IP アドレッシング：NAT コンフィギュレーション ガイド、Cisco IOS XE Release 3S（ASR 1000）

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

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

IP アドレス節約のための NAT 設定 1

機能情報の確認 2

IP アドレス節約のための NAT 設定に関する前提条件 2

アクセス リスト 2

NAT 要件 2

IP アドレス節約のための NAT 設定に関する制約事項 3

IP アドレス節約のための NAT 設定について 4

IP アドレス節約のために NAT を設定する利点 4

NAT の機能 5

NAT の用途 5

NAT の内部アドレスおよび外部アドレス 5

内部送信元アドレス変換 6

内部グローバル アドレスのオーバーロード 8

NAT のタイプ 9

NAT における TCP 負荷分散 9

スタティック IP アドレスのサポート 11

RADIUS 11

サービス拒絶攻撃 11

NAT を標的にするウイルスおよびワーム 11

IP アドレス節約のために NAT を設定する方法 12

内部送信元アドレスの設定 12

内部送信元アドレスのスタティック変換の設定 12

内部送信元アドレスのダイナミック変換の設定 14

NAT を使用した内部ユーザのインターネットへのアクセスの許可 17

アドレス変換タイムアウトの設定 19

変換タイムアウトの変更 19

オーバーロードが設定されている場合のタイムアウトの変更 19

NAT を使用してオーバーラップするネットワークに通信を許可するには 21
オーバーラップするネットワークのスタティック変換の設定 22
次の作業 23
オーバーラップするネットワークのダイナミック変換の設定 24
サーバ TCP ロード バランシングの設定 26
内部インターフェイスでのルート マップのイネーブル化 28
NAT Route Maps Outside-to-Inside サポートのイネーブル化 29
外部 IP アドレスのみの NAT の設定 31
NAT Default Inside Server 機能の設定 34
NAT ルータでの RTSP の再イネーブル化 35
スタティック IP アドレスを持つユーザのサポートの設定 36
NAT 変換のレート制限機能の設定 38
IP アドレス節約のための NAT 設定例 39
例：内部送信元アドレスのスタティック変換の設定 39
例：内部送信元アドレスのダイナミック変換の設定 40
例：NAT を使用した内部ユーザのインターネットへのアクセスの許可 40
例：NAT を使用したオーバーラップするネットワークに対する通信の許可 41
例：サーバ TCP のロード バランシングの設定 41
例：内部インターフェイスでのルート マップのイネーブル化 41
例：NAT Route Maps Outside-to-Inside サポートのイネーブル化 41
例：外部 IP アドレスのみの NAT の設定 42
例：スタティック IP アドレスを持つユーザのサポートの設定 42
例：NAT スタティック IP サポートの設定 42
例：NAT スタティック IP サポートに使用される RADIUS プロファイルの作成 42
例：NAT 変換のレート制限機能の設定 42
例：グローバル NAT レート制限の設定 43
例：特定の VRF インスタンスで使用される NAT レート制限の設定 43
例：すべての VRF インスタンスで使用される NAT レート制限の設定 43
例：アクセス コントロール リストで使用される NAT レート制限の設定 43
例：IP アドレスで使用される NAT レート制限の設定 44
次の作業 44

IP アドレス変換用の NAT の設定に関するその他の関連資料 44
IP アドレス節約のための NAT 設定に関する機能情報 45
NAT でのアプリケーション レベル ゲートウェイの使用 49
機能情報の確認 50
NAT でアプリケーション レベル ゲートウェイを使用するための要件 50
NAT でのアプリケーション レベル ゲートウェイの使用について 50
IPSec 50
NAT IPsec 設定の利点 51
IP ネットワークを経由する音声およびマルチメディア 52
H.323 v2 RAS に対する NAT サポート 52
v2 互換モードでの H.323 v3 および v4 に対する NAT サポート 53
NAT H.245 トンネリングのサポート 53
Skinny Client Control Protocol に対する NAT サポート 53
SCCP フラグメンテーションの NAT サポート 54
レイヤ 4 フォワーディングを使った NAT セグメンテーション 54
NAT でのアプリケーション レベル ゲートウェイの設定方法 55
NAT を通じた IPsec の設定 55
NAT を通じた IPsec ESP の設定 55
保持ポートのイネーブル化 56
NAT デバイスでの SPI マッチングのイネーブル化 57
エンドポイントでの SPI マッチングのイネーブル化 59
NAT に対する MultiPart SDP サポートのイネーブル化 60
IP Phone と Cisco CallManager の間での NAT の設定 61
NAT でアプリケーション レベル ゲートウェイを使用する場合の設定例 62
例：NAT 変換用のポートの指定 62
例：保持ポートのイネーブル化 62
例：SPI マッチングのイネーブル化 62
例：エンドポイントでの SPI マッチングのイネーブル化 62
例：NAT に対する MultiPart SDP サポートのイネーブル化 62
例：NAT 変換用のポートの指定 62
次の作業 63
NAT でアプリケーション レベル ゲートウェイを使用する場合のその他の関連資料 63

NAT でアプリケーション レベル ゲートウェイを使用する場合の機能情報 64
キャリア グレード ネットワーク アドレス変換 69
機能情報の確認 69
キャリア グレード ネットワーク アドレス変換の制約事項 70
キャリア グレード ネットワーク アドレス変換について 70
キャリア グレード NAT の概要 70
ブロードバンド アクセス集約のキャリア グレード NAT サポート 71
キャリア グレード ネットワーク アドレス変換の設定方法 72
スタティック キャリア グレード NAT の設定 72
ダイナミック キャリア グレード NAT の設定 75
ダイナミック ポート アドレスのキャリア グレード NAT の設定 78
キャリア グレード ネットワーク アドレス変換の設定例 80
例：スタティック キャリア グレード NAT の設定 80
例：ダイナミック キャリア グレード NAT の設定 81
例：ダイナミック ポート アドレス キャリア グレード NAT の設定 81
キャリア グレード ネットワーク アドレス変換に関するその他の関連資料 81
キャリア グレード ネットワーク アドレス変換の機能情報 82
ハイ アベイラビリティ用 NAT の設定 85
機能情報の確認 85
ハイ アベイラビリティ用 NAT 設定の前提条件 86
ハイ アベイラビリティ用 NAT の制限事項 86
ハイ アベイラビリティ用 NAT の設定について 86
ステートフル NAT 86
Outside-to-Inside 非対称 ALG の NAT ステートフル フェールオーバー サポート 87
HSRP との相互作用 87
変換グループ 87
ARP でのアドレス解決 87
非対称の外部から内部サポート用ステートフル フェールオーバー 88
ALG 用ステートフル フェールオーバー 89
ハイ アベイラビリティ用 NAT の設定方法 90
NAT ステートフル フェールオーバーの設定 90
NAT ステートフル フェールオーバー設定の制約事項 90

HSRP での SNAT の設定 91
プライマリ（アクティブ）ルータでの SNAT の設定 93
バックアップ（スタンバイ）ルータの SNAT の設定 94
非対称の外部から内部および ALG サポート用 NAT ステートフル フェールオーバーの設定 96
非対称の外部から内部および ALG サポート用 NAT ステートフル フェールオーバー機能設定の前提条件 96
HSRP での SNAT の設定 96
SNAT プライマリ バックアップの設定 98
HSRP 用 NAT スタティック マッピング サポートの設定 100
HSRP 用スタティック マッピング サポート設定の制限事項 101
NAT インターフェイスの HSRP イネーブル化 101
次の作業 103
HSRP 環境でスタティック NAT をイネーブル化 103
ハイ アベイラビリティ用の NAT の設定例 104
例：ステートフル NAT の設定 104
非対称の外部から内部および ALG サポート用 NAT ステートフル フェールオーバーの設定例 105
例：HSRP での SNAT の設定 105
例：SNAT プライマリ バックアップの設定 105
例：HSRP 環境のスタティック NAT の設定 106
その他の関連資料 106
ハイ アベイラビリティ用 NAT の設定に関する機能情報 108
ステートフル シャーシ間冗長化の設定 111
機能情報の確認 111
ステートフル シャーシ間冗長化の前提条件 112
ステートフル シャーシ間冗長化の制約事項 112
ステートフル シャーシ間冗長化について 112
ステートフル シャーシ間冗長化の概要 112
ステートフル シャーシ間冗長化の動作 113
ファイアウォールおよび NAT とのアソシエーション 116
LAN/LAN トポロジ 116

ステートフル シャーシ間冗長化の設定方法 117
コントロール インターフェイス プロトコルの設定 117
冗長グループの設定 119
冗長トラフィック インターフェイスの設定 123
ステートフル シャーシ間冗長化による NAT の設定 124
ステートフル シャーシ間冗長化の管理とモニタリング 126
ステートフル シャーシ間冗長化の設定例 128
例：コントロール インターフェイス プロトコルの設定 128
例：冗長グループの設定 128
例：冗長トラフィック インターフェイスの設定 128
例：ステートフル シャーシ間冗長化による NAT の設定 128
その他の関連資料 129
ステートフル シャーシ間冗長化の機能情報 130
ゾーンベースのファイアウォールおよび NAT に対するシャーシ間非対称ルーティング サポート 131
機能情報の確認 132
ゾーンベースのファイアウォールおよび NAT に対するシャーシ間非対称ルーティング サポートの制約事項 132
ゾーンベースのファイアウォールおよび NAT に対するシャーシ間非対称ルーティング サポートについて 132
非対称ルーティングの概要 132
ファイアウォールでの非対称ルーティング サポート 134
NAT の非対称ルーティング 135
WAN-LAN トポロジでの非対称ルーティング 135
ゾーンベースのファイアウォールおよび NAT に対するシャーシ間非対称ルーティング サポートの設定方法 136
冗長アプリケーション グループおよび冗長グループ プロトコルの設定 136
データ、コントロール、および非対称ルーティング インターフェイスの設定 139
インターフェイスでの冗長インターフェイス ID および非対称ルーティングの設定 142
非対称ルーティングを使用したダイナミック内部送信元変換の設定 143

ゾーンベースのファイアウォールおよび NAT に対するシャーシ間非対称ルーティング サポートの設定例 146
例：冗長アプリケーション グループおよび冗長グループ プロトコルの設定 146
例：データ、コントロール、および非対称ルーティング インターフェイスの設定 147
例：インターフェイスでの冗長インターフェイス ID および非対称ルーティングの設定 147
例：非対称ルーティングを使用したダイナミック内部送信元変換の設定 147
ゾーンベースのファイアウォールおよび NAT に対するシャーシ間非対称ルーティング サポートに関するその他の関連資料 148
ゾーンベースのファイアウォールおよび NAT に対するシャーシ間非対称ルーティング サポートの機能情報 149
MPLS VPN と NAT の統合 151
機能情報の確認 151
MPLS VPN と NAT 統合の前提条件 152
MPLS VPN と NAT 統合の制約事項 152
MPLS VPN と NAT の統合について 152
NAT と MPLS VPN との統合の利点 152
NAT と MPLS VPN との統合に関する実装オプション 152
PE ルータ上での NAT 統合のシナリオ 153
NAT と MPLS VPN との統合方法 154
MPLS VPN を使用した内部ダイナミック NAT の設定 154
MPLS VPN を使用した内部スタティック NAT の設定 156
MPLS VPN との外部ダイナミック NAT 設定 158
MPLS VPN との外部スタティック NAT 設定 159
MPLS VPN と NAT 統合の設定例 161
MPLS VPN との内部ダイナミック NAT の設定例 161
MPLS VPN との内部スタティック NAT の設定例 161
MPLS VPN との外部ダイナミック NAT の設定例 162
MPLS VPN との外部スタティック NAT の設定例 162
次の作業 162
MPLS VPN との NAT の統合に関するその他の関連資料 163
MPLS VPN と NAT の統合に関する機能情報 163

NAT のモニタリングおよびメンテナンス 165
機能情報の確認 165
NAT のモニタリングおよびメンテナンスの前提条件 166
NAT のモニタリングおよびメンテナンスの制約事項 166
NAT のモニタリングとメンテナンスについて 166
NAT の表示内容 166
変換エントリ 166
スタティック情報 167
Syslog の使用方法 168
NAT のモニタリング方法とメンテナンス方法 168
NAT 変換情報の表示 168
タイムアウト前の NAT エントリのクリア 170
Syslog での NAT 変換ロギングのイネーブル化 171
NAT のモニタリングおよびメンテナンスの例 172
例：Syslog での NAT 変換ロギングのイネーブル化 172
例：UDP NAT 変換のクリア 173
次の作業 173
NAT のモニタリングおよびメンテナンスに関するその他の関連資料 173
NAT のモニタリングとメンテナンスの機能情報 174
VRF 単位での NAT の High-Speed ロギングのイネーブル化 177
機能情報の確認 177
VRF 単位での NAT の High-Speed ロギングのイネーブル化について 178
NAT の High-Speed ロギング 178
VRF 単位での NAT の High-Speed ロギングのイネーブル化の設定方法 179
NAT 変換の High-Speed ロギングのイネーブル化 179
VRF 単位での NAT の High-Speed ロギングのイネーブル化の設定例 181
例：NAT 変換の High-Speed ロギングのイネーブル化 181
VRF 単位での NAT の High-Speed ロギングのイネーブル化に関するその他の関連資料 181
VRF 単位での NAT の High-Speed ロギングのイネーブル化の機能情報 182
ステートレス ネットワーク アドレス変換 64 183
機能情報の確認 184

ステートレス ネットワーク アドレス変換 64 の制約事項 184
ステートレス ネットワーク アドレス変換 64 について 184
IPv6 と IPv4 ネットワークにおける IP データグラムのフラグメンテーション 184
ステートレス NAT64 変換の ICMP の変換 185
IPv4-Translatable IPv6 アドレス 185
プレフィックス形式 185
サポートされるステートレス NAT64 シナリオ 186
ステートレス NAT64 変換の複数プレフィックス サポート 187
ステートレス ネットワーク アドレス変換 64 の設定方法 187
ステートレス NAT64 通信用のルーティング ネットワークの設定 187
ステートレス NAT64 変換の複数プレフィックスの設定 191
ステートレス NAT64 ルーティング ネットワークのモニタリングおよびメンテナンス 194
ステートレス ネットワーク アドレス変換 64 の設定例 197
ステートレス NAT64 変換のルーティング ネットワークの設定例 197
例：ステートレス NAT64 変換の複数プレフィックスの設定 198
その他の関連資料 198
ステートレス ネットワーク アドレス変換 64 の機能情報 199
用語集 200
ステートフル ネットワーク アドレス変換 64 203
機能情報の確認 203
ステートフル ネットワーク アドレス変換 64 の設定の前提条件 204
ステートフル ネットワーク アドレス変換 64 の設定の制約事項 204
ステートフル ネットワーク アドレス変換 64 について 205
ステートフル ネットワーク アドレス変換 64 205
ステートフル ネットワーク アドレス変換 64 のプレフィックス形式 206
Well Known Prefix 206
ステートフル IPv4-to-IPv6 パケット フロー 206
ステートフル IPv6-to-IPv4 パケット フロー 207
IP パケット フィルタリング 207
ステートフル NAT64 とステートレス NAT64 の違い 208
NAT64 の High-Speed ロギング 209

FTP64 アプリケーション レベル ゲートウェイ サポート 210
FTP64 NAT ALG ボックス内ハイ アベイラビリティ サポート 211
ステートフル NAT64 - シャーシ内冗長化 212
ステートフル ネットワーク アドレス変換 64 の設定方法 213
スタティック ステートフル ネットワーク アドレス変換 64 の設定 213
ダイナミック ステートフル ネットワーク アドレス変換 64 の設定 216
ダイナミック ポート アドレス変換ステートフル NAT64 の設定 220
ステートフル NAT64 ルーティング ネットワークのモニタリングおよびメンテナンス 223
ステートフル ネットワーク アドレス変換 64 の設定例 224
例：スタティック ステートフル ネットワーク アドレス変換 64 の設定 224
例：ダイナミック ステートフル ネットワーク アドレス変換 64 の設定 225
例：ダイナミック ポート アドレス変換ステートフル NAT64 の設定 225
その他の関連資料 226
ステートフル ネットワーク アドレス変換 64 の機能情報 227
用語集 229
ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化 231
機能情報の確認 231
ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化の制約事項 232
ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化について 232
ステートフル シャーシ間冗長化の動作 232
アクティブ/アクティブ フェールオーバー 235
アクティブ/スタンバイ フェールオーバー 236
LAN/LAN トポロジ 236
ステートフル NAT64 の冗長グループ 237
変換フィルタリング 238
FTP64 アプリケーション レベル ゲートウェイ サポート 238
ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化の設定方法 239
冗長グループ プロトコルの設定 239
アクティブ/スタンバイ ロード シェアリング用の冗長グループの設定 241
アクティブ/アクティブ ロード シェアリング用の冗長グループの設定 242

ステートフル NAT64 シャーシ間冗長化用のトラフィック インターフェイスの設定 245
シャーシ間冗長化用のスタティック ステートフル NAT64 の設定 247
ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化の設定例 251
例：冗長グループ プロトコルの設定 251
例：アクティブ/スタンバイ ロード シェアリング用の冗長グループの設定 251
例：アクティブ/アクティブ ロード シェアリング用の冗長グループの設定 251
例：ステートフル NAT64 シャーシ間冗長化用のトラフィック インターフェイスの設定 252
その他の関連資料 252
ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化の機能情報 253
変換を使用したアドレスおよびポートのマッピング 255
機能情報の確認 255
変換を使用したアドレスおよびポートのマッピングの制約事項 256
変換を使用したアドレスおよびポートのマッピングについて 256
変換を使用したアドレスおよびポートのマッピングの概要 256
MAP-T マッピング ルール 257
MAP-T アドレス形式 258
MAP-T カスタマー エッジ デバイスでのパケット転送 258
境界ルータでのパケット転送 259
MAP-T 用の ICMP/ICMPv6 ヘッダー変換 260
MAP-T での Path MTU 検出およびフラグメンテーション 260
変換を使用したアドレスおよびポートのマッピングの設定方法 261
変換を使用したアドレスおよびポートのマッピングの設定 261
変換を使用したアドレスおよびポートのマッピングの設定例 263
例：変換を使用したアドレスおよびポートのマッピングの設定 263
例：MAP-T 展開シナリオ 263
変換を使用したアドレスおよびポートのマッピングに関するその他の関連資料 264
変換を使用したアドレスおよびポートのマッピングの機能情報 265
用語集 266
ファイアウォールおよび NAT 対応の MSRPC ALG サポート 269
ファイアウォールおよび NAT 対応の MSRPC ALG サポートに関する制約事項 269

ファイアウォールおよび NAT 対応の MSRPC AIC サポートに関する制約事項 270
ファイアウォールおよび NAT 対応の MSRPC ALG サポートについて 270
アプリケーション レベル ゲートウェイ 270
MSRPC 270
ファイアウォールでの MSRPC ALG 271
NAT での MSRPC ALG 272
MSRPC ステートフル パーサー 272
ファイアウォールおよび NAT 対応の MSRPC ALG サポートの設定方法 273
レイヤ 4 MSRPC クラス マップおよびポリシー マップの設定 273
ゾーン ペアの設定および MSRPC ポリシー マップの付加 275
ファイアウォールおよび NAT 対応の MSRPC ALG サポートの設定例 276
例：レイヤ 4 MSRPC クラス マップおよびポリシー マップの設定 276
例：ゾーン ペアの設定および MSRPC ポリシー マップの付加 277
ファイアウォールおよび NAT 対応の MSRPC ALG サポートに関するその他の関連資料 277
ファイアウォールおよび NAT 対応の MSRPC ALG サポートの機能情報 278
ファイアウォールおよび NAT 対応の Sun RPC ALG サポート 281
機能情報の確認 281
ファイアウォールおよび NAT 対応の Sun RPC ALG サポートに関する制約事項 282
ファイアウォールおよび NAT 対応の Sun RPC ALG サポートについて 282
アプリケーション レベル ゲートウェイ 282
Sun RPC 283
ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの設定方法 284
Sun RPC ALG 対応のファイアウォールの設定 284
ファイアウォール ポリシー対応のレイヤ 4 クラス マップの設定 284
ファイアウォール ポリシー対応のレイヤ 7 クラス マップの設定 285
Sun RPC ファイアウォール ポリシー マップの設定 286
レイヤ 4 ポリシー マップへのレイヤ 7 ポリシー マップの付加 288
セキュリティ ゾーンとゾーン ペアの作成、およびゾーン ペアへのポリシー マップの付加 289
ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの設定例 293
例：ファイアウォール ポリシー対応のレイヤ 4 クラス マップの設定 293
例：ファイアウォール ポリシー対応のレイヤ 7 クラス マップの設定 293

例：Sun RPC ファイアウォール ポリシー マップの設定 293
例：レイヤ 4 ポリシー マップへのレイヤ 7 ポリシー マップの付加 293
例：セキュリティ ゾーンとゾーン ペアの作成、およびゾーン ペアへのポリシーマップの付加 293
例：Sun RPC ALG 対応のファイアウォールの設定 294
ファイアウォールおよび NAT 対応の Sun RPC ALG サポートに関するその他の関連資料 295
ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの機能情報 296
ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP 297
機能情報の確認 298
ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の制約事項 298
ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP について 298
アプリケーション レベル ゲートウェイ 298
基本 H.323 ALG サポート 299
vTCP for ALG サポートの概要 300
vTCP と NAT およびファイアウォール ALG 300
ハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の概要 300
ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の設定方法 301
NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の設定 301
ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の設定例 304
例：NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の設定 304
ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP に関するその他の関連資料 304
ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の機能情報 305
NAT およびファイアウォールに対する SIP ALG 強化 307

機能情報の確認 308
NAT およびファイアウォールに対する SIP ALG 強化の制約事項 308
NAT およびファイアウォールに対する SIP ALG 強化について 308
SIP の概要 308
アプリケーション レベル ゲートウェイ 309
SIP ALG ローカル データベース管理 309
SIP ALG Via ヘッダーのサポート 310
SIP ALG 方式のロギング サポート 310
SIP ALG PRACK コール フロー サポート 311
SIP ALG Record-Route ヘッダー サポート 311
NAT およびファイアウォールに対する SIP ALG 強化の設定方法 312
SIP に対する NAT サポートのイネーブル化 312
SIP インスペクションのイネーブル化 313
ゾーン ペアの設定および SIP ポリシー マップの付加 315
NAT およびファイアウォールに対する SIP ALG 強化の設定例 317
例：SIP に対する NAT サポートのイネーブル化 317
例：SIP インスペクションのイネーブル化 318
例：ゾーン ペアの設定および SIP ポリシー マップの付加 318
NAT およびファイアウォールに対する SIP ALG 強化に関するその他の関連資料 318
NAT およびファイアウォールに対する SIP ALG 強化の機能情報 319
NAT の Match-in-VRF サポート 321
機能情報の確認 321
NAT の Match-in-VRF サポートの制約事項 322
NAT の Match-in-VRF サポートについて 322
NAT の Match-in-VRF サポート 322
NAT の Match-in-VRF サポートの設定方法 323
スタティック NAT での Match-in-VRF の設定 323
ダイナミック NAT での Match-in-VRF の設定 325
NAT の Match-in-VRF サポートの設定例 327
例：スタティック NAT での Match-in-VRF の設定 327
例：ダイナミック NAT での Match-in-VRF の設定 328
その他の関連資料 328

NAT の Match-in-VRF サポートに関する機能情報 330

IP マルチキャスト ダイナミック NAT 331

機能情報の確認 331

IP マルチキャスト ダイナミック NAT の制約事項 332

IP マルチキャスト ダイナミック NAT について 332

NAT の機能 332

NAT の用途 332

NAT の内部アドレスおよび外部アドレス 333

アドレスのダイナミック変換 333

IP マルチキャスト ダイナミック NAT の設定方法 334

IP マルチキャスト ダイナミック NAT の設定 334

IP マルチキャスト ダイナミックな NAT の設定例 337

例：IP マルチキャスト ダイナミック NAT の設定 337

その他の関連資料 337

IP マルチキャスト ダイナミック NAT の機能情報 338

NAT での Paired-Address-Pooling サポート 341

機能情報の確認 341

NAT での Paired-Address-Pooling サポートの制約事項 342

NAT での Paired-Address-Pooling サポートについて 342

Paired-Address-Pooling サポートの概要 342

NAT での Paired-Address-Pooling サポートの設定方法 343

NAT での Paired-Address-Pooling サポートの設定 343

NAT での Paired-Address-Pooling サポートの設定例 345

例：NAT での Paired-Address-Pooling サポートの設定 345

NAT での Paired-Address-Pooling サポートに関するその他の関連資料 346

NAT での Paired-Address-Pooling サポートの機能情報 346

PPTP ポート アドレス変換 349

機能情報の確認 349

PPTP ポート アドレス変換の制約事項 350

PPTP ポート アドレス変換について 350

PPTP ALG サポートの概要 350

PPTP ポート アドレス変換の設定方法 351

ポート アドレス変換用の PPTP ALG の設定 **351**
PPTP ポート アドレス変換の設定例 **353**
例：ポート アドレス変換用の PPTP ALG の設定 **353**
PPTP ポート アドレス変換に関するその他の関連資料 **353**
PPTP ポート アドレス変換の機能情報 **354**

第 1 章

IP アドレス節約のための NAT 設定

このモジュールでは、IP アドレス節約のためにネットワーク アドレス変換（NAT）を設定し、内部および外部送信元アドレスを設定する方法について説明します。 このモジュールでは、IP アドレス節約のために NAT を設定することの利点についても説明します。

NAT では、未登録の IP アドレスを使用するプライベート IP インターネットワークがインターネットに接続できます。 NAT はルータ（通常、2 つのネットワークを接続するもの）で動作し、パケットを別のネットワークに転送する前に、社内ネットワークの（グローバルに一意のアドレスではなく）プライベート アドレスを正規のアドレスに変換します。 NAT は、ネットワーク全体の 1 つだけのアドレスを外部にアドバタイズするように設定できます。 この機能により、そのアドレスの後ろに内部ネットワーク全体を効果的に隠すことで、セキュリティが強化されます。

NAT は、エンタープライズ エッジでも使用され、内部ユーザのインターネットへのアクセスを許可し、メール サーバなど内部デバイスへのインターネット アクセスを許可します。

- 機能情報の確認，2 ページ
- IP アドレス節約のための NAT 設定に関する前提条件，2 ページ
- IP アドレス節約のための NAT 設定に関する制約事項，3 ページ
- IP アドレス節約のための NAT 設定について，4 ページ
- IP アドレス節約のために NAT を設定する方法，12 ページ
- IP アドレス節約のための NAT 設定例，39 ページ
- 次の作業，44 ページ
- IP アドレス変換用の NAT の設定に関するその他の関連資料，44 ページ
- IP アドレス節約のための NAT 設定に関する機能情報，45 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

IP アドレス節約のための NAT 設定に関する前提条件

アクセス リスト

このモジュールの設定作業で使用する必要のあるアクセス リストはすべて、設定作業を開始する前に設定しておく必要があります。 アクセス リストの設定方法の詳細については、『*IP Access List Sequence Numbering*』マニュアルを参照してください。

（注） NAT コマンドで使用するアクセス リストが指定されている場合、NAT は一般的によく使用される **permit ip any any** コマンドを、アクセス リストでサポートしません。

NAT 要件

ネットワークで NAT を設定する前に、NAT が設定されるインターフェイスおよびその目的を把握しておく必要があります。 次の要件を使用して、NAT の設定方法と使用方法を決定します。

- 次の場合に、NAT の内部および外部インターフェイスを定義します。
  - ユーザが属するインターフェイスが複数ある場合。
  - 複数のインターフェイスがインターネットに接続する場合。
- NAT により実行される必要がある操作を定義します。
  - 内部ユーザのインターネットへのアクセスを許可します。
  - インターネットがメールサーバなどの内部デバイスにアクセスすることを許可します。
  - オーバーラップするネットワークに通信を許可します。
  - 異なるアドレス方式を使用しているネットワークに通信を許可します。

- アプリケーション レベル ゲートウェイの使用を許可します。
- TCP トラフィックを別の TCP ポートまたはアドレスにリダイレクトします。
- ネットワーク移行時に NAT を使用します。

IP アドレス節約のための NAT 設定に関する制約事項

- インターフェイスでネットワーク アドレス変換（NAT）を設定すると、そのインターフェイスは、NAT のパケット フローに対して最適化されます。 NAT インターフェイスを通過する未変換パケットはすべて、そのパケットを変換する必要があるかどうかを決定する一連のチェックを受けます。 これらのチェックにより未変換パケット フローの遅延が増大するため、NAT インターフェイスを通過するすべてのパケットのパケット処理遅延に悪影響が生じます。 NAT インターフェイスは、NAT 専用トラフィックにのみ使用することを強く推奨します。 非 NAT パケットは分離する必要があり、これらのパケットは NAT が設定されていないインターフェイスを通過する必要があります。 非NAT トラフィックの分離には、ポリシー ベース ルーティング（PBR）を使用できます。
- NAT 仮想インターフェイス（NVI）は、Cisco IOS XE ソフトウェアではサポートされていません。
- スタブ ドメインにある多数のホストが、そのドメイン外との通信を行う場合、NAT は実用的ではありません。
- アプリケーションの中には、NAT デバイスにより変換できないような方法で、埋め込み IP アドレスを使用しているものがあります。 このようなアプリケーションは、NAT デバイスを使用しても透過的に、またはまったく機能しません。
- デフォルトでは、Session Initiation Protocol（SIP）のサポートはポート 5060 でイネーブルになっています。 したがって、NAT 対応デバイスはこのポートのパケットをすべて、SIP コール メッセージと解釈します。 同じシステムにある別のアプリケーションがポート 5060 を使用してパケットを送信している場合、NAT サービスはこのパケットを SIP コール メッセージとして解釈しようとするため、このパケットが破損する可能性があります。
- NAT はホストの素性を隠しますが、これは目的によっては、長所でもありますし、短所でもあります。
- NAT が設定されているデバイスは、ローカル ネットワークを外部にアドバタイズしない必要があります。 しかし、NAT が外部から受け取るルーティング情報は、通常どおり、スタブ ドメインにアドバタイズできます。
- NAT コマンドで使用するアクセス リストが指定されている場合、NAT は一般的によく使用される **permit ip any any** コマンドを、このアクセス リストではサポートしません。
- ポート範囲が指定されたアクセス リストは、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータではサポートされません。
- NAT の設定は Intelligent Services Gateway（ISG）のアクセス側ではサポートされません。

- デバイスの物理インターフェイスアドレスを、アドレスプールとして使用することはサポートされません。 NAT で、デバイスの物理インターフェイス アドレスを共有するには、NAT インターフェイスのオーバーロード設定を使用する必要があります。デバイスでは物理インターフェイス ポートを使用し、NAT では変換のために安全に使用できるポートに関する通信を受け取る必要があります。 この通信は、NAT インターフェイスのオーバーロードが設定されている場合にのみ行われます。
- ユーザが設定したすべての IP アドレス プールおよび NAT マッピングに関する情報が、**show ip nat statistics** コマンドの出力に表示されます。 NAT 設定に多数の IP アドレス プールおよび NAT マッピング（たとえば、1000 ～ 4000）がある場合、**show ip nat statistics** でのプールおよびマッピング統計の更新速度が非常に遅くなります。

IP アドレス節約のための NAT 設定について

IP アドレス節約のために NAT を設定する利点

組織が NAT を使用すると、既存のネットワークを持っていてインターネットにアクセスする必要がある場合に、IP アドレスが枯渇する問題を解決できます。 Network Information Center（NIC）登録 IP アドレスをまだ持っていないサイトはこのアドレスを取得する必要があります。また、255 以上のクライアントが存在する、または計画されている場合、Class B アドレスの不足が深刻な問題になります。 Cisco IOS XE NAT はこのような問題に対応するために、隠された数千の内部アドレスを、取得の容易な Class C アドレスの範囲にマップします。

内部ネットワークのクライアントのために IP アドレスをすでに登録しているサイトでも、ハッカーがクライアントを直接攻撃できないように、これらのアドレスをインターネットからは確認できないようにすることができます。クライアントアドレスを隠すことにより、セキュリティがさらに強化されます。 Cisco IOS XE NAT では、LAN 管理者は、インターネット割り当て番号局の予備プールを利用した Class A アドレスを自由に拡張することができます（RFC 1597）。 この拡張は組織内で行われます。LAN/インターネットインターフェイスでのアドレス変更を気にする必要はありません。

Cisco IOS XE ソフトウェアは、選択的またはダイナミックに NAT を実行できます。 この柔軟性のおかげで、ネットワーク管理者は、RFC 1597 および RFC 1918 アドレスまたは登録済みアドレスを混在させて使用できます。 NAT は、IP アドレスの簡略化や節約のためにさまざまなルータ上で使用できるように設計されています。 また、Cisco IOS XE NAT では、NAT に使用できる内部ホストを選択することもできます。

NAT には、NAT が設定されるルータを除き、ホストやルータを変更しなくても設定できるという大きな利点があります。

インターネットは、IP アドレス空間の枯渇とルーティングの拡大という 2 つの大きな問題に直面しています。 NAT は、組織の IP ネットワークを外部から見たときに、実際に使用されているものとは異なる IP アドレス空間が使用されているように見せる機能です。 したがって、NAT を使用すると、グローバルなルーティングが不可能なアドレスを持つ組織は、そのアドレスをグローバルにルーティング可能なアドレス空間に変換して、インターネットに接続できるようになりま

す。また、サービスプロバイダーの変更や、クラスレスドメイン間ルーティング（CIDR）ブロックへの自発的な再番号割り当てを行う組織は、NAT を使用して、適切に番号を割り当て直せるようになります。 NAT は RFC 1631 に記述されています。

NAT の機能

NAT が設定されたルータには、少なくとも内部ネットワークに対して 1 つ、外部ネットワークに対して 1 つのインターフェイスがあります。 標準的な環境では、NAT はスタブ ドメインとバックボーンの間の出口ルータに設定されます。 パケットがドメインから出て行くとき、NAT はローカルで意味のある送信元アドレスをグローバルで一意のアドレスに変換します。 パケットがドメインに入ってくるときは、NAT はグローバルで一意の宛先アドレスをローカルアドレスに変換します。 出力点が複数存在する場合、個々の NAT は同一の変換テーブルを持っていなければなりません。 アドレスが足りなくなって、パケットにアドレスを割り当てられなくなった場合、NAT はそのパケットをドロップし、インターネット制御メッセージプロトコル（ICMP）ホスト到達不能パケットを宛先に送信します。

NAT の用途

NAT は次のような場合に使用できます。

- インターネットに接続する必要はあるが、ホストのすべてがグローバルに一意の IP アドレスを持っているわけではない場合。 NAT では、未登録の IP アドレスを使用するプライベート IP インターネットワークがインターネットに接続できます。 NAT はスタブ ドメイン（内部ネットワーク）と、インターネットなどのパブリック ネットワーク（外部ネットワーク）との境界にあるルータ上に設定されます。 NAT はパケットを外部ネットワークに送信する前に、内部のローカル アドレスをグローバルに一意の IP アドレスに変換します。 接続性の問題への解決策として NAT が役立つのは、スタブ ドメイン内の比較的少数のホストが同時にドメインの外部と通信する場合のみです。 この場合、外部との通信が必要なときに、このドメインにある IP アドレスのごく一部をグローバルに一意な IP アドレスに変換する必要があります。また、これらのアドレスは使用されなくなったときに、再利用することもできます。
- 内部アドレスを変更する必要がある場合。 内部アドレスの変更には相当の工数がかかるため、変更する代わりに NAT を使用して変換することができます。
- TCP トラフィックの基本負荷を分散する必要がある場合。 TCP 負荷分散機能を使用して、1 つのグローバル IP アドレスを複数のローカル IP アドレスにマップできます。

NAT の内部アドレスおよび外部アドレス

NAT のコンテキスト内で使用される内部という用語は、変換する必要がある、組織が所有するネットワークを表します。 NAT が設定されている場合、このネットワーク内のホストは 1 つの空間に複数のアドレスを持ちます（ローカル アドレス空間と呼ばれます）。これらは、ネットワー

ク外のホストに対して別の空間に存在するものとして示されます（グローバル アドレス空間と呼ばれます）。

同様に、外部という用語はスタブ ネットワークの接続先で、通常、その組織の制御下にはないネットワークを表します。 外部ネットワーク内のホストを変換の対象にすることもできるため、これらのホストもローカル アドレスとグローバル アドレスを持つことができます。

NAT では、次の定義が使用されます。

- 内部ローカル アドレス：内部ネットワーク上のホストに割り当てられた IP アドレス。 このアドレスは、多くの場合、NIC やサービス プロバイダーにより割り当てられた正規の IP アドレスではありません。
- 内部グローバル アドレス：外部に向けて、1 つ以上の内部ローカル IP アドレスを表現した正規の IP アドレス（NIC またはサービス プロバイダーにより割り当てられたもの）。
- 外部ローカル アドレス：内部ネットワークから見た外部ホストの IP アドレス。 必ずしも正規のアドレスではありません。内部でルート可能なアドレス空間から割り当てられたものです。
- 外部グローバル アドレス：外部ネットワークに存在するホストに対して、ホストの所有者により割り当てられた IP アドレス。 このアドレスは、グローバルにルート可能なアドレス、またはネットワーク空間から割り当てられます。

ここでは、次の内容について説明します。

内部送信元アドレス変換

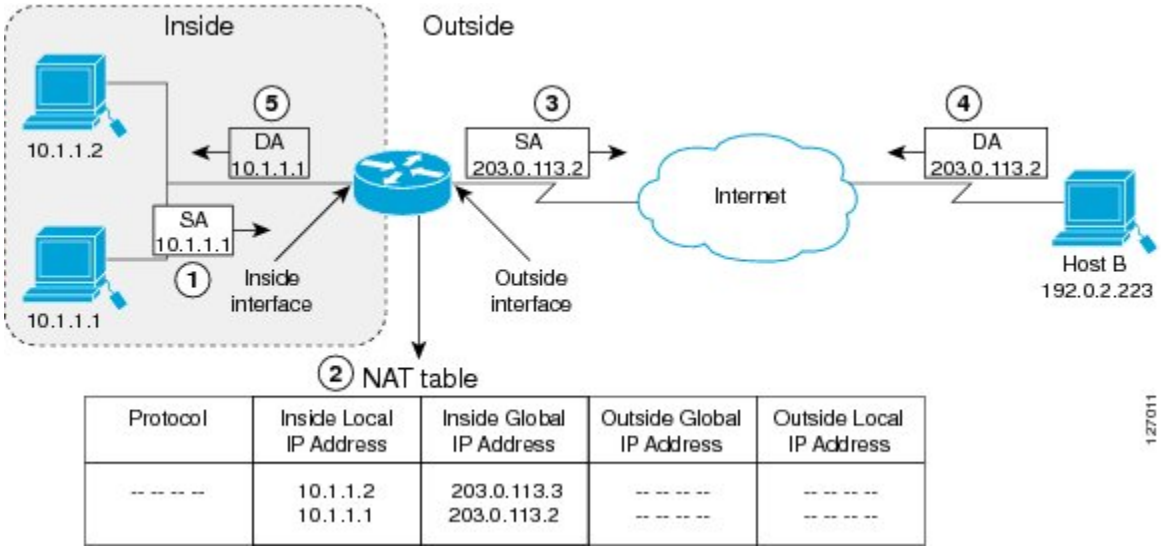
自分が属するネットワークの外部と通信するときに、自分の IP アドレスをグローバルに一意な IP アドレスに変換することができます。 スタティックまたはダイナミック内部送信元変換は、次のようにして設定できます。

- スタティック変換は、内部ローカル アドレスと内部グローバル アドレスの間に 1 対 1 のマッピングを設定します。 外部から固定アドレスを使って内部のホストにアクセスする必要がある場合には、スタティック変換が便利です。
- ダイナミック変換は、内部ローカル アドレスとグローバル アドレスのプールの間にマッピングを設定します。

Cisco IOS Release 15.1(3)T 以降のリリースでは、**traceroute** コマンドを設定すると、NAT により、すべての内部ローカル IP アドレスに対して同じ内部グローバル IP アドレスが返されます。

以下の図は、ネットワーク内部の送信元アドレスを、ネットワーク外部の送信元アドレスに変換するルータを表したものです。

図 *1*：*NAT* 内部送信元変換



次のプロセスでは、上の図に示した、内部送信元アドレス変換を説明しています。

1. ホスト 10.1.1.1 のユーザは外部ネットワークのホスト B への接続を開きます。
2. ルータでは、ホスト 10.1.1.1 から受信する最初のパケットによって、NAT テーブルをチェックします。NAT の設定に応じて、次のシナリオが考えられます。
   - スタティック変換エントリが設定されていた場合、ルータはステップ 3 に進みます。
   - 変換エントリが存在しない場合、ルータは送信元アドレス（SA）の 10.1.1.1 のダイナミック変換が必要であると判断し、ダイナミック アドレス プールから正規のグローバル アドレスを選択し、NAT テーブルに変換エントリを作成します。 このタイプの変換エントリは、単純エントリと呼ばれます。
3. ルータはホスト 10.1.1.1 の内部ローカル送信元アドレスを、この変換エントリのグローバル アドレスで置き換え、パケットを転送します。
4. ホスト B では、このパケットを受信し、内部グローバル IP 宛先アドレス（DA）の 203.0.113.2 を使用してホスト 10.1.1.1 に応答します。
5. 内部グローバル IP アドレスを持つパケットを受信したルータは、内部グローバル アドレスをキーに使用して、NAT テーブル検索を行います。 その後、このアドレスをホスト 10.1.1.1 の内部ローカル アドレスに変換し、パケットをホスト 10.1.1.1 に転送します。

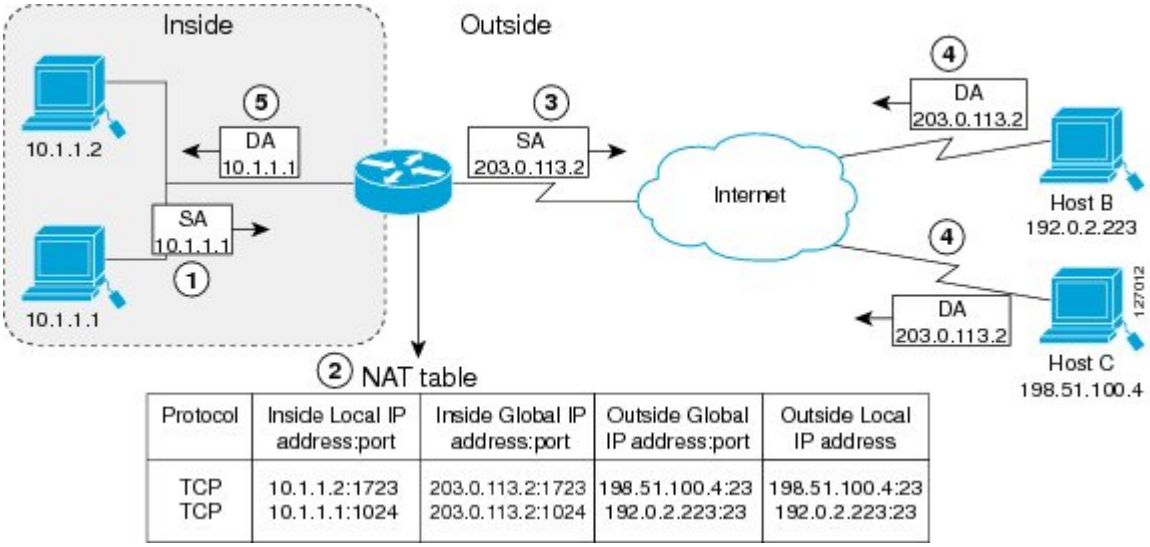
ホスト 10.1.1.1 はパケットを受信し、会話を続けます。 ルータは、受信パケットごとに、ステップ 2 ～ 5 を実行します。

内部グローバル アドレスのオーバーロード

ルータで多数のローカル アドレスに対して 1 つのグローバル アドレスを使用できるようにすることで、内部グローバル アドレス プールのアドレスを節約できます。このタイプの NAT 設定をオーバーロードと呼びます。 オーバーロードを設定すると、ルータではグローバル アドレスを適切なローカル アドレスに逆変換するために十分な、高レベル プロトコルからの情報（TCP ポート番号や UDP ポート番号など）が保持されます。 複数のローカル アドレスが 1 つのグローバル アドレスにマッピングされる場合、各内部ホストの TCP または UDP ポート番号によりローカル アドレスが区別されます。

以下の図は、内部グローバル アドレスが複数の内部ローカル アドレスを表す場合の NAT 操作を示します。 区別は、TCP ポート番号により行われます。

図 *2*：内部グローバル アドレスをオーバーロードする *NAT*



Protocol	Inside Local IP address:port	Inside Global IP address:port	Outside Global IP address:port	Outside Local IP address
TCP	10.1.1.2:1723	203.0.113.2:1723	198.51.100.4:23	198.51.100.4:23
TCP	10.1.1.1:1024	203.0.113.2:1024	192.0.2.223:23	192.0.2.223:23

上記の図に示すとおり、ルータは内部グローバル アドレスのオーバーロードにおいて次のプロセスを実行します。 ホスト B およびホスト C はいずれも、アドレス 203.0.113.2 にある 1 つのホストと通信していると信じています。 しかし、実際には、異なるホストと通信しています。区別にはポート番号が使用されます。 つまり、多数の内部ホストは、複数のポート番号を使用して、内部グローバル IP アドレスを共有することができます。

1. ホスト 10.1.1.1 のユーザはホスト B との接続を開きます。
2. ルータでは、ホスト 10.1.1.1 から受信する最初のパケットによって NAT テーブルをチェックします。NAT 設定に応じて、次のシナリオが考えられます。
   - 変換エントリが存在しない場合、ルータはアドレス 10.1.1.1 の変換が必要であると判断し、内部ローカル アドレス 10.1.1.1 から正式なグローバル アドレスへの変換をセットアップします。
   - オーバーロードがイネーブルで、別の変換がアクティブな場合、ルータではその変換のグローバル アドレスを再利用し、グローバル アドレスを逆変換するために使用できる十分

な情報を NAT テーブルのエントリとして保存します。 このタイプの変換エントリは、拡張エントリと呼ばれます。

3 ルータは内部ローカル送信元アドレス 10.1.1.1 を、選択されたグローバル アドレスで置き換え、パケットを転送します。

4 ホスト B はこのパケットを受信し、内部グローバル IP アドレス 203.0.113.2 を使用して、ホスト 10.1.1.1 に応答します。

5 ルータは、この内部グローバル IP アドレスを持つパケットを受信すると、このプロトコル、内部グローバル アドレスとポート、および外部アドレスとポートをキーとして使用して NAT テーブル検索を実行します。その後、このアドレスを内部ローカル アドレス 10.1.1.1 に変換し、パケットをホスト 10.1.1.1 に転送します。

ホスト 10.1.1.1 はパケットを受信し、会話を続けます。 ルータは、受信パケットごとに、ステップ 2 ～ 5 を実行します。

NAT のタイプ

NAT はルータ（通常、2 つのネットワークを接続するもの）で動作し、パケットが別のネットワークに転送される前に、内部ネットワークのプライベート（内部ローカル）アドレスをパブリック（内部グローバル）アドレスに変換します。 この機能により、ネットワーク全体を表す 1 つのアドレスのみを外部にアドバタイズするように NAT を設定できるようになります。 これにより、内部ネットワークを外部から効果的に隠すことができるため、セキュリティがさらに強化されます。

NAT のタイプは次のとおりです。

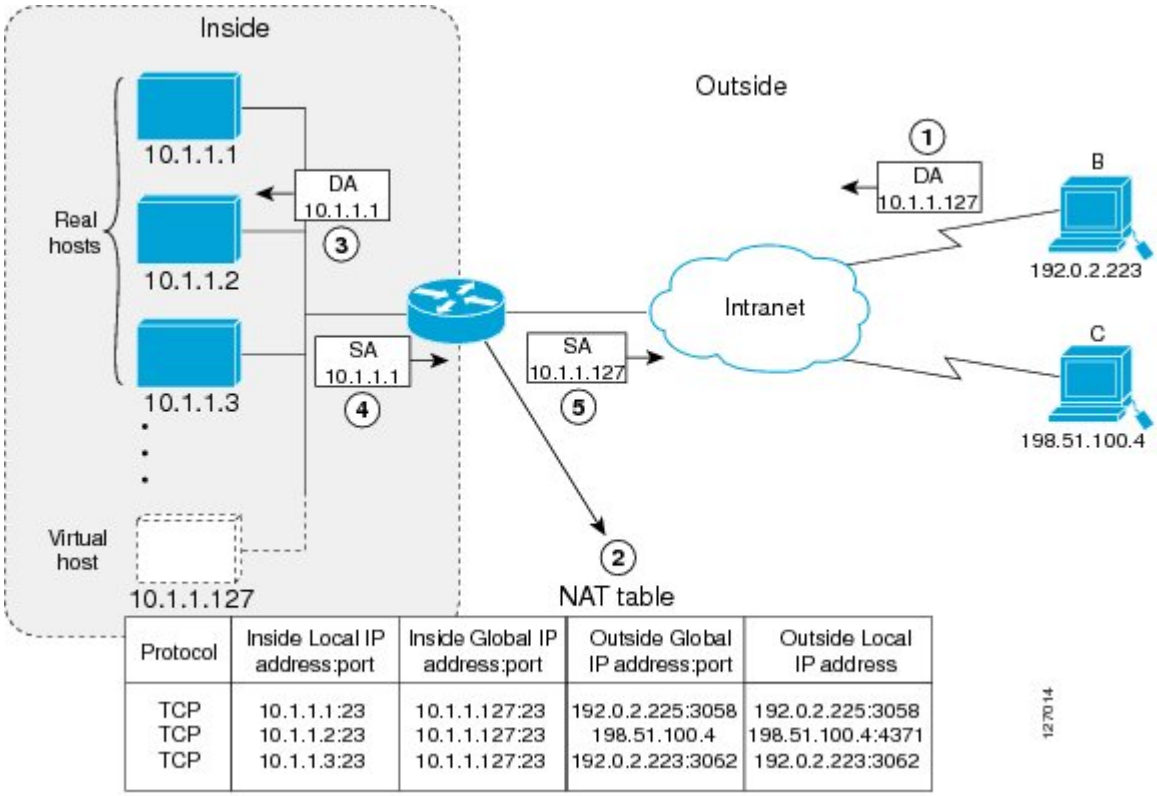
- スタティック アドレス変換（スタティック NAT）：ローカル アドレスとグローバル アドレスを 1 対 1 でマッピングできます。
- ダイナミック アドレス変換（ダイナミック NAT）：未登録の IP アドレスを、登録済み IP アドレスのプールから取得した登録済み IP アドレスにマッピングします。
- オーバーロード：複数の未登録 IP アドレスを、複数の異なるポートを使用して、1 つの登録済み IP アドレスにマッピングします（多対 1）。 この方法は、ポート アドレス変換（PAT）とも呼ばれます。 オーバーロードを使用することにより、使用できる正規のグローバル IP アドレスが 1 つのみでも、数千のユーザをインターネットに接続することができます。

NAT における TCP 負荷分散

組織の中には、使用頻度の高いホストとの通信を必要とするホストが複数存在することがあります。 NAT を使用して、複数の実ホストの間でのロード シェアリングを調整する仮想ホストを内部ネットワークに設定することができます。 アクセス リストと一致する DA はロータリー プールからのアドレスで置き換えられます。 割り当ては外部から内部への新しい接続が開かれた場合の

み、ラウンドロビンベースで行われます。TCP ではないトラフィックは、（その他の変換が有効化されていない限り）変換されずに通されます。 以下の図に、この機能を示します。

図 *3*：*NAT TCP* 負荷分散



Protocol	Inside Local IP address:port	Inside Global IP address:port	Outside Global IP address:port	Outside Local IP address
TCP	10.1.1.1:23	10.1.1.127:23	192.0.2.225:3058	192.0.2.225:3058
TCP	10.1.1.2:23	10.1.1.127:23	198.51.100.4	198.51.100.4:4371
TCP	10.1.1.3:23	10.1.1.127:23	192.0.2.223:3062	192.0.2.223:3062

ルータは、ロータリー アドレスを変換するときに次のプロセスを実行します。

1. ホスト B（192.0.2.223）のユーザが、10.1.1.127 にある仮想ホストへの接続を開きます。
2. ルータは接続要求を受信し、新しい変換を作成して、内部ローカル IP アドレスに、その次の実ホスト（10.1.1.1）を割り当てます。
3. ルータは宛先アドレスを、選択された実ホストのアドレスで置き換え、パケットを転送します。
4. ホスト 10.1.1.1 はこのパケットを受信し、応答します。
5. ルータはこのパケットを受信し、内部ローカルアドレスとポート番号、および外部アドレスとポート番号をキーに使用して、NAT テーブルを検索します。 次に、ルータは送信元アドレスを仮想ホストのアドレスに変換し、パケットを転送します。
6. 次回、接続が要求されると、ルータは内部ローカル アドレスに 10.1.1.2 を割り当てます。

スタティック IP アドレスのサポート

パブリック ワイヤレス LAN は、モバイル コンピューティング デバイスのユーザに、インターネットなどのパブリック ネットワークへのワイヤレス接続を提供します。

NAT スタティック IP アドレス サポート機能は、スタティック IP アドレスを使用して設定されているユーザをサポートするために、パブリック ワイヤレス LAN プロバイダーの機能を拡張するものです。スタティック IP アドレスを持つユーザをサポートするようにルータを設定すると、パブリック ワイヤレス LAN プロバイダーのサービスが多数の潜在的ユーザに広がるため、ユーザ満足度が高まり、収益の増加につながります。

スタティック IP アドレスを持つユーザは IP アドレスを変更しなくても、パブリック ワイヤレス LAN プロバイダーのサービスを使用できます。 スタティック IP クライアント用の NAT エントリが作成され、ルーティング可能なアドレスが提供されます。

RADIUS

RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。 ネットワーク アクセス サーバ（NAS）と RADIUS サーバとの通信は、UDP に基づいて行われます。 一般に、RADIUS プロトコルはコネクションレス型サービスと見なされます。 サーバのアベイラビリティ、再送信、タイムアウトに関する問題は、伝送プロトコルではなく、RADIUS 対応デバイスにより処理されます。

RADIUS はクライアント/サーバプロトコルです。通常、RADIUS クライアントは NAS で、RADIUS サーバは UNIX または Windows NT マシンで実行されているデーモン プロセスです。 クライアントは指定された RADIUS サーバにユーザ情報を渡し、返された応答に応じた動作をします。 RADIUS サーバは、ユーザ接続要求を受信し、ユーザを認証してから、このユーザへのサービス提供にクライアントが必要とする設定情報を返します。 RADIUS サーバは、他の RADIUS サーバや、他の種類の認証サーバに対するプロキシ クライアントとして動作します。

サービス拒絶攻撃

サービス拒絶（DoS）攻撃では、通常、ルータや Web サーバなどのターゲットを過負荷にし、機能しないようにする目的で標準プロトコルや接続プロセスが乱用されます。 DoS 攻撃は、悪意のあるユーザや、ウイルスまたはワームに感染したコンピュータから仕掛けられます。 多数のコンピュータがウイルスやワームに感染した場合などに起こる、一度に多数の場所からの攻撃は分散型 DoS 攻撃と呼ばれます。 このような分散型 DoS 攻撃は急速に広がり、数千に及ぶシステムを巻き込みます。

NAT を標的にするウイルスおよびワーム

ウイルスやワームはコンピュータやネットワーク機器を攻撃するために設計された悪意のあるプログラムです。 ウイルスは通常、個々のアプリケーションに埋め込まれていて、実行されたときにのみ動作しますが、ワームは自己増殖し、自力ですばやく伝染していくことができます。 特定

のウイルスやワームが明示的に NAT をターゲットにできない可能性がありますが、NAT リソースを使用して、自身を増殖させる可能性はあります。 NAT 変換のレート制限機能は、特定のホストやアクセス コントロール リスト、VPN ルーティングおよび転送（VRF）インスタンスを発生源とするウイルスやワームの影響を制限するために使用できます。

IP アドレス節約のために NAT を設定する方法

このセクションで説明する作業では、IP アドレス節約のために NAT を設定します。 このセクションに必須の作業は含まれていませんが、これらの作業のうち、少なくとも 1 つを実行する必要があります。 複数のタスクの実行が必要となる場合があります。

内部送信元アドレスの設定

スタティックまたはダイナミック変換のために内部送信元アドレスを設定できます。 要件に応じて、次の作業のいずれか 1 つを行います。

内部送信元アドレスのスタティック変換の設定

内部ローカル アドレスと内部グローバル アドレスとの間で 1 対 1 マッピングを可能にするには、内部送信元アドレスのスタティック変換を設定します。 外部から固定アドレスを使って内部のホストにアクセスする必要がある場合には、スタティック変換が便利です。

CSCtl04702 の修正を適用していると、スタティック内部送信元アドレスが内部グローバルアドレスに一致した場合に、**show ip aliases** コマンドの出力に両方のアドレスが表示されます。 スタティック内部送信元アドレスはインターフェイスアドレスとして表示され、内部グローバルアドレスはダイナミック アドレスとして表示されます。 修正の適用前に、スタティック内部送信元アドレスが内部グローバルアドレスに一致した場合、**show ip aliases** コマンドの出力にはスタティック内部送信元アドレスのみが表示されます。

（注） NAT が設定されているインターフェイスおよび **ip nat inside source static** コマンドを使用して設定されている内部アドレスには、異なる IP アドレスを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat inside source static** *local-ip global-ip*
4. **interface** *type number*
5. **ip address** *ip-address mask* [**secondary**]
6. **ip nat inside**
7. **exit**
8. **interface** *type number*
9. **ip address** *ip-address mask* [**secondary**]
10. **ip nat outside**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat inside source static** *local-ip global-ip* 例： `Device(config)# ip nat inside source static 10.10.10.1 172.16.131.1`	内部ローカル アドレスと内部グローバル アドレスとの間のスタティック変換を設定します。
ステップ 4	**interface** *type number* 例： `Device(config)# interface ethernet 1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip address** *ip-address mask* [**secondary**] 例： `Device(config-if)# ip address 10.114.11.39 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 6	**ip nat inside** 例： `Device(config-if)# ip nat inside`	内部と接続されることを示すマークをインターフェイスに付けます。
ステップ 7	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *type number* 例： `Device(config)# interface ethernet 0`	異なるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ip address** *ip-address mask* [**secondary**] 例： `Device(config-if)# ip address 172.31.232.182 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 10	**ip nat outside** 例： `Device(config-if)# ip nat outside`	外部と接続されることを示すマークをインターフェイスに付けます。
ステップ 11	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

内部送信元アドレスのダイナミック変換の設定

ダイナミック変換は、内部ローカルアドレスとグローバルアドレスのプールの間にマッピングを設定します。プライベート ネットワークに存在する複数のユーザがインターネットへのアクセスを必要としている場合には、ダイナミック変換が便利です。ダイナミックに設定されたプール IP アドレスは、必要に応じて使用し、インターネットへのアクセスが必要なくなったときにはリリースして別のユーザが使用できるようにすることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
4. **access-list** *access-list-number* **permit** *source* [*source-wildcard*]
5. **ip nat inside source list** *access-list-number* **pool** *name*
6. **interface** *type number*
7. **ip address** *ip-address mask*
8. **ip nat inside**
9. **exit**
10. **interface** *type number*
11. **ip address** *ip-address mask*
12. **ip nat outside**
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask*	**prefix-length** *prefix-length*} 例： `Device(config)# ip nat pool net-208 172.16.233.208 172.16.233.223 prefix-length 28`	必要に応じて割り当てられるグローバル アドレスのプールを定義します。
ステップ 4	**access-list** *access-list-number* **permit** *source* [*source-wildcard*] 例： `Device(config)# access-list 1 permit 192.168.34.0 0.0.0.255`	変換されるアドレスを許可する標準アクセス リストを定義します。

	コマンドまたはアクション	目的
ステップ 5	**ip nat inside source list** *access-list-number* **pool** *name* 例： `Device(config)# ip nat inside source list 1 pool net-208`	直前の手順で定義されたアクセス リストを指定して、ダイナミック送信元変換を設定します。
ステップ 6	**interface** *type number* 例： `Device(config)# interface ethernet 1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.114.11.39 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 8	**ip nat inside** 例： `Device(config-if)# ip nat inside`	内部と接続されることを示すマークをインターフェイスに付けます。
ステップ 9	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface ethernet 0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 172.16.232.182 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 12	**ip nat outside** 例： `Device(config-if)# ip nat outside`	外部と接続されることを示すマークをインターフェイスに付けます。
ステップ 13	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

NAT を使用した内部ユーザのインターネットへのアクセスの許可

グローバル アドレスのオーバーロードを使用して、内部ユーザにインターネットへのアクセスを許可し、内部グローバル アドレス プールのアドレスを節約するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
4. **access-list** *access-list-number* **permit** *source* [*source-wildcard*]
5. **ip nat inside source list** *access-list-number* **pool** *name* **overload**
6. **interface** *type number*
7. **ip address** *ip-address mask*
8. **ip nat inside**
9. **exit**
10. **interface** *type number*
11. **ip address** *ip-address mask*
12. **ip nat outside**
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} 例： `Device(config)# ip nat pool net-208 192.168.202.129 192.168.202.158 netmask 255.255.255.224`	必要に応じて割り当てられるグローバルアドレスのプールを定義します。

	コマンドまたはアクション	目的
ステップ 4	**access-list** *access-list-number* **permit** *source* [*source-wildcard*] 例： `Device(config)# access-list 1 permit 192.168.201.30 0.0.0.255`	変換されるアドレスを許可する標準アクセス リストを定義します。 • アクセス リストは、変換されるアドレスだけを許可する必要があります（各アクセスリストの最後には暗黙的な「deny all」があるので注意してください）。アクセス リストでアドレスを許可しすぎると、予期しない結果になる可能性があります。
ステップ 5	**ip nat inside source list** *access-list-number* **pool** *name* **overload** 例： `Device(config)# ip nat inside source list 1 pool net-208 overload`	ステップ 4 で定義されたアクセス リストを指定して、オーバーロードを使ったダイナミック送信元変換を設定します。
ステップ 6	**interface** *type number* 例： `Device(config)# interface ethernet 1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.168.201.1 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 8	**ip nat inside** 例： `Device(config-if)# ip nat inside`	内部と接続されることを示すマークをインターフェイスに付けます。
ステップ 9	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface ethernet 0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.168.201.29 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 12	**ip nat outside** 例： `Device(config-if)# ip nat outside`	外部と接続されることを示すマークをインターフェイスに付けます。
ステップ 13	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

アドレス変換タイムアウトの設定

ユーザ独自の NAT の設定に基づいてアドレス変換のタイムアウトを設定できます。

変換タイムアウトの変更

デフォルトでは、ダイナミック アドレス変換は一定の期間使用されていないとタイムアウトします。必要に応じて、タイムアウトのデフォルト値を変更できます。オーバーロードが設定されていない場合、単純な変換エントリは 24 時間後にタイムアウトします。 オーバーロードを使用しないダイナミック アドレス変換用にタイムアウト値を変更するように **ip nat translation timeout** *seconds* コマンドを設定します。

オーバーロードが設定されている場合のタイムアウトの変更

オーバーロードを設定した場合、変換エントリのタイムアウトを制御できるようになります。これは個々の変換エントリに、そのエントリを使用するトラフィックに関する詳しいコンテキストが含まれているからです。

設定に基づいて、この項で説明されているタイムアウトを変更できます。 ダイナミック設定用にグローバル IP アドレスをすばやく解放する必要がある場合は、**ip nat translation timeout** コマンドを使用して、デフォルトのタイムアウトより短いタイムアウトを設定する必要があります。 ただし、設定するタイムアウトは、次の作業で指定するコマンドを使用して設定された他のタイムアウトよりも長い必要があります。 TCP セッションが、両側またはリセット中の finish（FIN）パケットによって正しく閉じられない場合、**ip nat translation tcp-timeout** コマンドを使用して、デフォルト TCP タイムアウトを変更する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat translation** *seconds*
4. **ip nat translation udp-timeout** *seconds*
5. **ip nat translation dns-timeout** *seconds*
6. **ip nat translation tcp-timeout** *seconds*
7. **ip nat translation finrst-timeout** *seconds*
8. **ip nat translation icmp-timeout** *seconds*
9. **ip nat translation syn-timeout** *seconds*
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat translation** *seconds* 例： `Router(config)# ip nat translation 300`	（任意）NAT 変換がタイムアウトするまでの時間を変更します。 • デフォルトのタイムアウトは 24 時間で、ハーフエントリのエージング タイムに適用されます。
ステップ 4	**ip nat translation udp-timeout** *seconds* 例： `Router(config)# ip nat translation udp-timeout 300`	（任意）UDP のタイムアウト値を変更します。
ステップ 5	**ip nat translation dns-timeout** *seconds* 例： `Router(config)# ip nat translation dns-timeout 45`	（任意）ドメイン ネーム システム（DNS）のタイムアウト値を変更します。

	コマンドまたはアクション	目的
ステップ 6	**ip nat translation tcp-timeout** *seconds* 例： `Router(config)# ip nat translation tcp-timeout 2500`	（任意）TCP のタイムアウト値を変更します。 • デフォルトは 24 時間です。
ステップ 7	**ip nat translation finrst-timeout** *seconds* 例： `Router(config)# ip nat translation finrst-timeout 45`	（任意）finish および reset タイムアウト値を変更します。 • finrst-timeout：TCP セッションが finish-in（FIN-IN）および finish-out（FIN-OUT）の両方を受信した後、または TCP セッションのリセット後のエージングタイム。
ステップ 8	**ip nat translation icmp-timeout** *seconds* 例： `Router(config)# ip nat translation icmp-timeout 45`	（任意）ICMP のタイムアウト値を変更します。
ステップ 9	**ip nat translation syn-timeout** *seconds* 例： `Router(config)# ip nat translation syn-timeout 45`	（任意）同期（SYN）のタイムアウト値を変更します。 • TCP セッションで SYN が受信された場合にのみ、同期タイムアウトまたはエージング タイムが使用されます。 同期確認応答（SYNACK）が受信されると、タイムアウトは TCP タイムアウトに変更されます。
ステップ 10	**end** 例： `Router(config)# end`	（任意）グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

NAT を使用してオーバーラップするネットワークに通信を許可するには

この項では、同じ操作を実行する複数の作業をまとめて説明していますが、実装されている変換のタイプがスタティックか、ダイナミックかに応じて、これらの作業の実行方法は異なります。

実装されている変換のタイプに適用する作業を実行してください。

オーバーラップするネットワークのスタティック変換の設定

スタブ ネットワーク内の IP アドレスが別のネットワークに属する正式な IP アドレスであるときに、スタティック変換を使用して、これらのホストやルータと通信する必要がある場合は、オーバーラップするネットワークのスタティック変換を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat inside source static** *local-ip global-ip*
4. **interface** *type number*
5. **ip address** *ip-address mask*
6. **ip nat inside**
7. **exit**
8. **interface** *type number*
9. **ip address** *ip-address mask*
10. **ip nat outside**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat inside source static** *local-ip global-ip* 例： `Device(config)# ip nat inside source static 192.168.121.33 10.2.2.1`	内部ローカル アドレスと内部グローバル アドレスとの間のスタティック変換を設定します。
ステップ 4	**interface** *type number* 例： `Device(config)# interface ethernet 1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.114.11.39 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 6	**ip nat inside** 例： `Device(config-if)# ip nat inside`	内部と接続されることを示すマークをインターフェイスに付けます。
ステップ 7	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *type number* 例： `Device(config)# interface ethernet 0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 172.16.232.182 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 10	**ip nat outside** 例： `Device(config-if)# ip nat outside`	外部と接続されることを示すマークをインターフェイスに付けます。
ステップ 11	**end** 例： `Device(config-if)# end`	（任意）インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次の作業

必要な設定が完了したら、「NAT のモニタリングおよびメンテナンス」モジュールに進みます。

オーバーラップするネットワークのダイナミック変換の設定

スタブ ネットワーク内の IP アドレスが別のネットワークに属する正式な IP アドレスであるときに、ダイナミック変換を使用して、これらのホストやルータと通信する必要がある場合は、オーバーラップするネットワークのダイナミック変換を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
4. **access-list** *access-list-number* **permit** *source* [*source-wildcard*]
5. **ip nat outside source list** *access-list-number* **pool** *name*
6. **interface** *type number*
7. **ip address** *ip-address mask*
8. **ip nat inside**
9. **exit**
10. **interface** *type number*
11. **ip address** *ip-address mask*
12. **ip nat outside**
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask*	**prefix-length** *prefix-length*} 例： `Device(config)# ip nat pool net-10 10.0.1.0 10.0.1.255 prefix-length 24`	必要に応じて割り当てられるグローバルアドレスのプールを定義します。

	コマンドまたはアクション	目的
ステップ 4	**access-list** *access-list-number* **permit** *source* [*source-wildcard*] 例： `Device(config)# access-list 1 permit 10.114.11.0 0.0.0.255`	変換されるアドレスを許可する標準アクセス リストを定義します。 • アクセス リストは、変換されるアドレスだけを許可する必要があります（各アクセス リストの最後には暗黙的な「deny all」があるので注意してください）。アクセス リストでアドレスを許可しすぎると、予期しない結果になる可能性があります。
ステップ 5	**ip nat outside source list** *access-list-number* **pool** *name* 例： `Device(config)# ip nat outside source list 1 pool net-10`	ステップ 4 で定義されたアクセス リストを指定して、ダイナミック外部送信元変換を設定します。
ステップ 6	**interface** *type number* 例： `Device(config)# interface ethernet 1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.114.11.39 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 8	**ip nat inside** 例： `Device(config-if)# ip nat inside`	内部と接続されることを示すマークをインターフェイスに付けます。
ステップ 9	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface ethernet 0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 172.16.232.182 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 12	**ip nat outside** 例： `Device(config-if)# ip nat outside`	外部と接続されることを示すマークをインターフェイスに付けます。
ステップ 13	**end** 例： `Device(config-if)# end`	（任意）インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

サーバ TCP ロード バランシングの設定

宛先アドレス ロータリー変換を目的として、サーバTCPのロードバランシングを設定するには、この作業を実行します。 この作業で指定されるコマンドを使用すると、1 つの仮想ホストを多数の実ホストにマッピングできます。 仮想ホストとの間で開かれた新しいTCPセッションはそれぞれ、異なる実ホストとのセッションに変換されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} **type rotary**
4. **access-list** *access-list-number* **permit** *source* [*source-wildcard*]
5. **ip nat inside destination-list** *access-list-number* **pool** *name*
6. **interface** *type number*
7. **ip address** *ip-addressmask*
8. **ip nat inside**
9. **exit**
10. **interface** *type number*
11. **ip address** *ip-address mask*
12. **ip nat outside**
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} **type rotary** 例： `Device(config)# ip nat pool real-hosts 192.168.201.2 192.168.201.5 prefix-length 28 type rotary`	実ホストのアドレスを含むアドレス プールを定義します。
ステップ 4	**access-list** *access-list-number* **permit** *source* [*source-wildcard*] 例： `Device(config)# access-list 1 permit 192.168.201.30 0.0.0.255`	仮想ホストのアドレスを許可するアクセス リストを定義します。
ステップ 5	**ip nat inside destination-list** *access-list-number* **pool** *name* 例： `Device(config)# ip nat inside destination-list 2 pool real-hosts`	直前の手順で定義されたアクセス リストを指定して、ダイナミック内部宛先変換を設定します。
ステップ 6	**interface** *type number* 例： `Device(config)# interface ethernet 0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip address** *ip-addressmask* 例： `Device(config-if)# ip address 192.168.201.1 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 8	**ip nat inside** 例： `Device(config-if)# ip nat inside`	内部と接続されることを示すマークをインターフェイスに付けます。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface serial 0`	異なるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.168.15.129 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 12	**ip nat outside** 例： `Device(config-if)# ip nat outside`	外部と接続されることを示すマークをインターフェイスに付けます。
ステップ 13	**end** 例： `Device(config-if)# end`	（任意）インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

内部インターフェイスでのルート マップのイネーブル化

はじめる前に

作業で使用する必要のあるルート マップはすべて、設定作業を開始する前に設定しておく必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat inside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static** *local-ip global-ip* [**route-map** *map-name*]}
4. **exit**
5. **show ip nat translations** [**verbose**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat inside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static** *local-ip global-ip* [**route-map** *map-name*]} 例： `Device(config)# ip nat inside source static 192.168.201.6 192.168.201.21 route-map isp2`	NAT内部インターフェイスで設定されたスタティック NAT を使ったルート マッピングをイネーブルにします。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip nat translations** [**verbose**] 例： `Device# show ip nat translations`	（任意）アクティブな NAT を表示します。

NAT Route Maps Outside-to-Inside サポートのイネーブル化

NAT Route Maps Outside-to-Inside サポート機能により、外部から内部に向けて IP セッションを開始できるようにするネットワーク アドレス変換（NAT）ルート マップ コンフィギュレーションの設定が可能になります。 NAT Route Maps Outside-to-Inside サポート機能をイネーブルにするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat pool** *name start-ip end-ip* **netmask** *netmask*
4. **ip nat pool** *name start-ip end-ip* **netmask** *netmask*
5. **ip nat inside source route-map** *name* **pool** *name* [**reversible**]
6. **ip nat inside source route-map** *name* **pool** *name* [**reversible**]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device(config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat pool** *name start-ip end-ip* **netmask** *netmask* 例： `Device(config)# ip nat pool POOL-A 192.168.201.4 192.168.201.6 netmask 255.255.255.128`	NAT で使用されるネットワーク アドレス プールを定義します。
ステップ 4	**ip nat pool** *name start-ip end-ip* **netmask** *netmask* 例： `Device(config)# ip nat pool POOL-B 192.168.201.7 192.168.201.9 netmask 255.255.255.128`	NAT で使用されるネットワーク アドレス プールを定義します。
ステップ 5	**ip nat inside source route-map** *name* **pool** *name* [**reversible**] 例： `Device(config)# ip nat inside source route-map MAP-A pool POOL-A reversible`	Outside-to-Inside で開始されたセッションが、宛先ベースの NAT に対してルート マップを使用できるようにします。

	コマンドまたはアクション	目的
ステップ 6	**ip nat inside source route-map** *name* **pool** *name* [**reversible**] 例： `Device(config)# ip nat inside source route-map MAP-B pool POOL-B reversible`	Outside-to-Inside で開始されたセッションが、宛先ベースの NAT に対してルートマップを使用できるようにします。
ステップ 7	**end** 例： `Device(config)# end`	（任意）グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

外部 IP アドレスのみの NAT の設定

外部 IP アドレスの NAT を設定する場合、あらゆるアプリケーションおよびトラフィック タイプの埋め込み IP アドレスをすべて無視するように NAT を設定できます。 企業ネットワークの外部にあるホストとトラフィック間のトラフィックは、内部ネットワークを通過します。 NAT 用に設定されたデバイスは、内部ネットワーク内でルーティングできるアドレスにパケットを変換します。 目的の宛先が企業ネットワークの外部にある場合、パケットは外部アドレスに逆変換されて送信されます。

（注） 外部ローカル アドレス用のスタティック ルートを追加するように **ip nat outside source static** コマンドを設定すると、パケットの変換に遅延が生じ、パケットがドロップされます。 パケットがドロップされるのは、NAT がスタティック変換用に設定されている場合、初期同期（SYN）パケットのショートカットが作成されないためです。 パケットがドロップされないようにするには、**ip nat outside source static add-route** コマンドまたは **ip route** コマンドのいずれかを設定します。

外部 IP アドレスのみの NAT を設定する利点は、次のとおりです。

- 企業は、企業バックボーン ネットワークとしてインターネットを使用できます。
- ヘッダーの変換のみを必要とするネットワーク アーキテクチャを使用できます。
- 開始時点で、エンド クライアントに使用可能な IP アドレスが与えられます。 このアドレスは、IPsec 接続とトラフィック フローに使用されるアドレスです。
- 特別にルートを更新しなくても、パブリックおよびプライベート ネットワーク アーキテクチャがサポートされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat inside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static network** *local-ip global-ip* [**no-payload**]}
4. **ip nat inside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static** {**tcp** | **udp**} *local-ip local-port global-ip global-port* [**no-payload**]}
5. **ip nat inside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static** [**network**] *local-network-mask global-network-mask* [**no-payload**]}
6. **ip nat outside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static** *local-ip global-ip* [**no-payload**]}
7. **ip nat outside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static** {**tcp** | **udp**} *local-ip local-port global-ip global-port* [**no-payload**]}
8. **ip nat outside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static** [**network**] *local-network-mask global-network-mask* [**no-payload**]}
9. **exit**
10. **show ip nat translations** [**verbose**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat inside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static network** *local-ip global-ip* [**no-payload**]} 例： `Device(config)# ip nat inside source static network 10.1.1.1 192.168.251.0/24 no-payload`	内部ホスト デバイスでのネットワーク パケット変換をディセーブルにします。
ステップ 4	**ip nat inside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static** {**tcp** | **udp**} *local-ip local-port global-ip global-port* [**no-payload**]} 例： `Device(config)# ip nat inside source static tcp 10.1.1.1 2000 192.168.1.1 2000 no-payload`	内部ホスト デバイスでのポート パケット変換をディセーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**ip nat inside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static** [**network**] *local-network-mask global-network-mask* [**no-payload**]} 例： `Device(config)# ip nat inside source static 10.1.1.1 192.168.1.1 no-payload`	内部ホスト デバイスでのパケット変換をディセーブルにします。
ステップ 6	**ip nat outside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static** *local-ip global-ip* [**no-payload**]} 例： `Device(config)# ip nat outside source static 10.1.1.1 192.168.1.1 no-payload`	外部ホスト デバイスでのパケット変換をディセーブルにします。
ステップ 7	**ip nat outside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static** {**tcp** | **udp**} *local-ip local-port global-ip global-port* [**no-payload**]} 例： `Device(config)# ip nat outside source static tcp 10.1.1.1 20000 192.168.1.1 20000 no-payload`	外部ホスト デバイスでのポート パケット変換をディセーブルにします。
ステップ 8	**ip nat outside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static** [**network**] *local-network-mask global-network-mask* [**no-payload**]} 例： `Device(config)# ip nat outside source static network 10.1.1.1 192.168.251.0/24 no-payload`	外部ホスト デバイスでのネットワーク パケット変換をディセーブルにします。
ステップ 9	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 10	**show ip nat translations** [**verbose**] 例： `Device# show ip nat translations`	アクティブな NAT を表示します。

NAT Default Inside Server 機能の設定

NAT Default Inside Server 機能は、外部から、指定された内部ローカル アドレスにパケットを転送する場合に使用します。既存のダイナミック変換またはスタティック ポート変換に一致しないトラフィックはリダイレクトされ、パケットはドロップされません。

ダイナミック マッピングとインターフェイス オーバーロードは、ゲーム用デバイスに設定できます。 オンライン ゲームでは、外部トラフィックは異なる UDP に到着します。 パケットが、企業ネットワーク外からインターフェイス宛に送信され、完全に拡張されたエントリまたはスタティック ポート エントリに一致するものが NAT テーブルに存在しない場合、このパケットは、単純なスタティック エントリを使用してゲーム用デバイスに転送されます。

（注）
- この機能は、PC とは異なる IP アドレスを持つゲーム用デバイスを設定するために使用します。 迷惑なトラフィックや DoS 攻撃を回避するには、アクセス リストを使用します。
- PC から外部へのトラフィックについては、ルートマップを使用して、拡張エントリが作成されるようにしてください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat inside source static** *local-ip* **interface** *type number*
4. **ip nat inside source static tcp** *local-ip local-port* **interface** *global-port*
5. **exit**
6. **show ip nat translations** [**verbose**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ip nat inside source static** *local-ip* **interface** *type number* 例： `Device(config)# ip nat inside source static 10.1.1.1 interface Ethernet 1/1`	インターフェイス上でスタティック NAT をイネーブルにします。
ステップ 4	**ip nat inside source static tcp** *local-ip local-port* **interface** *global-port* 例： `Device(config)# ip nat inside source static tcp 10.1.1.1 23 interface 23`	（任意）外部からデバイスへの Telnet の使用をイネーブルにします。
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show ip nat translations** [**verbose**] 例： `Device# show ip nat translations`	（任意）アクティブな NAT を表示します。

NAT ルータでの RTSP の再イネーブル化

Real Time Streaming Protocol（RTSP）は、クライアント/サーバ マルチメディア プレゼンテーション制御プロトコルの一種で、マルチメディア アプリケーションの配信をサポートしています。RTSP を使用するアプリケーションには、Microsoft の Windows Media Services（WMS）、Apple Computer の QuickTime、RealNetworks の RealSystem G2 などがあります。

接続を成功させるには、RTSP プロトコルが NAT ルータを通過するときに、埋め込みアドレスとポートを変換する必要があります。 NAT では、ペイロードを解析し、RTSP ペイロード中の埋め込み情報を変換するために、Network Based Application Recognition（NBAR）アーキテクチャが使用されます。

RTSP はデフォルトでイネーブルになっています。 この設定がディセーブルになっている場合に、NAT ルータで RTSP を再度イネーブルにするには、**ip nat service rtsp port** *port-number* コマンドを使用します。

スタティック IP アドレスを持つユーザのサポートの設定

スタティック IP アドレスを持つユーザに対するサポートを設定すると、このようなユーザはパブリック ワイヤレス LAN 環境で IP セッションを確立できるようになります。

はじめる前に

スタティック IP アドレスを使用しているユーザのサポートを設定する前に、まず、ルータで NAT をイネーブルにし、RADIUS サーバ ホストを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip nat inside**
5. **exit**
6. **ip nat allow-static-host**
7. **ip nat pool** *name start-ip end-ip* **netmask** *netmask* **accounting** *list-name*
8. **ip nat inside source list** *access-list-number* **pool***name*
9. **access-list** *access-list-number* **deny ip** *source*
10. **end**
11. **show ip nat translations verbose**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface ethernet 1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ip nat inside** 例： `Device(config-if)# ip nat inside`	内部と接続されることを示すマークをインターフェイスに付けます。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip nat allow-static-host** 例： `Device(config)# ip nat allow-static-host`	スタティック IP アドレスのサポートをイネーブルにします。 • このインターフェイスでは、ダイナミック アドレス解決プロトコル（ARP）の学習はディセーブルされます。また、スタティック IP ホストの ARP エントリの作成と削除は NAT により制御されます。
ステップ 7	**ip nat pool** *name start-ip end-ip* **netmask** *netmask* **accounting** *list-name* 例： `Device(config)# ip nat pool pool1 172.16.0.0 172.16.0.254 netmask 255.255.255.0 accounting WLAN-ACCT`	スタティック IP ホストの認証に使用される、既存の RADIUS プロファイル名を指定します。
ステップ 8	**ip nat inside source list** *access-list-number* **pool***name* 例： `Device(config)# ip nat inside source list 1 pool net-208`	スタティック IP サポートに使用されるアクセス リストとプールを指定します。 • 指定されたアクセス リストはすべてのトラフィックを許可する必要があります。
ステップ 9	**access-list** *access-list-number* **deny ip** *source* 例： `Device(config)# access-list 1 deny ip 192.168.196.51`	NAT からデバイスのトラフィックを削除します。 • *source* 引数は、NAT スタティック IP サポート機能をサポートするデバイスの IP アドレスです。
ステップ 10	**end** 例： `Device(config)# end`	（任意）グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 11	**show ip nat translations verbose** 例： `Device# show ip nat translations verbose`	（任意）アクティブな NAT 変換および各変換テーブル エントリの追加情報（エントリがいつ作成および使用されたかなど）が表示されます。

例

次に、**show ip nat translations verbose** コマンドの出力例を示します。

```
Device# show ip nat translations verbose

--- 172.16.0.0 10.1.1.1           ---                 ---
create 00:05:59, use 00:03:39, left 23:56:20, Map-Id(In): 1, flags: none wlan-flags: Secure
 ARP added, Accounting Start sent Mac-Address:0010.7bc2.9ff6 Input-IDB:Ethernet1/2, use_count:
 0, entry-id:7, lc_entries: 0
```

NAT 変換のレート制限機能の設定

手順の概要

1. **enable**
2. **show ip nat translations**
3. **configure terminal**
4. **ip nat translation max-entries** {*number* | **all-vrf** *number* | **host** *ip-address number* | **list** *listname number* | **vrf** *name number*}
5. **end**
6. **show ip nat statistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip nat translations** 例： `Device# show ip nat translations`	（任意）アクティブな NAT を表示します。 • 特定のホスト、アクセス コントロール リスト、または VRF インスタンスが予想外に大量の NAT 要求を生成している場合、それが悪意のあるウイルスやワーム攻撃の元凶である可能性があります。
ステップ 3	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ip nat translation max-entries** {*number* | **all-vrf** *number* | **host** *ip-address number* | **list** *listname number* | **vrf** *name number*} 例： `Device(config)# ip nat translation max-entries 300`	指定された送信元に許容される NAT エントリの最大数を設定します。 • 許容される NAT エントリの最大数は 2147483647 ですが、通常の NAT レート制限の範囲は 100 ～ 300 エントリです。 • すべての VRF インスタンスに対する NAT レート制限を設定すると、各 VRF インスタンスは、指定した NAT エントリの最大数に制限されます。 • 特定の VRF インスタンスに対する NAT レート制限を設定する場合、すべての VRF インスタンスに許容される NAT エントリの最大数よりも大きい、または小さい値を、指定した VRF インスタンスに対する最大数に指定します。
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show ip nat statistics** 例： `Device# show ip nat statistics`	（任意）NAT レート制限の設定値を含む、現在の NAT 使用に関する情報を表示します。 • NAT レート制限の設定後、**show ip nat statistics** コマンドを使用して、現在の NAT レート制限の設定を検証します。

IP アドレス節約のための NAT 設定例

例：内部送信元アドレスのスタティック変換の設定

次に、10.114.11.0 ネットワークからアドレス指定される複数の内部ホストの、グローバルに一意な 172.31.233.208/28 ネットワークへの変換例を示します。 その後、10.114.11.0 ネットワーク（本物の 10.114.11.0 ネットワーク）の外部ホストからやってきたパケットは、変換後、10.0.1.0/24 ネットワークからのもののように見えます。

```
ip nat pool net-208 172.31.233.208 172.31.233.223 prefix-length 28
ip nat pool net-10 10.0.1.0 10.0.1.255 prefix-length 24
ip nat inside source list 1 pool net-208
ip nat outside source list 1 pool net-10
!
interface ethernet 0
 ip address 172.31.232.182 255.255.255.240
 ip nat outside
```

```
!
interface ethernet 1
 ip address 10.114.11.39 255.255.255.0
 ip nat inside
!
access-list 1 permit 10.114.11.0 0.0.0.255
```

次に、vrf1 および vrf2 VPN について、共有サービスへのスタティック ルートを持つプロバイダー エッジ（PE）ルータで設定された NAT の例を示します。 NAT は、内部送信元スタティック 1 対 1 変換として設定されます。

```
ip nat pool outside 10.4.4.1 10.4.4.254 netmask 255.255.255.0
ip nat outside source list 1 pool mypool
access-list 1 permit 172.16.18.0 0.0.0.255
ip nat inside source static 192.168.121.33 10.2.2.1 vrf vrf1
ip nat inside source static 192.169.121.33.10.2.2.2 vrf vrf2
```

例：内部送信元アドレスのダイナミック変換の設定

次の例では、内部ホストのアドレス 192.168.1.0 または 192.168.2.0 のネットワークが、グローバルに一意な 172.31.233.208/28 のネットワークにどのように変換されるかを示しています。

```
ip nat pool net-208 172.31.233.208 172.31.233.223 prefix-length 9
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 172.31.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

次の例では、どのようにして、NAT を実行しているプロバイダー エッジ（PE）デバイスにローカルなトラフィックのみが変換されるかを示しています。

```
ip nat inside source list 1 interface e 0 vrf vrf1 overload
ip nat inside source list 1 interface e 0 vrf vrf2 overload
!
ip route vrf vrf1 0.0.0.0 0.0.0.0 192.168.1.1
ip route vrf vrf2 0.0.0.0 0.0.0.0 192.168.1.1
!
access-list 1 permit 10.1.1.1.0 0.0.0.255
!
ip nat inside source list 1 interface e 1 vrf vrf1 overload
ip nat inside source list 1 interface e 1 vrf vrf2 overload
!
ip route vrf vrf1 0.0.0.0 0.0.0.0 172.16.1.1 global
ip route vrf vrf2 0.0.0.0 0.0.0.0 172.16.1.1 global
access-list 1 permit 10.1.1.0 0.0.0.255
```

例：NAT を使用した内部ユーザのインターネットへのアクセスの許可

次に、net-208 というアドレス プールの作成方法の例を示します。 このプールには、172.31.233.208 ～ 172.31.233.233 のアドレスが含まれます。 アクセス リスト 1 には、SA が 192.168.1.0 ～ 192.168.1.255 の範囲に含まれるパケットが許可されます。 変換が存在しない場合、アクセス リスト 1 に一致するパケットは、このプールに含まれるアドレスに変換されます。 ルータは複数の

ローカル アドレス（192.168.1.0 ～ 192.168.1.255）に、同じグローバル アドレスの使用を許可します。 ルータは接続を区別するためにポート番号を保持します。

```
ip nat pool net-208 172.31.233.208 172.31.233.233 netmask 255.255.255.240
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 pool net-208 overload
interface ethernet 1
 ip address 192.168.201.1 255.255.255.240
 ip nat inside
!
interface ethernet 0
 ip address 192.168.201.29 255.255.255.240
 ip nat outside
!
```

例：NAT を使用したオーバーラップするネットワークに対する通信の許可

例：サーバ TCP のロード バランシングの設定

次の例の目的は、一連の実ホストの間で接続が分散される仮想アドレスを定義することです。 プールは実ホストのアドレスを定義します。 アクセス リストは仮想アドレスを定義します。 変換がまだ存在しない場合、シリアル インターフェイス 0（外部インターフェイス）からの TCP パケットのうち、アクセス リストと一致する宛先を持つものは、このプールに含まれるアドレスに変換されます。

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
access-list 2 permit 192.168.15.1
ip nat inside destination list 2 pool real-hosts
interface ethernet 0
 ip address 192.168.15.129 255.255.255.240
 ip nat inside
!
interface serial 0
 ip address 192.168.15.17 255.255.255.240
 ip nat outside
!
```

例：内部インターフェイスでのルート マップのイネーブル化

```
ip nat inside source static 192.168.201.6 192.168.201.21
!
```

例：NAT Route Maps Outside-to-Inside サポートのイネーブル化

次の例では、宛先ベースのネットワーク アドレス変換（NAT）に対する Outside-to-Inside 変換を許可するようにルート マップ A およびルート マップ B を設定する方法を示します。

```
ip nat pool POOL-A 192.168.201.4 192.168.201.6 netmask 255.255.255.128
ip nat pool POOL-B 192.168.201.7 192.168.201.9 netmask 255.255.255.128
ip nat inside source route-map MAP-A pool POOL-A reversible
ip nat inside source route-map MAP-B pool POOL-B reversible
```

例：外部 IP アドレスのみの NAT の設定

```
ip nat inside source static network 10.1.1.1 192.168.2510/24 no-payload
ip nat inside source static tcp 10.1.1.1 2000 192.168.1.1 2000 no-payload
ip nat inside source static 10.1.1.1 192.168.1.1 no-payload
ip nat outside source static 10.1.1. 192.168.1.1 no-payload
ip nat outside source static tcp 10.1.1.1 20000 192.168.1.1 20000 no-payload
ip nat outside source static network 10.1.1.1 192.168.251.0/24 no-payload
```

例：スタティック IP アドレスを持つユーザのサポートの設定

```
interface ethernet 1
 ip nat inside
!
ip nat allow-static-host
ip nat pool pool1 172.16.0.0 172.16.0.254 netmask 255.255.255.0 accounting WLAN-ACCT
ip nat inside source list 1 pool net-208
access-list 1 deny ip 192.168.196.51
```

例：NAT スタティック IP サポートの設定

次の例では、192.168.196.51 にあるルータに対するスタティック IP アドレス サポートをイネーブルにする方法を示します。

```
interface ethernet 1
 ip nat inside
ip nat allow-static-host
ip nat pool net-208 172.16.1.1 172.16.1.10 netmask 255.255.255.0 accounting WLAN-ACCT
ip nat inside source list 1 pool net-208
access-list 1 deny ip 192.168.196.51
```

例：NAT スタティック IP サポートに使用される RADIUS プロファイルの作成

次の例では、NAT スタティック IP サポート機能で使用される RADIUS プロファイル aaa new-model の作成方法を示します

```
aaa new-model
!
aaa group server radius WLAN-RADIUS
 server 172.16.88.1 auth-port 1645 acct-port 1645
 server 172.16.88.1 auth-port 1645 acct-port 1646
!
aaa accounting network WLAN-ACCT start-stop group WLAN-RADIUS
aaa session-id common
ip radius source-interface Ethernet3/0
radius-server host 172.31.88.1 auth-port 1645 acct-port 1646
radius-server key cisco
```

例：NAT 変換のレート制限機能の設定

次の例では、許容される NAT エントリの最大数を 300 に制限する方法を示します。

```
ip nat translation max-entries 300
```

次の例では、VRF インスタンス「vrf1」の NAT エントリ数を 150 に制限する方法を示します。

```
ip nat translation max-entries vrf vrf1 150
```

次の例では、各 VRF インスタンスの NAT エントリ数を 200 に制限する方法を示します。

```
ip nat translation max-entries all-vrf 200
```

次の例では、VRF インスタンス「vrf2」の NAT エントリ数を 225 に、その他すべての VRF インスタンスの NAT エントリ数をそれぞれ 100 に制限する方法を示します。

```
ip nat translation max-entries all-vrf 100
ip nat translation max-entries vrf vrf2 225
```

次の例では、アクセス コントロール リスト「vrf3」の NAT エントリ数を 100 に制限する方法を示します。

```
ip nat translation max-entries list vrf3 100
```

次の例では、IP アドレス 10.0.0.1 にあるホストの NAT エントリ数を 300 に制限する方法を示します。

```
ip nat translation max-entries host 10.0.0.1 300
```

例：グローバル NAT レート制限の設定

次の例では、許容される NAT エントリの最大数を 300 に制限する方法を示します。

```
ip nat translation max-entries 300
```

例：特定の VRF インスタンスで使用される NAT レート制限の設定

次の例では、VRF インスタンス「vrf1」の NAT エントリ数を 150 に制限する方法を示します。

```
ip nat translation max-entries vrf vrf1 150
```

例：すべての VRF インスタンスで使用される NAT レート制限の設定

次の例では、各 VRF インスタンスの NAT エントリ数を 200 に制限する方法を示します。

```
ip nat translation max-entries all-vrf 200
```

次の例では、VRF インスタンス「vrf2」の NAT エントリ数を 225 に、その他すべての VRF インスタンスの NAT エントリ数をそれぞれ 100 に制限する方法を示します。

```
ip nat translation max-entries all-vrf 100
ip nat translation max-entries vrf vrf2 225
```

例：アクセス コントロール リストで使用される NAT レート制限の設定

次の例では、アクセス コントロール リスト「vrf3」の NAT エントリ数を 100 に制限する方法を示します。

```
ip nat translation max-entries list vrf3 100
```

例：IP アドレスで使用される NAT レート制限の設定

次の例では、IP アドレス 10.0.0.1 にあるホストの NAT エントリ数を 300 に制限する方法を示します。

```
ip nat translation max-entries host 10.0.0.1 300
```

次の作業

- アプリケーション レベル ゲートウェイで使用するための NAT の設定については、「NAT でのアプリケーション レベル ゲートウェイの使用」モジュールを参照してください。
- NAT を確認、モニタ、およびメンテナンスするには、「NAT のモニタリングおよびメンテナンス」モジュールを参照してください。
- NAT をマルチプロトコル ラベル スイッチング（MPLS）VPN と統合するには、「MPLS VPN と NAT の統合」モジュールを参照してください。
- ハイ アベイラビリティを得るための NAT の設定については、「ハイ アベイラビリティ用 NAT の設定」モジュールを参照してください。

IP アドレス変換用の NAT の設定に関するその他の関連資料

関連資料

関連項目	参照先
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
NAT コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト、使用上の注意事項、および例	『Cisco IOS IP Addressing Services Command Reference』
アプリケーション レベル ゲートウェイ	「*Using Application Level Gateways with NAT*」モジュール
IP アクセス リストへのシーケンス番号づけ	『IP Access List Sequence Numbering』マニュアル
RADIUS 属性の概要	『*RADIUS Attributes Overview and RADIUS IETF Attributes*』モジュール

標準および RFC

標準/RFC	タイトル
RFC 1597	『Internet Assigned Numbers Authority』
RFC 1631	『The IP Network Address Translation (NAT)』
RFC 1918	『Address Allocation for Private Internets』
RFC 2663	『IP Network Address Translation (NAT) Terminology and Considerations』
RFC 3022	『Traditional IP Network Address Translation (Traditional NAT)』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP アドレス節約のための NAT 設定に関する機能情報

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

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

表 *1*：*IP* アドレス節約のための *NAT* 設定に関する機能情報

機能名	リリース	機能情報
ルート マップを使用した宛先ベース NAT	Cisco IOS XE Release 2.1	ルート マップを使用した宛先ベース NAT 機能によって、ルート マップを使用した宛先ベース NAT に対するサポートが追加されます。
NAT 重複内部グローバル アドレス	Cisco IOS XE Release 2.1	Cisco IOS XE ソフトウェアでは、NAT 重複内部グローバル アドレス機能をサポートしています。
NAT ホスト番号保持	Cisco IOS XE Release 2.1	ネットワーク管理を容易にするため、サイトによっては、アドレスではなくプレフィックスを変換します。 これらのサイトでは、変換済みアドレスのホスト番号を元のアドレスのホスト番号と同じにする必要があります。2 つのプレフィックスの長さは同じである必要があります。 NAT ホスト番号保持機能は、match-host タイプのアドレス プールをダイナミック変換に設定することによりイネーブルにできます。
NAT パフォーマンスの向上：変換テーブルの最適化	Cisco IOS XE Release 2.1	NAT パフォーマンスの向上：変換テーブルの最適化機能は、変換テーブル エントリを格納するためのより優れた構造、およびテーブル エントリを IP 接続に関連付けるためのテーブルでの最適化された参照を提供します。
NAT Route Maps Outside-to-Inside サポート	Cisco IOS XE Release 2.2	NAT Route Maps Outside-to-Inside サポート機能により、外部から内部に向けて IP セッションを開始できるようにする NAT ルート マップ コンフィギュレーションの実装が可能になります。
NAT スタティック IP サポート	Cisco IOS XE Release 2.1	NAT スタティック IP サポート機能は、スタティック IP アドレスを持つユーザがパブリック ワイヤレス LAN 環境で IP セッションを確立できるようにサポートします。
NAT タイマー	Cisco IOS XE Release 2.1	NAT タイマー機能により、NAT 変換がタイムアウトするまでの時間を変更できます。

機能名	リリース	機能情報
外部 IP アドレスのみの NAT 変換	Cisco IOS XE Release 2.1	外部 IP アドレスのみの NAT 変換機能を使用して、あらゆるアプリケーションおよびトラフィック タイプの埋め込み IP アドレスをすべて無視するように NAT を設定できます。
NAT 変換のレート制限	Cisco IOS XE Release 2.1	NAT 変換のレート制限機能により、ルータ上でのネットワーク アドレス変換（NAT）動作の同時実行最大数を制限できるようになりました。 これにより、ユーザが NAT アドレスの使用方法をより詳細に管理できるようになるだけでなく、NAT 変換のレート制限機能を使用して、ウイルスやワーム、サービス拒絶攻撃の影響を制限できるようになります。

第 2 章

NAT でのアプリケーション レベル ゲートウェイの使用

このモジュールでは、ネットワーク アドレス変換（NAT）で使用されるアプリケーション レベル ゲートウェイ（ALG）を設定するための基本的な作業について説明します。 また、IP ヘッダー変換に ALG を使用するプロトコルについてもこのモジュールで説明します。

NAT は、アプリケーション データ ストリームで送信元および宛先 IP アドレスを伝送しない TCP/UDP トラフィックにおいて変換サービスを実行します。 送信元および宛先 IP アドレスを伝送しないプロトコルには、HTTP、TFTP、Telnet、Archie、Finger、ネットワーク タイム プロトコル（NTP）、ネットワーク ファイル システム（NFS）、リモート ログイン（rlogin）、リモート シェル（rsh）プロトコルおよびリモート コピー（rcp）が含まれます。

ペイロードに IP アドレス情報を埋め込むプロトコルは、ALG のサポートを必要とします。 NAT は、パケット ペイロードでの埋め込み IP アドレスおよびポート番号の変換や、制御チャネルからの新規接続/セッション情報の抽出といった、アプリケーション データ ストリーム（レイヤ 7）プロトコル固有のサービスを処理するためのさまざまな ALG を必要とします。

NAT は、サポートされる ALG を持つプロトコルに対し、仮想ルーティングおよび転送（VRF）をサポートします。

NAT を通じた IPsec ESP 機能のサポートにより、オーバーロード モード、またはポート アドレス変換（PAT）モードで設定された NAT デバイス経由で、複数の同時 IPsec Encapsulating Security Payload（ESP）トンネルまたは接続をサポートできるようになります。

- 機能情報の確認，50 ページ
- NAT でアプリケーション レベル ゲートウェイを使用するための要件，50 ページ
- NAT でのアプリケーション レベル ゲートウェイの使用について，50 ページ
- NAT でのアプリケーション レベル ゲートウェイの設定方法，55 ページ
- NAT でアプリケーション レベル ゲートウェイを使用する場合の設定例，62 ページ
- 次の作業，63 ページ

- NAT でアプリケーション レベル ゲートウェイを使用する場合のその他の関連資料，63 ページ
- NAT でアプリケーション レベル ゲートウェイを使用する場合の機能情報，64 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

NATでアプリケーションレベルゲートウェイを使用するための要件

- このモジュールの作業を実行する前に、「IP アドレス節約のための NAT 設定」モジュールで説明されている概念をよく理解しておく必要があります。
- このモジュールの作業で使用する必要のあるアクセス リストはすべて、設定作業を開始する前に設定しておく必要があります。 アクセス リストの設定方法の詳細については、『IP Access List Sequence Numbering』マニュアルを参照してください。
- このモジュールの作業を実行する前に、Session Initiation Protocol（SIP）および H.323 がディセーブルにされていないことを確認する必要があります。 SIP および H.323 はデフォルトでイネーブルです。

NATでのアプリケーションレベルゲートウェイの使用について

IPSec

IPsec は、オープン標準のフレームワークに含まれる IP プロトコル ファミリへの拡張セットで、インターネット上でプライベートな会話をセキュアに行えるようにするためにあります。 IETF により開発された標準に基づいて、IPsec はパブリック ネットワーク上でのデータ通信の機密性、整合性、および信頼性を保証し、暗号化によるセキュリティ サービスを提供します。

2 台のルータなど、2 つのピアの間にセキュリティ トンネルが提供され、どのパケットの機密性が高く、これらのセキュアなトンネル経由で送信されるべきと見なされるか、また、これらのトンネルの特徴を指定して、このような機密性の高いパケットを保護するにはどのパラメータを使用すべきかが判断されます。IPsec ピアは機密性の高いパケットを受信すると、適切でセキュアなトンネルを設定し、このトンネルを通じてパケットをリモート ピアに送信します。

カプセル化セキュリティ ペイロード（ESP）を使用する IPsec は、Network Address Port Translation（NAPT）、またはアドレス オーバーロードが設定されていない限り、特別なサポートなしに、NAT を実行しているルータを通過することができます。

複数のプライベート内部 IP アドレスを 1 つのパブリック外部 IP アドレスとして表した NAPT デバイスを通過する IPsec VPN 接続を行うときに、考慮しなければならない要因がいくつかあります。このような要因には、VPN サーバおよびクライアントの能力、NAPT デバイスの能力、NAPT デバイス上で同時に複数の接続が行われているかどうかが含まれます。

ルータに NAPT を使用する IPsec を設定する方法には、次の 2 通りがあります。

- TCP や UDP のようなレイヤ 4 プロトコルに IPsec をカプセル化する。この場合、IPsec は NAT を忍び出ることができます。NAT デバイスはカプセル化に気づきません。
- IPsec 固有のサポートを NAPT に追加します。この場合、IPsec は、NAT を忍び出るのとは逆の働きをします。IPSec ESP の NAT サポート：フェーズ II 機能は、インターネット キー交換（IKE）および ESP をサポートします。NAPT で設定された Cisco IOS ルータを通じたトンネル モードでカプセル化する必要はありません。

NAPT デバイスを経由する IPsec セッションを実行する場合は、TCP および UDP を使用することをお勧めします。ただし、すべての VPN サーバまたはクライアントで TCP または UDP がサポートされるわけではありません。

SPI マッチング

SPI マッチングは、複数の宛先ペアの間に VPN 接続を確立するために使用されます。NAT エントリはただちに設定済みのアクセス リストと一致するエンドポイントの変換テーブルに配置されます。

NAT IPsec 設定の利点

- NAT により、お客様は自分のネットワークにプライベート IP アドレスを導入し、インターネットへの接続、または別の企業ネットワークとの内部接続を行うときに、プライベート IP アドレスをパブリック IP アドレスに変換することができるようになります。
- Session Initiation Protocol（SIP）の NAT サポートによって、SIP ベースの VoIP ソリューションに NAT を導入する機能が追加されます。
- お客様は NAT ALG を使用して、自分の IP アドレス方式を制御し、H.323 v2 ゲートキーパー設定のサポートをすべて取り込むことができます。
- 通常、変換テーブルの ESP エントリの送信は、宛先から応答が届くまで、延期されます。予想可能なセキュリティ パラメータ インデックス（SPI）と SPI マッチングにより、SPI エントリが照合されるため、この延期を回避することができます。一部サードパーティのコンセ

ントレータでは、送信元ポートと受信ポートの両方でポート 500 を使用する必要があります。 これらのポートは、通常の NAT で必要であるように変更するのではなく、**ip nat service preserve-port** コマンドを使用して保持します。

IP ネットワークを経由する音声およびマルチメディア

SIP は、IETF Multiparty Multimedia Session Control（MMUSIC）Working Group により開発されたプロトコルです。 Cisco SIP 機能は Cisco ルータが IP ネットワーク経由した音声通話およびマルチメディア通話のセットアップを通知できるようにします。 SIP は、VoIP インターネットワーキング ソフトウェアの H.323 に代わるものです。

セッション記述プロトコル（SDP）は、マルチメディア セッションを記述するためのプロトコルです。 SDP は、SIP メッセージの本文で、複数のユーザが参加するマルチメディア セッションの作成および制御のために使用されるマルチメディア セッションを記述するために使用できます。

SIP に対する NAT サポート機能により、NAT を使って設定されたルータを通過する SIP 埋め込みメッセージは、変換後、パケットに暗号化されます。 SIP または SDP メッセージの変換には、NAT とともに ALG が使用されます。

（注） デフォルトでは、SIP のサポートはポート 5060 でイネーブルになっています。 したがって、NAT 対応デバイスはこのポートのパケットをすべて、SIP コール メッセージと解釈します。 同じシステムにある別のアプリケーションがポート 5060 を使用してパケットを送信している場合、NAT サービスはこのパケットを SIP コール メッセージとして解釈しようとするため、このパケットが破損する可能性があります。

H.323 v2 RAS に対する NAT サポート

Cisco IOS NAT は、Registration, Admission, and Status（RAS）プロトコルで送信されたものを含め、H.225 および H.245 メッセージ タイプをすべてサポートしています。 RAS は、ソフトウェア クライアントや VoIP デバイスにより、場所の登録、通話のセットアップ サポートの要求、および帯域幅の制御に使用される多数のメッセージを提供します。 RAS メッセージは、H.323 ゲートキーパーに向けて送信されます。

一部の RAS メッセージには、ペイロードに IP アドレス情報が含まれていますが、これは通常、ゲートキーパーへのユーザの登録、または別の登録済みユーザに関する情報の取得を意図したものです。 このようなメッセージが NAT に認識されない場合、誰にでも確認できる IP アドレスには変換されません。

Cisco IOS Release 12.2(2)T 以降のリリースでは、埋め込み IP アドレスがアドレス変換される可能性があるかどうかを検査できるようになりました。 Cisco IOS Release 12.2(2)T よりも前では、NAT で H.323 v2 RAS メッセージはサポートされていませんでした。

v2 互換モードでの H.323 v3 および v4 に対する NAT サポート

H.323は、パケットネットワーク経由でのオーディオ、ビデオ、およびデータ送信に関するITU-T仕様です。 NAT は、バージョン 1、バージョン 2、バージョン 3、およびバージョン 4 の 4 つのバージョンの H.323 プロトコルをサポートします。 v2 互換モードでの H.323 v3 および v4 に対する NAT サポート機能を使用すると、H.323 バージョン 3 およびバージョン 4 でコード化されたメッセージに H.323 バージョン 2 と互換性を持つフィールドが含まれている場合に、NAT ルータでこれらのメッセージをサポートできるようになります。 この機能では、アドレス変換を必要とする新しいメッセージ タイプまたは新しいフィールドなどの H.323 バージョン 3 およびバージョン 4 で導入された H.323 機能はサポートされません。

NAT H.245 トンネリングのサポート

NAT H.245 トンネリングのサポート機能では、H.323 ALG で H.245 トンネリングをサポートします。 H.245 トンネリングでは、メディア チャネル設定を作成するために必要な H.245 トンネルメッセージをサポートしています。

H.323 コールを行うには、TCP ポート 1720 で H.225 接続を開く必要があります。 H.225 接続が開かれると、H.245 セッションが開始され、確立されます。 H.323 接続は H.225 とは異なるチャネルで行うことができます。また、H.245 メッセージを H.225 メッセージに埋め込み、以前に確立された H.225 チャネルに送信することにより、同じ H.225 チャネル上で H.245 トンネリングを使用して行うこともできます。

H.245 トンネル型メッセージが NAT で理解されない場合、メディア アドレスおよびポート番号は NAT により変換されず、メディア トラフィックが失敗します。 H.245 トンネル型メッセージが NAT によって理解されない場合、H.245 FastConnect プロシージャは役に立ちません。これは、H.245 トンネル型メッセージが送信されるとすぐに、FastConnect が終了するためです。

Skinny Client Control Protocol に対する NAT サポート

Cisco IP Phone は、Cisco CallManager との接続、および登録に SCCP を使用します。

スケーラブルな環境で、IP Phone と Cisco CallManager の間に Cisco IOS NAT を設定できるようにするには、NAT は SCCP を検出し、メッセージで渡される情報を理解できなければなりません。電話での通話が可能な他の IP Phone ユーザの識別に使用される IP アドレスやポート情報を含むメッセージは両方向に行き来します。

Cisco CallManager 通信を行う SCCP クライアントは通常、内部から外部へ向かって進みます。Cisco CallManager が内部（NAT デバイスの背後）にある場合、Cisco CallManager IP アドレス接続を解決するには、ドメインネームシステム（DNS）を使用する必要があります。それ以外の場合は、内部にある Cisco CallManager にアクセスするようにスタティック NAT を設定する必要があります。

Cisco CallManager への接続を試みた IP Phone が設定済み NAT 規則と一致する場合、NAT はもともとの送信元 IP アドレスを変換して、設定済みプールにある IP アドレスで置き換えます。 この

新しいアドレスは Cisco CallManager に反映され、他の IP Phone ユーザから確認できるようになります。

SCCP フラグメンテーションの NAT サポート

Skinny Client Control Protocol（SCCP）メッセージ（スキニー制御メッセージとも呼ばれます）は、TCP 経由で交換されます。 IP Phone、または Cisco Unified CallManager のいずれかの TCP 最大セグメント サイズ（MSS）がスキニー制御メッセージのペイロードを下回るように設定されている場合、スキニー制御メッセージは、複数の TCP セグメントに分割されます。 この機能が導入される前は、NAT スキニー ALG でスキニー制御メッセージを再構成できなかったため、TCP セグメンテーション中にスキニー制御メッセージの交換が失敗していました。SCCP フラグメンテーションの NAT サポート機能は、NAT スキニー ALG の TCP セグメントに対するサポートを追加する機能です。これにより、IP 変換やポート変換を必要とする、分割されたペイロードがドロップされなくなります。

また、Virtual Fragmentation Reassembly（VFR）を使用して、スキニー制御メッセージを IP 分割することもできます。

Cisco IOS Release 15.1(3)T またはそれ以降のリリースでは、NAT はバージョン 17 以降の SCCP 電話で機能します。

レイヤ 4 フォワーディングを使った NAT セグメンテーション

レイヤ 4 フォワーディングを使った NAT セグメンテーション機能は、H.323、Skinny Client Control Protocol（SCCP）、および TCP ドメイン ネーム システム（DNS）プロトコル用に実装された機能です。 NAT は、複数のパケットに分割された H.323、SCCP、または TCP DNS メッセージの処理をサポートします。

レイヤ 4 フォワーディング、または TCP プロキシは、シーケンス番号の並べ替え、パケット内の番号の確認、最大セグメント サイズ（MSS）を超える変換後パケットの再分割、パケット損失の場合の再送信などのセッションを処理します。 また、レイヤ 4 フォワーディングは順番に並んでいないパケットの処理も行います。このようなパケットはバッファされ、ドロップされません。レイヤ 4 フォワーディングは受信したパケットをバッファし、順番に並んだパケットが使用できるようになったときに、NAT ALG に知らせます。また、受信したパケットについてエンド ホストに確認応答を送信し、NAT ALG から受信した変換後パケットを、出力パケット パスに送信します。

制約事項

レイヤ 4 フォワーディングを使った NAT セグメンテーションは、次の場合には機能しません。

- **ip inspect name** コマンドを使用するようにファイアウォールが設定されている。（コンテキストベース アクセス コントロール（CBAC）のファイアウォールはサポートされません。ゾーンベースのファイアウォールはサポートされています）
- H.323、SCCP、または TCP DNS メッセージのサイズが 18 KB を超える。

- マルチプロトコル ラベル スイッチング（MPLS）が設定されている。
- NAT と Cisco CallManager が同一のデバイス上に設定されている。 この場合、Call Manager Express のコロケーション ソリューションが使用されます。
- NAT 仮想インターフェイス（NVI）が設定されている。
- ステートフル ネットワーク アドレス変換（SNAT）がイネーブル化されている。
- パケット変換のため、**match-in-vrf** キーワードが **ip nat inside source** コマンドとともに設定されている。
- パケットが IPv6 パケットである。

NATでのアプリケーションレベルゲートウェイの設定方法

NAT を通じた IPsec の設定

NAT を通じた IPsec ESP の設定

NAT を通じた IPsec ESP により、オーバーロード モード、または PAT モードで設定された Cisco IOS NAT デバイス経由で、複数の同時 ESP トンネルまたは接続をサポートできるようになります。

NAT を通じた IPsec ESP を設定するには、次の作業を実行します。

（注） IPsec はスタティック NAT 設定のみならず、どのような NAT 設定についても設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat** [**inside** | **outside**] **source static** *local-ip global-ip* [**vrf** *vrf-name*]
4. **exit**
5. **show ip nat translations**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat** [**inside** | **outside**] **source static** *local-ip global-ip* [**vrf** *vrf-name*] 例： `Router(config)# ip nat inside source static 10.10.10.10 192.168.30.30`	スタティック NAT をイネーブルにします。
ステップ 4	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**show ip nat translations** 例： `Router# show ip nat translations`	（任意）アクティブな NAT を表示します。

保持ポートのイネーブル化

この作業は、送信元ポートにポート 500 を使用している IPsec トラフィックに対して使用します。送信元ポートとしてポート 500 を保持できるようにするには、このタスクを実行します。

（注） これは、ある特定の VPN コンセントレータで必要とされる作業です。 Cisco VPN デバイスでは、通常、この機能は使用されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat service list** *access-list-number* **IKE preserve-port**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat service list** *access-list-number* **IKE preserve-port** 例： `Router(config)# ip nat service list 10 IKE preserve-port`	ポートを保持するために、アクセス リストと一致する IPsec トラフィックを指定します。

NAT デバイスでの SPI マッチングのイネーブル化

（注） SPI マッチングはデフォルトでディセーブルにされています。

セキュリティ パラメータ インデックス（SPI）マッチングは、複数の宛先ペアの間に VPN 接続を確立するために使用されます。 NAT エントリはただちに設定済みのアクセス リストとマッチするエンドポイントの変換テーブルに配置されます。 SPI マッチングは、Cisco IOS Release 12.2(15)T に実装されている予測アルゴリズムに従って SPI を選択するエンドポイントでのみ使用できます。

予測可能で対称的な SPI の生成がイネーブル化されます。 NAT デバイス全体で複数の ESP 接続が望ましい場合は、NAT デバイスとともに SPI マッチングを使用する必要があります。

はじめる前に

送信元ルータと、並列処理をイネーブル化するリモート ゲートウェイの両方で、Cisco IOS ソフトウェアを実行する必要があります。

（注） SPI マッチングは、NAT デバイス、および両方のエンドポイント デバイスで設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat service list** *access-list-number* **ESP spi-match**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat service list** *access-list-number* **ESP spi-match** 例： `Router(config)# ip nat service list 10 ESP spi-match`	SPI マッチングをイネーブル化するアクセス リストを指定します。 • この例では、デバイスが両方ともシスコ デバイスで、マッチング可能な SPI を提供するように設定されていると仮定して、ESP トラフィック マッチング リスト 10 を NAT テーブルに入力します。

エンドポイントでの SPI マッチングのイネーブル化

はじめる前に

送信元デバイスと、並列処理をイネーブル化するリモート ゲートウェイの両方で、Cisco ソフトウェアを実行する必要があります。

（注） セキュリティ パラメータ インデックス（SPI）マッチングは、ネットワーク アドレス変換（NAT）デバイスおよび両方のエンドポイント デバイスに設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec nat-transparency spi-matching**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec nat-transparency spi-matching** 例： `Device(config)# crypto ipsec nat-transparency spi-matching`	両方のエンドポイントでSPIマッチングをイネーブル化します。
ステップ 4	**end** 例： `Device(config)# end`	グローバルコンフィギュレーションモードを終了し、特権 EXEC モードを開始します。

NAT に対する MultiPart SDP サポートのイネーブル化

NAT に対する MultiPart SDP サポート機能により、SIP ALG での MultiPart セッション記述プロトコル（SDP）のサポートが提供されます。 NAT に対する MultiPart SDP サポートはデフォルトでディセーブルです。

（注） NAT では、埋め込み IPv4 アドレスのみを変換します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat service allow-multipart**
4. **exit**
5. **show ip nat translations**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat service allow-multipart** 例： `Device(config)# ip nat service allow-multipart`	Multipart SDP をイネーブルにします。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 5	**show ip nat translations** 例： `Device# show ip nat translations`	（任意）アクティブな NAT を表示します。

IP Phone と Cisco CallManager の間での NAT の設定

ここでは、Cisco IP Phone における Cisco CallManager 通信のための Cisco Skinny Client Control Protocol（SCCP）の設定について説明します。 このセクションで説明する作業では、IP Phone と Cisco CallManager の間に NAT を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat service skinny tcp port** *number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat service skinny tcp port** *number* 例： `Router(config)# ip nat service skinny tcp port 20002`	指定された TCP ポートにスキニー プロトコルを設定します。

NATでアプリケーションレベルゲートウェイを使用する場合の設定例

例：NAT 変換用のポートの指定

```
ip nat service skinny tcp port 20002
```

例：保持ポートのイネーブル化

次の例では、サードパーティ コンセントレータの TCP ポート 500 の設定方法を示します。 アクセス リスト 10 が設定されています。

```
ip nat service list 10 IKE preserve-port
access-list 10 permit 10.1.1.1
```

例：SPI マッチングのイネーブル化

次の例に、SPIマッチングをイネーブルにする方法を示します。 アクセス リスト10が設定されています。

```
ip nat service list 10 ESP spi-match
access-list 10 permit 10.1.1.1
```

例：エンドポイントでの SPI マッチングのイネーブル化

```
crypto ipsec nat-transparency spi-matching
```

例：NAT に対する MultiPart SDP サポートのイネーブル化

```
ip nat service allow-multipart
```

例：NAT 変換用のポートの指定

```
ip nat service skinny tcp port 20002
```

次の作業

- NAT の概要、および IP アドレス節約のための NAT 設定については、「IP アドレス節約のための NAT 設定」モジュールを参照してください。
- NAT の検証、モニタリング、およびメンテナンスについては、「NAT のモニタリングおよびメンテナンス」モジュールを参照してください。
- NAT と MPLS VPN の統合については、「MPLS VPN と NAT の統合」モジュールを参照してください。
- ハイ アベイラビリティを得るための NAT の設定については、「ハイ アベイラビリティ用 NAT の設定」モジュールを参照してください。

NATでアプリケーションレベルゲートウェイを使用する場合のその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
NAT コマンド：コマンド構文の詳細、コマンド モード、デフォルト、使用上の注意事項、および例	『Cisco IOS IP Addressing Services Command Reference』
IP アクセス リストへのシーケンス番号づけ	『*IP Access List Sequence Numbering*』
NAT の IP アドレス節約	『*Configuring NAT for IP Address Conservation*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NAT でアプリケーション レベル ゲートウェイを使用する場合の機能情報

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

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

表 *2*：*NAT* でアプリケーション レベル ゲートウェイを使用する場合の機能情報

機能名	リリース	機能の設定情報
ALG - H.323 v6 サポート	Cisco IOS XE Release 3.6S	ALG - H.323 v6 は、H.323 v6 パケットの解析および H.323 メッセージにおける IPv4 アドレス情報のインスペクションおよび変換をサポートします。

機能名	リリース	機能の設定情報
ALG - SCCP バージョン 17 サポート	Cisco IOS XE Release 3.5S	ALG - SCCP バージョン 17 サポート機能により、SCCP ALG で SCCP バージョン 17 パケットを解析できるようになります。 Cisco Unified Communications Manager 7.0 および Cisco Unified Communications Manager 7.0 を使用する IP Phone では、SCCP バージョン 17 メッセージのみをサポートします。 SCCP バージョン 17 パケットは IPv6 パケットをサポートします。 SCCP ALG は SCCP メッセージの IPv4 アドレス情報のインスペクションおよび変換をサポートします。
NAT ALG - SIP REFER 方式	Cisco IOS XE Release 3.2S	NAT ALG - SIP REFER 方式機能は、無人（ブラインド）転送と有人（コンサルタティブ）転送の 2 つのタイプのコール転送をサポートします。
NAT ALG - SIP トランキング サポート	Cisco IOS XE Release 3.2S	NAT ALG - SIP トランキング サポート機能では、ローカル データベースを使用して、SIP トランク内のメディア関連情報をすべて格納します。 各コールのコール ID が、このローカル データベースをインデックス化するために使用されます。
NAT 基本 H.323 ALG サポート	Cisco IOS XE Release 2.1	NAT では、パケット ペイロード内の埋め込み IP アドレスおよびポート番号の変換や、制御チャネルからの新規接続/セッション情報の取得といった、レイヤ 7 プロトコル固有のサービスを処理するために、さまざまな ALG を必要とします。 NAT 基本 H.323 ALG サポート機能は、H.323 メッセージにこれらの固有サービスを提供します。
NAT DNS ALG サポート	Cisco IOS XE Release 2.1	NAT DNS ALG サポート機能では、DNS パケットの変換をサポートします。
NAT FTP ALG サポート	Cisco IOS XE Release 2.1	NAT FTP ALG サポート機能では、FTP パケットの変換をサポートします。

機能名	リリース	機能の設定情報
NAT H.323 RAS	Cisco IOS XE Release 2.4	NAT はすべての H.225 および H. 245 メッセージ タイプ（登録、アドミッション、およびステータス（RAS）プロトコルで送信されるものを含む）をサポートします。 RAS は、ソフトウェア クライアントや VoIP デバイスにより、場所の登録、通話のセットアップ サポートの要求、および帯域幅の制御に使用される多数のメッセージを提供します。RAS メッセージは、H.323 ゲートキーパーに向けて送信されます。
ICMP NAT ALG サポート	Cisco IOS XE Release 2.1	NAT ICMP ALG サポート機能では、ICMP パケットの変換をサポートします。
NAT NetBIOS ALG サポート	Cisco IOS XE Release 3.1S	NAT は、Network Basic Input Output System（NetBIOS）メッセージ変換サポートを提供します。 NAT NetBIOS ALG サポート機能には、デバイスの NetBIOS 固有情報を表示するために、**show platform hardware qfp [active | standby] feature alg statistics netbios** コマンドが導入されました。
NAT NetMeeting Directory（LDAP）	Cisco IOS XE Release 2.4	NAT NetMeeting Directory（LDAP）機能は、NetMeeting Directory LDAP メッセージに ALG サポートを提供します。
NAT RCMD ALG サポート	Cisco IOS XE Release 3.1S	NAT はリモート コマンド実行サービス（RCMD）メッセージの変換サポートを提供します。NAT RCMD ALG サポート機能には、デバイスの RCMD 固有情報を表示するために、**show platform software trace message process qfp active** コマンドが導入されました。
NAT RTSP ALG サポート	Cisco IOS XE Release 3.1S	NAT RTSP ALG サポート機能は、RTSP メッセージ変換サポートを提供します。
ビデオ用 NAT - SCCP	Cisco IOS XE Release 2.4	ビデオ用 NAT - SCCP 機能は、SCCP ビデオ メッセージ変換サポートを提供します。
T.38 Fax Relay のための NAT - SIP ALG Enhancement	Cisco IOS XE Release 2.4.1	T.38 Fax Relay のための NAT - SIP ALG Enhancement 機能では、IP 経由の T.38 Fax Relay の SIP ALG サポートに対する変換サポートを提供します。

機能名	リリース	機能の設定情報
NAT - SIP 拡張方式	Cisco IOS XE Release 2.4	NAT - SIP 拡張方式機能では、SIP の拡張方式をサポートします。
IP Phone から Cisco CallManager への NAT サポート	Cisco IOS XE Release 2.1	IP Phone から Cisco CallManager への NAT サポート機能では、Cisco IP Phone から Cisco CallManager への通信に Cisco SCCP を設定するための NAT サポートを追加します。
IPsec セキュリティ チェックに対する NAT サポート：フェーズ II	Cisco IOS XE Release 2.1	IPsec セキュリティ チェックに対する NAT サポート：フェーズ II 機能は、インターネット キー交換（IKE）および ESP のサポートを提供します。NAPT で設定されたデバイスを通じたトンネル モードでカプセル化する必要はありません。
SIP に対する NAT サポート	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.2S	SIP に対する NAT サポート機能によって、SIP ベースの VoIP ソリューション間に NAT を導入できるようになりました。
NAT TFTP ALG サポート	Cisco IOS XE Release 2.1	NAT TFTP ALG サポート機能では、TFTP パケットの変換をサポートします。
NAT VRF-Aware ALG サポート	Cisco IOS XE Release 2.5	NAT VRF-Aware ALG サポート機能では、サポート対象の ALG を持つプロトコルに対し、VPN ルーティングおよび転送（VRF）をサポートします。
NAT vTCP ALG サポート	Cisco IOS XE Release 3.1S Cisco IOS XE Release 3.2S	NAT vTCP ALG サポート機能では、ALG に対する TCP セグメンテーションおよび再構成を処理するための vTCP サポートを提供します。
NAT を介した IPsec ESP のサポート	Cisco IOS XE Release 2.1	NAT を介した IPsec ESP のサポート機能により、オーバーロード モードまたは PAT モードで設定された NAT デバイス経由で、複数の同時 IPsec ESP トンネルまたは接続をサポートできるようになります。

第 3 章

キャリアグレードネットワークアドレス変換

キャリア グレード ネットワーク アドレス変換（CGN）は、プライベート IPv4 アドレスをパブリック IPv4 アドレスに変換する大規模 NAT です。 CGN では、複数のプライベート IPv4 アドレスを少数の IPv4 アドレスに集約するために、Network Address and Port Translation 方式を採用しています。

このモジュールでは、CGN の概要と、CGN を設定する方法について説明します。

- 機能情報の確認，69 ページ
- キャリア グレード ネットワーク アドレス変換の制約事項，70 ページ
- キャリア グレード ネットワーク アドレス変換について，70 ページ
- キャリア グレード ネットワーク アドレス変換の設定方法，72 ページ
- キャリア グレード ネットワーク アドレス変換の設定例，80 ページ
- キャリア グレード ネットワーク アドレス変換に関するその他の関連資料，81 ページ
- キャリア グレード ネットワーク アドレス変換の機能情報，82 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

キャリア グレード ネットワーク アドレス変換の制約事項

- ボックスツーボックス（B2B）冗長性を持つ非対称ルーティングは、CGNモードではサポートされません。
- B2B 冗長性は、CGN を使用するブロードバンドではサポートされません。B2B はスタンドアロン CGN でサポートされます。
- ブロードバンドは従来の NAT ではサポートされません。
- CGN では、IP セッションはサポートされません。
- IP over Ethernet（IPoE）Intelligent Services Gateway（ISG）セッションは、CGN ではサポートされません。
- CGN の動作モードが **ip nat settings mode cgn** コマンドを使用して設定されている場合、NAT 外部マッピングは自動的にディセーブルになります。

キャリア グレード ネットワーク アドレス変換について

キャリア グレード NAT の概要

ネットワーク アドレス変換（NAT）は、プライベートおよびパブリック IP ネットワークの間に置かれ、非グローバルのプライベート IP アドレスおよびパブリック IP アドレスを使用して変換を行います。 NAT では、1 つ以上のプライベート IP アドレスを、Network Address and Port Translation（NAPT）手法を使用する、1 つ以上の（グローバルにルート可能な）パブリック IP アドレスにダイナミックにマッピングします。 従来、NAT ボックスは、ホーム内の複数のデバイスで設定された複数のプライベート IP アドレスを、サービス プロバイダーによって HGW 上で設定およびプロビジョニングされた単一のパブリック IP アドレスに変換するために、レジデンシャル ホーム ゲートウェイ（HGW）に配置されていました。 サービス プロバイダーは、複数の加入者が単一のグローバル IP アドレスを共有できるような方法で NAT を配置します。 サービス プロバイダーの NAT によって、数百万の NAT 変換に拡張され、この NAT はキャリア グレード NAT（CGN）になります。

CGN では、ネットワークの内部から外部に送信されるパケットには、送信元アドレス ポート変換のみが必要です。宛先アドレス ポート変換は必要ありません。 CGN は従来の NAT と同様にスタンドアロンで使用することも、ブロードバンド アクセス集約とともに使用することもできます。 CGN は、レイヤ 4 リダイレクトなどの Intelligent Services Gateway（ISG）機能およびトラフィック クラスなどの加入者サービスと共存します。

CGN は、**ip nat settings mode cgn** コマンドを使用して設定できます。 デフォルトまたは従来の NAT の動作モードに変更するには、**ip nat settings mode default** コマンドを使用します。 CGN モードでは、NAT 外部マッピングは設定できません。 ただし、デフォルトの NAT モードから CGN

モードに変更する場合、既存の外部マッピングをすべて削除する必要があります。 すべての外部マッピングを削除し、新しい外部マッピングが設定されないようにするには、**no ip nat settings support mapping outside** コマンドを使用します。 NAT を外部に設定するために使用されるコマンドの **no** 形式を使用することによっても、外部マッピングを削除できます。

宛先情報は保存されないため、CGN により、サポート可能な NAT 変換の数の拡張性が向上します。

CGN は、次の内容をサポートします。

- 従来の NAT でサポートされるすべてのアプリケーション レベル ゲートウェイ（ALG）。 サポートされる ALG の詳細については、『*IP* アドレッシング：*NAT* コンフィギュレーション ガイド』の「*NAT* でのアプリケーション レベル ゲートウェイの使用」モジュールを参照してください。
- エンドポイント独立マッピングとエンドポイント独立フィルタリング。
- VRF-Aware ソフトウェア インフラストラクチャ（VASI）およびポリシーベース ルーティング（PBR）を使用したヘアピニング。 ヘアピニングは、2 つの加入者が同じ NAT デバイスの背後にいるが、グローバル IP アドレスを使用してのみ互いを確認できる場合に行われます。
- ボックス間およびボックス内冗長性。
- 合法的傍受。
- NAT の High-Speed ロギング（HSL）レコードのロギング。 HSL の詳細については、『*IP* アドレッシング：*NAT* コンフィギュレーション ガイド』の「*NAT* のモニタリングおよびメンテナンス」モジュールの「NAT の High-Speed ロギング」の項を参照してください。
- 冗長またはスタンバイ出力点を介した接続を提供する複数の外部インターフェイスをサポートするための機能である、マルチホーミング。 設定されたルーティング トポロジによっては、外部インターフェイスとマークされているすべての出力インターフェイスで、以前に作成された変換を使用できます。
- 15 分間の TCP タイムアウト値。
- VPN ルーティングおよび転送（VRF）対応 NAT。

ブロードバンド アクセス集約のキャリア グレード NAT サポート

キャリア グレード ネットワーク アドレス変換（CGN）を独立した機能として設定することも、ブロード アクセス集約とともに CGN を使用することもできます。

ブロードバンド アクセス集約により、ケーブル、デジタル加入者線（DSL）、イーサネット、ISDN、および社内 VPN、サードパーティ製アプリケーション、およびインターネットに接続されているワイヤレス デバイスといった複数のテクノロジー間での接続が可能になります。

PPP over Ethernet（PPPoE）は、ネットワーク上のホストを、単純なブリッジング デバイス経由でリモート集約コンセントレータに接続します。 PPPoE は、世界中のブロードバンド ネットワークで一般的に使用されるアクセス プロトコルです。

PPPoE を CGN で使用するには、仮想テンプレートおよび RADIUS サーバでネットワーク アドレス変換（NAT）の内部設定がサポートされている必要があります。 NAT の内部設定は、RADIUS 認証の一部としてダウンロードする必要があります。 仮想テンプレートで **ip nat inside** コマンドを設定します。これは、**ip nat inside** 設定を継承する仮想アクセス インターフェイスにクローンされます。 RADIUS サーバで NAT の内部設定をサポートするには、**aaa policy interface-config allow-subinterface** コマンドを設定するか、加入者ごとに RADIUS プロファイル内で Cisco 属性と値のペア（AV ペア）の「lcp:allow-subinterface=yes」および「lcp:interface-config=ip nat inside」を設定します。

グローバル ルーティング テーブル内または VRF インスタンスで PPPoE セッションを終了できます。

CGN では、デュアル スタック（IPv4 および IPv6）PPP セッションをサポートします。 ただし、NAT の対象となるのは IPv4 トラフィックのみです。 IPv6 トラフィックは変換されません。これは、IPv6 ルーティング設定に従ってルーティングされます。

キャリア グレード ネットワーク アドレス変換の設定方法

ネットワーク設定に基づいて、スタティック、ダイナミック、またはダイナミック PAT キャリア グレード NAT を設定できます。

（注） キャリア グレード NAT が動作するためには、次の作業で説明する設定のいずれか 1 つ以上を使用する必要があります。

スタティック キャリア グレード NAT の設定

スタティック アドレス変換（スタティック NAT）により、ローカル アドレスとグローバル アドレスを 1 対 1 でマッピングできるようになります。 内部送信元アドレスのスタティック NAT をイネーブルにするには、**ip nat inside source static** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat settings mode cgn**
4. **ip nat inside source static** *local-ip global-ip*
5. **interface virtual-template** *number*
6. **ip nat inside**
7. **exit**
8. **interface** *type number*
9. **ip nat outside**
10. **end**
11. **show ip nat translations** [**verbose**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat settings mode cgn** 例： `Device(config)# ip nat settings mode cgn`	CGN 動作モードをイネーブルにします。
ステップ 4	**ip nat inside source static** *local-ip global-ip* 例： `Device(config)# ip nat inside source static 192.168.2.1 192.168.34.2`	内部送信元アドレスのスタティック キャリア グレード NAT をイネーブルにします。
ステップ 5	**interface virtual-template** *number* 例： `Device(config)# interface virtual-template 1`	仮想アクセス インターフェイスの作成時にダイナミックに設定して適用できる仮想テンプレート 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。

	コマンドまたはアクション	目的
ステップ 6	**ip nat inside** 例： `Device(config-if)# ip nat inside`	インターフェイスが内部ネットワーク（NAT 変換の対象となるネットワーク）に接続されることを示します。
ステップ 7	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 8	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ip nat outside** 例： `Device(config-if)# ip nat outside`	インターフェイスが外部ネットワークに接続されることを示します。
ステップ 10	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 11	**show ip nat translations** [**verbose**] 例： `Device# show ip nat translations`	アクティブな NAT 変換を表示します。

例

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

```
Device# show ip nat translations

Pro  Inside global         Inside local          Outside local         Outside global
udp  10.5.5.1:1025          192.0.2.1:4000        ---                    ---
udp  10.5.5.1:1024          192.0.2.3:4000        ---                    ---
udp  10.5.5.1:1026          192.0.2.2:4000        ---                    ---

Total number of translations: 3
```

次に、**show ip nat translations verbose** コマンドの出力例を示します。

```
Device# show ip nat translations verbose

Pro  Inside global         Inside local          Outside local         Outside global
udp  10.5.5.1:1025          192.0.2.1:4000        ---                    ---
  create: 02/15/12 11:38:01, use: 02/15/12 11:39:02, timeout: 00:00:00
  Map-Id(In): 1
  Mac-Address: 0000.0000.0000    Input-IDB: TenGigabitEthernet1/1/0
```

```
  entry-id: 0x0, use_count:1

udp  10.5.5.1:1024          192.0.2.3:4000        ---                   ---
  create: 02/15/12 11:38:00, use: 02/15/12 11:39:02, timeout: 00:00:00
  Map-Id(In): 1
  Mac-Address: 0000.0000.0000    Input-IDB: TenGigabitEthernet1/1/0
  entry-id: 0x0, use_count:1

udp  10.5.5.1:1026          192.0.2.2:4000        ---                   ---
  create: 02/15/12 11:38:00, use: 02/15/12 11:39:02, timeout: 00:00:00
  Map-Id(In): 1
  Mac-Address: 0000.0000.0000    Input-IDB: TenGigabitEthernet1/1/0
  entry-id: 0x0, use_count:1

Total number of translations: 3
```

ダイナミック キャリア グレード NAT の設定

ダイナミック アドレス変換（ダイナミック NAT）では、未登録の IP アドレスを、登録済み IP アドレス プールの登録済み IP アドレスにマッピングします。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat settings mode cgn**
4. **access-list** *standard-access-list-number* **permit** *source wildcard*
5. **access-list** *standard-access-list-number* **permit** *source wildcard*
6. **route-map** *map-tag*
7. **match ip address** [*access-list-number*]
8. **match ip next-hop** [*access-list-number*]
9. **exit**
10. **ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length*
11. **ip nat inside source route-map** *name* **pool** *name*
12. **interface virtual-template** *number*
13. **ip nat inside**
14. **exit**
15. **interface** *type number*
16. **ip nat outside**
17. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat settings mode cgn** 例： `Device(config)# ip nat settings mode cgn`	CGN 動作モードをイネーブルにします。
ステップ 4	**access-list** *standard-access-list-number* **permit** *source wildcard* 例： `Device(config)# access-list 1 permit 10.1.1.0 0.0.0.255`	標準アクセス リストを定義し、ホストを指定します。 • この手順で定義するアクセス リスト 1 は、**match ip address** コマンドにより使用されます。
ステップ 5	**access-list** *standard-access-list-number* **permit** *source wildcard* 例： `Device(config)# access-list 2 permit 10.5.5.0 0.0.0.255`	標準アクセス リストを定義し、ホストを指定します。 • この手順で定義するアクセス リスト 2 は、**match ip next-hop** コマンドにより使用されます。
ステップ 6	**route-map** *map-tag* 例： `Device(config)# route-map nat-route-map`	ルーティング プロトコル間でルートを再配布する条件を定義するか、ポリシー ルーティングをイネーブルにしてルート 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 7	**match ip address** [*access-list-number*] 例： `Device(config-route-map)# match ip address 1`	標準アクセス リスト、拡張アクセス リスト、またはプレフィックス リストで許可されている宛先ネットワーク番号アドレスを持つルートを配布するか、パケットに対してポリシー ルーティングを実行します。
ステップ 8	**match ip next-hop** [*access-list-number*] 例： `Device(config-route-map)# match ip next-hop 2`	指定のアクセス リストのいずれかが通過する、ネクスト ホップ ルータ アドレスを持ったルートをすべて再配布します。
ステップ 9	**exit** 例： `Device(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、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length*	NAT で使用される IP アドレス プールを定義します。

	コマンドまたはアクション	目的
	例： `Device(config)# ip nat pool nat-pool 10.1.1.1 10.1.254.254 prefix-length 16`	
ステップ 11	**ip nat inside source route-map** *name* **pool** *name* 例： `Device(config)# ip nat inside source route-map nat-route-map pool nat-pool`	内部送信元アドレスのダイナミック NAT をイネーブルにします。
ステップ 12	**interface virtual-template** *number* 例： `Device(config)# interface virtual-template 1`	仮想アクセス インターフェイスの作成時にダイナミックに設定して適用できる仮想テンプレート 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 13	**ip nat inside** 例： `Device(config-if)# ip nat inside`	インターフェイスが内部ネットワーク（NAT 変換の対象となるネットワーク）に接続されることを示します。
ステップ 14	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 15	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 16	**ip nat outside** 例： `Device(config-if)# ip nat outside`	インターフェイスが外部ネットワークに接続されることを示します。
ステップ 17	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ダイナミック ポート アドレスのキャリア グレード NAT の設定

ポート アドレス変換（PAT）（オーバーロード）は、複数の異なるポートを使用して、複数の未登録 IP アドレスを単一の登録済み IP アドレスにマッピングする（多対 1 マッピング）ダイナミック NAT の形式です。 PAT を使用すると、使用できる正規のグローバル IP アドレスが 1 つのみでも、数千のユーザをインターネットに接続することができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat settings mode cgn**
4. **ip nat inside source list** *number* **pool** *name* [**overload**]
5. **ip nat pool** *name start-ip end-ip* **netmask** *netmask*
6. **access-list** *standard-access-list-number* **permit** *source wildcard*
7. **interface virtual-template** *number*
8. **ip nat inside**
9. **exit**
10. **interface** *type number*
11. **ip nat outside**
12. **end**
13. **show ip nat statistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat settings mode cgn** 例： `Device(config)# ip nat settings mode cgn`	CGN 動作モードをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**ip nat inside source list** *number* **pool** *name* [**overload**] 例： `Device(config)# ip nat inside source list 1 pool nat-pool overload`	ルータで、複数のローカル アドレスに対して 1 つのグローバル アドレスを使用できるようにします。 • **overload** キーワードを設定すると、各内部ホストの TCP または UDP ポート番号によって、同じローカル IP アドレスを使用して複数の会話が区別されます。 • **overload** キーワードにより、オーバーロード（PAT）が設定されます。
ステップ 5	**ip nat pool** *name start-ip end-ip* **netmask** *netmask* 例： `Device(config)# ip nat pool nat-pool 10.1.1.1 10.1.254.254 netmask 255.255.0.0`	NAT で使用される IP アドレス プールを定義します。
ステップ 6	**access-list** *standard-access-list-number* **permit** *source wildcard* 例： `Device(config)# access-list 1 permit 172.16.0.0 255.255.0.0`	標準アクセス リストを定義し、ホストを指定します。
ステップ 7	**interface virtual-template** *number* 例： `Device(config)# interface virtual-template 1`	仮想アクセスインターフェイスの作成時にダイナミックに設定して適用できる仮想テンプレート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 8	**ip nat inside** 例： `Device(config-if)# ip nat inside`	インターフェイスが内部ネットワーク（NAT変換の対象となるネットワーク）に接続されることを示します。
ステップ 9	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/2`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 11	**ip nat outside** 例： `Device(config-if)# ip nat outside`	インターフェイスが外部ネットワークに接続されることを示します。
ステップ 12	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 13	**show ip nat statistics** 例： `Device# show ip nat statistics`	NAT の統計情報を表示します。

例

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

```
Device# show ip nat statistics

Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Outside interfaces:
  TenGigabitEthernet2/0/0, TenGigabitEthernet2/1/0, TenGigabitEthernet2/2/0
  TenGigabitEthernet2/3/0
Inside interfaces:
  TenGigabitEthernet1/0/0, TenGigabitEthernet1/1/0, TenGigabitEthernet1/2/0
  TenGigabitEthernet1/3/0
Hits: 59230465  Misses: 3
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 102 pool mypool refcount 3
 pool mypool: netmask 255.255.255.0
        start 10.5.5.1 end 10.5.5.5
        type generic, total addresses 5, allocated 1 (20%), misses 0
nat-limit statistics:
 max entry: max allowed 2147483647, used 3, missed 0
Pool stats drop: 0  Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0
```

キャリア グレード ネットワーク アドレス変換の設定例

例：スタティック キャリア グレード NAT の設定

```
Device# configure terminal
Device(config)# ip nat settings mode cgn
```

```
Device(config)# ip nat inside source static 192.168.2.1 192.168.34.2
Device(config)# interface virtual-template 1
Device(config-if)# ip nat inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# ip nat outside
Device(config-if)# end
```

例：ダイナミック キャリア グレード NAT の設定

```
Device# configure terminal
Device(config)# ip nat settings mode cgn
Device(config)# access-list 1 permit 10.1.1.0 0.0.0.255
Device(config)# access-list 2 permit 10.5.5.0 0.0.0.255
Device(config)# route-map nat-route-map
Device(config-route-map)# match ip address 1
Device(config-route-map)# match ip next-hop 2
Device(config-route-map)# exit
Device(config)# ip nat pool nat-pool 10.1.1.1 10.1.254.254 prefix-length 16
Device(config)# ip nat inside source route-map nat-route-map pool nat-pool
Device(config)# interface virtual-template 1
Device(config-if)# ip nat inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# ip nat outside
Device(config-if)# end
```

例：ダイナミック ポート アドレス キャリア グレード NAT の設定

```
Device# configure terminal
Device(config)# ip nat settings mode cgn
Device(config)# ip nat inside source list 1 pool nat-pool overload
Device(config)# ip nat pool nat-pool 10.1.1.1 10.1.254.254 netmask 255.255.0.0
Device(config)# access-list 1 permit 172.16.0.0 255.255.0.0
Device(config)# interface virtual-template 1
Device(config-if)# ip nat inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/0/3
Device(config-if)# ip nat outside
Device(config-if)# end
```

キャリア グレード ネットワーク アドレス変換に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
NAT コマンド	『IP Addressing Command Reference』
NAT ALG	「Using Application-Level Gateways with NAT」

関連項目	マニュアル タイトル
HSL メッセージ	「Monitoring and Maintaining NAT」

標準および RFC

標準/RFC	タイトル
RFC 4787	『*Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*』
RFC 5582	『*Location-to-URL Mapping Architecture and Framework*』

シスコのテクニカル サポート

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

キャリア グレード ネットワーク アドレス変換の機能情報

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

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

表 *3*：キャリア グレード ネットワーク アドレス変換の機能情報

機能名	リリース	機能情報
キャリア グレード ネットワーク アドレス変換	Cisco IOS XE Release 3.6S	キャリア グレード ネットワーク アドレス変換（CGN）は、プライベート IPv4 アドレスをパブリック IPv4 アドレスに変換する大規模 NAT です。 CGN では、複数のプライベート IPv4 アドレスを少数の IPv4 アドレスに集約するために、Network Address and Port Translation 方式を採用しています。 **ip nat settings mode** および **ip nat settings support mapping outside** コマンドが導入または変更されました。

第 4 章

ハイ アベイラビリティ用 NAT の設定

このモジュールでは、要求が高まりつつある強い復元力を持つ IP ネットワークをサポートするネットワーク アドレス変換（NAT）を設定するための手順について説明します。 このネットワーク復元力は、NAT 境界でのリンクやルータの障害に影響を受けることなくアプリケーションを接続し続けることが求められる状況で必要です。

- 機能情報の確認，85 ページ
- ハイ アベイラビリティ用 NAT 設定の前提条件，86 ページ
- ハイ アベイラビリティ用 NAT の制限事項，86 ページ
- ハイ アベイラビリティ用 NAT の設定について，86 ページ
- ハイ アベイラビリティ用 NAT の設定方法，90 ページ
- ハイ アベイラビリティ用の NAT の設定例，104 ページ
- その他の関連資料，106 ページ
- ハイ アベイラビリティ用 NAT の設定に関する機能情報，108 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

ハイ アベイラビリティ用 NAT 設定の前提条件

- このモジュールの作業を実行する前に、「IP アドレス節約のための NAT 設定」モジュールで説明されている概念をよく理解しておく必要があります。
- このモジュールの作業で使用する必要があるアクセス リストはすべて、NAT の設定作業を始める前に設定しておく必要があります。 アクセス リストの設定方法については、『IP Access List Sequence Numbering』マニュアルを参照してください。

（注） NAT コマンドで使用するアクセス リストが指定されている場合、NAT は一般によく使用される **permit ip any any** コマンドを、このアクセス リストではサポートしません。

ハイ アベイラビリティ用 NAT の制限事項

- シスコは Cisco IOS SNAT の販売終了およびサポート終了を発表しました。 詳細については、『End-of-Sale and End-of-Life Announcement for the Cisco IOS Stateful Failover of Network Address Translation (SNAT)』マニュアルを参照してください。
- アドレス解決プロトコル（ARP）クエリーには、常にホットスタンバイ ルーティング プロトコル（HSRP）のアクティブ ルータが応答します。 アクティブな HSRP ルータが失敗した場合、アップストリーム デバイスは新しい HSRP アクティブ ルータを指し、（もう利用できない可能性のある）元のアクティブ ルータを指す ARP エントリは持ちません。

ハイ アベイラビリティ用 NAT の設定について

ステートフル NAT

ステートフル NAT（SNAT）で、ダイナミックにマップされた NAT セッションを継続してサービスすることができます。 スタティックに定義されたセッションが冗長性の恩恵を受けるのに SNAT は必要ありません。 SNAT がない場合、ダイナミック NAT マッピングを使用するセッションは、重大な障害が発生した場合に深刻な影響を受け、再確立する必要があります。

SNAT は、ペイロード変換を行う必要のないプロトコルで使用することができます。

Outside-to-Inside 非対称 ALG の NAT ステートフル フェールオーバー サポート

非対称の外部から内部およびアプリケーション層ゲートウェイ（ALG）サポート用NATステートフル フェールオーバーで、外部から内部の複数のルーティング パスを許可し、パケットごとのロード バランシングを改善することで非対称パスの処理能力を改善します。 この機能はまた、Voice over IP、FTP、ドメイン ネーム システム（DNS）アプリケーションといった、埋め込み IP アドレッシングを含むトラフィックとのシームレスなフェールオーバー変換IPセッションを可能にします。

HSRP との相互作用

SNAT は、ホット スタンバイ ルーティング プロトコル（HSRP）で動作し、冗長性を持たせるように設定することができます。 アクティブおよびスタンバイ ステートの変更は、HSRP により管理されます。

SNAT は、特定のデータグラムを転送する作業に、さらにグローバルなコンテキストを適用します。 転送と並行して、アプリケーションのステートを理解することが考慮されます。 デバイスは、潜在的な失敗を避けるために、フローおよびデータを送信しているアプリケーションへの影響が少ないアクションを行うことができます。 ステートフルなコンテキストを共有する複数の NAT ルータは連携して動作することができ、サービスの可用性を高めることができます。

変換グループ

2 つ以上のネットワーク アドレス トランスレータは、変換グループとして機能します。 グループメンバーの 1 つは、IP アドレス情報の変換を必要とするトラフィックを処理します。 トランスレータは、アクティブなフローが発生するとバックアップ用トランスレータに通知します。 バックアップ用トランスレータは、アクティブなトランスレータからの情報を利用して重複した変換テーブル エントリを準備することができ、重大な障害でアクティブなトランスレータが妨害された場合、トラフィックは迅速にバックアップ用トランスレータに切り替えられます。 変換のステートが先に定義されていたのと同じネットワーク アドレス変換が使用されるため、トラフィックのフローは継続します。

ARP でのアドレス解決

IPのデバイスは、ローカルアドレス（ローカルセグメントまたはLANのデバイスを一意に識別）とネットワーク アドレス（デバイスが属するネットワークを識別）の両方を持つことができます。 ローカル アドレスは、より正確にはデータリンク アドレスとして知られています。その理由は、ローカル アドレスはパケット ヘッダーのデータリンク層（OSI モデルの第 2 層）の部分にあり、データリンクデバイス（ブリッジやすべてのデバイスインターフェイスなど）によって読み取られるからです。 ローカル アドレスが MAC アドレスと呼ばれるのは、データリンク層の MAC サブレイヤがそのレイヤのアドレスを処理するからです。

イーサネット上のデバイスと通信するために、たとえばCisco IOS ソフトウェアは、まずそのデバイスの 48 ビット MAC、つまりローカル データリンク アドレスを決定する必要があります。 IP アドレスからローカル データリンク アドレスを決定する処理は、アドレス解決と呼ばれています。 ローカル データリンク アドレスから IP アドレスを決定する処理は、逆アドレス解決と呼ばれています。

このソフトウェアは、アドレス解決のフォームとして、アドレス解決プロトコル（ARP）、プロキシ ARP、プローブ（ARP に類似）の 3 種類を使用します。 このソフトウェアは、逆アドレス解決プロトコル（RARP）も使用しています。 ARP、プロキシ ARP、RARP はそれぞれ、RFC 826、1027、903 で定義されています。 プローブは、Hewlett-Packard Company（HP）が IEEE-802.3 ネットワークで使用するために開発したプロトコルです。

ARP は、IP アドレスをメディアや MAC アドレスに関連付けるために使用されます。 ARP は IP アドレスを入力とし、関連するメディアのアドレスを決定します。 メディアまたは MAC アドレスが決定すると、IP アドレスまたはメディア アドレスの関連付けは、すぐ取得できるように ARP のキャッシュに保管されます。 その後、IP データグラムがリンク層フレームにカプセル化され、ネットワークを通じて送信されます。 イーサネット以外の IEEE 802 ネットワークにおける IP データグラムのカプセル化および ARP 要求/応答については、サブネットワーク アクセス プロトコル（SNAP）で規定されています。

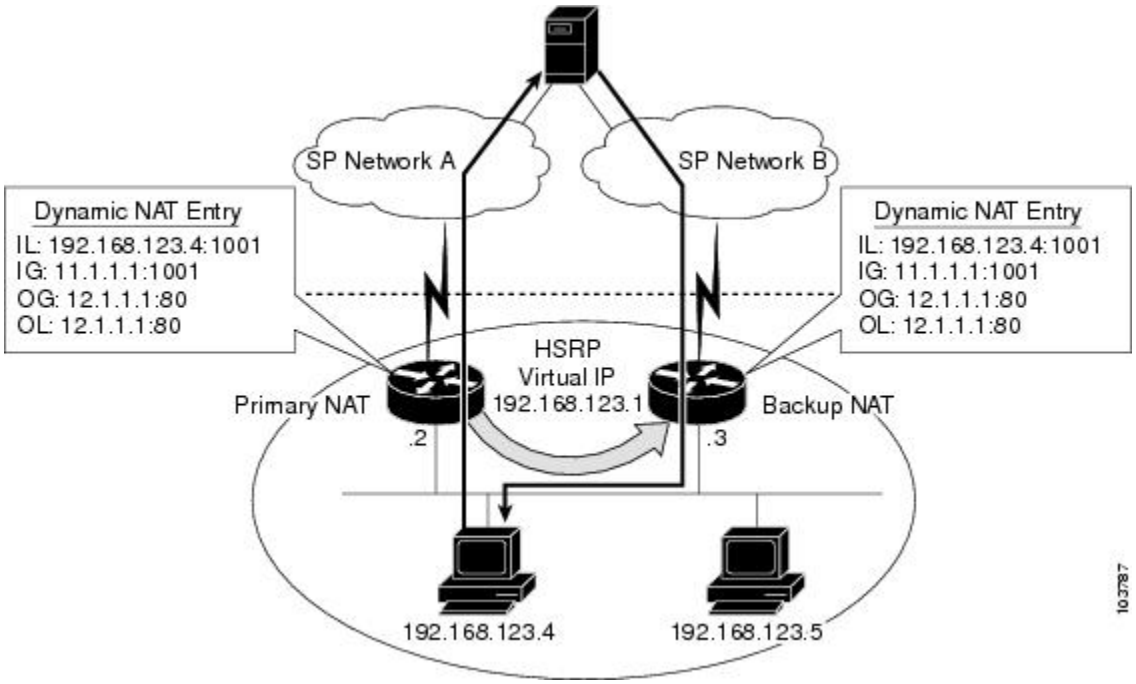
非対称の外部から内部サポート用ステートフル フェールオーバー

非対称の外部から内部サポート用ステートフル フェールオーバーにより、2 つの NAT ルータがプライマリおよびバックアップ計画に参加することができます。 ルータの 1 つはプライマリ NAT ルータに選ばれ、2 つ目のルータはバックアップ ルータとして動作します。 トラフィックがプライマリ NAT ルータでアクティブに変換されているとき、プライマリ NAT ルータは、NAT 変換テーブル エントリからの NAT 変換ステートでバックアップ NAT ルータを更新します。 プライマリ NAT ルータが失敗するか、休止した場合、バックアップ NAT ルータが自動的に引き継ぎます。 プライマリ ルータが復帰するとサービスを引き継ぎ、バックアップ NAT ルータからの更新を要求します。 戻りのトラフィックはプライマリまたはバックアップいずれかの NAT トランスレータが処理し、NAT 変換の完全性は維持されます。

バックアップ NAT ルータが非対称な IP トラフィックを受信し、そのパケットの NAT を実行するとき、プライマリ NAT ルータを更新して、プライマリとバックアップ両方の NAT 変換テーブルが確実に同期し続けているようにします。

次の図に、非対称の外部から内部および ALG サポート用 NAT ステートフル フェールオーバー機能の一般的な設定を示します。

図 *4*：ステートフル *NAT* 非対称の外部から内部サポート



ALG 用ステートフル フェールオーバー

ステートフル フェールオーバーに組み込まれたアドレス指定拡張で、セカンダリまたはバックアップの NAT ルータは NAT と IP トラフィックの配信を適切に扱うことができます。 NAT は、NAT機能を設定されているインターフェイスに入ってくる IP トラフィックすべてを検査します。検査の内容は、着信トラフィックを一連の変換ルールと照合することで、一致していればアドレス変換を実行します。 次に例を示します。

- 送信元アドレス範囲の照合
- 特定の宛先アドレス範囲の照合
- NAT に既知のアプリケーション リストと照合します。これらのアプリケーションは、コントロール プレーン ネゴシエーションやアプリケーション プロトコル内に埋め込まれた発信元 IP アドレスに特定の送信元ポートが必要な場合があります。

送信元ポートや IP アドレス情報を埋め込んだアプリケーションやプロトコルには、次のようなものがあります。

- H.323 Registration, Admission, and Status（RAS）プロトコル
- DNS クエリー

- NetMeeting Internet Locator Server（ILS）
- インターネット制御メッセージ プロトコル（ICMP）
- シンプル メール転送プロトコル（SMTP）
- ポイントツーポイント トンネリング プロトコル（PPTP）
- ネットワーク ファイル システム（NFS）

Cisco IOS NAT がサポートする最新の ALG プロトコルの全リストについては、次を参照してください。

http://www.cisco.com/en/US/tech/tk648/tk361/tech_brief09186a00801af2b9.html

ハイ アベイラビリティ用 NAT の設定方法

NAT ステートフル フェールオーバーの設定

ネットワーク アドレス変換の NAT ステートフル フェールオーバー機能は、ステートフル フェールオーバー機能のフェーズ 1 です。 複数の Network Address Translator を変換グループとして動作させる機能のサポートが導入されました。 NAT を実行中のバックアップ ルータは、アクティブなトランスレータが失敗する障害がおこると、変換サービスを提供します。 HTTP や telnet のようにペイロード変換が不要なプロトコルは、ステートフル NAT（SNAT）でサポートされています。

ここでは、次の手順について説明します。

NAT ステートフル フェールオーバー設定の制約事項

次のアプリケーションとプロトコルは、フェーズ I でサポートされていません。

- Application Level Gateway（ALG）
- FTP
- NetMeeting Directory（ILS）
- RAS
- SIP
- Skinny
- TFTP
- 非対称ルーティング

SNAT 機能には下位互換性がありません。 SNAT 機能およびこれらの機能が導入されているリリースについては、「ハイ アベイラビリティ用 NAT の設定に関する機能情報」および「Scalability for Stateful NAT」を参照してください。

HSRP での SNAT の設定

ルータ バックアップ装置を用意するためにHSRP を使用してステートフルNAT を設定するには、この作業を実行します。

（注） この作業は、**アクティブ**および**スタンバイ** ルータの両方で実行する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **standby** [*group-name*] **ip**[*ip-address*[**secondary**]]
5. **exit**
6. **ip nat stateful id** *id-number* {**redundancy** *name* **mapping-id** *map-number*}
7. **ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length*
8. **ip nat inside source** {**route-map** *name* **pool** *pool-name* **mapping-id** *map-number*} [**overload**]
9. **exit**
10. **show ip snat distributed verbose**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface ethernet 1/1`	インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**standby** [*group-name*] **ip**[*ip-address*[**secondary**]] 例： `Router(config-if)# standby SNATHSRP ip 10.1.1.1`	HSRP ルーティング プロトコルをイネーブルにします。
ステップ 5	**exit** 例： `Router(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip nat stateful id** *id-number* {**redundancy** *name* **mapping-id** *map-number*} 例： `Router(config)# ip nat stateful id 1 redundancy snathsrp mapping-id 10`	HSRP 用に設定されたルータで SNAT を指定します。
ステップ 7	**ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length* 例： `Router(config)# ip nat pool snatpool1 10.1.1.1 10.1.1.9 prefix-length 24`	IP アドレスのプールを定義します。
ステップ 8	**ip nat inside source** {**route-map** *name* **pool** *pool-name* **mapping-id** *map-number*} [**overload**] 例： `Router(config)# ip nat inside source route-map rm-101 pool snatpool1 mapping-id 10 overload`	HSRP 変換グループのステートフル NAT をイネーブルにします。
ステップ 9	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 10	**show ip snat distributed verbose** 例： `Router# show ip snat distributed verbose`	（任意）アクティブなステートフル NAT 変換を表示します。

プライマリ（アクティブ）ルータでの SNAT の設定

ご使用のプライマリ SNAT ルータを手動で設定するには、この作業を実行します。 この作業の完了後、「バックアップ（スタンバイ）ルータの SNAT の設定」の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat stateful id** *id-number* **primary** *ip-address* **peer** *ip-address* **mapping-id** *map-number*
4. **ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length*
5. **ip nat inside source route-map** *name* **pool** *pool-name* **mapping-id** *map-number* [**overload**]
6. **exit**
7. **show ip snat distributed verbose**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat stateful id** *id-number* **primary** *ip-address* **peer** *ip-address* **mapping-id** *map-number* 例： `Router(config)# ip nat stateful id 1 primary 10.10.10.10 peer 10.22.22.22 mapping-id 10`	プライマリ ルータのステートフル NAT を指定します。
ステップ 4	**ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length* 例： `Router(config)# ip nat pool SNATPOOL1 10.1.1.1 10.1.1.9 prefix-length 24`	IP アドレスのプールを定義します。

	コマンドまたはアクション	目的
ステップ 5	**ip nat inside source route-map** *name* **pool** *pool-name* **mapping-id** *map-number* [**overload**] 例： `Router(config)# ip nat inside source route-map rm-101 pool snatpool1 mapping-id 10 overload`	HSRP 変換グループのステートフル NAT をイネーブルにします。
ステップ 6	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 7	**show ip snat distributed verbose** 例： `Router# show ip snat distributed verbose`	（任意）アクティブなステートフル NAT 変換を表示します。

バックアップ（スタンバイ）ルータの SNAT の設定

ご使用のバックアップ（スタンバイ）SNAT ルータを手動で設定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat stateful id** *id-number* **backup** *ip-address* **peer** *ip-address* **mapping-id** *map-number*
4. **ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length*
5. **ip nat inside source route-map** *name* **pool** *pool-name* **mapping-id** *map-number* [**overload**]
6. **exit**
7. **show ip snat distributed verbose**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat stateful id** *id-number* **backup** *ip-address* **peer** *ip-address* **mapping-id** *map-number* 例： `Router(config)# ip nat stateful id 1 backup 10.2.2.2 peer 10.10.10.10 mapping-id 10`	バックアップ ルータのステートフル NAT を指定します。
ステップ 4	**ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length* 例： `Router(config)# ip nat pool SNATPOOL1 10.1.1.1 10.1.1.9 prefix-length 24`	IP アドレスのプールを定義します。
ステップ 5	**ip nat inside source route-map** *name* **pool** *pool-name* **mapping-id** *map-number* [**overload**] 例： `Router(config)# ip nat inside source route-map rm-101 pool snatpool1 mapping-id 10 overload`	HSRP 変換グループのステートフル NAT をイネーブルにします。
ステップ 6	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 7	**show ip snat distributed verbose** 例： `Router# show ip snat distributed verbose`	（任意）アクティブなステートフル NAT 変換を表示します。

非対称の外部から内部および ALG サポート用 NAT ステートフル フェールオーバーの設定

プライマリ NAT ルータが使用不可でない限り、ステートフル NAT フェーズ I には、NAT 変換エントリを制御したプライマリ NAT ルータを通過するセッションすべてが必要です。この要件で、NAT セッション制御に関連するパケットで、プライマリが認識せずにバックアップが移動される可能性を排除し、変換情報の完全性を保証します。同期した IP セッションがない場合、最終的に NAT は IP セッション エントリをタイム アウトし、その結果、シーケンスを外れた IP セッション ステートになります。

ここでは、次の手順について説明します。

非対称の外部から内部および ALG サポート用 NAT ステートフル フェールオーバー機能設定の前提条件

各ルータのネットワーク アドレス変換（NAT）の設定は同一になっている必要があります。

ステートフル フェールオーバーの非対称の外部から内部拡張には、次のような利点があります。

- 外部から内部の複数のルーティング パスをサポートする機能
- 外部から内部の非対称ルーティングのパケットごとのロード バランシングを処理する機能

HSRP での SNAT の設定

ご使用のホットスタンバイ ルータ プロトコル（HSRP）ルータをステートフル ネットワーク アドレス変換（SNAT）で設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **standby** [*group-name]* **ip**[*ip-address*[**secondary**]]
5. **exit**
6. **ip nat stateful id** *ip-address* **redundancy** *group-name* **mapping-id** *map-id*
7. **ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length*
8. **ip nat inside source static route-map** *name* **pool** *pool-name* **mapping-id** *map-id* [**overload**]
9. **ip nat inside destination list** *number* **pool** *name* **mapping-id** *map-id*
10. **ip nat outside source static** *global-ip local-ip* **extendable mapping-id** *map-id*
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface ethernet 1/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**standby** [*group-name]* **ip**[*ip-address*[**secondary**]] 例： `Router(config-if)# standby SNATHSRP ip 11.1.1.1 secondary`	HSRP ルーティング プロトコルをイネーブルにします。
ステップ 5	**exit** 例： `Router(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip nat stateful id** *ip-address* **redundancy** *group-name* **mapping-id** *map-id* 例： `Router(config)# ip nat stateful id 1 redundancy snathsrp mapping-id 10`	HSRP 用に設定されたルータで SNAT を指定します。
ステップ 7	**ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length* 例： `Router(config)# ip nat pool snatpool1 11.1.1.1 11.1.1.9 prefix-length 24`	IP アドレスのプールを定義します。

	コマンドまたはアクション	目的
ステップ 8	**ip nat inside source static route-map** *name* **pool** *pool-name* **mapping-id** *map-id* [**overload**] 例： `Router(config)# ip nat inside source static route-map rm-101 pool snatpool2 mapping-id 10 overload`	HSRP 変換グループのステートフル NAT をイネーブルにします。
ステップ 9	**ip nat inside destination list** *number* **pool** *name* **mapping-id** *map-id* 例： `Router(config)# ip nat inside destination list 1 pool snatpool2 mapping-id 10`	ローカル SNAT ルータで、ローカルに作成されたエントリの特定のセットをピア SNAT ルータに配布できるようにします。
ステップ 10	**ip nat outside source static** *global-ip local-ip* **extendable mapping-id** *map-id* 例： `Router(config)# ip nat outside source static 1.1.1.1 2.2.2.2 extendable mapping-id 10`	HSRP 変換グループのステートフル NAT をイネーブルにします。
ステップ 11	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了します。 • 設定を保存し、コンフィギュレーション モードを終了するには、**end** コマンドを使用します。

SNAT プライマリ バックアップの設定

非対称の外部から内部および ALG サポート用 NAT ステートフル フェールオーバー機能をイネーブルにするには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat stateful id** *id-number* **primary** *ip-address* **peer** *ip-address* **mapping-id** *map-id*
4. **ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length*
5. **ip nat inside source static route-map** *name* **pool** *pool-name* **mapping-id** *map-id* [**overload**]
6. **ip nat inside destination list** *number* **pool** *name* **mapping-id** *map-id*
7. **ip nat outside source Static** *global-ip local-ip* **extendable mapping-id** *map-id*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat stateful id** *id-number* **primary** *ip-address* **peer** *ip-address* **mapping-id** *map-id* 例： `Router(config)# ip nat stateful id 1 primary 1.1.1.1 peer 2.2.2.2 mapping-id 10`	プライマリ ルータのステートフル NAT を指定します。
ステップ 4	**ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length* 例： `Router(config)# parser config cache interface`	IP アドレスのプールを定義します。
ステップ 5	**ip nat inside source static route-map** *name* **pool** *pool-name* **mapping-id** *map-id* [**overload**] 例： `Router(config)# ip nat inside source static route-map rm-101 pool snatpool2 mapping-id 10 overload`	内部送信元アドレスのステートフル NAT で、ローカルに作成されたエントリの特定のセットをピア SNAT ルータに配布できるようにします。

	コマンドまたはアクション	目的
ステップ 6	**ip nat inside destination list** *number* **pool** *name* **mapping-id** *map-id* 例： `Router(config)# ip nat inside destination list 1 pool snatpool2 mapping-id 10 overload`	ローカル SNAT ルータが、ローカルに作成されたエントリをピア SNAT ルータに配布できるようにする内部宛先アドレスを定義します。
ステップ 7	**ip nat outside source Static** *global-ip local-ip* **extendable mapping-id** *map-id* 例： `Router(config)# ip nat outside source static 1.1.1.1 2.2.2.2 extendable mapping-id 10`	外部送信元アドレスのステートフル NAT で、ローカルに作成されたエントリの特定のセットをピア SNAT ルータに配布できるようにします。
ステップ 8	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了します。 • 設定を保存し、コンフィギュレーション モードを終了するには、**end** コマンドを使用します。

HSRP 用 NAT スタティック マッピング サポートの設定

NAT スタティック マッピングで設定され、ルータに所有されているアドレスに、アドレス解決プロトコル（ARP）のクエリーがトリガーされると、NAT は、ARP が指しているインターフェイス上のバーンドイン（焼き込まれた）MAC（BIA MAC）アドレスで応答します。2 つのルータはそれぞれ、HSRP アクティブとスタンバイの役割を果たします。 ルータの NAT 内部インターフェイスがイネーブルになり、グループに属するように設定される必要があります。

HSRP 用スタティック マッピング サポートを設定することの利点は次のとおりです。

- HSRP 用スタティック マッピング サポートを使用することで、タイムアウトし、ハイ アベイラビリティ環境のアップストリーム ARP キャッシュを再入力する必要なしに、確実にフェールオーバーすることができます。ハイ アベイラビリティ環境では、HSRP ルータのペアには、冗長性のために同一の NAT 設定がされています。
- HSRP のスタティック マッピングのサポートによって、HSRP がアクティブなルータだけが NAT アドレスにより設定されたルータの着信 ARP に応答する設定オプションが可能になりました。

HSRP 用 NAT スタティック マッピング サポートを設定するには次の両方の作業が必要で、アクティブ ルータおよびスタンバイ ルータ両方に実行する必要があります。

HSRP 用スタティック マッピング サポート設定の制限事項

- HSRPが存在する場合にHSRP用スタティック マッピング サポートを設定すると、スタティック マッピングの設定だけで NAT をサポートすることができます。
- スタティック NAT マッピングは、2 つ以上の HSRP ルータに反映される必要があります。その理由は、HSRP グループ内で NAT を実行中のルータ間では、NAT のステートは交換されないからです。
- 両方の HSRP ルータが同一のスタティック NAT を持つときの動作は予測不能で、ルータを同一の HSRP グループにリンクしている **hsrp** キーワードで設定されません。

NAT インターフェイスの HSRP イネーブル化

アクティブ ルータとスタンバイ ルータの両方の NAT インターフェイスで HSRP をイネーブルにするには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **no ip redirects**
6. **ip nat** {**inside** | **outside**}
7. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
8. **standby** [*group-number*] **name** [*group-name*]
9. **end**
10. **show standby**
11. **show ip nat translations** [**verbose**]

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface ethernet 1/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 192.168.1.27 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 5	**no ip redirects** 例： `Router(config-if)# no ip redirects`	リダイレクト メッセージの送信をディセーブルにします。
ステップ 6	**ip nat** {**inside** | **outside**} 例： `Router(config)# ip nat inside`	インターフェイスに、内部または外部に接続されているとマークします。
ステップ 7	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Router(config-if)# standby 10 ip 192.168.5.30`	HSRP ルーティング プロトコルをイネーブルにします。
ステップ 8	**standby** [*group-number*] **name** [*group-name*] 例： `Router(config-if)# standby 10 name HSRP1`	HSRP グループ名を設定します。
ステップ 9	**end** 例： `Router(config-if)# exit`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**show standby** 例： `Router# show standby`	（任意）HSRP の情報を表示します。
ステップ 11	**show ip nat translations** [**verbose**] 例： `Router# show ip nat translations verbose`	（任意）アクティブな NAT 変換を表示します。

次の作業

次の項に進み、HSRP 環境でスタティック NAT をイネーブルにします。

HSRP 環境でスタティック NAT をイネーブル化

ハイ アベイラビリティのために HRSP のスタティック マッピング サポートをイネーブルにするには、アクティブ ルータとスタンバイ ルータの両方でこの作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat inside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name*} [**overload**] | **static** *local-ip global-ip* **redundancy** *group-name*}
4. **ip nat outside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name*} [**overload**] | **static** *local-ip global-ip* **redundancy** *group-name*}
5. **exit**
6. **show ip nat translations** [**verbose**]

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat inside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name*} [**overload**] | **static** *local-ip global-ip* **redundancy** *group-name*} 例： `Router(config)# ip nat inside source static 192.168.5.33 10.10.10.5 redundancy HSRP1`	HSRP が NAT 内部インターフェイスに設定されている場合、BIA MAC を使用してルータが ARP クエリーに応答できるようにします。
ステップ 4	**ip nat outside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name*} [**overload**] | **static** *local-ip global-ip* **redundancy** *group-name*} 例： `Router(config)# ip nat outside source static 192.168.5.33 10.10.10.5 redundancy HSRP1`	HSRP が NAT 外部インターフェイスに設定されている場合、BIA MAC を使用してルータが ARP クエリーに応答できるようにします。
ステップ 5	**exit** 例： `Router(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 6	**show ip nat translations** [**verbose**] 例： `Router# show ip nat translations verbose`	（任意）アクティブな NAT 変換を表示します。

ハイ アベイラビリティ用の NAT の設定例

例：ステートフル NAT の設定

次の例では、HSRP を使用したステートフル NAT の設定とステートフル NAT プライマリ ルータおよびバックアップ ルータの設定を示します。

HSRP を使用した SNAT の例

```
ip nat Stateful id 1
redundancy SNATHSRP
mapping-id 10
ip nat pool SNATPOOL1 10.1.1.1 10.1.1.9 prefix-length 24
ip nat inside source route-map rm-101 pool SNATPOOL1 mapping-id 10 overload
ip classless
ip route 10.1.1.0 255.255.255.0 Null0
no ip http server
ip pim bidir-enable
```

SNAT プライマリおよびバックアップ設定の例

```
ip nat Stateful id 1
primary 10.88.194.17
peer 10.88.194.18
mapping-id 10
!
ip nat Stateful id 2
backup 10.88.194.18
peer 10.88.194.17
mapping-id 10
```

非対称の外部から内部および ALG サポート用 NAT ステートフル フェールオーバーの設定例

ここでは、次の例を示します。

例：HSRP での SNAT の設定

次の例は、HSRP を使用した SNAT の設定方法です。

```
ip nat Stateful id 1
redundancy SNATHSRP
mapping-id 10
ip nat pool SNATPOOL1 11.1.1.1 11.1.1.9 prefix-length 24
ip nat inside source route-map rm-101 pool SNATPOOL1 mapping-id 10 overload
ip classless
ip route 11.1.1.0 255.255.255.0 Null0
no ip http server
ip pim bidir-enable
```

例：SNAT プライマリ バックアップの設定

次の例では、プライマリおよびバックアップ ルータの SNAT の設定方法を示します。

```
ip nat Stateful id 1
primary 10.88.194.17
peer 10.88.194.18
mapping-id 10
!
ip nat Stateful id 2
backup 10.88.194.18
peer 10.88.194.17
mapping-id 10
```

例：HSRP 環境のスタティック NAT の設定

次の例では、HSRP 環境でのスタティック設定を使用した NAT のサポートを示します。 2 つのルータは HSRP アクティブとスタンバイの役割を果たしており、NAT 内部インターフェイスは HSRP イネーブルで、HSRP1 グループに属するように設定されています。

アクティブ ルータの設定

```
interface BVI10
 ip address 192.168.5.54 255.255.255.255.0
 no ip redirects
 ip nat inside
 standby 10 priority 105 preempt
 standby 10 name HSRP1
 standby 10 ip 192.168.5.30
 standby 10 track Ethernet2/1
!
!
 ip default-gateway 10.0.18.126
 ip nat inside source static 192.168.5.33 10.10.10.5 redundancy HSRP1
 ip classless
 ip route 10.10.10.0 255.255.255.0 Ethernet2/1
 ip route 172.22.33.0 255.255.255.0 Ethernet2/1
 no ip http server
```

スタンバイ ルータの設定

```
interface BVI10
 ip address 192.168.5.56 255.255.255.255.0
 no ip redirects
 ip nat inside
 standby 10 priority 100 preempt
 standby 10 name HSRP1
 standby 10 ip 192.168.5.30
 standby 10 track Ethernet3/1
!
 ip default-gateway 10.0.18.126
 ip nat inside source static 192.168.5.33 3.3.3.5 redundancy HSRP1
 ip classless
 ip route 10.0.32.231 255.255.255.255 Ethernet3/1
 ip route 10.10.10.0 255.255.255.0 Ethernet3/1
 no ip http server
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
NAT コマンド：コマンド構文、コマンド モード、コマンド履歴、使用に関する注意事項および例	『*Cisco IOS IP Addressing Services Command Reference*』

関連項目	マニュアル タイトル
IP アクセス リストへのシーケンス番号づけ	『*IP Access List Sequence Numbering*』マニュアル
NAT 設定作業	「Configuring NAT for IP Address Conservation」モジュール
NAT メンテナンス	「Monitoring and Maintaining NAT」モジュール
MPLS VPN での NAT の使用	「Integrating NAT with MPLS VPNs」モジュール

標準

標準	タイトル
なし	

MIB

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

RFC

RFC	タイトル
RFC 903	『*Reverse Address Resolution Protocol*』
RFC 826	『*Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware*』
RFC 1027	『*Using ARP to implement transparent subnet gateways*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ハイ アベイラビリティ用 NAT の設定に関する機能情報

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

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

表 4：ハイ アベイラビリティ用 *NAT* の設定に関する機能情報

機能名	リリース	機能の設定情報
Outside-to-Inside 非対称 ALG の NAT ステートフル フェールオーバー サポート	12.3(7)T	Outside-to-Inside 非対称アプリケーション層ゲートウェイ（ALG）の NAT ステートフル フェールオーバー機能のサポートは、複数の外部から内部へのルーティング パスと、パケットごとのロード バランシングを可能にすることで、非対称経路の扱いを向上させるものです。 この機能はまた、Voice over IP、FTP、ドメイン ネーム システム（DNS）アプリケーションといった、埋め込み IP アドレッシングを含むトラフィックとのシームレスなフェールオーバー変換 IP セッションを可能にします。
ネットワーク アドレス変換の NAT ステートフル フェールオーバー	12.2(13)T	ネットワーク アドレス変換の NAT ステートフル フェールオーバー機能は、ステートフル フェールオーバー機能のフェーズ 1 です。 複数の Network Address Translator を変換グループとして動作させる機能のサポートが導入されました。
ハイ アベイラビリティ向けの HSRP を使用した NAT スタティック マッピングのサポート	12.2(4)T 12.2(4)T2 Cisco IOS XE Release 2.1	HSRP のスタティック マッピングのサポートによって、HSRP がアクティブなルータだけが NAT アドレスにより設定されたルータの着信 ARP に応答する設定オプションが可能になりました。

第 5 章

ステートフル シャーシ間冗長化の設定

ステートフル シャーシ間冗長化機能を使用すると、デバイスのペアが互いのバックアップとして動作するように設定できます。

このモジュールでは、ステートフル シャーシ間冗長化の設定に関する概念情報および作業について説明します。

- 機能情報の確認，111 ページ
- ステートフル シャーシ間冗長化の前提条件，112 ページ
- ステートフル シャーシ間冗長化の制約事項，112 ページ
- ステートフル シャーシ間冗長化について，112 ページ
- ステートフル シャーシ間冗長化の設定方法，117 ページ
- ステートフル シャーシ間冗長化の設定例，128 ページ
- その他の関連資料，129 ページ
- ステートフル シャーシ間冗長化の機能情報，130 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

ステートフル シャーシ間冗長化の前提条件

冗長グループ アソシエーションおよびマッピング ID を持つネットワーク アドレス変換（NAT）ルールを含む、すべてのアプリケーション冗長性の設定は、両方のデバイスで同一である必要があります。同一でない場合、デバイス間で NAT セッションが同期化されず、NAT 冗長性が機能しません。

ステートフル シャーシ間冗長化の制約事項

- デフォルトでは、ネットワーク アドレス変換（NAT）ハイ アベイラビリティ（ボックス間およびボックス内）では、スタンバイ デバイスへの HTTP セッションの複製は行われません。 スイッチオーバー時にスタンバイ デバイスで HTTP セッションを複製するには、**ip nat switchover replication http** コマンドを設定する必要があります。
- 特定のアプリケーションでの NAT ペイロード変換中、ペイロード内に NAT 変換を必要とする IP アドレスが存在する場合があります。 その特定のアプリケーションのアプリケーション レベル ゲートウェイ（ALG）では、それらの IP アドレスのパケットを解析します。NAT によりこれらのアドレスが変換され、ALG により変換済みのアドレスが元のパケットに書き込まれます。

  フィックスアップにより、変換済み IP アドレスが元のパケットに書き込まれることが示されます。データが書き込まれると、パケットの長さが変更される場合があります。変更された場合、パケットの TCP シーケンス（SEQ）または確認応答（ACK）の値が、TCP 接続の存続期間にわたって NAT により調整されます。 NAT では、SEQ/ACK フィックスアップ中に、新しい TCP SEQ/ACK 値をパケットに書き込みます。

  たとえば、TCP ALG セッション中、SEQ/ACK 値は、ドメイン ネーム システム（DNS）、FTP/FTP64、H.323、リアルタイム ストリーミング プロトコル（RTSP）、および Session Initiation Protocol（SIP）などの、主に ASCII アプリケーションのフィックスアップを必要とする場合があります。 この SEQ/ACK の調整情報は、NAT セッションに関連付けられ、スタンバイ デバイスと定期的に同期されます。

  ステートフル スイッチオーバー時に、SEQ/ACK 情報が新しいアクティブ デバイスと完全に同期していないと、多くの場合、TCP 接続がアプリケーションのエンドポイントによってリセットされます。

ステートフル シャーシ間冗長化について

ステートフル シャーシ間冗長化の概要

フェールオーバー状態の数に基づいて、デバイスのグループからアクティブ デバイスを判別するように、ステートフル シャーシ間冗長化機能を設定できます。 フェールオーバーが発生すると、

中断なくスタンバイ デバイスが引き継ぎ、トラフィック フォワーディング サービスの実行とダイナミック ルーティング テーブルのメンテナンスを開始します。

ステートフル シャーシ間冗長化の動作

相互にホットスタンバイとして動作するようにデバイスのペアを設定できます。冗長性は、インターフェイス ベースで設定します。 冗長インターフェイスのペアは、冗長グループ（RG）と呼ばれます。冗長性はアプリケーション レベルで発生します。インターフェイスまたはデバイスで完全な物理的障害が発生しなくても、アプリケーションのスイッチオーバーが行われます。 スイッチオーバーが行われると、アプリケーション アクティビティは冗長インターフェイスでシームレスに実行を続けます。

以下の最初の図は、アクティブ/スタンバイのロード シェアリング シナリオを示しています。 図には、発信インターフェイスを 1 つ持つデバイス ペアに対してどのように RG が設定されているかが示されています。 2 番目の図は、アクティブ/アクティブのロード シェアリング シナリオを示しています。 以下の図は、発信インターフェイスを 2 つ持つデバイス ペアに対して、どのように 2 つの RG が設定されているかを示しています。 ASR1 のグループ A はスタンバイ RG で、ASR 2 のグループ A はアクティブ RG です。

いずれの場合でも、設定可能なコントロール リンクおよびデータ同期リンクによって冗長デバイスは参加します。 コントロール リンクは、デバイスのステータスを通信するために使用されます。 データ同期リンクは、ネットワーク アドレス変換（NAT）およびファイアウォールからステートフル情報を転送し、ステートフルデータベースを同期するために使用されます。 冗長イン

ターフェイスのペアは、冗長インターフェイス ID（RII）と呼ばれる、同じ固有 ID 番号で設定されます。

図 *5*：冗長グループの設定：*1* つの発信インターフェイス

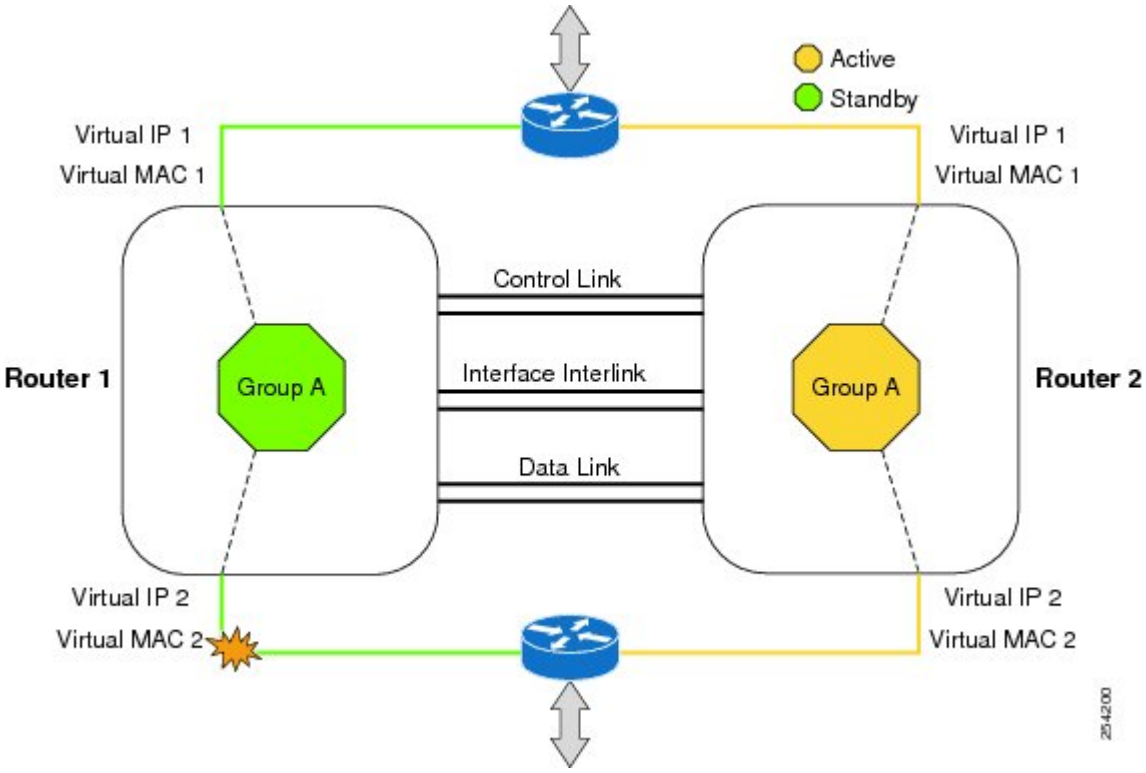
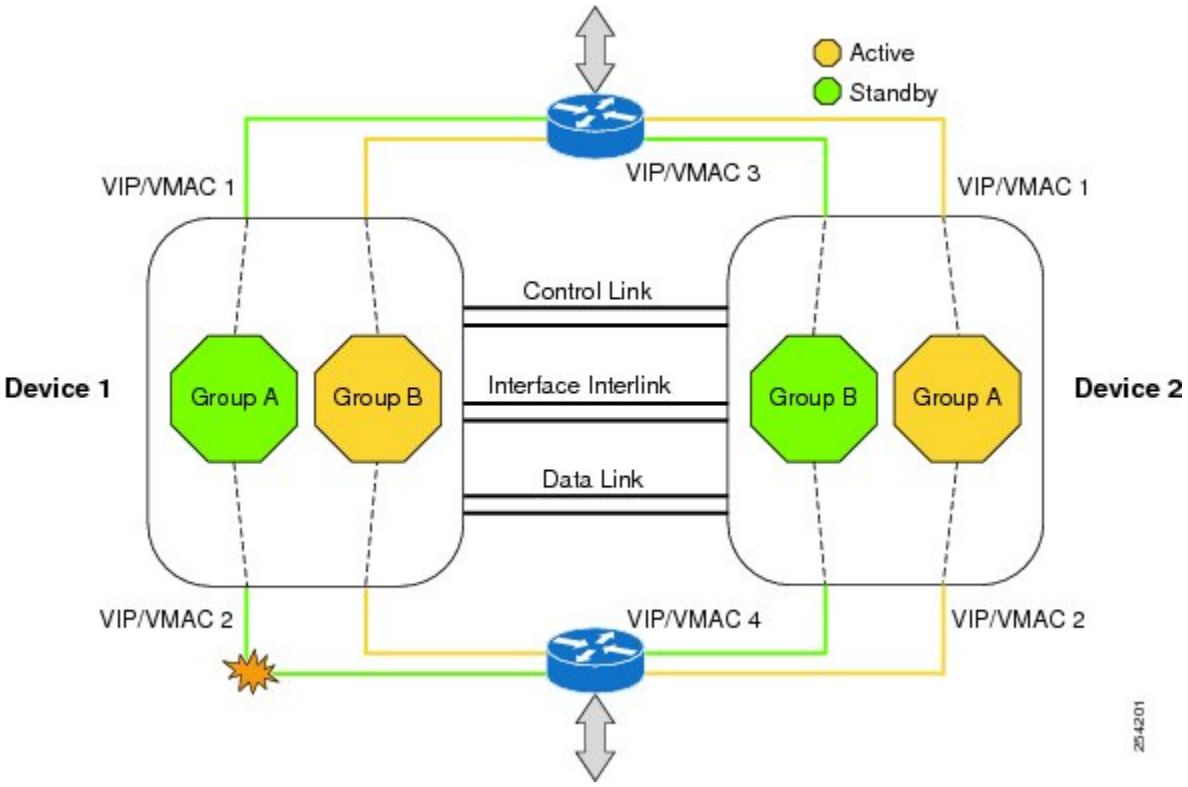


図 *6*：冗長グループの設定：*2* つの発信インターフェイス



冗長グループ メンバーのステータスは、コントロール リンクで送信される hello メッセージを使用することで判断できます。 ソフトウェアでは、設定可能な時間内にいずれかのデバイスが hello メッセージに応答しない場合、これを障害と見なし、スイッチオーバーを開始します。 ソフトウェアがミリ秒単位で障害を検出できるように、コントロール リンクでは、双方向フォワーディング検出（BFD）プロトコルと統合されているフェールオーバープロトコルを実行します。 hello メッセージについて次のパラメータを設定できます。

- hello タイム：hello メッセージの送信間隔。
- ホールド タイム：アクティブまたはスタンバイ デバイスがダウン状態であると宣言されるまでの時間。

hello タイムのデフォルトは、ホットスタンバイ ルータ プロトコル（HSRP）に合わせるために 3 秒です。また、ホールド タイムのデフォルトは 10 秒です。 また、**timers hellotime msec** コマンドを使用して、これらのタイマーをミリ秒単位で設定することもできます。

スイッチオーバーの影響を受けるインターフェイスのペアを判断するには、冗長インターフェイスの各ペアについて、固有の ID を設定する必要があります。 この ID は RII と呼ばれ、インターフェイスに関連付けられます。

スタンバイ デバイスへのスイッチオーバーは、各デバイスに設定された優先度の設定が変更された場合に発生することがあります。 最高の優先度値を持つデバイスが、アクティブデバイスとして動作します。 アクティブ デバイスまたはスタンバイ デバイスで障害が発生した場合、重みと呼ばれる設定可能な数値分、デバイスの優先度が減らされます。 アクティブ デバイスの優先度が、スタンバイデバイスの優先度を下回る場合、スイッチオーバーが発生し、スタンバイデバイ

スがアクティブ デバイスになります。 このデフォルトの動作を無効にするには、RG について preemption 属性をディセーブルにします。 また、インターフェイスのレイヤ 1 ステートがダウン状態になった場合に優先度を減らすように、各インターフェイスを設定できます。 設定された優先度により、RG のデフォルトの優先度が上書きされます。

RG の優先度を変更する各障害イベントにより、タイム スタンプ、影響を受けた RG、前の優先度、新しい優先度、および障害イベントの原因の説明を含む syslog エントリが生成されます。

スイッチオーバーは、デバイスまたはインターフェイスの優先度が、設定可能なしきい値レベルを下回った場合にも発生することがあります。

スタンバイ デバイスへのスイッチオーバーは、次の状況で発生します。

- アクティブ デバイスでパワー損失またはリロードが発生した場合（リロードを含む）。
- アクティブ デバイスの実行時優先度が、スタンバイ デバイスの実行時優先度を下回った場合（プリエンプションが設定されている場合）。
- アクティブ デバイスの実行時優先度が、設定されたしきい値を下回った場合。
- アクティブ デバイスの冗長グループが手動でリロードされた場合。 手動リロードには、**redundancy application reload group** *rg-number* コマンドを使用します。

ファイアウォールおよび NAT とのアソシエーション

ファイアウォールは、冗長グループのトラフィック インターフェイスとのアソシエーションを使用します。

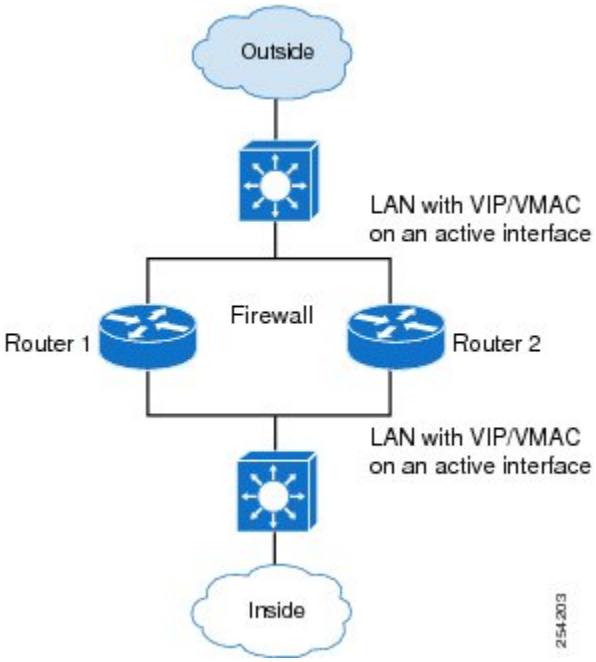
ネットワーク アドレス変換（NAT）により、冗長グループがマッピング ID に関連付けられます。

LAN/LAN トポロジ

以下の図は、LAN/LAN トポロジを示しています。 LAN/LAN トポロジでは、すべての参加デバイスが、内部および外部の両方で LAN インターフェイスを介して相互に接続されます。 このシナリオでは、スタティック ルーティングがアップストリームまたはダウンストリーム デバイスで適切な仮想 IP アドレスに設定されていれば、トラフィックは通常正しいファイアウォールに送られます。 Cisco ASR 1000 アグリゲーション サービス ルータでは、アップストリームまたはダウンストリーム デバイスでダイナミック ルーティングに参加します。 LAN 方向のインターフェイスでサポートされるダイナミック ルーティング設定では、ルーティング プロトコルのコンバージェ

ンスへの依存が生じないようにしてください。依存があると、高速フェールオーバー要件に適合しなくなります。

図 7：***LAN/LAN*** トポロジ



ステートフル シャーシ間冗長化の設定方法

コントロール インターフェイス プロトコルの設定

コントロール インターフェイス プロトコルの設定は、次の要素で構成されています。

- 認証情報
- グループ名
- hello タイム
- ホールド タイム
- プロトコル インスタンス
- 双方向フォワーディング検出（BFD）プロトコルの使用

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **mode sso**
5. **application redundancy**
6. **protocol** *number*
7. **name** *instance-name*
8. **timers hellotime** [**msec**] *number* **holdtime** [**msec**] *number*
9. **authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key* | **md5 key-chain** *key-chain-name*}
10. **bfd**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長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	**mode sso** 例： `Device(config-red)# mode sso`	冗長モードをステートフル スイッチオーバー（SSO）に設定します。
ステップ 5	**application redundancy** 例： `Device(config-red)# application redundancy`	冗長アプリケーション コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**protocol** *number* 例： `Device(config-red-app)# protocol 4`	コントロールインターフェイスに接続されるプロトコルインスタンスを指定し、冗長アプリケーションプロトコル コンフィギュレーション モードを開始します。
ステップ 7	**name** *instance-name* 例： `Device(config-red-app-prot)# name rg1`	（任意）プロトコルインスタンスに任意のエイリアスを指定します。
ステップ 8	**timers hellotime** [**msec**] *number* **holdtime** [**msec**] *number* 例： `Device(config-red-app-prot)# timers hellotime 3 holdtime 10`	helloメッセージが送信される間隔と、デバイスがダウン状態と宣言されるまでの時間を指定します。 • デフォルトの時間は、helloタイムは3秒、ホールドタイムは 10 秒です。
ステップ 9	**authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key* | **md5 key-chain** *key-chain-name*} 例： `Device(config-red-app-prot)# authentication text password`	認証情報を指定します。
ステップ 10	**bfd** 例： `Device(config-red-app-prot)# bfd`	（任意）コントロールインターフェイスで実行されているフェールオーバー プロトコルを BFD プロトコルと統合し、ミリ秒単位での障害検出を達成できるようにします。 • BFD はデフォルトでイネーブルになっています。
ステップ 11	**end** 例： `Device(config-red-app-prot)# end`	冗長アプリケーションプロトコル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

冗長グループの設定

冗長グループは、次の設定要素で構成されます。

- 各オブジェクトの優先度の減少量。
- 優先度を減少させる障害（オブジェクト）。
- フェールオーバー優先度。

- フェールオーバーのしきい値。
- グループ インスタンス。
- グループ名。
- 初期化遅延タイマー。
- 冗長グループ（RG）に関連付けられているインターフェイス。
- コントロール インターフェイスとして使用されるインターフェイス。
- データ インターフェイスとして使用されるインターフェイス。
- RG インターフェイスの冗長インターフェイス ID（RII）番号。

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** {**1** | **2**}
6. **name** *group-name*
7. **preempt**
8. **priority** *number* **failover-threshold** *number*
9. **track** *object-number* [**decrement** *number* | **shutdown**]
10. **timers delay** *seconds* [**reload** *seconds*]
11. **control** *interface-name* **protocol** *instance*
12. **data** *interface-name*
13. 別の冗長グループを作成するには、ステップ 3 ～ 12 を繰り返します。
14. **end**
15. **configure terminal**
16. **interface** *type number*
17. **redundancy group** *number* **ip** *address* **exclusive** [**decrement** *number*]
18. **redundancy rii** *number*
19. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長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	**application redundancy** 例： `Device(config-red)# application redundancy`	冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 5	**group** {**1** | **2**} 例： `Device(config-red-app)# group 1`	冗長グループのインスタンスを指定し、冗長アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 6	**name** *group-name* 例： `Device(config-red-app-grp)# name rg1`	（任意）プロトコル インスタンスに任意のエイリアスを指定します。
ステップ 7	**preempt** 例： `Device(config-red-app-grp)# preempt`	グループでのプリエンプションをイネーブルにし、デバイスの優先度に関係なく、スタンバイ デバイスがアクティブ デバイスをプリエンプション処理できるようにします。
ステップ 8	**priority** *number* **failover-threshold** *number* 例： `Device(config-red-app-grp)# priority 120 failover-threshold 80`	冗長グループの初期優先度とフェールオーバーしきい値を指定します。
ステップ 9	**track** *object-number* [**decrement** *number* | **shutdown**] 例： `Device(config-red-app-grp)# track 44 decrement 20`	イベントが発生した場合の、冗長グループの優先度の減少量を指定します。 • 冗長グループの優先度に影響する複数のオブジェクトを追跡できます。
ステップ 10	**timers delay** *seconds* [**reload** *seconds*] 例： `Device(config-red-app-grp)# timers delay 10 reload 20`	障害の発生後またはシステムのリロード後に開始されるロール ネゴシエーションの、冗長グループによる遅延時間を指定します。

	コマンドまたはアクション	目的
ステップ 11	**control** *interface-name* **protocol** *instance* 例： `Device(config-red-app-grp)# control GigabitEthernet0/1/0 protocol 1`	冗長グループに使用されるコントロール インターフェイスを指定します。 • このインターフェイスは、コントロール インターフェイス プロトコルのインスタンスにも関連付けられます。
ステップ 12	**data** *interface-name* 例： `Device(config-red-app-grp)# data GigabitEthernet0/1/2`	冗長グループに使用されるデータ インターフェイスを指定します。
ステップ 13	別の冗長グループを作成するには、ステップ 3 ～ 12 を繰り返します。	—
ステップ 14	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 15	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 16	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	冗長グループに関連付けるインターフェイスを選択し、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 17	**redundancy group** *number* **ip** *address* **exclusive** [**decrement** *number*] 例： `Device(config-if)# redundancy group 1 ip 10.10.1.1 exclusive decrement 20`	インターフェイスを、*number* 引数により識別される冗長グループに関連付けます。
ステップ 18	**redundancy rii** *number* 例： `Device(config-if)# redundancy rii 40`	このインターフェイスに関連付けられた RII の番号を指定します。 • この番号は、冗長グループ内の他のインターフェイスの RII と一致する必要があります。
ステップ 19	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

冗長トラフィック インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **ip nat outside**
6. **ip virtual-reassembly**
7. **negotiation auto**
8. **redundancy rii** *number*
9. **redundancy group** *number* **ip** *address* **exclusive** [**decrement** *number*]
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/5`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.1.1.2 255.0.0.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**ip nat outside** 例： `Device(config-if)# ip nat outside`	IP アドレス変換用の外部インターフェイスを設定します。
ステップ 6	**ip virtual-reassembly** 例： `Device(config-if)# ip virtual-reassembly`	インターフェイス上で Virtual Fragmentation Reassembly（VFR）をイネーブルにします。
ステップ 7	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビットイーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 8	**redundancy rii** *number* 例： `Device(config-if)# redundancy rii 200`	このインターフェイスに関連付けられた冗長インターフェイス ID（RII）の番号を指定します。 • この番号は、冗長グループ内の他のインターフェイスの RII と一致する必要があります。
ステップ 9	**redundancy group** *number* **ip** *address* **exclusive** [**decrement** *number*] 例： `Device(config-if)# redundancy group 1 ip 10.1.1.200 exclusive decrement 10`	インターフェイスを、*number* 引数により識別される冗長グループに関連付けます。
ステップ 10	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ステートフル シャーシ間冗長化による NAT の設定

マッピング ID を使用して、ネットワーク アドレス変換（NAT）を冗長グループに関連付ける必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
4. **ip nat inside source list** {{*access-list-number* | *access-list-name*} | **route-map** *name*} **pool** *name* [**redundancy** *redundancy-id* [**mapping-id** *map-id* | **overload** | **reversible** | **vrf** *name*]]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} 例： `Device(config)# ip nat pool VPN-18 10.10.0.0 10.10.255.255 netmask 255.255.0.0`	NAT で使用される IP アドレス プールを定義します。
ステップ 4	**ip nat inside source list** {{*access-list-number* | *access-list-name*} | **route-map** *name*} **pool** *name* [**redundancy** *redundancy-id* [**mapping-id** *map-id* | **overload** | **reversible** | **vrf** *name*]] 例： `Device(config)# ip nat inside source list acl-18 pool VPN-18 redundancy 2 mapping-id 152`	内部送信元アドレスの NAT をイネーブルにします。 • マッピング ID を使用して、NAT を冗長グループに関連付ける必要があります。
ステップ 5	**end** 例： `Device(config)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ステートフル シャーシ間冗長化の管理とモニタリング

このタスクのコンフィギュレーション コマンドはすべて任意です。 **show** コマンドは任意の順序で使用できます。

手順の概要

1. **enable**
2. **redundancy application reload group** *number* [**peer** | **self**]
3. **show redundancy application group** [*group-id* | **all**]
4. **show redundancy application transport** {**clients** | **group** [*group-id*]}
5. **show redundancy application protocol** {*protocol-id* | **group** [*group-id*]}
6. **show redundancy application faults group** [*group-id*]
7. **show redundancy application if-mgr group** [*group-id*]
8. **show redundancy application control-interface group** [*group-id*]
9. **show redundancy application data-interface group** [*group-id*]
10. **show monitor event-trace rg_infra all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**redundancy application reload group** *number* [**peer**	**self**] 例： `Device# redundancy application reload group 2 self`	強制的にアクティブ冗長グループ（RG）をリロードし、スタンバイ RG をアクティブ RG にします。 • 冗長性の設定が機能しているかどうかを検証するには、**redundancy application reload** コマンドを使用します。 このコマンドは、アクティブRGで入力する必要があります。
ステップ 3	**show redundancy application group** [*group-id*	**all**] 例： `Device# show redundancy application group 2`	指定されたグループまたはすべてのグループの概要情報を表示します。

	コマンドまたはアクション	目的
ステップ 4	**show redundancy application transport** {**clients** | **group** [*group-id*]} 例： `Device# show redundancy application transport group 2`	指定されたグループまたはすべてのグループの転送情報を表示します。
ステップ 5	**show redundancy application protocol** {*protocol-id* | **group** [*group-id*]} 例： `Device# show redundancy application protocol 2`	指定されたグループまたはすべてのグループのプロトコル情報を表示します。
ステップ 6	**show redundancy application faults group** [*group-id*] 例： `Device# show redundancy application faults group 2`	指定されたグループまたはすべてのグループの障害に関する情報を表示します。
ステップ 7	**show redundancy application if-mgr group** [*group-id*] 例： `Device# show redundancy application if-mgr group 2`	指定されたグループまたはすべてのグループのインターフェイス マネージャ（if-mgr）に関する情報を表示します。
ステップ 8	**show redundancy application control-interface group** [*group-id*] 例： `Device# show redundancy application control-interface group IF-2`	指定されたコントロールインターフェイスについて、冗長グループに関連付けられているインターフェイス情報を表示します。
ステップ 9	**show redundancy application data-interface group** [*group-id*] 例： `Device# show redundancy application data-interface group IF-2`	指定されたデータ インターフェイスについて、冗長グループに関連付けられているインターフェイス情報を表示します。
ステップ 10	**show monitor event-trace rg_infra all** 例： `Device# show monitor event-trace rg_infra all`	すべての冗長グループに関連付けられているイベント トレース情報を表示します。

ステートフル シャーシ間冗長化の設定例

例：コントロール インターフェイス プロトコルの設定

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# mode sso
Device(config-red)# application redundancy
Device(config-red-app)# protocol 4
Device(config-red-app-prot)# name rg1
Device(config-red-app-prot)# timers hellotime 3 holdtime 10
Device(config-red-app-prot)# authentication text password
Device(config-red-app-prot)# bfd
```

例：冗長グループの設定

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# name rg1
Device(config-red-app-grp)# preempt
Device(config-red-app-grp)# priority 120 failover-threshold 80
Device(config-red-app-grp)# track 44 decrement 20
Device(config-red-app-grp)# timers delay 10 reload 20
Device(config-red-app-grp)# control GigabitEthernet0/1/0 protocol 1
Device(config-red-app-grp)# data GigabitEthernet0/1/2
Device(config-red-app-grp)# end
Device# configure terminal
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# redundancy group 1 ip 10.10.1.1 exclusive decrement 20
Device(config-if)# redundancy rii 40
```

例：冗長トラフィック インターフェイスの設定

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/5
Device(config-if)# ip address 10.1.1.2 255.0.0.0
Device(config-if)# ip nat outside
Device(config-if)# ip virtual-reassembly
Device(config-if)# negotiation auto
Device(config-if)# redundancy rii 200
Device(config-if)# redundancy group 1 ip 10.1.1.200 exclusive decrement 10
```

例：ステートフル シャーシ間冗長化による NAT の設定

```
Device# configure terminal
Device(config)# ip nat pool VPN-18 10.10.0.0 10.10.255.255 netmask 255.255.0.0
Device(config)# ip nat inside source list acl-18 pool VPN-18 redundancy 2 mapping-id 152
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
IP アドレッシング コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト、使用上の注意事項、および例	『Cisco IOS IP Addressing Services Command Reference』
IP アドレッシング IP ルーティングの基本原理	『*IP Routing Primer*』

標準および RFC

標準/RFC	タイトル
RFC 791	『Internet Protocol』
RFC 1338	『Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy』
RFC 1466	『Guidelines for Management of IP Address Space』
RFC 1716	『Towards Requirements for IP Routers』
RFC 1918	『Address Allocation for Private Internets』
RFC 3330	『Special-Use IP Addresses』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	

ステートフル シャーシ間冗長化の機能情報

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

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

表 *5*：ステートフル シャーシ間冗長化の機能情報

機能名	リリース	機能情報
ステートフル シャーシ間冗長化	Cisco IOS XE Release 3.1S	ステートフル シャーシ間冗長化機能を使用すると、デバイスのペアが互いのバックアップとして動作するように設定できます。

第 6 章

ゾーンベースのファイアウォールおよびNATに対するシャーシ間非対称ルーティング サポート

ゾーンベースのファイアウォールおよび NAT に対するシャーシ間非対称ルーティング サポート機能では、パケット処理のための、スタンバイ冗長グループからアクティブ冗長グループへのパケットの転送をサポートします。 この機能がイネーブルでない場合、最初の同期（SYN）メッセージを受け取らなかったルータに転送された戻り TCP パケットはドロップされます。これらのパケットは、既知のセッションに属していないためです。

このモジュールでは、非対称ルーティングの概要と、非対称ルーティングの設定方法について説明します

- 機能情報の確認，132 ページ
- ゾーンベースのファイアウォールおよびNATに対するシャーシ間非対称ルーティング サポートの制約事項，132 ページ
- ゾーンベースのファイアウォールおよびNATに対するシャーシ間非対称ルーティング サポートについて，132 ページ
- ゾーンベースのファイアウォールおよびNATに対するシャーシ間非対称ルーティング サポートの設定方法，136 ページ
- ゾーンベースのファイアウォールおよびNATに対するシャーシ間非対称ルーティング サポートの設定例，146 ページ
- ゾーンベースのファイアウォールおよびNATに対するシャーシ間非対称ルーティング サポートに関するその他の関連資料，148 ページ
- ゾーンベースのファイアウォールおよびNATに対するシャーシ間非対称ルーティング サポートの機能情報，149 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

ゾーンベースのファイアウォールおよび NAT に対するシャーシ間非対称ルーティング サポートの制約事項

- マルチプロトコル ラベル スイッチング（MPLS）および VPN 経由の非対称ルーティングはサポートされません。
- 仮想 IP アドレスおよび仮想 MAC（VMAC）アドレスを使用する LAN では、非対称ルーティングをサポートしません。
- VPN ルーティングおよび転送（VRF）はサポートされません。

ゾーンベースのファイアウォールおよび NAT に対するシャーシ間非対称ルーティング サポートについて

非対称ルーティングの概要

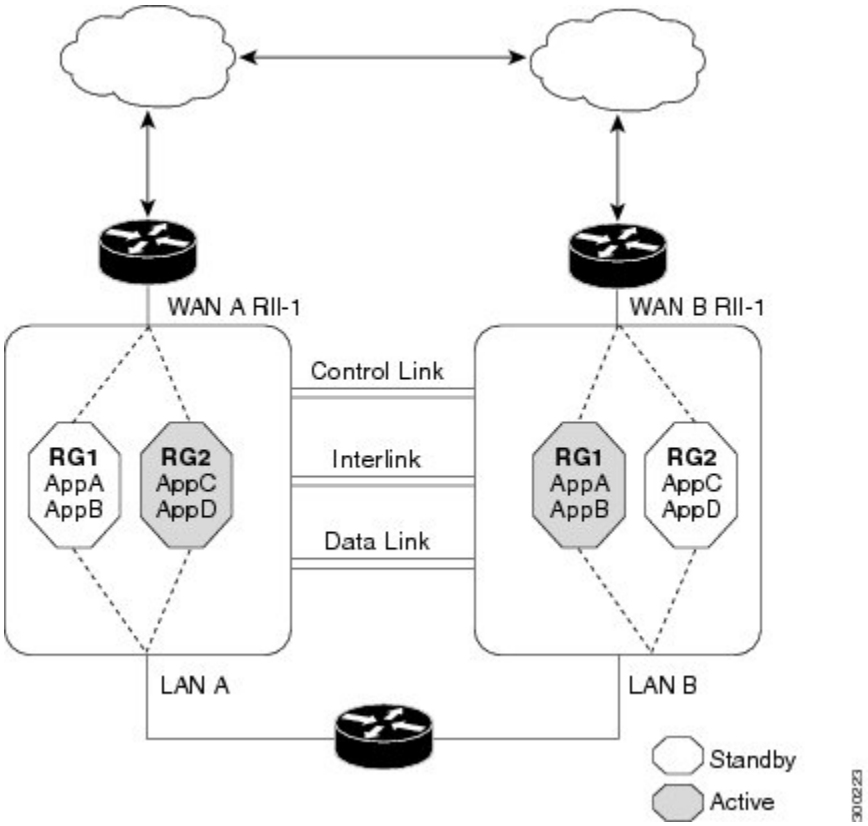
非対称ルーティングは、TCP または UDP 接続の複数のパケットが、異なるルートを経由して異なる方向に送信される場合に発生します。 非対称ルーティングでは、単一の TCP または UDP 接続に属しているパケットは、冗長グループ（RG）内の 1 つのインターフェイスを経由して転送され、同じ RG 内の別のインターフェイスを経由して戻されます。 非対称ルーティングでは、パケット フローは同じ RG 内にあります。 非対称ルーティングを設定する場合、スタンバイ RG で受信したパケットは処理のためにアクティブ RG にリダイレクトされます。 非対称ルーティングが設定されていない場合、スタンバイ RG で受信されたパケットがドロップされる可能性があります。

非対称ルーティングによって、特定のトラフィック フロー用の RG が決定されます。 RG のステートはパケット処理の決定において不可欠です。 RG がアクティブの場合、通常のパケット処理が実行されます。 RG がスタンバイ ステートにあり、非対称ルーティングおよび **asymmetric-routing always-divert enable** コマンドが設定されている場合、パケットはアクティブ RG に転送されます。

スタンバイ RG から受信したパケットを常にアクティブ RG に転送するには、**asymmetric-routing always-divert enable** コマンドを使用します。

以下の図は、異なる非対称ルーティングインターリンク インターフェイスによりパケットをアクティブ RG に転送する非対称ルーティング シナリオを示しています。

図 *8*：非対称ルーティング シナリオ



非対称ルーティングには、次のルールが適用されます。

- 冗長インターフェイス ID（RII）とインターフェイスの間には 1 対 1 マッピングが存在します。
- インターフェイスと RG の間には、1 対 *n* マッピングが存在します。（インターフェイスは、複数の RG を持つことができます）
- RG とそれを使用するアプリケーションの間には、1 対 *n* マッピングが存在します （複数のアプリケーションが同じ RG を使用できます）。
- RG とトラフィック フローの間には、1 対 1 マッピングが存在します。 トラフィック フローは、単一 RG にのみマッピングする必要があります。 トラフィック フローが複数の RG にマッピングされると、エラーが発生します。

- インターリンクに、すべてのRGインターリンク トラフィックをサポートするだけの十分な帯域幅があれば、RGおよび非対称ルーティング インターリンク間に1対1または1対*n*のマッピングが存在できます。

非対称ルーティングは、転送されるすべてのトラフィックを処理するインターリンク インターフェイスで構成されます。 非対称ルーティング インターリンク インターフェイスには、転送が予期されるすべてのトラフィックを処理するために十分な大きさの帯域幅が必要です。 IPv4アドレスは非対称ルーティング インターリンク インターフェイス上で設定する必要があり、非対称ルーティングインターフェイスのIPアドレスはこのインターフェイスからアクセス可能である必要があります。

（注） 非対称ルーティング インターリンク インターフェイスは、インターリンク トラフィックにのみ使用し、ハイアベイラビリティ（HA）コントロールまたはデータ インターフェイスとは共有しないことをお勧めします。これは、非対称ルーティング インターリンク インターフェイス上のトラフィック量が非常に大きくなる場合があるためです。

ファイアウォールでの非対称ルーティング サポート

ボックス内非対称ルーティング サポートのために、ファイアウォールでは、インターネット制御メッセージ プロトコル（ICMP）、TCP、およびUDPパケットのステートフル レイヤ3およびレイヤ4インスペクションを行います。 ファイアウォールは、パケットのウィンドウ サイズと順序を検証することにより、TCPパケットのステートフルインスペクションを実行します。 ステートフル インスペクション用に、ファイアウォールでは、トラフィックの双方向からのステート情報も必要とします。 ファイアウォールが行うICMP情報フローのインスペクションは限定的です。ICMPエコー要求および応答に関連付けられているシーケンス番号が確認されます。 ファイアウォールでスタンバイ冗長グループ（RG）とパケットフローの同期が行われるのは、そのパケットに対してセッションが確立された後です。 確立されるセッションは、TCP、UDPの2番目のパケット、およびICMPの情報メッセージに対するスリーウェイ ハンドシェイクです。 すべてのICMPフローがアクティブRGに送信されます。

ファイアウォールにより、ICMP、TCP、およびUDPプロトコルに属さないパケットについて、ポリシーのステートレスな検証が行われます。

ファイアウォールは、いつパケットフローをエージングアウトするかの判別に双方向トラフィックを利用し、検査済みのパケットフローをすべてアクティブRGに転送します。 パス ポリシーを持つパケット フローおよびポリシーおよびドロップ ポリシーのない同じゾーンを含むパス ポリシーは転送されません。

（注） ファイアウォールでは、スタンバイRGで受信したパケットをアクティブRGに転送する**asymmetric-routing always-divert enable**コマンドをサポートしていません。 デフォルトでは、ファイアウォールはすべてのパケット フローを強制的にアクティブRGに転送します。

NAT の非対称ルーティング

非対称ルーティングが設定されている場合、ネットワーク アドレス変換（NAT）のデフォルトでは、非 ALG パケットはアクティブ RG に転送するのではなく、スタンバイ RG で処理します。 NAT のみの設定（ファイアウォールが設定されていない場合）では、パケットの処理にアクティブおよびスタンバイ両方の RG を使用できます。 NAT のみの設定があり、非対称ルーティングを設定している場合のデフォルトの非対称ルーティング ルールは、NAT ではスタンバイ RG でパケットを選択的に処理する、というものです。 スタンバイ RG で受信したパケットをアクティブ RG に転送するには、**asymmetric-routing always-divert enable** コマンドを設定します。 または、NAT とともにファイアウォールを設定している場合のデフォルトの非対称ルーティング ルールは、常にパケットをアクティブ RG に転送する、というものです。

NAT がスタンバイ RG でパケットを受信したときに、パケットの転送が設定されていない場合、NAT では検索を実行してそのパケットのセッションが存在するかどうかを確認します。セッションが存在し、そのセッションに関連付けられた ALG がない場合、NAT はスタンバイ RG でパケットを処理します。セッションが存在している場合、スタンバイ RG でのパケットの処理によって、NAT トラフィックの帯域幅が大幅に増加します。

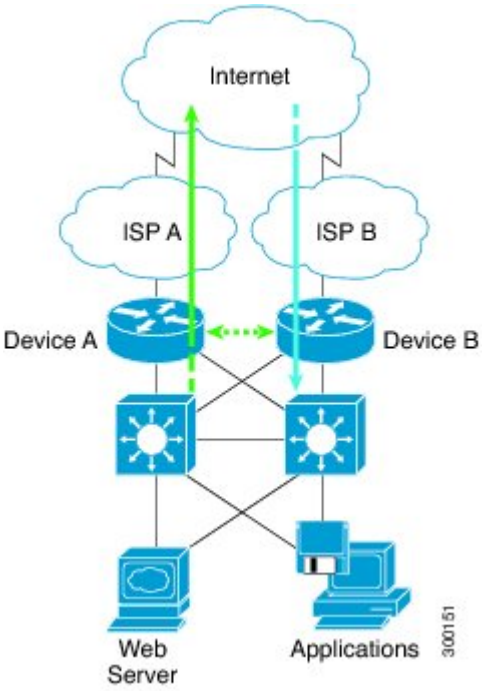
ALG は、ペイロードを識別および変換し、子フローを作成するために、NAT により使用されます。 ALG が正しく機能するには、双方向トラフィックが必要です。 NAT では、ALG に関連付けられているすべてのパケット フローで、すべてのトラフィックをアクティブ RG に転送する必要があります。 これは、セッションに関連付けられている ALG データがスタンバイ RG で検出されるかどうかを確認することによって行われます。 ALG データが存在する場合、非対称ルーティングのためにパケットが転送されます。

WAN-LAN トポロジでの非対称ルーティング

非対称ルーティングでサポートされるのは、WAN-LAN トポロジのみです。 WAN-LAN トポロジでは、デバイスは内部では LAN インターフェイスを介して接続され、外部では WAN インターフェイスを介して接続されます。 WAN リンク経由で受信したリターン トラフィックのルーティングは制御されません。 非対称ルーティングでは、WAN-LAN トポロジ内の WAN リンク経由で

受信したリターン トラフィックのルーティングを制御します。 以下の図は、WAN-LAN トポロジを示しています。

図 *9*：*WAN-LAN* トポロジでの非対称ルーティング



ゾーンベースのファイアウォールおよび NAT に対するシャーシ間非対称ルーティング サポートの設定方法

冗長アプリケーション グループおよび冗長グループ プロトコルの設定

冗長グループは、次の設定要素で構成されます。

- 各オブジェクトの優先度の減少量。
- 優先度を減少させる障害（オブジェクト）
- フェールオーバー優先度
- フェールオーバーしきい値
- グループ インスタンス
- グループ名

- 初期化遅延タイマー

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **name** *group-name*
7. **priority** *value* [**failover threshold** *value*]
8. **preempt**
9. **track** *object-number* **decrement** *number*
10. **exit**
11. **protocol** *id*
12. **timers hellotime** {*seconds* | **msec** *msec*} **holdtime** {*seconds* | **msec** *msec*}
13. **authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*] | **key-chain** *key-chain-name*}
14. **bfd**
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長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	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーションの冗長性を設定し、冗長アプリケーション コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長グループを設定し、冗長アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 6	**name** *group-name* 例： `Device(config-red-app-grp)# name group1`	プロトコル インスタンスに任意のエイリアスを指定します。
ステップ 7	**priority** *value* [**failover threshold** *value*] 例： `Device(config-red-app-grp)# priority 100 failover threshold 50`	冗長グループの初期優先度とフェールオーバーしきい値を指定します。
ステップ 8	**preempt** 例： `Device(config-red-app-grp)# preempt`	冗長グループに対するプリエンプションをイネーブルにし、スタンバイ デバイスがアクティブ デバイスをプリエンプション処理できるようにします。 • スタンバイ デバイスによりプリエンプション処理が行われるのは、その優先度がアクティブ デバイスの優先度より高い場合のみです。
ステップ 9	**track** *object-number* **decrement** *number* 例： `Device(config-red-app-grp)# track 50 decrement 50`	冗長グループの優先度値を指定します。この値は、追跡対象のオブジェクトでイベントが発生した場合に減らされます。
ステップ 10	**exit** 例： `Device(config-red-app-grp)# exit`	冗長アプリケーション グループ コンフィギュレーション モードを終了し、冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 11	**protocol** *id* 例： `Device(config-red-app)# protocol 1`	コントロール インターフェイスに接続されるプロトコル インスタンスを指定し、冗長アプリケーション プロトコル コンフィギュレーション モードを開始します。
ステップ 12	**timers hellotime** {*seconds* | **msec** *msec*} **holdtime** {*seconds* | **msec** *msec*} 例： `Device(config-red-app-prtcl)# timers hellotime 3 holdtime 10`	hello メッセージが送信される間隔と、デバイスがダウン状態と宣言されるまでの時間を指定します。 • holdtime は、hellotime の 3 倍以上に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 13	**authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*] | **key-chain** *key-chain-name*} 例： `Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100`	認証情報を指定します。
ステップ 14	**bfd** 例： `Device(config-red-app-prtcl)# bfd`	双方向フォワーディング検出（BFD）を使用してコントロール インターフェイスで実行されているフェールオーバー プロトコルを統合し、ミリ秒単位での障害検出を達成できるようにします。 • BFD はデフォルトでイネーブルになっています。
ステップ 15	**end** 例： `Device(config-red-app-prtcl)# end`	冗長アプリケーション プロトコル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

データ、コントロール、および非対称ルーティングインターフェイスの設定

この作業では、次の冗長グループ（RG）要素を設定します。

- コントロール インターフェイスとして使用されるインターフェイス。
- データ インターフェイスとして使用されるインターフェイス。
- 非対称ルーティングに使用されるインターフェイス。 これはオプションのタスクです。 この作業は、ネットワーク アドレス変換（NAT）に非対称ルーティングを設定する場合にのみ実行します。

（注） ゾーンベースのファイアウォールについて、非対称ルーティング、データ、およびコントロールは、別個のインターフェイスに設定する必要があります。 ただし、ネットワーク アドレス変換（NAT）については、非対称ルーティング、データ、およびコントロールを同じインターフェイスに設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **data** *interface-type interface-number*
7. **control** *interface-type interface-number* **protocol** *id*
8. **timers delay** *seconds* [**reload** *seconds*]
9. **asymmetric-routing interface** *type number*
10. **asymmetric-routing always-divert enable**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長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	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーションの冗長性を設定し、冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長グループ（RG）を設定し、冗長アプリケーション グループ 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 6	**data** *interface-type interface-number* 例： `Device(config-red-app-grp)# data GigabitEthernet 0/0/1`	RG よりに使用されるデータ インターフェイスを指定します。
ステップ 7	**control** *interface-type interface-number* **protocol** *id* 例： `Device(config-red-app-grp)# control GigabitEthernet 1/0/0 protocol 1`	RG により使用されるコントロール インターフェイスを指定します。 • コントロールインターフェイスは、コントロール インターフェイスプロトコルのインスタンスにも関連付けられます。
ステップ 8	**timers delay** *seconds* [**reload** *seconds*] 例： `Device(config-red-app-grp)# timers delay 100 reload 400`	障害の発生後またはシステムのリロード後に開始されるロール ネゴシエーションの、RG による遅延時間を指定します。
ステップ 9	**asymmetric-routing interface** *type number* 例： `Device(config-red-app-grp)# asymmetric-routing interface GigabitEthernet 0/1/1`	RGにより使用される非対称ルーティングインターフェイスを指定します。
ステップ 10	**asymmetric-routing always-divert enable** 例： `Device(config-red-app-grp)# asymmetric-routing always-divert enable`	スタンバイ RG から受信したパケットを常にアクティブ RG に転送します。
ステップ 11	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了し、特権EXECモードを開始します。

インターフェイスでの冗長インターフェイスIDおよび非対称ルーティングの設定

（注）
- データ インターフェイスまたはコントロール インターフェイスとして設定されているインターフェイスには、冗長インターフェイス ID（RII）は設定しないでください。
- RII および非対称ルーティングは、アクティブおよびスタンバイ両方のデバイスに設定する必要があります。
- 仮想 IP アドレスが設定されているインターフェイスでは、非対称ルーティングはイネーブルにできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **redundancy rii** *id*
5. **redundancy group** *id* [**decrement** *number*]
6. **redundancy asymmetric-routing enable**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/1/3`	冗長グループ（RG）に関連付けるインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**redundancy rii** *id* 例： `Device(config-if)# redundancy rii 600`	冗長インターフェイス ID（RII）を設定します。
ステップ 5	**redundancy group** *id* [**decrement** *number*] 例： `Device(config-if)# redundancy group 1 decrement 20`	RG冗長トラフィック インターフェイス コンフィギュレーションをイネーブルにし、インターフェイスがダウンした場合の優先度の減少量を指定します。 （注） 非対称ルーティングがイネーブルになっているトラフィック インターフェイスに RG を設定する必要はありません。
ステップ 6	**redundancy asymmetric-routing enable** 例： `Device(config-if)# redundancy asymmetric-routing enable`	各 RG に非対称フロー転送トンネルを確立します。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

非対称ルーティングを使用したダイナミック内部送信元変換の設定

次の設定は、非対称ルーティングを使用したダイナミック内部送信元変換の例です。 非対称ルーティングは、ダイナミック外部送信元、スタティック内部および外部送信元、およびポート アドレス変換（PAT）内部および外部送信元変換の各タイプの NAT 設定を使用して設定できます。 各タイプの NAT 設定の詳細については、「IP アドレス節約のための NAT 設定」の章を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **ip nat outside**
6. **exit**
7. **redundancy**
8. **application redundancy**
9. **group** *id*
10. **asymmetric-routing always-divert enable**
11. **end**
12. **configure terminal**
13. **ip nat pool** *name start-ip end-ip* {*mask* | **prefix-length** *prefix-length*}
14. **exit**
15. **ip nat inside source list** *acl-number* **pool** *name* **redundancy** *redundancy-id* **mapping-id** *map-id*
16. **access-list** *standard-acl-number* **permit** *source-address wildcard-bits*
17. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/3`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**ip nat outside** 例： `Device(config-if)# ip nat outside`	外部と接続されることを示すマークをインターフェイスに付けます。
ステップ 6	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 7	**redundancy** 例： `Device(config)# redundancy`	冗長性を設定し、冗長コンフィギュレーション モードを開始します。
ステップ 8	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーションの冗長性を設定し、冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 9	**group** *id* 例： `Device(config-red-app)# group 1`	冗長グループを設定し、冗長アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 10	**asymmetric-routing always-divert enable** 例： `Device(config-red-app-grp)# asymmetric-routing always-divert enable`	アクティブ デバイスにトラフィックを転送します。
ステップ 11	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 12	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 13	**ip nat pool** *name start-ip end-ip* {*mask* | **prefix-length** *prefix-length*} 例： `Device(config)# ip nat pool pool1 prefix-length 24`	グローバル アドレスのプールを定義します。 • IP NAT プール 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 14	**exit** 例： `Device(config-ipnat-pool)# exit`	IP NAT プール コンフィギュレーション モードを終了します。続いて、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 15	**ip nat inside source list** *acl-number* **pool** *name* **redundancy** *redundancy-id* **mapping-id** *map-id* 例： `Device(config)# ip nat inside source list pool pool1 redundancy 1 mapping-id 100`	内部送信元アドレスの NAT をイネーブルにし、マッピング ID を使用して NAT を冗長グループに関連付けます。
ステップ 16	**access-list** *standard-acl-number* **permit** *source-address wildcard-bits* 例： `Device(config)# access-list 10 permit 10.1.1.1 255.255.255.0`	変換する内部アドレスの標準のアクセス リストを定義します。
ステップ 17	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーンベースのファイアウォールおよび NAT に対するシャーシ間非対称ルーティング サポートの設定例

例：冗長アプリケーション グループおよび冗長グループ プロトコルの設定

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# name group1
Device(config-red-app-grp)# priority 100 failover threshold 50
Device(config-red-app-grp)# preempt
Device(config-red-app-grp)# track 50 decrement 50
Device(config-red-app-grp)# exit
Device(config-red-app)# protocol 1
Device(config-red-app-prtcl)# timers hellotime 3 holdtime 10
Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100
Device(config-red-app-prtcl)# bfd
Device(config-red-app-prtcl)# end
```

例：データ、コントロール、および非対称ルーティングインターフェイスの設定

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# data GigabitEthernet 0/0/1
Device(config-red-app-grp)# control GigabitEthernet 1/0/0 protocol 1
Device(config-red-app-grp)# timers delay 100 reload 400
Device(config-red-app-grp)# asymmetric-routing interface GigabitEthernet 0/1/1
Device(config-red-app-grp)# asymmetric-routing always-divert enable
Device(config-red-app-grp)# end
```

例：インターフェイスでの冗長インターフェイスIDおよび非対称ルーティングの設定

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/3
Device(config-if)# redundancy rii 600
Device(config-if)# redundancy group 1 decrement 20
Device(config-if)# redundancy asymmetric-routing enable
Device(config-if)# end
```

例：非対称ルーティングを使用したダイナミック内部送信元変換の設定

```
Device(config)# interface gigabitethernet 0/1/3
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# ip nat outside
Device(config-if)# exit
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# asymmetric-routing always-divert enable
Device(config-red-app-grp)# end
Device# configure terminal
Device(config)# ip nat pool pool1 prefix-length 24
Device(config-ipnat-pool)# exit
Device(config)# ip nat inside source list pool pool1 redundancy 1 mapping-id 100
Device(config)# access-list 10 permit 10.1.1.1 255.255.255.0
```

ゾーンベースのファイアウォールおよび NAT に対するシャーシ間非対称ルーティングサポートに関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
ファイアウォール シャーシ間冗長化	「Configuring Firewall Stateful Inter-Chassis Redundancy」モジュール
NAT シャーシ間冗長化	「Configuring Stateful Inter-Chassis Redundancy」モジュール

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ゾーンベースのファイアウォールおよび NAT に対するシャーシ間非対称ルーティング サポートの機能情報

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

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

表 *6*：ゾーンベースのファイアウォールおよび *NAT* に対するシャーシ間非対称ルーティング サポートの機能情報

機能名	リリース	機能情報
ゾーンベースのファイアウォールおよびNAT に対するシャーシ間非対称ルーティング サポート	Cisco IOS XE Release 3.5S	ゾーンベースのファイアウォールおよびNAT に対するシャーシ間非対称ルーティング サポート機能では、パケット処理のための、スタンバイ冗長グループからアクティブ冗長グループへのパケットの転送をサポートします。 コマンド **asymmetric-routing**、**redundancy asymmetric-routing enable** が導入または変更されました。

ゾーンベースのファイアウォールおよび NAT に対するシャーシ間非対称ルーティング サポートの機能情報

第 7 章

MPLS VPN と NAT の統合

MPLS VPN とのネットワーク アドレス変換（NAT）統合機能により、複数のマルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）を単一デバイスに設定して、連動するようにできます。 MPLS VPN がすべて同じ IP アドレッシング スキームを使用していたとしても、NAT は、どの MPLS VPN から IP トラフィックを受信するのかを区別できます。 この拡張により、複数の MPLS VPN の顧客がサービスを共有しながら、各 MPLS VPN が互いに完全に分離していることが保証されます。

- 機能情報の確認，151 ページ
- MPLS VPN と NAT 統合の前提条件，152 ページ
- MPLS VPN と NAT 統合の制約事項，152 ページ
- MPLS VPN と NAT の統合について，152 ページ
- NAT と MPLS VPN との統合方法，154 ページ
- MPLS VPN と NAT 統合の設定例，161 ページ
- 次の作業，162 ページ
- MPLS VPN との NAT の統合に関するその他の関連資料，163 ページ
- MPLS VPN と NAT の統合に関する機能情報，163 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

MPLS VPN と NAT 統合の前提条件

- このモジュールの作業を実行する前に、「IP アドレス節約のための NAT 設定」モジュールで説明されている概念をよく理解しておく必要があります。
- このモジュールの作業で使用する必要のあるアクセス リストはすべて、設定作業を開始する前に設定しておく必要があります。 アクセス リストの設定方法については、次の URL にある『*IP Access List Sequence Numbering*』マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsaclseq.htm

（注） NAT コマンドで使用するアクセス リストが指定されている場合、NAT は一般によく使用される **permit ip any any** コマンドを、このアクセス リストではサポートしません。

MPLS VPN と NAT 統合の制約事項

内部 VPN 間と NAT との統合はサポートされていません。

MPLS VPN と NAT の統合について

NAT と MPLS VPN との統合の利点

MPLS サービス プロバイダーは、インターネット接続、ドメイン ネーム サーバ（DNS）、および Voice over IP（VoIP）サービスなどの付加価値サービスを顧客に提供します。 プロバイダーでは、顧客がサービスに到達する際に顧客同士の IP アドレスが異なっていることを求めます。 MPLS VPN では、ネットワーク内で重複する IP アドレスを使用できるため、サービスを使用できるように NAT を実装する必要があります。

NAT と MPLS VPN との統合に関する実装オプション

MPLS VPN ネットワークで NAT を実装するには 2 つのアプローチがあります。 NAT は、すでに NAT でサポートされているカスタマー エッジ（CE）ルータに実装するか、プロバイダー エッジ（PE）ルータに実装できます。 NAT と MPLS VPN の統合機能によって、MPLS クラウド内の PE ルータ上に NAT を実装できます。

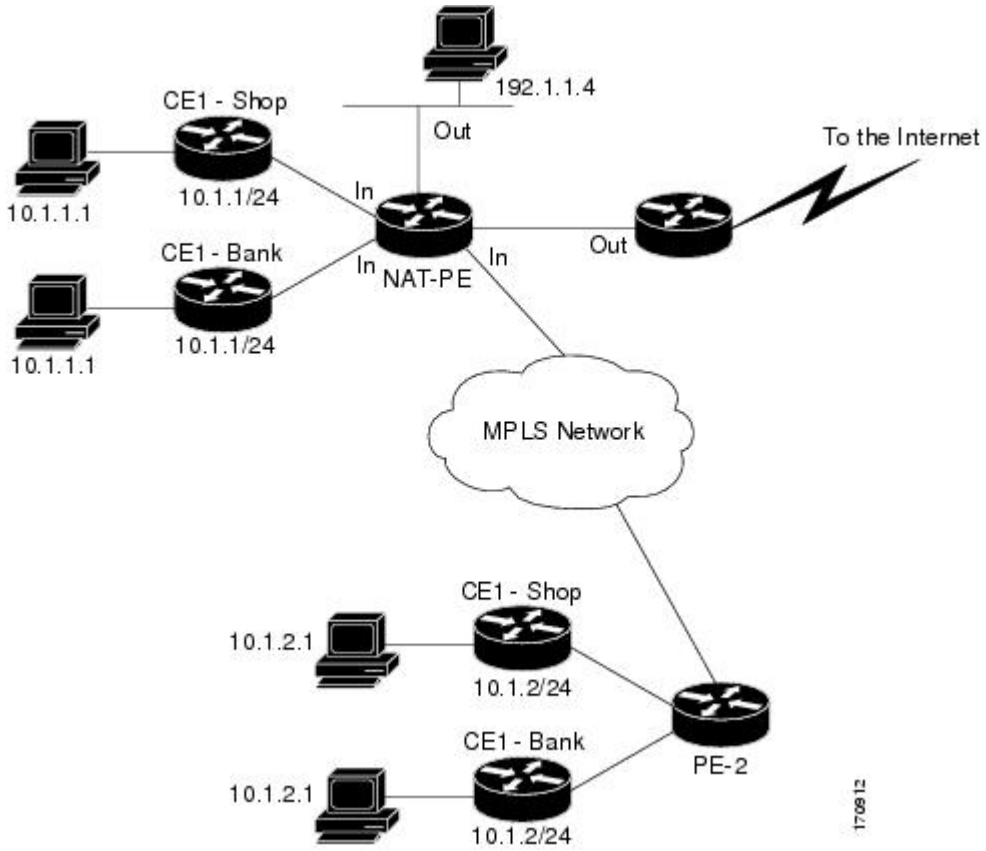
PE ルータ上での NAT 統合のシナリオ

次のシナリオで、PE ルータ上で NAT を統合できます。

- サービス ポイント：共有アクセスは、汎用インターフェイスまたは VPN インターフェイスから行えます。
- NAT ポイント：NAT は、共有アクセス ゲートウェイに直接接続された PE ルータ、または共有アクセス ゲートウェイに直接接続されていない PE ルータに設定できます。
- NAT インターフェイス：共有アクセス ゲートウェイ インターフェイスは通常、NAT の外部インターフェイスとして設定されます。 NAT の内部インターフェイスには、VPN の PE-CE インターフェイス、MPLS バックボーンへのインターフェイス、またはその両方のいずれかです。 共有アクセス ゲートウェイ インターフェイスは、内部インターフェイスとして設定することもできます。
- ルーティング タイプ：コモン サービスは、インターネット接続または共通サーバとすることができます。 インターネット接続に対して、デフォルト ルートがサービスを使用するすべての VPN カスタマーに伝播されます。 共通サーバ アクセスに対して、スタティックまたはダイナミックに学習されるルートが VPN カスタマーに伝播されます。
- NAT 設定：NAT は異なる設定（スタティック、ダイナミック、プール/インターフェイス オーバーロード、ルート マップ）を持つことができます。

以下の図に、MPLS VPN との典型的な NAT 統合を示します。 インターネットおよび集中型メール サービスに接続された PE ルータが、アドレス変換を実行するために使用されます。

図 *10*：*MPLS VPN* との典型的な *NAT* 統合



NAT と MPLS VPN との統合方法

ネットワークを設定する変換のタイプに応じて次の 1 つ以上の作業を実行します。

MPLS VPN を使用した内部ダイナミック NAT の設定

この作業を実行して、MPLS VPN と統合するためのダイナミック変換を行う NAT PE ルータを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat pool** *name start-ip end-ip* **netmask** *netmask*
4. **ip nat** [**inside** | **outside**] **source** [**list** {*access-list-number* | *access-list-name*} | **route-map** *name*] [**interface** *type number* | **pool** *pool-name*] **vrf** *vrf-name*[**overload**]
5. 設定する各 VPN に対してステップ 4 を繰り返します。
6. **ip route vrf** *vrf-name prefix mask interface-type interface-number next-hop-address*
7. 設定する各 VPN に対してステップ 6 を繰り返します。
8. **exit**
9. **show ip nat translations vrf** *vrf-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat pool** *name start-ip end-ip* **netmask** *netmask* 例： `Router(config)# ip nat pool inside 2.2.2.10 2.2.2.10 netmask 255.255.255.0`	NAT で使用される IP アドレス プールを定義します。
ステップ 4	**ip nat** [**inside**	**outside**] **source** [**list** {*access-list-number*	*access-list-name*}	**route-map** *name*] [**interface** *type number*	**pool** *pool-name*] **vrf** *vrf-name*[**overload**] 例： `Router(config)# ip nat inside source list 1 pool mypool vrf shop overload`	特定の VPN に NAT を設定できるようにします。
ステップ 5	設定する各 VPN に対してステップ 4 を繰り返します。	--

	コマンドまたはアクション	目的
ステップ 6	**ip route vrf** *vrf-name prefix mask interface-type interface-number next-hop-address* 例： `Router(config)# ip route vrf shop 0.0.0.0 0.0.0.0 ethernet 0 168.58.88.2`	特定の VPN に NAT を設定できるようにします。
ステップ 7	設定する各 VPN に対してステップ 6 を繰り返します。	--
ステップ 8	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 9	**show ip nat translations vrf** *vrf-name* 例： `Router# show ip nat translations vrf shop`	（任意）仮想ルーティング/転送（VRF）テーブル変換で使用される設定を表示します。

MPLS VPN を使用した内部スタティック NAT の設定

この作業を実行して、MPLS VPN と統合するためにスタティック変換を行う NAT PE ルータを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat inside source** {**static** {**esp** *local-ip* **interface** *type number* | *local-ip global-ip*}} [**extendable** | **mapping-id** *map-id*| **no-alias** | **no-payload** | **redundancy** *group-name* | **route-map** | **vrf** *name*]
4. 設定する各 VPN に対してステップ 3 を繰り返します。
5. **ip route vrf** *vrf-name* **prefix** *prefix mask next-hop-address* **global**
6. 設定する各 VPN に対してステップ 5 を繰り返します。
7. **exit**
8. **show ip nat translations vrf** *vrf-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権EXECモードなど、高位の権限レベルをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**ip nat inside source** {**static** {**esp** *local-ip* **interface** *type number* | *local-ip global-ip*}} [**extendable** | **mapping-id** *map-id*| **no-alias** | **no-payload** | **redundancy** *group-name* | **route-map** | **vrf** *name*]
	
	例：
	`Router(config)#`
	`ip nat inside source static 192.168.121.113 2.2.2.1 vrf shop`
		VRF で内部スタティック変換をイネーブルにします。

ステップ 4	設定する各VPNに対してステップ3を繰り返します。	--

ステップ 5	**ip route vrf** *vrf-name* **prefix** *prefix mask next-hop-address* **global**
	
	例：
	`Router(config)#`
	`ip route vrf shop 0.0.0.0 0.0.0.0 168.58.88.2 global`
		複数のカスタマーでルートを共有できるようになります。

ステップ 6	設定する各VPNに対してステップ5を繰り返します。	--
ステップ 7	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 8	**show ip nat translations vrf** *vrf-name* 例： `Router# show ip nat translations vrf shop`	（任意）VRF 変換に使用される設定を表示します。

MPLS VPN との外部ダイナミック NAT 設定

この手順を実行して、MPLS VPN と統合するためのダイナミック外部変換を行う NAT PE ルータを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat pool outside** *global-ip local-ip* **netmask** *netmask*
4. **ip nat inside source static** *local-ip global-ip* **vrf** *vrf-name*
5. 設定する各 VRF に対してステップ 4 を繰り返します。
6. **ip nat outside source static** *global-ip local-ip* **vrf** *vrf-name*
7. **exit**
8. **show ip nat translations vrf** *vrf-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**ip nat pool outside** *global-ip local-ip* **netmask** *netmask*
	
	例：
	`Router(config)#`
	`ip nat pool outside 4.4.4.1 4.4.4.254 netmask 255.255.255.00`
		設定済みの VRF を NAT 変換ルールと関連付けることができるようにします。

ステップ 4	**ip nat inside source static** *local-ip global-ip* **vrf** *vrf-name* 例： `Router(config)#`	複数のカスタマーでルートを共有できるようになります。

	コマンドまたはアクション	目的
	`ip nat inside source static 192.168.121.113 2.2.2.1 vrf shop`	
ステップ 5	設定する各 VRF に対してステップ 4 を繰り返します。	複数のカスタマーでルートを共有できるようになります。
ステップ 6	**ip nat outside source static** *global-ip local-ip* **vrf** *vrf-name* 例： `Router(config)# ip nat outside source static 168.58.88.2 4.4.4.1 vrf shop`	外部送信元アドレスの NAT 変換をイネーブルにします。
ステップ 7	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 8	**show ip nat translations vrf** *vrf-name* 例： `Router# show ip nat translations vrf shop`	（任意）VRF 変換に使用される設定を表示します。

MPLS VPN との外部スタティック NAT 設定

この作業を実行して、MPLS VPN と統合するためにスタティック外部変換を行う NAT PE ルータを設定します。

手順の概要

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **ip nat pool inside** *global-ip local-ip* **netmask** *netmask*
4. 設定するプールごとにステップ 3 を繰り返します。
5. **ip nat inside source list** *access-list-number* **pool** *pool-name* **vrf** *vrf-name*
6. 設定するプールごとにステップ 5 を繰り返します。
7. **ip nat outside source static** *global-ip local-ip* vrf *vrf-name*
8. 設定するすべての VPN に対してステップ 7 を繰り返します。
9. **exit**
10. **show ip nat translations vrf** *vrf-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure** {**terminal** | **memory** | **network**} 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat pool inside** *global-ip local-ip* **netmask** *netmask* 例： `Router(config)# ip nat pool inside1 2.2.1.1 2.2.1.254 netmask 255.255.255.0`	設定済みの VRF を NAT 変換ルールと関連付けることができるようにします。
ステップ 4	設定するプールごとにステップ 3 を繰り返します。	--

ステップ 5	**ip nat inside source list** *access-list-number* **pool** *pool-name* **vrf** *vrf-name*
	
	例：
	`Router(config)#`
	`ip nat inside source list 1 pool inside2 vrf shop`
		複数のカスタマーでルートを共有できるようになります。

ステップ 6	設定するプールごとにステップ 5 を繰り返します。	アクセス リストを定義します。

ステップ 7	**ip nat outside source static** *global-ip local-ip* vrf *vrf-name*
	
	例：
	`Router(config)#`
	`ip nat outside source static 168.58.88.2 4.4.4.1 vrf shop`
		複数のカスタマーでルートを共有できるようになります。

ステップ 8	設定するすべての VPN に対してステップ 7 を繰り返します。	--
ステップ 9	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**show ip nat translations vrf** *vrf-name* 例： `Router# show ip nat translations vrf shop`	（任意）VRF 変換に使用される設定を表示します。

MPLS VPN と NAT 統合の設定例

MPLS VPN との内部ダイナミック NAT の設定例

次に、MPLS VPN との内部ダイナミック NAT の設定例を示します。

```
!
ip nat pool inside 2.2.2.10 2.2.2.10 netmask 255.255.255.0
ip nat inside source list 1 pool inside vrf bank overload
ip nat inside source list 1 pool inside vrf park overload
ip nat inside source list 1 pool inside vrf shop overload
!
ip route vrf shop 0.0.0.0 0.0.0.0 Ethernet1/3 168.58.88.2
ip route vrf bank 0.0.0.0 0.0.0.0 Ethernet1/3 168.58.88.2
ip route vrf park 0.0.0.0 0.0.0.0 Ethernet1/3 168.58.88.2
!
access-list 1 permit 192.168.0.0 0.0.255.255
```

MPLS VPN との内部スタティック NAT の設定例

次に、MPLS VPN との内部スタティック NAT の設定例を示します。

```
!
ip nat inside source static 192.168.121.113 2.2.2.1 vrf shop
ip nat inside source static 192.168.122.49 2.2.2.2 vrf shop
ip nat inside source static 192.168.121.113 2.2.2.3 vrf bank
ip nat inside source static 192.168.22.49 2.2.2.4 vrf bank
ip nat inside source static 192.168.121.113 2.2.2.5 vrf park
ip nat inside source static 192.168.22.49 2.2.2.6 vrf park
ip nat inside source static 192.168.11.1 2.2.2.11 vrf shop
ip nat inside source static 192.168.11.3 2.2.2.12 vrf shop
ip nat inside source static 140.48.5.20 2.2.2.13 vrf shop
!
ip route 2.2.2.1 255.255.255.255 Ethernet1/0 192.168.121.113
ip route 2.2.2.2 255.255.255.255 Ethernet1/0 192.168.121.113
ip route 2.2.2.3 255.255.255.255 Serial2/1.1 192.168.121.113
ip route 2.2.2.4 255.255.255.255 Serial2/1.1 192.168.121.113
ip route 2.2.2.5 255.255.255.255 FastEthernet0/0 192.168.121.113
ip route 2.2.2.6 255.255.255.255 FastEthernet0/0 192.168.121.113
ip route 2.2.2.11 255.255.255.255 Ethernet1/0 192.168.121.113
ip route 2.2.2.12 255.255.255.255 Ethernet1/0 192.168.121.113
ip route 2.2.2.13 255.255.255.255 Ethernet1/0 192.168.121.113
```

MPLS VPN との外部ダイナミック NAT の設定例

次に、MPLS VPN との外部ダイナミック NAT の設定例を示します。

```
!
ip nat pool outside 4.4.4.1 4.4.4.254 netmask 255.255.255.0
ip nat inside source static 192.168.121.113 2.2.2.1 vrf shop
ip nat inside source static 192.168.122.49 2.2.2.2 vrf shop
ip nat inside source static 192.168.121.113 2.2.2.3 vrf bank
ip nat inside source static 192.168.22.49 2.2.2.4 vrf bank
ip nat inside source static 192.168.121.113 2.2.2.5 vrf park
ip nat inside source static 192.168.22.49 2.2.2.6 vrf park
ip nat outside source list 1 pool outside
!
```

MPLS VPN との外部スタティック NAT の設定例

次に、MPLS VPN との外部スタティック NAT の設定例を示します。

```
!
ip default-gateway 10.1.15.1
ip nat pool inside1 2.2.1.1 2.2.1.254 netmask 255.255.255.0
ip nat pool inside2 2.2.2.1 2.2.2.254 netmask 255.255.255.0
ip nat pool inside3 2.2.3.1 2.2.3.254 netmask 255.255.255.0
ip nat inside source list 1 pool inside2 vrf bank
ip nat inside source list 1 pool inside3 vrf park
ip nat inside source list 1 pool inside1 vrf shop
ip nat outside source static 168.58.88.2 4.4.4.1 vrf bank
ip nat outside source static 18.68.58.1 4.4.4.2 vrf park
ip nat outside source static 168.58.88.1 4.4.4.3 vrf shop
ip classless
ip route 192.170.10.0 255.255.255.0 Ethernet1/0 192.168.121.113
ip route 192.170.11.0 255.255.255.0 Serial2/1.1 192.168.121.113
ip route 192.170.12.0 255.255.255.0 FastEthernet0/0 192.168.121.113
ip route vrf shop 0.0.0.0 0.0.0.0 168.58.88.2 global
ip route vrf bank 0.0.0.0 0.0.0.0 168.58.88.2 global
ip route vrf park 0.0.0.0 0.0.0.0 168.58.88.2 global
no ip http server
!
access-list 1 permit 192.168.0.0 0.0.255.255
```

次の作業

- ネットワーク アドレス変換の詳細と IP アドレス節約のための NAT の設定については、「IP アドレス節約のための NAT 設定」モジュールを参照してください。
- NAT を確認、モニタ、およびメンテナンスするには、「NAT のモニタリングおよびメンテナンス」モジュールを参照してください。
- アプリケーション レベル ゲートウェイで NAT を使用するには、「アプリケーション レベル ゲートウェイでの NAT の使用」モジュールを参照してください。
- ハイ アベイラビリティを得るための NAT の設定については、「ハイ アベイラビリティ用 NAT の設定」モジュールを参照してください。

MPLS VPN との NAT の統合に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
IOS コマンド	『Cisco IOS Master Command List』
NAT コマンド	『Cisco IOS IP Addressing Services Command Reference』

標準および RFC

標準および RFC	タイトル
RFC 2547	『*BGP/MPLS VPNs*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

MPLS VPN と NAT の統合に関する機能情報

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

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

表 *7*：*MPLS VPN* と *NAT* の統合に関する機能情報

機能名	リリース	機能の設定情報
MPLS VPN と NAT の統合	12.1(13)T 15.1(1)SY	MPLS VPN と NAT の統合機能を使用すると、1 つのデバイスで、複数のマルチプロトコル ラベル スイッチング（MPLS）VPN がともに動作するように設定できます。

第 8 章

NAT のモニタリングおよびメンテナンス

このモジュールでは、次の内容について説明します。

- 変換情報と統計表示を使用したネットワーク アドレス変換（NAT）のモニタリング。
- タイムアウトの期限切れ前に NAT 変換をクリアすることによる、NAT のメンテナンス。
- システム エラー メッセージ、例外、他の情報の syslog によるログとトラッキングを利用した、NAT 変換のロギングのイネーブル化。

- 機能情報の確認，165 ページ
- NAT のモニタリングおよびメンテナンスの前提条件，166 ページ
- NAT のモニタリングおよびメンテナンスの制約事項，166 ページ
- NAT のモニタリングとメンテナンスについて，166 ページ
- NAT のモニタリング方法とメンテナンス方法，168 ページ
- NAT のモニタリングおよびメンテナンスの例，172 ページ
- 次の作業，173 ページ
- NAT のモニタリングおよびメンテナンスに関するその他の関連資料，173 ページ
- NAT のモニタリングとメンテナンスの機能情報，174 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

NAT のモニタリングおよびメンテナンスの前提条件

このモジュールの作業を実行する前に、「IP アドレス節約のための NAT 設定」モジュールで説明されている概念をよく理解し、ご使用のネットワークで NAT を設定しておく必要があります。

NAT のモニタリングおよびメンテナンスの制約事項

一連のルールを設定してネットワーク アドレス変換（NAT）データベースに変更を加えると、NAT データベースが過渡状態となります。データベースは、これらの変更が同期されると動作を開始します。 過渡状態の NAT では、NAT データベースへのアクセスを必要とする操作は許可されません。NAT データベースにアクセスしようとすると、「% NAT: System Busy. Try later.」メッセージがデバイスのコンソールに表示されます。 **debug** コマンドのログに、この過渡状態期間にドロップされたパケットに関する情報が表示されます。

この動作を回避するには、NAT 設定の変更をずらして行います。 または、NAT ルールの適用時に、**no ip nat inside** および **no ip nat outside** コマンドを使用して、インターフェイス レベルで NAT を一時的にディセーブルにします。

NAT のモニタリングとメンテナンスについて

NAT の表示内容

IP ネットワーク アドレス変換（NAT）の変換情報には、2 つの基本タイプがあります。

変換エントリ

次の内容を含む、変換エントリ情報。

- アドレスを識別するポートのプロトコル。
- 1 つ以上の内部のローカル IP アドレスを外部に対して表すために使用できる合法的な IP アドレス。
- 内部ネットワーク上のホストに割り当てられた IP アドレス（多くの場合 NIC やサービス プロバイダーにより割り当てられた合法的アドレスではない）。
- 外部ホストが内部ネットワークに出現するときの IP アドレス（多くの場合 NIC やサービス プロバイダーにより割り当てられた合法的アドレスではない）。

- 外部ネットワーク上のホストに、所有者が割り当てた IP アドレス。
- エントリが作成されてからの経過時間（「時間：分：秒」形式）。
- エントリが最後に使用されてからの経過時間（「時間：分：秒」形式）。
- 変換タイプを示すフラグ。 次のようなフラグがあります。
  - extended：拡張変換。
  - static：スタティック変換。
  - destination：循環式変換。
  - outside：外部変換。
  - timing out：TCP finish（FIN）または reset（RST）フラグにより、以後変換を使用しない。

スタティック情報

スタティック情報には次のような内容が含まれます。

- システム内でアクティブな変換の総数。 この数値は、変換が作成されるたびに増加し、変換がクリアまたはタイムアウトになるたびに減少します。
- **ip nat outside** コマンドで outside とマークされたインターフェイスのリスト。
- **ip nat inside** コマンドで inside とマークされたインターフェイスのリスト。
- ソフトウェアが変換テーブル参照を行ってエントリを発見した回数。
- ソフトウェアが変換テーブル参照を行ったが、エントリが見つからず、エントリ作成を試行する必要があった回数。
- ルータが起動されてから、期限切れになった変換の累積数。
- ダイナミック マッピングについての情報。
- 内部送信元変換についての情報。
- 変換に使用されているアクセス リスト番号。
- プールの名前。
- そのプールを使用している変換の数。
- プールで使用されている IP ネットワーク マスク。
- プール範囲の開始 IP アドレス。
- プール範囲の終了 IP アドレス。
- プールのタイプ。 汎用タイプまたは循環タイプです。
- 変換に使用可能なプール内のアドレスの数。

- 使用されているアドレスの数。
- プールからの割り当てに失敗した数。

NAT では、ログ オプションを持つアクセス コントロール リスト（ACL）をサポートしません。同様の機能は、次のオプションのいずれかを使用して実現できます。

- ロギング オプションを持つ物理インターフェイスまたは仮想 LAN（VLAN）
- NetFlow の使用。
- syslog 機能の使用。

Syslog の使用方法

Syslog 分析により、システム エラー メッセージ、例外、他の情報（デバイス コンフィギュレーションの変更など）の集約的なログ作成とトラッキングが行えます。記録されたエラーメッセージ データを使用して、ルータとネットワーク パフォーマンスの分析が行えます。 業務に重要な情報とメッセージをまとめたレポートを作成するよう、Syslog 分析をカスタマイズすることが可能です。

詳しくは、『*Resource Manager Essentials and Syslog Analysis: How-To*』マニュアルを参照してください。

http://www.cisco.com/warp/public/477/RME/rme_syslog.html

NAT のモニタリング方法とメンテナンス方法

NAT 変換情報の表示

手順の概要

1. **enable**
2. **show ip nat translations** [**verbose**]
3. **show ip nat statistics**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**show ip nat translations** [**verbose**] 例： `Device# show ip nat translations`	（任意）アクティブな NAT 変換を表示します。
ステップ 3	**show ip nat statistics** 例： `Device# show ip nat statistics`	（任意）アクティブな NAT 変換の統計を表示します。

例：

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

```
Device# show ip nat translations

Pro Inside global         Inside local       Outside local        Outside global
tcp 192.168.1.1:514      192.168.2.3:53     192.168.2.22:256     192.168.2.22:256
tcp 192.168.1.1:513      192.168.2.2:53     192.168.2.22:256     192.168.2.22:256
tcp 192.168.1.1:512      192.168.2.4:53     192.168.2.22:256     192.168.2.22:256
Total number of translations: 3
```

次に、**show ip nat translations verbose** コマンドの出力例を示します。

```
Device# show ip nat translations verbose

Pro Inside global        Inside local       Outside local      Outside global
tcp 192.168.1.1:514      192.168.2.3:53     192.168.2.22:256     192.168.2.22:256
         create 04/09/11 10:51:48, use 04/09/11 10:52:31, timeout: 00:01:00
         Map-Id(In):1, Mac-Address: 0000.0000.0000 Input-IDB: GigabitEthernet0/3/1
          entry-id: 0x8ef80350, use_count:1
tcp 192.168.1.1:513      192.168.2.2:53     192.168.2.22:256     192.168.2.22:256
         create 04/09/11 10:51:48, use 04/09/11 10:52:31, timeout: 00:01:00
         Map-Id(In):1, Mac-Address: 0000.0000.0000 Input-IDB: GigabitEthernet0/3/1
          entry-id: 0x8ef801b0, use_count:1
tcp 192.168.1.1:512      192.168.2.4:53     192.168.2.22:256     192.168.2.22:256
         create 04/09/11 10:51:48, use 04/09/11 10:52:31, timeout: 00:01:00
         Map-Id(In):1, Mac-Address: 0000.0000.0000 Input-IDB: GigabitEthernet0/3/1
          entry-id: 0x8ef80280, use_count:1
Total number of translations: 3
```

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

```
Device# show ip nat statistics

Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Outside interfaces:
GigabitEthernet0/3/0
Inside interfaces:
GigabitEthernet0/3/1
Hits: 3228980 Misses: 3
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool pool1 refcount 3
  pool pool1: netmask 255.255.255.0
  start 198.168.1.1 end 198.168.254.254
  type generic, total addresses 254, allocated 0 (0%), misses 0
  longest chain in pool: pool1's addr-hash: 0, average len 0,chains 0/256
  Pool stats drop: 0 Mapping stats drop: 0
  Port block alloc fail: 0
```

```
IP alias add fail: 0
Limit entry add fail: 0
```

タイムアウト前の NAT エントリのクリア

デフォルトでは、ある時点でダイナミック アドレス変換は NAT 変換テーブルからタイムアウトになります。 タイムアウトの前にエントリをクリアするには、次の作業を実行します。

手順の概要

1. **enable**
2. **clear ip nat translation inside** *global-ip local-ip* **outside** *local-ip global-ip*
3. **clear ip nat translation outside** *global-ip local-ip*
4. **clear ip nat translation** *protocol* **inside** *global-ip global-port local-ip local-port* **outside** *local-ip local-port global-ip global-port*
5. **clear ip nat translation** {* | [**forced**] | [**inside** *global-ip local-ip*] [**outside** *local-ip global-ip*]}
6. **clear ip nat translation inside** *global-ip local-ip* [**forced**]
7. **clear ip nat translation outside** *local-ip global-ip* [**forced**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear ip nat translation inside** *global-ip local-ip* **outside** *local-ip global-ip* 例： `Device# clear ip nat translation inside 192.168.2.209 192.168.2.95 outside 192.168.2.100 192.168.2.101`	（任意）内部変換を含む単一のダイナミック ハーフエントリ、またはダイナミック設定で作成された内部変換と外部変換の両方をクリアします。 • ダイナミック ハーフエントリがクリアされるのは、子変換を持たない場合だけです。
ステップ 3	**clear ip nat translation outside** *global-ip local-ip* 例： `Device# clear ip nat translation outside 192.168.2.100 192.168.2.80`	（任意）ダイナミック設定で作成された外部変換を含む単一のダイナミック ハーフエントリをクリアします。 • ダイナミック ハーフエントリがクリアされるのは、子変換を持たない場合だけです。
ステップ 4	**clear ip nat translation** *protocol* **inside** *global-ip global-port local-ip local-port* **outside** *local-ip local-port global-ip global-port*	（任意）UDP 変換エントリだけをクリアします。

	コマンドまたはアクション	目的
	例： `Device # clear ip nat translation udp inside 192.168.2.209 1220 192.168.2.195 1220 outside 192.168.2.13 53 192.168.2.132 53`	
ステップ 5	**clear ip nat translation** {* | [**forced**] | [**inside** *global-ip local-ip*] [**outside** *local-ip global-ip*]} 例： `Device# clear ip nat translation *`	（任意）ダイナミック変換すべて（***** もしくは **forced** キーワードを使用）、内部変換を含む単一のダイナミック ハーフエントリ、外部変換を含む単一のダイナミック ハーフエントリのいずれかをクリアします。 • 単一のダイナミック ハーフエントリがクリアされるのは、子変換を持たない場合だけです。
ステップ 6	**clear ip nat translation inside** *global-ip local-ip* [**forced**] 例： `Device# clear ip nat translation inside 192.168.2.209 192.168.2.195 forced`	（任意）対応する外部変換の有無にかかわらず、ダイナミック設定で作成された内部変換を含む単一のダイナミック ハーフエントリおよびその子変換を、強制的にクリアします。 • ダイナミック ハーフエントリは、子変換の有無に関係なく、必ずクリアされます。
ステップ 7	**clear ip nat translation outside** *local-ip global-ip* [**forced**] 例： `Device# clear ip nat translation outside 192.168.2.100 192.168.2.80 forced`	（任意）ダイナミック設定で作成された外部変換を含む単一のダイナミック ハーフエントリおよびその子変換を、強制的にクリアします。 • ダイナミック ハーフエントリは、子変換の有無に関係なく、必ずクリアされます。

Syslog での NAT 変換ロギングのイネーブル化

ネットワーク アドレス変換（NAT）をイネーブルにするには、**syslog** コマンドを使用します。

Syslog 分析により、システム エラー メッセージ、例外、他の情報（NAT 変換など）の集約的なログ作成とトラッキングが行えます。 記録されたエラー メッセージ データを使用して、ルータとネットワーク パフォーマンスの分析が行えます。 業務に重要な情報とメッセージをまとめたレポートを作成するよう、Syslog 分析をカスタマイズすることが可能です。

はじめる前に

この作業の実行前に、ロギングのイネーブル化の確認、サーバの IP アドレスの設定、捕捉するメッセージのレベル確定など、必要な **syslog** コマンドを特定しておく必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat log translations syslog**
4. **no logging console**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat log translations syslog** 例： `Device(config)# ip nat log translations syslog`	syslog の NAT 変換のロギングをイネーブルにします。
ステップ 4	**no logging console** 例： `Device(config)# no logging console`	（任意）ログのコンソールへの表示をディセーブルにします。 • コンソールへのロギングは、デフォルトでイネーブルになっています。

NAT のモニタリングおよびメンテナンスの例

例：Syslog での NAT 変換ロギングのイネーブル化

次の例に、syslog にネットワーク アドレス変換（NAT）エントリを記録する方法を示します。

```
Device(config)# logging on
Device(config)# logging 10.1.1.1
Device(config)# logging trap informational
Device(config)# ip nat log translations syslog
```

NAT 情報の記録フォーマット（インターネット制御メッセージプロトコル（ICMP）ping には NAT オーバーロード設定を介するなど）は、次のとおりです。

```
Apr 25 11:51:29 [10.0.19.182.204.28] 1: 00:01:13: NAT:Created icmp
10.135.5.2:7 171 10.106.151.30:7171 192.168.2.209:7171
192.168.2.209:7171
Apr 25 11:52:31 [10.0.19.182.204.28] 8: 00:02:15: NAT:Deleted icmp
10.135.5.2:7 172 10.106.151.30:7172 192.168.2.209:7172
192.168.2.209:7172
```

例：UDP NAT 変換のクリア

次に、UDP エントリのクリア前後のネットワーク アドレス変換（NAT）エントリの例を示します。

```
Device# show ip nat translation
Pro Inside global         Inside local         Outside local      Outside global
udp 192.168.2.20:1220     192.168.2.95:1220    192.168.2.22:53    192.168.2.20:53
tcp 192.168.2.20:11012    192.168.2.209:11012  171.69.1.220:23    192.168.2.20:23
tcp 192.168.2.20:1067     192.168.2.20:1067    192.168.2.20:23    192.168.2.20:23

Device# clear ip nat translation udp inside 192.168.2.20:1067 192.168.2.20:1067 outside
192.168.2.20:23 192.168.2.20:23
Device# show ip nat translation

Pro Inside global      Inside local        Outside local      Outside global
udp 192.168.2.20:1220  192.168.2.95:1220   192.168.2.22:53    192.168.2.20:53
tcp 192.168.2.20:11012 192.168.2.209:11012 171.69.1.220:23    192.168.2.20:23
```

次の作業

- アプリケーション レベル ゲートウェイで使用するための NAT の設定については、「NAT でのアプリケーション レベル ゲートウェイの使用」モジュールを参照してください。
- NAT と MPLS VPN の統合については、「MPLS VPN と NAT の統合」モジュールを参照してください。
- ハイ アベイラビリティを得るための NAT の設定については、「ハイ アベイラビリティ用 NAT の設定」モジュールを参照してください。

NAT のモニタリングおよびメンテナンスに関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
NAT コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『Cisco IOS IP Addressing Services Command Reference』
Resource Manager Essentials と Syslog 分析：方法	『Resource Manager Essentials and Syslog Analysis: How to』
IP アドレス節約のための NAT	「Configuring NAT for IP Address Conservation」モジュール

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NAT のモニタリングとメンテナンスの機能情報

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

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

表 *8*：*NAT* のモニタリングとメンテナンスの機能情報

機能名	リリース	機能情報
NAT：ダイナミック NAT ハーフエントリの強制的クリア	12.2(15)T	2 つ目の **forced** キーワードが **clear ip nat translation** コマンドに追加され、子変換の有無にかかわらずハーフエントリを削除できるようになりました。

第 9 章

VRF 単位での NAT の High-Speed ロギングのイネーブル化

VRF 単位での NAT の High-Speed ロギングのイネーブル化機能を使用すると、仮想ルーティングおよび転送（VRF）インスタンスに対し、ネットワーク アドレス変換（NAT）の High-Speed ロギング（HAL）をイネーブルおよびディセーブルにできます。

このモジュールでは、VRF に対し HSL をイネーブルにする方法について説明します。

- 機能情報の確認，177 ページ
- VRF 単位での NAT の High-Speed ロギングのイネーブル化について，178 ページ
- VRF 単位での NAT の High-Speed ロギングのイネーブル化の設定方法，179 ページ
- VRF 単位での NAT の High-Speed ロギングのイネーブル化の設定例，181 ページ
- VRF 単位での NAT の High-Speed ロギングのイネーブル化に関するその他の関連資料，181 ページ
- VRF 単位での NAT の High-Speed ロギングのイネーブル化の機能情報，182 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

VRF 単位での NAT の High-Speed ロギングのイネーブル化について

NAT の High-Speed ロギング

ネットワーク アドレス変換（NAT）では、High-Speed ロギング（HSL）がサポートされます。HSL が設定されると、NAT により、ルーティング デバイスを経由して外部コレクタに送信されるパケットのログが提供されます（バージョン 9 NetFlow 形式のレコードに類似）。 レコードは、各バインディング（バインディングは、ローカルアドレスとそのローカルアドレスの変換先となるグローバルアドレス間のアドレスバインディング）について、セッションが作成および破棄されるときに送信されます。 セッション レコードには、5 タプルの情報すべて（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコル）が含まれます。 タプルは、要素の順序付きリストです。 また、NAT は、NAT プールのアドレスがなくなると（プール枯渇とも呼びます）、HSL メッセージを送信します。 プール枯渇メッセージはレート制限を受けるため、プール枯渇状態になったすべてのパケットが HSL メッセージをトリガーすることはありません。

次の表に、HSL バインドおよびセッションの作成または破棄のテンプレートを示します。

表 *9*：*HSL* バインドおよびセッションの作成または破棄のテンプレート

フィールド	フォーマット	ID	値
送信元 IP アドレス	IPv4 アドレス	8	不定
変換された送信元 IP アドレス	IPv4 アドレス	225	不定
宛先 IP アドレス	IPv4 アドレス	12	不定
変換された宛先 IP アドレス	IPv4 アドレス	226	不定
元の送信元ポート	16 ビット ポート	7	不定
変換された送信元ポート	16 ビット ポート	227	不定
元の宛先ポート	16 ビット ポート	11	不定
変換された宛先ポート	16 ビット ポート	228	不定
仮想ルーティングおよび転送（VRF）ID	32 ビット ID	234	不定

フィールド	フォーマット	ID	値
プロトコル	8 ビット値	4	不定
イベント	8 ビット値	230	0：無効 1：イベントの追加 2：イベントの削除
UNIX タイムスタンプ（ミリ秒単位）	64 ビット値	323	不定 （注） このフィールドは、リリース バージョンに応じて使用可能になります。

次の表に、HSL プール枯渇テンプレートを示します。

表 *10*： *HSL* プール枯渇のテンプレート

フィールド	フォーマット	ID	値
NAT プール ID	32 ビット値	283	不定
NAT イベント	8 ビット値	230	3：プール枯渇

VRF 単位での NAT の High-Speed ロギングのイネーブル化の設定方法

NAT 変換の High-Speed ロギングのイネーブル化

すべてのネットワーク アドレス変換（NAT）の変換または特定の VPN の変換のみの High-Speed ロギング（HSL）をイネーブルまたはディセーブルにできます。

最初に、**ip nat log translations flow-export v9 udp destination** コマンドを使用して、すべての VPN および非 VPN 変換の HSL をイネーブルにする必要があります。 VPN 変換は、仮想ルーティングおよび転送（VRF）変換とも呼ばれます。

すべての NAT 変換の HSL をイネーブルにしたら、**ip nat log translations flow-export v9** *vrf-name* コマンドを使用して、特定の VPN の変換をイネーブルまたはディセーブルにできます。 このコ

マンドを使用すると、コマンドが明示的にイネーブルにされた VPN を除くすべての VPN の HSL がディセーブルになります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat log translations flow-export v9 udp destination** *addr port* **source** *interface interface-number*
4. **ip nat log translations flow-export v9** {*vrf-name* | **global-on**}
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat log translations flow-export v9 udp destination** *addr port* **source** *interface interface-number* 例： `Device(config)# ip nat log translations flow-export v9 udp destination 10.10.0.1 1020 source GigabitEthernet 0/0/0`	すべての VPN および非 VPN 変換の High-Speed ロギングをイネーブルにします。
ステップ 4	**ip nat log translations flow-export v9** {*vrf-name*	**global-on**} 例： `Device(config)# ip nat log translations flow-export v9 VPN-18`	特定の NAT VPN 変換の High-Speed ロギングをイネーブルまたはディセーブルにします。
ステップ 5	**exit** 例： `Device(config)# exit`	（任意）グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

VRF 単位での NAT の High-Speed ロギングのイネーブル化の設定例

例：NAT 変換の High-Speed ロギングのイネーブル化

```
Device# configure terminal
Device(config)# ip nat log translations flow-export v9 udp destination 10.10.0.1 1020 source
 GigabitEthernet 0/0/0
Device(config)# ip nat log translations flow-export v9 VPN-18
Device(config)# exit
```

VRF 単位での NAT の High-Speed ロギングのイネーブル化に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
NAT コマンド	『Cisco IOS IP Addressing Services Command Reference』

標準および RFC

標準/RFC	タイトル

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

VRF 単位での NAT の High-Speed ロギングのイネーブル化の機能情報

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

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

表 *11*：*VRF* 単位での *NAT* の *High-Speed* ロギングのイネーブル化の機能情報

機能名	リリース	機能情報
VRF 単位での NAT の High-Speed ロギングのイネーブル化	Cisco IOS XE Release 3.1S	VRF 単位での NAT の High-Speed ロギングのイネーブル化機能を使用すると、仮想ルーティングおよび転送（VRF）インスタンスに対し、ネットワーク アドレス変換（NAT）の High-Speed ロギング（HAL）をイネーブルおよびディセーブルにできます。 **ip nat log translations flow-export** コマンドが導入または変更されました。

第 10 章

ステートレス ネットワーク アドレス変換64

ステートレス ネットワーク アドレス変換 64（NAT64）機能は、IPv6 パケットの IPv4 パケットへの変換およびその逆の変換を行う変換メカニズムを提供します。 変換では、拡張ヘッダーを含む IPv6 ヘッダー全体の解析、関連情報の取得、および IPv6 ヘッダーの IPv4 ヘッダーへの変換が行われます。 同様に、IPv4 ヘッダーは IPv4 オプションを含む全体が解析され、IPv6 ヘッダーが作成されます。 この処理は、ステートレス NAT64 変換用に設定されたインターフェイス上で、パケットごとに行われます。

ステートレス NAT64 トランスレータは、ネイティブ IPv6 または IPv4 通信をイネーブルにし、IPv4 および IPv6 ネットワークが容易に共存できるようにします。

ステートレス NAT64 トランスレータでは、データパスにステート情報を保持しません。 このトランスレータは、IPv4/IPv6 変換のフレームワークに関する IETF ワーキング グループ Behavior Engineering for Hindrance Avoidance（BEHAVE）のドラフトに基づいています。 このドラフトでは、トランスポート層ヘッダーおよびインターネット制御メッセージ プロトコル（ICMP）などの、IPv6 パケットを IPv4 に（およびその逆に）変換するメカニズムについて説明しています。

- 機能情報の確認，184 ページ
- ステートレス ネットワーク アドレス変換 64 の制約事項，184 ページ
- ステートレス ネットワーク アドレス変換 64 について，184 ページ
- ステートレス ネットワーク アドレス変換 64 の設定方法，187 ページ
- ステートレス ネットワーク アドレス変換 64 の設定例，197 ページ
- その他の関連資料，198 ページ
- ステートレス ネットワーク アドレス変換 64 の機能情報，199 ページ
- 用語集，200 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

ステートレス ネットワーク アドレス変換 64 の制約事項

ステートレス NAT64 機能には、次のような制約事項が適用されます。

- ステートレス変換には、有効な IPv4-Translatable アドレスのみを使用できます。
- マルチキャストはサポートされません。
- 対応するアプリケーション層ゲートウェイ（ALG）を使用しないアプリケーションは、ステートレス NAT64 トランスレータで正常に動作しない場合があります。
- IPv4 オプション、IPv6 ルーティング ヘッダー、ホップバイホップ拡張ヘッダー、宛先オプション ヘッダー、および送信元ルーティング ヘッダーの変換はサポートされません。
- UDP チェックサムを含まない、フラグメント化された IPv4 UDP パケットは変換されません。
- ゼロ UDP チェックサムを持つ IPv6 パケットは変換されません。

ステートレス ネットワーク アドレス変換 64 について

IPv6 と IPv4 ネットワークにおける IP データグラムのフラグメンテーション

IPv4 ネットワークでは、すべての中間ルータが、IP データグラムのフラグメンテーションを行えます。 一方、IPv6 ネットワークでフラグメンテーションを行えるのは、発信元 IPv6 ホストのみです。 IPv6 ネットワークでのフラグメンテーションは IPv6 ホストによって行われるため、パスの最大伝送単位（PMTU）検出も IPv6 ホストが行う必要があります。 一方、IPv4 ネットワークで PMTU 検出を行うことはできません。IPv4 ネットワークでは、ルータがパケットのフラグメント化を許可されているためです。 IPv4 ネットワークでは、ステートレス NAT64 トランスレータを使用して、IPv6 データグラムがフラグメント化され、IPv4 ヘッダーに Don't Fragment（DF）ビッ

トが設定されます。 同様にトランスレータでは、IPv4 フラグメントが受信された場合、フラグメント ヘッダーを IPv6 パケットに追加できます。

ステートレス NAT64 変換の ICMP の変換

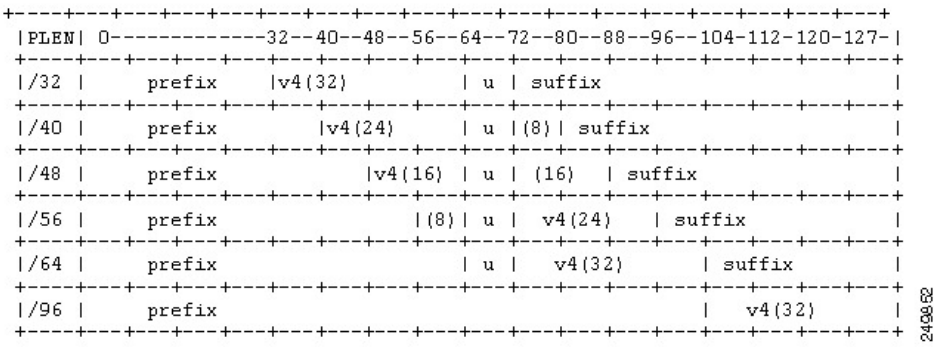
IP/ICMP 変換アルゴリズムに関する IETF ドラフトでは、IPv4 と IPv6 の間で変換する必要がある ICMP タイプまたはコードについて説明しています。 ICMP エラーは、実際の IP ヘッダーとトランスポート ヘッダーに埋め込まれます。 ICMP エラーが IP ヘッダーに埋め込まれるため、IP ヘッダーは正しく変換されません。 ICMP エラー パケットでは、ステートレス NAT64 変換は、外部ヘッダー用に 1 回と埋め込みヘッダー用にもう 1 回の、計 2 回適用する必要があります。

IPv4-Translatable IPv6 アドレス

IPv4-Translatable IPv6 アドレスは、ステートレス変換で使用するために IPv6 ノードに割り当てられる IPv6 アドレスです。 IPv4-Translatable アドレスは、可変長プレフィックス、埋め込み IPv4 アドレス、固定 Universal ビット（u-bit）で構成され、サフィックスが含まれる場合もあります。 IPv4 埋め込み IPv6 アドレスは、その 32 ビットに IPv4 アドレスが含まれている IPv6 アドレスです。 この形式は、IPv4-Converted および IPv4-Translatable IPv6 アドレスの両方で同じです。

以下の図は、複数の異なるプレフィックスおよび埋め込み IPv4 アドレス位置を持つ、IPv4-Translatable IPv6 アドレス形式を示しています。

図 *11*：*IPv4-Translatable IPv6* アドレス形式



プレフィックス形式

IPv6アドレスの先頭にある一連のビットは、フォーマットプレフィックスと呼ばれています。プレフィックス長は、プレフィックスを構成する、アドレスの左端の連続ビット数を指定する10進数値です。

埋め込み IPv4 アドレスを使用して、IPv6 パケットから IPv4 アドレスが作成されます。 ステートレス NAT64 トランスレータでは、プレフィックス長を使用して、IPv6-Translatable アドレスに埋め込まれているIPv4アドレスを取得する必要があります。 このトランスレータは、プレフィック

スおよびプレフィックス長に基づいてIPv6-Translatableアドレスを作成し、アルゴリズムに基づいて IPv4 アドレスを埋め込む必要があります。

IETF アドレス形式 BEHAVE ドラフトに従い、IPv6 アーキテクチャに定義された u-bit（ビット 70）をゼロに設定する必要があります。 u-bit の使用方法については、RFC 2464 を参照してください。 予約済みのオクテット（u-octet とも呼びます）は、IPv6アドレッシングアーキテクチャで定義されているホスト ID 形式との互換性のために予約されています。 IPv6 パケットを作成する場合、トランスレータでは、u-bit が改ざんされておらず、RFC 2373 に示されている値に設定されていることを確認する必要があります。 サフィックスは、トランスレータによりすべてゼロに設定されます。 IETF では、u-octet の 8 ビット（ビット範囲 64 ～ 71）をゼロに設定することを推奨しています。

32、40、48、56、64、または 96 のプレフィックス長がステートレス NAT64 変換でサポートされます。 Well Known Prefix（WKP）はサポートされません。 トラフィックが IPv4-to-IPv6 方向で送信される場合、ステートフル変換でのみ、WKP または設定済みプレフィックスのいずれかを追加できます。

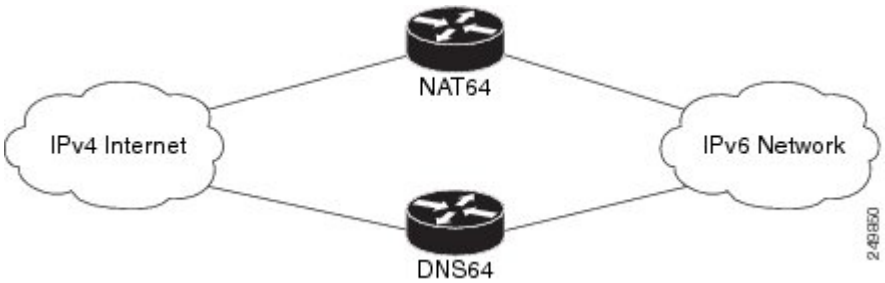
サポートされるステートレス NAT64 シナリオ

IPv4/IPv6 変換に関する IETF フレームワーク ドラフトでは、ステートレス NAT64 変換に関する 8 つの異なるネットワーク通信シナリオについて説明しています。 この項で説明する次のシナリオは、Cisco IOS ステートレス NAT64 機能によってサポートされています。

- シナリオ 1：IPv6 ネットワークから IPv4 インターネット
- シナリオ 2：IPv4 インターネットから IPv6 ネットワーク
- シナリオ 5：IPv6 ネットワークから IPv4 ネットワーク
- シナリオ 6：IPv4 ネットワークから IPv6 ネットワーク

以下の図は、シナリオ 1 と 2 のステートレス変換を示しています。 IPv6 専用ネットワークが IPv4 インターネットと通信します。

図 *12*：シナリオ *1* および *2* のステートレス変換

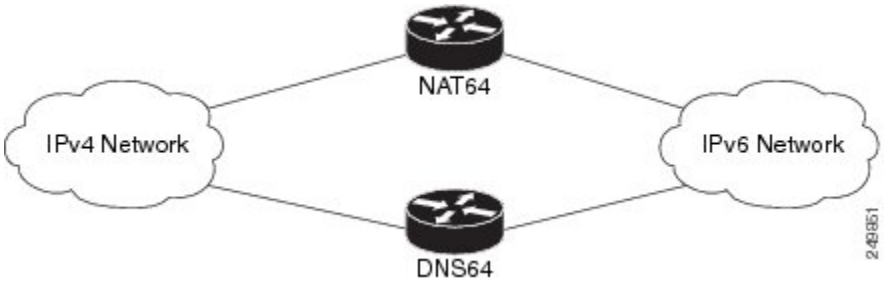


シナリオ 1 は IPv6 によって開始された接続で、シナリオ 2 は IPv4 によって開始された接続です。ステートレス NAT64 は、IPv6 アドレスが IPv4 に変換可能な場合にのみ、これら 2 つのシナリオの変換を行います。 これらの 2 つのシナリオでは、ステートレス NAT64 機能は IPv4 アドレスの枯渇に対応しません。これは、IPv4 インターネットと通信する各 IPv6 ホストが、グローバルに

ルート可能な IPv4 アドレスであるためです。 この消費は、デュアル スタックとしての IPv4 消費率に似ています。 一方、利点は、内部ネットワークが 100 % IPv6 であることです。これにより、管理（アクセス コントロール リスト、ルーティング テーブル）が容易になり、IPv4 はステートレス トランスレータが存在するエッジにのみ存在します。

以下の図は、シナリオ 5 と 6 のステートレス変換を示しています。 IPv4 ネットワークと IPv6 ネットワークは同じ組織内にあります。

図 *13*：シナリオ *5* および *6* のステートレス変換



使用される IPv4 アドレスは、パブリック IPv4 アドレスまたは RFC 1918 アドレスです。 使用される IPv6 アドレスは、パブリック IPv6 アドレスまたは固有ローカル アドレス（ULA）です。

これらのシナリオは、いずれも、IPv4 ネットワークと通信する IPv6 ネットワークで構成されます。 シナリオ 5 は IPv6 によって開始された接続で、シナリオ 6 は IPv4 によって開始された接続です。 IPv4 および IPv6 アドレスはパブリック アドレスではない場合があります。 これらのシナリオは、シナリオ 1 および 2 に似ています。 ステートレス NAT64 機能では、IPv6 アドレスが IPv4 に変換可能な場合に、これらのシナリオをサポートします。

ステートレス NAT64 変換の複数プレフィックス サポート

送信元および宛先アドレスに同じ IPv6 プレフィックスを使用するネットワーク トポロジでは、ルーティングが正しく処理されない場合があり、トラブルシューティングが困難になることがあります。 ステートレス NAT64 機能は、Cisco IOS XE Release 3.3S およびそれ以降のリリースにおけるこの問題に、ステートレス変換の複数プレフィックスをサポートすることにより対処します。 IPv4 インターネット全体が、IPv6 ネットワークで使用されるものとは異なるプレフィックスを使用して表されます。

ステートレス ネットワーク アドレス変換 64 の設定方法

ステートレス NAT64 通信用のルーティング ネットワークの設定

ステートレス NAT64 通信のルーティング ネットワークを設定および確認するには、次の作業を実行します。

はじめる前に

- ネットワーク内の任意のホストに割り当てられたIPv6アドレスには、有効なIPv4-Translatableアドレスが必要です（逆も同様）。
- この設定を有効にするには、**ipv6 unicast-routing** コマンドをイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **description** *string*
6. **ipv6 enable**
7. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}
8. **nat64 enable**
9. **exit**
10. **interface** *type number*
11. **description** *string*
12. **ip address** *ip-address mask*
13. **nat64 enable**
14. **exit**
15. **nat64 prefix stateless** *ipv6-prefix*/*length*
16. **nat64 route** *ipv4-prefix*/*mask interface-type interface-number*
17. **ipv6 route** *ipv4-prefix*/*length interface-type interface-number*
18. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 unicast-routing** 例： `Router(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 4	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**description** *string* 例： `Router(config-if)# description interface facing ipv6`	インターフェイスの設定に説明を加えます。
ステップ 6	**ipv6 enable** 例： `Router(config-if)# ipv6 enable`	インターフェイスで IPv6 処理をイネーブルにします。
ステップ 7	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} 例： `Router(config-if)# ipv6 address 2001:DB8::1/128`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 8	**nat64 enable** 例： `Router(config-if)# nat64 enable`	IPv6 インターフェイスで、ステートレス NAT64 変換をイネーブルにします。
ステップ 9	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Router(config)# interface gigabitethernet 1/2/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 11	**description** *string* 例： `Router(config-if)# description interface facing ipv4`	インターフェイスの設定に説明を加えます。
ステップ 12	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 198.51.100.1 255.255.255.0`	インターフェイスに IPv4 アドレスを設定します。
ステップ 13	**nat64 enable** 例： `Router(config-if)# nat64 enable`	IPv4 インターフェイスで、ステートレス NAT64 変換をイネーブルにします。
ステップ 14	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 15	**nat64 prefix stateless** *ipv6-prefix/length* 例： `Router(config)# nat64 prefix stateless 2001:0db8:0:1::/96`	IPv4 アドレスを IPv6 アドレスに変換するために IPv4 ホストに追加するステートレス NAT64 プレフィックスを定義します。 • このコマンドは、IPv6 ホスト用に IPv4-Translatable アドレスを作成するために使用する必要があるプレフィックスも指定します。
ステップ 16	**nat64 route** *ipv4-prefix/mask interface-type interface-number* 例： `Router(config)# nat64 route 203.0.113.0/24 gigabitethernet 0/0/0`	正しい IPv6 インターフェイスに IPv4 トラフィックをルーティングします。
ステップ 17	**ipv6 route** *ipv4-prefix/length interface-type interface-number* 例： `Router(config)# ipv6 route 2001:DB8:0:1::CB00:7100/120 gigabitethernet 0/0/0`	変換済みパケットを IPv4 アドレスにルーティングします。 • ネットワークで IPv6 ルーティング プロトコルが実行されていない場合は、**ipv6 route** コマンドを設定する必要があります。

	コマンドまたはアクション	目的
ステップ 18	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ステートレス NAT64 変換の複数プレフィックスの設定

ステートレス NAT64 変換の複数プレフィックスを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **ipv6 address** {*ipv6-address /prefix-length* | *prefix-name sub-bits/prefix-length*}
6. **ipv6 enable**
7. **nat64 enable**
8. **nat64 prefix stateless v6v4** *ipv6-prefix/length*
9. **exit**
10. **interface** *type number*
11. **ip address** *ip-address mask*
12. **negotiation auto**
13. **nat64 enable**
14. **exit**
15. **nat64 prefix stateless v4v6** *ipv6-prefix/length*
16. **nat64 route** *ipv4-prefix/mask interface-type interface-number*
17. **ipv6 route** *ipv6-prefix/length interface-type interface-number*
18. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** 例： `Router(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 4	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ipv6 address** {*ipv6-address /prefix-length* | *prefix-name sub-bits/prefix-length*} 例： `Router(config-if)# ipv6 address 2001:DB8::1/128`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 6	**ipv6 enable** 例： `Router(config-if)# ipv6 enable`	インターフェイスで IPv6 処理をイネーブルにします。
ステップ 7	**nat64 enable** 例： `Router(config-if)# nat64 enable`	IPv6 インターフェイスで、ステートレス NAT64 変換をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 8	**nat64 prefix stateless v6v4** *ipv6-prefix/length* 例： `Router(config-if)# nat64 prefix stateless v6v4 2001:0db8:0:1::/96`	ステートレス NAT64 変換のために、IPv6 アドレスを IPv4 ホストにマッピングします。 • コマンドに含まれる NAT64 プレフィックスは、IPv6-to-IPv4 方向に送信される送信元パケットのプレフィックスと同じです。
ステップ 9	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Router(config)# interface gigabitethernet 1/2/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 203.0.113.1 255.255.255.0`	インターフェイスに IPv4 アドレスを設定します。
ステップ 12	**negotiation auto** 例： `Router(config-if)# negotiation auto`	インターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーションプロトコルで設定できるようにします。
ステップ 13	**nat64 enable** 例： `Router(config-if)# nat64 enable`	IPv4 インターフェイスで、ステートレス NAT64 変換をイネーブルにします。
ステップ 14	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 15	**nat64 prefix stateless v4v6** *ipv6-prefix/length* 例： `Router(config)# nat64 prefix stateless v4v6 2001:DB8:2::1/96`	ステートレス NAT64 変換のために、IPv4 アドレスを IPv6 ホストにマッピングします。 • このコマンドは、IPv6 ホスト用に IPv4-Translatable アドレスを作成するプレフィックスを指定します。

	コマンドまたはアクション	目的
ステップ 16	**nat64 route** *ipv4-prefix/mask interface-type interface-number* 例： `Router(config)# nat64 route 203.0.113.0/24 gigabitethernet 0/0/0`	正しいIPv6インターフェイスにIPv4トラフィックをルーティングします。
ステップ 17	**ipv6 route** *ipv6-prefix/length interface-type interface-number* 例： `Router(config)# ipv6 route 2001:DB8:0:1::CB00:7100/120 gigabitethernet 0/0/0`	変換済みパケットを IPv4 アドレスにルーティングします。 • ネットワークで IPv6 ルーティング プロトコルが実行されていない場合は、**ipv6 route** コマンドを設定する必要があります。
ステップ 18	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ステートレス NAT64 ルーティング ネットワークのモニタリングおよびメンテナンス

ステートレス NAT64 ルーティング ネットワークの確認およびモニタリングを行うには、次の作業を実行します。 特権 EXEC モードでは、コマンドを任意の順序で入力できます。

手順の概要

1. **show nat64 statistics**
2. **show ipv6 route**
3. **show ip route**
4. **debug nat64** {**all** | **ha** {**all** | **info** | **trace** | **warn**} | **id-manager** | **info** | **issu** {**all** | **message** | **trace**} | **memory** | **statistics** | **trace** | **warn**}
5. **ping** [*protocol* [**tag**]] {*host-name* | *system-address*}

手順の詳細

ステップ 1　**show nat64 statistics**

このコマンドは、変換およびドロップされたパケットのグローバルおよびインターフェイス固有の統計を表示します。

例：

```
Router# show nat64 statistics

NAT64 Statistics
Global Stats:
   Packets translated (IPv4 -> IPv6): 21
   Packets translated (IPv6 -> IPv4): 15
GigabitEthernet0/0/1 (IPv4 configured, IPv6 configured):
   Packets translated (IPv4 -> IPv6): 5
   Packets translated (IPv6 -> IPv4): 0
   Packets dropped: 0
GigabitEthernet1/2/0 (IPv4 configured, IPv6 configured):
   Packets translated (IPv4 -> IPv6): 0
   Packets translated (IPv6 -> IPv4): 5
   Packets dropped: 0
```

ステップ 2 **show ipv6 route**

このコマンドは、設定されたステートレス プレフィックス、および IPv6 側を指している IPv4 埋め込み IPv6 アドレスの特定のルートを表示します。

例：

```
Router# show ipv6 route

IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
ND - Neighbor Discovery
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
LC  2001::1/128 [0/0] via FastEthernet0/3/4, receive
S   2001::1B01:10A/128 [1/0] via FastEthernet0/3/4, directly connected
S   3001::/96 [1/0] via ::42, NVI0
S   3001::1E1E:2/128 [1/0] via FastEthernet0/3/0, directly connected
LC  3001::C0A8:64D5/128 [0/0] via FastEthernet0/3/0, receive
L   FF00::/8 [0/0] via Null0, receive
```

ステップ 3 **show ip route**

このコマンドは、IPv4 側に到達した、インターネット内の IPv4 アドレスを表示します。

例：

```
Router# show ip route

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
Gateway of last resort is 10.119.254.240 to network 10.140.0.0
O E2 10.110.0.0 [160/5] via 10.119.254.6, 0:01:00, Ethernet2
E    10.67.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
O E2 10.68.132.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.130.0.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
```

```
E    10.128.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.129.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.65.129.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.10.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.75.139.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.16.208.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.84.148.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.31.223.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.44.236.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.141.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.140.0.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
IPv6 Routing Table - default - 6 entries
```

ステップ 4 **debug nat64** {**all** | **ha** {**all** | **info** | **trace** | **warn**} | **id-manager** | **info** | **issu** {**all** | **message** | **trace**} | **memory** | **statistics** | **trace** | **warn**}

このコマンドは、ステートレス NAT64 デバッグをイネーブルにします。

例：

```
Router# debug nat64 statistics

NAT64 statistics debugging is on
Sep 16 18:26:24.537 IST: NAT64 (stats): Received stats update for IDB(FastEthernet0/3/5)
Sep 16 18:26:24.537 IST: NAT64 (stats): Updating pkts_translated_v4v6 from 94368894 to 95856998
(is_delta(TRUE) value(1488104))
Sep 16 18:26:24.537 IST: NAT64 (stats): Received stats update for IDB(FastEthernet0/3/4)
Sep 16 18:26:24.537 IST: NAT64 (stats): Updating pkts_translated_v6v4 from 7771538 to 7894088
(is_delta(TRUE) value(122550))
Sep 16 18:26:24.537 IST: NAT64 (stats): Received global stats update
Sep 16 18:26:24.537 IST: NAT64 (stats): Updating pkts_translated_v4v6 from 1718650332 to 1720138437
 (is_delta(TRUE) value(1488105))
Sep 16 18:26:24.537 IST: NAT64 (stats): Updating pkts_translated_v6v4 from 1604459283 to 1604581833
 (is_delta(TRUE) value(122550))
```

ステップ 5 **ping** [*protocol* [**tag**]] {*host-name* | *system-address*}

IPv4 および IPv6 両方のインターフェイスで **nat64 enable** コマンドを設定した後に、**ping 198.168.0.2** コマンドを指定した場合の、IPv6 側からのパケット キャプチャの例を次に示します。

例：

```
Router# ping 198.168.0.2

Time             Source            Destination         Protocol       Info
1 0.000000       2001::c6a7:2      2001::c6a8:2        ICMPv6         Echo request
Frame 1: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
  Arrival Time: Oct 8, 2010 11:54:06.408354000 India Standard Time
  Epoch Time: 1286519046.408354000 seconds
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
  Frame Number: 1
  Frame Length: 118 bytes (944 bits)
  Capture Length: 118 bytes (944 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocol in frame: eth:lpv6:icmpv6: data]
Ethernet II, Src:Cisco_c3:64:94 (00:22:64:c3:64:94), Dst: Cisco_23:f2:30 (00:1f:6c:23:f2:30)
  Destination: Cisco_23:f2:30 (00:1f:6c:23:f2:30)
     Address: Cisco_23:f2:30 (00:1f:6c:23:f2:30)
     .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
     .... ...0 .... .... .... .... = LG bit: Globally unique address (factory default)
  Source: Cisco_c3:64:94 (00:22:64:c3:64:94)
    Address: Cisco_c3:64:94 (00:22:64:c3:64:94)
     .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
```

```
      .... ...0 .... .... .... .... = LG bit: Globally unique address (factory default)
  Type: IPv6 (0x86dd)
Internet Protocol Version 6, src: 2001::c6a7:2 (2001::c6a7:2), Dst: 2001::c6a8:2 (2001::c6a8:2)
   0110 .... = Version: 6
     [0110 .... = This field makes the filter "ip.version ==6" possible:: 6]
  .... 0000 0000 ... .... .... .... .... = Traffic class: 0x00000000
    .... 0000 00.. .... .... .... .... .... = Differentiated Services Field: Default (0x00000000)
    .... .... ..0. .... .... .... ... .... = ECN-Capable Transport (ECT): Not set
  .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 64
  Next header: 64
  Hop limit: 64
  Source: 2001::c6a7:2 (2001::c6a7:2)
  [Source Teredo Server IPv4: 0.0.0.0 (0.0.0.0)]
  [Source Teredo Port: 6535]
  [Source Teredo Client IPv4: 198.51.100.1 (198.51.100.1)]
  Destination: 2001:c6a8:2 (2001::c6a8:2)
  [Destination Teredo Server IPv4: 0.0.0.0 {0.0.0.0)]
  [Destination Teredo Port: 65535]
  [Destination Teredo Client IPv4: 198.51.100.2 {198.51.100.2)]
Internet Control Message Protocol v6
  Type: 128 (Echo request)
  Code: 0 (Should always be zero)
  Checksum: 0xaed2 [correct]
  ID: 0x5018
  Sequence: 0x0000
  Data (56 bytes)
    Data: 069ae4c0d3b060008090a0b0c0d0e0f1011121314151617...
    [Length: 57]
```

ステートレス ネットワーク アドレス変換 64 の設定例

ステートレス NAT64 変換のルーティング ネットワークの設定例

次の例に、ステートレス NAT64 変換のルーティング ネットワークを設定する方法を示します。

```
ipv6 unicast-routing
!
interface gigabitethernet 0/0/0
 description interface facing ipv6
 ipv6 enable
 ipv6 address 2001:DB8::1/128
 nat64 enable
!

interface gigabitethernet 1/2/0
 description interface facing ipv4
 ip address 198.51.100.1 255.255.255.0
 nat64 enable
!

nat64 prefix stateless 2001:0db8:0:1::/96
nat64 route 203.0.113.0/24 gigabitethernet 0/0/0
ipv6 route 2001:DB8:0:1::CB00:7100/120 gigabitethernet 0/0/0
```

例：ステートレス NAT64 変換の複数プレフィックスの設定

```
ipv6 unicast-routing
!
interface gigabitethernet 0/0/0
 ipv6 address 2001:DB8::1/128
 ipv6 enable
 nat64 enable
 nat64 prefix stateless v6v4 2001:0db8:0:1::/96
!
interface gigabitethernet 1/2/0
 ip address 198.51.100.1 255.255.255.0
 negotiation auto
 nat64 enable
!
nat64 prefix stateless v4v6 2001:DB8:2::1/96
ipv6 route 2001:DB8:0:1::CB00:7100/120 gigabitethernet 0/0/0
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
ハイ アベイラビリティ設定作業に対する HSRP および SNAT の使用	「Configuring NAT for High Availability」モジュール
NAT コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト、使用上の注意事項、および例	『*Cisco IOS IP Addressing Services Command Reference*』

標準

標準	タイトル
なし	--

MIB

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

RFC

RFC	タイトル
なし	--

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ステートレス ネットワーク アドレス変換 64 の機能情報

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

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

表 *12*：ステートレス ネットワーク アドレス変換 *64* の機能情報

機能名	リリース	機能情報
ステートレス ネットワーク アドレス変換 64	Cisco IOS XE Release 3.2S	ステートレス ネットワーク アドレス変換 64 機能は、IPv6 パケットの IPv4 パケットへの変換およびその逆の変換を行う変換メカニズムを提供します。変換では、拡張ヘッダーを含む IPv6 ヘッダー全体の解析、関連情報の取得、および IPv6 ヘッダーの IPv4 ヘッダーへの変換が行われます。 同様に、IPv4 ヘッダーは IPv4 オプションを含む全体が解析され、IPv6 ヘッダーが作成されます。 この処理は、ステートレス NAT64 変換用に設定されたインターフェイス上で、パケットごとに行われます。 コマンド **clear nat64 ha statistics**、**clear nat64 statistics**、**debug nat64**、**nat64 enable**、**nat64 prefix**、**nat64 route**、**show nat64 adjacency**、**show nat64 ha status**、**show nat64 prefix stateless**、**show nat64 routes**、および **show nat64 statistics** が導入または変更されました。

用語集

ALG：アプリケーション層ゲートウェイまたはアプリケーション レベル ゲートウェイ。

FP：転送プロセッサ。

IPv4-Converted アドレス：IPv4 ホストを表すために使用される IPv6 アドレス。 これらは、IPv4 アドレスへの明示的なマッピング関係を持ちます。 この関係は、IPv6 アドレスで IPv4 アドレスをマッピングすることにより、自動的に示されます。 ステートレスおよびステートフル トランスレータのいずれも、IPv4-Converted IPv6 アドレスを使用して IPv4 ホストを表します。

IPv6-Converted アドレス：ステートレス トランスレータの IPv6 ホストに割り当てられた IPv6 アドレス。 これらの IPv6-Converted アドレスは、IPv4 アドレスに対する明示的なマッピング関係を

持ちます。 この関係は、IPv6 アドレスで IPv4 アドレスをマッピングすることにより、自動的に示されます。 ステートレス トランスレータは、対応する IPv4 アドレスを使用して、IPv6 ホストを表します。 ステートフル トランスレータでは、IPv6-Converted アドレスは使用されません。これは、IPv6 ホストが、ダイナミック ステートを介して、トランスレータ内の IPv4 アドレス プールにより表されるためです。

NAT：ネットワーク アドレス変換（NAT）。

RP：ルート プロセッサ。

ステートフル変換：ステートフル変換では、フローで最初のパケットが受信されたときに、フローごとのステートが作成されます。 パケットの送信または受信によって、関連するネットワーク要素のデータ構造が作成または変更される場合、変換アルゴリズムはステートフルであるとされます。 ステートフル変換は、複数のトランスレータを同等に使用できる以外に、ある程度のレベルの拡張性もあります。 ステートフル変換は、IPv6 クライアントおよびピアが、マッピングされた IPv4 アドレスなしで IPv4 専用サーバおよびピアに接続できるように定義されています。

ステートレス変換：ステートフルではない変換アルゴリズムはステートレスと呼ばれます。 ステートレス変換ではスタティック変換テーブルを設定する必要があります。設定しない場合、変換対象のメッセージからアルゴリズムによって情報を取得できます。 ステートレス変換に必要な計算のオーバーヘッドは、ステートフル変換より少なくなります。 また、ステートを保持するために必要なメモリも少なくなります。これは、変換テーブルおよびその関連メソッドとプロセスは、ステートフルアルゴリズムに存在し、ステートレスアルゴリズムには存在しないためです。ステートレス変換では、IPv4 専用クライアントおよびピアが、IPv4 埋め込み IPv6 アドレスを備えた IPv6 専用サーバまたはピアへの接続を開始できるようにします。 IPv4 専用スタブ ネットワークまたは ISP IPv6 専用ネットワークのスケーラブルな調整も可能にします。 IPv6-to-IPv4 変換の送信元ポートは、適切にフローを識別できるように変更する必要がある場合があるため、IPv4-to-IPv6 方向の送信元ポートを変更する必要はありません。

第 11 章

ステートフル ネットワーク アドレス変換64

ステートフル ネットワーク アドレス変換 64 機能は、IPv6 パケットの IPv4 パケットへの変換およびその逆の変換を行う変換メカニズムを提供します。 ステートフル NAT64 トランスレータでは、設定済みのステートフル プレフィックスを使用して、IPv4 ホストの IPv4 アドレスから IPv6 アドレスへの変換およびその逆の変換をアルゴリズムにより行います。 同様に、IPv6 ホストの IPv6 アドレスから IPv4 アドレスへの変換およびその逆の変換がネットワーク アドレス変換（NAT）を使用して行われます。 ステートフル ネットワーク アドレス変換 64（NAT64）では、プロトコルおよび IP アドレスも変換します。 ステートフル NAT64 トランスレータは、ネイティブ IPv6 または IPv4 通信をイネーブルにし、IPv4 および IPv6 ネットワークが容易に共存できるようにします。

このマニュアルでは、ステートフル NAT64 の機能、およびステートフル NAT64 変換用のネットワークの設定方法について説明します。

- 機能情報の確認，203 ページ
- ステートフル ネットワーク アドレス変換 64 の設定の前提条件，204 ページ
- ステートフル ネットワーク アドレス変換 64 の設定の制約事項，204 ページ
- ステートフル ネットワーク アドレス変換 64 について，205 ページ
- ステートフル ネットワーク アドレス変換 64 の設定方法，213 ページ
- ステートフル ネットワーク アドレス変換 64 の設定例，224 ページ
- その他の関連資料，226 ページ
- ステートフル ネットワーク アドレス変換 64 の機能情報，227 ページ
- 用語集，229 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソ

フトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

ステートフル ネットワーク アドレス変換 64 の設定の前提条件

- ドメイン ネーム システム（DNS）トラフィックが動作するには、別個に DNS64 がインストールされ、稼働している必要があります。

ステートフル ネットワーク アドレス変換 64 の設定の制約事項

- 対応するアプリケーション レベル ゲートウェイ（ALG）を使用しないアプリケーションは、ステートフル NAT64 トランスレータで正常に動作しない場合があります。
- IP マルチキャストはサポートされていません。
- ステートフル NAT64 は、コールド冗長性のみをサポートします。 コールド冗長性とホット冗長性の、2 つの冗長性メカニズムがあります。 冗長性メカニズムにより、IPv6 ホストに対して透過的な NAT64 ボックスのスイッチオーバーが行われます。 コールド冗長性では、NAT64 ボックス間でステートのマッピングは同期されず、すでに確立されている接続が NAT64 ボックスのスイッチオーバー中に中断されます。
- IPv4 オプション、IPv6 ルーティング ヘッダー、ホップバイホップ拡張ヘッダー、宛先オプション ヘッダー、および送信元ルーティング ヘッダーの変換はサポートされません。
- 仮想ルーティングおよび転送（VRF）対応 NAT64 はサポートされません。
- ヘアピニングのループを回避するために、IPv6 から IPv4 へのトラフィック フローでは、ユーザが設定した宛先 IP アドレスとステートフル プレフィックスが一致している必要があります。 ただし、送信元 IP アドレス（IPv6 ホストの送信元アドレス）が、ステートフル プレフィックスに一致してはいけません。 送信元 IP アドレスがステートフル プレフィックスに一致する場合、パケットがドロップされます。

  ヘアピニングにより、ネットワーク アドレス変換（NAT）内の 2 つのエンドポイントが、通信のために相手の外部 IP アドレスおよびポートのみを使用している場合であっても、これらのエンドポイント間の相互通信が可能になります。

ステートフル ネットワーク アドレス変換 64 について

ステートフル ネットワーク アドレス変換 64

ステートフル NAT64 機能は、IPv6 パケットの IPv4 パケットへの変換およびその逆の変換を行う変換メカニズムを提供します。

ステートフル NAT64 では、インターネット制御メッセージ プロトコル（ICMP）、TCP、および UDP トラフィックをサポートします。 IPv6 ネットワークで生成され、IPv4 ネットワークに送信されるパケットは、ステートフル NAT64 トランスレータに対し IPv6 ネットワーク内でルーティングされます。 ステートフル NAT64 では、パケットを変換し、IPv4 ネットワークを介してそれらを IPv4 パケットとして転送します。 このプロセスは、IPv4 ネットワークに接続されているホストで生成され、IPv6 レシーバに送信されるトラフィックでは逆になります。

ステートフル NAT64 変換は対称的ではありません。これは、IPv6 アドレス空間が IPv4 アドレス空間より大きく、1 対 1 のアドレス マッピングが可能ではないためです。 ステートフル NAT64 で IPv6 から IPv4 への変換を実行するには、その前に、IPv6 アドレスおよび TCP/UDP ポートを IPv4 アドレスにバインドするステートが必要です。バインディング ステートは、IPv6 ネットワークから IPv4 ネットワークに送信される最初のパケットが変換されたときに、スタティックに設定されるか、ダイナミックに作成されます。バインディング ステートの作成後は、いずれの方向に送信されるパケットも変換されます。 ダイナミック バインディングでは、ステートフル NAT64 は、IPv6 専用ノードにより、IPv4 専用ノードに対して開始される通信をサポートします。 スタティック バインディングでは、IPv4 専用ノードにより IPv6 専用ノードに対して開始される通信およびその逆の通信をサポートします。ポートのオーバーロードが指定されたステートフル NAT64 では、IPv4 および IPv6 アドレス間に 1 対 *n* のマッピングを提供します。

ステートフル NAT 64 標準のフレームワークに関する Behavior Engineering for Hindrance Avoidance（BEHAVE）ドラフトに基づき、IPv6 ノードがステートフル NAT64 を介してトラフィックを開始し、着信パケットが既存のステートを持たない場合、次のイベントが発生します。

- 送信元 IPv6 アドレス（および送信元ポート）が、IPv4 で設定されたプール アドレス（および設定に基づくポート）に関連付けられます。
- 宛先 IPv6 アドレスは、設定された NAT64 ステートフル プレフィックスまたは Well Known Prefix（WKP）のいずれかを使用して、BEHAVE 変換ドラフトに基づき自動的に変換されます。
- パケットは、IPv6 から IPv4 に変換され、IPv4 ネットワークに転送されます。

着信パケットがステートフルである場合（着信パケットにステートが存在する場合）、NAT64 ではステートを識別し、そのステートを使用してパケットを変換します。

ステートフル NAT64 がインターフェイスに設定されている場合、Virtual Fragmentation Reassembly（VFR）が自動的に設定されます。

ステートフル ネットワーク アドレス変換 64 のプレフィックス形式

IPv6アドレスの先頭にある一連のビットは、フォーマットプレフィックスと呼ばれています。プレフィックス長は、プレフィックスを構成する、アドレスの左端の連続ビット数を指定する10進数値です。

パケットが IPv6 から IPv4 の方向に送信される場合、IPv4 ホスト アドレスは、プレフィックス長を使用する IPv6 パケットの宛先 IP アドレスから取得されます。 パケットが IPv4 から IPv6 の方向に送信される場合、IPv4ホストアドレスは、ステートフルプレフィックスを使用して作成されます。

IETF アドレス形式 BEHAVE ドラフトに従い、IPv6 アーキテクチャに定義された u-bit（ビット 70）をゼロに設定する必要があります。 u-bit の使用方法については、RFC 2464 を参照してください。 予約済みのオクテット（u-octet とも呼びます）は、IPv6アドレッシングアーキテクチャで定義されているホスト ID 形式との互換性のために予約されています。 IPv6 パケットを作成する場合、トランスレータでは、u-bit が改ざんされておらず、RFC 2373 に示されている値に設定されていることを確認する必要があります。 サフィックスは、トランスレータによりすべてゼロに設定されます。 IETF では、u-octet の 8 ビット（ビット範囲 64 ～ 71）をゼロに設定することを推奨しています。

Well Known Prefix

Well Known Prefix 64:FF9B::/96 がステートフル NAT64 でサポートされています。 ステートフル変換時に、ステートフル プレフィックスが（インターフェイスでまたはグローバルに）設定されていない場合、WKP プレフィックスを使用して IPv4 ホスト アドレスが変換されます。

ステートフル IPv4-to-IPv6 パケット フロー

ステートフル NAT64 の IPv4 開始パケットのパケット フローは次のとおりです。

- 宛先アドレスは、NAT 仮想インターフェイス（NVI）にルート指定されます。

  仮想インターフェイスは、ステートフル NAT64 が設定されたときに作成されます。 ステートフル NAT64 変換が機能するためには、すべてのパケットが NVI にルーティングされる必要があります。 アドレス プールを設定すると、ルートがプール内のすべての IPv4 アドレスに自動的に追加されます。 このルートは自動的に NVI を指します。

- IPv4 開始パケットは、スタティックまたはダイナミック バインディングにヒットします。

  ダイナミック アドレス バインディングは、ユーザがダイナミック ステートフル NAT64 を設定したときに、ステートフル NAT64 トランスレータによって作成されます。 バインディングは IPv6 および IPv4 アドレス プール間にダイナミックに作成されます。 ダイナミック バインディングは IPv6-to-IPv4 トラフィックによってトリガーされ、アドレスがダイナミックに割り当てられます。 設定に基づいて、スタティックまたはダイナミック バインディングを使用できます。

- IPv4 開始パケットはプロトコルにより変換され、パケットの宛先 IP アドレスはスタティックまたはダイナミック バインディングに基づいて IPv6 に設定されます。 ステートフル NAT64 トランスレータでは、ステートフル NAT64 プレフィックス（ステートフル プレフィックスが設定されている場合）または Well Known Prefix（WKP）（ステートフル プレフィックスが設定されていない場合）を使用して、送信元 IP アドレスを IPv6 に変換します。
- セッションは変換情報に基づいて作成されます。

後続の IPv4 開始パケットはすべて、以前に作成されたセッションに基づいて変換されます。

ステートフル IPv6-to-IPv4 パケット フロー

ステートフル IPv6 開始パケット フローは次のようになります。

- 最初の IPv6 パケットは、ステートフル プレフィックスに設定される自動ルーティング設定に基づいて、NAT 仮想インターフェイス（NVI）にルーティングされます。 ステートフル NAT64 では一連の参照を実行して、IPv6 パケットが設定されたマッピングのいずれかに一致するかどうかを、アクセス コントロール リスト（ACL）参照に基づいて判別します。 マッピングに基づいて、IPv4 アドレス（およびポート）が IPv6 宛先アドレスに関連付けられます。 IPv6 パケットが変換され、次の方法により IPv4 が作成されます。
  - 宛先 IPv4 アドレスを IPv6 アドレスからプレフィックスを削除することによって取得します。 送信元アドレスが、割り当てられた IPv4 アドレス（およびポート）で置き換えられます。
  - 残りのフィールドが IPv6 から IPv4 に変換され、有効な IPv4 パケットが作成されます。

（注） このプロトコル変換は、ステートレス NAT64 でも同一で、BEHAVE RFC ドラフトに記載されています。

- 新しい NAT64 変換がセッション データベースおよびバインド データベースに作成されます。 プールおよびポート データベースは、設定に応じて更新されます。 IPv6 パケット フローのリターン トラフィックと後続のトラフィックでは、このセッション データベース エントリを変換に使用します。

IP パケット フィルタリング

ステートフル ネットワーク アドレス変換 64（NAT64）では、IPv6 と IPv4 パケットをフィルタリングします。 ステートフルに変換された IPv6 パケットがトランスレータのリソースを消費するため、ステートフル トランスレータに送信されるすべての IPv6 パケットがフィルタリングされます。 これらのパケットは、スタティック設定ではパケット処理のプロセッサ リソース、メモリ リソース（常にセッション メモリ）を、ダイナミック設定では IPv4 アドレス リソースを、ポート アドレス変換（PAT）では IPv4 アドレスおよびポート リソースを消費します。

ステートフル NAT64 では、設定されたアクセス コントロール リスト（ACL）およびプレフィックス リストを利用して、NAT64 ステートの作成を許可されている IPv6 開始トラフィック フローをフィルタリングします。 IPv6 パケットのフィルタリングは IPv6-to-IPv4 の方向で行われます。これは、IPv6 ホストおよび IPv4 アドレス間のマッピングのダイナミックな割り当てを行えるのがこの方向のみであるためです。

ステートフル NAT64 は、PAT 設定を持つ IPv4-to-IPv6 パケット フローに対するエンドポイント依存フィルタリングをサポートします。 ステートフル NAT64 PAT 設定では、パケット フローは、IPv6 レルムから発信され、NAT64 ステート テーブルにステート情報を作成している必要があります。 以前に作成されたステートを持たない IPv4 側からのパケットはドロップされます。 エンドポイントに依存しないフィルタリングは、スタティック ネットワーク アドレス変換（NAT）および非 PAT 設定でサポートされます。

ステートフル NAT64 とステートレス NAT64 の違い

次の表に、ステートフル NAT64 とステートレス NAT64 の違いを示します。

表 *13*：ステートフル *NAT64* とステートレス *NAT64* の違い

サポートされる機能	ステートフル NAT64	ステートレス NAT64
アドレスの節約	IPv4 アドレスを節約する PAT またはオーバーロード設定の *N* 対 1 マッピング。	1 対 1 マッピング（1 つの IPv4 アドレスが各 IPv6 ホストに使用されます）。
アドレス レンジ	IPv6 システムは、任意のタイプの IPv6 アドレスを使用できます。	IPv6 システムには IPv4-Translatable アドレスが必要です（RFC 6052 に基づきます）。
サポートされる ALG	FTP64	なし
サポートされるプロトコル	ICMP、TCP、UDP	すべて
標準	Draft-ieft-behave-v6v4-xlate-stateful-12	Draft-ietf-behave-v6v4-xlate-05
ステートの構築	各トラフィック フローで、NAT64 トランスレータにステートが作成されます。 ステートの最大数は、サポートされる変換の数に応じて決まります。	トラフィック フローで、NAT64 トランスレータにステートは作成されません。 アルゴリズム処理は、パケット ヘッダーに対して実行されます。

NAT64 の High-Speed ロギング

リリースによっては、ステートフルNAT64でHigh-Speedロギング（HSL）がサポートされます。HSLが設定されると、NAT64により、ルーティングデバイスを経由して外部コレクタに送信されるパケットのログが提供されます（バージョン9NetFlow形式のレコードに類似）。レコードは、各バインディング（バインディングは、ローカルアドレスとそのローカルアドレスの変換先となるグローバルアドレス間のアドレスバインディング）について、セッションが作成および破棄されるときに送信されます。セッション レコードには、5 タプルの情報すべて（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコル）が含まれます。タプルは、要素の順序付きリストです。また、NAT64は、NAT64プールのアドレスがなくなると（プール枯渇とも呼びます）、HSLメッセージを送信します。プール枯渇メッセージはレート制限を受けるため、プール枯渇状態になったすべてのパケットがHSLメッセージをトリガーすることはありません。

NAT64 HSL ロギングをイネーブルにするには、**nat64 logging translations flow-export v9 udp destination** コマンドを設定します。

次の表に、HSLバインドおよびセッションの作成または破棄のテンプレートを示します。これらのフィールド（ログに表示される順序で示しています）は、ログコレクタによるHSLレコードのバイトの解釈方法について説明しています。一部のフィールドでは、セッションが作成、破棄、または変更されているかどうかによって値が異なります。

表 *14*： *HSL* バインドおよびセッションの作成または破棄のテンプレート

フィールド	フォーマット	ID	値
元の IPv6 アドレス	IPv6 アドレス	27	不定
変換されたIPv4アドレス	IPv6 アドレス	282	不定
変換されたIPv6アドレス	IPv4 アドレス	225	不定
元の IPv4 アドレス	IPv4 アドレス	12	不定
元の IPv6 ポート	16 ビット ポート	7	不定
変換されたIPv6ポート	16 ビット ポート	227	不定
変換されたIPv4ポート	16 ビット ポート	11	不定
元の IPv4 ポート	16 ビット ポート	228	不定

フィールド	フォーマット	ID	値
イベントのタイムスタンプ	64 ビット、ミリ秒（これは、レコードのイベントが発生したときに、ミリ秒単位の UNIX 時間を保持する 64 ビット フィールドです）	323	不定
VRF ID	32 ビット ID	234	0
プロトコル	8 ビット値	4	不定
イベント	8 ビット値	230	0：無効 1：イベントの追加 2：イベントの削除

次の表で、HSL プール枯渇テンプレートについて説明します（テンプレートで使用可能な順序で示しています）。

表 *15*：*HSL* プール枯渇のテンプレート

フィールド	フォーマット	ID	値
NAT プール ID	32 ビット値	283	不定
NAT イベント	8 ビット値	230	3：プール枯渇

FTP64 アプリケーション レベル ゲートウェイ サポート

FTP64（またはサービス FTP）アプリケーション レベル ゲートウェイ（ALG）は、ステートフル ネットワーク アドレス変換 64（NAT64）がレイヤ 7 データを処理できるようにします。 FTP64 ALG は、FTP 制御セッションのペイロードに埋め込まれている IP アドレスおよび TCP ポート情報を変換します。

NAT は、アプリケーション データ ストリームで送信元および宛先 IP アドレスを伝送しない TCP/UDP トラフィックを変換します。 ペイロード内（またはアプリケーション データ ストリーム内）に IP アドレス情報を埋め込むプロトコルには、ALG サポートが必要です。 ALG は、パケットペイロード内の埋め込みIPアドレスおよびポート番号の変換や、制御チャネルからの新規接続またはセッション情報の取得といった、アプリケーション データ ストリーム（レイヤ 7）プロトコル固有のサービスを処理します。

FTP64 は、ステートフル NAT64 がイネーブルにされたときに自動的にイネーブルになります。NAT64 FTP サービスをディセーブルにするには、**no nat64 service ftp** コマンドを使用します。

（注） FTP64 ALG は、ステートレス NAT64 変換ではサポートされません。

（注） FTP64 ALG は、IPv4 互換 IPv6 アドレスをサポートしません。

「*IPv6-to-IPv4 translation FTP considerations draft-ietf-behave-ftp64-02*」および RFC 2228 に基づき、FTP64 ALG は、コマンドおよび応答が FTP クライアントと FTP サーバの間で送受信されるときに、トランスペアレントモードに切り替える必要があります（トランスペアレントモードのデバイスはネットワークに表示されませんが、このデバイスはブリッジとして動作して、パケットの検査またはフィルタリングを行えます）。 クライアントが FTP AUTH コマンドを発行すると、FTP64 ALG は、制御チャネルセッションが終了するまで、制御チャネル上のすべてのデータを両方（イングレスとイーグレス）の方向に転送します。 同様に、AUTH ネゴシエーション中は、ネゴシエーションが成功したかどうかに関係なく、ALG はトランスペアレント モードである必要があります。

RFC 6384 に基づき、クライアント/サーバ通信中の FTP64 ALG の動作は異なります。 IPv6-to-IPv4 変換時、FTP64 ALG は、制御チャネルを介して送信されたデータを透過的にコピーして、トランスポート層セキュリティ（TLS）セッションが正しく動作するようにする必要があります。 ただし、クライアント コマンドおよびサーバ応答は FTP64 ALG から隠されています。 動作の一貫性を確保するには、クライアントによる最初の FTP AUTH コマンドの発行直後に、FTP64 ALG がコマンドおよび応答の変換を停止して、サーバからクライアントまたはその逆に送信される TCP データの透過的コピーを開始する必要があります。 サーバ応答が、FTP エラー/警告メッセージを表す 4*xx* または 5*xx* レンジ内にある場合、FTP64 ALG は AUTH コマンドを無視し、トランスペアレント モードに移行しないでいる必要があります。

CSCtu37975 よりも前では、IPv4 FTP サーバが許可ネゴシエーションを受け入れたか拒否したかに関係なく、IPv6 FTP クライアントが FTP AUTH コマンドを発行すると、FTP64 ALG によって AUTH セッションがトランスペアレント モード（またはバイパス モード）に移行されます。 セッションがトランスペアレント モードの場合、NAT はセッション内のパケットに対する変換を実行できません。 CSCtu37975 では、クライアント/サーバ通信中の FTP64 ALG の動作は RFC 6384 に準拠します。

FTP64 NAT ALG ボックス内ハイ アベイラビリティ サポート

リリースによっては、FTP64 アプリケーション レベル ゲートウェイ（ALG）により、ステートフル NAT64 のハイ アベイラビリティ（HA）サポートが追加されます。 FTP64 NAT ALG ボックス内 HA サポート機能では、単一シャーシ内の冗長転送プロセッサ（FP）間のステートフル スイッチオーバーをサポートしています。 FTP64 ALG によって提供される HA サポートは、ボックス内 HA およびインサービス ソフトウェア アップグレード（ISSU）の両方に適用可能です。

NAT64 ALG サービスをディセーブルにするには、**no nat64 service ftp** コマンドを使用します。

FTP64 ALG では、次のメッセージを受信するとデータを同期します。

- 230 個の応答後のユーザ認証フラグ。
- ALG ENABLE および ALG DISABLE メッセージの受信後の ALG ディセーブル/イネーブル フラグ。
- 最初の分割パケットの検出後のフラグメント検出情報。
- セグメンテーション終了の検出後の、フラグメント検出情報。

（注）
- 一部のリリースでは、ステートフル NAT64 はボックス内 HA のみをサポートします。
- FTP64 ALG の統計情報および FTP64 デバッグ ログが、FTP64 ALG によりスタンバイ デバイスに同期されることはありません。

ステートフル NAT64 - シャーシ内冗長化

リリースによっては、ステートフル NAT64 - シャーシ内冗長化機能のサポートを使用できます。単一のシャーシ内に使用できる 2 つ目の転送プロセッサ（FP）がある場合、ステートフル NAT64 - シャーシ内冗長化機能によって 2 つ目の FP をスタンバイ エンティティとして設定できます。 2 つ目の FP を接続すると、明示的な設定なしに冗長性が自動的に開始します。 スタンバイ FP が「ホット スタンバイ」になる（すべてのセッションが同期された状態になる）までには、短い遅延があります。 スタンバイ FP はステートフル NAT64 セッション情報のバックアップを保持し、アクティブな（1 つ目の）FP に障害が発生しても、NAT64 セッションはほとんど中断されません。

NAT64 冗長性情報は、次の場合にスタンバイ FP に送信されます。

- セッションまたはダイナミック バインドが作成された場合。
- セッションまたはダイナミック バインドが削除された場合。
- 定期更新中。 アクティブ FP は、経過時間に基づいてステート情報をスタンバイに対して更新します。 複製されたオブジェクトのすべての変更が、変更時にただちにスタンバイに送信されるわけではありません。 最も重要な更新はただちに送信され、その他の変更は定期更新によって通知されます。

スタンバイ FP が挿入されるかスタンバイ FP がリロードから回復すると、アクティブな FP はバルク同期を実行して、スタンバイ FP をアクティブ FP と同期します。 NAT はアグレッシブ同期を行って、アクティブ FP がすべてのステート情報をスタンバイ FP にプッシュするよう強制します。

NAT64 セッション情報に加えて、アプリケーション固有の情報（アプリケーション レベル ゲートウェイ（ALG）情報）も、スタンバイ FP に通知する必要があります。 各 ALG は、スタンバイで同期する必要のあるセッションごとのステートを持ちます。 ALG は、スタンバイ FP へのすべ

ての ALG ステート情報の送信をトリガーします。 NAT では、実際に ALG ステートを送信するメカニズムを提供し、特定のセッションにステートを関連付けます。

HTTP セッションは、スタンバイ FP にバックアップされません。 スイッチオーバー時にスタンバイ FP で HTTP セッションを複製するには、**nat64 switchover replicate http enable** コマンドを設定する必要があります。

（注） ステートフル NAT64 - シャーシ内冗長化機能では、ボックスツーボックス（B2B）冗長性および非対称ルーティングをサポートしていません。

ステートフル ネットワーク アドレス変換 64 の設定方法

ネットワーク設定に基づいて、スタティック、ダイナミック、またはダイナミック ポート アドレス変換（PAT）ステートフル NAT64 を設定できます。

（注） ステートフル NAT64 が機能するためには、次の作業で説明する設定のいずれか 1 つ以上を設定する必要があります。

スタティック ステートフル ネットワーク アドレス変換 64 の設定

スタティック IPv6 アドレスから IPv4 アドレスおよびその逆を設定できます。 任意で、ポートありまたはなしでスタティック ステートフル NAT64 を設定できます。 スタティック ステートフル NAT64 を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **description** *string*
6. **ipv6 enable**
7. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}
8. **nat64 enable**
9. **exit**
10. **interface** *type number*
11. **description** *string*
12. **ip address** *ip-address mask*
13. **nat64 enable**
14. **exit**
15. **nat64 prefix stateful** *ipv6-prefix*/*length*
16. **nat64 v6v4 static** *ipv6-address ipv4-address*
17. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 4	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**description** *string* 例： `Device(config-if)# description interface facing ipv6`	インターフェイスの設定に説明を加えます。
ステップ 6	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	インターフェイスで IPv6 処理をイネーブルにします。
ステップ 7	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} 例： `Device(config-if)# ipv6 address 2001:DB8:1::1/96`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 8	**nat64 enable** 例： `Device(config-if)# nat64 enable`	IPv6 インターフェイスで、NAT64 変換をイネーブルにします。
ステップ 9	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/2/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**description** *string* 例： `Device(config-if)# description interface facing ipv4`	インターフェイスの設定に説明を加えます。
ステップ 12	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 209.165.201.1 255.255.255.0`	インターフェイスに IPv4 アドレスを設定します。
ステップ 13	**nat64 enable** 例： `Device(config-if)# nat64 enable`	IPv4 インターフェイスで、NAT64 変換をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 14	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 15	**nat64 prefix stateful** *ipv6-prefix/length* 例： `Device(config)# nat64 prefix stateful 2001:DB8:1::1/96`	IPv4 アドレスを IPv6 アドレスに変換するために IPv4 ホストに追加するステートフル NAT64 プレフィックスを定義します。 • ステートフル NAT64 プレフィックスは、グローバル コンフィギュレーション レベルまたはインターフェイス レベルで設定できます。
ステップ 16	**nat64 v6v4 static** *ipv6-address ipv4-address* 例： `Device(config)# nat64 v6v4 static 2001:DB8:1::FFFE 209.165.201.1`	NAT64 IPv6-to-IPv4 スタティック アドレス マッピングをイネーブルにします。
ステップ 17	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ダイナミック ステートフル ネットワーク アドレス変換 64 の設定

ダイナミック ステートフル NAT64 設定は、アドレス プール内の IPv4 アドレスに対する IPv6 アドレスの 1 対 1 のマッピングを提供します。 アクティブな IPv6 ホストの数がプール内の IPv4 アドレスの数より少ない場合に、ダイナミック ステートフル NAT64 設定を使用できます。 ダイナミック ステートフル NAT64 を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **description** *string*
6. **ipv6 enable**
7. **ipv6** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}
8. **nat64 enable**
9. **exit**
10. **interface** *type number*
11. **description** *string*
12. **ip address** *ip-address mask*
13. **nat64 enable**
14. **exit**
15. **ipv6 access-list** *access-list-name*
16. **permit ipv6** *ipv6-address* **any**
17. **exit**
18. **nat64 prefix stateful** *ipv6-prefix*/*length*
19. **nat64 v4 pool** *pool-name start-ip-address end-ip-address*
20. **nat64 v6v4 list** *access-list-name* **pool** *pool-name*
21. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**description** *string* 例： `Device(config-if)# description interface facing ipv6`	インターフェイスの設定に説明を加えます。
ステップ 6	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	インターフェイスで IPv6 処理をイネーブルにします。
ステップ 7	**ipv6** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} 例： `Device(config-if)# ipv6 2001:DB8:1::1/96`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 8	**nat64 enable** 例： `Device(config-if)# nat64 enable`	IPv6 インターフェイスで、ステートフル NAT64 変換をイネーブルにします。
ステップ 9	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/2/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します
ステップ 11	**description** *string* 例： `Device(config-if)# description interface facing ipv4`	インターフェイスの設定に説明を加えます。
ステップ 12	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 209.165.201.24 255.255.255.0`	インターフェイスに IPv4 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 13	**nat64 enable** 例： `Device(config-if)# nat64 enable`	IPv4 インターフェイスで、ステートフル NAT64 変換をイネーブルにします。
ステップ 14	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 15	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list nat64-acl`	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 16	**permit ipv6** *ipv6-address* **any** 例： `Device(config-ipv6-acl)# permit ipv6 2001:DB8:2::/96 any`	IPv6 アクセス リストに許可条件を設定します。
ステップ 17	**exit** 例： `Device(config-ipv6-acl# exit`	IPv6 アクセス リスト コンフィギュレーション モードを終了し、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 18	**nat64 prefix stateful** *ipv6-prefix/length* 例： `Device(config)# nat64 prefix stateful 2001:DB8:1::1/96`	NAT64 IPv6-to-IPv4 アドレス マッピングをイネーブルにします。
ステップ 19	**nat64 v4 pool** *pool-name start-ip-address end-ip-address* 例： `Device(config)# nat64 v4 pool pool1 209.165.201.1 209.165.201.254`	ステートフル NAT64 IPv4 アドレス プールを定義します。
ステップ 20	**nat64 v6v4 list** *access-list-name* **pool** *pool-name* 例： `Device(config)# nat64 v6v4 list nat64-acl pool pool1`	NAT64 で、IPv6 送信元アドレスを IPv4 送信元アドレスに、IPv6 宛先アドレスを IPv4 宛先アドレスに、ダイナミックに変換します。

	コマンドまたはアクション	目的
ステップ 21	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ダイナミック ポート アドレス変換ステートフル NAT64 の設定

複数の IPv6 ホストを使用可能な IPv4 アドレスのプールに先着順で多重化（複数の IPv6 アドレスを単一の IPv4 プール アドレスにマッピング）するために、ポート アドレス変換（PAT）またはオーバーロード設定が使用されます。 ダイナミック PAT 設定は、IPv4 インターネットへの接続を可能にしながら、IPv4 アドレス空間を節約します。 PAT アドレス変換を設定するには、**nat64 v6v4 list** コマンドに **overload** キーワードを指定して設定します。 ダイナミック PAT ステートフル NAT64 を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **description** *string*
6. **ipv6 enable**
7. **ipv6** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}
8. **nat64 enable**
9. **exit**
10. **interface** *type number*
11. **description** *string*
12. **ip address** *ip-address mask*
13. **nat64 enable**
14. **exit**
15. **ipv6 access-list** *access-list-name*
16. **permit ipv6** *ipv6-address* **any**
17. **exit**
18. **nat64 prefix stateful** *ipv6-prefix*/*length*
19. **nat64 v4 pool** *pool-name start-ip-address end-ip-address*
20. **nat64 v6v4 list** *access-list-name* **pool** *pool-name* **overload**
21. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 4	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**description** *string* 例： `Device(config-if)# description interface facing ipv6`	インターフェイスの設定に説明を加えます。
ステップ 6	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	インターフェイスでIPv6処理をイネーブルにします。
ステップ 7	**ipv6** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} 例： `Device(config-if)# ipv6 2001:DB8:1::1/96`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 8	**nat64 enable** 例： `Device(config-if)# nat64 enable`	IPv6 インターフェイスで、ステートフル NAT64 変換をイネーブルにします。
ステップ 9	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/2/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します
ステップ 11	**description** *string* 例： `Device(config-if)# description interface facing ipv4`	インターフェイスの設定に説明を加えます。
ステップ 12	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 209.165.201.24 255.255.255.0`	インターフェイスに IPv4 アドレスを設定します。
ステップ 13	**nat64 enable** 例： `Device(config-if)# nat64 enable`	IPv6 インターフェイスで、ステートフル NAT64 変換をイネーブルにします。
ステップ 14	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 15	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list nat64-acl`	IPv6 アクセス リストを定義し、デバイスを IPv6 アクセス リスト コンフィギュレーション モードにします。
ステップ 16	**permit ipv6** *ipv6-address* **any** 例： `Device(config-ipv6-acl)# permit ipv6 2001:db8:2::/96 any`	IPv6 アクセス リストに許可条件を設定します。
ステップ 17	**exit** 例： `Device(config-ipv6-acl)# exit`	IPv6 アクセス リスト コンフィギュレーション モードを終了し、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 18	**nat64 prefix stateful** *ipv6-prefix/length* 例： `Device(config)# nat64 prefix stateful 2001:db8:1::1/96`	NAT64 IPv6-to-IPv4 アドレス マッピングをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 19	**nat64 v4 pool** *pool-name start-ip-address end-ip-address* 例： `Device(config)# nat64 v4 pool pool1 209.165.201.1 209.165.201.254`	ステートフル NAT64 IPv4 アドレス プールを定義します。
ステップ 20	**nat64 v6v4 list** *access-list-name* **pool** *pool-name* **overload** 例： `Device(config)# nat64 v6v4 list nat64-acl pool pool1 overload`	NAT64 PAT（オーバーロード アドレス変換）をイネーブルにします。
ステップ 21	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ステートフル NAT64 ルーティング ネットワークのモニタリングおよびメンテナンス

次のコマンドを任意の順序で使用して、ステートフル ネットワーク アドレス変換 64（NAT64）設定のステータスを表示します。

手順の概要

1. **show nat64 aliases** [*lower-address-range upper-address-range*]
2. **show nat64 logging**
3. **show nat64 prefix stateful** {**global** | {**interfaces** | **static-routes**} [**prefix** *ipv6-address*/*prefix-length*]}
4. **show nat64 timeouts**

手順の詳細

ステップ 1 **show nat64 aliases** [*lower-address-range upper-address-range*]
このコマンドは、NAT64 によって作成された IP エイリアスを表示します。

例：
```
Device# show nat64 aliases

Aliases configured: 1
```

```
Address   Table ID  Inserted   Flags   Send ARP   Reconcilable   Stale   Ref-Count
10.1.1.1  0         FALSE      0x0030  FALSE      TRUE           FALSE   1
```

ステップ 2 **show nat64 logging**
このコマンドは、NAT64 ロギングを表示します。

例：
```
Device# show nat64 logging

NAT64 Logging Type

Method       Protocol   Dst. Address   Dst. Port   Src. Port
translation
flow export  UDP        10.1.1.1       5000        60087
```

ステップ 3 **show nat64 prefix stateful** {**global** | {**interfaces** | **static-routes**} [**prefix** *ipv6-address*/*prefix-length*]}
このコマンドは、NAT64 ステートフル プレフィックスに関する情報を表示します。

例：
```
Device# show nat64 prefix stateful interfaces

Stateful Prefixes

Interface               NAT64   Enabled   Global Prefix
GigabitEthernet0/1/0    TRUE    TRUE      2001:DB8:1:1/96
GigabitEthernet0/1/3    TRUE    FALSE     2001:DB8:2:2/96
```

ステップ 4 **show nat64 timeouts**
このコマンドは、NAT64 変換セッション タイムアウトの統計情報を表示します。

例：
```
Device# show nat64 timeouts

NAT64 Timeout

Seconds    CLI Cfg    Uses 'All'    all flows
86400      FALSE      FALSE         udp
300        FALSE      TRUE          tcp
7200       FALSE      TRUE          tcp-transient
240        FALSE      FALSE         icmp
60         FALSE      TRUE
```

ステートフル ネットワーク アドレス変換 64 の設定例

例：スタティック ステートフル ネットワーク アドレス変換 64 の設定

```
Device# configure terminal
Device(config)# ipv6 unicast-routing
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# description interface facing ipv6
Device(config-if)# ipv6 enable
Device(config-if)# ipv6 address 2001:DB8:1::1/96
```

```
Device(confif-if)# nat64 enable
Device(config-fi)# exit
Device(config)# interface gigabitethernet 1/2/0
Device(config-if)# description interface facing ipv4
Device(config-if)# ip address 209.165.201.1 255.255.255.0
Device(config-if)# nat64 enable
Device(config-if)# exit
Device(config)# nat64 prefix stateful 2001:DB8:1::1/96
Device(config)# nat64 v6v4 static 2001:DB8:1::FFFE 209.165.201.1
Device(config)# end
```

例：ダイナミック ステートフル ネットワーク アドレス変換 64 の設定

```
Device# configure terminal
Device(config)# ipv6 unicast-routing
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# description interface facing ipv6
Device(config-if)# ipv6 enable
Device(config-if)# ipv6 2001:DB8:1::1/96
Device(config-if)# nat64 enable
Device(config-if)# exit
Device(config)# interface gigabitethernet 1/2/0
Device(config-if)# description interface facing ipv4
Device(config-if)# ip address 209.165.201.24 255.255.255.0
Device(config-if)# nat64 enable
Device(config-if)# exit
Device(config)# ipv6 access-list nat64-acl
Device(config-ipv6-acl)# permit ipv6 2001:db8:2::/96 any
Device(config-ipv6-acl)# exit
Device(config)# nat64 prefix stateful 2001:db8:1::1/96
Device(config)# nat64 v4 pool pool1 209.165.201.1 209.165.201.254
Device(config)# nat64 v6v4 list nat64-acl pool pool1
Device(config)# end
```

例：ダイナミック ポート アドレス変換ステートフル NAT64 の設定

```
enable
 configure terminal
  ipv6 unicast-routing
  interface gigabitethernet 0/0/0
   description interface facing ipv6
   ipv6 enable
   ipv6 2001:DB8:1::1/96
   nat64 enable
   exit
  interface gigabitethernet 1/2/0
   description interface facing ipv4
   ip address 209.165.201.24 255.255.255.0
   nat64 enable
   exit
  ipv6 access-list nat64-acl
   permit ipv6 2001:db8:2::/96 any
   exit
  nat64 prefix stateful 2001:db8:1::1/96
  nat64 v4 pool pool1 209.165.201.1 209.165.201.254
  nat64 v6v4 list nat64-acl pool pool1 overload
  end
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
NAT コマンド	『IP Addressing Services Command Reference』

標準および RFC

標準/RFC	タイトル
IPv4/IPv6 変換のフレームワーク	『Framework for IPv4/IPv6 Translation draft-ietf-behave-v6v4-framework-06』
IPv6-to-IPv4 変換の FTP ALG	『An FTP ALG for IPv6-to-IPv4 translation draft-ietf-behave-ftp64-06』
IP/ICMP 変換アルゴリズム	『IP/ICMP Translation Algorithm draft-ietf-behave-v6v4-xlate-10』
IPv4/IPv6 トランスレータの IPv6 アドレッシング	『IPv6 Addressing of IPv4/IPv6 Translators draft-ietf-behave-address-format-07』
RFC 2228	『FTP Security Extensions』
RFC 2373	『IP Version 6 Addressing Architecture』
RFC 2464	『Transmission of IPv6 Packets over Ethernet Networks』
RFC 2765	『Stateless IP/ICMP Translation Algorithm (SIIT)』
RFC 2766	Network Address Translation - Protocol Translation（NAT-PT）
RFC 4787	『Network Address Translation (NAT) Behavioral Requirements for Unicast UDP』
RFC 4966	『Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status』
RFC 6384	『An FTP Application Layer Gateway (ALG) for IPv6-to-IPv4 Translation』

標準/RFC	タイトル
ステートフルNAT64：IPv6クライアントからIPv4サーバへのネットワーク アドレスおよびプロトコル変換	『Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers draft-ietf-behave-v6v4-xlate-stateful-12』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーションWebサイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ステートフル ネットワーク アドレス変換 64 の機能情報

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

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

表 *16*：ステートフル ネットワーク アドレス変換 *64* の機能情報

機能名	リリース	機能情報
FTP64 NAT ALG ボックス内 HA サポート	Cisco IOS XE Release 3.5S	Cisco IOS XE Release 3.5S では、FTP64 ALG により、ステートフル NAT64 の HA サポートが追加されます。 FTP64 NAT ALG ボックス内 HA サポート機能では、単一シャーシ内の冗長 FP 間のステートフル スイッチオーバーをサポートしています。 FTP64 ALG によって提供される HA サポートは、ボックス内およびボックス間 HA およびインサービス ソフトウェア アップグレード（ISSU）の両方に適用可能です。
ステートフル NAT64 ALG - ステートフル FTP64 ALG サポート	Cisco IOS XE Release 3.4S	Cisco IOS XE Release 3.4S 以降のリリースでは、FTP64（またはサービス FTP）ALG をサポートしています。 FTP64 ALG は、ステートフル NAT64 でレイヤ 7 データを処理できるようにします。 FTP ALG は、FTP 制御セッションのペイロードに埋め込まれている IP アドレスおよび TCP ポート情報を変換します。 **nat64 service ftp** コマンドが導入または変換されました。
ステートフル NAT64 - シャーシ内冗長化	Cisco IOS XE Release 3.5S	Cisco IOS XE Release 3.5S 以降のリリースでは、ステートフル NAT64 - シャーシ内冗長化機能がサポートされます。 単一のシャーシ内に使用できる 2 つ目の転送プロセッサ（FP）がある場合、ステートフル NAT64 - シャーシ内冗長化機能によって 2 つ目の FP をスタンバイ エンティティとして設定できます。 スタンバイ FP はステートフル NAT64 セッション情報のバックアップを保持し、アクティブな（1 つ目の）FP に障害が発生しても、NAT64 セッションが中断されません。 **nat64 switchover replicate http port** コマンドが導入または変更されました。

機能名	リリース	機能情報
ステートフル ネットワーク アドレス変換 64	Cisco IOS XE Release 3.4S	ステートフル ネットワーク アドレス変換 64 機能は、IPv6 パケットの IPv4 パケットへの変換およびその逆の変換を行う変換メカニズムを提供します。 ステートフル NAT64 トランスレータでは、設定済みのステートフル プレフィックスを使用して、IPv4 ホストの IPv4 アドレスから IPv6 アドレスへの変換およびその逆の変換をアルゴリズムにより行います。 同様に、IPv6 ホストの IPv6 アドレスから IPv4 アドレスへの変換およびその逆の変換が NAT を使用して行われます。 コマンド **clear nat64 statistics**、**debug nat64**、**nat64 logging**、**nat64 prefix stateful**、**nat64 translation**, **nat64 v4**、**nat64 v4v6**、**nat64 v6v4**、**show nat64 aliases**、**show nat64 limits**、**show nat64 logging**、**show nat64 mappings dynamic**、**show nat64 mappings static**、**show nat64 services**、**show nat64 pools**、**show nat64 prefix stateful**、**show nat64 statistics**、**show nat64 timeouts**、および **show nat64 translations** が導入または変更されています。

用語集

ALG：アプリケーション層ゲートウェイまたはアプリケーション レベル ゲートウェイ。

FP：転送プロセッサ。

IPv4-Converted アドレス：IPv4 ホストを表すために使用される IPv6 アドレス。 これらは、IPv4 アドレスへの明示的なマッピング関係を持ちます。 この関係は、IPv6 アドレスで IPv4 アドレスをマッピングすることにより、自動的に示されます。 ステートレスおよびステートフル トランスレータのいずれも、IPv4-Converted IPv6 アドレスを使用して IPv4 ホストを表します。

IPv6-Converted アドレス：ステートレス トランスレータの IPv6 ホストに割り当てられた IPv6 アドレス。 これらの IPv6-Converted アドレスは、IPv4 アドレスに対する明示的なマッピング関係を持ちます。 この関係は、IPv6 アドレスで IPv4 アドレスをマッピングすることにより、自動的に示されます。 ステートレス トランスレータは、対応する IPv4 アドレスを使用して、IPv6 ホストを表します。 ステートフル トランスレータでは、IPv6-Converted アドレスは使用されません。これは、IPv6 ホストが、ダイナミック ステートを介して、トランスレータ内の IPv4 アドレス プールにより表されるためです。

NAT：ネットワーク アドレス変換（NAT）。

RP：ルート プロセッサ。

ステートフル変換：ステートフル変換では、フローで最初のパケットが受信されたときに、フローごとのステートが作成されます。 パケットの送信または受信によって、関連するネットワーク要素のデータ構造が作成または変更される場合、変換アルゴリズムはステートフルであるとされます。 ステートフル変換は、複数のトランスレータを同等に使用できる以外に、ある程度のレベルの拡張性もあります。 ステートフル変換は、IPv6 クライアントおよびピアが、マッピングされた IPv4 アドレスなしで IPv4 専用サーバおよびピアに接続できるように定義されています。

ステートレス変換：ステートフルではない変換アルゴリズムはステートレスと呼ばれます。 ステートレス変換ではスタティック変換テーブルを設定する必要があります。設定しない場合、変換対象のメッセージからアルゴリズムによって情報を取得できます。 ステートレス変換に必要な計算のオーバーヘッドは、ステートフル変換より少なくなります。 また、ステートを保持するために必要なメモリも少なくなります。これは、変換テーブルおよびその関連メソッドとプロセスは、ステートフルアルゴリズムに存在し、ステートレスアルゴリズムには存在しないためです。ステートレス変換では、IPv4 専用クライアントおよびピアが、IPv4 埋め込み IPv6 アドレスを備えた IPv6 専用サーバまたはピアへの接続を開始できるようにします。 IPv4 専用スタブ ネットワークまたは ISP IPv6 専用ネットワークのスケーラブルな調整も可能にします。 IPv6-to-IPv4 変換の送信元ポートは、適切にフローを識別できるように変更する必要がある場合があるため、IPv4-to-IPv6 方向の送信元ポートを変更する必要はありません。

第 12 章

ステートフル ネットワーク アドレス変換64 シャーシ間冗長化

ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化機能により、ステートフル ネットワーク アドレス変換 64（NAT64）にシャーシ間冗長化サポートが追加されます。 ステートフル シャーシ間冗長化を使用すると、デバイスのペアが互いのバックアップとして動作するように設定できます。

このモジュールでは、ステートフル NAT64 シャーシ間冗長化の設定方法について説明します。

- 機能情報の確認，231 ページ
- ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化の制約事項，232 ページ
- ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化について，232 ページ
- ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化の設定方法，239 ページ
- ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化の設定例，251 ページ
- その他の関連資料，252 ページ
- ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化の機能情報，253 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化の制約事項

- 非対称ルーティングはサポートされません。
- ボックスツーボックス（B2B）冗長性とシャーシ間冗長化の併用はサポートされません。
- NAT インターフェイス オーバーロード設定はサポートされません。

ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化について

ステートフル シャーシ間冗長化の動作

相互にホットスタンバイとして動作するようにデバイスのペアを設定できます。冗長性は、インターフェイス ベースで設定します。 冗長インターフェイスのペアは、冗長グループ（RG）と呼ばれます。冗長性はアプリケーション レベルで発生します。インターフェイスまたはデバイスで完全な物理的障害が発生しなくても、アプリケーションのスイッチオーバーが行われます。 スイッチオーバーが行われると、アプリケーション アクティビティは冗長インターフェイスでシームレスに実行を続けます。

以下の最初の図は、アクティブ/スタンバイのロード シェアリング シナリオを示しています。 図には、発信インターフェイスを 1 つ持つデバイス ペアに対してどのように RG が設定されているかが示されています。 2 番目の図は、アクティブ/アクティブのロード シェアリング シナリオを示しています。 以下の図は、発信インターフェイスを 2 つ持つデバイス ペアに対して、どのように 2 つの RG が設定されているかを示しています。 ASR1 のグループ A はスタンバイ RG で、ASR 2 のグループ A はアクティブ RG です。

いずれの場合でも、設定可能なコントロール リンクおよびデータ同期リンクによって冗長デバイスは参加します。 コントロール リンクは、デバイスのステータスを通信するために使用されます。 データ同期リンクは、ネットワーク アドレス変換（NAT）およびファイアウォールからステートフル情報を転送し、ステートフルデータベースを同期するために使用されます。冗長イン

ターフェイスのペアは、冗長インターフェイス ID（RII）と呼ばれる、同じ固有 ID 番号で設定されます。

図 *14*：冗長グループの設定：*1* つの発信インターフェイス

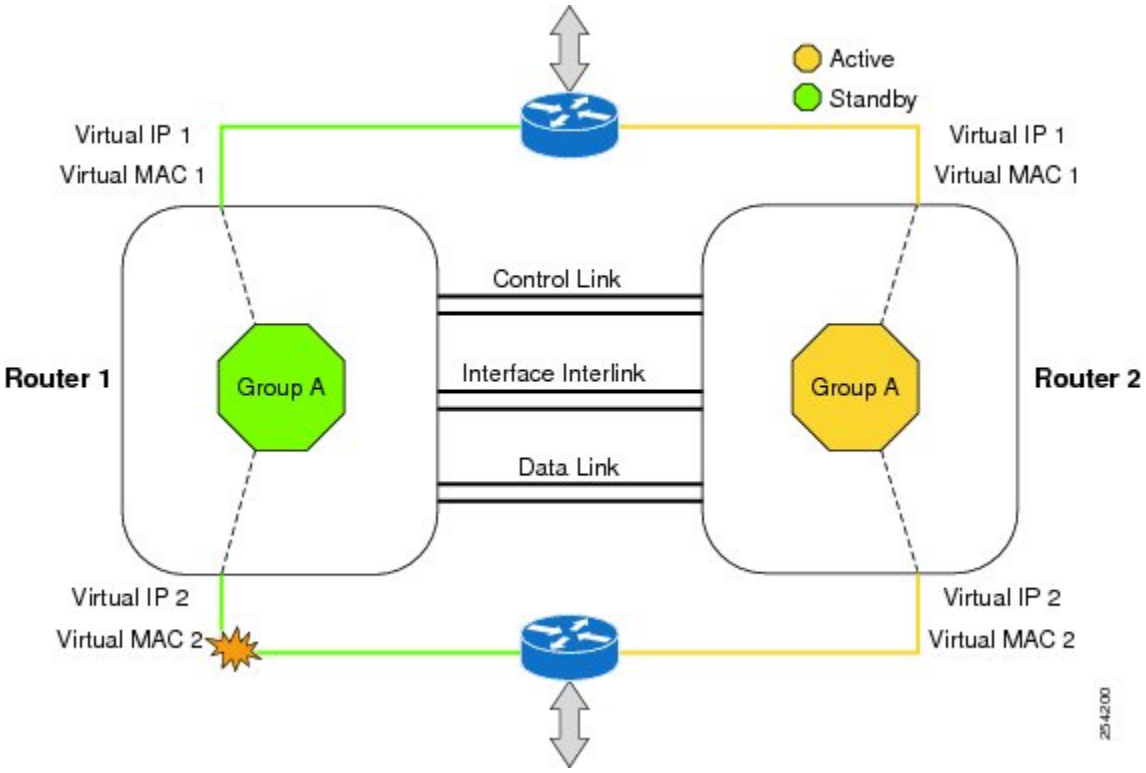
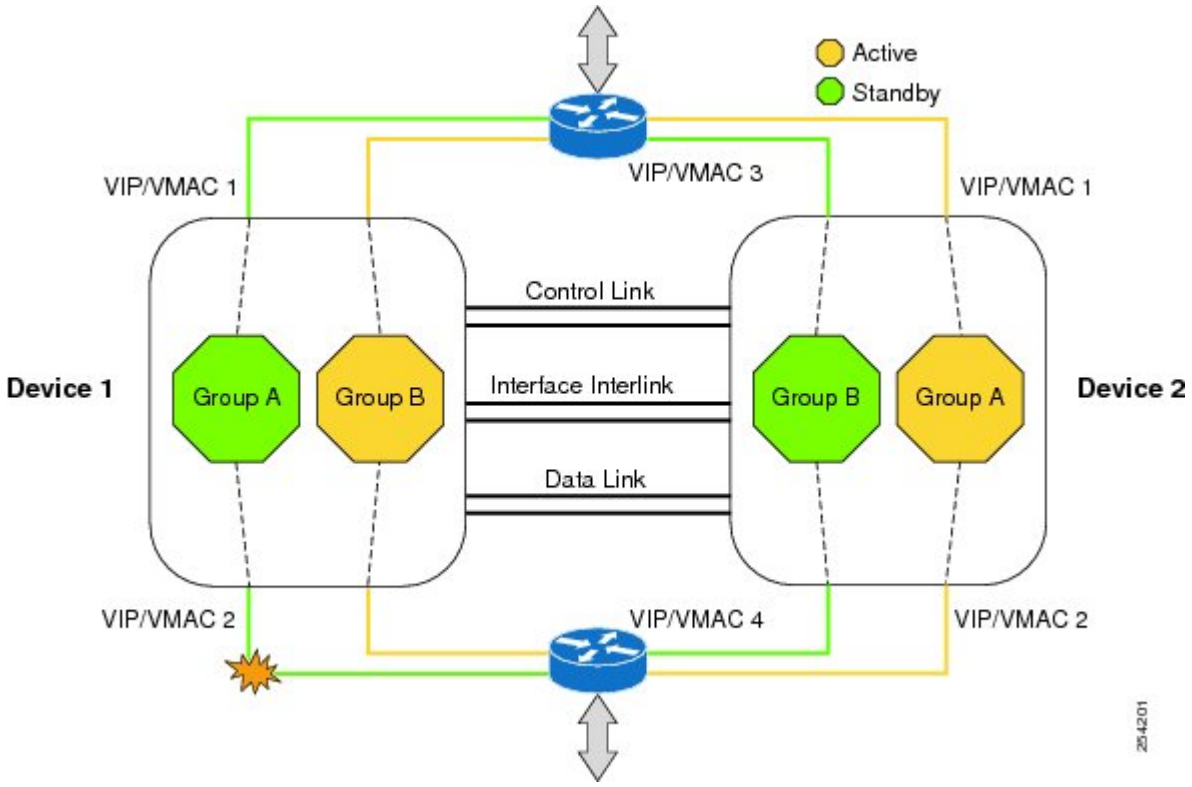


図 *15*：冗長グループの設定：*2* つの発信インターフェイス



冗長グループ メンバーのステータスは、コントロール リンクで送信される hello メッセージを使用することで判断できます。 ソフトウェアでは、設定可能な時間内にいずれかのデバイスが hello メッセージに応答しない場合、これを障害と見なし、スイッチオーバーを開始します。 ソフトウェアがミリ秒単位で障害を検出できるように、コントロール リンクでは、双方向フォワーディング検出（BFD）プロトコルと統合されているフェールオーバー プロトコルを実行します。 hello メッセージについて次のパラメータを設定できます。

- hello タイム：hello メッセージの送信間隔。
- ホールド タイム：アクティブまたはスタンバイ デバイスがダウン状態であると宣言されるまでの時間。

hello タイムのデフォルトは、ホットスタンバイ ルータ プロトコル（HSRP）に合わせるために 3 秒です。また、ホールド タイムのデフォルトは 10 秒です。 また、**timers hellotime msec** コマンドを使用して、これらのタイマーをミリ秒単位で設定することもできます。

スイッチオーバーの影響を受けるインターフェイスのペアを判断するには、冗長インターフェイスの各ペアについて、固有の ID を設定する必要があります。 この ID は RII と呼ばれ、インターフェイスに関連付けられます。

スタンバイ デバイスへのスイッチオーバーは、各デバイスに設定された優先度の設定が変更された場合に発生することがあります。 最高の優先度値を持つデバイスが、アクティブデバイスとして動作します。 アクティブ デバイスまたはスタンバイ デバイスで障害が発生した場合、重みと呼ばれる設定可能な数値分、デバイスの優先度が減らされます。 アクティブ デバイスの優先度が、スタンバイデバイスの優先度を下回る場合、スイッチオーバーが発生し、スタンバイデバイ

スがアクティブ デバイスになります。 このデフォルトの動作を無効にするには、RG について preemption 属性をディセーブルにします。 また、インターフェイスのレイヤ 1 ステートがダウン状態になった場合に優先度を減らすように、各インターフェイスを設定できます。 設定された優先度により、RG のデフォルトの優先度が上書きされます。

RG の優先度を変更する各障害イベントにより、タイム スタンプ、影響を受けた RG、前の優先度、新しい優先度、および障害イベントの原因の説明を含む syslog エントリが生成されます。

スイッチオーバーは、デバイスまたはインターフェイスの優先度が、設定可能なしきい値レベルを下回った場合にも発生することがあります。

スタンバイ デバイスへのスイッチオーバーは、次の状況で発生します。

- アクティブ デバイスでパワー損失またはリロードが発生した場合（リロードを含む）。
- アクティブ デバイスの実行時優先度が、スタンバイ デバイスの実行時優先度を下回った場合（プリエンプションが設定されている場合）。
- アクティブ デバイスの実行時優先度が、設定されたしきい値を下回った場合。
- アクティブ デバイスの冗長グループが手動でリロードされた場合。 手動リロードには、**redundancy application reload group** *rg-number* コマンドを使用します。

アクティブ/アクティブ フェールオーバー

アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、両方のデバイスがネットワーク トラフィックを処理できます。 アクティブ/アクティブ フェールオーバーでは、各冗長グループ（RG）でインターフェイスの仮想 MAC（VMAC）アドレスが生成されます。

アクティブ/アクティブ フェールオーバー ペアの一方のデバイスが、プライマリ（アクティブ）デバイスとして割り当てられ、もう一方はセカンダリ（スタンバイ）デバイスとして割り当てられます。 アクティブ/スタンバイ フェールオーバーとは異なり、この割り当ては、両方のデバイスが同時に起動した場合にいずれのデバイスがアクティブになるかを示すわけではありません。代わりに、プライマリ/セカンダリの割り当ては次のことを決定します。

- フェールオーバー ペアが同時に起動した場合に、そのペアに実行コンフィギュレーションを提供するデバイス。
- デバイスが同時に起動した場合に、フェールオーバー RG がアクティブ ステートで表示されるデバイス。 コンフィギュレーション内の各フェールオーバー RG がプライマリかセカンダリのデバイス プリファレンスに設定されます。 両方のフェールオーバー RG を 1 台のデバイスでアクティブ ステートになるように設定し、スタンバイ フェールオーバー RG をもう一方のデバイスに設定できます。 1 台のデバイスで、1 つのフェールオーバー RG をアクティブ ステートに、もう 1 つの RG をスタンバイ ステートにするように設定することもできます。

アクティブ/スタンバイ フェールオーバー

アクティブ/スタンバイ フェールオーバーでは、スタンバイ デバイスを使用して、障害の発生したデバイスの機能を引き継ぐことができます。障害の発生したアクティブデバイスはスタンバイステートに移行し、スタンバイデバイスがアクティブステートに移行します。アクティブステートになったデバイスは、障害の発生したデバイスの IP アドレスと MAC アドレスを引き継いで、トラフィックの処理を開始します。 スタンバイ ステートになったデバイスは、スタンバイ IP アドレスと MAC アドレスを引き継ぎます。 ネットワーク デバイスでは MAC と IP アドレスの組み合わせの変更が認識されないため、ネットワーク上のどこでも、アドレス解決プロトコル（ARP）エントリは変更されず、またタイムアウトしません。

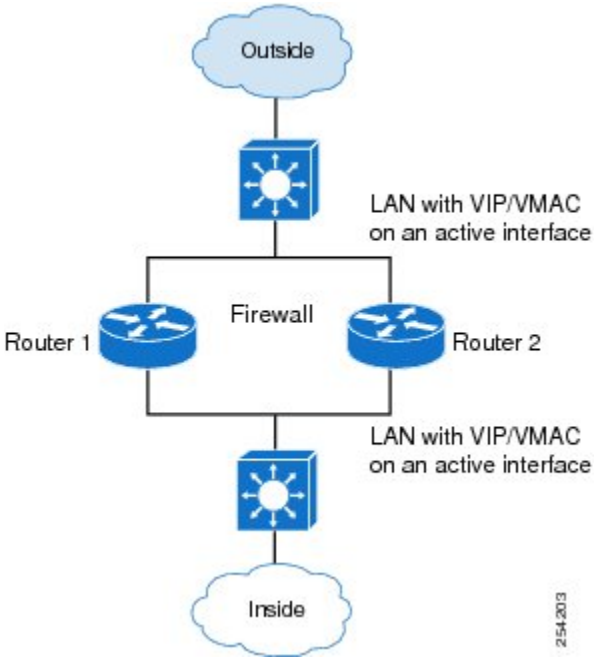
アクティブ/スタンバイ シナリオでは、フェールオーバーペアの2つのデバイス間の主な違いは、いずれのデバイスがアクティブで、いずれのデバイスがスタンバイか、つまり、使用している IP アドレスおよびトラフィックをアクティブに渡しているデバイスがいずれであるかによって決まります。 両方のデバイスが同時に起動した場合（かつ動作状態が同じである場合）、アクティブデバイスは常にアクティブ デバイスになります。 アクティブ デバイスの MAC アドレスは、常にアクティブな IP アドレスと組み合わされます。

LAN/LAN トポロジ

LAN/LAN トポロジでは、すべての参加デバイスが、内部および外部の両方で LAN インターフェイスを介して相互に接続されます。 このシナリオでは、スタティックルーティングがアップストリームまたはダウンストリームデバイスで適切な仮想IPアドレスに設定されていれば、トラフィックは通常正しいファイアウォールに送られます。 LAN方向のインターフェイスでサポートされるダイナミックルーティング設定では、ルーティングプロトコルのコンバージェンスへの依存が生

じないようにしてください。依存があると、高速フェールオーバー要件に適合しなくなります。以下の図は、LAN/LAN トポロジを示しています。

図 *16*：*LAN/LAN* シナリオ



ステートフル NAT64 の冗長グループ

ステートフル ネットワーク アドレス変換 64（NAT64）ボックスツーボックス（B2B）冗長性をサポートするには、すべてのステートフル NAT64 マッピングを冗長グループ（RG）に関連付ける必要があります。 1 つの RG に複数のステートフル NAT64 マッピングを関連付けることができます。 ステートフル NAT64 マッピングから作成されたセッションまたはバインドはすべて、ステートフル NAT64 のマッピング先である RG に関連付けられます。 B2B 冗長性では、ステートフル NAT64 ハイ アベイラビリティ（HA）メッセージをスタンバイ デバイスに送信するかどうかを決定するために、ステートフル NAT64 により、RG 内の作成、変更、または破棄されたセッションまたはバインドのステートが確認されます。

NAT バインディングは、ローカル IP アドレスとグローバル IP アドレス間の 1 対 1 のアソシエーションです。 セッションは 5 タプル（送信元 IP アドレス、宛先 IP アドレス、プロトコル、送信元ポート、宛先ポート）の情報によって識別されます。 セッションは通常、バインディングよりもはるかに速い速度で作成および破棄されます。

変換フィルタリング

RFC 4787 は、ネットワーク アドレス変換（NAT）に変換フィルタリング動作を提供します。 特定の外部エンドポイントから送信されるパケットをフィルタリングするために、次のオプションが NAT により使用されます。

- エンドポイントに依存しないフィルタリング：外部IPアドレスおよびポート送信元に関係なく、内部 IP アドレスおよびポートを宛先としないパケットをフィルタリングします。
- アドレス依存のフィルタリング：内部IPアドレスを宛先としないパケットをフィルタリングします。 NAT は、内部エンドポイントを宛先とするパケットもフィルタリングします。
- アドレスおよびポート依存のフィルタリング：内部 IP アドレスを宛先としないパケットをフィルタリングします。 NAT は、以前にエンドポイントに送信されたことがなく、内部エンドポイントを宛先とするパケットもフィルタリングします。

FTP64 アプリケーション レベル ゲートウェイ サポート

FTP64（またはサービス FTP）アプリケーション レベル ゲートウェイ（ALG）は、ステートフル ネットワーク アドレス変換 64（NAT64）がレイヤ 7 データを処理できるようにします。 FTP64 ALG は、FTP 制御セッションのペイロードに埋め込まれている IP アドレスおよび TCP ポート情報を変換します。

NAT は、アプリケーション データ ストリームで送信元および宛先 IP アドレスを伝送しない TCP/UDP トラフィックを変換します。 ペイロード内（またはアプリケーション データ ストリーム内）に IP アドレス情報を埋め込むプロトコルには、ALG サポートが必要です。 ALG は、パケットペイロード内の埋め込みIPアドレスおよびポート番号の変換や、制御チャネルからの新規接続またはセッション情報の取得といった、アプリケーション データ ストリーム（レイヤ 7）プロトコル固有のサービスを処理します。

FTP64 は、ステートフル NAT64 がイネーブルにされたときに自動的にイネーブルになります。 NAT64 FTP サービスをディセーブルにするには、**no nat64 service ftp** コマンドを使用します。

（注） FTP64 ALG は、ステートレス NAT64 変換ではサポートされません。

（注） FTP64 ALG は、IPv4 互換 IPv6 アドレスをサポートしません。

「*IPv6-to-IPv4 translation FTP considerations draft-ietf-behave-ftp64-02*」および RFC 2228 に基づき、FTP64 ALG は、コマンドおよび応答が FTP クライアントと FTP サーバの間で送受信されるときに、トランスペアレントモードに切り替える必要があります（トランスペアレントモードのデバイスはネットワークに表示されませんが、このデバイスはブリッジとして動作して、パケットの検査またはフィルタリングを行えます）。 クライアントが FTP AUTH コマンドを発行すると、FTP64 ALG は、制御チャネルセッションが終了するまで、制御チャネル上のすべてのデータを両

方（イングレスとイーグレス）の方向に転送します。 同様に、AUTH ネゴシエーション中は、ネゴシエーションが成功したかどうかに関係なく、ALG はトランスペアレント モードである必要があります。

RFC 6384 に基づき、クライアント/サーバ通信中の FTP64 ALG の動作は異なります。 IPv6-to-IPv4 変換時、FTP64 ALG は、制御チャネルを介して送信されたデータを透過的にコピーして、トランスポート層セキュリティ（TLS）セッションが正しく動作するようにする必要があります。 ただし、クライアント コマンドおよびサーバ応答は FTP64 ALG から隠されています。 動作の一貫性を確保するには、クライアントによる最初の FTP AUTH コマンドの発行直後に、FTP64 ALG がコマンドおよび応答の変換を停止して、サーバからクライアントまたはその逆に送信される TCP データの透過的コピーを開始する必要があります。 サーバ応答が、FTP エラー/警告メッセージを表す 4*xx* または 5*xx* レンジ内にある場合、FTP64 ALG は AUTH コマンドを無視し、トランスペアレント モードに移行しないでいる必要があります。

CSCtu37975 よりも前では、IPv4 FTP サーバが許可ネゴシエーションを受け入れたか拒否したかに関係なく、IPv6 FTP クライアントが FTP AUTH コマンドを発行すると、FTP64 ALG によって AUTH セッションがトランスペアレント モード（またはバイパス モード）に移行されます。 セッションがトランスペアレント モードの場合、NAT はセッション内のパケットに対する変換を実行できません。 CSCtu37975 では、クライアント/サーバ通信中の FTP64 ALG の動作は RFC 6384 に準拠します。

ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化の設定方法

冗長グループ プロトコルの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **protocol** *id*
6. **name** *group-name*
7. ステップ 3 ～ 6 を繰り返し、別のデバイスに冗長グループ プロトコルを設定します。
8. **timers hellotime** *seconds* **holdtime** *seconds*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長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	**application redundancy** 例： `Device(red)# application redundancy`	アプリケーションの冗長性を設定し、冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 5	**protocol** *id* 例： `Device(config-red-app)# protocol 1`	冗長グループのプロトコル インスタンスを定義し、冗長アプリケーション プロトコル 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	**name** *group-name* 例： `Device(config-red-app-prtcl)# name RG1`	冗長グループの名前を設定します。
ステップ 7	ステップ 3 ～ 6 を繰り返し、別のデバイスに冗長グループ プロトコルを設定します。	—
ステップ 8	**timers hellotime** *seconds* **holdtime** *seconds* 例： `Device(config-red-app-prtcl)# timers hellotime 1 holdtime 3`	冗長グループの hellotime および holdtime のメッセージ用のタイマーを設定します。
ステップ 9	**end** 例： `Device(config-red-app-prtcl)# end`	冗長アプリケーション プロトコル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

アクティブ/スタンバイ ロード シェアリング用の冗長グループの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **name** *group-name*
7. **control** *interface-type interface-number* **protocol** *id*
8. **data** *interface-type interface-number*
9. ステップ 3 ～ 8 を繰り返し、別の冗長グループを設定します。
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長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	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーションの冗長性を設定し、冗長アプリケーションコンフィギュレーションモードを開始します。
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長アプリケーション グループを設定し、冗長アプリケーション グループ 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 6	**name** *group-name* 例： `Device(config-red-app-grp)# name RG1`	冗長アプリケーション グループの名前を設定します。
ステップ 7	**control** *interface-type interface-number* **protocol** *id* 例： `Device(config-red-app-grp)# control gigabitethernet 0/0/1 protocol 1`	冗長アプリケーション グループのコントロール インターフェイス タイプと番号を設定します。
ステップ 8	**data** *interface-type interface-number* 例： `Device(config-red-app-grp)# data gigabitethernet 0/2/2`	冗長アプリケーション グループのデータ インターフェイス タイプと番号を設定します。
ステップ 9	ステップ 3 ～ 8 を繰り返し、別の冗長グループを設定します。	—
ステップ 10	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

アクティブ/アクティブ ロード シェアリング用の冗長グループの設定

アクティブ/アクティブ ロード シェアリング用に、同じデバイスに 2 つの冗長グループ（RG）を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **name** *group-name*
7. **priority** *value* [**failover-threshold** *value*]
8. **control** *interface-type interface-number* **protocol** *id*
9. **data** *interface-type interface-number*
10. **end**
11. **configure terminal**
12. **redundancy**
13. **application redundancy**
14. **group** *id*
15. **name** *group-name*
16. **priority** *value* [**failover-threshold** *value*]
17. **control** *interface-type interface-number* **protocol** *id*
18. **data** *interface-type interface-number*
19. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長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	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーションの冗長性を設定し、冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長アプリケーション グループを設定し、冗長アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 6	**name** *group-name* 例： `Device(config-red-app-grp)# name RG1`	冗長アプリケーション グループの名前を設定します。
ステップ 7	**priority** *value* [**failover-threshold** *value*] 例： `Device(config-red-app-grp)# priority 195 failover-threshold 190`	冗長グループのグループ優先度とフェールオーバーしきい値を指定します。
ステップ 8	**control** *interface-type interface-number* **protocol** *id* 例： `Device(config-red-app-grp)# control gigabitethernet 0/0/1 protocol 1`	冗長アプリケーション グループのコントロール インターフェイス タイプと番号を設定します。
ステップ 9	**data** *interface-type interface-number* 例： `Device(config-red-app-grp)# data gigabitethernet 0/2/2`	冗長アプリケーション グループのデータ インターフェイス タイプと番号を設定します。
ステップ 10	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 11	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 12	**redundancy** 例： `Device(config)# redundancy`	冗長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 13	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーションの冗長性を設定し、冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 14	**group** *id* 例： `Device(config-red-app)# group 2`	冗長アプリケーション グループを設定し、冗長アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 15	**name** *group-name* 例： `Device(config-red-app-grp)# name RG2`	冗長アプリケーション グループの名前を設定します。
ステップ 16	**priority** *value* [**failover-threshold** *value*] 例： `Device(config-red-app-grp)# priority 205 failover-threshold 200`	冗長グループのグループ優先度とフェールオーバーしきい値を指定します。
ステップ 17	**control** *interface-type interface-number* **protocol** *id* 例： `Device(config-red-app-grp)# control gigabitethernet 0/0/1 protocol 2`	冗長アプリケーション グループのコントロール インターフェイス タイプと番号を設定します。
ステップ 18	**data** *interface-type interface-number* 例： `Device(config-red-app-grp)# data gigabitethernet 0/2/2`	冗長アプリケーション グループのデータ インターフェイス タイプと番号を設定します。
ステップ 19	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ステートフル NAT64 シャーシ間冗長化用のトラフィック インターフェイスの設定

このタスクは、LAN/LAN シナリオに適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **redundancy rii** *id*
5. **redundancy group** *group-id* **ipv6** *ipv6-prefix*/*prefix-length* **exclusive decrement** *value*
6. **exit**
7. **interface** *type number*
8. **redundancy rii** *id*
9. **redundancy group** *group-id* **ipv6** *ipv6-prefix*/*prefix-length* **exclusive decrement** *value*
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**redundancy rii** *id* 例： `Device(config-if)# redundancy rii 100`	冗長グループ保護トラフィック インターフェイスの冗長インターフェイス ID（RII）を設定します。
ステップ 5	**redundancy group** *group-id* **ipv6** *ipv6-prefix*/*prefix-length* **exclusive decrement** *value* 例： `Device(config-if)# redundancy group 1 ipv6 2001:DB8:1::1:100/64 exclusive decrement 50`	IPv6 冗長性をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 7	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**redundancy rii** *id* 例： `Device(config-if)# redundancy rii 120`	冗長グループ保護トラフィック インターフェイスの RII を設定します。
ステップ 9	**redundancy group** *group-id* **ipv6** *ipv6-prefix*/*prefix-length* **exclusive decrement** *value* 例： `Device(config-if)# redundancy group 1 ipv6 2001:DB8:2::1:100/64 exclusive decrement 50`	IPv6 冗長性をイネーブルにします。
ステップ 10	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

シャーシ間冗長化用のスタティック ステートフル NAT64 の設定

スタティック ステートフルNAT64にシャーシ間冗長化を設定するには、次の作業を実行します。ダイナミック、スタティック、ポートアドレス変換（PAT）変換の、各タイプのNAT設定にシャーシ間冗長化を設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **ipv6 enable**
6. **ipv6 address** *ipv6-address*/*prefix-length*
7. **nat64 enable**
8. **exit**
9. ステップ 3 ～ 8 を繰り返し、別のインターフェイスで NAT64 を設定します。
10. **nat64 prefix stateful** *ipv6-prefix*/*length*
11. **nat64 v6v4 static** *ipv6-address ipv6-address* [**redundancy** *group-id* **mapping-id** *id*]
12. **nat64 v6v4 tcp** *ipv6-address ipv6-port ipv4-address ipv4-port* [**redundancy** *group-id* **mapping-id** *id*]
13. **end**
14. **show nat64 translations protocol tcp**
15. **show nat64 translations redundancy** *group-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 4	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	インターフェイスでIPv6処理をイネーブルにします。
ステップ 6	**ipv6 address** *ipv6-address*/*prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:1::1/96`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 7	**nat64 enable** 例： `Device(config-if)# nat64 enable`	IPv6 インターフェイスで、NAT64 変換をイネーブルにします。
ステップ 8	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 9	ステップ 3 ～ 8 を繰り返し、別のインターフェイスで NAT64 を設定します。	—
ステップ 10	**nat64 prefix stateful** *ipv6-prefix*/*length* 例： `Device(config)# nat64 prefix stateful 2001:DB8:1::1/96`	IPv4 アドレスを IPv6 アドレスに変換するために IPv4 ホストに追加するステートフル NAT64 プレフィックスを定義します。 • ステートフル NAT64 プレフィックスは、グローバル コンフィギュレーション レベルまたはインターフェイス コンフィギュレーション レベルで設定できます。
ステップ 11	**nat64 v6v4 static** *ipv6-address ipv6-address* [**redundancy** *group-id* **mapping-id** *id*] 例： `Device(config)# nat64 v6v4 static 2001:DB8:1::FFFE 209.165.201.1 redundancy 1 mapping-id 30`	NAT64 IPv6-to-IPv4 スタティック アドレス マッピングおよびシャーシ間冗長化をイネーブルにします。
ステップ 12	**nat64 v6v4 tcp** *ipv6-address ipv6-port ipv4-address ipv4-port* [**redundancy** *group-id* **mapping-id** *id*] 例： `Device(config)# nat64 v6v4 tcp 2001:DB8:1::1 redundancy 1 mapping-id 1`	スタティック マッピングを TCP プロトコル パケットに適用して、シャーシ間冗長化をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 13	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 14	**show nat64 translations protocol tcp** 例： `Device# show nat64 translations protocol tcp`	NAT64 プロトコル変換に関する情報を表示します。
ステップ 15	**show nat64 translations redundancy** *group-id* 例： `Device# show nat64 translations redundancy 1`	NAT64 冗長性変換に関する情報を表示します。

例：

次に、**show nat64 translations protocol tcp** コマンドの出力例を示します。

```
Device# show nat64 translations protocol tcp

 Proto  Original IPv4         Translated IPv4
        Translated IPv6       Original IPv6
 ------------------------------------------------------------------------------

 tcp    209.165.201.2:21      [2001:DB8:1::103]:32847
        10.2.1.1:80           [2001::11]:80
 tcp    209.165.201.2:21      [2001:DB8:1::104]:32848
        10.2.1.1:80           [2001::11]:80

 Total number of translations: 2
```

次に、**show nat64 translations redundancy** コマンドの出力例を示します。

```
Device# show nat64 translations redundancy 1

 Proto  Original IPv4         Translated IPv4
        Translated IPv6       Original IPv6
 ------------------------------------------------------------------------------

        209.165.201.2:21      [2001:DB8:1::103]:32847

 tcp    10.2.1.11:32863       [2001::3201:10b]:32863
        10.1.1.1:80           [2001::11]:80
 tcp    209.165.201.2:21      [2001:DB8:1::104]:32848
        10.1.1.1:80           [2001::11]:80

 Total number of translations: 3
```

ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化の設定例

例：冗長グループ プロトコルの設定

```
Device# configure terminal
Device(config)# redundancy
Device(red)# application redundancy
Device(config-red-app)# protocol 1
Device(config-red-app-prtcl)# name RG1
Device(config-red-app-prtcl)# timers hellotime 1 holdtime 3
Device(config-red-app-prtcl)# end
Device# configure terminal
Device(config)# redundancy
Device(red)# application redundancy
Device(config-red-app)# protocol 2
Device(config-red-app-prtcl)# name RG1
Device(config-red-app-prtcl)# end
```

例：アクティブ/スタンバイ ロード シェアリング用の冗長グループの設定

次の例に、アクティブ/スタンバイ ロード シェアリング用に、2 つのデバイスに冗長グループ（RG）を設定する方法を示します。

```
Device1# configure terminal
Device1(config)# redundancy
Device1(config-red)# application redundancy
Device1(config-red-app)# group 1
Device1(config-red-app-grp)# name RG1
Device1(config-red-app-grp)# control gigabitethernet 0/0/1 protocol 1
Device1(config-red-app-grp)# data gigabitethernet 0/2/2
Device1(config-red-app-grp)# end

Device2# configure terminal
Device2(config)# redundancy
Device2(config-red)# application redundancy
Device2(config-red-app)# group 1
Device2(config-red-app-grp)# name RG1
Device2(config-red-app-grp)# control gigabitethernet 0/0/1 protocol 1
Device2(config-red-app-grp)# data gigabitethernet 0/2/2
Device2(config-red-app-grp)# end
```

例：アクティブ/アクティブ ロード シェアリング用の冗長グループの設定

次の例に、アクティブ/アクティブ ロード シェアリング用に、同じデバイスに 2 つの冗長グループ（RG）を設定する方法を示します。

```
Device1# configure terminal
Device1(config)# redundancy
```

```
Device1(config-red)# application redundancy
Device1(config-red-app)# group 1
Device1(config-red-app-grp)# name RG1
Device1(config-red-app-grp)# priority 195 failover-threshold 190
Device1(config-red-app-grp)# control gigabitethernet 0/0/1 protocol 1
Device1(config-red-app-grp)# data gigabitethernet 0/2/2
Device1(config-red-app-grp)# end
Device1# configure terminal
Device1(config)# redundancy
Device1(config-red)# application redundancy
Device1(config-red-app)# group 2
Device1(config-red-app-grp)# name RG2
Device1(config-red-app-grp)# priority 205 failover-threshold 200
Device1(config-red-app-grp)# control gigabitethernet 0/0/1 protocol 2
Device1(config-red-app-grp)# data gigabitethernet 0/2/2
Device1(config-red-app-grp)# end

Device2# configure terminal
Device2(config)# redundancy
Device2(config-red)# application redundancy
Device2(config-red-app)# group 1
Device2(config-red-app-grp)# name RG1
Device2(config-red-app-grp)# priority 195 failover-threshold 190
Device2(config-red-app-grp)# control gigabitethernet 0/0/1 protocol 1
Device2(config-red-app-grp)# data gigabitethernet 0/2/2
Device2(config-red-app-grp)# end
Device2# configure terminal
Device2(config)# redundancy
Device2(config-red)# application redundancy
Device2(config-red-app)# group 2
Device2(config-red-app-grp)# name RG2
Device2(config-red-app-grp)# priority 205 failover-threshold 200
Device2(config-red-app-grp)# control gigabitethernet 0/0/1 protocol 2
Device2(config-red-app-grp)# data gigabitethernet 0/2/2
Device2(config-red-app-grp)# end
```

例：ステートフル NAT64 シャーシ間冗長化用のトラフィック インターフェイスの設定

```
Device# configure terminal
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# redundancy rii 100
Device(config-if)# redundancy group 1 ipv6 2001:DB8:1::1:100/64 exclusive decrement 50
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# redundancy rii 100
Device(config-if)# redundancy group 1 ipv6 2001:DB8::2:1:100/64 exclusive decrement 50
Device(config-if)# end
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
NAT コマンド	『IP Addressing Services Command Reference』

標準/RFC

標準/RFC	タイトル
RFC 4787	『*Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化の機能情報

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

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

表 *17*：ステートフル ネットワーク アドレス変換 *64* シャーシ間冗長化の機能情報

機能名	リリース	機能情報
ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化	Cisco IOS XE Release 3.7S	ステートフル ネットワーク アドレス変換 64 シャーシ間冗長化機能により、ステートフル ネットワーク アドレス変換 64（NAT64）にシャーシ間冗長化サポートが追加されます。 ステートフル シャーシ間冗長化を使用すると、デバイスのペアが互いのバックアップとして動作するように設定できます。 コマンド **clear nat64 translations**、**nat64 v4v6**、**nat64 v6v4**、**redundancy group (interface)**、**show nat64**、**show nat64 translations redundancy** が導入または変更されました。

第 13 章

変換を使用したアドレスおよびポートのマッピング

変換を使用したアドレスおよびポートのマッピング機能では、IPv6 ドメイン経由の IPv4 ホストへの接続を提供します。 変換を使用したアドレスおよびポートのマッピング（MAP-T）は、カスタマーエッジ（CE）デバイスおよび境界ルータでダブル変換（IPv4 から IPv6 およびその逆）を実行するメカニズムです。

このモジュールでは、MAP-T の概要と、この機能を設定する方法について説明します。

- 機能情報の確認，255 ページ
- 変換を使用したアドレスおよびポートのマッピングの制約事項，256 ページ
- 変換を使用したアドレスおよびポートのマッピングについて，256 ページ
- 変換を使用したアドレスおよびポートのマッピングの設定方法，261 ページ
- 変換を使用したアドレスおよびポートのマッピングの設定例，263 ページ
- 変換を使用したアドレスおよびポートのマッピングに関するその他の関連資料，264 ページ
- 変換を使用したアドレスおよびポートのマッピングの機能情報，265 ページ
- 用語集，266 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

変換を使用したアドレスおよびポートのマッピングの制約事項

- 変換を使用したアドレスおよびポートのマッピング（MAP-T）カスタマー エッジ（CE）機能はサポートされません。
- 最大 128 個の MAP-T ドメインがサポートされます。
- 転送マッピング ルール（FMR）はサポートされません。

変換を使用したアドレスおよびポートのマッピングについて

変換を使用したアドレスおよびポートのマッピングの概要

変換を使用したアドレスおよびポートのマッピング機能では、IPv6 ドメイン経由の IPv4 ホストへの接続を提供します。 変換を使用したアドレスおよびポートのマッピング（MAP-T）は、RFC 6052、6144、および 6145 で指定されている、既存のステートレス IPv4 および IPv6 アドレス変換手法を基にしています。

MAP-T は、カスタマー エッジ（CE）デバイスおよび境界ルータでダブル変換（IPv4 から IPv6 およびその逆）を実行するメカニズムです。 変換を使用したアドレスおよびポートのマッピング機能では、MAP-T 境界ルータ機能のみをサポートします。 この機能は MAP-T CE 機能はサポートしません。

変換を使用したアドレスおよびポートのマッピング機能では、ネットワーク アドレス変換 64（NAT64）変換エンジンを活用し、MAP-T 境界ルータ機能を NAT64 ステートレス機能に追加します。 MAP-T は、IPv4 および IPv6 インターフェイスでイネーブルにされます。 MAP-T では、IPv4 および IPv6 転送、IPv4 および IPv6 フラグメンテーション機能、および NAT64 変換機能を使用します。 MAP-T ドメインは、1 つ以上の MAP CE デバイスおよび境界ルータです。これらはすべて同じ IPv6 ネットワークに接続されています。

MAP-T CE デバイスは、ユーザのプライベート IPv4 アドレスおよびネイティブ IPv6 ネットワークを IPv6 専用 MAP-T ドメインに接続します。 MAP-T 境界ルータでは、ステートレス IPv4/IPv6 変換を使用して、1 つ以上の MAP-T ドメインで使用可能なすべてのデバイスに外部 IPv4 ネットワークを接続します。 MAP-T は、ネットワークごとに IPv6 プレフィックスを 1 つのみ必要とし、標準的な IPv6 プレフィックス/アドレス割り当てメカニズムをサポートします。 MAP-T ドメインには、IPv4-Translatable IPv6 アドレスを持つ標準的な IPv6 専用ホストまたはサーバが含まれます。

MAP-T では、IPv4 オーバーレイ ネットワークが動作している必要も、非ネイティブ IPv6 ネットワーク デバイスまたはサーバ機能を導入する必要もありません。

MAP-T 設定により、次の機能が提供されます。

- IPv4 エンド ホストが、IPv6 ドメインを経由して他の IPv4 ホストと通信する機能を保持します。
- 個別の IPv4 アドレス割り当ておよび事前定義されたポート範囲との IPv4 アドレス共有の両方を許可します。
- IPv4 専用エンド ホストおよび IPv6 がイネーブルにされているエンド ホストと、IPv4-Translatable IPv6 アドレスを使用するドメイン内のネイティブ IPv6 専用サーバとの間の通信を許可します。
- IPv6 ネイティブ ネットワーク操作の使用を許可します。これには、IP トラフィックの分類機能や、ドメイン外の IPv4 宛先に対するピアリング ポリシーに基づくルーティングの最適化といった、IP トラフィック ルーティング最適化ポリシーの実行機能が含まれます。

MAP-T マッピング ルール

マッピング ルールは、IPv4 プレフィックスおよび IPv4 アドレス間のマッピング、または共有 IPv4 アドレスおよび IPv6 プレフィックス/アドレス間のマッピングを定義します。 変換を使用したアドレスおよびポートのマッピング（MAP-T）ドメインごとに異なるマッピング ルールを使用します。

MAP-T 設定では、各 MAP-T ドメインに 1 つの基本マッピング ルール（BMR）、1 つのデフォルト マッピング ルール（DMR）、および 1 つ以上の転送マッピング ルール（FMR）があります。 MAP-T ドメインの BMR を設定する前に、DMR を設定する必要があります。

以下に、3 種類のマッピング ルールについて説明します。

- BMR は、MAP IPv6 アドレスまたはプレフィックスを設定します。 基本マッピング ルールは、送信元アドレス プレフィックスに対して設定されます。 IPv6 プレフィックスごとに設定できる基本マッピング ルールは 1 つのみです。 基本マッピング ルールは、MAP-T CE によって、それ自身に IPv4 アドレス、IPv4 プレフィックス、または IPv6 プレフィックスからの共有 IPv4 アドレスを設定するために使用されます。 基本マッピング ルールは、IPv4 宛先アドレスおよび宛先ポートが IPv6 アドレス/プレフィックスにマッピングされている場合のパケットの転送にも使用できます。 各 MAP-T ノード（CE デバイスが MAP-T ノードです）は、基本マッピング ルールを使用してプロビジョニングする必要があります。 MAP-T BMR のポート パラメータを設定するには、**port-parameters** コマンドを使用します。
- DMR は、MAP-T ドメイン外の宛先の IPv6 アドレスに IPv4 情報をマッピングするために使用される必須ルールです。 0.0.0.0/0 エントリは、このルール用に、MAP ルール テーブル（MRT）に自動的に設定されます。
- FMR はパケットを転送するために使用されます。 各 FMR によって、ルール IPv4 プレフィックスについて MRT 内にエントリが生成されます。 FMR は、MAP-T ドメイン内での IPv4 および IPv6 宛先のマッピングに使用されるオプションのルールです。

（注） FMR は、変換を使用したアドレスおよびポートのマッピング機能ではサポートされません。

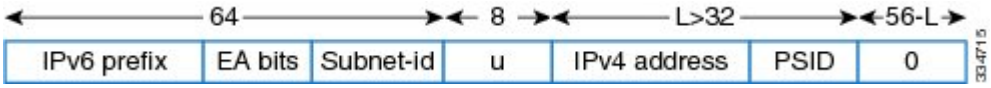
MAP-T アドレス形式

変換を使用したアドレスおよびポートのマッピング（MAP-T）カスタマーエッジ（CE）デバイスアドレス形式は、IETF ドラフト『Mapping of Address and Port (MAP)』により定義されます。 アドレス形式は、マッピングルール操作中に、送信元および宛先IPv6アドレスを作成するために使用されます。

（注） 転送マッピング ルール（FMR）は、変換を使用したアドレスおよびポートのマッピング機能ではサポートされません。

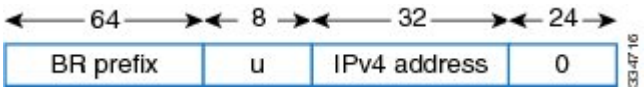
以下の図は、MAP-T 設定で定義されている、マッピングされた CE アドレス形式を示します。 このアドレス形式は、基本マッピング ルール（BMR）および FMR 操作で使用されます。

図 *17*： *BMR* および *FMR* の *IPv4-Translatable* アドレス



以下の図は、MAP-T のデフォルトマッピングルール（DMR）で使用されるアドレス形式である、MAP-T 設定に固有の IPv4-Translated アドレスを示します。

図 *18*： *DMR* 用の *IPv4-Translated* アドレス



MAP-T カスタマー エッジ デバイスでのパケット転送

（注） 変換を使用したアドレスおよびポートのマッピング機能では、MAP-T カスタマーエッジ（CE）機能をサポートしていません。 CE 機能は、サードパーティ製デバイスにより提供されます。

IPv4-to-IPv6 パケット転送

IPv4 パケットを受信する、変換を使用したアドレスおよびポートのマッピング（MAP-T）CE デバイスは、ネットワーク アドレス変換（NAT）を実行し、適切な NAT ステートフル バインディングを作成します。 作成される IPv4 パケットには、MAP-T で定義される送信元 IPv4 アドレスおよび送信元トランスポート番号が含まれます。 この IPv4 パケットは、IPv4-to-IPv6 ステートレス変換を実行する CE の MAP-T に転送されます。 続けて、IPv6 送信元および宛先アドレスが MAP-T 変換によって取得され、IPv4 ヘッダーが IPv6 ヘッダーに置き換えられます。

IPv6-to-IPv4 パケット転送

IPv6 パケットを受信する MAP-T CE デバイスは、通常の IPv6 操作を実行します。 基本マッピング ルール（BMR）アドレスを宛先とするパケットのみが CE の MAP-T に送信されます。 他の IPv6 トラフィックはすべて、CE デバイス上で IPv6 ルーティング ルールに基づいて転送されます。 CE デバイスは、MAP-T から受信するパケットのトランスポート層宛先ポート番号が、設定された範囲内にあるかどうかを確認し、その範囲内にあるポート番号を持つパケットを転送します。 CE デバイスは、設定に準拠しないパケットをすべてドロップし、インターネット制御メッセージ プロトコル バージョン 6（ICMPv6）の「Address Unreachable」メッセージで応答します。

境界ルータでのパケット転送

IPv4-to-IPv6 パケット転送

着信 IPv4 パケットは IPv4 入力インターフェイスにより処理され、宛先ルート検索によって、IPv4 パケットが、変換を使用したアドレスおよびポートのマッピング（MAP-T）仮想インターフェイスにルーティングされます。 境界ルータでは、IPv4 プレフィックス ルックアップ単位（PLU）ツリーに照らしてパケットを比較し、対応する基本マッピング ルール（BMR）、デフォルト マッピング ルール（DMR）、および転送マッピング ルール（FMR）を取得します。 BMR または FMR ルールに基づき、境界ルータは、埋め込みアドレス（EA）ビットを符号化し、サフィックスを追加することにより、IPv6 宛先アドレスを作成します。 IPv6 送信元アドレスは DMR ルールから作成されます。

IPv6 送信元および宛先アドレスの作成後、パケットではネットワーク アドレス変換 64（NAT64）IPv4-to-IPv6 変換を使用して、IPv6 パケットを作成します。 ルーティング検索は IPv6 パケットで実行され、パケットは IPv6 出力インターフェイスに処理および伝送のために転送されます。

IPv6-to-IPv4 パケット転送

着信 IPv6 パケットは IPv6 入力インターフェイスにより処理され、宛先ルート検索によって IPv6 パケットが MAP-T 仮想インターフェイスにルーティングされます。 ソフトウェアは、IPv6 PLU ツリーに照らしてパケットを比較し、対応する BMR、DMR、および FMR ルールを取得します。 境界ルータは、ポートセット ID（PSID）およびポートセットが一致するかどうかを確認します。 ポート セット ID およびポート セットが一致する場合、DMR ルールは IPv6 パケットのパケット宛先に一致します。 BMR および FMR に基づき、境界ルータは、IPv4 送信元アドレスを作成し、IPv6 宛先アドレスから IPv4 宛先アドレスを抽出します。 IPv6 パケットでは、NAT64 IPv6-to-IPv4 変換エンジンを使用して、IPv6 パケットから IPv4 パケットを作成します。 ルーティング検索は

IPv4パケットで実行され、IPv4パケットはIPv4出力インターフェイスに処理および伝送のために転送されます。

MAP-T 用の ICMP/ICMPv6 ヘッダー変換

変換を使用したアドレスおよびポートのマッピング（MAP-T）カスタマーエッジ（CE）デバイスおよび境界ルータでは、ポート範囲のアドレス共有のために ICMP/ICMPv6 変換を使用します。

送信元および宛先アドレスを表すために 2 つのポート フィールドを提供する TCP および UDP とは異なり、インターネット制御メッセージ プロトコル（ICMP）および ICMP バージョン 6（ICMPv6）クエリー メッセージ ヘッダーには ID フィールドが 1 つだけあります。

MAP-T CE デバイス外に存在する IPv4 ホストから送信された ICMP クエリー メッセージでは、ICMP ID フィールドは IPv4 ホストを識別するためにだけ使用されます。 MAP-T CE デバイスでは ID フィールドを、IPv4-to-IPv6 変換中に基本マッピング ルール（BMR）により取得されるポート セット値に書き換え、境界ルータでは ICMPv6 パケットを ICMP に変換します。

MAP-T 境界ルータでは、MAP-T ドメイン内の共有アドレス宛の、ID フィールドを含む ICMP パケットを受信した場合、そのIDフィールドを宛先ポートの代わりとして使用して、IPv6宛先アドレスを決定します。 境界ルータは、IDフィールドを含まないパケットについては、ポート情報なしで宛先 IPv4 アドレスをマッピングすることにより宛先 IPv6 アドレスを取得し、対応する CE デバイスが ICMPv6 パケットを ICMP に変換します。

MAP-T での Path MTU 検出およびフラグメンテーション

変換を使用したアドレスおよびポートのマッピング（MAP-T）では、IPv4 ヘッダーのサイズ（20 個を超えるオクテット）および IPv6 ヘッダーのサイズ（40 個のオクテット）が異なるため、IPv4-to-IPv6 変換でパス最大伝送単位（MTU）検出およびフラグメンテーションを使用します。 MTU では、インターフェイスがパケットのフラグメンテーションを必要とせずに送信できるパケットの最大サイズを定義します。 MTU より大きい IP パケットは、IP フラグメンテーション プロシージャを経由する必要があります。

IPv4 ノードがパケット ヘッダーに Don't Fragment（DF）ビットを設定してパス MTU 検出を実行すると、パス MTU 検出は MAP-T 境界ルータおよびカスタマー エッジ（CE）トランスレータにわたりエンドツーエンドで動作します。 IPv4 パス MTU 検出中は、IPv4 デバイスまたは IPv6 デバイスが ICMP の「Packet Too Big」メッセージを送信元に送信できます。 IPv6 デバイスがこれらのメッセージをインターネット制御メッセージプロトコルバージョン 6（ICMPv6）エラーとして送信すると、そのメッセージ後のパケットはトランスレータを通過し、結果として IPv4 送信元に適切な ICMP エラー メッセージが送信されます。

IPv4 送信元で DF ビットが設定されない場合、トランスレータでは IPv4 パケットをフラグメント化して、パケットが最少の MTU 1280 バイト IPv6 パケット内に収まるようパケットをフラグメント ヘッダーに含めます。 パケットが送信元または IPv4 デバイスのいずれかによってフラグメント化されると、パケットが正しく再構成されるように、フラグメントの識別番号の下位 16 ビットが MAP-T ドメインを経由してエンドツーエンドで伝送されます。

変換を使用したアドレスおよびポートのマッピングの設定方法

変換を使用したアドレスおよびポートのマッピングの設定

はじめる前に

前提条件

- 変換を使用したアドレスおよびポートのマッピング機能を設定するインターフェイスで **ipv6 enable** コマンドを設定します。
- 基本マッピング ルールを設定する前に、デフォルト マッピング ルールを設定します。
- 変換を使用したアドレスおよびポートのマッピング（MAP-T）の設定中、デフォルトマッピング ルール（DMR）プレフィックス、IPv6 ユーザ プレフィックス、および埋め込みアドレス（EA）ビットが追加された IPv6 プレフィックスは 64 ビット以下である必要があり、共有率、連続するポート、開始ポートの合計が 16 ビットである必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **nat64 map-t domain** *number*
4. **default-mapping-rule** *ipv6-prefix*/*prefix-length*
5. **basic-mapping-rule**
6. **ipv6-prefix** *prefix*/*length*
7. **ipv4-prefix** *prefix*/*length*
8. **port-parameters share-ratio** *ratio* [**start-port** *port-number*]
9. **end**
10. **show nat64 map-t domain** *name*

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**nat64 map-t domain** *number* 例： `Device(config)# nat64 map-t domain 1`	変換を使用したアドレスおよびポートのネットワーク アドレス変換 64（NAT64）マッピング（MAP-T）ドメインを設定し、NAT64 MAP-T コンフィギュレーション モードを開始します。
ステップ 4	**default-mapping-rule** *ipv6-prefix*/*prefix-length* 例： `Device(config-nat64-mapt)# default-mapping-rule 2001:DB8:B001:FFFF::/64`	MAP-T ドメインのデフォルト ドメイン マッピング ルールを設定します。
ステップ 5	**basic-mapping-rule** 例： `Device(config-nat64-mapt)# basic-mapping-rule`	MAP-T ドメインの基本マッピング ルール（BMR）を設定し、NAT64 MAP-T BMR 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	**ipv6-prefix** *prefix*/*length* 例： `Device(config-nat64-mapt-bmr)# ipv6-prefix 2001:DB8:B001::/56`	MAP-T BMR の IPv6 アドレスおよびプレフィックスを設定します。
ステップ 7	**ipv4-prefix** *prefix*/*length* 例： `Device(config-nat64-mapt-bmr)# ipv4-prefix 209.165.202.129/28`	MAP-T BMR の IPv4 アドレスおよびプレフィックスを設定します。
ステップ 8	**port-parameters share-ratio** *ratio* [**start-port** *port-number*] 例： `Device(config-nat64-mapt-bmr)# port-parameters share-ratio 16`	MAP-T BMR のポート パラメータを設定します。
ステップ 9	**end** 例： `Device(config-nat64-mapt-bmr)# end`	NAT64 MAP-T BMR コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**show nat64 map-t domain** *name* 例： `Device# show nat64 map-t domain 1`	MAP-T ドメイン情報を表示します。

例：

次に、**show nat64 map-t domain** コマンドの出力例を示します。

```
Device# show nat64 map-t domain 1

MAP-T Domain 1
   Mode MAP-T
   Default-mapping-rule
      Ip-v6-prefix 2001:DB8:B001:FFFF::/64
   Basic-mapping-rule
      Ip-v6-prefix 2001:DB8:B001::/56
      Ip-v4-prefix 209.165.202.129/28
      Port-parameters
         Share-ratio 16   Contiguous-ports 256   Start-port 4096
         Share-ratio-bits 4   Contiguous-ports-bits 8   Port-offset-bits 4
```

変換を使用したアドレスおよびポートのマッピングの設定例

例：変換を使用したアドレスおよびポートのマッピングの設定

```
Device# configure terminal
Device(config)# nat64 map-t domain 1
Device(config-nat64-mapt)# default-mapping-rule 2001:DB8:B001:FFFF::/64
Device(config-nat64-mapt)# basic-mapping-rule
Device(config-nat64-mapt-bmr)# ipv6-prefix 2001:DB8:B001::/56
Device(config-nat64-mapt-bmr)# ipv4-prefix 209.165.202.129/28
Device(config-nat64-mapt-bmr)# port-parameters share-ratio 16
Device(config-nat64-mapt-bmr)# end
```

例：MAP-T 展開シナリオ

次の図に、変換を使用したアドレスおよびポートのマッピング（MAP-T）の展開シナリオを示します。

MAP-T 展開シナリオの設定を次に示します。

```
Device# configure terminal
Device(config)# nat64 map-t domain 1
Device(config-nat64-mapt)# default-mapping-rule 2001:DB8:B001:FFFF::/64
Device(config-nat64-mapt)# basic-mapping-rule
Device(config-nat64-mapt-bmr)# ipv6-prefix 2001:DB8:B001::/48
Device(config-nat64-mapt-bmr)# ipv4-prefix 202.38.102.128/28
```

```
Device(config-nat64-mapt-bmr)# port-parameters share-ratio 16 start-port 1024
Device(config-nat64-mapt-bmr)# end
```

PC において：

IPv4 パケットは、192.168.1.12 から 74.1.1.1 に送信されます。 カスタマー エッジ（CE）デバイスで、変換を使用したアドレスおよびポートのマッピング（MAP-T）機能によってパケットが 2001:DB8:B001:20:CB:2666:8200:: Dest: 2001:DB8:B001:FFFF:4a:01001:100:: に変換されます。

境界ルータで、MAP-T 境界ルータによってパケットが次のように変換されます。

パケット送信元 192.168.1.2 ---> 74.1.1.1、source 6400、destination port: 80

CPE で、MAP-T CE 機能により、

パケットが 2001:DA8:B001:20:CB:2666:8200:: Dest: 2001:DA8:B001:FFFF:4a:0101:100:: に変換されます

BR で、MAP-T BR 機能により、パケットが

Src:203.38.102.130 Dst:74.1.1.1 SrcPort:6400 DstPort:80 に変換されます

エンド デバイスから：

Src:74.1.1.1 Dst:203.38.102.130 SrcPort:80 DstPort:6400

BR で、MAP-T BR 機能により、パケットが

Src: 2001:DA8:B001:FFFF:4a:0101:100:: Dest: 2001:DA8:B001:20:CB:2666:8200:: に変換されます

CE で、MAP-T CE 機能により、パケットが

Src: 2001:DA8:B001:FFFF:4a:0101:100:: Dest: 2001:DA8:B001:20:CB:2666:8200::

から

Src:74.1.1.1 Dst:203.38.102.130 SrcPort:80 Dstport:6400 に変換されます

例に問題がある場合はお知らせください。

変換を使用したアドレスおよびポートのマッピングに関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
NAT コマンド	『Cisco IOS IP Addressing Services Command Reference』

標準および RFC

標準/RFC	タイトル
MAP	『Mapping of Address and Port (MAP)』
MAP 変換	『MAP Translation (MAP-T) - specification』
RFC 6052	『IPv6 Addressing of IPv4/IPv6 Translators』
RFC 6144	『Framework for IPv4/IPv6 Translation』
RFC 6145	『IP/ICMP Translation Algorithm』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

変換を使用したアドレスおよびポートのマッピングの機能情報

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

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

表 *18*：変換を使用したアドレスおよびポートのマッピングの機能情報

機能名	リリース	機能情報
変換を使用したアドレスおよびポートのマッピング	Cisco IOS XE Release 3.8S	変換を使用したアドレスおよびポートのマッピング機能では、IPv6 ドメイン経由の IPv4 ホストへの接続を提供します。 MAP-T は、CE デバイスおよび境界ルータでダブル変換（IPv4 から IPv6 およびその逆）を実行するメカニズムです。 コマンド **basic-mapping-rule**、**default-mapping-rule**、**ipv4-prefix**、**ipv6-prefix**、**mode (nat64)**、**nat64 map-t domain**、**port-parameters**、および **show nat64 map-t** が導入または変更されています。

用語集

EA ビット：埋め込みアドレス ビット。 IPv6 アドレスの IPv4 EA ビットは、IPv4 プレフィックス/アドレス（またはその一部）または共有 IPv4 アドレス（またはその一部）とポート セット ID を識別します。

IP フラグメンテーション：データグラムが、後に再構成が可能な多数の断片に分割されるプロセス。 IP ヘッダー内の More Fragments および Don't Fragment（DF）フラグとともに、IP 送信元、宛先、識別番号、合計長、およびフラグメントのオフセット フィールドが IP フラグメンテーションおよび再構成のために使用されます。 DF ビットは IP ヘッダー内のビットで、このビットは、デバイスがパケットのフラグメント化を許可されているかどうか判別します。

IPv4-Translatable アドレス：IPv4 ホストを表すために使用される IPv6 アドレス。 これらのアドレスは、IPv6 アドレスへの明示的なマッピング関係を持ちます。 この関係は、IPv6 アドレスで IPv4 アドレスをマッピングすることにより、自動的に示されます。 ステートレスおよびステートフル トランスレータはいずれも IPv4-Translatable（IPv4-Converted とも呼びます）IPv6 アドレスを使用して IPv4 ホストを表します。

IPv6-Translatable アドレス：ステートレス変換のために IPv6 ホストに割り当てられる IPv6 アドレス。 これらの IPv6-Translatable アドレス（IPv6-Converted アドレスとも呼びます）は、IPv4 アドレスへの明示的なマッピング関係を持ちます。 この関係は、IPv6 アドレスで IPv4 アドレスをマッピングすることにより、自動的に示されます。 ステートレス トランスレータは、対応する IPv4 アドレスを使用して、IPv6 ホストを表します。 ステートフル トランスレータでは、IPv6-Translatable アドレスは使用されません。これは、IPv6 ホストが、ダイナミック ステートを介して、トランスレータ内の IPv4 アドレス プールにより表されるためです。

MAP ルール：IPv4プレフィックス、IPv4アドレス、または共有IPv4アドレスと、IPv6プレフィックスまたはアドレス間のマッピングを定義するパラメータのセット。 各 MAP ドメインで異なるマッピング ルール セットが使用されます。

MAP-T 境界ルータ：MAP-T ドメインに接続を提供する、MAP ドメインのエッジにある、変換を使用したアドレスおよびポートのマッピング（MAP-T）対応ルータまたはトランスレータ。 境界リレールータには、少なくとも1つのIPv6対応インターフェイスと、ネイティブIPv4ネットワークに接続されている 1 つの IPv4 インターフェイスがあり、このルータは複数の MAP-T ドメインに対応できます。

MAP-T CE：MAP-T 展開で、カスタマー エッジ（CE）ルータとして動作するデバイス。 MAP ルールを採用する一般的な MAP-T CE デバイスは、1 つの WAN 側インターフェイスと 1 つ以上のLAN側インターフェイスを持つ家庭向けサイトに対応します。 MAP-T CEデバイスは、MAP-T ドメインのコンテキスト内で「CE」と呼ばれることもあります。

MAP-T ドメイン：変換を使用したアドレスおよびポートのマッピング（MAP-T）ドメイン。 1つ以上のカスタマー エッジ（CE）デバイスおよび境界ルータ。すべて同じ IPv6 ネットワークに接続されています。 サービス プロバイダーは、単一の MAP-T ドメインを展開することも、複数の MAP ドメインを使用することもできます。

MRT：MAP ルール テーブル。 最長一致検索をサポートするアドレスおよびポート対応データ構造。 MRT は MAP-T 転送機能により使用されます。

パス MTU：パス最大伝送単位（MTU）検出は、エンドポイント間のパスのフラグメンテーションを防止します。 パス MTU 検出は、パケットの送信元から宛先までのパス上で、最も低い MTU をダイナミックに判断するために使用されます。 パス MTU 検出は、TCP および UDP でのみサポートされます。 パス MTU 検出は IPv6 では必須ですが、IPv4 ではオプションです。 IPv6 デバイスによりパケットがフラグメント化されることはありません。パケットをフラグメント化できるのは送信元のみです。

ステートフル変換：フローで最初のパケットが受信されたときに、フローごとのステートを作成します。 パケットの送信または受信によって、関連するネットワーク要素のデータ構造が作成または変更される場合、変換アルゴリズムはステートフルであるとされます。 ステートフル変換は、複数のトランスレータを同等に使用できる以外に、ある程度のレベルの拡張性もあります。ステートフル変換では、IPv6クライアントおよびピアが、マッピングされたIPv4アドレスなしでIPv4 専用サーバおよびピアに接続できるようにします。

ステートレス変換：ステートフルではない変換アルゴリズム。 ステートレス変換ではスタティック変換テーブルを設定する必要があります。設定しない場合、変換対象のメッセージからアルゴリズムによって情報を取得できます。 ステートレス変換に必要な計算のオーバーヘッドは、ステートフル変換より少なくなります。 また、ステートを保持するために必要なメモリも少なくなります。これは、変換テーブルおよびその関連メソッドとプロセスは、ステートフル アルゴリズムに存在し、ステートレス アルゴリズムには存在しないためです。 ステートレス変換では、IPv4 専用クライアントおよびピアが、IPv4 埋め込み IPv6 アドレスを備えた IPv6 専用サーバまたはピアへの接続を開始できるようにします。 IPv4 専用スタブ ネットワークまたは ISP IPv6 専用ネットワークのスケーラブルな調整も可能にします。 IPv6-to-IPv4 変換の送信元ポートは、適切にフローを識別できるように変更する必要がある場合があるため、IPv4-to-IPv6 方向の送信元ポートを変更する必要はありません。

第 14 章

ファイアウォールおよびNAT対応のMSRPC ALGサポート

ファイアウォールおよびNAT対応のMSRPC ALGサポート機能は、ファイアウォールおよびネットワーク アドレス変換（NAT）での、Microsoft（MS）リモート プロシージャ コール（RPC）アプリケーション レベル ゲートウェイ（ALG）のサポートを提供します。MSRPC ALGは、MSRPCプロトコルのディープ パケット インスペクション（DPI）を提供します。MSRPC ALGは、ネットワーク管理者に、MSRPCパケットで検索可能な一致基準を定義するための一致フィルタの設定を許可するプロビジョニング システムと連携します。

- ファイアウォールおよびNAT対応のMSRPC ALGサポートに関する制約事項，269 ページ
- ファイアウォールおよびNAT対応のMSRPC AICサポートに関する制約事項，270 ページ
- ファイアウォールおよびNAT対応のMSRPC ALGサポートについて，270 ページ
- ファイアウォールおよびNAT対応のMSRPC ALGサポートの設定方法，273 ページ
- ファイアウォールおよびNAT対応のMSRPC ALGサポートの設定例，276 ページ
- ファイアウォールおよびNAT対応のMSRPC ALGサポートに関するその他の関連資料，277 ページ
- ファイアウォールおよびNAT対応のMSRPC ALGサポートの機能情報，278 ページ

ファイアウォールおよびNAT対応のMSRPC ALGサポートに関する制約事項

- パケットにMSRPC ALGを適用する前に、Cisco IOS XEファイアウォールとNATをイネーブルにする必要があります。

ファイアウォールおよび NAT 対応の MSRPC AIC サポートに関する制約事項

- TCP-based MSRPC のみがサポートされます。
- **allow** および **reset** コマンドを同時に設定することはできません。
- DPI に **match protocol msrpc** コマンドを設定する必要があります。

ファイアウォールおよび NAT 対応の MSRPC ALG サポートについて

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション層ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内のIPアドレス情報を変換するアプリケーションです。 ALG はアプリケーション層プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。 これらのアクションは、ファイアウォールおよび NAT の設定に応じた次の 1 つ以上のアクションです。

- ダイナミック TCP または UDP ポートを使用したサーバ アプリケーションとの通信をクライアント アプリケーションに許可します。
- アプリケーション固有のコマンドを認識し、それらのコマンドに対するきめ細かなセキュリティ制御を提供します。
- データ交換を行う 2 台のホスト間のデータの複数のストリームまたはセッションを同期します。
- アプリケーション ペイロードで使用可能なネットワーク層アドレス情報を変換します。

ファイアウォールがピンホールを開き、NATは、アプリケーション層データ ストリームで送信元および宛先 IP アドレスを伝送しない TCP または UDP トラフィックで変換サービスを実行します。 IPアドレス情報を埋め込む特定のプロトコルまたはアプリケーションには、ALGのサポートが必要です。

MSRPC

MSRPCは、サーバおよび企業に対し一連のアプリケーションとサービスを公開するために開発者が使用するフレームワークです。 RPCは、クライアントおよびサーバ ソフトウェアがネットワークを介して通信できるようにするための、プロセス間通信技術です。 MSRPC は、さまざまな

Microsoft アプリケーションが使用するアプリケーション層プロトコルです。 MSRPC は、さまざまなトランスポート プロトコルで、コネクション型（CO）およびコネクレションレス型（CL）両方の分散コンピューティング環境（DCE）RPC モードをサポートします。 MSRPC のすべてのサービスで、プライマリ接続と呼ばれる最初のセッションが確立されます。 MSRPC の一部のサービスにより、1024 ～ 65535 の間のポート範囲を宛先ポートとして、セカンダリ セッションが確立されます。

ファイアウォールおよび NAT がイネーブルになったときに MSRPC が動作するようにするには、MSRPC パケットのインスペクションに加え、ALG で、ダイナミック ファイアウォール セッションの確立や、NAT 後のパケット コンテンツの修正など、MSRPC 固有の問題を処理する必要があります。

MSRPC プロトコル インスペクションを適用すると、ほとんどの MSRPC サービスがサポートされるため、レイヤ 7 ポリシー フィルタが不要になります。

ファイアウォールでの MSRPC ALG

MSRPC プロトコルを検査するようにファイアウォールを設定すると、MSRPC ALG によって MSRPC メッセージの解析が開始されます。 次の表は、ファイアウォールおよび NAT 対応の MSRPC ALG サポート機能でサポートされるプロトコル データ ユニット（PDU）のタイプについて説明しています。

表 *19*：サポートされる *PDU* タイプ

PDU	番号	タイプ	説明
REQUEST	0	コール	コール要求を開始します。
RESPONSE	2	コール	コール要求に応答します。
FAULT	3	コール	RPC ランタイム、RPC スタブ、または RPC 固有の例外を示します。
BIND	11	アソシエーション	本文データのプレゼンテーションのネゴシエーションを開始します。
BIND_ACK	12	アソシエーション	バインド要求を受け入れます。
BIND_NAK	13	アソシエーション	アソシエーション要求を拒否します。

PDU	番号	タイプ	説明
ALTER_CONTEXT	14	アソシエーション	別のインターフェイスまたはバージョンについて追加のプレゼンテーションのネゴシエーションを要求するか、新しいセキュリティ コンテキストをネゴシエートするか、またはその両方を行います。
ALTER_CONTEXT_RESP	15	アソシエーション	ALTER_CONTEXT PDU に応答します。 有効な値は accept または deny です。
SHUTDOWN	17	コール	クライアントに接続の終了を要求し、関連するリソースを解放します。
CO_CANCEL	18	コール	接続をキャンセルするか、孤立させます。 このメッセージは、クライアントがキャンセルのエラーを検出した場合に送信されます。
ORPHANED	19	コール	進行中の要求、およびまだ完全に送信されていない要求を中断するか、進行中の（多くの場合時間のかかる）応答を中断します。

NAT での MSRPC ALG

NAT では、MSRPC パケットを受信すると、パケット ペイロードを解析し、埋め込み IP アドレスを変換するためのトークンを作成する MSRPC ALG を呼び出します。 このトークンは NAT に渡され、ユーザの NAT 設定に従ってアドレスまたはポートを変換します。 変換後のアドレスは、MSRPC ALG によってパケット ペイロードに再び書き込まれます。

ファイアウォールと NAT の両方を設定している場合、NAT は ALG を最初に呼び出します。

MSRPC ステートフル パーサー

MSRPC ステート マシンまたはパーサーは、MSRPC ALG の中枢です。 MSRPC ステートフル パーサーは、すべてのステートフル情報を、いずれの機能が最初にパーサーを起動したかに応じて、ファイアウォールまたは NAT 内に保持します。 パーサーは、MSRPC プロトコル パケットの DPI を提供します。 これは、プロトコルへの準拠を確認し、シーケンス外コマンドや不正パケットを

検出します。 ステート マシンでは、パケットの解析時に、さまざまなデータを記録し、NAT およびファイアウォール インスペクション用に正しいトークン情報を入力します。

ファイアウォールおよび NAT 対応の MSRPC ALG サポートの設定方法

（注） デフォルトでは、NAT をイネーブルにすると、MSRPC ALG は自動的にイネーブルになります。 NAT のみの設定では MSRPC ALG を明示的にイネーブルにする必要はありません。 NAT において MSRPC ALG をディセーブルにするには、**no ip nat service alg** コマンドを使用します。

レイヤ 4 MSRPC クラス マップおよびポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Router(config)# class-map type inspect match-any msrpc-cmap`	トラフィック クラスの検査タイプ クラス マップを作成し、QoS クラスマップ 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	**match protocol** *protocol-name* 例： `Router(config-cmap)# match protocol msrpc`	指定されたプロトコルを基づくクラス マップの一致基準を設定します。 • 検査タイプ クラス マップでは Cisco IOS XE ステートフル パケット インスペクションがサポートするプロトコルのみを一致基準として使用できます。
ステップ 5	**exit** 例： `Router(config-cmap)# exit`	QoS クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**policy-map type inspect** *policy-map-name* 例： `Router(config)# policy-map type inspect msrpc-pmap`	レイヤ 3 またはレイヤ 4 の検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 7	**class type inspect** *class-map-name* 例： `Router(config-pmap)# class type inspect msrpc-class-map`	アクションを実行する対象のトラフィック（クラス）を指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**inspect** 例： `Router(config-pmap-c)# inspect`	Cisco IOS XE ステートフル パケット インスペクションをイネーブルにします。
ステップ 9	**end** 例： `Router(config-pmap-c)# end`	QoS ポリシー マップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーン ペアの設定および MSRPC ポリシー マップの付加

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *security-zone-name*
4. **exit**
5. **zone security** *security-zone-name*
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** [*destination-zone*]]
8. **service-policy type inspect** *policy-map-name*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Rotuer# 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	**zone security** *security-zone-name* 例： `Router(config)# zone security in-zone`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 5	**zone security** *security-zone-name* 例： `Router(config)# zone security out-zone`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** [*destination-zone*]] 例： `Router(config)# zone-pair security in-out source in-zone destination out-zone`	ゾーン ペアを作成し、セキュリティ ゾーン ペア コンフィギュレーション モードを開始します。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Router(config-sec-zone-pair)# service-policy type inspect msrpc-pmap`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**end** 例： `Router(config-sec-zone-pair)# end`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ファイアウォールおよび NAT 対応の MSRPC ALG サポートの設定例

例：レイヤ 4 MSRPC クラス マップおよびポリシー マップの設定

```
Router# configure terminal
Router(config)# class-map type inspect match-any msrpc-cmap
Router(config-cmap)# match protocol msrpc
Router(config-cmap)# exit
Router(config)# policy-map type inspect msrpc-pmap
Router(config-pmap)# class type inspect msrpc-cmap
Router(config-pmap-c)# inspect
Router(config-pmap-c)# end
```

例：ゾーン ペアの設定および MSRPC ポリシー マップの付加

```
Router# configure terminal
Router(config)# zone security in-zone
Router(config-sec-zone)# exit
Router(config)# zone security out-zone
Router(config-sec-zone)# exit
Router(config)# zone-pair security in-out source in-zone destination out-zone
Router(config-sec-zone-pair)# service-policy type inspect msrpc-pmap
Router(config-sec-zone-pair)# end
```

ファイアウォールおよび NAT 対応の MSRPC ALG サポートに関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
NAT コマンド	『Cisco IOS IP Addressing Services Command Reference』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
NAT ALG	「Using Application-Level Gateways with NAT」モジュール
ALG サポート	『*NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォールおよび NAT 対応の MSRPC ALG サポートの機能情報

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

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

表 *20*：ファイアウォールおよび *NAT* 対応の *MSRPC ALG* サポートの機能情報

機能名	リリース	機能情報
ファイアウォールおよび NAT 対応の MSRPC ALG サポート	Cisco IOS XE Release 3.5S	ファイアウォールおよび NAT 対応の MSRPC ALG サポート機能は、ファイアウォールおよび NAT における MSRPC ALG のサポートを提供します。MSRPC ALG は、MSRPC プロトコルのディープ パケット インスペクションを提供します。MSRPC ALG は、ネットワーク管理者に、MSRPC パケットで検索可能な一致基準を定義するための一致フィルタの設定を許可するプロビジョニング システムと連携します。 コマンド **ip nat service msrpc**、**match protocol msrpc** が導入または変更されました。

第 15 章

ファイアウォールおよびNAT対応のSun RPC ALG サポート

ファイアウォールおよびNAT 対応の Sun RPC ALG サポート機能により、ファイアウォールおよびネットワーク アドレス変換（NAT）における Sun Microsystems リモート プロシージャ コール（RPC）アプリケーション レベル ゲートウェイ（ALG）のサポートが追加されます。 Sun RPC は、リモート サーバ プログラム内の関数をクライアント プログラムが呼び出すことができるようにするアプリケーション層プロトコルです。 このモジュールでは、Sun RPC ALG を設定する方法について説明します。

- 機能情報の確認，281 ページ
- ファイアウォールおよび NAT 対応の Sun RPC ALG サポートに関する制約事項，282 ページ
- ファイアウォールおよび NAT 対応の Sun RPC ALG サポートについて，282 ページ
- ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの設定方法，284 ページ
- ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの設定例，293 ページ
- ファイアウォールおよびNAT 対応の Sun RPC ALG サポートに関するその他の関連資料，295 ページ
- ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの機能情報，296 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

ファイアウォールおよび NAT 対応の Sun RPC ALG サポートに関する制約事項

- リリースによっては、Cisco ASR 1000 アグリゲーション サービス ルータで次の設定が動作しないものがあります。 レイヤ 4 またはレイヤ 7 クラス マップの検査アクションを設定した場合、ポート マッパー プロトコルの well-known ポート（111）に一致するパケットが、レイヤ 7 インスペクションなしでファイアウォールを通過します。 レイヤ 7 インスペクションが行われない場合、トラフィック フロー用にファイアウォール ピンホールが開かれず、Sun リモート プロシージャ コール（RPC）がファイアウォールによってブロックされます。 回避策として、Sun RPC プログラム番号に **match program-number** コマンドを設定します。
- ポート マッパー プロトコル バージョン 2 のみがサポートされます。他のバージョンはいずれもサポートされません。
- RPC バージョン 2 のみサポートされます。

ファイアウォールおよび NAT 対応の Sun RPC ALG サポートについて

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション層ゲートウェイとも呼ばれ、アプリケーション パケットのペイロード内の IP アドレス情報を変換するアプリケーションです。 ALG はアプリケーション層プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。 これらのアクションは、ファイアウォールおよび NAT の設定に応じた次の 1 つ以上のアクションです。

- ダイナミック TCP または UDP ポートを使用したサーバ アプリケーションとの通信をクライアント アプリケーションに許可します。
- アプリケーション固有のコマンドを認識し、それらのコマンドに対するきめ細かなセキュリティ制御を提供します。
- データ交換を行う 2 台のホスト間のデータの複数のストリームまたはセッションを同期します。
- アプリケーション ペイロードで使用可能なネットワーク層アドレス情報を変換します。

ファイアウォールがピンホールを開き、NATは、アプリケーション層データ ストリームで送信元および宛先 IP アドレスを伝送しない TCP または UDP トラフィックで変換サービスを実行します。 IPアドレス情報を埋め込む特定のプロトコルまたはアプリケーションには、ALGのサポートが必要です。

Sun RPC

Sun リモート プロシージャ コール（RPC）アプリケーション レベル ゲートウェイ（ALG）は、Sun RPCプロトコルのディープ パケット インスペクションを実行します。 Sun RPC ALG は、ネットワーク管理者に一致フィルタの設定を許可するプロビジョニング システムと連携します。各一致フィルタで、Sun RPCパケット内で検索される一致基準が定義され、その基準に一致するパケットのみが許可されます。

RPC では、クライアント プログラムは、サーバ プログラム内のプロシージャを呼び出します。 RPC ライブラリは、プロシージャ引数をネットワーク メッセージ内にパッケージ化し、メッセージをサーバに送信します。次にサーバは、RPCライブラリを使用して、ネットワーク メッセージからプロシージャ引数を取り出し、指定されたサーバ プロシージャを呼び出します。 サーバ プロシージャがRPCに戻ると、戻り値がネットワーク メッセージ内にパッケージ化され、クライアントに送り返されます。

Sun RPCプロトコルの詳細については、RFC 1057、『*RPC: Remote Procedure Call Protocol Specification Version 2*』を参照してください。

ファイアウォール対応の Sun RPC ALG サポート

ポリシーとクラス マップを使用して作成される、ゾーン ベースのファイアウォールを使用して Sun RPC ALG を設定できます。 レイヤ 7 クラス マップによって、ネットワーク管理者に一致フィルタの設定が許可されます。 このフィルタでは、Sun RPC パケット内で検索するプログラム番号を指定します。 Sun RPC レイヤ 7 ポリシー マップは、**service-policy** コマンドにより、レイヤ 4 ポリシー マップの子ポリシーとして設定します。

レイヤ 7 ファイアウォール ポリシーを設定しないで Sun RPC レイヤ 4 クラス マップを設定すると、Sun RPC により戻されるトラフィックはファイアウォールを通過しますが、セッションはレイヤ7で検査されません。 セッションが検査されないため、後続のRPC呼び出しがファイアウォールによってブロックされます。 Sun RPC レイヤ 4 クラス マップおよびレイヤ 7 ポリシーを設定すると、レイヤ 7 インスペクションが使用できるようになります。 一致フィルタを持たないポリシーである、空のレイヤ 7 ファイアウォール ポリシーを設定できます。

NAT 対応の Sun RPC ALG サポート

デフォルトでは、ネットワーク アドレス変換（NAT）をイネーブルにすると、Sun RPC ALG が自動的にイネーブルになります。 NAT において Sun RPC ALG をディセーブルにするには、**no ip nat service alg** コマンドを使用します。

ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの設定方法

ファイアウォールおよびNATがイネーブルの場合にSun RPCを動作させるには、ALGでSun RPCパケットを検査する必要があります。 またALGでは、ダイナミック ファイアウォール セッションの確立、NAT 変換後のパケット コンテンツの修正など、Sun RPC 固有の問題も処理します。

Sun RPC ALG 対応のファイアウォールの設定

Sun RPC プロトコルに検索アクションを設定している場合（**match protocol sunrpc** コマンドをレイヤ 4 クラス マップに指定している場合）、レイヤ 7 Sun リモート プロシージャ コール（RPC）ポリシー マップを設定する必要があります

セキュリティ ゾーンと検査ルールの両方を同じインターフェイスに設定しないでください。この設定は機能しない場合があります。

Sun RPC ALG 対応のファイアウォールを設定するには、次の作業を実行します。

ファイアウォール ポリシー対応のレイヤ 4 クラス マップの設定

ネットワーク トラフィックを分類するためのレイヤ 4 クラス マップを設定するには、この作業を実行します。 **match-all** キーワードを **class-map type inspect** コマンドに指定すると、Sun RPC トラフィックは、クラス マップ内のすべての Sun リモート プロシージャ コール（RPC）レイヤ 7 フィルタ（プログラム番号により指定）に一致します。 **match-any** キーワードを **class-map type inspect** に指定した場合、Sun RPC トラフィックでは、クラス マップ内の 1 つ以上の Sun RPC レイヤ 7 フィルタ（プログラム番号により指定）に一致する必要があります。

レイヤ 4 クラス マップを設定するには、**class-map type inspect {match-any | match-all}** *classm-map-name* コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect** {**match-any** | **match-all**} *class-map-name*
4. **match protocol** *protocol-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect** {**match-any** | **match-all**} *class-map-name* 例： `Device(config)# class-map type inspect match-any sunrpc-l4-cmap`	レイヤ 4 検査タイプ クラス マップを作成し、QoS クラス 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	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol sunrpc`	指定したプロトコルに基づいてクラスマップの一致基準を設定します。
ステップ 5	**end** 例： `Device(config-cmap)# end`	QoS クラス マップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ファイアウォール ポリシー対応のレイヤ 7 クラス マップの設定

ネットワーク トラフィックを分類するためのレイヤ 7 クラス マップを設定するには、この作業を実行します。 この設定により、Sun RPC を使用する、マウント（100005）やネットワーク ファイル システム（NFS）（100003）などのプログラムがイネーブルになります。 100005 および 100003 は Sun RPC プログラムの番号です。 デフォルトでは、Sun RPC ALG はすべてのプログラムをブロックします。

Sun RPC プログラムおよびプログラム番号の詳細については、RFC 1057、『*RPC: Remote Procedure Call Protocol Specification Version 2*』を参照してください。

レイヤ 7 クラス マップを設定するには、**class-map type inspect** *protocol-name* コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name*
4. **match program-number** *program-number*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name* 例： `Device(config)# class-map type inspect sunrpc match-any sunrpc-l7-cmap`	レイヤ7（アプリケーション固有）検査タイプ クラスマップを作成し、QoS クラスマップ 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	**match program-number** *program-number* 例： `Device(config-cmap)# match program-number 100005`	許可する RPC プロトコル プログラム番号を一致基準として指定します。
ステップ 5	**end** 例： `Device(config-cmap)# end`	QoS クラス マップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

Sun RPC ファイアウォール ポリシー マップの設定

Sun リモート プロシージャ コール（RPC）ファイアウォール ポリシー マップを設定するには、この作業を実行します。 ポリシー マップを使用して、レイヤ 7 ファイアウォール ポリシーのクラス マップで定義する Sun RPC レイヤ 7 クラスごとにパケット転送を許可します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *protocol-name policy-map-name*
4. **class type inspect** *protocol-name class-map-name*
5. **allow**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect** *protocol-name policy-map-name* 例： `Device(config)# policy-map type inspect sunrpc sunrpc-l7-pmap`	レイヤ 7（プロトコル固有）検査タイプ ポリシー マップを作成し、QoS ポリシー 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	**class type inspect** *protocol-name class-map-name* 例： `Device(config-pmap)# class type inspect sunrpc sunrpc-l7-cmap`	アクションを実行する対象のトラフィック クラスを指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**allow** 例： `Device(config-pmap-c)# allow`	パケット転送を許可します。
ステップ 6	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシー マップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

レイヤ 4 ポリシー マップへのレイヤ 7 ポリシー マップの付加

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class** {*class-map-name* | **class-default**}
5. **inspect** [*parameter-map-name*]
6. **service-policy** *protocol-name policy-map-name*
7. **exit**
8. **class class-default**
9. **drop**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect sunrpc-l4-pmap`	レイヤ 4 検査タイプ ポリシー マップを作成し、QoS ポリシー 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	**class** {*class-map-name*	**class-default**} 例： `Device(config-pmap)# class sunrpc-l4-cmap`	アクションを実行する対象のクラスを関連付け、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**inspect** [*parameter-map-name*] 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 6	**service-policy** *protocol-name policy-map-name* 例： `Device(config-pmap-c)# service-policy sunrpc sunrpc-l7-pmap`	レイヤ 7 ポリシー マップを最上位のレイヤ 4 ポリシー マップに付加します。
ステップ 7	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoS ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 8	**class class-default** 例： `Device(config-pmap)# class class-default`	ポリシーを設定する前にデフォルト クラス（一般的にクラスデフォルト クラスと呼ばれます）を指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 9	**drop** 例： `Device(config-pmap-c)# drop`	特定のクラスに属するパケットを廃棄するトラフィック クラスを設定します。
ステップ 10	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

セキュリティ ゾーンとゾーン ペアの作成、およびゾーン ペアへのポリシー マップの付加

ゾーン ペアを作成するには、2 つのセキュリティ ゾーンが必要です。 ただし、1 つのセキュリティ ゾーンのみ作成でき、もう 1 つのセキュリティ ゾーンはシステム定義のセキュリティ ゾーンにすることができます。 システム定義のセキュリティ ゾーンまたはセルフ ゾーンを作成するには、**self** キーワードを指定した **zone-pair security** コマンドを設定します。

（注） セルフ ゾーンを選択する場合、検査アクションは設定できません。

この作業では、次のことを行います。

- セキュリティ ゾーンを作成します。
- ゾーン ペアを定義します。

- セキュリティ ゾーンにインターフェイスを割り当てます。
- ポリシー マップをゾーン ペアに付加します。

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** {*zone-name* | **default**}
4. **exit**
5. **zone security** {*zone-name* | **default**}
6. **exit**
7. **zone-pair security** *zone-pair-name* **source** *source-zone-name* **destination** *destination-zone-name*
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
12. **zone-member security** *zone-name*
13. **exit**
14. **interface** *type number*
15. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
16. **zone-member security** *zone-name*
17. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** {*zone-name*	**default**} 例： `Device(config)# zone security z-client`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 設定には、ゾーン ペアを作成するために、送信元ゾーンと宛先ゾーンの 2 つのセキュリティ ゾーンが必要です。

	コマンドまたはアクション	目的
		• ゾーン ペアでは、送信元ゾーンまたは宛先ゾーンとして、デフォルト ゾーンまたはセルフ ゾーンを使用できます。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**zone security** {*zone-name* | **default**} 例： `Device(config)# zone security z-server`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 設定には、ゾーンペアを作成するために、送信元ゾーンと宛先ゾーンの 2 つのセキュリティ ゾーンが必要です。 • ゾーン ペアでは、送信元ゾーンまたは宛先ゾーンとして、デフォルト ゾーンを使用できます。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**zone-pair security** *zone-pair-name* **source** *source-zone-name* **destination** *destination-zone-name* 例： `Device(config)# zone-pair security clt2srv source z-client destination z-server`	ゾーン ペアを作成し、セキュリティ ゾーン ペア コンフィギュレーション モードを開始します。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect sunrpc-l4-pmap`	ファイアウォール ポリシー マップをゾーン ペアに付加します。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 2/0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] 例： `Device(config-if)# ip address 192.168.6.5 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 12	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security z-client`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 13	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 14	**interface** *type number* 例： `Device(config)# interface gigabitethernet 2/1/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 15	**ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] 例： `Device(config-if)# ip address 192.168.6.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 16	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security z-server`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 17	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの設定例

例：ファイアウォール ポリシー対応のレイヤ 4 クラス マップの設定

```
Device# configure terminal
Device(config)# class-map type inspect match-any sunrpc-l4-cmap
Device(config-cmap)# match protocol sunrpc
Device(config-cmap)# end
```

例：ファイアウォール ポリシー対応のレイヤ 7 クラス マップの設定

```
Device# configure terminal
Device(config)# class-map type inspect sunrpc match-any sunrpc-l7-cmap
Device(config-cmap)# match program-number 100005
Device(config-cmap)# end
```

例：Sun RPC ファイアウォール ポリシー マップの設定

```
Device# configure terminal
Device(config)# policy-map type inspect sunrpc sunrpc-l7-pmap
Device(config-pmap)# class type inspect sunrpc sunrpc-l7-cmap
Device(config-pmap-c)# allow
Device(config-pmap-c)# end
```

例：レイヤ 4 ポリシー マップへのレイヤ 7 ポリシー マップの付加

```
Device# configure terminal
Device(config)# policy-map type inspect sunrpcl4-pmap
Device(config-pmap)# class sunrpcl4-cmap
Device(config-pmap-c)# inspect
Device(config-pmap-c)# service-policy sunrpc sunrpc-l7-pmap
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# drop
Device(config-pmap-c)# end
```

例：セキュリティ ゾーンとゾーン ペアの作成、およびゾーン ペアへのポリシー マップの付加

```
Device# configure terminal
Device(config)# zone security z-client
Device(config-sec-zone)# exit
Device(config)# zone security z-server
Device(config-sec-zone)# exit
Device(config)# zone-pair security clt2srv source z-client destination z-server
Device(config-sec-zone-pair)# service-policy type inspect sunrpc-l4-pmap
```

```
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 2/0/0
Device(config-if)# ip address 192.168.6.5 255.255.255.0
Device(config-if)# zone-member security z-client
Device(config-if)# exit
Device(config)# interface gigabitethernet 2/1/1
Device(config-if)# ip address 192.168.6.1 255.255.255.0
Device(config-if)# zone-member security z-server
Device(config-if)# end
```

例：Sun RPC ALG 対応のファイアウォールの設定

次に、Sun リモートプロシージャ コール（RPC）アプリケーション レベル ゲートウェイ（ALG）サポートのファイアウォール設定の例を示します。

```
class-map type inspect sunrpc match-any sunrpc-l7-cmap
 match program-number 100005
!
class-map type inspect match-any sunrpc-l4-cmap
 match protocol sunrpc
!
!
policy-map type inspect sunrpc sunrpc-l7-pmap
 class type inspect sunrpc sunrpc-l7-cmap
  allow
!
!
policy-map type inspect sunrpc-l4-pmap
 class type inspect sunrpc-l4-cmap
  inspect
  service-policy sunrpc sunrpc-l7-pmap
!
 class class-default
  drop
!
!
zone security z-client
!
zone security z-server
!
zone-pair security clt2srv source z-client destination z-server
 service-policy type inspect sunrpc-l4-pmap
!
interface GigabitEthernet 2/0/0
 ip address 192.168.10.1 255.255.255.0
 zone-member security z-client
!
interface GigabitEthernet 2/1/1
 ip address 192.168.23.1 255.255.255.0
 zone-member security z-server
!
```

ファイアウォールおよび NAT 対応の Sun RPC ALG サポートに関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
IP アドレッシング コマンド	『IP Addressing Services Command Reference』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

標準および RFC

標準/RFC	タイトル
RFC 1057	『*RPC: Remote Procedure Call Protocol Specification Version 2*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの機能情報

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

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

表 *21*：ファイアウォールおよび *NAT* 対応の *Sun RPC ALG* サポートの機能情報

機能名	リリース	機能情報
ファイアウォールおよび NAT 対応の Sun RPC ALG サポート	Cisco IOS XE Release 3.2S	ファイアウォールおよび NAT 対応の Sun RPC ALG サポート機能は、ファイアウォールおよび NAT における Sun RPC ALG のサポートを追加します。 **match protocol** コマンドが導入または変更されました。

第 16 章

ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP

ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP 機能は、単一の H.323 メッセージではない TCP セグメントをサポートするよう H.323 アプリケーション レベル ゲートウェイ（ALG）を拡張します。 仮想 TCP（vTCP）は TCP セグメントの再構成をサポートします。 この機能の導入前は、H.323 ALG では、完全な H.323 メッセージである TCP セグメントのみを処理していました。 TCP セグメントが複数のメッセージである場合、H.323 ALG では TCP セグメントを無視し、パケットは処理されずに渡されていました。

このモジュールでは、ファイアウォールに対するハイ アベイラビリティ（HA）サポートを備えた ALG - H.323 vTCP の設定方法について説明します。

- 機能情報の確認，298 ページ
- ファイアウォールおよびNAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の制約事項，298 ページ
- ファイアウォールおよびNAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP について，298 ページ
- ファイアウォールおよびNAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の設定方法，301 ページ
- ファイアウォールおよびNAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の設定例，304 ページ
- ファイアウォールおよびNAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP に関するその他の関連資料，304 ページ
- ファイアウォールおよびNAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の機能情報，305 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

ファイアウォールおよびNATに対するハイ アベイラビリティ サポートを備えたALG - H.323 vTCP の制約事項

- 着信 TCP セグメントが完全な H.323 メッセージではない場合、H.323 ALG ではメッセージの残りを待機中に TCP セグメントをバッファします。 バッファされたデータは、ハイ アベイラビリティ（HA）を得るためにスタンバイ デバイスに同期されません。
- vTCP によるデータのバッファ開始時に、H.323 ALG のパフォーマンスが影響を受ける可能性があります。

ファイアウォールおよびNATに対するハイ アベイラビリティ サポートを備えたALG - H.323 vTCP について

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション層ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内のIPアドレス情報を変換するアプリケーションです。 ALG はアプリケーション層プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。 これらのアクションは、ファイアウォールおよび NAT の設定に応じた次の 1 つ以上のアクションです。

- ダイナミック TCP または UDP ポートを使用したサーバ アプリケーションとの通信をクライアント アプリケーションに許可します。
- アプリケーション固有のコマンドを認識し、それらのコマンドに対するきめ細かなセキュリティ制御を提供します。

- データ交換を行う 2 台のホスト間のデータの複数のストリームまたはセッションを同期します。
- アプリケーション ペイロードで使用可能なネットワーク層アドレス情報を変換します。

ファイアウォールがピンホールを開き、NATは、アプリケーション層データ ストリームで送信元および宛先 IP アドレスを伝送しない TCP または UDP トラフィックで変換サービスを実行します。 IPアドレス情報を埋め込む特定のプロトコルまたはアプリケーションには、ALGのサポートが必要です。

基本 H.323 ALG サポート

H.323 は、パケット ベース ネットワーク経由のマルチメディア送信用に一連のネットワーク要素およびプロトコルを定義する ITU-T が公開している推奨事項です。 H.323 は、マルチメディアの送信で使用されるネットワーク要素数を定義します。

現在、ほとんどの H.323 実装ではシグナリング用の転送メカニズムとして TCP を利用していますが、H.323 バージョン 2 では基本 UDP トランスポートがイネーブルにされます。

- H.323端末：この要素は、別のH.323端末またはゲートウェイとの双方向通信を提供するネットワークのエンドポイントです。
- H.323 ゲートウェイ：この要素は、H.323端末とH.323をサポートしない他の端末との間のプロトコル変換を提供します。
- H.323 ゲートキーパー：この要素は、アドレス変換、ネットワーク アクセス コントロール、帯域幅管理といったサービスを提供し、H.323 端末およびゲートウェイで構成されます。

次のコア プロトコルが、H.323 仕様で規定されています。

- H.225：このプロトコルは、任意の2つのH.323エンティティ間で、通信を確立するために使用されるコール シグナリング方法について規定しています。
- H.225 登録、アドミッション、およびステータス（RAS）：このプロトコルは、アドレス解決およびアドミッション制御サービス用に、H.323 エンドポイントとゲートウェイによって使用されます。
- H.245：このプロトコルは、マルチメディア通信機能の交換、およびオーディオ、ビデオ、およびデータ用の論理チャネルの開閉のために使用されます。

示されているプロトコルに加え、H.323 仕様では、リアルタイム トランスポート（RTP）プロトコルや、オーディオ（G.711、G.729など）およびビデオ（H.261、H.263、およびH.264）コーデックなどのさまざまなIETFプロトコルの使用についても規定しています。

NAT では、パケット ペイロード内の埋め込み IP アドレスおよびポート番号の変換や、制御チャネルからの新規接続/セッション情報の取得といった、レイヤ 7 プロトコル固有のサービスを処理するために、さまざまなALGを必要とします。 H.323 ALG は、H.323 メッセージに対し、これら特定のサービスを実行します。

vTCP for ALG サポートの概要

レイヤ 7 プロトコルは TCP を使用してデータ転送を行い、TCP ペイロードはアプリケーション設計、最大セグメント サイズ（MSS）、TCP ウィンドウ サイズなどのさまざまな理由によりセグメント化が可能です。 ファイアウォールおよび NAT でサポートされる ALG には、パケット インスペクションのために TCP フラグメントを認識する機能がありません。 vTCP は、TCP セグメントを理解し、TCP ペイロードを解析するために ALG で使用される汎用フレームワークです。

vTCP は、TCP ペイロード全体で埋め込みデータを書き直す必要がある NAT およびセッション開始プロトコル（SIP）などのアプリケーションで役立ちます。 ファイアウォールでは、vTCP を使用して ALG がパケット間のデータ分割をサポートできるようにします。

ファイアウォールおよび NAT ALG を設定すると、vTCP 機能がアクティブ化されます。

TCP 確認応答と確実な送信

vTCP は 2 つの TCP ホスト間に存在するため、TCP セグメントを他のホストに送信するまで一時的に保存するためのバッファ スペースが必要です。 vTCP は、データ伝送がホスト間で適切に行われるようにします。 vTCP では、データ伝送用にさらに多くのデータが必要な場合、送信ホストに TCP 確認応答（ACK）を送信します。 vTCP ではまた、受信ホストにより送信される ACK を TCP フローの始めから追跡し、確認応答データを注意深くモニタします。

vTCP は、TCP セグメントを再構成します。 着信セグメントの IP ヘッダーおよび TCP ヘッダー情報は、確実な送信のために vTCP バッファに保存されます。

vTCP では、NAT 対応アプリケーションの発信セグメントの長さを細かく変更できます。 vTCP は最後のセグメントのデータ長を長くするか、新しいセグメントを作成して、追加のデータを伝送することができます。 新しく作成されたセグメントの IP ヘッダーまたは TCP ヘッダー コンテンツは、オリジナルの着信セグメントから派生したものです。 IP ヘッダーの合計の長さと TCP ヘッダーのシーケンス番号は、必要に応じて調整されます。

vTCP と NAT およびファイアウォール ALG

ALG は、NAT およびファイアウォールのサブコンポーネントです。 NAT とファイアウォールのいずれにも、ダイナミックに ALG を連結させるためのフレームワークがあります。 ファイアウォールがレイヤ 7 インスペクションを実行するか、NAT がレイヤ 7 フィックスアップを実行すると、ALG により登録されたパーサー機能が呼び出され、ALG がパケット インスペクションを引き継ぎます。 vTCP は、NAT およびファイアウォールと、これらのアプリケーションを使用する ALG との間を仲介します。 言い換えると、パケットはまず vTCP によって処理されてから、ALG に渡されます。 vTCP は、TCP 接続内で両方向の TCP セグメントを再構成します。

ハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の概要

ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP 機能は、単一の H.323 メッセージではない TCP セグメントをサポートするよう H.323 アプリケー

ション レベル ゲートウェイ（ALG）を拡張します。 H.323 ALG が vTCP と組み合わせられると、ファイアウォールおよび NAT は vTCP を介して H.323 ALG と対話します。 vTCP がデータのバッファを開始すると、ハイ アベイラビリティ（HA）機能が影響を受けます。これは、vTCP ではバッファされたデータをスタンバイ デバイスに同期できないためです。vTCP によるデータのバッファ中にスタンバイ デバイスへのスイッチオーバーが発生した場合、バッファされたデータがスタンバイ デバイスに同期されていないと、接続がリセットされることがあります。バッファされたデータが vTCP により確認されると、それらのデータは失われ、接続がリセットされます。ファイアウォールおよび NAT は HA のためにデータを同期します。 vTCP はスタンバイ デバイスへの現在の接続状態のみを同期し、エラーが発生すると、接続がリセットされます。

ファイアウォールおよびNATに対するハイ アベイラビリティ サポートを備えたALG - H.323 vTCP の設定方法

NATに対するハイ アベイラビリティ サポートを備えたALG - H.323 vTCP の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip nat inside**
5. **exit**
6. **interface** *type number*
7. **ip nat outside**
8. **exit**
9. **ip nat pool** *pool-name start-ip end-ip* **prefix-length** *prefix-length*
10. **ip nat inside source list pool** *pool-name*
11. **access-list** *access-list-number* **permit** *source* [*source-wildcard*]
12. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip nat inside** 例： `Device(config-if)# ip nat inside`	インターフェイスが内部ネットワーク（NAT 変換の対象となるネットワーク）に接続されることを示します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 6	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip nat outside** 例： `Device(config-if)# ip nat outside`	インターフェイスが外部ネットワークに接続されることを示します。
ステップ 8	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 9	**ip nat pool** *pool-name start-ip end-ip* **prefix-length** *prefix-length* 例： `Device(config)# ip nat pool pool1 10.1.1.10 10.1.1.100 prefix-length 24`	NAT で使用される IP アドレス プールを定義します。
ステップ 10	**ip nat inside source list pool** *pool-name* 例： `Device(config)# ip nat inside source list pool pool1`	内部送信元アドレスの NAT をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 11	**access-list** *access-list-number* **permit** *source* [*source-wildcard*] 例： `Device(config)# access-list 1 permit 10.0.0.0 255.255.255.0`	標準 IP アクセス リストを定義し、条件に合致している場合にパケットへのアクセスを許可します。
ステップ 12	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

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

```
Device# show ip nat statistics

Total active translations: 2 (0 static, 2 dynamic; 1 extended)
Outside interfaces:
  GigabitEthernet0/0/1
Inside interfaces:
  GigabitEthernet0/1/1
Hits: 0  Misses: 25
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool pool1 refcount 2
 pool pool1: netmask 255.255.255.0
        start 10.1.1.10 end 10.1.1.100
        type generic, total addresses 91, allocated 1 (1%), misses 0
nat-limit statistics:
 max entry: max allowed 0, used 0, missed 0
Pool stats drop: 0  Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0
```

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

```
Device# show ip nat translations

Pro  Inside global         Inside local          Outside local         Outside global
---  10.1.1.10             10.2.1.2              ---                   ---
udp  10.1.1.10:75          10.2.1.2:75           10.1.1.1:69           10.1.1.1:69
Total number of translations: 2
```

ファイアウォールおよびNATに対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の設定例

例：NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の設定

```
Device# configure terminal
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# ip nat inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# ip nat outside
Device(config-if)# exit
Device(config)# ip nat pool pool1 10.1.1.10 10.1.1.100 prefix-length 24
Device(config)# ip nat inside source list pool pool1
Device(config)# access-list 1 permit 10.0.0.0 255.255.255.0
Device(config)# end
```

ファイアウォールおよびNATに対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Commands List, All Releases』
ファイアウォール コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
NAT コマンド	『IP Addressing Services Command Reference』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォールおよびNATに対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の機能情報

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

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

表 *22*：ファイアウォールおよび *NAT* に対するハイ アベイラビリティ サポートを備えた *ALG - H.323 vTCP* の機能情報

機能名	リリース	機能情報
ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP	Cisco IOS XE Release 3.7S	ファイアウォールおよびNAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP 機能は、単一の H.323 メッセージではない TCP セグメントをサポートするよう H.323 ALG を拡張します。 vTCP は、セグメントの再構成をサポートします。 この機能の導入前は、H.323 ALG では、完全な H.323 メッセージである TCP セグメントのみを処理していました。 TCP セグメントが複数のメッセージである場合、H.323 ALG では TCP セグメントを無視し、パケットは処理されずに渡されていました。

ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の機能情報

第 17 章

NAT およびファイアウォールに対する SIP ALG 強化

NAT およびファイアウォールに対する SIP ALG 強化機能は、既存のネットワーク アドレス変換（NAT）およびファイアウォール対応のセッション開始プロトコル（SIP）アプリケーション レベル ゲートウェイ（ALG）サポートよりも優れたメモリ管理および RFC 準拠を提供します。 この機能では、次の拡張機能が提供されます。

- すべての SIP レイヤ 7 データのローカル データベースの管理
- Via ヘッダーの処理
- 追加の SIP メソッドのロギングのサポート
- Provisional Response Acknowledgment（PRACK）コール フローのサポート
- Record-Route ヘッダーのサポート

上記の拡張機能はデフォルトで使用可能です。NAT またはファイアウォールでの追加の設定は必要ありません。

このモジュールでは、SIP ALG 拡張機能について説明し、SIP の NAT およびファイアウォール サポートをイネーブルにする方法について説明します。

- 機能情報の確認，308 ページ
- NAT およびファイアウォールに対する SIP ALG 強化の制約事項，308 ページ
- NAT およびファイアウォールに対する SIP ALG 強化について，308 ページ
- NAT およびファイアウォールに対する SIP ALG 強化の設定方法，312 ページ
- NAT およびファイアウォールに対する SIP ALG 強化の設定例，317 ページ
- NAT およびファイアウォールに対する SIP ALG 強化に関するその他の関連資料，318 ページ
- NAT およびファイアウォールに対する SIP ALG 強化の機能情報，319 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

NAT およびファイアウォールに対する SIP ALG 強化の制約事項

- セッション開始プロトコル（SIP）アプリケーション レベル ゲートウェイ（ALG）では、セキュリティ機能は提供されません。
- SIP ALG は、コール ID に基づいてローカル データベースを管理します。 同じコール ID を持つ 2 つの異なるクライアントから 2 つのコールを受信したために、コール ID の重複が発生する場合がまれにあります。

NAT およびファイアウォールに対する SIP ALG 強化について

SIP の概要

セッション開始プロトコル（SIP）は、1 人または複数の参加者とのセッションを作成、変更、および終了するためのアプリケーション層コントロール（シグナリング）プロトコルです。 SIPセッションには、インターネット電話の通話、マルチメディアの配布、マルチメディア会議などがあります。 SIP は HTTP のような要求/応答トランザクション モデルに基づいています。 各トランザクションは、サーバで特定のメソッドまたは関数を呼び出す 1 つの要求と 1 つ以上の応答で構成されます。

セッションの作成に使用される SIP の招待は、互換性のあるメディア タイプのセットに参加者が同意できるセッション記述を伝送しています。 SIP は、プロキシ サーバと呼ばれる要素を利用して、ユーザの所在地への要求のルーティング、サービスのためのユーザ認証および許可、プロバイダーのコールルーティング ポリシーの実装、およびユーザへの機能提供を行っています。 また、SIP には、プロキシ サーバから使用できるように、ユーザの所在地をアップロードできる登録機能があります。 SIP は複数のトランスポート プロトコルを基礎として実行されます。

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション層ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内のIPアドレス情報を変換するアプリケーションです。 ALG はアプリケーション層プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。 これらのアクションは、ファイアウォールおよび NAT の設定に応じた次の 1 つ以上のアクションです。

- ダイナミック TCP または UDP ポートを使用したサーバ アプリケーションとの通信をクライアント アプリケーションに許可します。
- アプリケーション固有のコマンドを認識し、それらのコマンドに対するきめ細かなセキュリティ制御を提供します。
- データ交換を行う 2 台のホスト間のデータの複数のストリームまたはセッションを同期します。
- アプリケーション ペイロードで使用可能なネットワーク層アドレス情報を変換します。

ファイアウォールがピンホールを開き、NATは、アプリケーション層データ ストリームで送信元および宛先 IP アドレスを伝送しない TCP または UDP トラフィックで変換サービスを実行します。 IPアドレス情報を埋め込む特定のプロトコルまたはアプリケーションには、ALGのサポートが必要です。

SIP ALG ローカル データベース管理

セッション開始プロトコル（SIP）トランクは、SIP を使用した IP ネットワーク経由での IP PBX からサービス プロバイダーへの直接接続です。 SIP トランクには、多数の同時発生コールが存在できます。 コール セットアップ プロセス中、すべてのコールは、コールの確立に同じ制御チャネルを使用します。 複数のコールが、コール セットアップに同じ制御チャネルを使用します。 同じ制御チャネルが複数のコールで使用される場合、制御チャネル セッションに保存されているステートフル情報の信頼性が失われます。 SIP ステートフル情報は、メディア データを送信するためにクライアントおよびサーバのエンドポイントで使用されるIPアドレスやポート番号などのメディア チャネル情報で構成されます。メディア チャネル情報は、ファイアウォールおよびNATで、D チャネル用のファイアウォール ピンホールおよびネットワーク アドレス変換（NAT）ドアをそれぞれ作成するために使用されます。 複数のコールがコールセットアップに同じ制御チャネルを使用するため、メディア データのセットが複数存在します。

SIP トランクでは、複数のコールが同じファイアウォールおよび NAT セッションを共有します。 NAT およびファイアウォールでは、SIP パケットの 5 タプル（送信元アドレス、宛先アドレス、送信元ポート、宛先ポート、およびプロトコル）を使用して、SIPセッションを識別および管理します。 5タプルを使用してコールを識別および照合する従来の方法では、SIPトランキングが完全にはサポートされません。そのため、多くの場合、レイヤ 7 データのメモリ リークやコールの照合の問題が発生します。

他のアプリケーション レベル ゲートウェイ（ALG）とは対照的に、SIP ALG では、通常の SIP コールおよび SIP トランクに埋め込まれている SIP コールに含まれるすべてのメディア関連情報

を保存するために、ローカルデータベースを使用してSIP レイヤ7データを管理します。 SIP ALG では、SIP メッセージに含まれる Call-ID ヘッダー フィールドを使用して、コールの照合のためにローカル データベースを検索したり、コールを管理および終了したりします。 Call-ID ヘッダー フィールドは、同じ SIP ダイアログに属するメッセージを識別するダイアログ ID です。

SIP ALG では、コール ID を使用して、ローカル データベースでの検索およびメモリ リソースの管理を行います。 SIP ALG がレイヤ 7 データ レコードをデータベースから解放できない特定のシナリオでは、データベース内にコール レコードが残っていないことを確認するために、セッション タイマーを使用してリソースが管理および解放されます。

（注） すべてのレイヤ7データはローカルデータベースを使用してSIP ALGにより管理されるため、SIP ALG が SIP レイヤ 7 データを解放するためにファイアウォールおよび NAT で応答することはありません。SIP ALG 自身がデータを解放します。 すべての NAT 変換およびファイアウォール セッションをクリアするために **clear** コマンドを使用する場合、ローカル データベース内の SIP レイヤ 7 データは解放されません。

SIP ALG Via ヘッダーのサポート

セッション開始プロトコル（SIP）INVITE 要求には、Via ヘッダー フィールドが含まれます。 Via ヘッダー フィールドは、SIP 要求が通過するトランスポート パスを示します。 Via ヘッダーには、後続の SIP 応答のリターン パスに関する情報も含まれています。これには、応答メッセージが送信される IP アドレスとポートが含まれます。

SIP ALG では、受信した各 SIP 要求の Via ヘッダー フィールドの最初の値に基づいて、ファイアウォール ピンホールまたはネットワーク アドレス変換（NAT）ドアを作成します。ただし、確認応答（ACK）メッセージは除きます。 ポート番号情報が最初の Via ヘッダーに含まれていない場合、ポート番号は 5060 と想定されます。

SIP ALG 方式のロギング サポート

NAT およびファイアウォールに対する SIP ALG 強化機能では、セッション開始プロトコル（SIP）アプリケーション レベル ゲートウェイ（ALG）統計で、次の方式の詳細ロギングをサポートします。

- PUBLISH
- OPTIONS
- 1XX（100、180、183 を除く）
- 2XX（200 を除く）

SIP ALG 統計に記録される既存の SIP 方式には、ACK、BYE、CANCEL、INFO、INVITE、MESSAGE、NOTIFY、REFER、REGISTER、SUBSCRIBE、および 1XX-6XX があります。

SIP ALG PRACK コール フロー サポート

セッション開始プロトコル（SIP）では、最終応答と暫定応答の 2 種類の応答が定義されています。最終応答では要求の処理結果が伝達され、信頼性の高い方法で送信されます。一方、暫定応答では要求処理の進行状況に関する情報が伝えられ、信頼性の高い方法では送信されません。

Provisional Response Acknowledgement（PRACK）は、暫定応答用の確認応答（ACK）システムを提供する SIP 方式です。 PRACK を使用すると、SIP エンドポイント間の SIP の暫定応答を確実に交換できます。 SIP の信頼性の高い暫定応答は、メディア情報が交換され、リソース予約がコールの接続前に実行できるようにします。

SIP は、接続ネゴシエーション中に、セッション記述プロトコル（SDP）の接続、メディア、および属性のフィールドを使用します。 SIP アプリケーション レベル ゲートウェイ（ALG）は、PRACK メッセージ内の SDP 情報をサポートします。 メディア情報が PRACK メッセージ内に存在する場合、SIP ALG はメディア情報を取得して処理します。 また、SIP ALG は後続のメディア ストリームでのメディア チャネルの作成を行います。 SIP ALG では、PRACK メッセージ内の SDP 情報に基づいて、ファイアウォール ピンホールおよび NAT ドアを作成します。

SIP ALG Record-Route ヘッダー サポート

Record-Route ヘッダー フィールドは、セッション開始プロトコル（SIP）プロキシによって SIP 要求に追加され、SIP ダイアログにおける将来の要求がプロキシ経由でルーティングされるよう強制します。 これにより、ダイアログ内で送信されるメッセージはすべての SIP プロキシを経由し、SIP 要求に Record-Route ヘッダー フィールドが追加されます。 Record-Route ヘッダー フィールドには、プロキシを識別する、グローバルに到達可能な Uniform Resource Identifier（URI）が含まれます。

SIP アプリケーション レベル ゲートウェイ（ALG）は Contact ヘッダーを解析し、Contact ヘッダー内の IP アドレスおよびポート値を使用して、ファイアウォール ピンホールおよびネットワーク アドレス変換（NAT）ドアを作成します。 さらに、SIP ALG では、プロキシ経由でルーティングされる将来のメッセージ用にファイアウォール ピンホールおよび NAT ドアを作成するための Record-Route ヘッダーの解析をサポートします。

Record-Route ヘッダーを解析することにより、SIP ALG では次のシナリオをサポートします。

- Cisco ASR 1000 アグリゲーション サービス ルータが、2 つのプロキシ間に配置されます。
- Cisco ASR 1000 アグリゲーション サービス ルータが、ユーザ エージェント クライアント（UAC）とプロキシの間に配置されます。
- Cisco ASR 1000 アグリゲーション サービス ルータが、プロキシとユーザ エージェント サーバ（UAS）の間に配置されます。
- クライアントとサーバの間にプロキシが存在しません。 このシナリオではレコードのルーティングは行われません。

NAT およびファイアウォールに対する SIP ALG 強化の設定方法

SIP に対する NAT サポートのイネーブル化

SIP に対する NAT サポートは、デフォルトでポート 5060 でイネーブルになります。 この機能がディセーブルの場合、SIP に対する NAT のサポートを再びイネーブルにするには、この作業を実行します。 SIP に対する NAT サポートをディセーブルにするには、**no ip nat service sip** コマンドを使用してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat service sip** {**tcp** | **udp**} **port** *port-number*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat service sip** {**tcp**	**udp**} **port** *port-number* 例： `Device(config)# ip nat service sip tcp port 5060`	SIP に対する NAT サポートをイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SIP インスペクションのイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **exit**
10. **class class-default**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any sip-class1`	検査タイプ クラス マップを作成し、クラス 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	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol sip`	指定したプロトコルに基づいてクラス マップの一致基準を設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(config-cmap)# exit`	クラスマップ コンフィギュレーション モードを終了します。
ステップ 6	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect sip-policy`	検査タイプ ポリシー マップを作成し、ポリシー 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 7	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect sip-class1`	アクションを実行するクラスを指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 9	**exit** 例： `Device(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシーマップ コンフィギュレーションモードに戻ります。
ステップ 10	**class class-default** 例： `Device(config-pmap)# class class-default`	これらのポリシー マップ設定が事前に定義したデフォルト クラスに適用されることを指定します。 • 設定済みクラスマップの一致基準のいずれともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。
ステップ 11	**end** 例： `Device(config-pmap)# end`	ポリシー マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ゾーン ペアの設定および SIP ポリシー マップの付加

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** {*zone-name* | **default**}
4. **exit**
5. **zone security** {*zone-name* | **default**}
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *zone-name*
12. **exit**
13. **interface** *type number*
14. **zone-member security** *zone-name*
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** {*zone-name*	**default**} 例： `Device(config)# zone security zone1`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**zone security** {*zone-name* | **default**} 例： `Device(config)# zone security zone2`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]] 例： `Device(config)# zone-pair security in-out source zone1 destination zone2`	ゾーン ペアを作成し、セキュリティ ゾーン ペア コンフィギュレーション モードに戻ります。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect sip-policy`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security zone1`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。

	コマンドまたはアクション	目的
		（注） インターフェイスをセキュリティゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（デバイス宛のトラフィックまたはデバイス発信のトラフィックを除く）は、デフォルトでドロップされます。 トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。 ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 13	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security zone2`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。
ステップ 15	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

NAT およびファイアウォールに対する SIP ALG 強化の設定例

例：SIP に対する NAT サポートのイネーブル化

```
Device> enable
Device# configure terminal
Device(config)# ip nat service sip tcp port 5060
Device(config)# end
```

例：SIP インスペクションのイネーブル化

```
class-map type inspect match-any sip-class1
 match protocol sip
!
policy-map type inspect sip-policy
 class type inspect sip-class1
  inspect
!
class class-default
```

例：ゾーン ペアの設定および SIP ポリシー マップの付加

```
zone security zone1
!
zone security zone2
!
zone-pair security in-out source zone1 destination zone2
 service-policy type inspect sip-policy
!
interface gigabitethernet 0/0/0
 zone security zone1
!
interface gigabitethernet 0/1/1
 zone security zone2
```

NAT およびファイアウォールに対する SIP ALG 強化に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
NAT 設定	『*IP Addressing: NAT Configuration Guide*』
ファイアウォールの設定	『*Security Configuration Guide: Zone-Based Policy Firewall*』
NAT コマンド	『Cisco IOS IP Addressing Services Command Reference』
ファイアウォール コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

関連項目	マニュアル タイトル
NAT およびファイアウォール ALG サポート	『NAT and Firewall ALG and AIC Support on Cisco ASR 1000 Series Aggregation Services Routers』マトリクス

標準および RFC

標準/RFC	タイトル
RFC 3261	『*SIP: Session Initiation Protocol*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NAT およびファイアウォールに対する SIP ALG 強化の機能情報

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

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

表 *23*：*NAT* およびファイアウォールに対する *SIP ALG* 強化の機能情報

機能名	リリース	機能情報
NAT およびファイアウォールに対する SIP ALG 強化	Cisco IOS XE Release 3.8S	NAT およびファイアウォールに対する SIP ALG 強化機能では、既存の NAT およびファイアウォールに対する SIP ALG サポートよりも優れたメモリ管理および RFC 準拠を提供します。

第 18 章

NAT の Match-in-VRF サポート

NAT の Match-in-VRF サポート機能では、同じ VPN ルーティングおよび転送（VRF）インスタンス内の 2 つのホスト間で通信するパケットのネットワーク アドレス変換（NAT）をサポートしています。 VPN 内 NAT では、エンド ホストのローカルおよびグローバル アドレス空間の両方がそれぞれの VPN に隔離されるため、ホストの変換後のアドレスが互いにオーバーラップします。 NAT の Match-in-VRF サポート機能では、VPN 間での変換後のアドレスのアドレス空間の分離をサポートします。

- 機能情報の確認，321 ページ
- NAT の Match-in-VRF サポートの制約事項，322 ページ
- NAT の Match-in-VRF サポートについて，322 ページ
- NAT の Match-in-VRF サポートの設定方法，323 ページ
- NAT の Match-in-VRF サポートの設定例，327 ページ
- その他の関連資料，328 ページ
- NAT の Match-in-VRF サポートに関する機能情報，330 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

NAT の Match-in-VRF サポートの制約事項

NAT の Match-in-VRF サポート機能は、インターフェイス オーバーロード設定ではサポートされません。

NAT の Match-in-VRF サポートについて

NAT の Match-in-VRF サポート

Cisco IOS XE Release 3.5S 以降のリリースでは、NAT の Match-in-VRF サポート機能は、同じ VPN 内の 2 つのホスト間で通信するパケットの NAT をサポートします。

VRF 対応 NAT では、異なる VPN ルーティングおよび転送（VRF）インスタンス内のプライベートアドレス空間のホスト、およびインターネットまたはグローバル ドメイン内の共通サーバ間の通信をイネーブルにします。 内部ホストの IP アドレスは互いにオーバーラップするため、VRF 対応 NAT では、オーバーラップしている内部 IP アドレスをグローバルに一意なアドレスに変換することによって、これらのホスト間の通信を容易にします。 NAT の Match-in-VRF サポート機能では、VPN 内 NAT 機能をサポートすることにより、VRF 対応 NAT を拡張します。 VPN 内 NAT では、エンド ホストのローカルおよびグローバル アドレス空間の両方がそれぞれの VPN に隔離されるため、ホストの変換後のアドレスが互いにオーバーラップします。 変換後のアドレスのアドレス空間を VPN 間で分離するには、**match-in-vrf** キーワードを NAT マッピング（**ip nat inside source** コマンド）設定に設定します。 スタティックおよびダイナミック NAT 設定の両方で、**match-in-vrf** キーワードがサポートされます。

（注） VRF をサポートするすべての NAT コマンドで **match-in-vrf** キーワードがサポートされます。NAT 外部ルール（**ip nat outside source** コマンド）では Match-in-VRF 機能がデフォルトでサポートされるため、**match-in-vrf** キーワードは NAT 外部ルールではサポートされません。

VRF 対応 NAT では、内部グローバル アドレスの IP エイリアスとアドレス解決プロトコル（ARP）エントリは、グローバル ドメインで設定されます。 VPN 内 NAT では、内部グローバル アドレスの IP エイリアスおよび ARP エントリは、変換が実行される VRF で設定されます。 VPN 内 NAT では、**match-in-vrf** キーワードの設定は、1 つ以上の NAT 外部インターフェイスが同じ VRF で設定されることを意味します。 その VRF 内の ARP エントリは、外部ホストからの ARP 要求に応答します。

内部アドレスが設定されている場合、Match-in-VRF は VRF トラフィックのアドレス変換中に内部マッピングにより決定されます。 アドレス変換に IP アドレスの外部マッピングのみを設定している場合は、Match-in-VRF が機能します。 変換エントリが内部および外部両方のマッピングにより作成されている場合、**match-in-vrf** キーワードは内部マッピングにより決定されます。

NAT の Match-in-VRF サポート機能では、同じ IP アドレス プールを使用する複数のダイナミック マッピング設定をサポートしています。

NAT の Match-in-VRF サポートの設定方法

スタティック NAT での Match-in-VRF の設定

スタティック NAT 変換を設定し、同じ VRF 内で NAT 内部および外部トラフィックをイネーブルにするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat inside source static** *local-ip global-ip* [**vrf** *vrf-name* [**match-in-vrf**]]
4. **interface** *type number*
5. **ip address** *ip-address mask* [**secondary**]
6. **ip nat inside**
7. **ip vrf forwarding** *vrf-name*
8. **exit**
9. **interface** *type number*
10. **ip address** *ip-address mask*
11. **ip nat outside**
12. **ip vrf forwarding** *vrf-name*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat inside source static** *local-ip global-ip* [**vrf** *vrf-name* [**match-in-vrf**]] 例： `Router(config)# ip nat inside source static 10.10.10.1 172.16.131.1 vrf vrf1 match-in-vrf`	内部ローカル アドレスと内部グローバル アドレスとの間のスタティック変換を設定します。 • **match-in-vrf** キーワードにより、同じ VRF 内の NAT 内部および外部トラフィックがイネーブルになります。

	コマンドまたはアクション	目的
ステップ 4	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip address** *ip-address mask* [**secondary**] 例： `Router(config-if)# ip address 10.114.11.39 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 6	**ip nat inside** 例： `Router(config-if)# ip nat inside`	内部と接続されることを示すマークをインターフェイスに付けます。
ステップ 7	**ip vrf forwarding** *vrf-name* 例： `Router(config-if)# ip vrf forwarding vrf1`	VRF をインターフェイスまたはサブインターフェイスと関連付けます。
ステップ 8	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/0/0`	異なるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 172.31.232.182 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 11	**ip nat outside** 例： `Router(config-if)# ip nat outside`	外部と接続されることを示すマークをインターフェイスに付けます。 （注） NAT 外部ルールは、Match-in-VRF 機能をデフォルトでサポートします。
ステップ 12	**ip vrf forwarding** *vrf-name* 例： `Router(config-if)# ip vrf forwarding vrf1`	VRF をインターフェイスまたはサブインターフェイスと関連付けます。

	コマンドまたはアクション	目的
ステップ 13	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ダイナミック NAT での Match-in-VRF の設定

ダイナミック NAT 変換に同じアドレス プールを設定し、同じ VRF 内で NAT 内部および外部トラフィックをイネーブルにするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat inside source list** *access-list-number* **pool** *pool-name* [**vrf** *vrf-name* [**match-in-vrf**]]
4. **access-list** *access-list-number* **permit source** [*source-wildcard*]
5. **ip nat inside source list** *access-list-number* **pool** *pool-name* **vrf** *vrf-name* [**match-in-vrf**]
6. **interface** *type number*
7. **ip address** *ip-address mask*
8. **ip nat inside**
9. **ip vrf forwarding** *vrf-name*
10. **exit**
11. **interface** *type number*
12. **ip address** *ip-address mask*
13. **ip nat outside**
14. **ip vrf forwarding** *vrf-name*
15. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat inside source list** *access-list-number* **pool** *pool-name* [**vrf** *vrf-name* [**match-in-vrf**]] 例： `Router(config)# ip nat inside source list 1 pool shared-pool vrf vrf1 match-in-vrf`	複数のダイナミック マッピングに同じアドレス プールを設定できるようにします。 • **match-in-vrf** キーワードにより、同じ VRF 内の NAT 内部および外部トラフィックがイネーブルになります。
ステップ 4	**access-list** *access-list-number* **permit source** [*source-wildcard*] 例： `Router(config)# access-list 1 permit 192.168.34.0 0.0.0.255`	変換されるアドレスを許可する標準アクセス リストを定義します。
ステップ 5	**ip nat inside source list** *access-list-number* **pool** *pool-name* **vrf** *vrf-name* [**match-in-vrf**] 例： `Router(config)# ip nat inside source list 1 pool shared-pool vrf vpn1`	直前の手順で定義されたアクセス リストを指定して、ダイナミック送信元変換を設定します。
ステップ 6	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 172.31.232.182 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 8	**ip nat inside** 例： `Router(config-if)# ip nat inside`	内部と接続されることを示すマークをインターフェイスに付けます。
ステップ 9	**ip vrf forwarding** *vrf-name* 例： `Router(config-if)# ip vrf forwarding vpn1`	VRF をインターフェイスまたはサブインターフェイスと関連付けます。

	コマンドまたはアクション	目的
ステップ 10	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/0/0`	異なるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 172.31.232.182 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 13	**ip nat outside** 例： `Router(config-if)# ip nat outside`	外部と接続されることを示すマークをインターフェイスに付けます。 （注） NAT 外部ルールは、Match-in-VRF 機能をデフォルトでサポートします。
ステップ 14	**ip vrf forwarding** *vrf-name* 例： `Router(config-if)# ip vrf forwarding vpn1`	VRF をインターフェイスまたはサブインターフェイスと関連付けます。
ステップ 15	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

NAT の Match-in-VRF サポートの設定例

例：スタティック NAT での Match-in-VRF の設定

次の例に、ローカル IP アドレス 10.10.10.1 とグローバル IP アドレス 172.16.131.1 の間にスタティック NAT 変換を設定する方法を示します。 **match-in-vrf** キーワードにより、同じ VRF 内の NAT 内部および外部トラフィックがイネーブルになります。

```
Router# configure terminal
Router(config)# ip nat inside source static 10.10.10.1 172.16.131.1 vrf vrf1 match-in-vrf
Router(config)# interface gigabitethernet 0/0/1
Router(config-if)# ip address 10.114.11.39 255.255.255.0
```

```
Router(config-if)# ip nat inside
Router(config-if)# ip vrf forwarding vrf1
Router(config-if)# exit
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# ip address 172.31.232.182 255.255.255.240
Router(config-if)# ip nat outside
Router(config-if)# ip vrf forwarding vrf1
Router(config-if)# end
```

例：ダイナミック NAT での Match-in-VRF の設定

次の例に、ダイナミック NAT マッピングに同じアドレス プールを設定する方法を示します。**match-in-vrf** キーワードにより、同じ VRF 内の NAT 内部および外部トラフィックがイネーブルになります。

```
Router# configure terminal
Router(config)# ip nat inside source list 1 pool shared-pool vrf vrf1 match-in-vrf
Router(config)# access-list 1 permit 192.168.34.0 0.0.0.255
Router(config)# ip nat inside source list 1 pool shared-pool vrf vpn1
Router(config)# interface gigabitethernet 0/0/1
Router(config-if)# ip address 172.31.232.182 255.255.255.240
Router(config-if)# ip nat inside
Router(config-if)# ip vrf forwarding vpn1
Router(config-if)# exit
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# ip address 172.31.232.182 255.255.255.240
Router(config-if)# ip nat outside
Router(config-if)# ip vrf forwarding vpn1
Router(config-if)# end
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
NAT コマンド：コマンド構文、コマンド モード、コマンド履歴、使用に関する注意事項および例	『*Cisco IOS IP Addressing Services Command Reference*』
IP アクセス リストへのシーケンス番号づけ	『*IP Access List Sequence Numbering*』マニュアル
NAT 設定作業	「Configuring NAT for IP Address Conservation」モジュール
NAT メンテナンス	「Monitoring and Maintaining NAT」モジュール
MPLS VPN での NAT の使用	「Integrating NAT with MPLS VPNs」モジュール

標準

標準	タイトル
なし	

MIB

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

RFC

RFC	タイトル
RFC 903	『*Reverse Address Resolution Protocol*』
RFC 826	『*Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware*』
RFC 1027	『*Using ARP to implement transparent subnet gateways*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NAT の Match-in-VRF サポートに関する機能情報

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

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

表 *24*：*NAT* の *Match-in-VRF* サポートに関する機能情報

機能名	リリース	機能情報
NAT の Match-in-VRF サポート	Cisco IOS XE Release 3.5S	NAT の Match-in-VRF サポート機能では、同じ VPN 内の 2 つのホスト間で通信するパケットの NAT 変換をサポートします。

第 19 章

IP マルチキャスト ダイナミック NAT

IP マルチキャスト ダイナミック ネットワーク アドレス変換（NAT）機能では、マルチキャスト パケットの送信元アドレス変換をサポートしています。 送信元アドレス変換は、インターネットに接続する必要があるが、すべてのホストがグローバルに一意な IP アドレスを持っているわけではない場合に使用できます。 NAT はパケットを外部ネットワークに送信する前に、内部のローカル アドレスをグローバルに一意の IP アドレスに変換します。 IP マルチキャスト ダイナミック変換では、内部ローカル アドレスと、外部グローバル アドレス プールのいずれか 1 つのアドレス間に 1 対 1 のマッピングを確立します。

- 機能情報の確認，331 ページ
- IP マルチキャスト ダイナミック NAT の制約事項，332 ページ
- IP マルチキャスト ダイナミック NAT について，332 ページ
- IP マルチキャスト ダイナミック NAT の設定方法，334 ページ
- IP マルチキャスト ダイナミックな NAT の設定例，337 ページ
- その他の関連資料，337 ページ
- IP マルチキャスト ダイナミック NAT の機能情報，338 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

IP マルチキャスト ダイナミック NAT の制約事項

IP マルチキャスト ダイナミック NAT 機能では、次の変換はサポートされません。

- IPv4-to-IPv6 アドレス変換。
- マルチキャスト宛先アドレス変換。
- マルチキャスト用のポート アドレス変換（PAT）のオーバーローディング。
- 送信元および宛先アドレス変換。
- ユニキャスト アドレスからマルチキャスト アドレスへの変換。

IP マルチキャスト ダイナミック NAT について

NAT の機能

NAT が設定されたルータには、少なくとも内部ネットワークに対して 1 つ、外部ネットワークに対して 1 つのインターフェイスがあります。 標準的な環境では、NAT はスタブ ドメインとバックボーンの間の出口ルータに設定されます。 パケットがドメインから出て行くとき、NAT はローカルで意味のある送信元アドレスをグローバルで一意のアドレスに変換します。 パケットがドメインに入ってくるときは、NAT はグローバルで一意の宛先アドレスをローカルアドレスに変換します。 出力点が複数存在する場合、個々の NAT は同一の変換テーブルを持っていなければなりません。 アドレスが足りなくなって、パケットにアドレスを割り当てられなくなった場合、NAT はそのパケットをドロップし、インターネット制御メッセージプロトコル（ICMP）ホスト到達不能パケットを宛先に送信します。

NAT の用途

NAT は次のような場合に使用できます。

- インターネットに接続する必要はあるが、ホストのすべてがグローバルに一意の IP アドレスを持っているわけではない場合。 NAT では、未登録の IP アドレスを使用するプライベート IP インターネットワークがインターネットに接続できます。 NAT はスタブ ドメイン（内部ネットワーク）と、インターネットなどのパブリック ネットワーク（外部ネットワーク）との境界にあるルータ上に設定されます。 NAT はパケットを外部ネットワークに送信する前に、内部のローカル アドレスをグローバルに一意の IP アドレスに変換します。 接続性の問題への解決策として NAT が役立つのは、スタブ ドメイン内の比較的少数のホストが同時にドメインの外部と通信する場合のみです。 この場合、外部との通信が必要なときに、このドメインにある IP アドレスのごく一部をグローバルに一意な IP アドレスに変換する必要があります。また、これらのアドレスは使用されなくなったときに、再利用することもできます。

- 内部アドレスを変更する必要がある場合。 内部アドレスの変更には相当の工数がかかるため、変更する代わりに NAT を使用して変換することができます。
- TCP トラフィックの基本負荷を分散する必要がある場合。 TCP 負荷分散機能を使用して、1 つのグローバル IP アドレスを複数のローカル IP アドレスにマップできます。

NAT の内部アドレスおよび外部アドレス

NAT のコンテキスト内で使用される内部という用語は、変換する必要がある、組織が所有するネットワークを表します。 NAT が設定されている場合、このネットワーク内のホストは 1 つの空間に複数のアドレスを持ちます（ローカル アドレス空間と呼ばれます）。これらは、ネットワーク外のホストに対して別の空間に存在するものとして示されます（グローバル アドレス空間と呼ばれます）。

同様に、外部という用語はスタブ ネットワークの接続先で、通常、その組織の制御下にはないネットワークを表します。 外部ネットワーク内のホストを変換の対象にすることもできるため、これらのホストもローカル アドレスとグローバル アドレスを持つことができます。

NAT では、次の定義が使用されます。

- 内部ローカル アドレス：内部ネットワーク上のホストに割り当てられた IP アドレス。 このアドレスは、多くの場合、NIC やサービス プロバイダーにより割り当てられた正規の IP アドレスではありません。
- 内部グローバル アドレス：外部に向けて、1 つ以上の内部ローカル IP アドレスを表現した正規の IP アドレス（NIC またはサービス プロバイダーにより割り当てられたもの）。
- 外部ローカル アドレス：内部ネットワークから見た外部ホストの IP アドレス。 必ずしも正規のアドレスではありません。内部でルート可能なアドレス空間から割り当てられたものです。
- 外部グローバル アドレス：外部ネットワークに存在するホストに対して、ホストの所有者により割り当てられた IP アドレス。 このアドレスは、グローバルにルート可能なアドレス、またはネットワーク空間から割り当てられます。

ここでは、次の内容について説明します。

アドレスのダイナミック変換

ダイナミック変換は、内部ローカル アドレスとグローバル アドレスのプールの間にマッピングを設定します。プライベート ネットワークに存在する複数のユーザがインターネットへのアクセスを必要としている場合には、ダイナミック変換が便利です。 ダイナミックに設定されたプール IP アドレスは、必要に応じて使用し、インターネットへのアクセスが必要なくなったときにはリリースして別のユーザが使用できるようにすることができます。

（注） 内部グローバル アドレスまたは外部ローカル アドレスが NAT ルータに直接接続されているサブネットに属している場合、ルータでは、アドレス解決プロトコル（ARP）要求に応答できるように、それらのアドレスの IP エイリアスを追加します。 ただし、そのルータが宛先ではないパケットにルータ自身が応答する状況が発生し、セキュリティ上の問題を引き起こす可能性があります。 これは、エイリアスが追加されたいずれかのアドレスを宛先とする着信インターネット制御メッセージ プロトコル（ICMP）または UDP パケットが、NAT テーブルに対応する NAT 変換を持っていない場合に、ルータ自身がネットワーク タイム プロトコル（NTP）などの対応するサービスを実行すると発生する可能性があります。 このような状況は、軽微なセキュリティ リスクを引き起こすことがあります。

IP マルチキャスト ダイナミック NAT の設定方法

IP マルチキャスト ダイナミック NAT の設定

（注） IP マルチキャスト ダイナミック変換では、内部ローカル アドレスと、外部グローバル アドレス プールのいずれか 1 つのアドレス間に 1 対 1 のマッピングを確立します

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} [**type** {**match-host** | **rotary**}]
4. **access-list** *access-list-number* **permit** *source-address wildcard-bits* [**any**]
5. **ip nat inside source list** *access-list-number* **pool** *name*
6. **ip multicast-routing distributed**
7. **interface** *type number*
8. **ip address** *ip-address mask*
9. **ip pim sparse-mode**
10. **ip nat inside**
11. **exit**
12. **interface** *type number*
13. **ip address** *ip-address mask*
14. **ip pim sparse-mode**
15. **ip nat outside**
16. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} [**type** {**match-host** | **rotary**}] 例： `Router(config)# ip nat pool mypool 10.41.10.1 10.41.10.23 netmask 255.255.255.0`	必要に応じて割り当てられるグローバル アドレスのプールを定義します。
ステップ 4	**access-list** *access-list-number* **permit** *source-address wildcard-bits* [**any**] 例： `Router(config)# access-list 100 permit 10.3.2.0 0.0.0.255 any`	変換する内部アドレスの標準のアクセス リストを定義します。
ステップ 5	**ip nat inside source list** *access-list-number* **pool** *name* 例： `Router(config)# ip nat inside source list 100 pool mypool`	直前の手順で定義されたアクセスリストを指定して、ダイナミック送信元変換を設定します。
ステップ 6	**ip multicast-routing distributed** 例： `Router(config)# ip multicast-routing distributed`	Multicast Distributed Switching（MDS）をイネーブルにします。
ステップ 7	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 8	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 10.1.1.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 9	**ip pim sparse-mode** 例： `Router(config-if)# ip pim sparse-mode`	インターフェイスに対する Protocol Independent Multicast（PIM）のスパース モード動作をイネーブルにします。
ステップ 10	**ip nat inside** 例： `Router(config-if)# ip nat inside`	インターフェイスが内部ネットワーク（NAT 変換の対象となるネットワーク）に接続されることを示します。
ステップ 11	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 12	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/0/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 13	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 10.2.2.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 14	**ip pim sparse-mode** 例： `Router(config-if)# ip pim sparse-mode`	インターフェイスに対する PIM のスパース モード動作をイネーブルにします。
ステップ 15	**ip nat outside** 例： `Router(config-if)# ip nat outside`	インターフェイスが外部ネットワークに接続されることを示します。
ステップ 16	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

IP マルチキャスト ダイナミックな NAT の設定例

例：IP マルチキャスト ダイナミック NAT の設定

```
Router# configure terminal
Router(config)# ip nat pool mypool 10.41.10.1 10.41.10.23 netmask 255.255.255.0
Router(config)# access-list 100 permit 10.3.2.0 0.0.0.255 any
Router(config)# ip nat inside source list 100 pool mypool
Router(config)# ip multicast-routing distributed
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# ip pim sparse-mode
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface gigabitethernet 0/0/1
Router(config-if)# ip address 10.2.2.1 255.255.255.0
Router(config-if)# ip pim sparse-mode
Router(config-if)# ip nat outside
Router(config-if)# end
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
NAT コマンド	『Cisco IOS IP Addressing Services Command Reference』
IP アドレス節約のための NAT 設定	「Configuring NAT for IP Address Conservation」モジュール

標準および RFC

標準/RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP マルチキャスト ダイナミック NAT の機能情報

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

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

表 *25* : *IP* マルチキャスト ダイナミック *NAT* の機能情報

機能名	リリース	機能情報
IP マルチキャスト ダイナミック NAT	Cisco IOS XE Release 3.4S	IP マルチキャスト ダイナミック ネットワーク アドレス変換機能では、マルチキャスト パケットの送信元アドレス変換をサポートしています。 送信元アドレス変換は、インターネットに接続する必要があるが、すべてのホストがグローバルに一意な IP アドレスを持っているわけではない場合に使用できます。 NAT はパケットを外部ネットワークに送信する前に、内部のローカル アドレスをグローバルに一意の IP アドレスに変換します。 IP マルチキャスト ダイナミック変換では、内部ローカル アドレスと、外部グローバル アドレス プールのいずれか 1 つのアドレス間に 1 対 1 のマッピングを確立します。

第 20 章

NAT での Paired-Address-Pooling サポート

ローカル IP アドレスを常に単一のグローバル IP アドレスとして表示するネットワーク アドレス変換（NAT）の機能を Paired-Address-Pooling と呼びます。 Paired-Address-Pooling は、ポート アドレス変換（PAT）でのみサポートされます。

Paired-Address-Pooling サポート機能の導入前は、PAT 設定があり、かつ新しいグローバル アドレスまたはポートが必要な場合に、IP アドレス プールで次に使用可能なアドレスが割り当てられていました。 ローカル アドレスが常に単一のグローバル アドレスにマッピングされるよう保証するメカニズムはありませんでした。 Paired-Address-Pooling サポート機能では、1 つのローカル アドレスを常に 1 つのグローバル アドレスにマッピングする機能を提供します。

このモジュールでは、NAT で Paired-Address-Pooling サポートを設定する方法について説明します。

- 機能情報の確認，341 ページ
- NAT での Paired-Address-Pooling サポートの制約事項，342 ページ
- NAT での Paired-Address-Pooling サポートについて，342 ページ
- NAT での Paired-Address-Pooling サポートの設定方法，343 ページ
- NAT での Paired-Address-Pooling サポートの設定例，345 ページ
- NAT での Paired-Address-Pooling サポートに関するその他の関連資料，346 ページ
- NAT での Paired-Address-Pooling サポートの機能情報，346 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

NAT での Paired-Address-Pooling サポートの制約事項

Paired-Address-Pooling では、次の理由により、標準のネットワーク アドレス変換（NAT）設定よりも多くのメモリが使用され、変換のスケーリングがはるかに小さくなります。

- 各ローカル アドレスを追跡する新しいデータ構造の使用。
- Paired-Address-Pooling 制限の使用。 グローバル アドレス上のユーザ数が設定された制限値に達すると、次のグローバル アドレスが Paired-Address-Pooling に使用されます。
  Paired-Address-Pooling 制限では、標準の NAT に比べて多くのメモリを使用し、アドレス プール内のより多くのグローバル アドレスを必要とします。

NAT での Paired-Address-Pooling サポートについて

Paired-Address-Pooling サポートの概要

IP アドレス プールは、IP アドレスのグループです。 IP アドレスの範囲を割り当て、その範囲に名前を付けることによって、IPアドレスプールを作成します。プール内のアドレスをユーザに割り振るか、割り当てます。

ローカル IP アドレスを常に単一のグローバル IP アドレスとして表示するネットワーク アドレス変換（NAT）の機能を Paired-Address-Pooling と呼びます。 ローカルアドレスは、ネットワークの内部に存在する任意のアドレスであり、グローバル アドレスは、ネットワークの外部に存在する任意のアドレスです。 Paired-Address-Pooling は、ポート アドレス変換（PAT）にのみ設定できます。これは、ダイナミック NAT 設定とスタティック NAT 設定は、デフォルトで、組み合わせによる設定であるためです。 PAT（オーバーロードとも呼ばれます）は、複数の異なるポートを使用して、複数の未登録 IP アドレスを単一の登録済み IP アドレスにマッピングする（多対 1）ダイナミック NAT の形式です。 Paired-Address-Pooling は、クラシック（デフォルト）およびキャリアグレード NAT（CGN）モードの両方でサポートされます。

Paired-Address-Pooling 設定では、ローカル アドレスは常に単一のグローバル アドレスとして表示されます。 たとえば、ユーザ A がグローバル アドレス G1 と組み合わされた場合、その組み合わせは、ユーザ A にアクティブなセッションがある限り存続します。 アクティブなセッションがない場合、組み合わせが削除されます。 ユーザ A に再びアクティブ セッションができた場合、ユーザ A は別のグローバル アドレスと組み合わされることがあります。

ローカルアドレスが新しいセッションを開始し、そのグローバルアドレスに対してリソース（ポート）が不十分である場合、パケットがドロップされます。 グローバルアドレス上のユーザ数が設定された制限値に達すると、次のグローバル アドレスが Paired-Address-Pooling に使用されます。 Paired-Address-Pooling によってグローバル アドレスに関連付けられているユーザがポート番号を

取得できない場合、パケットがドロップされ、NAT ドロップ コードが増分します。また、インターネット制御メッセージ プロトコル（ICMP）メッセージは送信されません。

Paired-Address-Pooling では、アドレスの選択に充てん方式を使用します。 充てん方式では、次のグローバルアドレスに進む前に、単一のグローバルアドレスに最大限可能な数のユーザを収めます（追加します）。

NAT での Paired-Address-Pooling サポートの設定方法

NAT での Paired-Address-Pooling サポートの設定

（注） ネットワーク アドレス変換（NAT）コンフィギュレーション モードを Paired-Address-Pooling コンフィギュレーション モードに変更した場合、およびその逆に変更した場合、既存の NAT セッションがすべて削除されます。

NAT の Paired-Address-Pooling モードを設定するには、**ip nat settings pap** コマンドを使用します。これを削除するには、**no ip nat settings pap** コマンドを使用します。

Paired-Address-Pooling モードを設定すると、すべてのプールとオーバーロードのマッピングが Paired-Address-Pooling 方式で動作するようになります。

NAT 設定に基づき、NAT のスタティックまたはダイナミック ルールを使用できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat settings pap** [**limit** {**1000** | **120** | **250** | **30** | **500** | **60**}]
4. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
5. **access-list** *access-list-number* **permit** *source* [*source-wildcard*]
6. **ip nat inside source list** *access-list-number* **pool** *name* **overload**
7. **interface** *type number*
8. **ip address** *ip-address mask*
9. **ip nat inside**
10. **exit**
11. **interface** *type number*
12. **ip address** *ip-address mask*
13. **ip nat outside**
14. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat settings pap** [**limit** {**1000** | **120** | **250** | **30** | **500** | **60**}] 例： `Device(config)# ip nat settings pap`	NAT の Paired-Address-Pooling コンフィギュレーション モードを設定します。 • グローバル アドレスごとに使用できるローカル アドレスの数を制限するには、**limit** キーワードを使用します。 デフォルトは 120 です。
ステップ 4	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} 例： `Device(config)# ip nat pool net-208 192.168.202.129 192.168.202.158 netmask 255.255.255.240`	必要に応じて割り当てられるグローバル アドレスのプールを定義します。
ステップ 5	**access-list** *access-list-number* **permit** *source* [*source-wildcard*] 例： `Device(config)# access-list 1 permit 192.168.34.0 0.0.0.255`	変換されるアドレスを許可する標準アクセス リストを定義します。
ステップ 6	**ip nat inside source list** *access-list-number* **pool** *name* **overload** 例： `Device(config)# ip nat inside source list 1 pool net-208 overload`	ダイナミック ポート アドレス変換（PAT）または NAT オーバーロードを設定し、ステップ 4 およびステップ 5 で定義したアクセス リストおよび IP アドレス プールを指定します。
ステップ 7	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.114.11.39 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 9	**ip nat inside** 例： `Device(config-if)# ip nat inside`	NAT の対象となる内部ネットワークにインターフェイスを接続します。
ステップ 10	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/2`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 172.16.232.182 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 13	**ip nat outside** 例： `Device(config-if)# ip nat outside`	外部ネットワークにインターフェイスを接続します。
ステップ 14	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

NAT での Paired-Address-Pooling サポートの設定例

例：NAT での Paired-Address-Pooling サポートの設定

次の例に、ネットワーク アドレス変換（NAT）ルールとともに Paired-Address-Pooling を設定する方法を示します。 この例では、アクセス リストおよびアドレス プールが指定されたダイナミック NAT 設定を示しています。 NAT 設定に基づき、スタティックまたはダイナミック NAT ルールを設定できます。

```
Device# configure terminal
Device(config)# ip nat settings pap
Device(config)# ip nat pool net-208 192.168.202.129 192.168.202.158 netmask 255.255.255.240
Device(config)# access-list 1 permit 192.168.34.0 0.0.0.255
Device(config)# ip nat inside source list 1 pool net-208 overload
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# ip address 10.114.11.39 255.255.255.0
```

```
Device(config-if)# ip nat inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/2
Device(config-if)# ip address 172.16.232.182 255.255.255.240
Device(config-if)# ip nat outside
Device(config-if)# end
```

NAT での Paired-Address-Pooling サポートに関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
NAT コマンド	『Cisco IOS IP Addressing Services Command Reference』

シスコのテクニカル サポート

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

NAT での Paired-Address-Pooling サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを

示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

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

表 *26*：*NAT* での *Paired-Address-Pooling* サポートの機能情報

機能名	リリース	機能情報
NAT での Paired-Address-Pooling サポート	Cisco IOS XE Release 3.9S	ローカル IP アドレスを常に単一のグローバル IP アドレスとして表示するネットワークアドレス変換（NAT）の機能を Paired-Address-Pooling と呼びます。Paired-Address-Pooling は、ポートアドレス変換（PAT）でのみサポートされます。 **ip nat settings pap** コマンドが導入または変更されました。

第 21 章

PPTP ポート アドレス変換

PPTP ポート アドレス変換機能では、ポート アドレス変換（PAT）設定用のポイントツーポイント トンネリング プロトコル（PPTP）アプリケーション層ゲートウェイ（ALG）をサポートしています。 PAT 設定では、PPTP ALG によって PPTP パケットを解析する必要があります。 ネットワーク アドレス変換（NAT）が設定されている場合、PPTP ALG はデフォルトでイネーブルです。

このモジュールでは、PAT 用に PPTP ALG を設定する方法について説明します。

- 機能情報の確認，349 ページ
- PPTP ポート アドレス変換の制約事項，350 ページ
- PPTP ポート アドレス変換について，350 ページ
- PPTP ポート アドレス変換の設定方法，351 ページ
- PPTP ポート アドレス変換の設定例，353 ページ
- PPTP ポート アドレス変換に関するその他の関連資料，353 ページ
- PPTP ポート アドレス変換の機能情報，354 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

PPTP ポート アドレス変換の制約事項

- ポイントツーポイント トンネリング プロトコル（PPTP）アプリケーション層ゲートウェイ（ALG）では、仮想 TCP（vTCP）および TCP セグメントをサポートしません。
- NAT クライアントとサーバが同じコール ID を使用している場合、PPTP ALG は、キャリア グレード ネットワーク アドレス変換（NAT）モードでは動作しません。

PPTP ポート アドレス変換について

PPTP ALG サポートの概要

ポイントツーポイント トンネリング プロトコル（PPTP）は、TCP/IP ベースのデータ ネットワークに VPN を作成することにより、リモート クライアントからエンタープライズ サーバへのデータのセキュアな転送を可能にするネットワーク プロトコルです。 PPTP では、インターネットまたはその他のパブリック TCP/IP ベースのネットワーク経由での伝送用に PPP パケットを IP データグラムにカプセル化します。

PPTP は、通信している PPTP ネットワーク サーバ（PNS）と PPTP アクセス コンセントレータ（PAC）のペアごとにトンネルを確立します。 トンネルが設定されると、PPP パケットは、拡張総称ルーティング カプセル化（GRE）を使用して交換されます。 GRE ヘッダー内に存在するコール ID が特定の PPP パケットが属するセッションを示します。

ネットワーク アドレス変換（NAT）は、PPTP メッセージの IP アドレスとポート番号のみを変換します。 スタティックおよびダイナミック NAT 設定は、PPTP アプリケーション層ゲートウェイ（ALG）がなくても、PPTP で動作します。 ただし、ポート アドレス変換（PAT）設定では、PPTP ヘッダーを解析し、PPTP 制御パケットのコール ID の変換を容易にするために PPTP ALG を必要とします。 次に NAT は、GRE ヘッダーを解析し、PPTP データ セッション用にコール ID を変換します。 PPTP ALG は、PPTP ペイロード内の埋め込み IP アドレスは変換しません。 NAT が設定されている場合、PPTP ALG はデフォルトでイネーブルです。

NAT ではデフォルト TCP ポート（1723）で受信する PPTP パケットを認識し、制御パケットを解析するために PPTP ALG を呼び出します。 NAT はグローバル アドレスまたはポート番号を割り当てて、PPTP ALG により解析されるコール ID を変換します。 クライアントおよびサーバのコール ID に基づいて、NAT では PPTP ALG の要求に基づく 2 つのドアを作成します。（ドアは、完全な NAT セッション エントリを作成するために十分な情報がない場合に作成されます。 ドアには、送信元 IP アドレスおよび宛先 IP アドレスとポートに関する情報が含まれます）。クライアントとサーバ間の双方向データ通信用に、2 つの NAT セッションが作成されます（1 つはサーバのコール ID で、もう 1 つはクライアントのコール ID で作成されます）。 NAT では、RFC 2673 に準拠するデータ パケットの GRE パケット ヘッダーを変換します。

PPTP は TCP ベースのプロトコルです。 したがって、NAT が PPTP パケットとして TCP パケットを認識すると、PPTP ALG 解析コールバック関数が呼び出されます。 PPTP ALG は、PPTP ヘッダーから埋め込みコール ID を取得し、ヘッダーの変換トークンを作成します。 また、PPTP ALG

は、関連する GRE トンネルの D チャネルを作成します。 ALG 解析後、NAT は ALG によって作成されたトークンを処理します。

PPTP ポート アドレス変換の設定方法

ポート アドレス変換用の PPTP ALG の設定

ネットワーク アドレス変換（NAT）が設定されている場合、ポイントツーポイント トンネリング プロトコル（PPTP）アプリケーション層ゲートウェイ（ALG）はデフォルトでイネーブルです。 PPTP ALG をディセーブルにするには、**no ip nat service pptp** コマンドを使用します。 アプリケーションの PPTP ALG 変換を再びイネーブルにするには、**ip nat service pptp** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip nat inside**
5. **exit**
6. **interface** *type number*
7. **ip nat outside**
8. **exit**
9. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
10. **ip nat inside source list** {*access-list-number* | *access-list-name*} **pool** *name* **overload**
11. **ip access-list standard** *access-list-name*
12. **permit** *host-ip*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	インターフェイスをイネーブルにし、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip nat inside** 例： `Device(config-if)# ip nat inside`	NATの対象となる内部ネットワークにインターフェイスを接続します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 6	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/0`	インターフェイスをイネーブルにし、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip nat outside** 例： `Device(config-if)# ip nat outside`	外部ネットワークにインターフェイスを接続します。
ステップ 8	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 9	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} 例： `Device(config)# ip nat pool pptp-pool 192.168.0.1 192.168.0.234 prefix-length 24`	NAT 変換で使用される IP アドレス プールを定義します。
ステップ 10	**ip nat inside source list** {*access-list-number* | *access-list-name*} **pool** *name* **overload** 例： `Device(config)# ip nat inside source list pptp-acl pool pptp-pool overload`	内部送信元アドレスの NAT をイネーブルにします。 • オーバーロードが設定されている場合、各内部ホストの TCP または UDP ポート番号により、同じローカル IP アドレスを使用して複数の会話が区別されます。
ステップ 11	**ip access-list standard** *access-list-name* 例： `Device(config)# ip access-list standard pptp-acl`	パケット フィルタリングをイネーブルにするために標準 IP アクセス リストを名前で定義し、標準アクセス リスト コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 12	**permit** *host-ip* 例： `Device(config-std-nacl)# permit 10.1.1.1`	名前付き IP アクセス リストに、パケットを許可する条件を設定します。
ステップ 13	**end** 例： `Device(config-std-nacl)# end`	標準アクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

PPTP ポート アドレス変換の設定例

例：ポート アドレス変換用の PPTP ALG の設定

```
Device# configure terminal
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# ip nat inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/0
Device(config-if)# ip nat outside
Device(config-if)# exit
Device(config)# ip nat pool pptp-pool 192.168.0.1 192.168.0.234 prefix-length 24
Device(config)# ip nat inside source list pptp-acl pool pptp-pool overload
Device(config)# ip access-list standard pptp-acl
Device(config-std-nacl)# permit 10.1.1.1
Device(config-std-nacl)# end
```

PPTP ポート アドレス変換に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
NAT コマンド	『Cisco IOS IP Addressing Services Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 2637	『*Point-to-Point Tunneling Protocol (PPTP)*』

シスコのテクニカル サポート

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

PPTP ポート アドレス変換の機能情報

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

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

表 *27* : *PPTP* ポート アドレス変換の機能情報

機能名	リリース	機能情報
PPTP ポート アドレス変換サポート	Cisco IOS XE Release 3.9S	PPTP ポート アドレス変換サポート機能では、ポート アドレス変換（PAT）設定用のポイントツーポイント トンネリング プロトコル（PPTP）アプリケーション層ゲートウェイ（ALG）を導入しています。 PAT 設定では、PPTP ALG によって PPTP パケットを解析する必要があります。 ネットワーク アドレス変換（NAT）が設定されている場合、PPTP ALG はデフォルトでイネーブルです。 コマンド **debug platform hardware qfp feature alg datapath pptp**、**ip nat service pptp**、**show platform hardware qfp feature alg statistics pptp** が導入または変更されました。