. **no preempt**
7. **no shutdown**
8. (任意) **show vrrp**
9. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	interface interface -type slot/port 例 : switch(config)# switch(config-if)# interface ethernet 2/1	インターフェイス設定モードを開始します。
ステップ 3	no switchport 例 : switch(config-if)# no switchport	そのインターフェイスを、レイヤ3ルーテッドインターフェイスとして設定します。
ステップ 4	vrrp number 例 : switch(config-if)# vrrp 250 switch(config-if-vrrp)#	仮想ルータ グループを作成します。範囲は 1 ～ 255 です。
ステップ 5	shutdown 例 : switch(config-if-vrrp)# shutdown switch(config-if-vrrp)#	VRRP グループを無効にします。デフォルトでは、ディセーブルです。
ステップ 6	no preempt 例 : switch(config-if-vrrp)# no preempt	preempt オプションをディセーブルにして、プライオリティが上位のバックアップが使用されてもプライマリが変わらないようにします。
ステップ 7	no shutdown 例 : switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#	VRRP グループを有効にします。デフォルトでは、ディセーブルです。
ステップ 8	(任意) show vrrp 例 : switch(config-if-vrrp)# show vrrp	VRRP 情報を表示します。
ステップ 9	(任意) copy running-config startup-config 例 : switch(config-if-vrrp)# copy running-config startup-config	この設定変更を保存します。

VRRP インターフェイス ステート トラッキングの設定

インターフェイスのステート追跡機能では、スイッチ内の他のインターフェイスのステートに基づいて、仮想ルータのプライオリティが変更されます。トラッキング対象のインターフェイスがダウンしたり、IP アドレスが削除されると、Cisco NX-OS はトラッキングのプライオリティ値を仮想ルータに割り当てます。トラッキング対象のインターフェイスがオンライン状態になり、IP アドレスがこのインターフェイスに設定されると、Cisco NX-OS は仮想ルータに設定されていたプライオリティを復元します（[VRRP プライオリティの設定](#)を参照）。



- (注) インターフェイス ステート トラッキングを動作させるには、インターフェイス上でプリエンブションをイネーブルにする必要があります。



- (注) VRRP はレイヤ 2 インターフェイスのトラッキングをサポートしていません。

始める前に

VRRP 機能が有効になっていることを確認します（[VRRP の設定](#)のセクションを参照）。

インターフェイス上で IP アドレスを設定していることを確認します（[IPv4 アドレスの設定](#)のセクションを参照）。

仮想ルータが有効になっていることを確認します（[VRRP グループの設定](#)のセクションを参照）。

手順の概要

1. **configure terminal**
2. **interface interface -type slot/port**
3. **no switchport**
4. **vrrp number**
5. **shutdown**
6. **track interface type number priority value**
7. **no shutdown**
8. (任意) **show vrrp**
9. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	interface interface -type slot/port 例 : switch(config)# switch(config-if)# interface ethernet 2/1	インターフェイス設定モードを開始します。
ステップ 3	no switchport 例 : switch(config-if)# no switchport	そのインターフェイスを、レイヤ3ルーテッドインターフェイスとして設定します。
ステップ 4	vrrp number 例 : switch(config-if)# vrrp 250 switch(config-if-vrrp)#	仮想ルータ グループを作成します。範囲は 1 ～ 255 です。
ステップ 5	shutdown 例 : switch(config-if-vrrp)# shutdown switch(config-if-vrrp)#	VRRP グループを無効にします。デフォルトでは、ディセーブルです。
ステップ 6	track interface type number priority value 例 : switch(config-if-vrrp)# track interface ethernet 2/10 priority 254	VRRP グループのインターフェイスプライオリティ トラッキングをイネーブルにします。プライオリティの範囲は 1 ～ 254 です。
ステップ 7	no shutdown 例 : switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#	VRRP グループを有効にします。デフォルトでは、ディセーブルです。
ステップ 8	(任意) show vrrp 例 : switch(config-if-vrrp)# show vrrp	VRRP 情報を表示します。
ステップ 9	(任意) copy running-config startup-config 例 :	この設定変更を保存します。

	コマンドまたはアクション	目的
	<code>switch(config-if-vrrp)# copy running-config startup-config</code>	

VRRPv3 の設定

VRRPv3 の有効化

VRRPv3 グループを構成して有効にするには、その前に VRRPv3 機能をグローバルで有効にする必要があります。

VRRPv3 機能を有効にするには、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。

コマンド	目的
feature vrrpv3 例 : <code>switch(config)# feature vrrpv3</code>	VRRP バージョン 3 を有効にします。このコマンドの <code>no</code> 形式を使用すると、VDC で VRRPv3 が無効になります。 VRRPv2 が現在設定されている場合は、グローバル設定モードで <code>no feature vrrp</code> コマンドを使用して VRRPv2 設定を削除し、その後 <code>feature vrrpv3</code> コマンドを使用して VRRPv3 を有効にします。

VRRPv3 グループの構成

VRRPv3 グループを作成し、仮想 IP アドレスを割り当て、グループをイネーブルにすることができます。

VRRPv3 グループに構成できる仮想 IPv4 アドレスは 1 つです。プライマリ VRRPv3 ルータはデフォルトで、仮想 IP アドレスを直接宛先とするパケットをドロップします。これは、VRRPv3 プライマリがパケットを転送するネクストホップルータとしてのみ想定されているからです。アプリケーションによっては、Cisco NX-OS が仮想ルータ IP 宛のパケットを受け付けるようにする必要があります。仮想 IP アドレスに `secondary` オプションを使用すると、ローカルルータが VRRPv3 マスターの場合、これらのパケットを受け付けるようになります。



(注) VRRPv3 グループを構成した場合は、そのグループをアクティブにするために、グループを明示的に有効にする必要があります。

始める前に

- VRRPv3 機能が有効になっていることを確認します。
- インターフェイス上で IP アドレスを構成していることを確認します。

手順の概要

1. **configure terminal**
2. **interface interface -type slot/port**
3. **[no] vrrpv3 number address-family { ipv4 | ipv6 }**
4. (任意) **[no] address ip-address [primary | secondary]**
5. (任意) **[no] description** 説明
6. (任意) **[no] match-address**
7. (任意) **[no] preempt [delay minimum seconds]**
8. (任意) **[no] priority level**
9. (任意) **[no] timers advertise interval**
10. **[no] vrrpv2**
11. (任意) **[no] shutdown**
12. (任意) **show fhrp [interface-type interface-number] [verbose]**
13. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 interface -type slot/port 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 3	[no] vrrpv3 number address-family { ipv4 ipv6 } 例 : <pre>switch(config-if)# vrrpv3 5 address-family ipv4 switch(config-if-vrrpv3-group)#</pre>	VRRPv3 グループを作成し、VRRPv3 グループ設定モードを開始します。範囲は 1 ～ 255 です。 このコマンドの no 形式を使用すると、そのサブモード内で定義されたすべてのコンフィギュレーションが削除されます。
ステップ 4	(任意) [no] address ip-address [primary secondary] 例 : <pre>switch(config-if-vrrpv3-group)# address 100.0.1.10 primary</pre>	VRRPv3 グループのプライマリ アドレスまたはセカンダリ IPv4 または IPv6 アドレスを指定します。 (注) VRRPv3 グループでセカンダリ IP アドレスを使用するには、まず同じグループでプライマリ IP アドレスを設定する必要があります。

	コマンドまたはアクション	目的
ステップ 5	(任意) [no] description 説明 例 : <pre>switch(config-if-vrrpv3-group)# description group3</pre>	VRRPv3 グループの説明を指定します。最大 80 文字の英数字を入力できます。
ステップ 6	(任意) [no] match-address 例 : <pre>switch(config-if-vrrpv3-group)# match-address</pre>	アドバタイズメントパケットのセカンダリ アドレスを設定したアドレスと照合します。
ステップ 7	(任意) [no] preempt [delay minimum seconds] 例 : <pre>switch(config-if-vrrpv3-group)# preempt delay minimum 30</pre>	オプションの延期時間を指定して、プライオリティの低いプライマリ スイッチのプリエンプションをイネーブルにします。範囲は 0～3600 です。
ステップ 8	(任意) [no] priority level 例 : <pre>switch(config-if-vrrpv3-group)# priority 3</pre>	VRRPv3 グループのプライオリティを指定します。範囲は 1～254 です。
ステップ 9	(任意) [no] timers advertise interval 例 : <pre>switch(config-if-vrrpv3-group)# timers advertise 1000</pre>	アドバタイズメント タイマーを設定します (ミリ秒単位)。範囲は 100～40950 です。 (注) シスコは、このタイマーを 1 秒以上の値に設定することを推奨します。
ステップ 10	[no] vrrpv2 例 : <pre>switch(config-if-vrrpv3-group)# vrrpv2</pre>	VRRPv2 のみをサポートしているデバイスとの相互運用性を確保するために、VRRPv2 に対するサポートも同時に有効にします。 (注) VRRPv2 互換モードは、VRRPv2 から VRRPv3 にアップグレードするために提供されます。これは完全な VRRPv2 実装ではないので、アップグレードを実行する場合にのみ使用してください。
ステップ 11	(任意) [no] shutdown 例 : <pre>switch(config-if-vrrp3-group)# shutdown</pre>	VRRPv3 グループの VRRP 構成を無効にします。
ステップ 12	(任意) show fhrp [interface-type interface-number] [verbose] 例 : <pre>switch(config-if-vrrp3-group)# show fhrp port-channel 101 verbose</pre>	ファーストホップ冗長性プロトコル (FHRP) の情報を表示します。 詳細情報を表示するには、 verbose キーワードを使用します。

	コマンドまたはアクション	目的
ステップ 13	(任意) copy running-config startup-config 例 : <pre>switch(config-if-vrrp3-group)# copy running-config startup-config</pre>	この設定変更を保存します。

FHRP クライアント前の初期化前遅延時間の構成

FHRP クライアントの初期化の遅延時間を構成できます。



- (注) すべての FHRP プロトコルで、アグレッシブ タイマーの使用は、CPU スパイクを引き起こし、制御パケットフローを増加させるため、推奨しません。VRRPv3 の場合、VRRP ノードの適切なフェールオーバーのために十分なインターフェイス遅延/リロード遅延を構成する必要があります。

この機能を構成するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
fhrp delay {[minimum] [reload] seconds } 例 : <pre>switch(config)# fhrp delay minimum 34</pre>	FHRP クライアントの初期化の遅延期間を指定します。指定できる範囲は 0 ～ 3600 秒です。 minimum キーワードで、インターフェイスが使用可能になった後の遅延時間を構成します。 reload コマンドで、デバイスのリロード後の遅延時間を構成します。

VRRPv3 コントロールグループの設定

VRRPv3 コントロール グループを設定できます。

始める前に

- VRRPv3 機能が有効になっていることを確認します。
- インターフェイス上で IP アドレスを構成していることを確認します。

手順の概要

1. **configure terminal**
2. **interface interface - type slot/port**
3. **[no] ip address ip-address mask [secondary]**

4. **[no] vrrpv3 number address-family { ipv4 | ipv6 }**
5. (任意) **[no] address ip-address [primary | secondary]**
6. (任意) **[no] shutdown**
7. **[show fhrp [interface-type interface-number] [verbose]**
8. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 interface - type slot/port 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 3	[no] ip address ip-address mask [secondary] 例 : <pre>switch(config-if)# ip address 209.165.200.230 255.255.255.224</pre>	インターフェイスの IP アドレスを設定します。 (注) secondary キーワードを使用して、インターフェイスで追加の IP アドレスを構成できます。
ステップ 4	[no] vrrpv3 number address-family { ipv4 ipv6 } 例 : <pre>switch(config-if)# vrrpv3 5 address-family ipv4 switch(config-if-vrrpv3-group)#</pre>	VRRPv3 グループを作成し、VRRPv3 グループ設定モードを開始します。範囲は 1 ～ 255 です。
ステップ 5	(任意) [no] address ip-address [primary secondary] 例 : <pre>switch(config-if-vrrpv3-group)# address 209.165.200.227 primary</pre>	VRRPv3 グループのプライマリ アドレスまたはセカンダリ IPv4 または IPv6 アドレスを指定します。
ステップ 6	(任意) [no] shutdown 例 : <pre>switch(config-if-vrrpv3-group)# shutdown</pre>	VRRPv3 グループの VRRP 構成を無効にします。
ステップ 7	[show fhrp [interface-type interface-number] [verbose] 例 :	ファースト ホップ冗長性プロトコル (FHRP) の情報を表示します。

	コマンドまたはアクション	目的
	<code>switch(config-if-vrrp3-group)# show fhrp port-channel 101 verbose</code>	詳細情報を表示するには、 verbose キーワードを使用します。
ステップ 8	copy running-config startup-config 例 : <code>switch(config-if-vrrp3-group)# copy running-config startup-config</code>	この設定変更を保存します。

VRRPv2 設定の確認

VRRPv2 の構成情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show vrrpv2	すべてのグループについて、VRRP ステータスを表示します。
<code>show vrrpv2 vr group-number</code>	1 つの VRRP グループについて、VRRP ステータスを表示します。
show vrrp v2 vr number interface interface-type port configuration	インターフェイスの仮想ルータ設定を表示します。
show vrrpv2 vr number interface interface-type portstatus	インターフェイスの仮想ルータステータスを表示します。
<code>show fhrp [interface-type interface-number] [verbose]</code>	ファースト ホップ冗長性プロトコル (FHRP) の情報を表示します。
show interface interface-type	インターフェイスの仮想ルータ設定を表示します。

VRRPv3 設定の確認

`show vrrpv3` コマンド出力のフィールドについては、次の表を参照してください。

コマンド	目的
<code>></code>	ファイルにリダイレクトします
<code>>></code>	追加モードでファイルにリダイレクトします
<code>all</code>	すべての VRRPV3 情報
<code>brief</code>	概要出力

コマンド	目的
detail	詳細出力
ethernet	イーサネット IEEE 802.3z
ipv4	IPv4
ipv6	IPv6
loopback	ループバック インターフェイス
port-channel	ポートチャネル インターフェイス
統計情報	統計情報の出力
vlan	VLAN インターフェイス
	コマンド出力をフィルタにパイプします

たとえば、`show vrrpv3 statistics` コマンドを使用して、VRRPv3 統計情報を表示します。

VRRP 統計情報の表示

VRRP の統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
<code>show vrrp statistics interface interface-type port vr number</code>	仮想ルータ情報を表示します。
<code>show vrrp statistics</code>	VRRP の統計情報を表示します。

特定のインターフェイスについて、IPv4 VRRP 統計情報を消去するには、`clear vrrp vr` コマンドを使用します。

指定した IPv4 仮想ルータについて、すべての統計情報を消去するには、`clear vrrp ipv4` コマンドを使用します。

VRRPv2 の設定例

この例では、ルータ A とルータ B はそれぞれ 3 つの VRRP グループに属しています。コンフィギュレーションにおいて、各グループのプロパティは次のとおりです。

- グループ 1 :
 - 仮想 IP アドレスは 10.1.0.10 です。
 - ルータ A は優先順位 120 で、このグループのプライマリになります。

- アドバタイズ インターバルは 3 秒です。
 - プリエンプションはイネーブルです。
- グループ 5 :
- ルータ B はプライオリティ 200 で、このグループのマスターになります。
 - アドバタイズ インターバルは 30 秒です。
 - プリエンプションはイネーブルです。
- グループ 100 :
- ルータ A は、IP アドレスが上位 (10.1.0.2) なので、このグループのプライマリになります。
 - アドバタイズ インターバルはデフォルトの 1 秒です。
 - プリエンプションはディセーブルです。

ルータ A

```
interface ethernet 1/0
no switchport

ip address 10.1.0.2/16
no shutdown
vrrpv2 1
priority 120
authentication text cisco
advertisement-interval 3
address 10.1.0.10
no shutdown
vrrpv2 5
priority 100
advertisement-interval 30
address 10.1.0.50
no shutdown
vrrpv2 100
no preempt
address 10.1.0.100
no shutdown
```

ルータ B

```
interface ethernet 1/0
no switchport

ip address 10.2.0.1/2
no shutdown
vrrpv2 1
priority 100
authentication text cisco
advertisement-interval 3
address 10.2.0.10
no shutdown
```

```
vrrpv2 5
priority 200
advertisement-interval 30
address 10.2.0.50
no shutdown
vrrpv2 100
no preempt
address 10.2.0.100
no shutdown
```

VRRPv3 の構成例

VRRPv3 の次の構成例を参照してください。

```
interface Vlan20
vrrpv3 10 address-family ipv4
timers advertise 1000
priority 100
preempt
match-address
no vrrpv2
address 20.1.1.1 primary
address 20.1.1.5 secondary
vrrpv3 10 address-family ipv6
timers advertise 1000
priority 100
preempt
match-address
no vrrpv2
address fe80::1 primary
address 2011::5
```

その他の参考資料

VRRP の実装に関連する詳細情報については、次の項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
Hot Standby Router Protocol の設定	『Configuring HSRP』



第 20 章

オブジェクト トラッキングの設定

この章では、Cisco NX-OS スイッチ上でオブジェクト トラッキングを設定する方法について説明します。

この章は、次の項で構成されています。

- [オブジェクト トラッキングについて \(561 ページ\)](#)
- [オブジェクト トラッキングに関する注意事項と制約事項 \(563 ページ\)](#)
- [オブジェクト トラッキングのデフォルト設定 \(563 ページ\)](#)
- [オブジェクト トラッキングの設定 \(563 ページ\)](#)
- [オブジェクト トラッキングの設定の確認 \(574 ページ\)](#)
- [オブジェクト トラッキングの設定例 \(574 ページ\)](#)
- [関連項目 \(575 ページ\)](#)
- [その他の参考資料 \(575 ページ\)](#)

オブジェクト トラッキングについて

オブジェクト トラッキングを使用すると、インターフェイス ラインプロトコル ステート、IP ルーティング、ルート到達可能性などの、スイッチ上の特定のオブジェクトをトラッキングし、トラッキング対象オブジェクトのステートが変化したときに対処できます。この機能により、ネットワークのアベイラビリティが向上し、オブジェクトがダウンした場合のリカバリ時間が短縮されます。

オブジェクト トラッキングの概要

オブジェクト トラッキング機能を使用すると、トラッキング対象オブジェクトを作成できます。複数のクライアントでこのオブジェクトを使用し、トラッキング対象オブジェクトが変化したときのクライアント動作を変更できます。複数のクライアントがそれぞれの関心をトラッキングプロセスに登録し、同じオブジェクトをトラッキングし、オブジェクトのステートが変化したときに異なるアクションを実行します。

クライアントには次の機能が含まれます。

- ホットスタンバイ冗長プロトコル (HSRP)

- 仮想ルータ冗長プロトコル (VRRP)
- Embedded Event Manager (EEM)

オブジェクトトラッキングは、トラッキング対象オブジェクトのステータスをモニタし、変更があった場合は関係クライアントに伝えます。各トラッキング対象オブジェクトは、一意の番号で識別します。クライアントはこの番号を使用して、トラッキング対象オブジェクトのステータスの変化したときに実行するアクションを設定できます。

Cisco NX-OS がトラッキングするオブジェクトタイプは、次のとおりです。

- インターフェイスラインプロトコルステート：ラインプロトコルステートがアップまたはダウンかどうかをトラッキングします。
- インターフェイス IP ルーティングステート：インターフェイスに IPv4 アドレスが設定されていて、IPv4 ルーティングがイネーブルでアクティブかどうかをトラッキングします。
- IP ルート到達可能性：IPv4 ルートが存在していて、ローカルスイッチから到達可能かどうかをトラッキングします。

たとえば、HSRP を設定すると、冗長ルータの 1 つをネットワークの他の部分に接続するインターフェイスのラインプロトコルをトラッキングできます。そのリンクがダウンした場合、影響のある HSRP ルータのプライオリティを変更できます。

オブジェクトトラッキングリスト

オブジェクトトラッキングリストを使用すると、複数のオブジェクトのステータスをまとめてトラッキングできます。オブジェクトトラッキングリストは次の機能をサポートします。

- ブール「and」機能：トラッキングリストオブジェクトがアップになるには、トラッキングリスト内に定義された各オブジェクトがアップ状態である必要があります。
- ブール「or」機能：トラッキング対象オブジェクトがアップになるには、トラッキングリスト内に定義された少なくとも 1 つのオブジェクトがアップ状態である必要があります。
- しきい値パーセンテージ：トラッキング対象リストに含まれるアップオブジェクトのパーセンテージが、アップ状態になるトラッキングリストの設定されたアップしきい値を上回っている必要があります。トラッキング対象リストに含まれるダウンオブジェクトのパーセンテージが設定されたトラッキングリストのダウンしきい値を上回っている場合、トラッキング対象リストはダウンとしてマークされます。
- しきい値の重み：トラッキング対象リスト内の各オブジェクトに重み値を割り当て、トラッキングリストに重みしきい値を割り当てます。すべてのアップオブジェクトの重み値の合計がトラッキングリストの重みアップしきい値を超えている場合、トラッキングリストはアップ状態になります。すべてのダウンオブジェクトの重み値の合計がトラッキングリストの重みダウンしきい値を超えている場合、トラッキングリストはダウン状態になります。

トラックリストの詳細については、「[ブール式によるオブジェクトトラックリストの設定](#)」を参照してください。

仮想化のサポート

オブジェクトトラッキングは仮想ルーティングおよび転送（VRF）インスタンスをサポートします。デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS はユーザーをデフォルトの VRF に配置します。Cisco NX-OS はデフォルトで、デフォルト VRF のオブジェクトのルート到達可能ステータスをトラッキングします。別の VRF のオブジェクトをトラッキングする場合は、オブジェクトをその VRF のメンバとして設定する必要があります（「[デフォルト以外の VRF に対してオブジェクトトラッキングを設定する](#)」の項を参照）。

詳細については、「[レイヤ 3 仮想化の設定](#)」を参照してください。

オブジェクトトラッキングに関する注意事項と制約事項

オブジェクトトラッキング設定時の注意事項および制約事項は、次のとおりです。

- 最大 500 のトラッキング対象オブジェクトをサポートします。
- イーサネット、サブインターフェイス、トンネル、ポートチャネル、ループバックインターフェイス、および VLAN インターフェイスをサポートします。
- HSRP グループごとに 1 つのトラッキング対象オブジェクトをサポートします。

オブジェクトトラッキングのデフォルト設定

下の表に、オブジェクトトラッキングパラメータのデフォルト設定を示します。

表 25: デフォルトのオブジェクトトラッキングパラメータ

パラメータ	デフォルト
Tracked Object VRF	デフォルト VRF のメンバ

オブジェクトトラッキングの設定

インターフェイスに対するオブジェクトトラッキングの設定

インターフェイスのラインプロトコルまたは IPv4 ルーティングの状態をトラッキングするように Cisco NX-OS を設定できます。

手順の概要

1. **configure terminal**
2. **track object-id interface interface-type number { ip routing | line-protocol }**
3. (任意) **show track [object-id]**
4. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	track object-id interface interface-type number { ip routing line-protocol } 例 : <pre>switch(config)# track 1 interface ethernet 1/2 line-protocol switch(config-track#</pre>	インターフェイスのトラッキング対象オブジェクトを作成し、トラッキング コンフィギュレーション モードを開始します。 <i>object-id</i> の範囲は 1 ～ 500 です。
ステップ 3	(任意) show track [object-id] 例 : <pre>switch(config-track)# show track 1</pre>	オブジェクトのトラッキング情報を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config-track)# copy running-config startup-config</pre>	この設定変更を保存します。

例

Ethernet 1/2 上でライン プロトコル ステートのオブジェクト トラッキングを設定する例を示します。

```
switch# configure terminal
switch(config)# track 1 interface ethernet 1/2 line-protocol
switch(config-track)# copy running-config startup-config
```

Ethernet 1/2 上で IPv4 ルーティング ステートのオブジェクト トラッキングを設定する例を示します。

```
switch# configure terminal
switch(config)# track 2 interface ethernet 1/2 ip routing
switch(config-track)# copy running-config startup-config
```

ルート到達可能性に対するオブジェクトトラッキングの設定

IP ルートの存在および到達可能性をトラッキングするように Cisco NX-OS を設定できます。

手順の概要

1. **configure terminal**
2. **track object-id ip route prefix/length reachability**
3. (任意) **show track [object-id]**
4. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	track object-id ip route prefix/length reachability 例： switch(config)# track 2 ip route 192.0.2.0/8 reachability switch(config-track)#	ルートのトラッキング対象オブジェクトを作成し、トラッキング コンフィギュレーション モードを開始します。 <i>object-id</i> の範囲は 1 ～ 500 です。IP のプレフィックスフォーマットは A.B.C.D/length です。length の範囲は 1 ～ 32 です。
ステップ 3	(任意) show track [object-id] 例： switch(config-track)# show track 1	オブジェクトのトラッキング情報を表示します。
ステップ 4	(任意) copy running-config startup-config 例： switch(config-track)# copy running-config startup-config	この設定変更を保存します。

例

次に、デフォルト VRF で IPv4 ルートのオブジェクトトラッキングを設定する例を示します。

```
switch# configure terminal
switch(config)# track 4 ip route 192.0.2.0/8 reachability
switch(config-track)# copy running-config startup-config
```

ブール式を含むオブジェクトトラッキングリストの設定

複数のトラッキング対象オブジェクトを含むオブジェクトトラッキングリストを設定できます。トラッキング対象リストには1つまたは複数のオブジェクトが含まれます。ブール式では、「and」または「or」演算子を使用して2種類の演算を実行できます。たとえば、「and」演算子を使用して2つのインターフェイスをトラッキングする場合、「アップ」は両方のインターフェイスがアップであることを意味し、「ダウン」はどちらかのインターフェイスがダウンであることを意味します。

手順の概要

1. **configure terminal**
2. **track track-number list boolean { and | or }**
3. **object object-id [not]**
4. (任意) **show track**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	track track-number list boolean { and or } 例 : <pre>switch(config)# track 1 list boolean and switch(config-track)#</pre>	トラッキング対象リストオブジェクトを設定し、トラッキング設定モードを開始します。トラッキング対象リストのステータスがブール式に基づいて決まることを指定します。キーワードは次のとおりです。 • and : すべてのオブジェクトがアップである場合にリストがアップになり、1つ以上のオブジェクトがダウンの場合にリストがダウンになることを指定します。たとえば2つのインターフェイスをトラッキングする場合、アップは両方のインターフェイスがアップ状態であることを表し、ダウンはいずれかのインターフェイスがダウン状態であることを表します。 • or : 少なくとも1つのオブジェクトがアップであればリストがアップになるように指定します。たとえば2つのインターフェイスをトラッキングする場合、アップはいずれか一方のインターフェイスがアップ状態であることを意味

	コマンドまたはアクション	目的
		し、ダウンは両方のインターフェイスがダウン状態であることを意味します。 <i>track-number</i> の範囲は 1 ～ 500 です。
ステップ 3	object object-id [not] 例 : <pre>switch(config-track)# object 10</pre>	トラッキングリストにトラッキング対象オブジェクトを追加します。 <i>object-id</i> の範囲は 1 ～ 500 です。オプションの not キーワードを指定すると、トラッキング対象オブジェクトのステータスが否定されます。 (注) 例では、オブジェクト 10 がアップのときに、トラッキング対象リストがオブジェクト 10 をダウンとして検出します。
ステップ 4	(任意) show track 例 : <pre>switch(config-track)# show track</pre>	オブジェクトのトラッキング情報を表示します。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config-track)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、複数のオブジェクトを含むトラッキングリストをブール「and」で設定する例を示します。

```
switch# configure terminal
switch(config)# track 1 list boolean and
switch(config-track)# object 10
switch(config-track)# object 20 not
```

パーセンテージしきい値を含むオブジェクトトラッキングリストの設定

パーセンテージしきい値を含むオブジェクトトラッキングリストを設定できます。トラッキング対象リストには1つまたは複数のオブジェクトが含まれます。トラッキングリストがアップ状態になるには、アップオブジェクトのパーセンテージがトラッキングリストに設定されたパーセントしきい値を超えている必要があります。たとえば、追跡対象リストに3つのオブジェクトが含まれており、アップしきい値を60%に設定した場合は、2つのオブジェクト（全オブジェクトの66%）がアップ状態になるまで、追跡リストがアップ状態になりません。

手順の概要

1. **configure terminal**
2. **track track-number list threshold percentage**
3. **threshold percentage up up-value down down-value**
4. (任意) **object [object-id]**
5. (任意) **show track**
6. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	track track-number list threshold percentage 例 : <pre>switch(config)# track 1 list threshold percentage switch(config-track)#</pre>	トラッキング対象リストオブジェクトを設定し、トラッキング設定モードを開始します。トラッキング対象リストのステータスが設定されたしきい値パーセントに基づいて決まることを指定します。 <i>track-number</i> の範囲は 1 ～ 500 です。
ステップ 3	threshold percentage up up-value down down-value 例 : <pre>switch(config-track)# threshold percentage up 70 down 30</pre>	トラッキング対象リストのしきい値パーセントを設定します。指定できる範囲は 0 ～ 100% です。
ステップ 4	(任意) object [object-id] 例 : <pre>switch(config-track)# object 10</pre>	トラッキングリストにトラッキング対象オブジェクトを追加します。 <i>object-id</i> の範囲は 1 ～ 500 です。
ステップ 5	(任意) show track 例 : <pre>switch(config-track)# show track</pre>	オブジェクトのトラッキング情報を表示します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config-track)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、アップしきい値が 70 % でダウンしきい値が 30 % の追跡リストを設定する例を示します。

```
switch# configure terminal
switch(config)# track 1 list threshold percentage
switch(config-track)# threshold percentage up 70 down 30
switch(config-track)# object 10
switch(config-track)# object 20
switch(config-track)# object 30
```

重みしきい値を含むオブジェクトトラッキングリストの設定

重みしきい値を含むオブジェクトトラッキングリストを設定できます。トラッキング対象リストには 1 つまたは複数のオブジェクトが含まれます。トラッキングリストがアップステートになるには、アップオブジェクトの重み値の合計がトラッキングリストに設定されたアップ重みしきい値を超えている必要があります。たとえば、トラッキング対象リストに重み値がデフォルトの 10 である 3 つのオブジェクトがあり、アップしきい値を 15 に設定した場合、トラッキングリストがアップ状態になるには、2 つのオブジェクトがアップ状態になる（重み値の合計が 20 になる）必要があります。

手順の概要

1. **configure terminal**
2. **track track-number list threshold weight**
3. **threshold weight up up-value down down-value**
4. **object object-id weight value**
5. （任意） **show track**
6. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	track track-number list threshold weight 例： switch(config)# track 1 list threshold weight switch(config-track)#	トラッキング対象リストオブジェクトを設定し、トラッキング設定モードを開始します。トラッキング対象リストのステートが設定されたしきい値重みに基づいて決まることを指定します。

	コマンドまたはアクション	目的
		<i>track-number</i> の範囲は 1 ～ 500 です。
ステップ 3	threshold weight up up-value down down-value 例： switch(config-track)# threshold weight up 30 down 10	トラッキング対象リストのしきい値重みを設定します。指定できる範囲は 1 ～ 255 です。
ステップ 4	object object-id weight value 例： switch(config-track)# object 10 weight 15	トラッキングリストにトラッキング対象オブジェクトを追加します。 <i>object-id</i> の範囲は 1 ～ 500 です。 <i>value</i> の範囲は 1 ～ 255 です。デフォルトの重み値は 10 です。
ステップ 5	(任意) show track 例： switch(config-track)# show track	オブジェクトのトラッキング情報を表示します。
ステップ 6	(任意) copy running-config startup-config 例： switch(config-track)# copy running-config startup-config	この設定変更を保存します。

例

次に、トラッキングリストのアップ重みしきい値を 30、ダウンしきい値を 10 にそれぞれ設定する例を示します。

```
switch# configure terminal
switch(config)# track 1 list threshold weight
switch(config-track)# threshold weight up 30 down 10
switch(config-track)# object 10 weight 15
switch(config-track)# object 20 weight 15
switch(config-track)# object 30
```

この例では、オブジェクト 10 とオブジェクト 20 がアップの場合にトラッキングリストがアップになり、3 つのオブジェクトがすべてダウンの場合にトラッキングリストがダウンになります。

オブジェクトトラッキングの遅延の設定

トラッキング対象オブジェクトまたはオブジェクトトラッキングリストに対して、オブジェクトまたはリストがステートの変化を開始したときに適用する遅延を設定できます。トラッキング対象オブジェクトまたはトラッキングリストは、ステートの変化が発生したときに遅延タイマーを開始しますが、遅延タイマーが切れるまでステートの変化を認識しません。遅延タイマーが切れると、Cisco NX-OS は再びオブジェクトのステートを確認し、オブジェクトまたは

リストが現在も変更されたステータスのままだった場合にだけステータスの変化を記録します。オブジェクトトラッキングは遅延タイマーが切れる前の中間的なステータスの変化を無視します。

たとえば、インターフェイス ライン プロトコルのトラッキング対象オブジェクトがアップステータスであり、ダウン遅延が 20 秒に設定されている場合は、ラインプロトコルがダウンになると遅延タイマーが開始します。20 秒後にラインプロトコルがダウンになっていなければ、このオブジェクトはダウンステータスになりません。

トラッキング対象オブジェクトまたはトラッキングリストには、独立したアップ遅延とダウン遅延を設定できます。遅延を削除すると、オブジェクトトラッキングからアップ遅延とダウン遅延の両方が削除されます。

遅延は任意の時点で変更できます。オブジェクトまたはリストがトリガーされたイベントから遅延タイマーをすでにカウントしている場合は、次のようにして新しい遅延が計算されます。

- 新しい設定値が古い設定値より小さい場合は、新しい値でタイマーが開始します。
- 新しい設定値が古い設定値より大きい場合は、新しい設定値から現在のタイマーのカウントダウンを引き、古い設定値を引いたものがタイマーになります。

手順の概要

1. **configure terminal**
2. **track object- id { parameters }**
3. **track track-number list{ parameters }**
4. **delay { up up-time [down down-time] | down down-time [up up-time]}**
5. (任意) **show track**
6. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	track object- id { parameters } 例 : <pre>switch(config)# track 2 ip route 192.0.2.0/8 reachability switch(config-track)#</pre>	ルートのトラッキング対象オブジェクトを作成し、トラッキング コンフィギュレーション モードを開始します。 <i>object-id</i> の範囲は 1 ～ 500 です。IP のプレフィックスフォーマットは A.B.C.D/length です。length の範囲は 1 ～ 32 です。

	コマンドまたはアクション	目的
ステップ 3	track track-number list{ parameters } 例 : <pre>switch(config)# track 1 list threshold weight switch(config-track)#</pre>	トラッキング対象リストオブジェクトを設定し、トラッキング設定モードを開始します。トラッキング対象リストのステータスが設定されたしきい値重みに基づいて決まることを指定します。 <i>track-number</i> の範囲は 1 ～ 500 です。
ステップ 4	delay { up up-time [down down-time] down down-time [up up-time] } 例 : <pre>switch(config-track)# delay up 20 down 30</pre>	オブジェクトの遅延タイマーを設定します。指定できる範囲は 0 ～ 180 秒です。
ステップ 5	(任意) show track 例 : <pre>switch(config-track)# show track</pre>	オブジェクトのトラッキング情報を表示します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config-track)# copy running-config startup-config</pre>	この設定変更を保存します。

例

次に、ルートのオブジェクトトラッキングを設定し、遅延タイマーを使用する例を示します。

```
switch# configure terminal
switch(config)# track 2 ip route 209.165.201.0/8 reachability
switch(config-track)# delay up 20 down 30
switch(config-track)# copy running-config startup-config
```

次に、トラッキングリストのアップ重みしきい値を 30、ダウンしきい値を 10 にそれぞれ設定し、遅延タイマーを使用する例を示します。

```
switch# configure terminal
switch(config)# track 1 list threshold weight
switch(config-track)# threshold weight up 30 down 10
switch(config-track)# object 10 weight 15
switch(config-track)# object 20 weight 15
switch(config-track)# object 30
switch(config-track)# delay up 20 down 30
```

次に、インターフェイスがシャットダウンする前後の **show track** コマンドの出力に表示された遅延タイマーの例を示します。

```
switch(config-track)# show track
Track 1
Interface loopback1 Line Protocol
Line Protocol is UP
1 changes, last change 00:00:13
Delay down 10 secs
```

```
switch(config-track)# interface loopback 1
switch(config-if)# shutdown
switch(config-if)# show track
Track 1
Interface loopback1 Line Protocol
Line Protocol is delayed DOWN (8 secs remaining)<----- delay timer counting down
1 changes, last change 00:00:22
Delay down 10 secs
```

非デフォルト VRF に対するオブジェクトトラッキングの設定

特定の VRF でオブジェクトをトラッキングするように Cisco NX-OS を設定できます。

手順の概要

1. **configure terminal**
2. **track object-id ip route *prefix/length* reachability**
3. **vrf member *vrf-name***
4. (任意) **show track [*object-id*]**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	track object-id ip route <i>prefix/length</i> reachability 例 : switch(config)# track 2 ip route 192.0.2.0/8 reachability switch(config-track)#	ルートのトラッキング対象オブジェクトを作成し、トラッキング コンフィギュレーション モードを開始します。 <i>object-id</i> の範囲は 1 ～ 500 です。IP のプレフィックスフォーマットは A.B.C.D/length です。length の範囲は 1 ～ 32 です。
ステップ 3	vrf member <i>vrf-name</i> 例 : switch(config-track)# vrf member Red	設定されたオブジェクトのトラッキングに使用する VRF を設定します。
ステップ 4	(任意) show track [<i>object-id</i>] 例 : switch(config-track)# show track 3	オブジェクトのトラッキング情報を表示します。

	コマンドまたはアクション	目的
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config-track)# copy running-config startup-config</pre>	この設定変更を保存します。

例

ルートのオブジェクトトラッキングを設定し、VRF Red を使用して、そのオブジェクトの到達可能性情報を調べる例を示します。

```
switch# configure terminal
switch(config)# track 2 ip route 209.165.201.0/8 reachability
switch(config-track)# vrf member Red
switch(config-track)# copy running-config startup-config
```

次に、トラッキング対象オブジェクト 2 を変更して、VRF Red の代わりに VRF Blue を使用してこのオブジェクトの到達可能性情報を調べるようにする例を示します。

```
switch# configure terminal
switch(config)# track 2
switch(config-track)# vrf member Blue
switch(config-track)# copy running-config startup-config
```

オブジェクトトラッキングの設定の確認

オブジェクトトラッキングの設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show track [<i>object-id</i>] [brief]	1つまたは複数のオブジェクトについて、オブジェクトトラッキング情報を表示します。
show track [<i>object-id</i>] interface [brief]	インターフェイススペースのオブジェクトトラッキング情報を表示します。
show track [<i>object-id</i>] ip-route [brief]	IPv4 ルートベースのオブジェクトトラッキング情報を表示します。

オブジェクトトラッキングの設定例

次の例は、ルート到達可能性に対してオブジェクトトラッキングを設定し、VRF Red を使用してルートの到達可能性情報を調べる方法を示しています。

```
switch# configure terminal
switch(config)# track 2 ip route 209.165.201.0/8 reachability
switch(config-track)# vrf member Red
```

```
switch(config-track)# copy running-config startup-config
```

関連項目

オブジェクトトラッキングの関連情報については、次の項目を参照してください。

- [レイヤ 3 仮想化の設定](#)
- [『Configuring HSRP』](#)

その他の参考資料

オブジェクトトラッキングの実装に関連する詳細情報については、次の項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
Embedded Event Manager の設定	Cisco Nexus 3600 システム管理の構成ガイド



付録 A

IETF RFC

この付録は、サポートされている IETF RFC の一覧です。

- [IETF RFC \(577 ページ\)](#)

IETF RFC

BGP の RFC

RFC	タイトル
RFC 1997	<i>BGP</i> コミュニティの属性
RFC 2385	<i>TCP MD5</i> シグネチャ オプションを使用した <i>BGP</i> セッションの保護
RFC 2439	<i>BGP</i> ルート フラップ ダンピング
RFC 2519	ドメイン ルート間集約のフレームワーク
RFC 2858	<i>BGP-4</i> のマルチプロトコル拡張
RFC 3065	<i>BGP</i> の自律システム連合
RFC 3392	<i>BGP-4</i> による機能のアドバタイズメント
RFC 4271	ボーダー ゲートウェイ プロトコル 4 (<i>BGP-4</i>)
RFC 4273	<i>BGP-4</i> の管理対象オブジェクトの定義
RFC 4456	<i>BGP</i> ルート リフレクション: フルメッシュ内部 <i>BGP (IBGP)</i> の代替
RFC 4486	<i>BGP Cease</i> 通知メッセージのサブコード
RFC 4893	4 オクテット AS 番号スペースの <i>BGP</i> サポート
RFC 5004	1 つの外部から別の外部への <i>BGP</i> 最良パス移行の回避

RFC	タイトル
RFC 5549	IPv6 ネクスト ホップを使用した IPv4 ネットワーク レイヤ到達可能性情報のアドバタイズ
RFC 7606	BGP 更新メッセージの改訂されたエラー処理
draft-ietf-idr-bgp4-mib-15.txt	BGP4-MIB

ファーストホップ冗長プロトコルに関する RFC

RFC	タイトル
RFC 2281	『Hot Standby Redundancy Protocol』
RFC 3768	『Virtual Router Redundancy Protocol』

IP サービスに関する RFC

RFC	タイトル
RFC 786	UDP
RFC 791	IP
RFC 792	ICMP
RFC 793	[TCP]
RFC 826	『ARP』
RFC 1027	『Proxy ARP』
RFC 1591	『DNS Client』
RFC 1812	『IPv4 routers』

OSPF の RFC

RFC	タイトル
RFC 2328	『OSPF Version 2』
RFC 3101	『The OSPF Not-So-Stubby Area (NSSA) Option』

RFC	タイトル
RFC 2370	『 <i>The OSPF Opaque LSA Option</i> 』
RFC 3137	『 <i>OSPF Stub Router Advertisement</i> 』

RIP に関する RFC

RFC	タイトル
RFC 2453	<i>RIP</i> バージョン 2
RFC 2082	<i>RIP-2 MD5</i> 認証



索引

A

additional-paths receive [333](#)
additional-paths selection route-map [335](#)
additional-paths send [333](#)
address-family {ipv4 | ipv6} {multicast | unicast} [322, 324](#)
address-family ipv4 unicast [386–387, 392–393, 396–397](#)
area [104–105](#)

B

BGP [326](#)
「Configuring Authentication」 [326](#)

C

capability additional-paths receive [332](#)
capability additional-paths send [332](#)
clear ip rip statistics [400](#)
clear rip policy statistics redistribute [400](#)

D

default-information originate [392–393](#)
default-metric [109–110, 392–393](#)
distance [386–387](#)

E

enhanced-error [343](#)

F

feature pbr [504–505](#)
feature rip [385–386](#)

G

graceful-restart [375](#)
graceful-restart-helper [375–376](#)

I

inherit peer [322–323](#)
インターフェイス [388](#)
RIP の設定 [388](#)
ip rip authentication keychain [389–390](#)
ip rip authentication mode [389–390](#)
ip rip metric-offset [399](#)
ip rip passive-interface [391](#)
ip rip poison-reverse [391](#)
ip rip route-filter [399](#)
ip rip summary-address [392](#)
ip router rip [388–389, 396–397](#)
ip-address [396–397](#)

M

maximum-paths [386–387](#)
maximum-peers [322–323](#)
metric direct 0 [394–395](#)

N

neighbor [322–323](#)

P

path-attribute discard [342](#)
path-attribute treat-as-withdraw [342](#)

R

redistribute [109–110, 392–393, 396–397](#)
restart rip [388](#)
RIP [381, 384–385, 398, 400](#)
ガイドライン [384](#)
確認 [400](#)
仮想化のサポート [384](#)
高可用性 [384](#)
制限事項 [384](#)
説明 [381](#)
前提条件 [384](#)
調整 [398](#)

RIP (続き)

デフォルト設定 385

有効化 385

ライセンス要件 384

RIP インスタンス 386–387

再起動 387

作成 386

RIPv2 認証 382

RIP 統計情報 400

表示 400

RIP 認証 389

構成 389

RIP の設定 388

インターフェイス上 388

route-map 454–455, 459

router bgp 322–323, 374–375

router rip 386–387, 392–397

S

show bgp {ipv4 | ipv6} unicast path-attribute discard 343

show bgp {ipv4 | ipv6} unicast path-attribute unknown 343

show bgp ipv6 unicast 334–336, 343

show bgp {ipv4|ipv6} unicast neighbors 322, 324

show bgp neighbor 332–333

show feature 385–386, 504–505

show ip rip 386–389, 396, 398, 400

show ip bgp neighbors 322, 324

show ip rip instance 400

show ip rip route 392–393

show ipv6 routers interface 322, 324

show ip ospf 104–105

show running-config bgp 375–376

show running-config rip 394–395

show running-configuration rip 400

split horizon with poison reverse 391

構成 391

T

timers basic 399

timers prefix-peer-timeout 375

V

vrf 396–397

vrf context 396

vrf member 396–397

か

ガイドライン 384

RIP 384

確認 400

RIP 400

仮想化 396

構成 396

仮想化のサポート 384

RIP 384

<

グレースフル リスタート 374

設定 374

こ

高可用性 384

RIP 384

さ

作成 386

RIP インスタンス 386

す

スプリット ホライズン 382

せ

制限事項 384

RIP 384

前提条件 384

RIP 384

ち

調整 398

RIP 398

て

デフォルト設定 385

RIP 385

と

等コストマルチパス (ECMP) 384

は

パッシブ インターフェイス 391

構成 391

ら

ライセンス要件 [384](#)

る

ルート再配布 [383, 392](#)
構成 [392](#)

ルート集約 [383, 392](#)

構成 [392](#)

ルートのフィルタリング [383](#)

ろ

ロード バランシング [384](#)

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。